GOETHE UNIVERSITÄT FRANKFURT AM MAIN

www.uni-frankfurt.de

Logikbasierte Systeme der KI; Wissensverarbeitung

Prädikatenlogik, SMT-Solver

Prof. Dr. M. Schmidt-Schauß

SoSe 2023

Stand der Folien: 1. Mai 2023

SMT = SAT mit extra Theorien

Erweiterung der Aussagenlogik mit quantorenfreien Formeln.
Satisfiability **M**odulo **T**heories (SMT).

Idee:	Aussagenlogische Formeln mit Formeln zu reellen Zahlen, Integer, Listen, Array, Bitvektoren usw.
Test:	(Un)Erfüllbarkeit von (speziellen) 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?

1): $a + 2 \leq c$ gilt wegen $a < b \wedge b < c$

2): Das widerspricht $a = c - 1$

Also: Eingabeformel unerfüllbar

SMT Beispiele: Theorie: Ganze Zahlen

Allgemeinere Beispielformel:

$$
\begin{array}{lllll}
 & A \vee \neg B & \vee & & a < b \vee b \neq c \\
\wedge & \neg A & \vee & & d < c * c + a \\
\wedge & B & \vee & & a = c - 1 \\
 & (aussagenlogisch) & & & \text{Formelanteil zu ganzen Zahlen}
\end{array}
$$

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

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

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: $\{A, C , \neg D\}$ ist widersprüchlich!

SMT-Beispiel.
Theorie = nicht-interpretierte Funktionssymbole

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

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: $\{A, C , \neg D\}$ 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

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

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: $\{A, C , \neg D\}$ 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

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

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: $\{A, C , \neg D\}$ 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. $\Longrightarrow$ Eingabe-Formel ist widersprüchlich

SMT-Beispiel.
Theorie = nicht-interpretierte Funktionssymbole

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

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: $\{A, C , \neg D\}$ 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. $\Longrightarrow$ Eingabe-Formel ist widersprüchlich

Erfolg!:

$$g(a) = c \quad \wedge \quad \big(f(g(a)) \neq f(c) \vee g(a) = d\big) \text{ impliziert } c = d$$