Homework 1
Propositional Sequent Calculus

15-316: Software Foundations of Security & Privacy
Frank Pfenning

Due Tuesday, September 10, 2024
70 points

Your solution should be handed in as file `hw1.pdf` to Gradescope. If at all possible, write your solution in LaTeX. The handout `hw1-seq.zip` includes the LaTeX sources for Lecture 2 (`02-prop.tex`) and the necessary style files which provide some examples for rules, derivations, and proofs.

1 Validity and Counterexamples (20 points)

For each of following sequents, either show a sequent calculus derivation as evidence that it is valid, or show an incomplete derivation where all leaves consist only of propositional variables. In the latter case, also read off all assignments of truth values to propositional variables that are counterexamples to the validity of the original sequent. (This technique was shown at the beginning of Lecture 3.)

Task 1 (5 points) $\cdot \vdash ((p \to q) \to p) \to p$

Task 2 (5 points) $\cdot \vdash ((p \to q) \to q) \to p$

Task 3 (5 points) $\neg(p \wedge q) \vdash (\neg p) \wedge (\neg q)$

Task 4 (5 points) $(\neg p) \wedge (\neg q) \vdash \neg(p \wedge q)$

2 Rule Design (40 points)

In this problem we ask you to give right and left sequent calculus rules for some logical constants and a new connective. Whatever rules you give should preserve all the good properties of the sequent calculus for propositional logic, that is:

(a) They should be *sound*.

(b) They should be *invertible*.

(c) All their premises should be smaller than the conclusion, when counting the number of logical connectives and constants $\top$ and $\bot$ in a sequent.

The last two items combine to entail completeness and decidability. **You only need to prove these properties when explicitly asked but your rules should nonetheless satisfy them. When you do write out proofs, please follow the template for $\to L$ (soundness, page L2.11) and $\vee R$ (invertibility, page L2.12) in the lecture notes to make them easy for us to grade.**

Task 5 (5 points) *Give right and left rules for the logical constant $\top$ (truth).*

Task 6 (5 points) *Given right and left rules for the logical constant $\bot$ (falsehood).*

We define a new connective $F \mathbin{\overline{\wedge}} G$ by the following truth table.

F	G	$F \mathbin{\overline{\wedge}} G$
$\top$	$\top$	$\bot$
$\top$	$\bot$	$\top$
$\bot$	$\top$	$\top$
$\bot$	$\bot$	$\top$

In the remainder of this problem we ask you to give right and left rules for this new connective. These rules should preserve all the good properties listed at the beginning of the problem.

Task 7 (5 points) *Give the right rule or rules for $\overline{\wedge}$.*

Task 8 (5 points) *Prove your right rule(s) are* sound.

Task 9 (5 points) *Prove your right rule(s) are* invertible.

Task 10 (5 points) *Give the left rule or rules for $\overline{\wedge}$.*

Task 11 (5 points) *Prove your left rule(s) are* sound.

Task 12 (5 points) *Prove your left rule(s) are* invertible.

3 Cut (10 points)

Gentzen's system also included the rule of *cut* which can introduce a lemma F into a proof: the first premise proves it while the second premise assumes it. Here is one way to formulate it:

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

Task 13 (5 points) *Prove that the rule of* cut *is* sound.

Task 14 (5 points) *Prove that the rule of* cut *is* redundant, *that is, if we can prove a sequent using it, we can also prove it without using this rule.*

So cut is sound but redundant. It can be used to shorten proofs, but it is not easy to devise strategies for finding appropriate formulas F (which is unknown if you apply this rule bottom-up, as we do during proof search).