Another Proof of the Modularization Theorem

Douglas R. Smith
Kestrel Institute
3260 Hillview Avenue
Palo Alto, California 94304
3 February 1993

This note builds on the ideas of the proof of the Modularization Theorem in [1, 2] and Veloso's more recent proof.

I assume that (1) theories are single-sorted and (2) a theory morphism is presented by a signature morphism: a symbol-to-symbol map. The symbol map can be straightforwardly extended to a language translation.

If A is a theory, let $\Sigma_A = FUN_A \bigcup PRED_A$ be the function and predicate symbols of A, L_A the sentences of A, and Ax_A the axioms of A.

Here are some basic results needed in the proof. First, consider the properties of proofs under translation by a signature morphism.

Proposition 1. *(Deducibility is preserved under translation by signature morphism).*
Let $g : \Sigma_A \to \Sigma_B$ be a signature morphism, $J \subseteq L_A$, and $\phi \in L_A$, then

$$J \vdash \phi \implies g(J) \vdash g(\phi).$$

Proof: Show for each of the inference rules of the logic (e.g. resolution) that it is preserved under translation.

Corollary 1. If g is injective, then $g(J) \vdash g(\phi) \implies J \vdash \phi$.

proof:

$g(J) \vdash g(\phi)$

$\implies$ applying Proposition 1

$g^{-1}(g(J)) \vdash g^{-1}(g(\phi))$

$\implies$ simplifying

$J \vdash \phi$.

Comment: The proposition and the corollary just show that the name of a symbol doesn't matter very much – proofs are isomorphic up to renaming.

To generalize the Corollary to arbitrary signature morphisms, we need to account for the identifications that g makes on Σ_A.

Let[1]

$$Id_{fun}(g) = \{\forall(x)(f_1(x) = f_2(x)) \mid f_1, f_2 \in FUN_A \ \wedge \ g(f_1) = g(f_2)\}$$

[1] These definitions need to be elaborated to handle the different arities of function and predicates.

$$Id_{pred}(g) = \{\forall(x)(p_1(x) \equiv p_2(x)) \mid p_1, p_2 \in PRED_A \wedge g(p_1) = g(p_2)\}$$

$$Id(g) = Id_{fun}(g) \bigcup Id_{pred}(g).$$

Proposition 2. *(Preservation of proofs under back-translation).*
Let $g : A \to B$ be a signature morphism, $J \subseteq L_A$, and $\phi \in L_A$, then

$$g(J) \vdash g(\phi) \implies J \bigcup Id(g) \vdash \phi.$$

Proof: The trick is to create an injective variant of g, called g^*, by requiring that $g^* = g$ except when g maps two symbols p, q to the same symbol, in which case g^* maps p and q to fresh symbols. The effect of identifying p and q can be added back in via an axiom of the form $p = q$; i.e. the identities in $Id(g)$.

$g(J) \vdash g(\phi)$

$\implies$ see above

$g^*(J) \bigcup g^*(Id(g)) \vdash g^*(\phi)$

$\implies$ applying Proposition 1

$g^{*-1}(g^*(J) \bigcup g^*(Id(g))) \vdash g^{*-1}(g^*(\phi))$

$\equiv$ simplifying

$J \bigcup Id(g) \vdash \phi.$

Proposition 3. *(Preservation of conservativeness under addition of axioms).*
If $\langle \Sigma_A, Ax_A \rangle \leq \langle \Sigma_B, Ax_B \rangle$ and $J \subseteq L_A$
then $\langle \Sigma_A, Ax_A \bigcup J \rangle \leq \langle \Sigma_B, Ax_B \bigcup J \rangle$.

Proof: Let $\phi \in L_A$.

$Ax_B \bigcup J \vdash \phi$

$\implies$ using compactness (if necessary) and the deduction theorem

$Ax_B \vdash J \implies \phi$

$\implies$ since $\langle \Sigma_A, Ax_A \rangle \leq \langle \Sigma_B, Ax_B \rangle$

$Ax_A \vdash J \implies \phi$

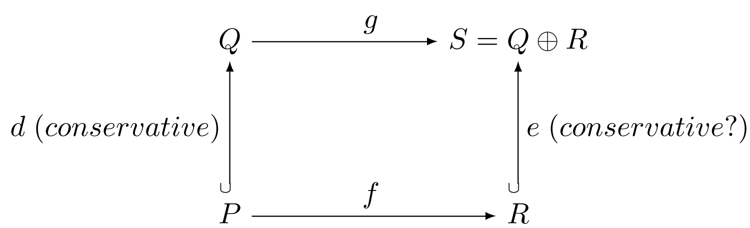
$\implies$ using the deduction theorem

$Ax_A \bigcup J \vdash \phi.$

The Craig Interpolation Lemma is critical to the proof of the Modularization Theorem. The "splitting" version goes as follows.

Craig Interpolation Lemma. Given theories A and B,
if $\phi \in L_B$, and $Ax_A \bigcup Ax_B \vdash \phi$
then there exists $I \subseteq L_A \cap L_B$ such that
(1) $Ax_A \vdash I$
(2) $Ax_B \bigcup I \vdash \phi$.

The Modularization Theorem is concerned with the preservation of properties of morphisms under a pushout operation.



We are given theory P and a conservative extension to Q, and a theory morphism $f : P \rightarrow R$. The pushout construction creates theory $S = Q \oplus R$ plus the theory morphisms g and e. The Modularization Theorem asserts that the inclusion $e : R \rightarrow S$ is conservative.

Modularization Theorem. The pushout construction preserves conservativeness.

Proof: To show that $e : R \rightarrow S$ is conservative, assume $\phi \in L_R$ and $Ax_S \vdash \phi$. We must show that $Ax_R \vdash \phi$. The pushout construction of S gives us $L_S = g(L_Q) \bigcup L_R$ and $Ax_S = g(Ax_Q) \bigcup Ax_R$. We can apply the Craig Interpolation Lemma via the correspondance

$$\begin{array}{rcl} L_A & \mapsto & g(L_Q) \\ Ax_A & \mapsto & g(Ax_Q) \\ L_B & \mapsto & L_R \\ Bx_B & \mapsto & Ax_R \end{array}$$

So there exists some set of sentences $I \subseteq g(L_Q) \cap L_R$ such that
(1) $g(Ax_Q) \vdash I$
(2) $Ax_R \bigcup I \vdash \phi$.

We'll show that $g(Ax_P) \vdash I$, but assume it for now and prove the theorem. We know $Ax_R \vdash g(Ax_P)$ since g is a theory morphism, so combining these we get $Ax_R \vdash I$. Judgement (2) is then equivalent to the desired result: $Ax_R \vdash \phi$.

So it remains to prove $g(Ax_P) \vdash I$. First, note that since $I \subseteq g(L_Q) \cap L_R$, there is some subset of sentences $J \subseteq L_P$ such that $I = g(J)$ ($I \subseteq g(L_Q)$ means that each sentence in I is the translation of a sentence of L_Q, and furthermore $I \subseteq L_R$ means that each such sentence could only have come from L_P). Second, note that by Proposition 3 (and the assumption $P \leq Q$) we have

$$\langle \Sigma_P, Ax_P \bigcup Id(g) \rangle \leq \langle \Sigma_Q, Ax_Q \bigcup Id(g) \rangle.$$

Third, note that $g(Id(g))$ is universally valid, since each identity in $Id(g)$ translates to the form $p = p$.

$g(Ax_P) \vdash I$ follows from $g(Ax_Q) \vdash I$ (judgement (1) above) as follows:

$g(Ax_Q) \vdash I$

$\equiv$ first note above

$g(Ax_Q) \vdash g(J)$

$\Longrightarrow$ applying Proposition 2

$Ax_Q \bigcup Id(g) \vdash J$

$\Longrightarrow$ second note above

$Ax_P \bigcup Id(g) \vdash J$

$\Longrightarrow$ applying Proposition 1

$g(Ax_P \bigcup Id(g)) \vdash g(J)$

$\Longrightarrow$ third note above

$g(Ax_P) \vdash I.$

QED

Corollary 2. If R is consistent, then so is the pushout theory.

Veloso has also proved the following interesting results.

Proposition 4. *(Preservation of conservativeness under addition of operator symbols).* If $\langle \Sigma_A, Ax_A \rangle \leq \langle \Sigma_B, Ax_B \rangle$ and Ψ is a fresh set of operator symbols (i.e. $\Psi \cap \Sigma_B = \{\}$) then $\langle \Sigma_A \bigcup \Psi, Ax_A \rangle \leq \langle \Sigma_B \bigcup \Psi, Ax_B \rangle$.

Surprisingly, Proposition 4 is equivalent in first-order logics to the Craig Interpolation Lemma.

References

[1] Turski, W. M., and Maibaum, T. E. *The Specification of Computer Programs.* Addison-Wesley, Wokingham, England, 1987.

[2] Veloso, P. A., and Maibaum, T. On the modularization theorem for logical specification. *Information Processing Letters 53*, 5 (1995), 287–293.