Integration of SMT-LIB Support into Maple

Stephen Forrest
29 July 2017
SC² Workshop, Kaiserslautern
SMT-CAS Integration

• Some SMT solvers presently incorporate computer algebra techniques in their theory solvers.
  • Examples: veriT [3], SMT-RAT [4]

• Alternate avenue of co-operation: CAS dispatching instances of SMT problems which it encounters in the course of symbolic computation to a SAT/SMT solver
  • Examples: many, e.g. see [5]
Logic in Maple

• Maple’s built-in logic is three-valued (true, false, FAIL)

• Also has a package (Logic) for two-valued propositional logic:
  • **BooleanSimplify** – return an equivalent but more compact formula if one exists
  • **Dual** – construct the logical dual
  • **Equivalent** – check equivalence of two formulae
  • **Normalize** – convert to a normal form (CNF or DNF)
  • **Satisfy / Satisfiable** – generate a satisfying truth assignment
  • **Tautology** – check if formula holds for all truth assignments

• Since Maple 2016, **Satisfy** and related commands use MiniSat.

• Package does not support existential or universal quantification
Maple Assume Facility (1)

- Maple's assume facility allows checking of Boolean propositions subject to declared assumptions.

- Assumptions consist of Boolean predicates or properties attached to specified symbols.

- Two main commands exist:
  - `is`: equivalent of $\forall$
  - `coulditbe`: equivalent of $\exists$

General form (fV stands for “free variables”):

- `is(p) assuming q` $\rightarrow \forall fV(q,p)$ $(q \Rightarrow p)$
- `coulditbe(p) assuming q` $\rightarrow \exists fV(q,p)$ $(q \Rightarrow p)$
Maple Assume Facility (2)

- Maple's assume facility allows checking of propositions subject to assumptions.

\[
\cos(n \pi) \text{ assuming } n :: \text{integer};
\]

\[
(-1)^n
\]

\[
\text{coulditbe}\left(\frac{i}{3}, \text{integer}\right) \text{ assuming } \frac{i}{2} :: \text{integer}
\]

\[
\text{true}
\]

\[
\text{is}\left(-\frac{(4a^2 + 1)^2}{8a^4} < 0 \text{ and } -\frac{(4a^2 + 1)^4}{32a^8} < 0 \text{ and } -\frac{(4a^2 + 1)^4}{64a^8} < 0\right) \text{ assuming } a > 0;
\]

\[
\text{true}
\]

- Queries often include inequalities but in practice rarely have significant Boolean structure.
Maple Assume Facility (3)

• Symbolic evaluation in Maple makes regular use of the assume facility and its associated queries

• Example: evaluation of symbolic product

\[
\prod_{n=a}^{b} f(n), n=a..b;
\]

• Implementation includes a case which computes the roots of \( f(n) \) and checks whether any of them are integers in the range \([a, b]\) using the could it be command.
## Invocations of `is/coulditbe` in tests

<table>
<thead>
<tr>
<th>Description</th>
<th><code>is</code></th>
<th><code>coulditbe</code></th>
</tr>
</thead>
<tbody>
<tr>
<td>Total distinct queries</td>
<td>24085</td>
<td>5771</td>
</tr>
<tr>
<td>Queries with result true</td>
<td>2335</td>
<td>3582</td>
</tr>
<tr>
<td>Queries with result false</td>
<td>19020</td>
<td>1519</td>
</tr>
<tr>
<td>Queries with result FAIL</td>
<td>2730</td>
<td>670</td>
</tr>
<tr>
<td>Queries including addition</td>
<td>9849</td>
<td>2022</td>
</tr>
<tr>
<td>Queries including multiplication</td>
<td>17097</td>
<td>3106</td>
</tr>
<tr>
<td>Queries including equations, inequations, or inequalities</td>
<td>11333</td>
<td>4439</td>
</tr>
<tr>
<td>Queries including integer exponents &gt;= 2</td>
<td>7965</td>
<td>875</td>
</tr>
<tr>
<td>Queries including complex arithmetic</td>
<td>6215</td>
<td>389</td>
</tr>
<tr>
<td>Queries with Boolean structure (<code>¬,∨, ∧</code>)</td>
<td>564</td>
<td>168</td>
</tr>
</tbody>
</table>
Relations between logics induce a partial order.

[Source: http://smtlib.cs.uiowa.edu/logics.shtml]
SMTLIB Package in Maple

- **SMTLIB** is a Maple package implementing connection to an external SMT solver using the SMT-LIB2 language [1].

- New in Maple 2017, with plans to expand for 2018

- Upcoming version of the package will offer:
  - **ToString** – translate input to string encoding SMT-LIB 2 query (in Maple 2017)
  - **Satisfiable** – check for satisfiability (to be added)
  - **Satisfy** – generate a satisfying truth assignment (to be added)

- Supports some Maple primitives not supported by Logic package: (forall, exists, abs, floor, iquo, irem, piecewise)

- The default SMT solver used is Z3, but the interface permits an alternate SMT solver executable to be specified.
Type Inference

Traverse input expression with the goal of assigning one of the types \{\texttt{Bool}, \texttt{Int}, \texttt{Real}\} to each symbol in the input

1. If type was explicitly provided by the user, done.
   \texttt{Satisfy( a + b < 3 ) assuming a::real, b::real;}

2. If expression occurs as an operand in an expression where only one type could be valid, assign that type:
   \texttt{Satisfy( a^2 > 1 or abs(c) > 0 or d );}

3. Propagate resolved types through expression:
   \texttt{Satisfy( a^2 + 2 = b ) assuming a::integer;}
   \texttt{Satisfy( \{ a * b = 2.5, b = 1.5 \} )}

4. Remaining ambiguous expressions:
   - If symbol appears in an arithmetic context, assign to \texttt{Int}
   - Otherwise, assign to \texttt{Bool}
Supported SMT-LIB 2 Logics

**Dark green** indicates logics for which all formulas correspond to some possible input to the Maple SMTLIB[Satisfy] command.

**Light green** indicates logics for which a proper subset of formulas correspond to some possible input to the Maple SMTLIB[Satisfy] command.
Examples

```maple
> SMTLIBLink:-Satisfy( {w^3+x^3=y^3+z^3, w>0, x>0, y>0, z>0, w<>y, w<>z}, logic="QF_NIA");
   {w = 10, x = 9, y = 12, z = 1}
> SMTLIBLink:-Satisfiable( {x^4+y^4+z^4=w^4, x>0, y>0, z>0, w>=1}, logic="QF_NIA");
   FAIL

> expr := forall([x,y],exists(w,x+w=y));
   expr := \(\forall([x,y], \exists(w, x+w=y))\)
> SMTLIBLink:-Satisfiable( expr, logic="LIA" );
   true
> SMTLIBLink:-Satisfy({x^2+3*x*y+y^2 < 100, x<5, y>=100}, logic="QF_NRA", show_smtlib);
   (set-option :produce-models true)
   (set-logic QF_NRA)
   (declare-fun x () Real)
   (declare-fun y () Real)
   (assert (and (<= 100 y) (< x 5) (< (+ (* x x) (* (* x y) 3) (* y y)) 100)))
   (check-sat)
   (get-value (x y))
   (exit)
   {x = -264, y = 101}
```
Future Work

• Examine incorporating solver link into Maple proper, i.e. using SMT as a general-purpose tool for solving SMT instances which arise during evaluation of symbolic expressions.

• Find ways of meaningfully incorporating other parts of the SMT-LIB 2 specification into Maple:
  • Support additional types
    • Uninterpreted functions (QF_UF and logics including it)
    • Arrays, bit vectors
    • Floating-point arithmetic?
    • Algebraic datatypes? (new in SMT-LIB 2.6)
  • Offer undecidable cores / proof of UNSAT to user
References


Questions

- Thank you!