Little Engines of Proof: Lecture 10

N. Shankar, L. de Moura, H. Ruess, A. Tiwari

shankar@csl.sri.com

URL: http://www.csl.sri.com/~shankar/LEP.html

Computer Science Laboratory

SRI International

Menlo Park, CA

List solver

Configuration (E, S) with

- K a set of *fresh* variables (disjoint from X),
- E a set of Σ_L-equalities,
- S a functional solution set.

A *cons* term c is a Σ_L-term not containing any $car(.)$ or $cdr(.)$.

In the solver rules, all terms are assumed to be canonical.

Elim	$\dfrac{K,\ E,\ S}{K \cup \{k_1, k_2\},\ R[car(x) := k_1, cdr(x) := k_2],\ R \cup S}$ if $k_1, k_2 \notin K$, $car(x)$ or $cdr(x)$ in E and $R := \{x = cons(k_1, k_2)\}$
Ext	$\dfrac{K,\ \{cons(a_1, b_1) = cons(a_2, b_2)\} \cup E,\ S}{K, \{a_1 = a_2,\ b_1 = b_2\} \cup E,\ S}$
Triv	$\dfrac{K,\ \{a = a\} \cup E,\ S}{K, E,\ S}$
Comp	$\dfrac{K,\ \{x = c\} \cup E,\ S}{K, \sigma_{\mathcal{L}}(\{x = c\}[E]),\ S \circ \{x = c\}} x \notin vars(c), x \notin K, c$ a cons term
Bot	$\dfrac{K,\ \{x = c\} \cup E,\ S}{\bot} x \in vars(c), c$ a cons term
Fuse	$\dfrac{K,\ \{k = c\} \cup E,\ S}{K,\ \{k = c\}[E], S \triangleright \{k = c\}} k \in K, k \notin vars(c), c$ a cons term

Rules Subst, Bot, and Fuse are applied symmetrically.

List Solver (Cont.)

Exercise. Show termination of the list solver rules.

Excercise. Show that all list solver rules are $\mathcal{L}$-preserving.

For list equality $a = b$, let $(\emptyset, \{\sigma_{\mathcal{L}}(a) = \sigma_{\mathcal{L}}(b)\}, \emptyset)$ be a starting configuration. An irreducible configuration is either $\bot$ or of the form $(K,\ \emptyset,\ S)$ with S a functional solution set with $dom(S) \subseteq vars(a = b)$.

In the first case, define $solve_{\mathcal{L}}(a = b)$ to be $\bot$ and otherwise we arbitrarily choose (using Hilbert's ϵ combinator) an irreducible configuration of the form $(K,\ \emptyset,\ S)$ and define $solve_{\mathcal{L}}(a = b) := S$.

This is a $\mathcal{L}$-solver since S *$\mathcal{L}$-preserves* $a = b$.

Examples

$$
\begin{array}{lcl}
 & & (\emptyset,\ \{x = cons(car(x), y)\},\ \emptyset) \\
\text{CarE} & \rightsquigarrow & (\{k_1, k_2\}, \\
 & & \ \{cons(k_1, k_2) = cons(k_1, y)\}, \\
 & & \ \{x = cons(k_1, k_2)\}) \\
\text{Ext} & \rightsquigarrow & (\{k_1, k_2\},\ \{k_1 = k_1,\ k_2 = y\},\ \{x = cons(k_1, k_2)\}) \\
\text{Triv} & \rightsquigarrow & (\{k_1, k_2\},\ \{k_2 = y\},\ \{x = cons(k_1, k_2)\}) \\
\text{Fuse} & \rightsquigarrow & (\{k_1, k_2\},\ \emptyset,\ \{y = k_2,\ x = cons(k_1, k_2)\})
\end{array}
$$

Finite Sequences

Have a length n associated with them. Content is indexed from 0 to $n-1$ from left to right.

- $sel_{n,i,j}(.)$
  Selection of the $j - i + 1$ elements i through j
  $(0 \leq i \leq j < n)$

- $conc_{n,m}(.,.)$
  Concatenation of two finite sequences of length n and m.

- We usually omit parameters and write $x_n * y_m$ for concatenation and $x_n[i:j]$ for selection.

Canonizer for Finite Sequences

The equality theory $\mathcal{F}$ is given by:

$$
\begin{array}{rcl}
x_n[0:n-1] & = & x_n \\
x[i:j][k:l] & = & x[k+i:l+i] \\
(x_n * y_m)[i:j] & = & \begin{cases} x_n[i:j] & \text{if} \quad j < n \\ y_m[i-n:j-n] & \text{if} \quad n \leq i \\ x_n[i:n-1] * y_m[0:j-1] & \text{if} \quad i < n \leq j \end{cases} \\
x[i:j] * x[j+1:k] & = & x[i:k]
\end{array}
$$

and $. * .$ is associative.

Canonizer. $\sigma_{\mathcal{F}}(a)$ is the unique normal form of the TRS above. $\sigma_{\mathcal{F}}(a)$ is therefore a concatenation of extractions on variables.

Solver for Finite Sequences

p_n, q_n range over terms not containing any concatenation.

x_n is identified with $x[0:n-1]$.

We assume all terms and equalities to be well-formed (an example for a non-well-formed equality is $x[2:4] = y[7:10]$).

Interesting subcase: solve $x_n[j:i] = x_n[l:k]$ (wlog $j \leq l$)

$$
\begin{array}{rcl}
j = l, i = k & : & \text{valid} \\
i < l & : & x_n = b_{j-1} * a_{i-j+1} * d_{l-i-1} * a_{i-j+1} * e_{n-k-1} \\
i \geq l & : & x_n = b_{j-1} * a_{l-j}^{k-j+1} * d_{n-k-1}
\end{array}
$$

Fresh variables b, d, e are omitted if their respective lengths evaluate to 0.

Solver for Finite Sequences (Cont.)

$$\mathit{Dec}_{=} \quad \frac{\{p_n * a = q_n * b\} \ \cup \ E, \ S}{\{p_n = q_n, \ a = b\} \ \cup \ E, \ S}$$

$$\mathit{Dec}_{<} \quad \frac{\{p_n * a = q_m * b\} \ \cup \ E, \ S}{\{p_n = \sigma_{\mathcal{F}}(q_m[0 : n-1]), \ a = \sigma_{\mathcal{F}}(q_m[n : m-1]) * b\} \ \cup \ E, \ S} n < m$$

$$\mathit{Dec}_{>} \quad \frac{p_n * a = q_m * b \ \cup \ E, \ S}{\{q_m = \sigma_{\mathcal{F}}(p_n[0 : m-1]), \ \sigma_{\mathcal{F}}(p_n[m : n-1]) * a = b\} \ \cup \ E, \ S} n > m$$

$$\mathit{Solve} \quad \frac{x_n[i : j] = a \ \cup \ E, \ S}{\sigma_{\mathcal{F}}(\{x_n = b\}[E]), \ S \circ \{x_n = b\}} x_n \notin \mathit{subterms}(a), b = u_i * a * v_{n-j}$$

$$\mathit{Chunk}_1 \quad \frac{x_n[i : j] = x_n[k : l] \ \cup \ E, \ S}{\{x_n[i : l] = u^{((l-i+1)/k-i)}\} \ \cup \ E, \ S} i < k, (l-i+1)/(k-i), u \text{ fresh}$$

$$\mathit{Chunk}_2 \quad \frac{x_n[i : j] = x_n[k : l] \ \cup \ E, \ S}{\{x_n[i : l] = u_h * (v_{h'} * w_h)^{(l-i-h+1)/(k-i)}\} \ \cup \ E, \ S}$$

with $i < k$, not $(l - i + 1)x/(k - i)$

$h = (l - i + 1) \, \mathit{mod} \, (k - i)$, $h' = k - i - h$, $u, \ v, \ w$ fresh.

$$\mathit{Triv} \quad \frac{a = a \ \cup \ E, \ S}{E, \ S}$$

Example

$$
\begin{array}{ll}
 & (\{x_{16}[0 : 7] * y_8 = y_8 * z_8\}, \ \emptyset) \\
\leadsto & (\{x_{16}[0 : 7] = y_8, \ y_8 = z_8\}, \ \emptyset) \\
\leadsto & (\{x_{16}[0 : 7] = z_8\}, \ \{y_8 = z_8\}) \\
\leadsto & (\emptyset, \ \{y_8 = z_8, \ x_{16} = z_8 * a_8\})
\end{array}
$$

Encodings and Extensions

Arrays.

$$
\begin{array}{rcl}
\mathit{update}_{i,n}(a_n, x_1) & := & a_n[0 : i-1] * x_1 * a_n[i+1 : n-1] \\
\mathit{select}_{i,n}(a_n) & := & a_n[i : i]
\end{array}
$$

Exercise. State the finite sequence solver rules directly in terms of the functional arrays signature above.

Strings. Add character constants to finite sequence signature, and add canonization and solving rules accordingly.

Bitvectors

- Add bitvector constants, and add canonization and solving rules accordingly.
- Many operators such as rotation and shifting can be encoded.
- Add bitwise operators. Canonical forms include BDDs with $x_n[i : j]$ in conditional part. Finite sequence solver extended with BDD solver.
- Adding finite arithmetic based on carry-lookahead addition leads to bitwise splitting.

Nonfixed-sized finite sequences

Example.

1. $x_n * 1_1 * y_m = z_2 * 1 * w_2$
2. $x_l * 1_1 * 0_1 = 1_1 * 0_1 * x_l$

Eqn 1 solvable iff if $n = 1$, $m = 3$ or $m = 1$, $n = 3$, whereas eqn 2 solvable iff l is even.

Splitting based on side conditions, which can be decided using the Diophantine problem for addition and divisibility:

$\exists x_1, \ldots, x_n : \ldots \wedge x_m = x_j + x_k \wedge \ldots \wedge x_m = x_j \wedge \ldots \wedge x_m = p \wedge \ldots$

Solving word problems with concatenation and variables of unknown size is also known as Löb's (west) or Markov's (east) problem.

Exercises

Exercise. Is the solver for nonfixed-sized finite sequences terminating?

Exercise. Show that there is no nonfixed-sized bitvector solver for the bitvector theory including concatenation, extraction, and bitwise logical operations.