Mechanising Craig's Interpolation Theorem for Intuitionistic Logic in Isabelle

University of St Andrews Computer Science Research Report
Peter Chapman

Ridge's paper "Craig's Interpolation Theorem formalised and mechanised in Isabelle/HOL" uses a classical sequent calculus [2]. We will concentrate rather on the intuitionistic case. This has some benefits, in that certain cases are ruled out due to the restriction on the succedents in sequents. We begin by giving the full informal proof of the theorem, of which only a sketch is usually given in the literature [3], and then proceed to alter Ridge's *Isabelle* theory files to formalise this case.

1 The Informal Proof

The theorem can be stated, specific to the intuitionistic case, as follows;

> Suppose $\Gamma\Gamma' \Rightarrow D$. Then, there exists an F such that
>
> 1. $\Gamma \Rightarrow F$ and $\Gamma', F \Rightarrow D$.
> 2. Any predicate that occurs positively in F occurs positively in Γ and D and negatively in Γ'.
> 3. Any predicate that occurs negatively in F occurs negatively in Γ and D and positively in Γ'.

We write this more succinctly as $\Gamma; \Gamma' \overset{F}{\Longrightarrow} D$. The proof then proceeds as in cut admissibility, by case analysis.

1.1 Axioms

1.1.1 Ax

In the case where the derivation of $\Gamma\Gamma' \Rightarrow D$ ends with an axiom, with D an atomic formula P, there are two cases. The first has $P \in \Gamma$ so Γ is Γ'', P, and the other where $P \in \Gamma'$ so Γ' is Γ''', P. In the former, we need to find a formula A such that

$$\Gamma, P \Rightarrow A \text{ and } A, \Gamma' \Rightarrow P$$

A suitable candidate is $A \equiv P$, which would make both axioms too. Therefore, for this case we have $\Gamma, P; \Gamma' \overset{P}{\Longrightarrow} P$.

In the other case, we require an A so that

$$\Gamma \Rightarrow A \text{ and } A, P, \Gamma' \Rightarrow P$$

which only hold for general Γ if we have $A \equiv \bot \supset \bot$; in other words, $\top$. Therefore, for this case we have $\Gamma; P, \Gamma' \overset{\bot \supset \bot}{\Longrightarrow} P$.

The properties from the theorem are easily verified.

1.1.2 L$\bot$

Again, we have two subcases depending on whether $\bot$ is in with Γ or Γ'. In the first case we have to find A such that

$$\Gamma, \bot \Rightarrow A \text{ and } A, \Gamma' \Rightarrow C$$

both hold. We could take $A \equiv C$, to make the left part of the formula an instance of $L\bot$ and the right an instance of Ax, but this only works if C is atomic, so instead we choose $A \equiv \bot$. Therefore, for this case we have $\Gamma, \bot; \Gamma' \overset{\bot}{\Longrightarrow} C$.

The other case, with $\bot$ in Γ', is equivalent to the same case in Ax, and so we have $\Gamma; \bot, \Gamma' \overset{\bot \supset \bot}{\Longrightarrow} C$.

1.2 Inductive Step; The Rules

1.2.1 $L\supset$

We make the distinction as to whether the formula $A \supset B$ appears with Γ or Γ'. From now on, we will say that the *left* case is where the principal formula is in Γ, and the *right* is where it is in Γ'.

1.2.2 Left Case

We look at the premisses of the rule $L\supset$, and using the induction hypothesis we must assign interpolants to each. We must then decide where to split each premiss to obtain a valid interpolant for the conclusion. So, we have

$$\frac{\Gamma, A \supset B, \Gamma \overset{C}{\Longrightarrow} A \quad \Gamma, B, \Gamma' \overset{D}{\Longrightarrow} E}{\Gamma, A \supset B; \Gamma' \Rightarrow E}$$

where either of the commas in the premisses could become semi-colons. Some brief experimentation reveals that we should split the first premiss as $\Gamma'; A \supset B, \Gamma$ and the second as $\Gamma, B; \Gamma'$. This gives us the four sequents $\Gamma' \Rightarrow C$, $A \supset B, \Gamma, C \Rightarrow A$, $\Gamma, B \Rightarrow D$ and $\Gamma', D \Rightarrow E$.

Taking the first and fourth of these we can create the deduction

$$\cfrac{\cfrac{\Gamma' \Rightarrow C}{\Gamma', C \supset D \Rightarrow C}\, w \quad \Gamma', D \Rightarrow E}{\Gamma', C \supset D \Rightarrow E}\, L\supset$$

whereas using the second and third we can create the deduction

$$\cfrac{\cfrac{A \supset B, \Gamma, C \Rightarrow A \quad \cfrac{\Gamma, B \Rightarrow D}{B, \Gamma, A \supset B, C \Rightarrow D}\, w}{\Gamma, A \supset B, C \Rightarrow D}\, L\supset}{\Gamma, A \supset B \Rightarrow C \supset D}\, R\supset$$

This is precisely the form we need, with the interpolant being $C \supset D$. We can therefore conclude that the following is a valid deduction for this case

$$\frac{\Gamma'; A \supset B, \Gamma \overset{C}{\Longrightarrow} A \quad \Gamma, B; \Gamma' \overset{D}{\Longrightarrow} E}{\Gamma, A \supset B; \Gamma' \overset{C \supset D}{\Longrightarrow} E}$$

1.2.3 Right Case

In this case, assuming via the induction hypothesis that the first premiss has interpolant C and the second premiss interpolant D, we split both premisses on the right, so $\Gamma; A \supset B, \Gamma' \overset{C}{\Longrightarrow} A$ and $\Gamma; B, \Gamma' \overset{D}{\Longrightarrow} E$. We then obtain the four sequents $\Gamma \Rightarrow C$, $\Gamma', A \supset B, C \Rightarrow A$, $\Gamma \Rightarrow D$ and $\Gamma', B, D \Rightarrow E$. Naturally, we pair them up according to contexts. The first and third premisses therefore give

$$\frac{\Gamma \Rightarrow C \quad \Gamma \Rightarrow D}{\Gamma \Rightarrow C \wedge D}\, R\wedge$$

whereas the remaining two sequents give

$$\cfrac{\cfrac{\Gamma', A\supset B, C \Rightarrow A}{\Gamma', A\supset B, C, D \Rightarrow A}\,w \quad \cfrac{\Gamma', B, D \Rightarrow E}{\Gamma', B, C, D \Rightarrow E}\,w}{\cfrac{\Gamma', A\supset B, C, D \Rightarrow E}{\Gamma', A\supset B, C\wedge D \Rightarrow E}\,L\wedge}\,L\supset$$

which gives us the required interpolant as $C \wedge D$:

$$\frac{\Gamma; A\supset B, \Gamma' \overset{C}{\Longrightarrow} A \quad \Gamma; B, \Gamma' \overset{D}{\Longrightarrow} E}{\Gamma; A\supset B, \Gamma' \overset{C\wedge D}{\Longrightarrow} E}$$

1.2.4 $R\supset$

Here there is only one possible way to split the antecedent, since there is no distinguished formula in it. We split the premiss on the right, and suppose the interpolant of the premiss is C. We therefore have the two sequents $\Gamma \Rightarrow C$ and $\Gamma', A, C \Rightarrow B$. Leaving the first alone, we have the simple deduction for the second

$$\frac{\Gamma', A, C \Rightarrow B}{\Gamma', C \Rightarrow A\supset B}\,R\supset$$

which gives us the interpolant for the whole as C:

$$\frac{\Gamma; A, \Gamma' \overset{C}{\Longrightarrow} B}{\Gamma; \Gamma' \overset{C}{\Longrightarrow} A\supset B}$$

1.2.5 $L\wedge$

1.2.6 Left Case

The only premiss of $L\wedge$ is $\Gamma, A, B, \Gamma' \Rightarrow D$. Assuming we give this an interpolant C, and split A, B likewise on the left, we get the two sequents $\Gamma, A, B \Rightarrow C$ and $\Gamma', C \Rightarrow D$. We leave the second of these alone, and taking the first we obtain the deduction

$$\frac{\Gamma, A, B \Rightarrow C}{\Gamma, A\wedge B \Rightarrow C}\,L\wedge$$

This is exactly the form we need for the conclusion of the rule, however, so we can conclude that C is the interpolant:

$$\frac{\Gamma, A, B; \Gamma' \overset{C}{\Longrightarrow} D}{\Gamma, A \wedge B; \Gamma' \overset{C}{\Longrightarrow} D}$$

1.2.7 Right Case

Again, this is fairly straightforward. We split the premiss in the same way as the conclusion, to obtain the sequents $\Gamma \Rightarrow C$ and $\Gamma', C, A, B \Rightarrow D$, assuming C is the interpolant. One application of $L\wedge$ on the second sequent gives us that C is likewise the interpolant for the conclusion:

$$\frac{\Gamma; A, B, \Gamma' \overset{C}{\Longrightarrow} D}{\Gamma; A \wedge B, \Gamma' \overset{C}{\Longrightarrow} D}$$

1.2.8 $R\wedge$

Again, we can only split the conclusion in one way, likewise we can only split the premisses in one way. Therefore, assuming that the interpolant for the first premiss is C and the interpolant for the second premiss is D, we get the four sequents $\Gamma \Rightarrow C$, $\Gamma', C \Rightarrow A$, $\Gamma \Rightarrow D$ and $\Gamma', D \Rightarrow B$. Pairing them up by context, we get

$$\frac{\Gamma \Rightarrow C \quad \Gamma \Rightarrow D}{\Gamma \Rightarrow C \wedge D}\ R\wedge$$

and

$$\cfrac{\cfrac{\cfrac{\Gamma', C \Rightarrow A}{\Gamma', C, D \Rightarrow A}\ w \quad \cfrac{\Gamma', D \Rightarrow B}{\Gamma', C, D \Rightarrow B}\ w}{\Gamma', C, D \Rightarrow A \wedge B}\ R\wedge}{\Gamma', C \wedge D \Rightarrow A \wedge B}\ L\wedge$$

which means that $C \wedge D$ is the interpolant:

$$\frac{\Gamma; \Gamma' \overset{C}{\Longrightarrow} A \quad \Gamma; \Gamma' \overset{D}{\Longrightarrow} B}{\Gamma; \Gamma' \overset{C \wedge D}{\Longrightarrow} A \wedge B}$$

1.2.9 $L\lor$

1.2.10 Left Case

Assume that the interpolant for the first premiss is C, and the interpolant for the second premiss is D. Now, split both of the premisses on the left, to obtain the four sequents $\Gamma, A \Rightarrow C$, $\Gamma', C \Rightarrow E$, $\Gamma, B \Rightarrow D$ and $\Gamma', D \Rightarrow E$. Again, pairing up by contexts, we see that we have

$$\frac{\Gamma', C \Rightarrow E \quad \Gamma', D \Rightarrow E}{\Gamma', C \lor D \Rightarrow E}\ L\lor$$

and

$$\frac{\dfrac{\Gamma, A \Rightarrow C}{\Gamma, A \Rightarrow C \lor D}\ R\lor \quad \dfrac{\Gamma, B \Rightarrow D}{\Gamma, B \Rightarrow C \lor D}\ R\lor}{\Gamma, A \lor B \Rightarrow C \lor D}\ L\lor$$

This means the required interpolant is $C \lor D$, giving a derivation:

$$\frac{\Gamma, A; \Gamma' \stackrel{C}{\Longrightarrow} E \quad \Gamma, B; \Gamma' \stackrel{D}{\Longrightarrow} E}{\Gamma, A \lor B; \Gamma' \stackrel{C \lor D}{\Longrightarrow} E}$$

1.2.11 Right Case

Again, we split both premisses on the right, which gives us the sequents, assuming that C and D are the interpolants, $\Gamma \Rightarrow C$, $\Gamma', A, C \Rightarrow E$, $\Gamma \Rightarrow D$ and $\Gamma', B, D \Rightarrow E$. Combining these gives the deductions

$$\frac{\Gamma \Rightarrow C \quad \Gamma \Rightarrow D}{\Gamma \Rightarrow C \land D}\ R\land$$

and

$$\frac{\dfrac{\dfrac{\Gamma', A, C \Rightarrow E}{\Gamma', A, C, D \Rightarrow E}\ w \quad \dfrac{\Gamma', B, D \Rightarrow E}{\Gamma', B, C, D \Rightarrow E}\ w}{\Gamma', A \lor B, C, D \Rightarrow E}\ L\lor}{\Gamma', A \lor B, C \land D \Rightarrow E}\ L\land$$

meaning that $C \land D$ is the interpolant, as shown below:

$$\frac{\Gamma; A, \Gamma' \stackrel{C}{\Longrightarrow} E \quad \Gamma; B, \Gamma' \stackrel{D}{\Longrightarrow} E}{\Gamma; A \lor B, \Gamma' \stackrel{C \land B}{\Longrightarrow} E}$$

1.2.12 $R\vee$

We can only split this in one way, and likewise the premiss. Suppose the interpolant from the induction hypothesis is C, and assume further that we used the rule $R\vee_1$. Then we have the sequents $\Gamma \Rightarrow C$ and $\Gamma', C \Rightarrow A$. Using the rule $R\vee_1$ on the second, we obtain $\Gamma', C \Rightarrow A \vee B$. Therefore the interpolant in this case is C, and is given by the deduction

$$\frac{\Gamma; \Gamma' \overset{C}{\Longrightarrow} A}{\Gamma; \Gamma' \overset{C}{\Longrightarrow} A \vee B}$$

We get the same result if $R\vee_2$ was used in both situations.

1.2.13 $L\forall$

1.2.14 Left Case

We split the premiss in the same way as the conclusion. Therefore we have the sequents $\Gamma, \forall x A, [t/x]A \Rightarrow C$ and $\Gamma', C \Rightarrow D$, where C is the interpolant. The first sequent leads to the derivation

$$\frac{\Gamma, \forall x A, [t/x]A \Rightarrow C}{\Gamma, \forall x A \Rightarrow C}\ L\forall$$

which, when used with the other sequent, gives us that the interpolant for this rule is simply C:

$$\frac{\Gamma, \forall x A, [t/x]A; \Gamma' \overset{C}{\Longrightarrow} D}{\Gamma, \forall x A; \Gamma' \overset{C}{\Longrightarrow} D}$$

1.2.15 Right Case

We split the premiss in the same way as the conclusion. This gives us sequents $\Gamma \Rightarrow C$ and $\Gamma', \forall x A, [t/x]A, C \Rightarrow D$. One application of $L\forall$ on the latter supplies C as the interpolant for the whole formula:

$$\frac{\Gamma; \forall x A, [t/x]A, \Gamma' \overset{C}{\Longrightarrow} D}{\Gamma; \forall x A, \Gamma' \overset{C}{\Longrightarrow} D}$$

1.2.16 $R\forall$

There is only one way to split the context of the conclusion, and likewise only one way to split the premiss. Assuming C to be the interpolant of the premiss, we get the two sequents $\Gamma \Rightarrow C$ and $\Gamma', C \Rightarrow [y/x]A$. The rule $R\forall$ requires that y is not free for the antecedent. By assumption we have that y is not in the free variables of Γ', however we may still have free variables in C. To ensure that y cannot be a free variable of the interpolant, we remove all free variables of C by universal quantification over them. Thus we have one application of $R\forall$ on the left derivation, and one application of $L\forall$ followed by an application of $R\forall$ for the other:

$$\cfrac{\cfrac{\Gamma', C \Rightarrow [y/x]A}{\Gamma', \forall\vec{x}C \Rightarrow [y/x]A}}{\Gamma', \forall\vec{x}C \Rightarrow \forall xA}$$

where $\vec{x}$ are the free variables of C. Thus, we have that the interpolant is $\forall\vec{x}C$:

$$\frac{\Gamma; \Gamma' \overset{C}{\Longrightarrow} [y/x]A}{\Gamma; \Gamma' \overset{\forall\vec{x}C}{\Longrightarrow} \forall xA}$$

1.2.17 $L\exists$

1.2.18 Left Case

As is often the case, we split the premiss on the left as well. Therefore, we have the two sequents $\Gamma, [y/x]A \Rightarrow C$ and $\Gamma', C \Rightarrow D$, where C is the interpolant supplied by the induction hypothesis. As in the case for $R\forall$, the side condition on the rule means that y cannot be free for the deduction. This means we have to remove any possible free variables in the left premiss. The rule $R\exists$ does not have any side conditions about the freeness of variables, so we use that to get the interpolant:

$$\cfrac{\cfrac{\Gamma, [y/x]A \Rightarrow C}{\Gamma, [y/x]A \Rightarrow \exists\vec{x}C}}{\Gamma, \exists xA \Rightarrow \exists\vec{x}C}$$

where, as before, $\vec{x}$ are the free variables of C. We can use $L\exists$ without restriction in the second premiss, so the interpolant is $\exists\vec{x}C$:

$$\frac{\Gamma, [y/x]A; \Gamma' \overset{C}{\Longrightarrow} D}{\Gamma, \exists xA; \Gamma' \overset{\exists\vec{x}C}{\Longrightarrow} D}$$

1.2.19 Right Case

Splitting the premiss in the same way as the conclusion, we get the sequents $\Gamma \Rightarrow C$ and $\Gamma', [y/x]A, C \Rightarrow D$. In order to apply $L\exists$ in the second of these, we need to ensure that y is not free for C. We do this using the rule $L\forall$, since this does have any side conditions. Therefore we get the deduction

$$\dfrac{\dfrac{\Gamma', [y/x]A, C \Rightarrow D}{\Gamma', [y/x]A, \forall\vec{x}C \Rightarrow D}}{\Gamma', \exists xA, \forall\vec{x}C \Rightarrow D}$$

where we have $\vec{x}$ are the free variables of C. We can apply $R\forall$ to the other derivation, thus obtaining $\forall\vec{x}C$ as the interpolant:

$$\dfrac{\Gamma; [y/x]A, \Gamma' \overset{C}{\Longrightarrow} D}{\Gamma; \exists xA, \Gamma' \overset{\forall\vec{x}C}{\Longrightarrow} D}$$

1.2.20 $R\exists$

There is only one way to split both the conclusion and the premiss here, which gives us the sequents, if C is the interpolant for the premiss, $\Gamma \Rightarrow C$ and $\Gamma', C \Rightarrow [t/x]A$. Using the latter of these, we get

$$\dfrac{\Gamma', C \Rightarrow [t/x]A}{\Gamma', C \Rightarrow \exists xA}\ L\exists$$

which means that the interpolant in this case C, as can be seen below:

$$\dfrac{\Gamma; \Gamma' \overset{C}{\Longrightarrow} [t/x]A}{\Gamma; \Gamma' \overset{C}{\Longrightarrow} \exists xA}$$

2 Differences between the Intuitionistic and Classical Systems

When we move from the classical system, where the succedents can be multisets, to the intuitionistic system, where we can only have single formulae on the right, a few issues arise. From the side of proof theory, it means that some of the rules need to be rewritten, or discarded entirely. From the practical side, the implementation needs to be changed slightly to allow for this difference.

2.1 Theoretical Considerations

In the classical system, the rule for disjunction on the right allows for both subformulae of the disjunction to be carried into the premiss:

$$\frac{\Gamma \Rightarrow \Delta, A, B}{\Gamma \Rightarrow \Delta, A \vee B} \; R\vee$$

This is something that is not possible in the intuitionistic system; we need to introduce two right disjunction rules picking out which formula (A or B) is present in the premiss.

We can also remove entirely the rule *WR*, since it relies on adding something to the succedent. For this to be feasible, we would need an empty succedent, which is not possible. We can also remove the rules for negation, and simply deal with this as a special case of implication.

A large problem, however, is that the rules for implication have been omitted from Ridge's treatment. This is because the classical tautology $A \supset B \equiv \neg A \vee B$ allows us to form implications without explicitly introducing a new connective. Unfortunately, the above tautology is not intuitionistically valid; we need all the connectives as primitives rather than formed from the others.

When we introduce the two rules for dealing with an implication, we need to be aware that a *positive* occurrence of $A \supset B$ has A as a *negative* subformula, and B as a *positive* subformula. Since this is a fundamental part of the theorem, we need to be careful to model this correctly.

The theorem we are proving in the intuitionistic case is somewhat different as well. In the classical case, we need to split the succedent as well as the antecedent, to choose where the interpolant "goes". This extra step is avoided, making the proof considerably simpler.

2.2 Practical Implications

In Ridge's case, it was necessary to model sequents as pairs of sets of formulae. For our purposes, it suffices to model sequents as pairs consisting of a set of formulae (the antecedent) and a single formula (the succedent). This means that where Ridge has the condition that, for instance, $A \wedge B \in \Delta_1$, we need the condition $A \wedge B \equiv C$, where C is the "general" succedent. All of the rules in the implementation must be changed in this way, however it is a minor undertaking and causes no unforeseen problems.

The adding of implication as a primitive, as stated above, needs to be treated correctly when considering positive and negative occurrences in a sequent. However, due to the way that the functions *pos* and *neg* are defined, we can simply add the rules

- $pos\ (\supset AB) = (neg\ A) \cup (pos\ B)$
- $neg\ (\supset AB) = (pos\ A) \cup (neg\ B)$

3 The Formal Proof

Details of the implementation can be found in Ridge's paper. It is very easy to understand, since it does not rely on heavily on terms, so the structure of the deduction can be seen directly.

We will begin with the propositional fragment. For the most part, the proof is fairly similar to the classical one. The only differences arise when the informal proof for the classical system diverges from the intuitionistic informal proof. As stated early, we will also have fewer cases due to the lack of a context-split on the right hand side. However, we can easily adapt the formal proof for the cases where informal proofs (roughly) coincide. Given all of the rules, we apply `case-tac` which gives us a subgoal for every different final rule. Some massaging of the proposition then takes place to get it in a suitable state, after which we split again for the different clauses of the theorem.

The first of these subgoals is always the existence of the two deductions that give us $\Gamma \Rightarrow F$ and $\Gamma', F \Rightarrow C$. We simply encode the relevant deduction from the informal proof. As an example, consider the case where we have the last rule used being $R\wedge$. For the sake of readability, we have represented certain ASCII characters in their more normal form:

$$
\begin{array}{lcl}
\text{let dlr}' & = & \text{WeakL}(\{C, D\} \cup \Gamma', A)\ \text{dlr in} \\
\text{let dlr}'' & = & \text{WeakL}(\{C \wedge D, C, D\} \cup \Gamma', A)\ \text{dlr}'\ \text{in} \\
\text{let dlr}''' & = & \text{FConjL}(\{C \wedge D\} \cup \Gamma', A)\ \text{dlr}''\ \text{in} \\
 & & \\
\text{let drr}' & = & \text{WeakL}(\{C, D\} \cup \Gamma', B)\ \text{drr in} \\
\text{let drr}'' & = & \text{WeakL}(\{C \wedge D, C, D\} \cup \Gamma', B)\ \text{drr}'\ \text{in} \\
\text{let drr}''' & = & \text{FConjL}(\{C \wedge D\} \cup \Gamma', B)\ \text{drr}''\ \text{in} \\
 & & \\
 & & \text{FConjR}(\{C \wedge D\} \cup \Gamma', A \wedge B)\ \text{dlr}'''\ \text{drr}'''
\end{array}
$$

This corresponds to the derivation in §1.2.8 (except that the rules $L\wedge$ and $R\wedge$ have been permuted), with the extra weakening being a requirement of the implementation. The deduction *dlr* has root $\Gamma', C \Rightarrow A$, and the deduction drr has root $\Gamma', D \Rightarrow B$. These are supplied by *Isabelle* as part of the induction hypothesis. We, in turn, supply this deduction as a witness for $\exists dr.\text{root } dr = \Gamma', C \wedge D \Rightarrow A \wedge B$.

3.1 Some Problems

Earlier we said that Ridge avoided using $\supset$ as a primitive. As was expected, these cases gave the most problems. The "existence of derivation" part of the theorem was relatively straightforward to implement, we simply needed to be careful that we split correctly in the left-case for $L \supset$ (see §1.2.1). What caused more problems was the polarity part of the theorem. Since we have $C \supset D$ as the interpolant, we need some additional lemmas to handle implication. Most notable is one which states if $C \supset D \in \Gamma$, then $\text{pos}(\Gamma) \cup \text{pos}(D) = \text{pos}(\Gamma)$, and the three equivalent lemmas (one for positivity with C, one for negativity with D and one for negativity with C). Without these the theorem is not provable.

In general, however, any problems can quickly be overcome, either by a slight restating of certain properties, or the introduction of new, basic lemmas which are given to the simplifier.

3.2 Notes on the implementation

In this section we will give details of what various tactic lines within the proof script actually do. When reading an *Isabelle* proof script, we have little idea of why a particular tactic was used, since we cannot see the proof state (unless we are actually stepping through the proof). More details can be found in [1],[4].

A proof state in *Isabelle* is in two sections, the premisses, which we can assume, and the conclusion, which we have to show, using the premisses and perhaps some additional lemmas:

1. $[|\ A_0\ ;\ \ldots\ ;\ A_n\ |] \Rightarrow C$

where C may be some general formula. Tactics known as *elim* rules work on the structure of the hypotheses. For instance, if A_0 was the formula $A_{0,0} \wedge \ldots \wedge A_{0,m}$, then the tactic `apply (elim conjE)` would remove the formula A_0 from the premisses, and add all the individual formulae $A_{0,0}, \ldots, A_{0,m}$. The *intro* tactics, on the other hand, are for use in the conclusion. So if C was $C_0 \wedge \ldots \wedge C_k$ and we used the tactic `intro conjI`, *Isabelle* would remove the original subgoal and replace it with $k+1$ new subgoals, each with the same set of premisses.

If we have a quantified formula in the premisses, we can instantiate it using the tactic `drule-tac x=A in spec` where x refers to the *outermost* quantifier, and A is what we wish to instantiate it with. `drule` refers to the fact that this is a destructive rule; we remove the quantified formula and replace it with the instantiated formula. We can also instantiate in the conclusion; we use the tactic `rule-tac x=A in exI` where x is the marker for the outermost (existential) quantifier, and A is what we wish to use as the instance.

References

[1] T. Nipkow, L. Paulson, and M. Wenzel. *A Proof Assistant for Higher-Order Logic.* Number 2283 in Lecture Notes in Computer Science. Springer-Verlag, 2005.

[2] T. Ridge. Craig's interpolation theorem formalised and mechanised in Isabelle/HOL. *Logic in Computer Science*, 2006.

[3] A. S. Troelstra and H. Schwichtenberg. *Basic Proof Theory.* Number 43 in Cambridge Tracts in Computer Science. Cambridge University Press, second edition, 2000.

[4] M. Wenzel. *Isabelle/Isar Reference Manual*, 2002.