15-414: Bug Catching: Automated Program Verification

Lecture Notes on Sequent Calculus

Matt Fredrikson*

Carnegie Mellon University
Lecture 13
Thursday, March 2, 2023

1 Introduction

In our quest for a formal (and hence implementable) theory of imperative programs, we specified programs and formulas in dynamic logic. We have also provided a collection of axioms that allow us break down the structure of complex programs into simpler ones, until we have a formula in arithmetic using the usual logical connectives such as equality and inequality, conjunction, disjunction, implication, and quantification. We have also formalized how to *calculate* weakest preconditions and strongest postconditions for a program, both of which are purely logical formulas without any reference to programs. What we have not yet specified is how we reason about such logical formulas—in our implementation we just mapped them map to corresponding formulas in Why3.

In this lecture we begin to close this gap and introduce the *sequent calculus* as a means to formalize logical reasoning. We do not yet talk about *arithmetic*, which will be the subject of another lecture. We think of the sequent calculus as a *human-oriented calculus* of proofs rather than a *machine-oriented calculus* which we will introduce in the next part of the course.

The sequent calculus was devised by Gentzen [**?**] as a way to prove the consistency of first-order logic and, ultimately, the consistency of arithmetic. *Consistency* here means that within a formal system of axioms and rules of inference we cannot derive a contradiction. Since then, the sequent calculus has found many related applications in logic, automated deduction, and programming languages. The course *15-317 Constructive*

*Closely adapted from notes written by Frank Pfenning in Spring 2022

Logic looks much more deeply into the sequent calculus and its applications in computer science.

In this lecture we focus somewhat narrowly on the sequent calculus as used in program verification.

Learning goals. After this lecture, you should be able to:

- Reproduce the inference rules of the sequent calculus for the usual logical connectives and quantifiers
- Use sequent calculus to prove simple logical entailments
- Employ the mathematical semantics of sequents to verify or refute the correctness of rules.

2 What is a Sequent?

Given formulas P_i and Q, a sequent has the form

$$P_1, \ldots, P_n \vdash Q$$

where $P_1, \ldots, P_n$ are the *antecedents* and Q is the *succedent* of the sequent. Logically, the P_i are *assumptions* and Q is the *goal* we are trying to prove. We usually abbreviate a sequent as $\Gamma \vdash Q$ where Γ stands for an (unordered) collection of antecedents.

Whenever you interact with Why3 in the IDE and examine the "Task" (a name for the verification condition for a part of the program), it is presented in the form of a sequent.

As an example, consider the theory of arrays, using the terminology `state` for arrays, `var` for the domain, and `int` for the codomain, as introduced for our formalization of dynamic logic. We would like to prove a simple property, namely that for two consecutive writes to the same index, the second one overwrites the first.

```
1  module ArrayTheory
2
3    type state   (* abstract *)
4    type var     (* abstract *)
5
6    (*********************************)
7    (* "array" operations and axioms *)
8    (*********************************)
9    function read (omega : state) (x : var) : int
10   function write (omega : state) (x : var) (v : int) : state
11
12   axiom read_eq : forall x y omega v.
13     x = y -> read (write omega x v) y = v
14   axiom read_ne : forall x y omega v.
15     x <> y -> read (write omega x v) y = read omega y
16
17   (* extensionality *)
```

```
18   axiom ext : forall omega nu.
19     (forall x. read omega x = read nu x) -> omega = nu
20
21   goal ex1 : forall omega x v1 v2.
22     read (write (write omega x v1) x v2) x = v2
23
24 end
```

In the Why3 IDE, if we highlight `ex1` and examine the Task, we see:

```
1  ---------------------------- Local Context ----------------------------
2  type state
3
4  type var
5
6  function read state var : int
7
8  function write state var int : state
9
10 axiom read_eq :
11   forall x:var, y:var, omega:state, v:int.
12    x = y -> read (write omega x v) y = v
13
14 axiom read_ne :
15   forall x:var, y:var, omega:state, v:int.
16    not x = y -> read (write omega x v) y = read omega y
17
18 axiom ext :
19   forall omega:state, nu:state.
20    (forall x:var. read omega x = read nu x) -> omega = nu
21
22 ------------------------------- Goal -------------------------------
23
24 goal ex1 :
25   forall omega:state, x:var, v1:int, v2:int.
26    read (write (write omega x v1) x v2) x = v2
```

The "local context" here contains the *antecedents* of the sequent and the part marked "goal" is the *succedent*. So a sequent is a convenient way to visualize and communicate the state of proof search.

3 Inference Rules

We now develop *inference rules* for breaking down goals into simpler ones, which is analogous the "splitting" a goal in Why3. For example, to break down a conjunction we have to prove both conjuncts.

$$\frac{\Gamma \vdash P \quad \Gamma \vdash Q}{\Gamma \vdash P \wedge Q} \wedge R$$

This is called the *right rule for conjunction* $\wedge R$ since it breaks down the right-hand side of the sequent.

The usual reading of such rule would be from the *premises* to the *conclusion*: *if P and Q are true, so is $P \wedge Q$*. We read these from the conclusion to the premises: *in order to prove $P \wedge Q$ it is sufficient to prove both P and Q*. We prefer this latter reading. For example, we make all antecedents in Γ available in both premises even if only a subset of them may ultimately be needed.

There is a corresponding *left rule* to break down an antecedent $P \wedge Q$:

$$\frac{\Gamma, P, Q \vdash R}{\Gamma, P \wedge Q \vdash R} \wedge L$$

This expresses that we can break down an assumption $P \wedge Q$ into separate assumptions P and Q.

The way we organize the sequent calculus is that for each logical operator we develop rules to break it down on the right and on the left of the turnstile $\vdash$. Let's consider implication $P \to Q$ as another example. In the right rule, we just assume P and proceed with the proof of Q.

$$\frac{\Gamma, P \vdash Q}{\Gamma \vdash P \to Q} \to R$$

Next, how do we *use an assumption $P \to Q$*? We use it to justify the assumption Q if we also have a proof of P. That is:

$$\frac{\Gamma \vdash P \quad \Gamma, Q \vdash R}{\Gamma, P \to Q \vdash R} \to L$$

This last rule is a little bit tricky, so it is fair to ask: how do we know the rules are correct? Before we can answer that we need to ask: what does it mean for a rule to be correct?

Ultimately, we should like to establish something like that formulas P are *valid*, that is, true for all possible assignment of values to variables. We write this as $\models P$. Because we want to prove *validity* we start with

$$\cdot \vdash P$$

and hope that a proof of P in the sequent calculus lets us conclude the validity of P. That suggests the following definition:

> *A sequent $P_1, \ldots, P_n \vdash Q$ is* valid *if the formula $P_1 \wedge \ldots \wedge P_n \to Q$ is valid.*

The next step this to define:

> *An inference rule is* sound *if the conclusion is valid if all premises are.*

In the bottom-up direction this means that if we can prove all the premises of a rule, then the original conclusion we were trying to deduce must be valid.

Let's check the soundness of the two rules for implication. For that, we recall the meaning of implication:

$$\omega \models P \to Q \quad \text{iff whenever } \omega \models P \text{ then } \omega \models Q$$

We write $\bigwedge\Gamma$ for the conjunction of all antecedents Γ. For the implication right rule we have to prove

If $\bigwedge\Gamma \wedge P \to Q$ is valid then $\bigwedge\Gamma \to (P \to Q)$ is valid.

So we assume

$$\forall\omega.\, \omega \models \bigwedge\Gamma \wedge P \to Q$$

We have to show that

$$\forall\nu.\, \nu \models \bigwedge\Gamma \to (P \to Q)$$

So, for an arbitrary ν we assume $\nu \models \bigwedge\Gamma$ and $\nu \models P$ and have to show $\nu \models Q$. Instantiate the assumption with $\omega = \nu$ and the fact that $\nu \models \bigwedge\Gamma \wedge P$. This allows us to conclude $\nu \models Q$, which is what we needed in this case.

To prove the left rule

$$\frac{\Gamma \vdash P \quad \Gamma, Q \vdash R}{\Gamma, P \to Q \vdash R}\ {\to}L$$

we assume $\forall\omega.\, \omega \models \bigwedge\Gamma \to P$ and $\forall\omega.\, \omega \models \bigwedge\Gamma \wedge Q \to R$. We have to show

$$\forall\nu.\, \nu \models \bigwedge\Gamma \wedge (P \to Q) \to R$$

We break this down, assuming $\nu \models \bigwedge\Gamma$, $\nu \models P \to Q$, with the goal of proving $\nu \models R$. Instantiating the first assumption (from the first premise) with $\omega = \nu$ we conclude $\nu \models P$, and from that $\nu \models Q$. Using the second assumption (from the second premise) we can use that to conclude $\nu \models R$, which is what we had to show.

We can also talk about the *completeness* of a set of inference rules. Here it would mean that if $\models P$ then $\cdot \vdash P$. This is true for Gentzen's sequent calculus, assuming that the quantifiers range over a domain about which we make no assumptions except that it is nonempty. If we quantify over integers the situation is more complicated.

4 The Difference Between Implication and Entailment

So, what is the difference between $P \vdash Q$ and $P \to Q$? One answer is that the first one is expresses the *validity* of $P \to Q$ while the latter expresses the *truth* of $P \to Q$. In particular, we can embed $P \to Q$ inside other formulas, such as as $(P \to Q) \to R$, which we cannot with entailment. A statement such as $(P \vdash Q) \vdash R$ is not permitted in the sequent calculus and would require the $\Box$ modality to express as a single formula.

Equally important is the pragmatic difference between the two. In proving a sequent $P \vdash Q$ we break down the structure of P and Q and apply rules (in the bottom-up direction) to make progress towards a proof. The discipline here is to apply the right

and left rules only once a formula has percolated to the top of the sequent. There are other calculi of so-called *deep inference* that allow applying rules to be applied anywhere *inside* a formula, but such a calculus has a fundamentally different nature from the sequent calculus.

A similar explanation applies to the difference, say, between $P \wedge Q$ and P, Q among the antecedents.

5 Multiple Conclusions

In Why3, or even while carrying out "ordinary mathematical reasoning", we usually have multiple antecedents (assumptions) but just one succedent (goal). In order to write our rules for *disjunctions* it is convenient to be able to "hedge our bet" and not (yet) commit to which disjunct is true. That is, instead of

$$\frac{\Gamma \vdash A}{\Gamma \vdash A \vee B} \vee R_1 \qquad \frac{\Gamma \vdash B}{\Gamma \vdash A \vee B} \vee R_2$$

we write

$$\frac{\Gamma \vdash A, B}{\Gamma \vdash A \vee B} \vee R$$

If, for example, A is again a disjunction we'd like to be able to apply this rule again. This means the succedent should allow multiple formulas interpreted disjunctively.

$$P_1, \ldots, P_n \vdash Q_1, \ldots, Q_k$$

which we abbreviate as

$$\Gamma \vdash \Delta$$

and is *valid* if $\bigwedge \Gamma \to \bigvee \Delta$.

For disjunction we then get the following two rules

$$\frac{\Gamma \vdash P, Q, \Delta}{\Gamma \vdash P \vee Q, \Delta} \vee R \qquad \frac{\Gamma, P \vdash \Delta \quad \Gamma, Q \vdash \Delta}{\Gamma, P \vee Q \vdash \Delta} \vee L$$

We can recognize $\vee L$ as a rule of cases: if we know P or Q we can distinguish both cases to prove Δ.

Before we move on, we should revisit the previous rules and generalize the succedents.

$$\frac{\Gamma \vdash P, \Delta \quad \Gamma \vdash Q, \Delta}{\Gamma \vdash P \wedge Q, \Delta} \wedge R \qquad \frac{\Gamma, P, Q \vdash \Delta}{\Gamma, P \wedge Q \vdash \Delta} \wedge L$$

$$\frac{\Gamma, P \vdash Q, \Delta}{\Gamma \vdash P \to Q, \Delta} \to R \qquad \frac{\Gamma \vdash P, \Delta \quad \Gamma, Q \vdash \Delta}{\Gamma, P \to Q \vdash \Delta} \to L$$

One thing you might notice is that, so far, we don't have any means to complete a proof in this format! A key rule for this is the so-called *identity* rule which completes a proof when an antecedent matches a succedent.

$$\frac{}{\Gamma, P \vdash P, \Delta}\ \mathsf{id}$$

Unlike the right and left rules for the connectives, this rule is independent of the formula P.

There is a counterpart of identity called *cut* that allows us to introduce a lemma P; we just need to make sure we can prove it before assuming it.

$$\frac{\Gamma \vdash P, \Delta \quad \Gamma, P \vdash \Delta}{\Gamma \vdash \Delta}\ \mathsf{cut}$$

While cut can be wonderfully helpful in proving things by hand, it is an obstacle if we consider the task of systematically (perhaps automatically) constructing a proof bottom up. It would require us the devise a (true) lemma P which can help us prove Δ, which presents essentially an infinite range of possibilities.

Gentzen's main theorem (his *Hauptsatz*) is that the rule of cut is redundant in the sense that if there is a proof with the cut rule then there is always another one (potentially much larger) that doesn't use cut. Because all other rules just decompose formulas or close off proofs, this property implies that the sequent calculus is consistent and cannot prove a contradiction.

6 Intuitionistic vs. Classical Reasoning

The rules we have presented so far model so-called *classical reasoning*, which is appropriate here due to the particular mathematical semantics we have given to formulas and sequents. There is also *constructive reasoning* which imposes a stronger burden of proof. For example, a proof of $P \to Q$ should provide an effective way to construct a proof of Q given a proof of P. Similarly, a proof of $P \vee Q$ should provide a method to decide whether P or Q is true. This different view of what is typically the same logical language is the subject of *15-317 Constructive Logic*. In constructive logic every proof, by its very nature, represents a program that can be executed. In this course we take programs to be separately defined and reasoned about in dynamic logic.

An example to illustrate the difference is $P \vee (P \to Q)$. Classically, this is valid: if P is true the left disjunct holds, and if P is false then the right disjunct holds. Constructively, it is not valid, because we cannot decide (without more knowledge about P and Q) which of the two disjuncts is true. The classical proof in the sequent calculus would be

$$\dfrac{\dfrac{\dfrac{}{P \vdash P, Q}\ \mathsf{id}}{\cdot \vdash P, P \to Q}\ {\to}R}{\cdot \vdash P \vee (P \to Q)}\ {\vee}R$$

As an intuitionist, I could object to this proof in two respects. First, I could say that you cannot hedge your bets but should decide between the two disjuncts at the $\vee R$ rule. This was Gentzen's way of making the distinction, insisting the there be a single succedent in the intuitionistic sequent calculus. It is also possible to accept a postponed choice, in which case the deeper flaw here would be in the $\to R$ rule. That's because the formula $P \to Q$ says the proof of Q may use the assumption P, but actually we then use P not to prove Q but the other disjunct (which may be considered "out of scope").

7 Quantification

To prove $\forall x.\, P(x)$ we have to prove $P(a)$ for an arbitrary a. In the proof rule we just have to make sure there are no spurious assumptions about a, that is, it doesn't yet occur in the sequent. Otherwise, we could prove formulas like $P(a) \to \forall x.\, P(x)$ which is certainly false if our domain of quantification has more than one element.

$$\frac{\Gamma \vdash P(a), \Delta \quad (a \text{ not in } \Gamma,\, P(x), \text{ or } \Delta)}{\Gamma \vdash \forall x.\, P(x), \Delta}\ \forall R$$

Because similar side conditions are common, they are sometimes omitted, just annotating the justification itself with a, indicating it must be "fresh".

$$\frac{\Gamma \vdash P(a), \Delta}{\Gamma \vdash \forall x.\, P(x), \Delta}\ \forall R^a$$

The left rule instantiates the quantifier with an arbitrary expression e. This instantiation must be a so-called *capture-avoiding substitution* or *uniform substitution*, making sure no variable confusion arises from the instantiation. We write $P(e)$ for the capture-avoiding substitution of e for x in $P(x)$.

$$\frac{\Gamma, P(e) \vdash \Delta}{\Gamma, \forall x.\, P(x) \vdash \Delta}\ \forall L$$

The issue that arises here is that we may need the quantifier more than once. Here is a simple example:

$$\forall x.\, x = f(x) \vdash a = f(f(a))$$

We need to instantiate x with a and then also with $f(a)$ to complete this proof. There are two standard ways of handling this: we can leave a copy of the quantified formula itself among the antecedents whenever we instantiate it. Another is to add an explicit rule

$$\frac{\Gamma, P, P \vdash \Delta}{\Gamma, P \vdash \Delta}\ \mathsf{contraction}L$$

For proof search, we actually think of this rule as *duplication*, but read in the traditional direction it is *contraction*. If we add this rule we have to carefully control its use during

proof search because we could easily create too many copies of P, flooding our search space. Similarly, we also have to control the instantiation of universally quantified antecedent which is an interesting and complex topic in the design of theorem provers.

Existential quantification is dual, with the role of the left- and right-hand sides reverse from universal quantification.

$$\frac{\Gamma \vdash P(e), \Delta}{\Gamma \vdash \exists x.\, P(x), \Delta}\ \exists R \qquad \frac{\Gamma, P(a) \vdash \Delta}{\Gamma, \exists x.\, P(x) \vdash \Delta}\ \exists L^a$$

The side condition that a be fresh applies here in the $\exists L$ rule. It turns out we also need a rule of contraction for the right-hand side.

$$\frac{\Gamma \vdash P, P, \Delta}{\Gamma \vdash P, \Delta}\ \mathsf{contraction}R$$

8 Summary

We have provided a set of rules for the usual connectives and quantifiers as all as the $\Box$ modality. We can also turn the axioms that break down the programs in dynamic logic into inference rules without problems. We have not yet discussed anything specific to the integers—everything was independent of the domain of quantification. We will follow up with rules regarding integers in the next lecture. We add the rules for negation

$\neg P$.

$$\frac{}{\Gamma, P \vdash P, \Delta}\ \mathsf{id} \qquad \frac{\Gamma \vdash P, \Delta \quad \Gamma, P \vdash \Delta}{\Gamma \vdash \Delta}\ \mathsf{cut}$$

$$\frac{\Gamma, P \vdash \Delta}{\Gamma \vdash \neg P, \Delta}\ \neg R \qquad \frac{\Gamma \vdash P, \Delta}{\Gamma, \neg P \vdash \Delta}\ \neg L$$

$$\frac{\Gamma \vdash P, \Delta \quad \Gamma \vdash Q, \Delta}{\Gamma \vdash P \wedge Q, \Delta}\ \wedge R \qquad \frac{\Gamma, P, Q \vdash \Delta}{\Gamma, P \wedge Q \vdash \Delta}\ \wedge L$$

$$\frac{\Gamma \vdash P, Q, \Delta}{\Gamma \vdash P \vee Q, \Delta}\ \vee R \qquad \frac{\Gamma, P \vdash \Delta \quad \Gamma, Q \vdash \Delta}{\Gamma, P \vee Q \vdash \Delta}\ \vee L$$

$$\frac{\Gamma, P \vdash Q, \Delta}{\Gamma \vdash P \to Q, \Delta}\ \to R \qquad \frac{\Gamma \vdash P, \Delta \quad \Gamma, Q \vdash \Delta}{\Gamma, P \to Q \vdash \Delta}\ \to L$$

$$\frac{\Gamma \vdash P, P, \Delta}{\Gamma \vdash P, \Delta}\ \mathsf{contraction} R \qquad \frac{\Gamma, P, P \vdash \Delta}{\Gamma, P \vdash \Delta}\ \mathsf{contraction} L$$

$$\frac{\Gamma \vdash P(a), \Delta}{\Gamma \vdash \forall x.\, P(x), \Delta}\ \forall R^a \qquad \frac{\Gamma, P(e) \vdash \Delta}{\Gamma, \forall x.\, P(x) \vdash \Delta}\ \forall L$$

$$\frac{\Gamma \vdash P(e), \Delta}{\Gamma \vdash \exists x.\, P(x), \Delta}\ \exists R \qquad \frac{\Gamma, P(a) \vdash \Delta}{\Gamma, \exists x.\, P(x) \vdash \Delta}\ \exists L^a$$

9 Intuitionistic vs. Classical Reasoning Revisited

As a mathematical example of the difference between intuitionistic and classical reasoning, let's consider the following proposition:

> *There exist irrational numbers a and b such that a^b is rational.*

Here is a classical proof of this proposition.

Consider $\sqrt{2}^{\sqrt{2}}$. There are two cases:

$\sqrt{2}^{\sqrt{2}}$ is rational.
Then $a = b = \sqrt{2}$ satisfy our proposition.

$\sqrt{2}^{\sqrt{2}}$ is irrational. Then $a = \sqrt{2}^{\sqrt{2}}$ and $b = \sqrt{2}$ satisfy our proposition
because $a^b = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^2 = 2$ is rational

Even though we have mathematically proven our proposition, we have avoided to give definitive irrational a and b that make a^b true. In other words, we have hedged our bets.

In intuitionistic logic, we would not accept the proof above as given because it does not exhibit witnesses for the existentials. However, it *does carry significant information*! From an intuitionists point of view, the above proof shows:

> *If $\sqrt{2}^{\sqrt{2}}$ is either rational or irrational, then there exist irrational a and b such that a^b is rational.*

This expresses if we can determine the status of $\sqrt{2}^{\sqrt{2}}$ then we can construct witnesses a and b, and the proof shows how to do that.

This example is not an isolated instance. An intuitionist can understand any classical proof as an intuitionistic one *but of a different theorem*, assuming some instances of the law of excluded middle. So intuitionistic logic is more expressive because we can *enforce* constructive existence with $\vdash P \vee Q$ (we must be able to prove either $\vdash P$ or $\vdash Q$) and $\vdash \exists x.\, P(x)$ (there must be a witness e such that $\vdash P(e)$) which classical logic can not.

In the proof above, once formalized in the sequent calculus, we would apply contraction on the right-hand side to obtain two copies of the existential. However, because it involves arithmetic we cannot fully formalize it in our pure sequent calculus. Here is another, purely logical example illustrating the difference.

$$\cdot \vdash \exists x.\, \forall y.\, P(x) \to P(y)$$

Is this even true? We reason as follows: either $P(z)$ is always true, in which case it doesn't matter which x we pick. Or $P(z)$ is false for some $z = a$. Then we use this a to instantiate x and the implication is true because $P(a)$ is false. Constructively, this reasoning fails because we don't actually construct a witness for the existential, we just say that either there is one or there isn't.

In the sequent calculus the classical proof with $\mathsf{contraction}R$ is the following:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{P(a), P(e) \vdash P(a), P(b)}\,\mathsf{id}}{P(a) \vdash P(e) \to P(a), P(b)}\,{\to}R}{\cdot \vdash P(e) \to P(a), P(a) \to P(b)}\,{\to}R}{\cdot \vdash P(e) \to P(a), \forall y.\, P(a) \to P(y)}\,\forall R^b}{\cdot \vdash P(e) \to P(a), \exists x.\, \forall y.\, P(x) \to P(y)}\,\exists R}{\cdot \vdash \forall y.\, P(e) \to P(y), \exists x.\, \forall y.\, P(x) \to P(y)}\,\forall R^a}{\cdot \vdash \exists x.\, \forall y.\, P(x) \to P(y), \exists x.\, \forall y.\, P(x) \to P(y)}\,\exists R}{\cdot \vdash \exists x.\, \forall y.\, P(x) \to P(y)}\,\mathsf{contraction}R$$

In this proof, the choice of e is irrelevant.

10 Some Aspects of Proof Search

When we use the sequent calculus for proof search then the rule of contraction (really: duplication when considered upwards) is impractical. Instead, we can analyze when we might need an assumption again, and when we can drop it. For example, in the rule

$$\frac{\Gamma, P, Q \vdash \Delta}{\Gamma, P \wedge Q \vdash \Delta}\ \wedge L$$

there is not need to "keep" $P \wedge Q$ among the antecedents since P and Q separately are strong enough to imply $P \wedge Q$. On the other hand, as already demonstrated we may need an assumption $\forall x.\, P(x)$ more than once. Such considerations lead to the following version of the sequent calculus without explicit rules for contraction.[11] We put the rule of cut in [brackets] because by Gentzen's cut elimination theorem it is in fact unnecessary. Even if it can shorten proofs considerably, during actually proof search it is often difficult to see what the formula P should be because it may be directly related to the formulas in the conclusion.

$$\frac{}{\Gamma, P \vdash P, \Delta}\ \mathsf{id} \qquad \left[\ \frac{\Gamma \vdash P, \Delta \quad \Gamma, P \vdash \Delta}{\Gamma \vdash \Delta}\ \mathsf{cut}\ \right]$$

$$\frac{\Gamma, P \vdash \Delta}{\Gamma \vdash \neg P, \Delta}\ \neg R \qquad \frac{\Gamma \vdash P, \Delta}{\Gamma, \neg P \vdash \Delta}\ \neg L$$

$$\frac{\Gamma \vdash P, \Delta \quad \Gamma \vdash Q, \Delta}{\Gamma \vdash P \wedge Q, \Delta}\ \wedge R \qquad \frac{\Gamma, P, Q \vdash \Delta}{\Gamma, P \wedge Q \vdash \Delta}\ \wedge L$$

$$\frac{\Gamma \vdash P, Q, \Delta}{\Gamma \vdash P \vee Q, \Delta}\ \vee R \qquad \frac{\Gamma, P \vdash \Delta \quad \Gamma, Q \vdash \Delta}{\Gamma, P \vee Q \vdash \Delta}\ \vee L$$

$$\frac{\Gamma, P \vdash Q, \Delta}{\Gamma \vdash P \to Q, \Delta}\ \to R \qquad \frac{\Gamma \vdash P, \Delta \quad \Gamma, Q \vdash \Delta}{\Gamma, P \to Q \vdash \Delta}\ \to L$$

$$\frac{\Gamma \vdash P(a), \Delta}{\Gamma \vdash \forall x.\, P(x), \Delta}\ \forall R^a \qquad \frac{\Gamma, \forall x.\, P(x), P(e) \vdash \Delta}{\Gamma, \forall x.\, P(x) \vdash \Delta}\ \forall L$$

$$\frac{\Gamma \vdash P(e), \exists x.\, P(x), \Delta}{\Gamma \vdash \exists x.\, P(x), \Delta}\ \exists R \qquad \frac{\Gamma, P(a) \vdash \Delta}{\Gamma, \exists x.\, P(x) \vdash \Delta}\ \exists L^a$$

In lecture we also discussed the so-called *invertibility* of rules in the version without cut: which rules can be applied "blindly" and which rules may require backtracking. In the classical formulation above with multiple conclusion, in fact *all rules are invertible*, that is, all premises are valid if and only if the conclusion is valid.

[11] This is slightly different from the rules presented in lecture.

The rules that would give us pause are first and foremost those that break a proof goal into two subgoals, which are $\wedge R$, $\vee L$, and $\to L$. For example, the $\vee L$ rule splits a proof into considering two cases. But it is possible that in fact the proof doesn't require this case split, in which case we have simply duplicated our work. If we have multiple disjunctions, we might in fact do an exponential amount of unnecessary work.

The other rules to treat with caution are $\forall L$ and $\exists R$ because they (necessarily) preserve the principal formula of the rule so they could be applied infinitely often, for different terms e.

In practice, human-oriented prover interfaces tend to avoid multiple conclusions because they are not very intuitive. In those case other rules are generally available so every valid sequent can still be proved. For example, we could "reduce" $\Gamma \vdash A \vee B$ to $\Gamma, \neg A, \neg B \vdash \bot$, proceeding indirectly. We put "reduction" in quotes because even though we eliminate the disjunction, we introduce two negations, so the nature of the rules changes somewhat.

11 Validity of Formulas[13]

An important aspect of reasoning about programs was the modal operator $\Box P$, expressing that P is *valid*. We needed this, for example, when reasoning with loop invariants.

$$[\alpha^*]Q \leftarrow J \wedge \Box(J \to [\alpha]J) \wedge \Box(J \to Q)$$

Recall the semantics:

$$\omega \models \Box P \quad \text{iff } \nu \models P \text{ for every } \nu$$

The first approximation of our right rule would say that we have to forget all our assumptions, because they may not be true in every ν, while the left rule just deduces the truth of P from its validity.

$$\frac{\cdot \vdash P}{\Gamma \vdash \Box P, \Delta}\,\Box R \qquad \frac{\Gamma, P \vdash \Delta}{\Gamma, \Box P \vdash \Delta}\,\Box L$$

It is easy to convince oneself that these rules are *sound*: if the premises are valid, so are the conclusions. However, they are incomplete in a strange way. For example, we cannot prove $\Box(P \to Q) \to \Box P \to \Box Q$. Let's pause after two $\to R$ rules

$$\Box(P \to Q), \Box P \vdash \Box Q$$

If we try to use $\Box R$ we get stuck immediately because we are left to prove Q without assumptions. But even if we strip the boxes on the left with the $\Box L$ rules, the situation does not change fundamentally. We need to *generalize* our right rule $\Box R$ so that all antecedents of the form $\Box -$ survive. That's justified because such formulas are assumed to be *valid*. We write

$$\frac{\Box\Psi \vdash P}{\Box\Psi, \Gamma \vdash \Box P, \Delta}\,\Box R$$

[13] This material was not covered in lecture.

where $\Box\Psi$ means that every formula in Ψ is of the form $\Box -$.

While these rules are now better, there are still some shortcomings which can addressed by explicitly distinguishing antecedents that are *valid* from those that are *merely true* (see [**?**]).

Assuming there are no assumptions about validity for formulas, we can now turn our axiom for reasoning with invariants,

$$[\alpha^*]Q \leftarrow J \wedge \Box(J \rightarrow [\alpha]J) \wedge \Box(J \rightarrow Q)$$

into an inference rule

$$\frac{\Gamma \vdash J, \Delta \quad J \vdash [\alpha]J \quad J \vdash Q}{\Gamma \vdash [\alpha^*]Q, \Delta}\ \mathsf{inv}$$

Note how we have dropped Γ and Δ in the second and third premise to reflect the validity requirements for these entailments.

Other axioms decomposing programs in dynamic logic are bi-implications and can therefore easily be turned into inference rules. For example:

$$\frac{\Gamma \vdash [\alpha][\beta]P, \Delta}{\Gamma \vdash [\alpha\,;\,\beta]P, \Delta}\ [;]R \qquad \frac{\Gamma, [\alpha][\beta]P \vdash \Delta}{\Gamma, [\alpha\,;\,\beta]P \vdash \Delta}\ [;]L$$

We won't bother with the remaining rules.

References