Interpolation

<u>Motivation:</u> Consider

$$A_1, \ldots, A_n \models C \ ,$$

where C is some mathematical theorem and the A_i are specific axioms, definitions, lemmas, or other theorems. (Let $A = A_1 \wedge \cdots \wedge A_n$.)

A may contain symbols that do not occur in C, and vice versa.

Can we find a sentence B, such that

$$A \models B \quad \text{and} \quad B \models C$$

where B contains only symbols occurring in both: A <u>and</u> C?

As stated above, the answer is <u>no</u>.

<u>Example:</u> (Failure of interpolation)
Let A be $\exists x F(x) \wedge \neg\forall x F(x)$ and let C be $\exists u \exists v\, u \neq v$.
$A \models C$, but there are no common symbols (except $\exists$ and $\neg$).

Focussing on more modest requirements we can state:

<u>Proposition:</u> (Interpolation w.r.t. constants)
If $A \models C$ then there is a B such that $A \models B$ and $B \models C$, where B contains only <u>constants</u> that occur in A as well as in C.

<u>Proof:</u> Take $\exists v_1 \ldots \exists v_n A^*$ for B, where A^* results from A by replacing the constants $c_1, \ldots c_n$, that do not occur in C by the new variables $v_1, \ldots v_n$. It is easy to check $q.e.d.$

More interestingly, let $L(F)$ denote <u>all non-logical symbols</u> in F:

<u>Theorem:</u> (Craig's Interpolation Theorem)
If $A \models C$ then there is a B such that $A \models B$ and $B \models C$, where $L(B) \subseteq L(A) \cap L(C)$.

B is called <u>interpolant</u> from A to C.

Proof of Craig's Interpolation Theorem

<u>Degenerate case:</u> A and C are valid or unsatisfiable.

Let A be $\exists x F(x) \wedge \forall x \neg F(x)$ and let C be $\exists u P(u)$.

$\exists x\, x \neq x$ may serve as interpolant.

$\Rightarrow$ We may have to use '$=$' in the <u>interpolant</u> B, even if it neither occurs in A or nor in C:

Other ways deal to with this case:

- $\diamond$ Exclude unsatisfiable sentences A and valid sentences C.
- $\diamond$ Include the truth constants $\perp, \top$ as (0-ary) connectives.

For the rest of the proof we may assume that A is satisfiable and that C is not valid.

<u>Note</u>:
– $A \models C$ iff $\{A, \neg C\}$ is unsatisfiable.
– B is an interpolant of A to C iff
$A \models B$, $\neg C \models \neg B$, and $L(B) \subseteq L(A) \cap L(C)$.

We proceed <u>indirectly</u> and show:
If there is no interpolant of A to C, then $\{A, \neg C\}$ is satisfiable.

We use the <u>model existence lemma</u>, i.e.: appeal to (S0)–(S8).

Some useful <u>terminology</u>:

- $\diamond$ B is said to <u>separate</u> Γ_L from Γ_R iff $\Gamma_L \models B$, $\Gamma_R \models \neg B$, and $L(B) \subseteq L(\Gamma_L) \cap L(\Gamma_R)$.
- $\diamond$ Γ is called <u>divisible (without separation)</u> if it can be written as $\Gamma = \Gamma_L \cup \Gamma_R$, where Γ_L and Γ_R are satisfiable, and <u>no</u> sentence separates Γ_L from Γ_R.

B is an interpolant of A to C iff B separates $\{A\}$ from $\{\neg C\}$.

Proof without identity and function symbols

Let S be the set of divisible L-sets.
It remains to establish (S0)–(S6) for S.

(S0) trivial [why ?]

(S1): Suppose $\Gamma = \Gamma_L \cup \Gamma_R$ is divisible, and $D, \neg D \in \Gamma$.
Since Γ_L and Γ_R are satisfiable we conclude w.l.o.g.:
$D \in \Gamma_L$, $\neg D \in \Gamma_R$. But this means that D separates Γ_L from Γ_R, in contradiction to the assumption of divisibility.

(S2): Suppose $\Gamma = \Gamma_L \cup \Gamma_R$ is divisible, and $\neg\neg D \in \Gamma$.
W.l.o.g., $\neg\neg D \in \Gamma_L$ and hence $\Gamma_L \models D$. This implies that also $(\Gamma_L \cup \{D\}) \cup \Gamma_R$ divisible, and thus that $\Gamma \cup \{D\} \in S$.

(S4)–(S6): Analogous to (S2). [[Blackboard, if needed]]

(S3): Suppose $\Gamma = \Gamma_L \cup \Gamma_R$ is divisible, and $D_1 \vee D_2 \in \Gamma$.
W.l.o.g., $D_1 \vee D_2 \in \Gamma_L$.
If $\Gamma_L \cup \{D_1\}$ is unsatisfiable (i.e., if $\Gamma_L \models \neg D_1$), then (since $\Gamma_L \models D_1 \vee D_2$) we have $\Gamma_L \models D_2$. Hence we can argue like for (S2). (Analogously, if $\Gamma_L \cup \{D_2\}$ is unsatifiable.)
It remains to investigate the case where $\Gamma_L \cup \{D_i\}$ is satisfiable for both i:
In this case, $(\Gamma_L \cup \{D_i\}) \cup \Gamma_R$ is divisible unless there is a B_i separating $\Gamma_L \cup \{D_i\}$ from Γ_R, for $i \in \{1, 2\}$, respectively.
But $\Gamma_L \cup \{D_1\} \models B_1$, $\Gamma_L \cup \{D_2\} \models B_2$, and $D_1 \vee D_2 \in \Gamma_L$ implies $\Gamma_L \models B_1 \vee B_2$. Moreover, $\Gamma_R \models \neg B_i$ for $i \in \{1, 2\}$ implies $\Gamma_R \models \neg(B_1 \vee B_2)$.
$L(B_i) \subseteq L(\Gamma_L) \cap L(\Gamma_R)$, for both i, therefore also $L(B_1 \vee B_2) \subseteq L(\Gamma_L) \cap L(\Gamma_R)$. This means that $B_1 \vee B_2$ separates Γ_L from Γ_R, contrary to the assumption that Γ is divisible without separation. $Q.e.d.$.

Adding identity and function symbols

The case with identity (but without function symbols) is reduced to the case without identity by replacing $=$ with a non-logical predicate symbol $\equiv$.

Terminology:
Let E_A [E_C] be the conjunction of the equivalence axioms and the congruence axioms for the predicates in A [C] (using $\equiv$ for the congruence relation).
F^* ... F, where $=$ is replaced by $\equiv$.

Fact:
Any interpolant B^* from $E_A \wedge A^*$ to $E_C \rightarrow C^*$ can be re-translated into an interpolant B from A to C.

Similarly, appropriate 'definitions' of functions by predicates allow to reduce the case with function symbols to the case without function symbols. [[Detais in [BBJ]]]

Combining theories — joint consistency

DEF:
A theory T (in L) is a set of sentences (over L) that is closed w.r.t. logical consequence: $T \models F$ implies $F \in T$.
F is also called a theorem of T.

Combining theories is an important and practically relevant topic in software verification.
[Can you explain why?]

Note:
For satisfiable theories T_1, T_2, in general:

- $T_1 \cup T_2$ is not a theory
- the theory $\{F : T_1 \cup T_2 \models F\}$ is not satisfiable

even if the languages $L(T_1)$ and $L(T_2)$ are disjoint.

Lemma:
Let T_1, T_2 be theories. $T_1 \cup T_2$ is satisfiable iff there is no sentence $A \in T_1$, where $\neg A \in T_2$.

Note:

- The lemma expresses the following:
  joint satisfiability = joint consistency
  (Note that this is a kind of completeness statement!)
- The lemma is wrong for many non-classical logics.

Proof: The 'only if' part is trivial.

The 'if' part follows from compactness and interpolation:
Suppose $T_1 \cup T_2$ is unsatisfiable, then already some finite $S_0 \subseteq T_1 \cup T_2$ is unsatisfiable.
We will show that there is an $A \in T_1$, where $\neg A \in T_2$.

Let $\{F_1, \ldots, F_m\} = S_0 \cap T_1$ and $\{G_1, \ldots, G_n\} = S_0 \cap T_2$.
Note: If one of these two sets is empty, then already T_1 or T_2 is unsatisfiable. In that case, we may take $A = \forall x\, x = x$ or $A = \neg\forall x\, x = x$, respectively.

Let $A = F_1 \wedge \ldots \wedge F_m$ and $C = \neg(G_1 \wedge \ldots \wedge G_n)$.
$\{A, \neg C\}$ is unsatisfiable, therefore $A \models C$.

Consider the interpolant B from A to C:

$A \in T_1$ and $A \models B$, therefore $B \in T_1$.
Similarly, $\neg C \in T_2$ and $\neg C \models \neg B$, therefore $\neg B \in T_2$.

Thus B is the required $A \in T_1$, where $\neg A \in T_2$. $Q.e.d.$.

Joint consistency (ctd.)

DEF: Theory T' is a conservative extension of theory T if $T \subseteq T'$ and every $F \in T'$ over $L(T)$ is already in T.

Theorem: (Joint conservative extensions theorem)
For $i = 0, 1, 2$ let T_i be a theory over L_i, where $L_0 = L_1 \cap L_2$.
Let T_3 consist of the consequences of $T_1 \cup T_2$ over $L_1 \cup L_2$.
If T_1 and T_2 are conservative extensions of T_0, then so is T_3.

Proof: We have to show: $B \in T_3$ for B in L_0 implies $B \in T_0$.
$B \in T_3$ implies $T_1 \cup T_2 \cup \{\neg B\}$ is unsatisfiable.
By the above Lemma, for some $D \in T_1$: $\neg D \in T_2 \cup \{\neg B\}$, where D is in L_0. Hence also $\neg B \to \neg D$ is in L_0.
$T_2 \cup \{\neg B\} \models \neg D$, $\neg B \to \neg D \in T_2$. Since T_2 is a conservative extensions of T_0, we conclude $\neg B \to \neg D \in T_0$. Since T_1 is a conservative extensions of T_0, we have $D \in T_0$. But $\{D, \neg B \to \neg D\} \models B$, and therefore $B \in T_0$. $Q.e.d.$.

Joint consistency (ctd.)

Corollary: (Robinson's joint consistency theorem)
For $i = 0, 1, 2$ let T_i be a theory over L_i, where $L_0 = L_1 \cap L_2$.
If T_0 is complete, and $T_1 \supseteq T_0$ as well as $T_2 \supseteq T_0$ are satisfiable, then $T_1 \cup T_2$ is satisfiable.

Proof:
Any satisfiable extension of a complete theory is conservative.
Any conservative extension of a satisfiable theory is satisfiable.
Thus if the T_i are as specified, then we may apply the joint conservative extensions theorem to conclude that the theory consisting of all consequences of $T_1 \cup T_2$ is satisfiable.
Therefore $T_1 \cup T_2$ itself is satisfiable. $Q.e.d.$.

Note:
We have proved Robinson's joint consistency theorem
using Craig's interpolation theorem.
Also the converse is possible. (See [BBJ], page 265.)

In any case:
the (term) model existence lemma is essentially involved
in proving all of the following:

- ◇ Compactness theorem
- ◇ Löwenheim-Skolem theorem
- ◇ Completeness (in different versions)
- ◇ Craig's interpolation theorem
- ◇ Robinson's joint consistency theorem
- ◇ Beth's definability theorem