Introduction to First-Order Satisfiability

IA085: Satisfiability and Automated Reasoning

Martin Jonáš

FI MUNI, Spring 2024

Where are we?

Satisfiability modulo theories (SMT)

- $x = 1 \land x = y + y \land y > 0$
- is it satisfiable over reals?
- is it satisfiable over integers?
- is it satisfiable over integers represented by 8 bits?
- is it satisfiable over floating point numbers represented by 32 bits?

For next four lectures, we will be dealing mostly with quantifier-free formulas.

Applications

SMT solvers are widely used in practice

- planning
- scheduling
- verification of hardware
- compiler optimizations
- verification of software
- ...

Applications

```
int x = read();
int y = read();
int z = read();
if (x > 10 && y != 0)
{
  print(z / (x + y));
}
```

Contains division by zero precisely if the formula

$$x > 10 \quad \wedge \quad \neg(y = 0) \quad \wedge \quad x + y = 0$$

is satisfiable.

First-order logic

First-Order Logic

Propositional logic speaks only about atomic propositions

- are true or false
- have no internal structure

First-order logic speaks about objects, their properties and relations among them.

First-Order Logic

Propositional logic speaks only about atomic propositions

- are true or false
- have no internal structure

First-order logic speaks about objects, their properties and relations among them.
Examples

- $\exists s.\, \mathrm{Human}(s) \;\wedge\; \mathrm{Mortal}(s).$
- $\forall s.\, \mathrm{Human}(s) \;\rightarrow\; \mathrm{Mortal}(s).$
- $\exists x \exists y.\, x < 5 \;\wedge\; y < 3 \;\wedge\; 2 \cdot (x + y) > 20.$

First-Order Logic

Propositional logic speaks only about atomic propositions

- are true or false
- have no internal structure

First-order logic speaks about objects, their properties and relations among them.
Examples

- $\exists s.\, \mathrm{Human}(s) \ \wedge \ \mathrm{Mortal}(s).$
- $\forall s.\, \mathrm{Human}(s) \ \rightarrow \ \mathrm{Mortal}(s).$
- $\exists x \exists y.\, x < 5 \ \wedge \ y < 3 \ \wedge \ 2 \cdot (x + y) > 20.$

First-Order Logic

Propositional logic speaks only about atomic propositions

- are true or false
- have no internal structure

First-order logic speaks about objects, their properties and relations among them.
Examples

- $\exists s.\, \mathrm{Human}(s) \ \wedge\ \mathrm{Mortal}(s).$
- $\forall s.\, \mathrm{Human}(s) \ \rightarrow\ \mathrm{Mortal}(s).$
- $\exists x \exists y.\, x < 5 \ \wedge\ y < 3 \ \wedge\ 2 \cdot (x + y) > 20.$

In addition to logical symbols, first-order formulas contain variables, constant symbols, function symbols, and predicate symbols.

First-Order Logic – Syntax

Suppose we have

- a set $\Sigma^F = \{f, g, \ldots\}$ of function symbols and
- a set $\Sigma^P = \{R, S, \ldots\}$ of predicate symbols.

Each function symbol f and predicate symbol P has its arity $\mathrm{ar}(f)$ and $\mathrm{ar}(P)$.
Function symbols of arity 0 are called constants.

The set $\Sigma = \Sigma^F \cup \Sigma^P$ is called a signature.

Example

- $\Sigma^F = \{+, -, 0, 1\}$
- $\Sigma^P = \{=, \leq\}$

(Σ-)Term

1. a variable – $x, y, z, \ldots$
2. a function symbol applied to $\mathrm{ar}(f)$ terms – $f(x)$, $g(f(x), y)$, ...

(Σ-)Term

1. a variable – $x, y, z, \ldots$
2. a function symbol applied to $\mathrm{ar}(f)$ terms – $f(x)$, $g(f(x), y)$, ...

(Σ)-Literal

1. a predicate symbol applied to $\mathrm{ar}(P)$ terms – $R(x), S(f(x), y), \ldots$
2. a negation of predicate symbol applied to $\mathrm{ar}(P)$ terms – $\neg R(x), \neg S(f(x), y), \ldots$

First-Order Logic – Syntax

(Σ-)Term

1. a variable – $x, y, z, \ldots$
2. a function symbol applied to $\mathrm{ar}(f)$ terms – $f(x)$, $g(f(x), y)$, ...

(Σ)-Literal

1. a predicate symbol applied to $\mathrm{ar}(P)$ terms – $R(x), S(f(x), y), \ldots$
2. a negation of predicate symbol applied to $\mathrm{ar}(P)$ terms – $\neg R(x), \neg S(f(x), y), \ldots$

(Σ)-Formula

1. a Boolean combination of literals – $(R(x) \vee \neg R(y)) \wedge S(f(x), y), \ldots$
2. a quantifier applied to a formula – $\forall x \left(R(x)\right), \ldots$.

First-Order Logic – Syntactic Conventions and Terminology

Notation

- instead of $+(r, s)$ write $r + s$ (also for other infix function symbols)
- instead of $\leq (r, s)$ write $r \leq s$ (also for other infix predicate symbols)
- instead of 1() write 1 (also for other constants)
- instead of $\forall x \forall y (\varphi \wedge \psi)$ write $\forall x \forall y.\, \varphi \wedge \psi$

Terminology

- an occurrence of a variable is free if it is not bound by a quantifier
- a formula without free occurrences of variables is closed or a sentence

First-Order Logic – Semantics

Is the following formula true?

$$\forall x \exists y.\, x < y \;\wedge\; y < x + 1$$

First-Order Logic – Semantics

Is the following formula true?

$$\forall x \exists y.\, x < y \ \wedge\ y < x + 1$$

It depends.

First-Order Logic – Semantics

Is the following formula true?

$$\forall x \exists y.\, x < y \ \land \ y < x + 1$$

It depends.

- What is the domain of x and y?
- What does the function symbol $+$ mean?
- What does the predicate symbol $<$ mean?

First-Order Logic – Semantics

Is the following formula true?

$$\forall x \exists y.\, x < y \;\wedge\; y < x + 1$$

It depends.

- What is the domain of x and y?
- What does the function symbol $+$ mean?
- What does the predicate symbol $<$ mean?

Is the following formula true?

$$\forall x \exists y.\, x < y \;\wedge\; y < x + 1$$

It depends.

- What is the domain of x and y?
- What does the function symbol $+$ mean?
- What does the predicate symbol $<$ mean?

Meaning of these three things is given by a Σ-structure.

Σ-structure $\mathcal{A}$

- determines the set of objects and behavior of functions/predicates
- a pair of
  1. a non-empty set A called the universe,
  2. a map $(\_)^{\mathcal{A}}$ that
     - to each $f \in \Sigma^F$ assigns a function $f^{\mathcal{A}} \colon A^{\mathrm{ar}(f)} \to A$,
     - to each $R \in \Sigma^P \setminus \{=\}$ assigns a relation $R^{\mathcal{A}} \subseteq A^{\mathrm{ar}(R)}$,
     - we suppose that $=^A$ is the identity relation.

$\mathcal{A} = \big(A, (\_)^{\mathcal{A}}\big)$ where

$$
\begin{aligned}
A &= \mathbb{Z} \\
+^{\mathcal{A}}(x, y) &= x + y \\
<^{\mathcal{A}} &= \{(x, y) \mid x < y\} \\
1^{\mathcal{A}} &= 1
\end{aligned}
$$

First-Order Logic – Structure Examples

$\mathcal{A} = \big(A, (\_)^{\mathcal{A}}\big)$ where

$$\begin{aligned} A &= \mathbb{Z} \\ +^{\mathcal{A}}(x, y) &= x + y \\ <^{\mathcal{A}} &= \{(x, y) \mid x < y\} \\ 1^{\mathcal{A}} &= 1 \end{aligned}$$

$\mathcal{B} = \big(B, (\_)^{\mathcal{B}}\big)$ where

$$\begin{aligned} B &= \{\circ, \bullet\} \\ +^{\mathcal{B}}(x, y) &= y \\ <^{\mathcal{B}} &= \{(\circ, \circ), (\bullet, \circ)\} \\ 1^{\mathcal{B}} &= \bullet \end{aligned}$$

First-Order Logic – Interpretation

The formulas can also contain free variables.

Valuation for a Σ-structure $\mathcal{A} = (A, (\_)^{\mathcal{A}})$

- determines the values of the variables
- a map $\mu \colon \mathit{Vars} \to A$

Σ-interpretation

- a pair $(\mathcal{A}, \mu)$ of a Σ-structure and a valuation

Given an interpretation $\mathcal{I} = (\mathcal{A}, \mu)$, we can evaluate

- each term t to a value $[\![t]\!]^{\mathcal{I}} \in A$
- each formula φ to a value $[\![\varphi]\!]^{\mathcal{I}} \in \{\top, \bot\}$

$\mathcal{A} = \big(\mathbb{Z}, (\_)^{\mathcal{A}}\big)$ where

$$\begin{aligned} +^{\mathcal{A}}(x, y) &= x + y \\ <^{\mathcal{A}} &= \{(x, y) \mid x < y\} \\ 1^{\mathcal{A}} &= 1 \end{aligned}$$

First-Order Logic – Evaluation

$\mathcal{A} = (\mathbb{Z}, (\_)^{\mathcal{A}})$ where

$$
\begin{aligned}
+^{\mathcal{A}}(x, y) &= x + y \\
<^{\mathcal{A}} &= \{(x, y) \mid x < y\} \\
1^{\mathcal{A}} &= 1
\end{aligned}
$$

Given $\mu(x) = 1, \mu(y) = 3$:

- $[\![y + 1]\!]^{(\mathcal{A},\mu)} \ =$

$\mathcal{A} = (\mathbb{Z}, (\_)^{\mathcal{A}})$ where

$$
\begin{aligned}
+^{\mathcal{A}}(x, y) &= x + y \\
<^{\mathcal{A}} &= \{(x, y) \mid x < y\} \\
1^{\mathcal{A}} &= 1
\end{aligned}
$$

Given $\mu(x) = 1, \mu(y) = 3$:

- $[\![y + 1]\!]^{(\mathcal{A},\mu)} \; = \; 4$
- $[\![y + 1 < x]\!]^{(\mathcal{A},\mu)} \; =$

$\mathcal{A} = (\mathbb{Z}, (\_)^{\mathcal{A}})$ where

$$
\begin{aligned}
+^{\mathcal{A}}(x, y) &= x + y \\
<^{\mathcal{A}} &= \{(x, y) \mid x < y\} \\
1^{\mathcal{A}} &= 1
\end{aligned}
$$

Given $\mu(x) = 1, \mu(y) = 3$:

- $[\![y + 1]\!]^{(\mathcal{A},\mu)} \ = \ 4$
- $[\![y + 1 < x]\!]^{(\mathcal{A},\mu)} \ = \ \bot$
- $[\![(x < y) \wedge (y + 1 < x)]\!]^{(\mathcal{A},\mu)} \ =$

$\mathcal{A} = \left(\mathbb{Z}, (\_)^{\mathcal{A}}\right)$ where

$$+^{\mathcal{A}}(x,y) = x + y$$
$$<^{\mathcal{A}} = \{(x,y) \mid x < y\}$$
$$1^{\mathcal{A}} = 1$$

Given $\mu(x) = 1, \mu(y) = 3$:

- $[\![y+1]\!]^{(\mathcal{A},\mu)} \;=\; 4$
- $[\![y+1 < x]\!]^{(\mathcal{A},\mu)} \;=\; \bot$
- $[\![(x<y) \wedge (y+1<x)]\!]^{(\mathcal{A},\mu)} \;=\; \bot$

$\mathcal{B} = \left(\{\circ, \bullet\}, (\_)^{\mathcal{B}}\right)$ where

$$+^{\mathcal{B}}(x,y) = y$$
$$<^{\mathcal{B}} = \{(\circ,\circ), (\bullet,\circ)\}$$
$$1^{\mathcal{B}} = \bullet$$

Given $\mu(x) = \circ, \mu(y) = \circ$:

- $[\![y+1]\!]^{(\mathcal{B},\mu)} \;=$

First-Order Logic – Evaluation

$\mathcal{A} = (\mathbb{Z}, (\_)^{\mathcal{A}})$ where

$$+^{\mathcal{A}}(x,y) = x + y$$
$$<^{\mathcal{A}} = \{(x,y) \mid x < y\}$$
$$1^{\mathcal{A}} = 1$$

Given $\mu(x) = 1, \mu(y) = 3$:

- $[\![y+1]\!]^{(\mathcal{A},\mu)} \;=\; 4$
- $[\![y+1 < x]\!]^{(\mathcal{A},\mu)} \;=\; \bot$
- $[\![(x<y) \wedge (y+1<x)]\!]^{(\mathcal{A},\mu)} \;=\; \bot$

$\mathcal{B} = (\{\circ, \bullet\}, (\_)^{\mathcal{B}})$ where

$$+^{\mathcal{B}}(x,y) = y$$
$$<^{\mathcal{B}} = \{(\circ,\circ), (\bullet,\circ)\}$$
$$1^{\mathcal{B}} = \bullet$$

Given $\mu(x) = \circ, \mu(y) = \circ$:

- $[\![y+1]\!]^{(\mathcal{B},\mu)} \;=\; \bullet$
- $[\![y+1 < x]\!]^{(\mathcal{B},\mu)} \;=$

First-Order Logic – Evaluation

$\mathcal{A} = (\mathbb{Z}, (\_)^{\mathcal{A}})$ where

$$+^{\mathcal{A}}(x, y) = x + y$$
$$<^{\mathcal{A}} = \{(x, y) \mid x < y\}$$
$$1^{\mathcal{A}} = 1$$

Given $\mu(x) = 1, \mu(y) = 3$:

- $[\![y + 1]\!]^{(\mathcal{A},\mu)} \;=\; 4$
- $[\![y + 1 < x]\!]^{(\mathcal{A},\mu)} \;=\; \bot$
- $[\![(x < y) \wedge (y + 1 < x)]\!]^{(\mathcal{A},\mu)} \;=\; \bot$

$\mathcal{B} = (\{\circ, \bullet\}, (\_)^{\mathcal{B}})$ where

$$+^{\mathcal{B}}(x, y) = y$$
$$<^{\mathcal{B}} = \{(\circ, \circ), (\bullet, \circ)\}$$
$$1^{\mathcal{B}} = \bullet$$

Given $\mu(x) = \circ, \mu(y) = \circ$:

- $[\![y + 1]\!]^{(\mathcal{B},\mu)} \;=\; \bullet$
- $[\![y + 1 < x]\!]^{(\mathcal{B},\mu)} \;=\; \top$
- $[\![(x < y) \wedge (y + 1 < x)]\!]^{(\mathcal{B},\mu)} \;=$

First-Order Logic – Evaluation

$\mathcal{A} = (\mathbb{Z}, (\_)^{\mathcal{A}})$ where

$$+^{\mathcal{A}}(x, y) = x + y$$
$$<^{\mathcal{A}} = \{(x, y) \mid x < y\}$$
$$1^{\mathcal{A}} = 1$$

Given $\mu(x) = 1, \mu(y) = 3$:

- $[\![y + 1]\!]^{(\mathcal{A},\mu)} = 4$
- $[\![y + 1 < x]\!]^{(\mathcal{A},\mu)} = \bot$
- $[\![(x < y) \land (y + 1 < x)]\!]^{(\mathcal{A},\mu)} = \bot$

$\mathcal{B} = (\{\circ, \bullet\}, (\_)^{\mathcal{B}})$ where

$$+^{\mathcal{B}}(x, y) = y$$
$$<^{\mathcal{B}} = \{(\circ, \circ), (\bullet, \circ)\}$$
$$1^{\mathcal{B}} = \bullet$$

Given $\mu(x) = \circ, \mu(y) = \circ$:

- $[\![y + 1]\!]^{(\mathcal{B},\mu)} = \bullet$
- $[\![y + 1 < x]\!]^{(\mathcal{B},\mu)} = \top$
- $[\![(x < y) \land (y + 1 < x)]\!]^{(\mathcal{B},\mu)} = \top$

Interpretation $\mathcal{I}$ satisfies formula φ

- if $[\![\varphi]\!]^{\mathcal{I}} = \top$
- written $\mathcal{I} \models \varphi$

Entailment and Validity

Formula φ **entails** formula ψ

- if every interpretation that satisfies φ also satisfies ψ
- written $\varphi \models \psi$
- example: $f(x) = y \land x = z \;\models\; f(z) = y$
- negative example: $x < y \;\not\models\; x + 1 < y + 1$

Formula φ is **valid**

- if every interpretation satisfies φ
- written $\models \varphi$
- example: $\models P(f(x)) \lor \neg P(f(x))$
- negative example: $\not\models x + 0 = x$

First-Order Satisfiability

Definition
Formula φ is satisfiable if there is a Σ-interpretation $(\mathcal{A}, \mu)$ such that $(\mathcal{A}, \mu) \models \varphi$.

First-Order Satisfiability

Definition
Formula φ is satisfiable if there is a Σ-interpretation $(\mathcal{A}, \mu)$ such that $(\mathcal{A}, \mu) \models \varphi$.

Is formula $(x < y) \ \wedge \ (y + 1 < x)$ satisfiable?

Definition
Formula φ is satisfiable if there is a Σ-interpretation $(\mathcal{A}, \mu)$ such that $(\mathcal{A}, \mu) \models \varphi$.

Is formula $(x < y) \;\wedge\; (y + 1 < x)$ satisfiable? Yes. ☹

First-Order Satisfiability

Definition
Formula φ is satisfiable if there is a Σ-interpretation $(\mathcal{A}, \mu)$ such that $(\mathcal{A}, \mu) \models \varphi$.

Is formula $(x < y) \ \wedge \ (y + 1 < x)$ satisfiable? Yes. ☹

Solution

Pick a subset of Σ-structures in which we are interested.

This gives rise to the Satisfiability Modulo Theories

Satisfiability Modulo Theories (SMT)

Definition
A (Σ-)theory is a set of Σ-structures.

Definition
A formula φ is satisfiable modulo theory T if there is a Σ-interpretation $(\mathcal{A}, \mu)$ with $\mathcal{A} \in T$ such that $(\mathcal{A}, \mu) \models \varphi$.

Satisfiability Modulo Theories – Example

Consider the structure $\mathcal{Z}$ with the universe $\mathbb{Z}$ and the standard interpretation of operations $+$, $<$, and 1.

The formula $(x < y) \ \wedge \ (y + 1 < x)$ is unsatisfiable modulo theory $T = \{\mathcal{Z}\}$.

The formula $(x < y) \ \wedge \ (y < x + 2)$ is satisfiable modulo theory $T = \{\mathcal{Z}\}$.

Linear Integer Arithmetic (LIA)

- $\Sigma = \{0, 1, +, -, =, \leq\}$
- T_{LIA} is a set of a single structure with $A = \mathbb{Z}$ and the standard interpretation of operations

Linear Integer Arithmetic (LIA)

- $\Sigma = \{0, 1, +, -, =, \leq\}$
- T_{LIA} is a set of a single structure with $A = \mathbb{Z}$ and the standard interpretation of operations

$$1 \leq x \quad \wedge \quad (3 \leq x + y) \quad \wedge \quad (1 \leq y)$$

T-models

$\mathcal{I} = (\mathcal{A}, \mu)$ is T-model of φ

- if $\mathcal{A} \in T$ and $[\![\varphi]\!]^{\mathcal{I}} = \top$
- written $\mathcal{I} \models_T \varphi$

Entailment and Validity

φ **T-entails** ψ

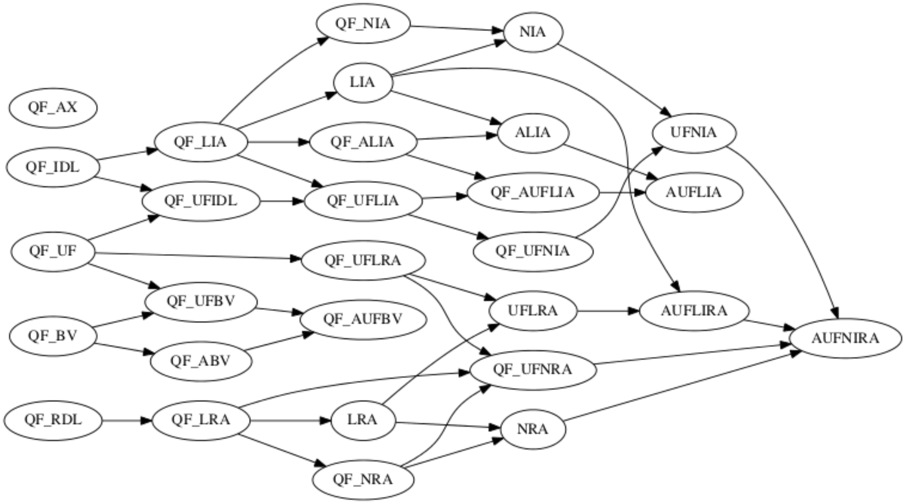
- if every T-model of φ is also a T-model of ψ
- written $\varphi \models_T \psi$
- example: $x < y \models_{T_{\mathrm{LIA}}} x + 1 < y + 1$

φ is **T-valid**

- if every $\mathcal{I} = (\mathcal{A}, \mu)$ with $\mathcal{A} \in T$ is a T-model of φ
- equivalently $\top \models_T \varphi$
- written $\models_T \varphi$
- example: $\models_{T_{\mathrm{LIA}}} x + 0 = x$

Theories of interest

Logics in SMT-LIB



[https://smtlib.cs.uiowa.edu/logics.shtml]

Linear Integer Arithmetic (LIA)

- $\Sigma = \{0, 1, +, -, =, \leq\}$
- T_{LIA} is a set of a single structure with $A = \mathbb{Z}$ and the standard interpretation of operations

Linear Integer Arithmetic (LIA)

- $\Sigma = \{0, 1, +, -, =, \leq\}$
- T_{LIA} is a set of a single structure with $A = \mathbb{Z}$ and the standard interpretation of operations

$$1 \leq x \quad \wedge \quad (3 \leq x + y) \quad \wedge \quad (1 \leq y)$$

Linear Integer Arithmetic (LIA)

- $\Sigma = \{0, 1, +, -, =, \leq\}$
- T_{LIA} is a set of a single structure with $A = \mathbb{Z}$ and the standard interpretation of operations

$$1 \leq x \quad \wedge \quad (3 \leq x + y) \quad \wedge \quad (1 \leq y)$$

- satisfiability of arbitrary formulas is decidable

Linear Integer Arithmetic (LIA)

- $\Sigma = \{0, 1, +, -, =, \leq\}$
- T_{LIA} is a set of a single structure with $A = \mathbb{Z}$ and the standard interpretation of operations

$$1 \leq x \quad \wedge \quad (3 \leq x + y) \quad \wedge \quad (1 \leq y)$$

- satisfiability of arbitrary formulas is decidable
- complexity of satisfiability of arbitrary formulas is in $\Omega(2^{2^n})$ (Fischer, Rabin, 1974)

Linear Integer Arithmetic (LIA)

- $\Sigma = \{0, 1, +, -, =, \leq\}$
- T_{LIA} is a set of a single structure with $A = \mathbb{Z}$ and the standard interpretation of operations

$$1 \leq x \quad \wedge \quad (3 \leq x + y) \quad \wedge \quad (1 \leq y)$$

- satisfiability of arbitrary formulas is decidable
- complexity of satisfiability of arbitrary formulas is in $\Omega(2^{2^n})$ (Fischer, Rabin, 1974)
- complexity of satisfiability of arbitrary formulas is in $\mathcal{O}(2^{2^{2^{kn}}})$ (Oppen, 1978)

Linear Integer Arithmetic (LIA)

- $\Sigma = \{0, 1, +, -, =, \leq\}$
- T_{LIA} is a set of a single structure with $A = \mathbb{Z}$ and the standard interpretation of operations

$$1 \leq x \quad \wedge \quad (3 \leq x + y) \quad \wedge \quad (1 \leq y)$$

- satisfiability of arbitrary formulas is decidable
- complexity of satisfiability of arbitrary formulas is in $\Omega(2^{2^n})$ (Fischer, Rabin, 1974)
- complexity of satisfiability of arbitrary formulas is in $\mathcal{O}(2^{2^{2^{kn}}})$ (Oppen, 1978)
- satisfiability of quantifier-free formulas is NP-complete

Linear Integer Arithmetic (LIA)

- $\Sigma = \{0, 1, +, -, =, \leq\}$
- T_{LIA} is a set of a single structure with $A = \mathbb{Z}$ and the standard interpretation of operations

$$1 \leq x \quad \wedge \quad (3 \leq x + y) \quad \wedge \quad (1 \leq y)$$

- satisfiability of arbitrary formulas is decidable
- complexity of satisfiability of arbitrary formulas is in $\Omega(2^{2^n})$ (Fischer, Rabin, 1974)
- complexity of satisfiability of arbitrary formulas is in $\mathcal{O}(2^{2^{2^{kn}}})$ (Oppen, 1978)
- satisfiability of quantifier-free formulas is NP-complete
- satisfiability of conjunctions of literals is NP-complete

Linear Rational Arithmetic (LRA)

- $\Sigma = \{0, 1, +, -, =, \leq\}$
- T_{LRA} is a set of a single structure with $A = \mathbb{Q}$ and the standard interpretation of operations

Linear Rational Arithmetic (LRA)

- $\Sigma = \{0, 1, +, -, =, \leq\}$
- T_{LRA} is a set of a single structure with $A = \mathbb{Q}$ and the standard interpretation of operations

$$1 \leq x \quad \wedge \quad (3 \leq x + y) \quad \wedge \quad (1 \leq y)$$

Linear Rational Arithmetic (LRA)

- $\Sigma = \{0, 1, +, -, =, \leq\}$
- T_{LRA} is a set of a single structure with $A = \mathbb{Q}$ and the standard interpretation of operations

$$1 \leq x \quad \land \quad (3 \leq x + y) \quad \land \quad (1 \leq y)$$

- satisfiability of arbitrary formulas is decidable

Linear Rational Arithmetic (LRA)

- $\Sigma = \{0, 1, +, -, =, \leq\}$
- T_{LRA} is a set of a single structure with $A = \mathbb{Q}$ and the standard interpretation of operations

$$1 \leq x \quad \wedge \quad (3 \leq x + y) \quad \wedge \quad (1 \leq y)$$

- satisfiability of arbitrary formulas is decidable
- complexity of satisfiability of arbitrary formulas is in $\Omega(2^n)$ (Fischer, Rabin, 1974)

Linear Rational Arithmetic (LRA)

- $\Sigma = \{0, 1, +, -, =, \leq\}$
- T_{LRA} is a set of a single structure with $A = \mathbb{Q}$ and the standard interpretation of operations

$$1 \leq x \quad \wedge \quad (3 \leq x + y) \quad \wedge \quad (1 \leq y)$$

- satisfiability of arbitrary formulas is decidable
- complexity of satisfiability of arbitrary formulas is in $\Omega(2^n)$ (Fischer, Rabin, 1974)
- complexity of satisfiability of arbitrary formulas is in $\mathcal{O}(2^{2^{kn}})$ (Ferrante, Rackoff, 1975)

Linear Rational Arithmetic (LRA)

- $\Sigma = \{0, 1, +, -, =, \leq\}$
- T_{LRA} is a set of a single structure with $A = \mathbb{Q}$ and the standard interpretation of operations

$$1 \leq x \quad \wedge \quad (3 \leq x + y) \quad \wedge \quad (1 \leq y)$$

- satisfiability of arbitrary formulas is decidable
- complexity of satisfiability of arbitrary formulas is in $\Omega(2^n)$ (Fischer, Rabin, 1974)
- complexity of satisfiability of arbitrary formulas is in $\mathcal{O}(2^{2^{kn}})$ (Ferrante, Rackoff, 1975)
- satisfiability of quantifier-free formulas is NP-complete

- $\Sigma = \{0, 1, +, -, =, \leq\}$
- T_{LRA} is a set of a single structure with $A = \mathbb{Q}$ and the standard interpretation of operations

$$1 \leq x \quad \wedge \quad (3 \leq x + y) \quad \wedge \quad (1 \leq y)$$

- satisfiability of arbitrary formulas is decidable
- complexity of satisfiability of arbitrary formulas is in $\Omega(2^n)$ (Fischer, Rabin, 1974)
- complexity of satisfiability of arbitrary formulas is in $\mathcal{O}(2^{2^{kn}})$ (Ferrante, Rackoff, 1975)
- satisfiability of quantifier-free formulas is NP-complete
- satisfiability of conjunctions of literals in P (Khachiyan, 1979)

Theory of Non-Linear Integer Arithmetic (NIA)

- $\Sigma = \{0, 1, +, -, \cdot, =, \leq\}$
- T_{NIA} is a set of a single structure with $A = \mathbb{Z}$ and the standard interpretation of operations

Theory of Non-Linear Integer Arithmetic (NIA)

- $\Sigma = \{0, 1, +, -, \cdot, =, \leq\}$
- T_{NIA} is a set of a single structure with $A = \mathbb{Z}$ and the standard interpretation of operations

$$1 \leq x \quad \wedge \quad (3 \leq x \cdot y) \quad \wedge \quad (1 \leq y)$$

Theory of Non-Linear Integer Arithmetic (NIA)

- $\Sigma = \{0, 1, +, -, \cdot, =, \leq\}$
- T_{NIA} is a set of a single structure with $A = \mathbb{Z}$ and the standard interpretation of operations

$$1 \leq x \quad \wedge \quad (3 \leq x \cdot y) \quad \wedge \quad (1 \leq y)$$

- satisfiability of conjunctions of quantifier-free formulas is undecidable (Matiyasevich, 1971)

Non-Linear Real Arithmetic (NRA)

- $\Sigma = \{0, 1, +, -, \cdot, =, \leq\}$
- T_{NRA} is a set of a single structure with $A = \mathbb{R}$ and the standard interpretation of operations

Non-Linear Real Arithmetic (NRA)

- $\Sigma = \{0, 1, +, -, \cdot, =, \leq\}$
- T_{NRA} is a set of a single structure with $A = \mathbb{R}$ and the standard interpretation of operations

$$1 \leq x \quad \wedge \quad (3 \leq x \cdot y) \quad \wedge \quad (1 \leq y)$$

Non-Linear Real Arithmetic (NRA)

- $\Sigma = \{0, 1, +, -, \cdot, =, \leq\}$
- T_{NRA} is a set of a single structure with $A = \mathbb{R}$ and the standard interpretation of operations

$$1 \leq x \quad \wedge \quad (3 \leq x \cdot y) \quad \wedge \quad (1 \leq y)$$

- satisfiability of arbitrary formulas is decidable (Tarski, 1951)

Non-Linear Real Arithmetic (NRA)

- $\Sigma = \{0, 1, +, -, \cdot, =, \leq\}$
- T_{NRA} is a set of a single structure with $A = \mathbb{R}$ and the standard interpretation of operations

$$1 \leq x \quad \wedge \quad (3 \leq x \cdot y) \quad \wedge \quad (1 \leq y)$$

- satisfiability of arbitrary formulas is decidable (Tarski, 1951)
- complexity of satisfiability of arbitrary formulas is in $\mathcal{O}(2^{2^{kn}})$ (Collins, 1975)

Non-Linear Real Arithmetic (NRA)

- $\Sigma = \{0, 1, +, -, \cdot, =, \leq\}$
- T_{NRA} is a set of a single structure with $A = \mathbb{R}$ and the standard interpretation of operations

$$1 \leq x \quad \land \quad (3 \leq x \cdot y) \quad \land \quad (1 \leq y)$$

- satisfiability of arbitrary formulas is decidable (Tarski, 1951)
- complexity of satisfiability of arbitrary formulas is in $\mathcal{O}(2^{2^{kn}})$ (Collins, 1975)
- complexity of satisfiability of conjunctions of literals in $\mathcal{O}(2^{2^{kn}})$

Arrays (A)

- $\Sigma = \{\mathrm{read}, \mathrm{write}, =\}$
- T_A is a set of structures, where A is a set of arrays and elements and
  - $\mathrm{read}(a, i)$ is interpreted as an element on index i of array a
  - $\mathrm{write}(a, i, v)$ is interpreted as an array a after replacing element on index i by v
  - equality is defined only for elements

Arrays (A)

- $\Sigma = \{\mathrm{read}, \mathrm{write}, =\}$
- T_A is a set of structures, where A is a set of arrays and elements and
  - $\mathrm{read}(a, i)$ is interpreted as an element on index i of array a
  - $\mathrm{write}(a, i, v)$ is interpreted as an array a after replacing element on index i by v
  - equality is defined only for elements

$$\mathrm{read}(a, i) = u \quad \wedge \quad (\mathrm{read}(a, i) = \mathrm{read}(\mathrm{write}(a, i, v), i))$$

Arrays (A)

- $\Sigma = \{\mathrm{read}, \mathrm{write}, =\}$
- T_A is a set of structures, where A is a set of arrays and elements and
  - $\mathrm{read}(a, i)$ is interpreted as an element on index i of array a
  - $\mathrm{write}(a, i, v)$ is interpreted as an array a after replacing element on index i by v
  - equality is defined only for elements

$$\mathrm{read}(a, i) = u \quad \wedge \quad (\mathrm{read}(a, i) = \mathrm{read}(\mathrm{write}(a, i, v), i))$$

- satisfiability of arbitrary formulas is undecidable

Arrays (A)

- $\Sigma = \{\mathrm{read}, \mathrm{write}, =\}$
- T_A is a set of structures, where A is a set of arrays and elements and
  - $\mathrm{read}(a, i)$ is interpreted as an element on index i of array a
  - $\mathrm{write}(a, i, v)$ is interpreted as an array a after replacing element on index i by v
  - equality is defined only for elements

$$\mathrm{read}(a, i) = u \quad \wedge \quad (\mathrm{read}(a, i) = \mathrm{read}(\mathrm{write}(a, i, v), i))$$

- satisfiability of arbitrary formulas is undecidable
- satisfiability of quantifier-free formulas is NP-complete

Arrays with Extensionality (AX)

- $\Sigma = \{\mathrm{read}, \mathrm{write}, =\}$
- T_A is a set of structures where A is a set of arrays and elements and
  - $\mathrm{read}(a, i)$ is interpreted as an element on index i of array a
  - $\mathrm{write}(a, i, v)$ is interpreted as an array a after replacing element on index i by v

Arrays with Extensionality (AX)

- $\Sigma = \{\mathrm{read}, \mathrm{write}, =\}$
- T_A is a set of structures where A is a set of arrays and elements and
  - $\mathrm{read}(a, i)$ is interpreted as an element on index i of array a
  - $\mathrm{write}(a, i, v)$ is interpreted as an array a after replacing element on index i by v

$$\mathrm{read}(a, i) = u \quad \wedge \quad (b = \mathrm{write}(a, i, v)) \quad \wedge \quad (a = b)$$

Arrays with Extensionality (AX)

- $\Sigma = \{\mathrm{read}, \mathrm{write}, =\}$
- T_A is a set of structures where A is a set of arrays and elements and
  - $\mathrm{read}(a, i)$ is interpreted as an element on index i of array a
  - $\mathrm{write}(a, i, v)$ is interpreted as an array a after replacing element on index i by v

$$\mathrm{read}(a, i) = u \quad \wedge \quad (b = \mathrm{write}(a, i, v)) \quad \wedge \quad (a = b)$$

- satisfiability of arbitrary formulas is undecidable

Arrays with Extensionality (AX)

- $\Sigma = \{\mathrm{read}, \mathrm{write}, =\}$
- T_A is a set of structures where A is a set of arrays and elements and
  - $\mathrm{read}(a, i)$ is interpreted as an element on index i of array a
  - $\mathrm{write}(a, i, v)$ is interpreted as an array a after replacing element on index i by v

$$\mathrm{read}(a, i) = u \quad \wedge \quad (b = \mathrm{write}(a, i, v)) \quad \wedge \quad (a = b)$$

- satisfiability of arbitrary formulas is undecidable
- satisfiability of quantifier-free formulas is NP-complete

Fixed-Size Bit-Vectors (BV)

- $\Sigma = \{+_{[k]}, \times_{[k]}, \&_{[k]}, =, <^u_{[k]}, <^s_{[k]}$ $1_{[k]}, 2_{[k]}\}$ and many more
- T_{BV} is a set of structures where BV is a set of finite sequences of bits (bit-vectors) and
  - $+_{[k]}$ adds two sequences of k-bits representing unsigned integers and returns a sequence of k-bits
  - $1_{[k]}$ is a sequence of k-bits that represents unsigned number 1
  - $\dots$

Fixed-Size Bit-Vectors (BV)

- $\Sigma = \{+_{[k]}, \times_{[k]}, \&_{[k]}, =, <^u_{[k]}, <^s_{[k]}\ 1_{[k]}, 2_{[k]}\}$ and many more
- T_{BV} is a set of structures where BV is a set of finite sequences of bits (bit-vectors) and
  - $+_{[k]}$ adds two sequences of k-bits representing unsigned integers and returns a sequence of k-bits
  - $1_{[k]}$ is a sequence of k-bits that represents unsigned number 1
  - $\ldots$

$$x +_{[8]} 2_{[8]} \quad <^u_{[8]} \quad x_{[8]}$$

Fixed-Size Bit-Vectors (BV)

- $\Sigma = \{+_{[k]}, \times_{[k]}, \&_{[k]}, =, <^u_{[k]}, <^s_{[k]}\ 1_{[k]}, 2_{[k]}\}$ and many more
- T_{BV} is a set of structures where BV is a set of finite sequences of bits (bit-vectors) and
  - $+_{[k]}$ adds two sequences of k-bits representing unsigned integers and returns a sequence of k-bits
  - $1_{[k]}$ is a sequence of k-bits that represents unsigned number 1
  - $\ldots$

$$x +_{[8]} 2_{[8]} \quad <^u_{[8]} \quad x_{[8]}$$

- satisfiability of arbitrary formulas is PSPACE-complete

Fixed-Size Bit-Vectors (BV)

- $\Sigma = \{+_{[k]}, \times_{[k]}, \&_{[k]}, =, <^u_{[k]}, <^s_{[k]}\ 1_{[k]}, 2_{[k]}\}$ and many more
- T_{BV} is a set of structures where BV is a set of finite sequences of bits (bit-vectors) and
  - $+_{[k]}$ adds two sequences of k-bits representing unsigned integers and returns a sequence of k-bits
  - $1_{[k]}$ is a sequence of k-bits that represents unsigned number 1
  - $\ldots$

$$x +_{[8]} 2_{[8]} \quad <^u_{[8]} \quad x_{[8]}$$

- satisfiability of arbitrary formulas is PSPACE-complete
- satisfiability of quantifier-free formulas is NP-complete

Equality and Uninterpreted Functions (UF)

- $\Sigma = \{=, f, g, h, \ldots\}$
- T_{UF} is a set of all Σ-structures

Equality and Uninterpreted Functions (UF)

- $\Sigma = \{=, f, g, h, \dots\}$
- T_{UF} is a set of all Σ-structures

$$x = v \ \wedge\ y = g(z) \quad \wedge \quad f(g(x)) \neq f(y) \quad \wedge \quad z = v$$

Equality and Uninterpreted Functions (UF)

- $\Sigma = \{=, f, g, h, \ldots\}$
- T_{UF} is a set of all Σ-structures

$$x = v \ \wedge \ y = g(z) \quad \wedge \quad f(g(x)) \neq f(y) \quad \wedge \quad z = v$$

- satisfiability of arbitrary formulas is undecidable

Equality and Uninterpreted Functions (UF)

- $\Sigma = \{=, f, g, h, \ldots\}$
- T_{UF} is a set of all Σ-structures

$$x = v \ \wedge\ y = g(z) \quad \wedge \quad f(g(x)) \neq f(y) \quad \wedge \quad z = v$$

- satisfiability of arbitrary formulas is undecidable
- satisfiability of quantifier-free formulas is decidable (Ackermann, 1954)

Equality and Uninterpreted Functions (UF)

- $\Sigma = \{=, f, g, h, \ldots\}$
- T_{UF} is a set of all Σ-structures

$$x = v \;\wedge\; y = g(z) \quad\wedge\quad f(g(x)) \neq f(y) \quad\wedge\quad z = v$$

- satisfiability of arbitrary formulas is undecidable
- satisfiability of quantifier-free formulas is decidable (Ackermann, 1954)
- satisfiability of quantifier-free formulas is NP-complete

Equality and Uninterpreted Functions (UF)

- $\Sigma = \{=, f, g, h, \ldots\}$
- T_{UF} is a set of all Σ-structures

$$x = v \;\wedge\; y = g(z) \quad \wedge \quad f(g(x)) \neq f(y) \quad \wedge \quad z = v$$

- satisfiability of arbitrary formulas is undecidable
- satisfiability of quantifier-free formulas is decidable (Ackermann, 1954)
- satisfiability of quantifier-free formulas is NP-complete
- satisfiability of conjunctions of literals is in $\mathcal{O}(n \cdot \log(n))$

More theories

- theory of strings ($s_1 \mathbin{+\!\!+}\ s_2$, $\mathrm{len}(s)$, $\mathrm{substr}(s, \mathit{from}, \mathit{to})$, $\mathrm{contains}(s_1, s_2)$, $\ldots$)

More theories

- theory of strings ($s_1 \mathbin{+\!\!+} s_2$, $\mathrm{len}(s)$, $\mathrm{substr}(s, \mathit{from}, \mathit{to})$, $\mathrm{contains}(s_1, s_2)$, $\ldots$)
- theory of lists,

More theories

- theory of strings ($s_1 \mathbin{+\!\!+}\ s_2, \mathrm{len}(s), \mathrm{substr}(s, \mathit{from}, \mathit{to}), \mathrm{contains}(s_1, s_2), \ldots$)
- theory of lists,
- theory of floating point numbers (IEEE-754),

More theories

- theory of strings ($s_1 + s_2$, $\mathrm{len}(s)$, $\mathrm{substr}(s, \mathit{from}, \mathit{to})$, $\mathrm{contains}(s_1, s_2)$, $\ldots$)
- theory of lists,
- theory of floating point numbers (IEEE-754),
- theory of recursive data structures,

More theories

- theory of strings ($s_1 \mathbin{+\!\!+} s_2$, $\mathrm{len}(s)$, $\mathrm{substr}(s, \mathit{from}, \mathit{to})$, $\mathrm{contains}(s_1, s_2)$, $\ldots$)
- theory of lists,
- theory of floating point numbers (IEEE-754),
- theory of recursive data structures,
- theory of groups,

More theories

- theory of strings ($s_1 +\!\!+\ s_2, \mathrm{len}(s), \mathrm{substr}(s, \mathit{from}, \mathit{to}), \mathrm{contains}(s_1, s_2), \ldots$)
- theory of lists,
- theory of floating point numbers (IEEE-754),
- theory of recursive data structures,
- theory of groups,
- ...

Standard view of theories

Definition
A (Σ-)theory is a set of closed Σ-formulas.

Definition
A formula φ is satisfiable modulo theory T if there is a Σ-interpretation $\mathcal{I}$ such that

- $\mathcal{I} \models \varphi$ and
- $\mathcal{I} \models \psi$ for all $\psi \in T$

Linear Natural Arithmetic

- $\Sigma = \{0, 1, +, =, \leq\}$

SMT definition

- $T = \{(\mathbb{N}, (\_)^{\mathbb{N}})\}$, where $(\_)^{\mathbb{N}}$ is the obvious standard interpretation

Standard definition (Presburger axioms)

$$
\begin{aligned}
T = \{&\forall x.\ \neg(0 = x + 1),\\
&\forall x \forall y.\ x + 1 = y + 1 \rightarrow x = y,\\
&\forall x.\ x + 0 = x,\\
&\forall x \forall y.\ x + (y + 1) = (x + y) + 1\} \cup\\
&\{(P(0) \wedge \forall x (P(x) \rightarrow P(x + 1))) \rightarrow \forall y P(y) \mid P \text{ is a formula with free variable } x\}
\end{aligned}
$$

Two views of theories

More examples

- The theory of uninterpreted functions with equality is $T_{\mathrm{UF}} =$

Two views of theories

More examples

- The theory of uninterpreted functions with equality is $T_{\mathrm{UF}} =$

More examples

- The theory of uninterpreted functions with equality is $T_{\mathrm{UF}} = \emptyset$

More examples

- The theory of uninterpreted functions with equality is $T_{\mathrm{UF}} = \emptyset$
- The axioms of theory of arrays (McCarthy):

$$
\begin{aligned}
T_A = \{\, & \forall a, i, j.\, (i = j \;\rightarrow\; \mathrm{read}(a, i) = \mathrm{read}(a, j)), \\
& \forall a, v, i, j.\, (i = j \;\rightarrow\; \mathrm{read}(\mathrm{write}(a, i, v), j) = v), \\
& \forall a, v, i, j.\, (i \neq j \;\rightarrow\; \mathrm{read}(\mathrm{write}(a, i, v), j) = \mathrm{read}(a, j))\}
\end{aligned}
$$

Two views of theories

These two views are equivalent

Two views of theories

These two views are equivalent

- set of Σ-structures $\Rightarrow$ the set of formulas that are true in all these structures

Two views of theories

These two views are equivalent

- set of Σ-structures $\Rightarrow$ the set of formulas that are true in all these structures
- set of axioms $\Rightarrow$ the set of Σ-structures that satisfy all the axioms

Two views of theories

These two views are equivalent

- set of Σ-structures $\Rightarrow$ the set of formulas that are true in all these structures
- set of axioms $\Rightarrow$ the set of Σ-structures that satisfy all the axioms

Two views of theories

These two views are equivalent

- set of Σ-structures $\Rightarrow$ the set of formulas that are true in all these structures
- set of axioms $\Rightarrow$ the set of Σ-structures that satisfy all the axioms

Sometimes, one view is better

- A set of structures satisfying axioms of Peano arithmetic is not easily describable.

Two views of theories

These two views are equivalent

- set of Σ-structures $\Rightarrow$ the set of formulas that are true in all these structures
- set of axioms $\Rightarrow$ the set of Σ-structures that satisfy all the axioms

Sometimes, one view is better

- A set of structures satisfying axioms of Peano arithmetic is not easily describable.
- A set of axioms for NRA is infinite and complicated.

Two views of theories

These two views are equivalent

- set of Σ-structures $\Rightarrow$ the set of formulas that are true in all these structures
- set of axioms $\Rightarrow$ the set of Σ-structures that satisfy all the axioms

Sometimes, one view is better

- A set of structures satisfying axioms of Peano arithmetic is not easily describable.
- A set of axioms for NRA is infinite and complicated.
- A set of axioms for NIA is not recursive.

Two views of theories

These two views are equivalent

- set of Σ-structures $\Rightarrow$ the set of formulas that are true in all these structures
- set of axioms $\Rightarrow$ the set of Σ-structures that satisfy all the axioms

Sometimes, one view is better

- A set of structures satisfying axioms of Peano arithmetic is not easily describable.
- A set of axioms for NRA is infinite and complicated.
- A set of axioms for NIA is not recursive.

Two views of theories

These two views are equivalent

- set of Σ-structures $\Rightarrow$ the set of formulas that are true in all these structures
- set of axioms $\Rightarrow$ the set of Σ-structures that satisfy all the axioms

Sometimes, one view is better

- A set of structures satisfying axioms of Peano arithmetic is not easily describable.
- A set of axioms for NRA is infinite and complicated.
- A set of axioms for NIA is not recursive. (, 1931)

Two views of theories

These two views are equivalent

- set of Σ-structures $\Rightarrow$ the set of formulas that are true in all these structures
- set of axioms $\Rightarrow$ the set of Σ-structures that satisfy all the axioms

Sometimes, one view is better

- A set of structures satisfying axioms of Peano arithmetic is not easily describable.
- A set of axioms for NRA is infinite and complicated.
- A set of axioms for NIA is not recursive. (Gödel, 1931)

Next time

- algorithms solving SMT
- CDCL(T) algorithm