Logic and Proof

Exercises

2021

Contents

1. Introduction

1. Determine whether the truth value of the following sentences is true, false, unknown, or if the sentence is not a proper logical statement. Justify all of your answers, and give satisfying and falsifying valuations of the variables where appropriate.

   a) Broccoli is delicious.

   b) x likes broccoli.

   c) The area of a circle of radius r is πr^2.

   d) Larry Paulson was born in x.

   e) Larry Paulson est né aux États-Unis.

   f) This sentence is false.

   g) Every even number greater than 2 can be written as the sum of two primes.

   h) There exists a unique prime n that satisfies $a^n + b^n = c^n$ for some positive integers a, b and c.

   i) There are two people in Peterborough with the exact same number of hairs on their head.

2. a) Write two closed statements (without variables): one true and one false.

   b) Write three statements with at least two variables: one valid, one satisfiable and one unsatisfiable. Give satisfying and falsifying interpretations where appropriate.

   c) Write a set S of at least three statements containing at least one (common) variable such that every statement is satisfiable, but the set is inconsistent.

2. Propositional logic

1. Verify de Morgan's laws and Peirce's Law using truth tables.

2. Each of the following formulas is satisfiable but not valid. Exhibit an interpretation that makes the formula true and another that makes the formula false.

$$P \to Q \qquad \neg(P \lor Q \lor R) \qquad P \lor Q \to P \land Q \qquad \neg(P \land Q) \land \neg(Q \lor R) \land (P \lor R)$$

3. Associate each of the following terms with one of the propositional equivalences on Slide 205. Give a number-theoretic example for each property.

   unit, distributivity, idempotence, commutativity, inverse, associativity, annihilation

4. Convert each of the following propositional formulas into Conjunctive Normal Form and also into Disjunctive Normal Form. For each formula, state whether it is valid, satisfiable, or unsatisfiable; justify each answer.

$$(P \to Q) \land (Q \to P) \qquad ((P \land Q) \lor R) \land \neg(P \lor R) \qquad \neg(P \lor Q \lor R) \lor ((P \land Q) \lor R)$$

3. Proof systems for propositional logic

1. Briefly compare and contrast the following three formal proof systems:

   - Hilbert-style deductive system

- Gentzen-style natural deduction
- Gentzen-style sequent calculus

2. a) Proof systems employ many "if X then Y"-style connectives and assertions on different reasoning levels. Explain, with examples, the differences and similarities between

$$A \land B \to C \qquad A, B \vdash C \qquad A, B \vDash C \qquad A, B \Rightarrow C \qquad \frac{A \quad B}{C} \qquad \begin{array}{c}[A \land B]\\ \vdots \\ C\end{array}$$

   b) Separate the statements above based on whether they belong to the *syntax* or the *semantics* of propositional logic. Which proof systems are the constructs associated with?

3. Prove the following sequents:

$$\neg\neg A \Rightarrow A \qquad A \land B \Rightarrow B \land A \qquad (A \lor B) \land (A \lor C) \Rightarrow A \lor (B \land C)$$
$$\neg(A \lor B) \Rightarrow \neg A \land \neg B \qquad \Rightarrow (A \land \neg A) \to B \qquad \Rightarrow ((A \to B) \to A) \to A$$

   (You can write the proof trees upside-down if you prefer, so you don't have to reserve space.)

4. Derive the sequent calculus rules for the connectives $\longleftrightarrow$ (iff) and $\oplus$ (exclusive or). Note that other connectives must not appear in these rules.

4. First-order logic

1. To test your understanding of quantifiers, consider the following formulas: *everybody loves somebody* vs. *there is somebody that everybody loves*:

$$\forall x.\, \exists y.\, \mathsf{loves}(x, y) \qquad \exists y.\, \forall x.\, \mathsf{loves}(x, y)$$

   Does the first imply the second? Does the second imply the first? Consider both the informal meaning and the formal semantics defined in the course.

2. Let $\approx$ be a 2-place predicate symbol, which we write using infix notation as $x \approx y$ instead of $\approx(x, y)$.

   a) Give three formulas in FOL describing the axioms that make $\approx$ an *equivalence relation*.

   b) Let the universe be the set $\mathbb{N}$ of natural numbers. Which axioms hold if $I[\approx]$ is:

      (i) the empty relation, $\emptyset$?

      (ii) the universal relation, $\{(x, y) \mid x, y \in \mathbb{N}\}$?

      (iii) the equality relation, $\{(x, x) \mid x \in \mathbb{N}\}$?

      (iv) the relation $\{(x, y) \mid x, y \in \mathbb{N} \land x + y \text{ is even}\}$?

      (v) the relation $\{(x, y) \mid x, y \in \mathbb{N} \land x + y = 100\}$?

      (vi) the relation $\{(x, y) \mid x, y \in \mathbb{N} \land x \leq y\}$?

3. Taking R as 2-place relation symbol and $=$ denoting equality, consider the following axioms:

$$\forall x.\, \neg R(x,x) \tag{1}$$
$$\forall x,y.\, \neg(R(x,y) \land R(y,x)) \tag{2}$$
$$\forall x,y,z.\, R(x,y) \land R(y,z) \to R(x,z) \tag{3}$$
$$\forall x,y.\, R(x,y) \lor (x = y) \lor R(y,x) \tag{4}$$
$$\forall x,y.\, R(x,z) \to \exists y.\, R(x,y) \land R(y,z) \tag{5}$$

   a) Exhibit two interpretations that satisfy axioms 1–5.

   b) Exhibit two interpretations that satisfy axioms 1–4 and falsify axiom 5.

   c) Exhibit two interpretations that satisfy axioms 1–3 and falsify axioms 4 and 5.

   Hint: Consider simple examples such as $R(x,y) = x < y$ on some appropriate domain.

4. Some textbook and paper authors like to use nonstandard notation, or even define their own syntax for some particular formal system. While often difficult to read and generally not recommended, there is nothing inherently wrong with this practice – as long as the meaning (semantics) is defined appropriately, the syntax can be whatever the author chooses to use.

   Suppose that a particularly creative logician decides to reinvent the syntax of first-order logic. Below are three logically valid formulas written in the syntax which should hold for any formula A and predicate P and Q containing a free variable x.

$$\overbrace{\left[P(x), \boxed{P(x)}\right]}^{x} \qquad \boxed{\boxed{A}} \triangleright A \qquad \boxed{\overbrace{\left[P(x), \boxed{Q(x)}\right]}^{x}} \bowtie \underbrace{\left\langle \boxed{P(x)}, Q(x) \right\rangle}_{x}$$

   a) Describe the formal syntax of this logic as a grammar, giving the different syntactic forms of a formula A (see e.g. Slide 201). You may assume that the syntax already includes atomic formulas made up of a relation symbol $P, Q, R \ldots$ applied to some number of terms.

   b) Consider a formula A in the syntax presented above. Let $\mathcal{I}$ be an interpretation of the symbols and V a valuation for the formula. Give a *truth definition* for the formula A by defining a predicate $\models_{\mathcal{I},V} A$ which holds when A is true in $\mathcal{I}$ under V. Make sure that the three formulas above are true with your definition.

   c) The formula below is a statement about arithmetic on natural numbers. Give an interpretation $\mathcal{I} = (D, I)$ of the constant, function, and relation symbols, and a valuation V of the free variables, which satisfy this formula.

$$\left\langle \overbrace{\left[n \sim \bullet, \underbrace{n \sim k^{+}}_{k} \right]}^{n}, \left\langle v \sim \bullet^{+++}, \boxed{\underbrace{\bullet \sim \ell^{+}}_{\ell}} \right\rangle \right\rangle$$

Optional exercise

1. Using OCaml, define datatypes for representing propositions and interpretations. Write a function to test whether or not a proposition holds under an interpretation (both supplied as arguments). Write a function to convert a proposition to Negation Normal Form.

5. Formal reasoning in first-order logic

1. a) For each of the following FOL formulas, circle the free variables, and underline the bound variables. Connect each bound variable to its binding occurrence (either graphically, by numbering, or whatever works for you).

   i. $\forall x.\ x = x$

   ii. $\exists x.\ P(x, y) \land \forall y.\ \neg P(y, x)$

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

   iv. $\exists z.\ P(x, y) \land Q(x, z)$

   v. $\forall x.\ (P(x) \to Q(x)) \land S(x, y)$

   vi. $P(x, \forall z.\ (\exists x.\ Q(y, x)) \to Q(x, z))$

   b) Apply the substitution $[x \mapsto f(x, y), y \mapsto g(z)]$ to the formulas above.

2. Consider the following proof attempt of the set-theoretic conjecture:

$$\forall A, B.\ \mathcal{P}(A \cup B) = \mathcal{P}(A) \cup \mathcal{P}(B)$$

   Proof. Let A, B be sets. We prove the proposition using equational reasoning:

$$\begin{aligned}
\mathcal{P}(A \cup B) &= \{X \mid X \subseteq A \cup B\} && \text{(def. of powerset)} \\
&= \{X \mid \forall x.\ x \in X \to x \in A \cup B\} && \text{(def. of subsets)} \\
&= \{X \mid \forall x.\ x \in X \to (x \in A \lor x \in B)\} && \text{(def. of union)} \\
&= \{X \mid \forall x.\ (x \in X \to x \in A) \lor (x \in X \to x \in B)\} && \text{(lemma of prop. logic)} \\
&= \{X \mid (X \subseteq A) \lor (X \subseteq B)\} && \text{(def. of subsets)} \\
&= \{X \mid X \subseteq A\} \cup \{X \mid X \subseteq B\} && \text{(def. of union)} \\
&= \mathcal{P}(A) \cup \mathcal{P}(B) && \text{(def. of powerset)} \quad \square
\end{aligned}$$

   Is this a valid proof? Why or why not?

3. Verify the following equivalences by appealing to the truth definition of FOL.

$$\neg(\exists x.\ P(x)) \simeq \forall x.\ \neg P(x) \qquad (\forall x.\ P(x)) \land R \simeq \forall x.\ (P(x) \land R)$$
$$(\exists x.\ P(x)) \lor (\exists x.\ Q(x)) \simeq \exists x.\ (P(x) \lor Q(x))$$

4. Prove the equivalence $(\forall x.\ P(x) \lor P(a)) \simeq P(a)$.

5. Prove the following sequents. *Hint*: the last one requires two uses of $(\forall l)$.

$$(\forall x.\ P(x)) \land (\forall x.\ Q(x)) \Rightarrow \forall y.\ (P(y) \land Q(y))$$
$$\forall x.\ P(x) \land Q(x) \Rightarrow (\forall y.\ P(y)) \land (\forall y.\ Q(y))$$

$$\forall x.\, P(x) \to P(f(x)), P(a) \Rightarrow P(f(f(a)))$$

6. Prove the following sequents. *Hint*: the last one requires two uses of $(\exists r)$.

$$P(a) \vee \exists x.\, P(f(x)) \Rightarrow \exists y.\, P(y)$$
$$\exists x.\, P(x) \vee Q(x) \Rightarrow (\exists y.\, P(y)) \vee (\exists y.\, Q(y))$$
$$\Rightarrow \exists z.\, P(z) \to P(a) \wedge P(b)$$

7. Prove the formula $\neg\forall y.\, (Q(a) \vee Q(b)) \wedge \neg Q(y)$ using equivalences, and then formally using the sequent calculus.

6. Clause methods for propositional logic

1. Outline the steps of the Davis–Putnam–Logeman–Loveland method. Explain the goal of the method, and why the steps of the algorithm are sound. Why does the empty clause represent a contradiction?
2. Apply the DPLL procedure to the clause set:

$$\{P, Q\} \qquad \{\neg P, Q\} \qquad \{P, \neg Q\} \qquad \{\neg P, \neg Q\}$$

3. Explain the resolution algorithm and how it differs from DPLL.
4. Use resolution (showing the steps of converting the formula into clauses) to prove at least three of the following formulas.

$$(P \to Q \vee R) \to ((P \to Q) \vee (P \to R))$$
$$((P \to Q) \to P) \to P$$
$$(Q \to R) \wedge (R \to P \wedge Q) \wedge (P \to Q \vee R) \to (P \leftrightarrow Q)$$
$$(P \wedge Q \to R) \wedge (P \vee Q \vee R) \to ((P \leftrightarrow Q) \to R)$$
$$(P \to R) \wedge (R \wedge P \to S) \to (P \wedge Q \to R \wedge S)$$

5. Convert these axioms to clauses, showing all steps. Then prove $\mathrm{Winterstorm} \to \mathrm{Miserable}$ by resolution.

$$\mathrm{Wet} \wedge \mathrm{Cold} \to \mathrm{Miserable}$$
$$\mathrm{Winterstorm} \to \mathrm{Storm} \wedge \mathrm{Cold}$$
$$\mathrm{Storm} \to \mathrm{Rain} \wedge \mathrm{Windy}$$
$$\mathrm{Rain} \wedge (\mathrm{Windy} \vee \neg\mathrm{Umbrella}) \to \mathrm{Wet}$$

7. Skolem functions, Herbrand's Theorem and unification

1. a) Explain the process of Skolemisation on a formula of your choice.

   b) The notes state that "[Skolemisation] does not preserve the meaning of a formula. However, it does preserve *inconsistency*, which is the critical property". Justify the two claims in this statement, demonstrating them on your example above.

2. Skolemize the following formulas, dropping all quantifiers.

$$\forall u.\, \exists x, y.\, P(x, y) \qquad \exists x, y.\, \forall z.\, \exists w.\, P(x, y, z, w) \qquad \forall u.\, (\exists x.\, P(x, x)) \land \forall v.\, \exists y.\, Q(u, y)$$

3. Consider a first-order language A with z and o as constant symbols, with n as a 1-place function symbol and a as a 2-place function symbol, and with C as a 2-place predicate symbol.

   a) Describe the Herbrand universe for this language.

   b) This language has an interpretation $\mathcal{I}$ in the domain $D = \mathbb{Z}$ of integers, with z and o interpreted as $0 \in \mathbb{Z}$ and $1 \in \mathbb{Z}$ respectively, n being the negation function $x \mapsto -x$, a being the addition function $x, y \mapsto x + y$, and C being the less-than comparison relation $x, y \mapsto x < y$. What is the Herbrand model of the symbols of the language with respect to this interpretation $\mathcal{I}$?

4. For at least three of the following pairs of terms, give a most general unifier or explain why none exists. Do not rename variables prior to performing the unification.

$$\begin{array}{rl}
f(g(x), z) & f(y, h(y)) \\
j(x, y, z) & j(f(y, y), f(z, z), f(a, a)) \\
j(x, z, x) & j(y, f(y), z) \\
j(f(x), y, a) & j(y, z, z) \\
j(g(x), a, y) & j(z, x, f(z, z))
\end{array}$$

5. Which of the following substitutions are most general unifiers for the terms $f(x, y, z)$ and $f(w, w, v)$?

$$[x/y, x/w, v/z] \qquad [y/x, y/w, v/z] \qquad [y/x, v/z]$$
$$[x/y, x/z, x/w, x/v] \qquad [u/x, u/y, u/w, y/z, y/v]$$

8. First-order resolution

1. What techniques allow us to convert first-order formulas into "propositional" clauses, and prove them using resolution? How are quantifiers and variables handled?

2. Is the clause $\{P(x, b), P(a, y)\}$ logically equivalent to the unit clause $\{P(a, b)\}$? Is the clause $\{P(y, y), P(y, a)\}$ logically equivalent to $\{P(y, a)\}$? Explain both answers.

3. Show that every set S of definite clauses is consistent. *Hint*: first consider propositional logic, then extend your argument to first order logic.

4. Convert the following formulas into clauses, showing each step: negating the formula, eliminating $\to$ and $\leftrightarrow$, pushing in negations, Skolemising, dropping the universal quantifiers, and

converting the resulting formula into CNF. Apply resolution (and possibly factoring) to prove or disprove the formulas in each case.

$$(\exists x.\ \forall y.\ R(x,y)) \to (\forall y.\ \exists x.\ R(x,y))$$
$$(\forall y.\ \exists x.\ R(x,y)) \to (\exists x.\ \forall y.\ R(x,y))$$
$$\exists x.\ \forall y,z.\ (P(y) \to Q(z)) \to (P(x) \to Q(x))$$
$$\neg(\exists y.\ \forall x.\ R(x,y) \leftrightarrow \neg(\exists z.\ R(x,z) \land R(z,x)))$$

5. Refute the following set of clauses using resolution and factoring.

$$① \{P(x,b), P(a,y)\} \qquad ② \{\neg P(x,b), \neg P(c,y)\} \qquad ③ \{\neg P(x,d), \neg P(a,y)\}$$

6. Prove the following formulas by resolution, showing all steps of the conversion into clauses. Note that P is just a predicate symbol, so in particular, x is not free in P.

$$(\forall x.\ P \lor Q(x)) \to (P \lor \forall x.\ Q(x)) \qquad \exists x,y.\ (R(x,y) \to \forall z,w.\ R(z,w))$$

9. Optional exercises

1. In your own words, explain the motivation behind Herbrand interpretations.
   - How is a Herbrand interpretation constructed from a set of clauses S?
   - Why do we need Herbrand interpretations?
   - What is the significance of the Skolem–Gödel–Herbrand Theorem?

   If you wish, consult a pre-2013 version of the course lecture notes, which discuss Herbrand models in more detail.

2. Consider the Prolog program consisting of the definite clauses

$$P(f(x,y)) \leftarrow Q(x), R(y)$$
$$Q(g(z)) \leftarrow R(z)$$
$$R(a) \leftarrow$$

   Describe the Prolog computation starting from the goal clause $\leftarrow P(v)$. Keep track of the substitutions affecting v to determine what answer the Prolog system would return.

10. Decision procedures and SMT solvers

1. In Fourier–Motzkin variable elimination, any variable not bounded both above and below is deleted from the problem. For example, given the set of constraints

$$3x \geq y \qquad x \geq 0 \qquad y \geq z \qquad z \leq 1 \qquad z \geq 0$$

   the variables x and then y can be removed (with their constraints), reducing the problem to $z \leq 1 \land z \geq 0$. Explain how this happens and why it is correct.

2. Apply Fourier–Motzkin variable elimination to the following sets of constraints.

a) ① $x \geq z$ ② $y \geq 2z$ ③ $z \geq 0$ ④ $x + y \leq z$

b) ① $x \leq 2y$ ② $x \leq y + 3$ ③ $z \leq x$ ④ $0 \leq z$ ⑤ $y \leq 4x$

3. Summarise the main ideas behind SMT solvers: how do they combine decision procedures with clause-based methods and what kinds of problems do they allow us to solve?

4. Apply the SMT algorithm sketched in the notes to the following set of clauses. Recall that the constraints $\boxed{c > 0}$ and $\boxed{c < 0}$ are unrelated.

$$\{c = 0, c > 0\} \qquad \{a \neq b\} \qquad \{c < 0, a = b\}$$

11. Binary decision diagrams

1. Compute the BDD for each of the following formulas, taking the variables as alphabetically ordered.

$$P \land Q \to Q \land P \qquad P \lor Q \to P \land Q \qquad \neg(P \lor Q) \lor P \qquad \neg(P \land Q) \leftrightarrow (P \lor R)$$

2. Verify these equivalences using BDDs.

$$(P \land Q) \land R \simeq P \land (Q \land R) \qquad (P \lor Q) \lor R \simeq P \lor (Q \lor R)$$
$$P \lor (Q \land R) \simeq (P \lor Q) \land (P \lor R) \qquad P \land (Q \lor R) \simeq (P \land Q) \lor (P \land R)$$
$$\neg(P \land Q) \simeq \neg P \lor \neg Q \qquad (P \leftrightarrow Q) \leftrightarrow R \simeq P \leftrightarrow (Q \leftrightarrow R)$$
$$(P \lor Q) \to R \simeq (P \to R) \land (Q \to R) \qquad (P \land Q) \to R \simeq P \to (Q \to R)$$

12. Modal logics

1. Explain why adding the T, 4 and B axioms make the transition relation reflexive, transitive and symmetric, respectively? Consider both the informal meaning and the formal semantics.

2. Why does the dual of an operator string equivalence also hold? For example, how can we deduce $\Diamond\Diamond A \simeq \Diamond A$ from $\Box\Box A \simeq \Box A$?

3. a) Prove the sequents $\Diamond(A \lor B) \Rightarrow \Diamond A, \Diamond B$ and $\Diamond A \lor \Diamond B \Rightarrow \Diamond(A \lor B)$, thus proving the equivalence $\Diamond(A \lor B) \simeq \Diamond A \lor \Diamond B$.

   b) Similarly, prove the equivalence $\Box(A \land B) \simeq \Box A \land \Box B$.

4. Prove the following sequents.

$$\Diamond(A \to B), \Box A \Rightarrow \Diamond B \qquad \Box\Diamond\Box A, \Box\Diamond\Box B \Rightarrow \Box\Diamond\Box(A \land B)$$

13. Tableaux-based methods

1. Use the free-variable tableau calculus to prove the following formulas.

$$(\exists y.\, \forall x.\, R(x,y)) \to (\forall x.\, \exists y.\, R(x,y))$$
$$(P(a,b) \lor \exists z.\, P(z,z)) \to \exists x,y.\, P(x,y)$$

$$((\exists x.\, P(x)) \to Q) \to (\forall x.\, P(x) \to Q)$$

2. Compare the sequent calculus, resolution and the free-variable tableau calculus by using each of them to prove the following formula.

$$(P(a, b) \lor \exists z.\, P(z, z)) \to \exists x, y.\, P(x, y)$$

Optional exercise

Temporal logic is not the only type of modal logic: depending on how we interpret $\Box A$, we can admit different axioms and relational properties for our logic. Some are of philosophical interest, while others have found use in computer science and mathematics. Below are a few examples:

Name	**Domain**	**Interpretation of $\Box A$**	**Interpretation of $\Diamond A$**
Temporal	time	A always holds	
Alethic	necessity		A possibly holds
Doxastic	belief	I believe that A holds	
Epistemic	knowledge		For all I know, A holds
Deontic	duty	It is obligatory that A holds	

a) Complete the table either by intuition or through research. Recall that $\Diamond A$ is defined as $\neg\Box\neg A$.

b) Assign each of the formulae below to the modal logics in which they could be reasonably assumed as axioms. For example, does belief of A imply the truth of A?

   a) $\Box(A \to B) \land \Box A \to \Box B$
   b) $\Box A \to A$
   c) $\Box A \to \Box\Box A$
   d) $\Diamond A \to \Box\Diamond A$
   e) $\Diamond\top$
   f) $\Box A \to \Diamond A$

c) *Provability logic* is an interesting variant of a modal logic which interprets $\Box A$ as "*A is provable in the theory T*" where T is some axiomatic system that we are working in (such as Peano arithmetic). What (if anything) can we say about a particular system T if we know that:

   (i) the formula $\Box A \to A$ is an axiom?
   (ii) the formula $\neg\Box\bot$ is an axiom?
   (iii) the formula $\Box A \to \Diamond A$ is *not* an axiom?