A simple rewrite proof of the equational interpolation theorem

Theorem 1 ([1]) *$\Gamma \models l = r \Longrightarrow \exists I\, \Gamma \models I$ & $I \models l = r$, with $\Sigma(I) \subseteq \Sigma(\Gamma) \cap \Sigma(l = r)$.*

Example 2 *Let $\Gamma = \{a_i = b, b = c_i, f(x,x) = g(x,x) \mid i \in \{1,2\}\}$, $l = f(H(a_1), H(a_2))$ and let $r = g(H(c_1), H(c_2))$. Then we have $\Gamma \models l = r$ and choosing the interpolant $I = \{a_1 = a_2, c_1 = c_2, a_1 = c_1, f(x,x) = g(x,x)\}$ yields $\Gamma \models I$ & $I \models l = r$. Note that $\Sigma(I) \subseteq \Sigma(\Gamma) \cap \Sigma(l = r)$ holds, since $\Sigma(l = r) = \Sigma(I) \cup \{H\}$, $\Sigma(\Gamma) = \Sigma(I) \cup \{b\}$ and $\Sigma(I) = \{a_i, c_i, f, g \mid i \in \{1,2\}\}$.*

Symbols in $\Sigma(l = r) - \Sigma(\Gamma)$ are said to be *alien* and ranged over by capitals, and the other symbols are *native* and ranged over by ordinary letters. For convenience we will treat variables in l and r as nullary function symbols. Our proof is based on the equivalence between equality in the equational logic for Γ and convertibility w.r.t. the rewrite relation $\rightarrow_\Gamma$ generated by Γ: $\Gamma \models l = r \iff l \leftrightarrow^*_\Gamma r$. Applied to the example:

$$l \leftrightarrow f(H(b), H(a_2)) \leftrightarrow f(H(b), H(b)) \leftrightarrow g(H(b), H(b)) \leftrightarrow g(H(b), H(c_2)) \leftrightarrow r$$

Our proof of the theorem formalises the idea that aliens partition l and r into native parts, such that equality of l and r can be reduced to a number of equalities on those parts. The next lemma establishes this for the top part. It employs the fact that any term s can be uniquely partitioned into a maximal (possibly empty) native context part and a vector of *aliens*, i.e. terms with alien symbols as heads. This will be indicated by writing a term s as $C[\![\vec{s}]\!]$. For instance, l is written as $C[\![l_1, l_2]\!]$, with maximal native context $C = f(\Box, \Box)$, and aliens $l_1 = H(a_1)$ and $l_2 = H(a_2)$.

Lemma 3 *If $C[\![\vec{s}]\!] \leftrightarrow^*_\Gamma D[\![\vec{t}]\!]$, then $C[\vec{x}] \leftrightarrow^*_\Gamma D[\vec{y}]$ holds for some $\vec{x}$ and $\vec{y}$, such that identity of variables in the latter conversion implies convertibility-without-head-steps of the corresponding aliens in the former.*

Proof A first application of [2, Lemma 3.2.1.4] yields $\vec{x}$ and $\vec{y}$ such that convertibility holds. Another application of the lemma shows that convertibility can be strengthened to convertibility-without-head-steps. (A proof by induction on the length of the conversion is easy as well.) $\Box$

Proof (of Theorem 1) Suppose $l \leftrightarrow^*_\Gamma r$. The proof is by induction on the maximal number of alien symbols on any path from the root to a leaf in $l = C[\![\vec{l}]\!]$ or $r = D[\![\vec{r}]\!]$. By the lemma $C[\vec{x}] \leftrightarrow^*_\Gamma D[\vec{y}]$ holds, for some $\vec{x}$ and $\vec{y}$ such that occurrences of the same variable in this conversion implies convertibility-without-head-steps of the corresponding aliens in $l \leftrightarrow^*_\Gamma r$. By the IH this implies that we can find an interpolant for each of these conversions. We conclude by taking the union of all these interpolants and the single equation $C[\vec{x}] = D[\vec{y}]$. $\Box$

This establishes a property stronger than ordinary interpolation: all equations in the interpolant are only between (variable substitution instances of) the maximal native parts of l and r.

Interpolation trivially holds for higher-order equational logic, but fails for rewrite logic.

Example 4 *In higher-order equational logic, take $I = \{\lambda\vec{x}.l[\vec{X}{:=}\vec{x}] = \lambda\vec{x}.r[\vec{X}{:=}\vec{x}]\}$, where $\vec{X}$ is the vector of alien symbols occurring in l or r.*

Counterexample 5 *Consider Example 2, replacing all $=$s by $\geq$s. Then no interpolant can be found. The problem is that we* can *put assumptions like $a_i \geq c_j$ for $i, j \in \{1,2\}$ in the interpolant, but this only allows us to derive such things as $f(H(a_1), H(a_2)) \geq g(H(c_i), H(c_i))$ (for the* same *index $i \in \{1,2\}$ in the rhs) since $f(x,x){=}g(x,x)$ forces 'synchronisation' between the two arguments of f: in the absence of b and in the presence of H, synchronisation forces identity either of a_1 and a_2 or of c_1 and c_2.*

References

[1] P.H. Rodenburg and R.J. van Glabbeek. An interpolation theorem in equational logic. Talk presented at PAM, CWI, 11th December 2002.

[2] E. Tidén. *First-Order Unification in Combinations of Equational Theories.* PhD thesis, The Royal Institute of Technology, Department of Numerical Analysis and Computer Science, Stockholm, Sweden, August 1986. TRITA-NA-8604.