# 15-399 Supplementary Notes: Proof Search

Robert Harper

July 26, 2006

## Sequent Calculus

Gentzen's *sequent calculus* may be seen as a "meta-logic" for performing proof search in natural deduction. Roughly speaking, to find a proof of the hypothetical judgement

$$A_1\ \mathit{true}, \ldots, A_n\ \mathit{true} \vdash A\ \mathit{true},$$

we work both ends towards the middle, proceeding "upwards" from the goal, $A$, and "downwards" from the hypotheses, $A_i$, until a derivation can be found. This process is formalized by the concept of a *normal proof*, which is one that follows this strategy; it always suffices to search for a normal proof when searching for a proof.

The sequent calculus transforms this "bidirectional" search for a normal proof into a "unidirectional", or *goal-directed*, search. Sequent calculus has one categorical judgement form, the *sequent*, written

$$A_1, \ldots, A_n \Rightarrow A,$$

whose intended meaning is that

$$A_1{\downarrow}, \ldots, A_n{\downarrow} \vdash A{\uparrow}$$

is derivable according to the rules of normal proofs in natural deduction. The propositions on the left of the "$\Rightarrow$" are called the *premises*, or *antecedents*, of the sequent, and the proposition on the right is called its *goal*, or *succedent*.

The key feature of sequent calculus is that *all primitive rules are introduction rules*, which means that we may always work "bottom-up" from the intended goal to find a derivation whose leaves are *initial sequents* of the form

$$A_1, \ldots, A_n \Rightarrow A_i.$$

To check whether a proposition $A\ \mathit{true}$ is derivable, we search for a proof in sequent calculus of the *final sequent*, $\Rightarrow A$, whose antecedent is empty and whose succedent is the intended goal.

It turns out that we may arrange the rules of the sequent calculus so as to minimize indeterminacy and to guarantee that the search process terminates, either with a derivation of the intended proposition, or with the assurance that no derivation exists. Indeterminacy inevitably arises because of arbitrary choices that must be made during the search. For example, if the goal is a disjunction $A = A_1 \vee A_2$, then the decision to pursue a proof of $A_1$ must be reconsidered if that effort fails; perhaps $A_2$ is provable after all, or perhaps neither is provable (in which case $A$ is not provable). Other sources of indeterminacy are inessential. For example, if the goal is $A = A_1 \wedge A_2$, then we may choose at any time to decompose this into two sub-goals, $A_1$ and $A_2$, without fear of losing our way, since both conjuncts must be proved in any case.

## Gentzen's LJ

The sequent calculus LJ is defined by the following rules of inference:

$$\frac{}{\Gamma, A \Rightarrow A}\ (\mathit{init})$$

$$\frac{}{\Gamma \Rightarrow \top}\ (\top R)$$

$$\frac{}{\Gamma, \bot \Rightarrow A}\ (\bot\, L)$$

$$\frac{\Gamma, A, B \Rightarrow C}{\Gamma, A \wedge B \Rightarrow C}\ (\wedge L) \qquad \frac{\Gamma \Rightarrow A \quad \Gamma \Rightarrow B}{\Gamma \Rightarrow A \wedge B}\ (\wedge R)$$

$$\frac{\Gamma, A \Rightarrow C \quad \Gamma, B \Rightarrow C}{\Gamma, A \vee B \Rightarrow C}\ (\vee L) \qquad \frac{\Gamma \Rightarrow A}{\Gamma \Rightarrow A \vee B}\ (\vee R_1^*) \quad \frac{\Gamma \Rightarrow B}{\Gamma \Rightarrow A \vee B}\ (\vee R_2^*)$$

$$\frac{\Gamma, A \supset B \Rightarrow A \quad \Gamma, B \Rightarrow C}{\Gamma, A \supset B \Rightarrow C}\ (\supset L^*) \qquad \frac{\Gamma, A \Rightarrow B}{\Gamma \Rightarrow A \supset B}\ (\supset R)$$

All rules, except those marked with an asterisk, are *invertible*, which means that the premises are derivable if the conclusion is derivable. Equivalently, there is no loss of generality in applying an invertible rule whenever it makes sense to do so. Thus, the only sources of indeterminacy are those rules marked with an asterisk.

All "left" rules, except the rule $\supset L$ rule, have the property that the principal proposition of the inference occurs only in the conclusion, and not in any of the premises. This means that, when applied "backwards" during proof search, these rules drop the principal formula from the antecedent(s) of the sequent after the inference is applied, thereby ensuring that the same inference cannot be applied a second time.

The exception is the $\supset L$ rule, which propagates the principal formula, $A \supset B$, to the first premise (but not the second). This is essential for completeness! Were we not to do this, the rules would be too weak to capture

every possible proof. However, this means that we must be careful to avoid re-applying the same inference fruitlessly during proof search.

## Dyckhoff's Variant of LJ

Dyckhoff's variant of LJ avoids the problem with replication of the principal proposition of the $\supset L$ rule to the first premise by breaking down the inference into separate cases, according to the structure of the left-hand side of the implication. Specifically, the $\supset L$ rule is replaced by the following five special cases:

$$\frac{\Gamma, B \Rightarrow C}{\Gamma, \top \supset B \Rightarrow C}\ (\top \supset L) \qquad \frac{\Gamma \Rightarrow C}{\Gamma, \bot \supset B \Rightarrow C}\ (\bot \supset L)$$

$$\frac{\Gamma, A_1 \supset (A_2 \supset B) \Rightarrow C}{\Gamma, (A_1 \wedge A_2) \supset B \Rightarrow C}\ (\wedge \supset L) \qquad \frac{\Gamma, A_1 \supset B, A_2 \supset B \Rightarrow C}{\Gamma, (A_1 \vee A_2) \supset B \Rightarrow C}\ (\vee \supset L)$$

$$\frac{\Gamma, A_2 \supset B, A_1 \Rightarrow A_2 \quad \Gamma, B \Rightarrow C}{\Gamma, (A_1 \supset A_2) \supset B \Rightarrow C}\ (\supset \supset L)$$

Observe that, when read bottom-up, each rule replaces the principal premise of the inference, an implication, by premises of smaller "degree", where we measure the degree of a proposition by counting conjunctions as 2 and all other connectives as 1, adding them up to determine the degree of a proposition.

If we wish to accomodate atomic propositions other than $\bot$ and $\top$, then we must add the following rule to the preceding five rules governing implication on the left:

$$\frac{\Gamma, B, P \Rightarrow C}{\Gamma, P \supset B, P \Rightarrow C}\ (P \supset L)$$

## Proof Search

Dyckhoff's variant of LJ gives rise to a search procedure that determines whether or not a given proposition is provable in constructive logic. The procedure works by maintaining a collection of *partial derivations*, which it attempts to extend to a *complete derivation*, or determine that no completion is possible. A partial derivation is a finitely branching tree of sequents each of whose interior nodes is labelled by an LJ rule whose conclusion is that node and whose premises are the children of that node. A partial derivation may be *extended* by choosing a leaf node, labelling it with an LJ rule ending with that sequent, and adding children corresponding to the premises of the chosen rule. (Note that applying the rule for the initial sequent "closes off" the leaf, resulting in a node with no children.) A complete derivation is one for which there are no leaf nodes remaining; an incompletable derivation is one for which there is some leaf node that cannot be expanded by any rule.

A search procedure to determine whether or not a proposition $A$ is provable may be described as follows. Maintain a deck of cards on each of which is inscribed a partial derivation whose root is the final sequent $\Rightarrow A$. Initially, the deck consists of a single card with the partial derivation being the leaf $\Rightarrow A$. A step of the procedure consists of selecting a single card from the deck, and replacing it with zero or more new cards. If no cards remain to be chosen from the deck, the original goal is not provable; if the card is inscribed with a complete derivation, the process terminates with that derivation. Otherwise, the inscribed derivation contains at least one leaf sequent $B_1, \ldots, B_k \Rightarrow B$, which we select for expansion. On as many fresh cards as necessary, inscribe the result of expanding the chosen partial derivation by as many rules as apply at that leaf, inscribing one expansion per card. Discard the original, insert the newly incribed cards into the deck, and repeat the process.

At each step we replace one card with many cards, on each of which is inscribed an expansion of the partial derivation inscribed on the chosen card. The result of the expansion may contain fewer, the same, or more leaves than were present on the expanded derivation, corresponding to which rule is used to perform the expansion. Thus, in the worst case, there is, in two different senses, "more work" to be done as a result of a single step in the search process: many new derivations may replace the chosen one, each of which may contain more leaves than the expanded derivation. Why, then, does the process terminate? The key observation is that each new leaf in each new derivation is of a lesser degree than the leaf at which expansion is performed. Therefore, even though we replace a bit of "work" to be done with "more work", each new bit of work is "easier" than that represented by the chosen sequent. Since degrees are natural numbers, this process cannot continue forever — we must, at some point, finish what remains to be done (or realize that it is impossible to do so because no expansion applies).