EECS3342 System Specification and Refinement
Fall 2026

Digest of Lecture 13, October 29, 2026

Sequent Proofs via Inference Rules

Jackie Wang

How to use this Digest

Use this digest as a **roadmap and checklist**. It highlights the main ideas, important examples, common pitfalls, practice targets, and where to return in the course materials. It does **not** replace attending or reviewing the session, using the recording when needed, studying Jackie's annotated iPad notes and other official course materials, completing assigned work, or practising independently. Use it to identify what you understand, what you need to revisit, and what you should be able to do on your own.

If time is limited, start with the sections most relevant to your current review and return to the rest later; selective use is better than skipping the digest because it looks long.

This is an AI-assisted study roadmap reviewed by Jackie and grounded in the session transcript and Jackie's annotated iPad notes. Like any course document, it may still contain an error or omission. If something seems technically doubtful or inconsistent with the original course materials, return to those materials and ask Jackie for clarification rather than treating the digest as final authority.

Table of Contents

Main Ideas 2

Roadmap 2

Key Terms, Notation, and Structures 4

Key Examples and Demonstrations 5

Common Pitfalls and Misconceptions 6

What You Should Be Able to Do 6

Suggested Practice 7

Where to Review 7

Closing Reminder 8

Main Ideas

- The session moved from **stating invariant-preservation proof obligations** to actually **proving sequents with inference rules**. The running example was the Bridge Controller obligation `ML_out/inv0_1/INV`.
- A sequent and an inference rule are related but different objects. A sequent such as $H \vdash G$ is something to prove; an inference rule tells you how one sequent may be rewritten into one or more new sequents that are sufficient to prove instead.
- **Monotonicity (MON)** is the first major proof step: remove hypotheses that are not useful for the current goal. For the worked `ML_out` proof, MON reduces the original obligation to $n \in \mathbb{N} \vdash n + 1 \in \mathbb{N}$, which then matches the Peano axiom rule $P2$ exactly.
- Inference-rule application requires **exact pattern matching**. Extra hypotheses cannot simply be ignored informally when applying an axiom rule; they must first be removed by a valid rule such as MON.
- Some rules branch. The **OR_L** rule turns one sequent with a disjunctive hypothesis into two independent proof branches. Both branches must be discharged; they are not recombined later in the proof process used in this course.
- For assessment planning, Written Test 2 is scheduled for **November 18**. Jackie said the inference rules needed for the test will be provided as a PDF reference; the goal is therefore operational fluency with the rules rather than memorizing their statements.

Roadmap

1. Immediate priorities and upcoming assessment work

Jackie identified **Written Test 2 on November 18** as the remaining scheduled in-term test. The guide and practice questions are expected at least one week in advance, and the covered inference rules will be provided as a PDF reference during the test. For Written Test 2 preparation, Jackie specifically asked students to revisit the earlier lecture material on how adding invariants or events, or modifying event guards, changes the generated proof obligations and which existing obligations must be revisited. He also stated that **Lab 3 is due Wednesday, November 4**. A further programming-test review opportunity was announced for **Wednesday, November 4, 1:30–3:30 p.m.**, with Shanru available for students who want to inspect their submission before deciding whether to request a regrade.

2. Reconstructing one invariant-preservation sequent

The technical work began by returning to the formal invariant-preservation rule and instantiating one concrete proof obligation: `ML_out/inv0_1/INV`. The hypotheses come from the context axiom, all pre-state invariants, and the guard of the selected event. The goal is only the selected invariant in the post-state.

For the current M_0 model, the sequent is

$$\begin{array}{c} d \in \mathbb{N} \\ n \in \mathbb{N} \\ n \leq d \\ \text{true} \end{array} \quad \vdash \quad n+1 \in \mathbb{N}.$$

The post-state form is obtained by first thinking of $n' \in \mathbb{N}$ and then using the before-after predicate $n' = n + 1$. Jackie emphasized that the primed intermediate form and explanatory comments are scratchwork; the final sequent should contain the substituted goal.

3. Reading an inference rule backward

The general inference-rule shape is

$$\frac{\mathcal{A}}{\mathcal{C}}\ L,$$

where $\mathcal{C}$ is the single consequent sequent to prove, $\mathcal{A}$ is a set of antecedent sequents, and L names the rule. Operationally, start from $\mathcal{C}$ and rewrite backward: **to prove $\mathcal{C}$, it is sufficient to prove all sequents in $\mathcal{A}$.** If the antecedent is empty, the consequence is an axiom/base case and closes that proof branch.

4. Monotonicity as hypothesis pruning

The MON rule used in class is

$$\frac{H_1 \vdash G}{H_1, H_2 \vdash G}\ \text{MON}.$$

The bottom sequent is the current obligation. Applying MON lets you continue with the same goal G while keeping only the hypotheses grouped as H_1 and dropping the irrelevant group H_2.

Jackie's practical advice was to inspect the **goal first**: identify the variables that matter, then decide which hypotheses are actually useful. MON is not merely cosmetic; it is often needed before a later rule can match exactly.

5. Completing the first proof with an axiom rule

For `ML_out/inv0_1/INV`, the goal $n + 1 \in \mathbb{N}$ points directly to the hypothesis $n \in \mathbb{N}$ as useful. MON removes the other hypotheses, leaving

$$n \in \mathbb{N} \vdash n + 1 \in \mathbb{N}.$$

This now matches the Peano axiom rule $P2$ exactly, so the branch closes. The important lesson is the proof architecture:

$$\text{generated PO} \longrightarrow \text{recursive rewrite rule(s)} \longrightarrow \text{axiom/base case}.$$

6. From linear derivations to proof trees: OR_L

The OR_L rule handles a disjunctive hypothesis:

$$\frac{H, P \vdash R \qquad H, Q \vdash R}{H, P \vee Q \vdash R}\ \text{OR_L}.$$

Applying the rule **splits** one obligation into two independent branches. The non-disjunctive hypotheses H are copied into both branches, while P and Q are considered separately. Both branches must prove the same goal R.

Jackie used a nuclear-reactor reliability example only to illustrate the shape: if reliable behavior is required under either normal-temperature operation or a high-temperature shutdown condition, the two cases must be proved separately.

7. First inference-rule set and preparation for the next proofs

The final page of Jackie's annotated iPad notes groups the rules into **axiom/base rules** and **recursive rules**. The session explicitly reviewed $P1$, $P2$, $P2'$, $P3$, INC, DEC, OR_L, and MON at a survey level, while MON and OR_L received the main worked development. OR_R1 and OR_R2 appeared on the rule sheet but were left for subsequent study rather than being worked through in this session. Jackie asked students to review the remaining recursive rules and prepare to continue with M_0 proofs in the next class.

Key Terms, Notation, and Structures

Sequent $H \vdash G$
An object-level statement to prove. Its logical reading is that the hypotheses H imply the goal G.

Inference rule $\dfrac{\mathcal{A}}{\mathcal{C}}\ L$
A named proof-rewriting rule. To prove the consequent sequent $\mathcal{C}$, it is sufficient to prove the antecedent sequent(s) in $\mathcal{A}$.

Axiom/base rule
An inference rule with no antecedent sequents. Reaching an exact match with its consequence closes that proof branch.

Recursive rule
A rule that rewrites the current proof obligation into one or more further sequents that must still be proved.

MON (Monotonicity)

$$\frac{H_1 \vdash G}{H_1, H_2 \vdash G}\ \text{MON}.$$

It preserves the goal and removes a group of hypotheses that are not needed for the intended proof.

OR_L

$$\frac{H, P \vdash R \qquad H, Q \vdash R}{H, P \vee Q \vdash R}\ \text{OR_L}.$$

A disjunction on the left of the turnstile creates two independent proof branches.

$P1$ **and** $P2$
Two Peano-number axiom rules emphasized in the session:

$$\vdash 0 \in \mathbb{N}, \qquad n \in \mathbb{N} \vdash n + 1 \in \mathbb{N}.$$

Key Examples and Demonstrations

Example 1: Formulating `ML_out/inv0_1/INV`

Setup. The model has constant d, variable n, axiom $d \in \mathbb{N}$, invariants $n \in \mathbb{N}$ and $n \leq d$, and the current `ML_out` guard is `true`. Its effect is $n' = n + 1$.

Main point. The invariant-preservation rule uses all axioms, all pre-state invariants, and the selected event guard as hypotheses, but proves only one selected post-state invariant at a time. For `inv0_1`, the post-state target $n' \in \mathbb{N}$ becomes $n + 1 \in \mathbb{N}$ by the BAP.

What to practise. Reconstruct PO2, PO3, and PO4 from the same rule, using Jackie's annotated iPad notes and the lecture material as the source of the exact model components.

Example 2: Proving PO1 with MON and $P2$

Starting point.

$$d \in \mathbb{N},\ n \in \mathbb{N},\ n \leq d,\ \text{true} \vdash n + 1 \in \mathbb{N}.$$

Decisive step. The goal depends on n, and the useful hypothesis is $n \in \mathbb{N}$. Apply MON to discard the other hypotheses, obtaining

$$n \in \mathbb{N} \vdash n + 1 \in \mathbb{N}.$$

This matches $P2$ exactly, so the proof closes.

Why the alternative is wrong. Applying $P2$ directly to the original sequent is invalid because the extra hypotheses prevent an exact match with the axiom-rule pattern.

Example 3: OR_L and two independent branches

Setup. Start with $H, P \vee Q \vdash R$.

Main point. OR_L replaces this one obligation by two: $H, P \vdash R$ and $H, Q \vdash R$. The common hypotheses H and goal R are copied to both branches; each disjunct is handled separately.

What to practise. Draw the two-branch proof-tree shape from Jackie's annotated iPad notes and explain why proving only one branch is insufficient.

Common Pitfalls and Misconceptions

- **Confusing sequents with inference rules.** A sequent is the statement to prove; an inference rule is a named mechanism for rewriting sequents during a proof.
- **Reading an inference rule in the wrong direction.** In proof construction, begin with the consequence at the bottom and move backward to the antecedent premise(s) that are sufficient to prove instead.
- **Ignoring extra hypotheses informally.** You cannot say that an axiom such as $P2$ applies just because its useful hypothesis appears somewhere in a larger hypothesis set. The entire sequent must match the rule pattern; use MON first when extra hypotheses must be removed.
- **Changing the goal when applying MON.** MON drops hypotheses; the goal remains unchanged.
- **Treating OR_L as a combination rule.** In this course it is used to split one obligation into two independent branches. Both branches must be discharged.
- **Including scratch annotations in a formal sequent answer.** Jackie used intermediate primed forms and comments to explain the construction, but told students not to include those explanatory scratch annotations as part of the final formal sequent on an assessment.

What You Should Be Able to Do

After this session, you should be able to:

- construct a concrete invariant-preservation sequent from the model's axioms, pre-state invariants, selected event guard, selected post-state invariant, and before-after predicate;
- explain why invariant preservation is proved **one invariant at a time for one event at a time**;
- distinguish the syntax and role of a sequent from those of an inference rule;
- read an inference rule backward as a proof step: identify the current consequence and the antecedent sequent(s) that are sufficient to prove instead;
- apply MON by partitioning the hypotheses into useful and removable groups while preserving the goal;
- justify why an axiom rule such as $P2$ requires exact pattern matching rather than informal omission of extra hypotheses;

- reproduce the proof skeleton for `ML_out/inv0_1/INV`: formulate the PO, apply MON, and close with $P2$;
- apply OR_L to a disjunctive hypothesis and represent the result as two independent branches that must both be proved;
- distinguish axiom/base rules from recursive rules in the first rule set and recognize the role each type plays in a complete proof tree.

Suggested Practice

1. **Reconstruct the remaining invariant-preservation obligations.** Starting from the M_0 model, write PO2, PO3, and PO4 yourself rather than copying them from the solution material.
2. **Reproduce the PO1 proof from understanding.** Begin with the full sequent, identify relevant variables and hypotheses, apply MON, and explain why the resulting sequent matches $P2$ exactly.
3. **Compare the rule shapes.** Put $H \vdash G$ beside $\frac{A}{C}\ L$ and explain, in your own words, which is the proof obligation and which is the proof-rewriting mechanism.
4. **Redraw OR_L as a proof tree.** Start from $H, P \lor Q \vdash R$, split it into the two required branches, and identify what is copied and what changes between the branches.
5. **Review the first inference-rule sheet.** Jackie explicitly recommended becoming familiar with the rules before the next class. Focus on recognizing the green axiom/base cases versus the red recursive cases, and practise reading each rule from consequence to antecedent(s).
6. **Revisit the earlier proof-obligation generation page for Written Test 2.** Review how adding an invariant, adding an event, or modifying an event guard changes the proof obligations that must be generated or revisited.

Where to Review

- **Jackie's annotated iPad notes, p. 3:** construction of `ML_out/inv0_1/INV`, including the BAP substitution from the post-state invariant to $n + 1 \in \mathbb{N}$.
- **Jackie's annotated iPad notes, pp. 4–6:** inference-rule syntax/semantics, MON, and the side-by-side distinction between a sequent and an inference rule.
- **Jackie's annotated iPad notes, pp. 7–8:** the worked PO1 proof, the valid MON-to-$P2$ path, the invalid direct-$P2$ alternative, and the general proof-step/base-case structure.
- **Jackie's annotated iPad notes, p. 9:** OR_L, its two-branch interpretation, and the informal reactor example used to explain why both disjunctive cases must establish the same goal.

- **Jackie's annotated iPad notes, p. 10:** the first inference-rule collection, with green axiom/base rules and red recursive rules. Use this page to review $P1$, $P2$, $P2'$, $P3$, INC, DEC, OR_L, OR_R1, OR_R2, and MON at the level introduced in this session.
- **Course lecture site:** the newly posted resource described in class as "Notes - example inference rule number one," which Jackie said summarizes the first set of inference rules needed for the coming lectures.

Closing Reminder

Use this digest as a roadmap for active review, not as a substitute for the learning process itself. Attend Jackie's in-person sessions and pay attention to how he develops ideas and works through the important reasoning step by step. If a transition, explanation, example, or reasoning step remains unclear afterwards, return to the recording to fill that gap.

For structured review, start with Jackie's annotated iPad notes because they most closely reflect the actual flow and development of the class. Work through them in manageable logical units. After each logical unit, study the corresponding part of the presentation slides alongside it. Jackie does not normally teach by reading the slides line by line, so the slides may contain relevant supporting material that was not explicitly read aloud.

Finally, choose a suitable selection of the important reasoning from this session and work through it again on your own. In particular, reconstruct at least one invariant-preservation sequent, carry out the MON-to-axiom proof structure, and redraw the OR_L branching pattern from understanding. The goal is not to memorize Jackie's recorded steps, but to determine whether you can reproduce the reasoning from your own understanding and explain why the important steps work.