

Logikbasierte Systeme der KI; Wissensverarbeitung

Prädikatenlogik, SMT-Solver

Prof. Dr. M. Schmidt-Schauß

SoSe 2022

SMT = SAT mit extra Theorien

Erweiterung der Aussagenlogik mit quantorenfreien Formeln.
Satisfiability Modulo Theories (SMT).

Idee: Aussagenlogische Formeln mit Formeln zu reellen Zahlen, Integer, Listen, Array, Bitvektoren usw.

Test: (Un)Erfüllbarkeit der Formeln

SMT solver: zB Z3 and CVC4, ...

SMT Beispiele

Theorie: Ganze Zahlen mit $=, <, >, \leq, \geq$
Operatoren; $+, -, *$ und evtl. weitere
Keine Quantoren,
keine (nicht-interpretierten) Funktionssymbole

Beispielformel:

$$a < b \wedge b < c \wedge c * c < d \wedge a = c - 1$$

Frage: Erfüllbar oder unerfüllbar?

SMT Beispiele

Theorie: Ganze Zahlen mit $==, <, >, \leq, \geq$
Operatoren; $+, -, *$ und evtl. weitere
Keine Quantoren,
keine (nicht-interpretierten) Funktionssymbole

Beispielformel:

$$a < b \wedge b < c \wedge c * c < d \wedge a = c - 1$$

Frage: Erfüllbar oder unerfüllbar?

Es muss gelten: $a + 2 \leq c$.

Das widerspricht $a = c - 1$

Allgemeinere Beispielformel:

$$\begin{array}{l} A \vee \neg B \quad \vee \quad a < b \vee b \neq c \\ \wedge \quad \neg A \quad \quad \vee \quad d < c * c + a \\ \wedge \quad B \quad \quad \quad \vee \quad a = c - 1 \end{array}$$

Fragen Bedeutung der Formeln / Semantik?

Welche syntaktischen / semantischen Beschränkungen?

Wie erweitert man den DPLL-Algorithmus?

SMT Allgemein

Formelformat

Klausel: $F \vee G$

F Aussagenlogische Klausel

G : Theorie-Formel Z.B.

Konjunktion von (Un-)Gleichungen über \mathbb{Z}

Formel: Konjunktion von Klauseln

Deduktions-Algorithmen spezifisch für Theorien:

- Entscheidungsverfahren für Konjunktionen von Theorie-Klauseln
- oder: Herleitung von einfachen Formeln aus einer gegebenen Konjunktion von Literalen.

SMT-Beispiel. Theorie = nicht-interpretierte Funktionssymbole

$$\Phi = \{ \underbrace{g(a) = c}_A \wedge (\underbrace{f(g(a)) \neq f(c)}_{\neg B} \vee \underbrace{g(a) = d}_C) \wedge \underbrace{c \neq d}_{\neg D} \}$$

Vorgehen: SAT -Solver und Theorie-Solver abwechselnd.

1. SAT: $A, \neg B \vee C, \neg D$ hat Modell $A, C, \neg D$
2. Theorie-Solver: ist widersprüchlich!

SMT-Beispiel. Theorie = nicht-interpretierte Funktionssymbole

$$\Phi = \underbrace{\{g(a) = c\}}_A \wedge \underbrace{\{f(g(a)) \neq f(c)\}}_{\neg B} \vee \underbrace{\{g(a) = d\}}_C \wedge \underbrace{\{c \neq d\}}_{\neg D}$$

Vorgehen: SAT -Solver und Theorie-Solver abwechselnd.

1. SAT: $A, \neg B \vee C, \neg D$ hat Modell $A, C, \neg D$
2. Theorie-Solver: ist widersprüchlich!
3. SAT: $A, \neg B \vee C, \neg D, \neg A \vee \neg C \vee D$ hat als Modell $A, \neg B, \neg C, \neg D$.
4. Theorie-Solver: $A, \neg B$ ist bereits widersprüchlich!

SMT-Beispiel. Theorie = nicht-interpretierte Funktionssymbole

$$\Phi = \{ \underbrace{g(a) = c}_A \wedge \underbrace{(f(g(a)) \neq f(c) \vee g(a) = d)}_{\neg B} \wedge \underbrace{c \neq d}_{\neg D} \}$$

Vorgehen: SAT -Solver und Theorie-Solver abwechselnd.

1. SAT: $A, \neg B \vee C, \neg D$ hat Modell $A, C, \neg D$
2. Theorie-Solver: ist widersprüchlich!
3. SAT: $A, \neg B \vee C, \neg D, \neg A \vee \neg C \vee D$ hat als Modell $A, \neg B, \neg C, \neg D$.
4. Theorie-Solver: $A, \neg B$ ist bereits widersprüchlich!
5. SAT: $A, \neg B \vee C, \neg D, \neg A \vee \neg C \vee D, \neg A \vee B$ ist widersprüchlich

SMT-Beispiel. Theorie = nicht-interpretierte Funktionssymbole

$$\Phi = \{ \underbrace{g(a) = c}_A \wedge (\underbrace{f(g(a)) \neq f(c)}_{\neg B} \vee \underbrace{g(a) = d}_C) \wedge \underbrace{c \neq d}_{\neg D} \}$$

Vorgehen: SAT -Solver und Theorie-Solver abwechselnd.

1. SAT: $A, \neg B \vee C, \neg D$ hat Modell $A, C, \neg D$
2. Theorie-Solver: ist widersprüchlich!
3. SAT: $A, \neg B \vee C, \neg D, \neg A \vee \neg C \vee D$ hat als Modell $A, \neg B, \neg C, \neg D$.
4. Theorie-Solver: $A, \neg B$ ist bereits widersprüchlich!
5. SAT: $A, \neg B \vee C, \neg D, \neg A \vee \neg C \vee D, \neg A \vee B$ ist widersprüchlich
6. \implies Eingabe-Formel ist widersprüchlich