CS245 Logic and Computation

Alice Gao

December 9, 2019

Contents

1 Propositional Logic

1.1 Translations

Exercise 1. *Translate the following three sentences into propositional logic.*

- **Nadhi will eat a fruit if it is an apple.**
- **Nadhi will eat a fruit only if it is an apple.**
- **Nadhi will eat a fruit if and only if it is an apple.**

Solution: n: Nadhi will eat a fruit.
a: The fruit is an apple.

- **Nadhi will eat a fruit if it is an apple.**

  Translation: $(a \rightarrow n)$

  If the fruit is an apple, we know that Nadhi will eat it.

  If the fruit is not an apple, Nadhi may or may not eat it.

  The set of apples is a subset of the set of fruits that Nadhi eats.

- **Nadhi will eat a fruit only if it is an apple.**

  Translation: $(n \rightarrow a)$

  If Nadhi eats a fruit, then we know that it is an apple.

  If Nadhi does not eat a fruit, the fruit may or may not be an apple.

  The set of fruits that Nadhi eats is a subset of the set of apples.

- **Nadhi will eat a fruit if and only if it is an apple.**

  Translation: $(n \leftrightarrow a)$

  If Nadhi eats a fruit, then it is an apple.

  If Nadhi does not eat a fruit, then it is not an apple.

  The set of fruits that Nadhi eats and the set of apples coincide.

Exercise 2. *Translate the following sentence into multiple propositional formulas. Show that they are logically equivalent using a truth table.*

Soo-Jin will eat an apple or an orange but not both.

Solution: a: Soo-Jin will eat an apple. o: Soo-Jin will eat an orange.

This sentence translates into an exclusive OR. There are many ways of writing down a formula for an exclusive OR.

- $((a \lor o) \land (\neg(a \land o)))$

  a or o is true, but not both.

- $((a \lor o) \land ((\neg a) \lor (\neg o)))$

  a or o is true, and a is false or o is false.

- $((a \land (\neg o)) \lor ((\neg a) \land o))$

  a is true and o is false, or a is false and o is true.

- $(\neg(a \leftrightarrow o))$

  It is not the case that a and o have the same truth value.

- $((\neg a) \leftrightarrow o) \vDash\!\!\Dashv (a \leftrightarrow (\neg o))$

  negated a and o have the same truth value.

Exercise 3. *Translate the following sentence into at least three syntactically different propositional formulas. Show that they are logically equivalent using a truth table.*

If it is sunny tomorrow, then I will play golf, provided that I am relaxed.

Solution:

- s: It is sunny tomorrow.
- g: I will play golf.
- r: I am relaxed.

I can think of three ways of translating this sentence into a propositional formula.

- Interpretation 1: If it is sunny tomorrow, then, if I am relaxed, then I will play golf.

  Translation: $(s \to (r \to g))$.

  Sunny tomorrow is the premise for the first.

- Interpretation 2: If it is sunny tomorrow and I am relaxed, then I will play golf.

  Translation: $((s \land r) \to g)$.

  Sunny tomorrow and being relaxed together are premises for playing golf.

- Interpretation 3: If I am relaxed, then, if it is sunny tomorrow, I will play golf.

  Translation: $(r \to (s \to g))$.

  Being relaxed is the premise for the rest.

All three interpretations are logically equivalent.

Exercise 4. *Translate the following sentence into a propositional formula.*

If I ace CS 245, I will get a job at Google; otherwise I will apply for the Geek Squad.

Solution: Define the propositional variables:

- a: I ace CS 245.
- g: I will get a job at Google.
- s: I will apply for the Geek Squad.

First, let's break down this sentence into two parts by the semicolon.

The first part translates into an implication because of the key word "if". It becomes $(a \to g)$.

In the second part, "otherwise" means that "if I don't ace CS 245". After rephrasing, the second part becomes "If I don't ace CS 245, then I will apply for the Geek Squad." This is another implication $((\neg a) \to s)$.

Now the tricky part is: what connective should we use to connect the two parts together? Two natural options are $\land$ and $\lor$. The $\lor$ option seems possible because the sentence could be rephrase as "If I ace CS 245, ...; or otherwise ...."
The correct connective to use is $\land$ for the following reasons.

Let's consider the scenario in which I ace CS 245, I don't get a job at Google and I apply for the Geek Squad. In this case, is the sentence true or false? Intuitively, the sentence should be false, because the first implication is violated when I ace CS 245 but do not get a job at Google. Now let's look at the truth values of the two possible propositional formulas:

- If we use $\land$ as the connective, the resulting formula $((a \to g) \land ((\neg a) \to s))$ is false in this scenario. The truth value of the formula is the same as the truth value of the sentence in this scenario.
- If we use $\lor$ as the connective, the resulting formula $((a \to g) \land ((\neg a) \to s))$ is true in this scenario. This truth value of the formula is different from the truth value of the sentence in this scenario. Therefore, $\lor$ is not the correct connective to use because the resulting formula has a different meaning from the formula.

Exercise 5. *Translate the following sentence into two propositional formulas and explain why the two formulas are not logically equivalent.*

Sidney will carry an umbrella unless it is sunny.

Solution: Define the propositional variables.
u: Sidney will carry an umbrella.
s: It is sunny.

- Interpretation 1:

  Intuitively, many people understand “unless” as an “exclusive OR”, which means that exactly one of the two parts of the sentence is true at a time.

  With this interpretation, “unless” is equivalent to an “if and only if not”. The sentence is true under the following two scenarios:

  - It is not sunny and Sidney carries an umbrella.
  - It is sunny and Sidney does not carry an umbrella.

  Note that this interpretation does not allow Sidney to carry an umbrella when it is sunny. So the sentence is false when u and s are both true.

  In propositional logic, this is equivalent to

$$\begin{aligned} &((\neg u) \leftrightarrow s) && (1)\\ &\models\!\!\!\!\Dashv (((\neg u) \wedge s) \vee (u \wedge (\neg s))) && (2)\\ &\models\!\!\!\!\Dashv ((u \vee s) \wedge (\neg (u \wedge s))) && (3)\\ &\models\!\!\!\!\Dashv ((u \vee s) \wedge ((\neg u) \vee (\neg s))). && (4)\end{aligned}$$

  All the formulas above are equivalent. They look different but their meanings are the same.

- Interpretation 2:

  Alternatively, you may think of “unless” as meaning “if not”. Then the sentence becomes: if it is not sunny, then Sidney will carry an umbrella. In propositional logic, this becomes:

$$\begin{aligned} &((\neg s) \to u) && (5)\\ &\models\!\!\!\!\Dashv ((\neg (\neg s)) \vee u) && (6)\\ &\models\!\!\!\!\Dashv (s \vee u). && (7)\end{aligned}$$

  Under this interpretation, this sentence is true under three scenarios:

  - It is not sunny and Sidney carries an umbrella.

  - It is sunny and Sidney does not carry an umbrella.
  - It is sunny and Sidney carries an umbrella.

Notice that this interpretation allows Sidney to carry an umbrella when it is sunny. So the sentence is true when u and s are both true.

1.2 Structural Induction

1.2.1 A template for structural induction on well-formed propositional formulas

Theorem: Every well-formed propositional formula A has the property P.

Proof by structural induction:

Define $P(A)$ to be that A has the property P.

Base case: A is a propositional variable p. We need to prove that $P(p)$ holds.

Induction step:

Case 1: A is a well-formed propositional formula of the form $(\neg B)$ where B is a well-formed propositional formula.
Induction hypothesis: Assume that P(B) holds.
Prove that $P((\neg B))$ holds.

Case 2: A is a well-formed propositional formula of the form $B * C)$ where B and C are well-formed propositional formulas and $*$ is one of $\wedge$, $\vee$, $\rightarrow$, and $\leftrightarrow$.
Induction hypothesis: Assume that $P(B)$ and $P(C)$ hold.
Prove that $P((B * C))$ holds.

By the principle of structural induction, $P(A)$ holds for every well-formed propositional formula A.

QED

Theorem 1. *Every well-formed propositional formula has an equal number of opening and closing brackets.*

Solution: Each check mark indicates one point awarded to an important step of your proof.

Proof by Structural Induction. Let $P(\varphi)$ denote that the well-formed formula φ has an equal number of opening and closing brackets. ✓
Let $op(\varphi)$ and $cl(\varphi)$ denote the number of opening and closing brackets of φ respectively.

Base case: φ is a propositional symbol q. Prove that $P(q)$ holds.

q has zero opening and zero closing bracket. Thus, $P(\varphi)$ holds. ✓

Induction step:

Case 1: φ is $(\neg a)$, where a is well-formed.
Induction hypothesis: Assume that $P(a)$ holds (i.e. $op(a) = cl(a)$). ✓
We need to prove that $P((\neg a))$ holds.

$$\begin{align*}
& op((\neg a)) \tag{8}\\
& = 1 + op(a) \text{ By inspection of } (\neg a) \tag{9}\\
& = 1 + cl(a) \text{ By induction hypothesis}\checkmark \tag{10}\\
& = cl((\neg a)) \text{ By inspection of } (\neg a) \tag{11}
\end{align*}$$

Thus, $P((\neg a))$ holds.

Case 2: φ is $(a * b)$ where a and b are well-formed and $*$ is one of the four binary connectives $\wedge, \vee, \rightarrow, \leftrightarrow$.
Induction hypothesis: Assume that $P(a)$ ✓ and $P(b)$ ✓ hold (i.e. $op(a) = cl(a)$ and $op(b) = cl(b)$).
We need to prove that $P((a * b))$ holds.

$$\begin{align*}
op((a * b)) & = 1 + op(a) + op(b) \text{ By inspection of } (a * b) \tag{12}\\
& = 1 + cl(a) + cl(b) \text{ By induction hypothesis}\checkmark\checkmark \tag{13}\\
& = cl(a * b) \text{ By inspection of } (a * b) \tag{14}
\end{align*}$$

Thus, $P((a * b))$ holds.

By the principle of structural induction, $P(\varphi)$ holds for every well-formed formula φ. ✓ QED

□

Theorem 2. *Every proper prefix of a well-formed formula has more opening than closing brackets.*

Solution:

Proof by Structural Induction. Let $P(\varphi)$ denote that every proper prefix of the well-formed formula φ has more opening than closing brackets.
Let $op(\varphi)$ and $cl(\varphi)$ denote the number of opening and closing brackets of φ respectively.

Base case: φ is a propositional variable q. Prove that $P(q)$ holds.

Induction step:

Case 1: φ is $(\neg a)$, where a is well-formed.
Induction hypothesis: Assume that $P(a)$ holds.
We need to prove that $P((\neg a))$ holds.
Let m denote any proper prefix of a. There are four possible proper prefixes of $(\neg a)$: $($, $(\neg$, $(\neg m$, and $(\neg a$. We will prove the four cases separately.

$$op(() = 1 \tag{15}$$
$$cl(() = 0 \tag{16}$$
$$op(() > cl(() \tag{17}$$

$$op((\neg) = 1 \tag{18}$$
$$cl((\neg) = 0 \tag{19}$$
$$op((\neg) > cl(() \tag{20}$$

$$op((\neg m) \tag{21}$$
$$= 1 + op(m) \tag{22}$$
$$> 1 + cl(m) \text{ By the induction hypothesis on } m \tag{23}$$
$$> cl(m) \tag{24}$$
$$= cl((\neg m) \tag{25}$$

$$op((\neg a) \tag{26}$$
$$= 1 + op(a) \tag{27}$$
$$= 1 + cl(a) \text{ By Theorem 1 and } a \text{ is a well-formed formula} \tag{28}$$
$$> cl(a) \tag{29}$$
$$= cl((\neg a) \tag{30}$$

Case 2: φ is $(a * b)$ where a and b are well-formed and $*$ is a binary connective. Let m and n denote any proper prefix of a and b respectively.

Induction hypothesis: Assume that $P(a)$ and $P(b)$ hold. In other words, $P(m)$ and $P(n)$ are true.

We need to prove that $P((a * b))$ holds.

There are six possible proper prefixes of $(a * b)$: (, $(m$, $(a$, $(a*$, $(a * n$, and $(a * b$.

$$op(() = 1 \tag{31}$$
$$cl(() = 0 \tag{32}$$
$$op(() > cl(() \tag{33}$$

$$op((m) \tag{34}$$
$$= 1 + op(m) \tag{35}$$
$$> 1 + cl(m) \text{ By the induction hypothesis on } m \tag{36}$$
$$> cl(m) \tag{37}$$
$$= cl((m) \tag{38}$$

$$op((a) \tag{39}$$
$$= 1 + op(a) \tag{40}$$
$$= 1 + cl(a) \text{ By Theorem 1 and } a \text{ is a well-formed formula} \tag{41}$$
$$> cl(a) \tag{42}$$
$$= cl((a) \tag{43}$$

$$op((a*) \tag{44}$$
$$= 1 + op(a) \tag{45}$$
$$= 1 + cl(a) \text{ By Theorem 1 and } a \text{ is a well-formed formula} \tag{46}$$
$$> cl(a) \tag{47}$$
$$= cl((a*) \tag{48}$$

$$
\begin{aligned}
&op((a * n) && (49)\\
&= 1 + op(a) + op(n) && (50)\\
&= 1 + cl(a) + op(n) \text{ By Theorem 1 and } a \text{ is a well-formed formula} && (51)\\
&> 1 + cl(a) + cl(n) \text{ By the induction hypothesis on } n && (52)\\
&> cl(a) + cl(n) && (53)\\
&= cl((a * n) && (54)
\end{aligned}
$$

$$
\begin{aligned}
&op((a * b) && (55)\\
&= 1 + op(a) + op(b) && (56)\\
&= 1 + cl(a) + cl(b) \text{ By Theorem 1 and } a \text{ is a well-formed formula} && (57)\\
&> cl(a) + cl(b) && (58)\\
&= cl((a * b) && (59)
\end{aligned}
$$

By the principle of structural induction, $P(\varphi)$ holds for every well-formed formula φ. QED

□

Theorem 3. *Consider the set $I(X, C, P)$ inductively defined by the domain set $X = \mathbb{R}$, the core set $C = \{0, 2\}$, and the set of operations $P = \{f1(x, y) = x + y, f2(x, y) = x - y\}$. Every element in $I(X, C, P)$ is an even integer.*

Solution:

Proof by Structural Induction. Base case: We need to prove that every element of the core set C is an even integer. 0 is even because $0 = 2 * 0$. 2 is even because $2 = 2 * 1$.

Induction step:

Case 1: Let $x, y \in I(X, C, P)$.
Induction hypotheses: Assume that x and y are even integers.
We will prove that $f1(x, y)$ is an even integer.
x and y are even integers. Thus, by the induction hypotheses, $x = 2m$ and $y = 2n$ where m and n are integers. Then, $f1(x, y) = x + y = 2m + 2n = 2(m + n)$. Since $(m + n)$ is an integer, $f1(x, y)$ is an even integer.

Case 2: Let $x, y \in I(X, C, P)$.
Induction hypotheses: Assume that x and y are even integers.
We will prove that $f2(x, y)$ is an even integer.
x and y are even integers. Thus, by the induction hypotheses, $x = 2m$ and $y = 2n$ where m and n are integers. Then, $f2(x, y) = x - y = 2m - 2n = 2(m - n)$. Since $(m - n)$ is an integer, $f2(x, y)$ is an even integer.

By the principle of structural induction, every element of $I(X, C, P)$ is an even integer.

□

1.3 The Semantics of an Implication

Exercise 6. *Do you really understand an implication? We will find out.*

- *Think of an implication as a promise that someone made to you. In what case can you prove that the promise has been broken (i.e. the implication is false)?*
- *When the premise is true, what is the relationship between the truth value of the conclusion and the truth value of the implication?*
- *When the premise is false, the implication is vacuously true. Could you come up with an intuitive explanation for this?*
- *If the conclusion is true, is the implication true or false?*
- *The implication* $(a \rightarrow b)$ *is logically equivalent to* $((\neg a) \vee b)$*. Does this equivalent formula make sense to you? Explain.*

1.4 Tautology, Contradiction, and Satisfiable but Not a Tautology

Exercise 7. *Determine whether each of the following formulas is a tautology, satisfiable but not a tautology, or a contradiction.*

- p

  Solution: Answer: Satisfiable but not a tautology.

  Reason: True when p is true and false when p is false.

- $((r \wedge s) \rightarrow r)$

  Solution: Answer: Tautology.

  Reason: When r is true, the conclusion of the implication is true, so the implication is true. When r is false, the premise of the implication is false, so the implication is vacuously true.

- $((\neg(p \leftrightarrow q)) \leftrightarrow (q \vee p))$

  Solution: Answer: Satisfiable but not a tautology

  Reason: It's tempting to say "these two formulas don't mean the same thing so the biconditional is false". However, go back to truth values. When p is true and q is false, both sides of the biconditional are true and the biconditional itself is true. When p and q are both true, the left side is false but the right is true, and so the biconditional is false.

- $((((p \vee q) \wedge (p \vee (\neg q))) \wedge ((\neg p) \vee q)) \wedge ((\neg p) \vee (\neg q)))$

  Solution: Answer: Contradiction

  Reason: The first half can be simplfiied to $(p \vee (q \wedge (\neg q)))$, which is $(p \vee F)$ or p. The second half can be simplfiied to $(\neg p)$. Thus, the entire formula is $(p \wedge (\neg p))$, which is a contradiction.

1.5 Logical Equivalence

Exercise 8. *"If it is sunny, I will play golf, provided that I am relaxed."*
s: it is sunny. g: I will play golf. r: I am relaxed.

There are three possible translations:

1. $(r \rightarrow (s \rightarrow g))$
2. $((s \wedge r) \rightarrow g)$
3. $(s \rightarrow (r \rightarrow g))$

Prove that all three translations are logically equivalent.

Solution: Part 1: $(r \rightarrow (s \rightarrow g)) \vDash\dashv ((s \wedge r) \rightarrow g)$.

Proof.

$$(r \rightarrow (s \rightarrow g)) \tag{60}$$
$$\vDash\dashv (r \rightarrow ((\neg s) \vee g)) \qquad \text{Implication} \tag{61}$$
$$\vDash\dashv ((\neg r) \vee ((\neg s) \vee g)) \qquad \text{Implication} \tag{62}$$
$$\vDash\dashv (((\neg r) \vee (\neg s)) \vee g) \qquad \text{Associativity} \tag{63}$$
$$\vDash\dashv (((\neg (r \wedge s)) \vee g) \qquad \text{De Morgan} \tag{64}$$
$$\vDash\dashv ((r \wedge s) \rightarrow g) \qquad \text{Implication} \tag{65}$$
$$\vDash\dashv ((s \wedge r) \rightarrow g) \qquad \text{Commutativity} \tag{66}$$

□

Part 2: $(r \rightarrow (s \rightarrow g)) \vDash\dashv (s \rightarrow (r \rightarrow g))$.

Proof.

$$(r \rightarrow (s \rightarrow g)) \tag{67}$$
$$\vDash\dashv (r \rightarrow ((\neg s) \vee g)) \qquad \text{Implication} \tag{68}$$
$$\vDash\dashv ((\neg r) \vee ((\neg s) \vee g)) \qquad \text{Implication} \tag{69}$$
$$\vDash\dashv (((\neg r) \vee (\neg s)) \vee g) \qquad \text{Associativity} \tag{70}$$
$$\vDash\dashv (((\neg s) \vee (\neg r)) \vee g) \qquad \text{Commutativity} \tag{71}$$
$$\vDash\dashv ((\neg s) \vee ((\neg r) \vee g)) \qquad \text{Associativity} \tag{72}$$
$$\vDash\dashv ((\neg s) \vee (r \rightarrow g)) \qquad \text{Implication} \tag{73}$$
$$\vDash\dashv (s \rightarrow (r \rightarrow g)) \qquad \text{Implication} \tag{74}$$

□

Exercise 9. *"If it snows then I will not go to class but I will do my assignment."*
s: it snows. c: I will go to class. a: I will do my assignment.

There are two possible translations:

1. $((s \to (\neg c)) \wedge a)$
2. $(s \to ((\neg c) \wedge a))$

Prove that the two translations are NOT logically equivalent.

Solution:

Proof. We need to find a valuation t under which the two formulas have different values.
Consider the truth valuation t where $t(s) = 0$, $t(c) = 1$, and $t(a) = 0$.
The two formulas have different values under t, as shown below.

- $((s \to (\neg c)) \wedge a)^t = 0$
- $(s \to ((\neg c) \wedge a))^t = 1$

□

1.6 Analyzing Conditional Code

Consider the following code fragment:

```
if (input > 0 || !output) {
  if (!(output && queuelength < 100)) {
    P1
  } else if (output && !(queuelength < 100)) {
    P2
  } else {
        P3
  }
} else {
  P4
}
```

Define the propositional variables:

- i: input > 0
- u: output
- q: queuelength < 100

The code fragment becomes the following. We'll call this code fragment #1.

```
if ( i || !u ) {
  if ( !(u && q) ) {
    P1
  } else if ( u && !q ) {
    P2
  } else { P3 }
} else { P4 }
```

Code fragment #2:

```
if (( i && u) && q) {
  P3
} else if (!i && u) {
  P4
} else {
  P1
}
```

Prove that these two pieces of code fragments are equivalent:
Solution:

Prove that the condition leading to P_2 is logically equivalent to 0.
The condition leading to P_2:

$$(((i \vee (\neg u)) \wedge (\neg(\neg(u \wedge q)))) \wedge (u \wedge (\neg q))) \tag{75}$$

$$\mathrel{\Dashv\!\vDash} (((i \vee (\neg u)) \wedge (u \wedge q)) \wedge (u \wedge (\neg q))) \qquad \text{Double Negation} \tag{76}$$

$$\mathrel{\Dashv\!\vDash} ((i \vee (\neg u)) \wedge ((u \wedge u) \wedge (q \wedge (\neg q)))) \qquad \text{Associativity, Commutativity} \tag{77}$$

$$\mathrel{\Dashv\!\vDash} ((i \vee (\neg u)) \wedge (u \wedge (q \wedge (\neg q)))) \qquad \text{Idempotence} \tag{78}$$

$$\mathrel{\Dashv\!\vDash} ((i \vee (\neg u)) \wedge (u \wedge 0)) \qquad \text{Contradiction} \tag{79}$$

$$\mathrel{\Dashv\!\vDash} ((i \vee (\neg u)) \wedge 0) \qquad \text{Simplification 1} \tag{80}$$

$$\mathrel{\Dashv\!\vDash} 0 \qquad \text{Simplification 1} \tag{81}$$

$$\tag{82}$$

Prove that the condition leading to P_3 is true if and only if all three variables are true.
The condition leading to P_3:

$$(((i \vee (\neg u)) \wedge (u \wedge q)) \wedge (\neg(u \wedge (\neg q)))) \tag{83}$$

$$\mathrel{\Dashv\!\vDash} (((i \vee (\neg u)) \wedge (u \wedge q)) \wedge ((\neg u) \vee (\neg(\neg q)))) \qquad \text{De Morgan} \tag{84}$$

$$\mathrel{\Dashv\!\vDash} (((i \vee (\neg u)) \wedge (u \wedge q)) \wedge ((\neg u) \vee q)) \qquad \text{Double Negation} \tag{85}$$

$$\mathrel{\Dashv\!\vDash} ((i \vee (\neg u)) \wedge (u \wedge (q \wedge ((\neg u) \vee q)))) \qquad \text{Associativity} \tag{86}$$

$$\mathrel{\Dashv\!\vDash} ((i \vee (\neg u)) \wedge (u \wedge q)) \qquad \text{Simplification 2} \tag{87}$$

$$\mathrel{\Dashv\!\vDash} ((i \vee (\neg u)) \wedge u) \wedge q) \qquad \text{Associativity} \tag{88}$$

$$\mathrel{\Dashv\!\vDash} (((i \wedge u) \vee ((\neg u) \wedge u)) \wedge q) \qquad \text{Distributivity} \tag{89}$$

$$\mathrel{\Dashv\!\vDash} (((i \wedge u) \vee 0) \wedge q) \qquad \text{Contradiction} \tag{90}$$

$$\mathrel{\Dashv\!\vDash} ((i \wedge u) \wedge q) \qquad \text{Simplification 1} \tag{91}$$

Prove that the condition leading to P_4 is true if and only if i is false and u is true.
The condition leading to P_4:

$$(\neg(i \vee (\neg u))) \tag{92}$$

$$((\neg i) \wedge (\neg(\neg u))) \qquad \text{De Morgan} \tag{93}$$

$$\mathrel{\Dashv\!\vDash} ((\neg i) \wedge u) \qquad \text{Double Negation} \tag{94}$$

The condition leading to P_1:

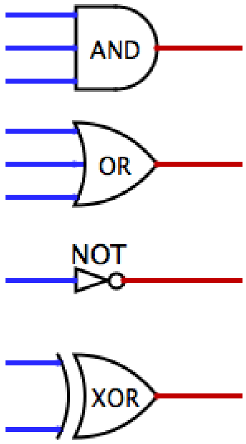
$$((i \vee (\neg u)) \wedge (\neg(u \wedge q))) \tag{95}$$

$$\mathrel{\Dashv\!\vDash} ((i \vee (\neg u)) \wedge ((\neg u) \vee (\neg q))) \qquad \text{De Morgan} \tag{96}$$

$$\mathrel{\Dashv\!\vDash} ((\neg u) \vee (i \wedge (\neg q))) \qquad \text{Distributivity} \tag{97}$$

1.7 Circuit Design

Basic gates:



Problem: Your instructors, Alice, Carmen, and Collin, are choosing questions to be put on the midterm. For each problem, each instructor votes either yes or not. A question is chosen if it receives two or more yes votes. Design a circuit, which outputs yes whenever a question is chosen.

1. Draw the truth table based on the problem description.

x	y	z	output
1	1	1	1
1	1	0	1
1	0	1	1
1	0	0	0
0	1	1	1
0	1	0	0
0	0	1	0
0	0	0	0

2. Convert the truth table into a propositional formula.

3. Then, convert the formula to a circuit.

Solution:

Solution 1:

1. Convert the truth table into a propositional formula.

   Convert each row of the truth table to a conjunction.

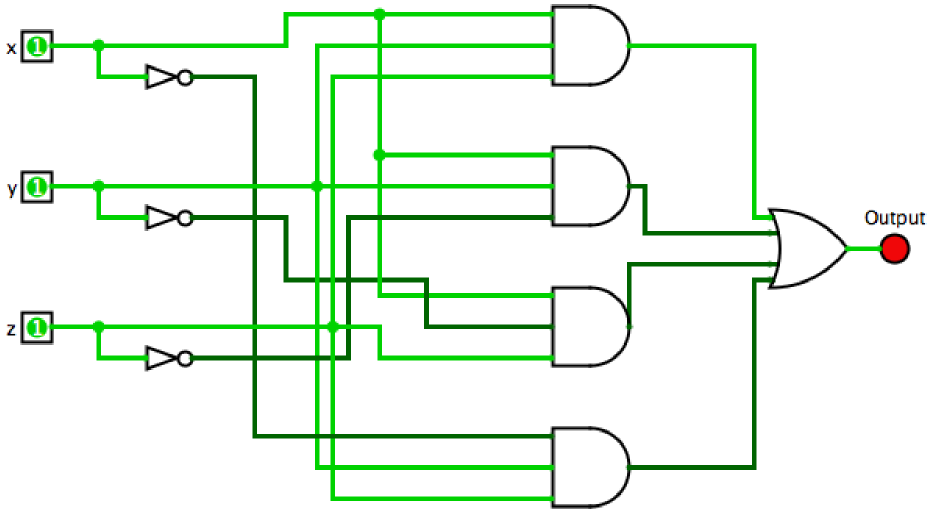
   If a variable is true in that row, write it down. Otherwise, if the variable is false, write down its negation. Then connect all variables or their negations together using AND.

   - $((x \wedge y) \wedge z)$
   - $((x \wedge y) \wedge (\neg z))$
   - $((x \wedge (\neg y)) \wedge z)$
   - $(((\neg x) \wedge y) \wedge z)$

   Connect all formulas into a disjunction.

   $(((((x \wedge y) \wedge z) \vee ((x \wedge y) \wedge (\neg z))) \vee ((x \wedge (\neg y)) \wedge z)) \vee (((\neg x) \wedge y) \wedge z))$

2. Draw the circuit.



   Making a circuit clear and readable can be challenging. Here are some advice on drawing circuits:

   - Determine where to put the inputs and the outputs first.
   - Determine where to put the major gates (the OR at the end, and one AND for each scenario).
   - Try to draw wires horizontally or vertically, not at an angle.
   - Indicate clearly whether two crossing wires are connected or not.

Solution 2:

1. Convert the truth table into a propositional formula.

   Converts rows 1-3 to a propositional formula.

   $(x \wedge (y \vee z))$

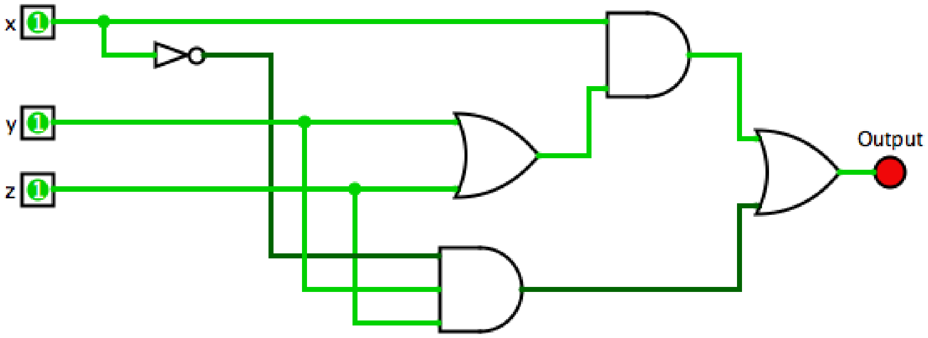
   Convert row 5 to a propositional formula.

   $(((\neg x) \wedge y) \wedge z)$

   Connect all formulas into a disjunction.

   $((x \wedge (y \vee z)) \vee (((\neg x) \wedge y) \wedge z))$

2. Draw the circuit.



Solution 3:

1. Convert the truth table into a propositional formula.

   Convert rows 1 and 5 into a propositional formula.

   $(y \wedge z)$

   Convert rows 2 and 3 into a propositional formula.

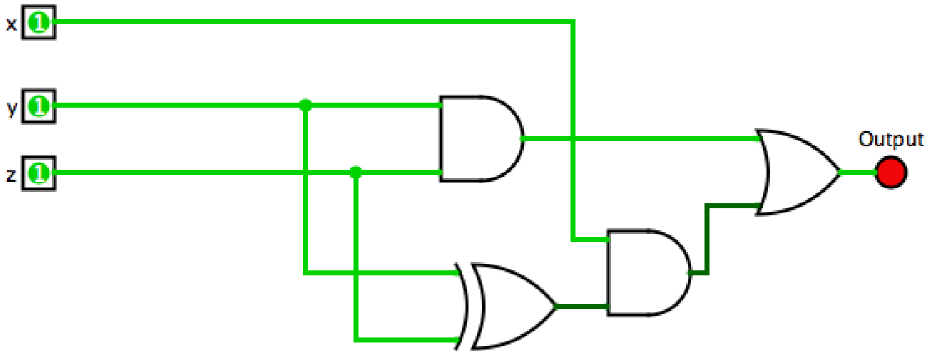
   $(x \wedge (y \oplus z))$

   For convenience, we will use the symbol $\oplus$ to represent an exclusive OR. However, you are only allowed to use this symbol in circuit design problems. You are not allowed to use this symbol for other problems because it is not a basic connective based on the definition of well-formed formulas.

   Connect all formulas into a disjunction.

   $((y \wedge z) \vee (x \wedge (y \oplus z)))$

2. Draw the circuit.



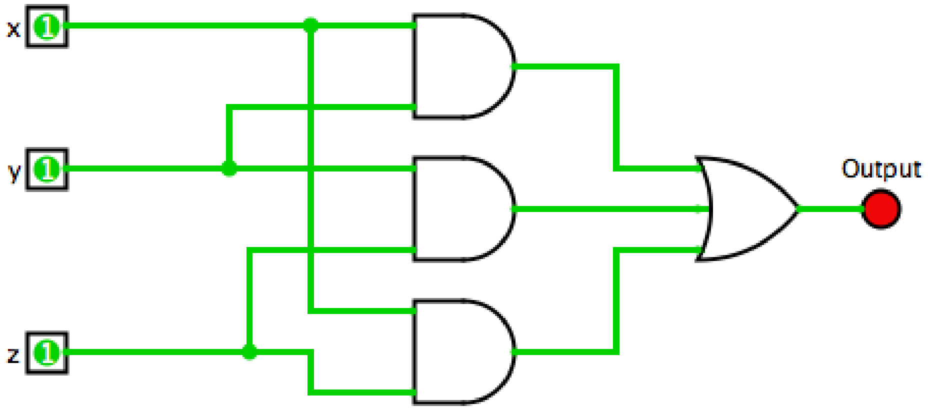
Solution 4 (contributed by Triman Kandola)

1. Convert the truth table into a propositional formula.

   $(((x \wedge y) \vee (x \wedge z)) \vee (y \wedge z))$

   This formula intuitively makes sense. If two people are already voting yes, then I don't care about what the third vote is.

2. Draw the circuit.



1.8 Tautological Consequence

Exercise 10. *Let* $\Sigma = \{(p \to q), (q \to r)\}$*. Is* Σ *satisfiable? Why or why not?*

Solution: Σ is satisfied by the truth valuation t where $t(p) = 1$, $t(q) = 1$ and $t(r) = 1$. Note that $(p \to q)^t = 1$ and $(q \to r)^t = 1$. Thus, Σ is satisfiable.

Exercise 11. *Let* $\Sigma = \emptyset$*. Is* Σ *satisfiable? Why or why not?*

Solution: Σ is satisfiable. In fact, any truth valuation satisfies Σ.
A truth valuation t satisfies Σ if and only if, for any formula A, if A is in Σ, then $A^t = 1$. Since $\Sigma = \emptyset$, no formula is in Σ. The premise of the implication is false for any A, so the implication is true for every A. Therefore, any truth valuation satisfies $\Sigma = \emptyset$.

Exercise 12. *Let* $\Sigma = \{p, (\neg p)\}$*. Is* Σ *satisfiable? Why or why not?*

Solution: Σ is not satisfiable. To show this, we need to show that, under every truth valuation, at least one formula in Σ is false.

Consider an arbitrary truth valuation t. Under t, p is either true or false.

- If $p^t = 1$, then $(\neg p)^t = 0$. t does not satisfy Σ.
- If $p^t = 0$, then t does not satisfy Σ.

In both cases, t does not satisfy Σ. Therefore, no truth valuation can satisfy Σ. Σ is not satisfiable.

Exercise 13. *Prove that* $\{(\neg(p \wedge q)), (p \rightarrow q)\} \vDash (\neg p)$.

Solution:

Proof. Consider a truth valuation t such that $(\neg(p \wedge q))^t = 1$ and $(p \rightarrow q)^t = 1$.

Since $(p \rightarrow q)^t = 1$, it is not the case that $p^t = 1$ and $q^t = 0$.
Since $(\neg(p \wedge q))^t = 1$, it is not the case that $p^t = 1$ and $q^t = 1$.

Thus, the two premises are true under two scenarios:

- $p^t = 0$ and $q^t = 1$: In this case, $(\neg p)^t = 1$.
- $p^t = 0$ and $q^t = 0$: In this case, $(\neg p)^t = 1$.

In both scenarios, the conclusion is true. Thus, the tautological consequence holds. □

Exercise 14. *Prove that* $\{(\neg(p \wedge q)), (p \rightarrow q)\} \not\vDash (p \leftrightarrow q)$.

Solution:

Proof. Consider the truth valuation t where $p^t = 0$ and $q^t = 1$.

By definitions of the connectives, $(\neg(p \wedge q))^t = 1$, $(p \rightarrow q)^t = 1$ and $(p \leftrightarrow q)^t = 0$. Thus, the tautological consequence does not hold. □

Exercise 15. *Prove that* $\emptyset \vDash ((p \wedge q) \rightarrow p))$.

Solution:

Proof. Since there is no premise, we need to prove that the conclusion $((p \wedge q) \rightarrow p))$ is a tautology.
Consider any truth valuation t. Under t, p must be either true or false.

- $p^t = 1$: The conclusion of the implication $((p \wedge q) \rightarrow p))$is true. Therefore, the implication is true.
- $p^t = 0$: The premise of the implication $((p \wedge q) \rightarrow p))$ is true. Therefore, the implication is true.

Thus, the conclusion is true under any truth valuation and is a tautology. The tautological consequence holds. □

Exercise 16. *Prove that* $\{r, (p \to (r \to q))\} \vDash (p \to (q \wedge r))$.

Solution:

Proof. Consider a truth valuation t where $r^t = 1$ and $(p \to (r \to q))^t = 1$. We need to show that $(p \to (q \wedge r))^t = 1$.

Consider two cases: $p^t = 0$ and $p^t = 1$.

If $p^t = 0$, then $(p \to (q \wedge r))^t = 1$.

Otherwise, suppose that $p^t = 1$. We need to show that $(q \wedge r)^t = 1$.
By the definition of implication, $(r \to q)^t = 1$ since $(p \to (r \to q))^t = 1$. Since $r^t = 1$ and $(r \to q)^t = 1$, then $q^t = 1$ by the definition of implication. By the definition of $\wedge$, $(q \wedge r)^t = 1$ since q and r are both true under t. Therefore, $(p \to (q \wedge r))^t = 1$.

In both cases, the conclusion is true under t. The tautological consequence holds. □

Exercise 17. *Prove that* $\{(\neg p), (q \to p)\} \not\vDash ((\neg p) \wedge q)$.

Solution:

Remark 1. *We need to come up with a truth valuation under which both premises are true and the conclusion is false.*
$(\neg p)$ has to be true. So p has to be false under this truth valuation.
$(q \to p)$ has to be true and p is false. Thus, q must be false under this truth valuation.
Therefore, this truth valuation must make p false and q false.

Proof. Consider the truth valuation t where $p^t = 0$ and $q^t - 0$.

Under this truth valuation, $(\neg p)^t = 1$ and $(q \to p)^t = 1$. Both premises are true.

Under this truth valuation, $((\neg p) \wedge q)^t = 0$. The conclusion is false.

Therefore, the tautological consequence does not hold. □

Exercise 18. *Prove that* $\{p, (\neg p)\} \vDash r$.

Solution:

Proof. Consider any truth valuation t under which both premises are true. If such a truth valuation exists, we have to show that r must be true under this truth valuation.

However, such a truth valuation does not exist. There are two possible cases. p is true or p is false. If p is false, then this truth valuation does not satisfy the first premise. If p is true under this truth valuation, then $(\neg p)$ must be false. This truth valuation does not satisfy the second premise.

Since no truth valuation satisfies both premises, the tautological consequence holds. □

1.9 Formal Deduction

1.9.1 Rules of Formal Deduction

membership ($\in$)

$$\begin{aligned} &\text{if } A \in \Sigma, \\ &\text{then } \Sigma \vdash A. \end{aligned}$$

Addition of premises ($+$)

$$\begin{aligned} &\text{if } \Sigma \vdash A, \\ &\text{then } \Sigma, \Sigma' \vdash A. \end{aligned}$$

Special case: Reflexivity (Ref)

$$A \vdash A.$$

And introduction ($\wedge +$)

$$\begin{aligned} \text{if } &\Sigma \vdash A, \\ &\Sigma \vdash B, \\ \text{then } &\Sigma \vdash A \wedge B. \end{aligned}$$

And elimination ($\wedge -$)

$$\begin{aligned} \text{if } &\Sigma \vdash A \wedge B, \\ \text{then } &\Sigma \vdash A. \\ \text{if } &\Sigma \vdash A \wedge B, \\ \text{then } &\Sigma \vdash B. \end{aligned}$$

Or introduction ($\vee +$)

$$\begin{aligned} \text{if } &\Sigma \vdash A, \\ \text{then } &\Sigma \vdash A \vee B. \\ \text{if } &\Sigma \vdash B, \\ \text{then } &\Sigma \vdash A \vee B. \end{aligned}$$

Or elimination ($\vee -$)

$$\begin{aligned} \text{if } &\Sigma, A \vdash C, \\ &\Sigma, B \vdash C, \\ \text{then } &\Sigma, A \vee B \vdash C. \end{aligned}$$

Negation introduction ($\neg +$)

$$\begin{aligned} \text{if } &\Sigma, A \vdash B, \\ &\Sigma, A \vdash \neg B, \\ \text{then } &\Sigma \vdash \neg A. \end{aligned}$$

Negation elimination ($\neg -$)

$$\begin{aligned} \text{if } &\Sigma, \neg A \vdash B, \\ &\Sigma, \neg A \vdash \neg B, \\ \text{then } &\Sigma \vdash A. \end{aligned}$$

Implication introduction ($\to +$)

$$\begin{aligned} \text{if } &\Sigma, A \vdash B, \\ \text{then } &\Sigma \vdash A \to B. \end{aligned}$$

Implication elimination ($\to -$)

$$\begin{aligned} \text{if } &\Sigma \vdash A, \\ &\Sigma \vdash A \to B, \\ \text{then } &\Sigma \vdash B. \end{aligned}$$

Equivalence introduction ($\leftrightarrow +$)

$$\begin{aligned} \text{if } & \Sigma, A \vdash B, \\ & \Sigma, B \vdash A, \\ \text{then } & \Sigma \vdash A \leftrightarrow B. \end{aligned}$$

Equivalence elimination ($\leftrightarrow -$)

$$\begin{aligned} \text{if } & \Sigma \vdash A, \\ & \Sigma \vdash A \leftrightarrow B, \\ \text{then } & \Sigma \vdash B. \\ \text{if } & \Sigma \vdash B, \\ & \Sigma \vdash A \leftrightarrow B, \\ \text{then } & \Sigma \vdash A. \end{aligned}$$

Comments:

- For each connective, the rules come in pairs. The introduction rule produces a conclusion with the connective in it. The elimination rule produces a conclusion without the connective.
- A and B can be any propositional formula. In particular, A and B can be the same.
- Σ and Σ' are sets of propositional formulas.
- Σ, A means $\Sigma \cup \{A\}$. Σ, Σ' means $\Sigma \cup \Sigma'$.

1.9.2 Format of a Formal Deduction Proof

- Every line contains: a line number, a set of premises, the $\vdash$ symbol, a conclusion, and a justification containing a formal deduction rule and possibly line numbers.
- The last line of a proof is the same as the original statement to be proved.
- Every line of the proof can be justified in two ways: (1) using the premises on the left of $\vdash$ using the membership $\in$ rule. (2) using one or more conclusions on previous lines by using any other formal deduction rule.
- You have to bring a premise to the right of $\vdash$ before you can use it in a subsequent line.

1.9.3 Strategies for writing a formal deduction proof

What is the thought process for producing a formal deduction proof?

- I've found that it is most effective to generate a proof backwards starting from the last line of the proof.
- Write down the statement to be proved as the last line of the proof. Work backwards from here.
- Look at the conclusion carefully. What is the structure of the conclusion (what is the last connective applied in the formula? Can you apply an introduction rule to produce the conclusion?
- Look at each premise carefully. What is the structure of the premise (what is the last connective applied in the formula)? Can you apply an elimination rule to simplify it and to produce a new formula?
- Working backwards from the conclusion is often more effective than working forward from the premises. It keeps your eyes on the prize.
- If no rule is applicable, consider using $\neg+$ or $\neg-$. The negation rules are "universal". They can be applied in any situation but beware that they are not always helpful.
- **When do we stop?**

  We can stop this process when we are able to justify every line of our proof. Usually, we end this process by justifying the last line produced using the membership $\in$ rule.

Why are we allowed to add premises to the left of $\vdash$?

- Think about adding a premise on the left of $\vdash$ as making an assumption in our proof. For example, when you are proving a property of a natural number, you may write your proof as follows: case 1, n is even ... case 2, n is odd ... Here n is even and n is odd are additional assumptions made in your proof. Adding a premise on the left is the same as making such an additional assumption.

- We are only able to add a premise on the left of $\vdash$ if a formal deduction rule allows us to do so.
- Eventually, we will need to remove the additional premises from the left of $\vdash$ in order to produce the conclusion required in the original statement to be proved.

1.9.4 And elimination and introduction

Exercise 19. *Show that* $(p \wedge q), (r \wedge s) \vdash (q \wedge s)$.

Solution:

$$\begin{array}{lll}
(1) & p \wedge q, r \wedge s \vdash p \wedge q & \text{by } (\in) \\
(2) & p \wedge q, r \wedge s \vdash q & \text{by } \wedge -, 1 \\
(3) & p \wedge q, r \wedge s \vdash r \wedge s & \text{by } (\in) \\
(4) & p \wedge q, r \wedge s \vdash s & \text{by } \wedge -, 3 \\
(5) & p \wedge q, r \wedge s \vdash q \wedge s & \text{by } \wedge +, 2, 4
\end{array}$$

Exercise 20. *Show that* $((p \wedge q) \wedge r) \vdash (p \wedge (q \wedge r))$.

Solution:

$$\begin{array}{lll}
(1) & (p \wedge q) \wedge r \vdash (p \wedge q) \wedge r & \text{by } (\in) \\
(2) & (p \wedge q) \wedge r \vdash (p \wedge q) & \text{by } \wedge -, 1 \\
(3) & (p \wedge q) \wedge r \vdash r & \text{by } \wedge -, 1 \\
(4) & (p \wedge q) \wedge r \vdash p & \text{by } \wedge -, 2 \\
(5) & (p \wedge q) \wedge r \vdash q & \text{by } \wedge -, 2 \\
(6) & (p \wedge q) \wedge r \vdash q \wedge r & \text{by } \wedge +, 3, 5 \\
(7) & (p \wedge q) \wedge r \vdash p \wedge (q \wedge r) & \text{by } \wedge +, 4, 6
\end{array}$$

1.9.5 Implication introduction and elimination

Exercise 21. *Show that* $(p \to q), (q \to r) \vdash (p \to r)$.

Solution:

(1)	$p \to q, q \to r, p \vdash p \to q$	by $(\in)$
(2)	$p \to q, q \to r, p \vdash p$	by $(\in)$
(3)	$p \to q, q \to r, p \vdash q$	by $(\to -, 1, 2)$
(4)	$p \to q, q \to r, p \vdash q \to r$	by $(\in)$
(5)	$p \to q, q \to r, p \vdash r$	by $(\to -, 3, 4)$
(6)	$p \to q, q \to r \vdash p \to r$	by $(\to +, 5)$

Exercise 22. *Show that* $(p \to (q \to r)), (p \to q) \vdash (p \to r)$.

Solution:

(1)	$p \to (q \to r), p \to q, p \vdash p$	by $(\in)$
(2)	$p \to (q \to r), p \to q, p \vdash p \to q$	by $(\in)$
(3)	$p \to (q \to r), p \to q, p \vdash q$	by $(\to -, 1, 2)$
(4)	$p \to (q \to r), p \to q, p \vdash p \to (q \to r)$	by $(\in)$
(5)	$p \to (q \to r), p \to q, p \vdash q \to r$	by $(\to -, 1, 4)$
(6)	$p \to (q \to r), p \to q, p \vdash r$	by $(\to -, 3, 5)$
(7)	$p \to (q \to r), p \to q \vdash p \to r$	by $(\to +, 6)$

Exercise 23. *Show that* $(p \to (q \to r)) \vdash ((p \wedge q) \to r)$.

Solution:

$$\begin{array}{lcl}
(1) & p \to (q \to r), p \wedge q \vdash p \wedge q & \text{by } (\in) \\
(2) & p \to (q \to r), p \wedge q \vdash p & \text{by } (\wedge-, 1) \\
(3) & p \to (q \to r), p \wedge q \vdash p \to (q \to r) & \text{by } (\in) \\
(4) & p \to (q \to r), p \wedge q \vdash q & \text{by } (\wedge-, 1) \\
(5) & p \to (q \to r), p \wedge q \vdash q \to r & \text{by } (\to -, 2, 3) \\
(6) & p \to (q \to r), p \wedge q \vdash r & \text{by } (\to -, 4, 5) \\
(7) & p \to (q \to r) \vdash (p \wedge q) \to r & \text{by } (\to +, 6)
\end{array}$$

Exercise 24. *Show that* $((p \wedge q) \to r) \vdash (p \to (q \to r))$.

Solution:

$$\begin{array}{lcl}
(1) & (p \wedge q) \to r, p, q \vdash (p \wedge q) \to r & \text{by } (\in) \\
(2) & (p \wedge q) \to r, p, q \vdash p & \text{by } (\in) \\
(3) & (p \wedge q) \to r, p, q \vdash q & \text{by } (\in) \\
(4) & (p \wedge q) \to r, p, q \vdash p \wedge q & \text{by } (\wedge+, 2, 3) \\
(5) & (p \wedge q) \to r, p, q \vdash r & \text{by } (\to -, 1, 4) \\
(6) & (p \wedge q) \to r, p \vdash q \to r & \text{by } (\to +, 5) \\
(7) & (p \wedge q) \to r \vdash p \to (q \to r) & \text{by } (\to +, 6)
\end{array}$$

1.9.6 Or introduction and elimination

Exercise 25. *Show that* $(p \vee q) \vdash ((p \to q) \vee (q \to p))$.

Solution:

(1)	$p, q \vdash p$	by $(\in)$
(2)	$p \vdash q \to p$	by $(\to +, 1)$
(3)	$q, p \vdash q$	by $(\in)$
(4)	$q \vdash p \to q$	by $(\to +, 1)$
(5)	$p \vdash (p \to q) \vee (q \to p)$	by $(\vee +, 2)$
(6)	$q \vdash (p \to q) \vee (q \to p)$	by $(\vee +, 4)$
(7)	$(p \vee q) \vdash (p \to q) \vee (q \to p)$	by $(\vee -, 5, 6)$

Exercise 26. *Show that* $(p \to q) \vdash ((r \vee p) \to (r \vee q))$.

Solution:

(1)	$p \to q, p \vdash p$	by $(\in)$
(2)	$p \to q, p \vdash p \to q$	by $(\in)$
(3)	$p \to q, p \vdash q$	by $(\to -, 1, 2)$
(4)	$p \to q, r \vdash r$	by $(\in)$
(5)	$p \to q, r \vdash (r \vee q)$	by $(\vee +, 4)$
(6)	$p \to q, p \vdash (r \vee q)$	by $(\vee +, 3)$
(7)	$p \to q, r \vee p \vdash (r \vee q)$	by $(\vee -, 5, 6)$
(8)	$p \to q \vdash (r \vee p) \to (r \vee q)$	by $(\to +, 7)$

Exercise 27. *Show that* $((p \wedge q) \vee (p \wedge r)) \vdash (p \wedge (q \vee r))$.

Solution:

(1)	$p \wedge q \vdash p \wedge q$	by $(\in)$
(2)	$p \wedge q \vdash q$	by $(\wedge-, 1)$
(3)	$p \wedge q \vdash q \vee r$	by $(\vee+, 2)$
(4)	$p \wedge q \vdash p$	by $(\wedge-, 1)$
(5)	$p \wedge r \vdash p \wedge r$	by $(\in)$
(6)	$p \wedge r \vdash r$	by $(\wedge-, 5)$
(7)	$p \wedge r \vdash q \vee r$	by $(\vee+, 6)$
(8)	$p \wedge r \vdash p$	by $(\wedge-, 5)$
(9)	$p \wedge q \vdash p \wedge (q \vee r)$	by $(\wedge+, 3, 4)$
(10)	$p \wedge r \vdash p \wedge (q \vee r)$	by $(\wedge+, 7, 8)$
(11)	$(p \wedge q) \vee (p \wedge r) \vdash p \wedge (q \vee r)$	by $(\vee-, 9, 10)$

Exercise 28. *Show that* $(p \wedge (q \vee r)) \vdash ((p \wedge q) \vee (p \wedge r))$.

Solution:

(1)	$(p \wedge (q \vee r)) \vdash (p \wedge (q \vee r))$	by (Ref)
(2)	$(p \wedge (q \vee r)) \vdash p$	by $(\wedge-, 1)$
(3)	$(p \wedge (q \vee r)) \vdash q \vee r$	by $(\wedge-, 1)$
(4)	$(p \wedge (q \vee r)), q \vdash q$	by $(\in)$
(5)	$(p \wedge (q \vee r)), q \vdash p$	by $(+, 2)$
(6)	$(p \wedge (q \vee r)), q \vdash p \wedge q$	by $(\wedge+, 4, 5)$
(7)	$(p \wedge (q \vee r)), q \vdash (p \wedge q) \vee (p \wedge r)$	by $(\vee+, 6)$
(8)	$(p \wedge (q \vee r)), r \vdash r$	by $(\in)$
(9)	$(p \wedge (q \vee r)), r \vdash p$	by $(+, 2)$
(10)	$(p \wedge (q \vee r)), r \vdash p \wedge r$	by $(\wedge+, 8, 9)$
(11)	$(p \wedge (q \vee r)), r \vdash (p \wedge q) \vee (p \wedge r)$	by $(\vee+, 10)$
(12)	$(p \wedge (q \vee r)), q \vee r \vdash (p \wedge q) \vee (p \wedge r)$	by $(\vee-, 7, 11)$
(13)	$(p \wedge (q \vee r)) \vdash (q \vee r) \to (p \wedge q) \vee (p \wedge r)$	by $(\to +, 12)$
(14)	$(p \wedge (q \vee r)) \vdash (p \wedge q) \vee (p \wedge r)$	by $(\to -, 3, 13)$

1.9.7 Negation introduction and elimination

Exercise 29. *Show that* $p \to (\neg p) \vdash (\neg p)$.

Solution:

(1)	$p \to (\neg p), p \vdash p$	by $(\in)$
(2)	$p \to (\neg p), p \vdash p \to (\neg p)$	by $(\in)$
(3)	$p \to (\neg p), p \vdash (\neg p)$	by $(\to -, 1, 2)$
(4)	$p \to (\neg p) \vdash (\neg p)$	by $(\neg +, 1, 3)$

Exercise 30. *Show that* $(p \to (q \to r)), p, (\neg r) \vdash (\neg q)$.

Solution:

(1)	$p \to (q \to r), p, (\neg r), q \vdash p$	by $(\in)$
(2)	$p \to (q \to r), p, (\neg r), q \vdash p \to (q \to r)$	by $(\in)$
(3)	$p \to (q \to r), p, (\neg r), q \vdash q \to r$	by $(\to -, 1, 2)$
(4)	$p \to (q \to r), p, (\neg r), q \vdash q$	by $(\in)$
(5)	$p \to (q \to r), p, (\neg r), q \vdash r$	by $(\to -, 3, 4)$
(6)	$p \to (q \to r), p, (\neg r), q \vdash (\neg r)$	by $(\in)$
(7)	$p \to (q \to r), p, (\neg r) \vdash (\neg q)$	by $(\neg +, 5, 6)$

Exercise 31. *Show that* $(p \to q), (\neg q) \vdash (\neg p)$.

Solution:

$$\begin{array}{lcl}
(1) & p \to q, \neg q, p \vdash p & \text{by } (\in) \\
(2) & p \to q, \neg q, p \vdash p \to q & \text{by } (\in) \\
(3) & p \to q, \neg q, p \vdash q & \text{by } (\to -, 1, 2) \\
(4) & p \to q, \neg q, p \vdash \neg q & \text{by } (\in) \\
(5) & p \to q, \neg q \vdash \neg p & \text{by } (\neg -, 3, 4)
\end{array}$$

Exercise 32. *Show that* $(\neg p) \to (\neg q) \vdash (q \to p)$.

Solution:

$$\begin{array}{lcl}
(1) & (\neg p) \to (\neg q), q, \neg p \vdash \neg p & \text{by } (\in) \\
(2) & (\neg p) \to (\neg q), q, \neg p \vdash (\neg p) \to (\neg q) & \text{by } (\in) \\
(3) & (\neg p) \to (\neg q), q, \neg p \vdash q & \text{by } (\in) \\
(4) & (\neg p) \to (\neg q), q, \neg p \vdash \neg q & \text{by } (\to -, 1, 2) \\
(5) & (\neg p) \to (\neg q), q \vdash p & \text{by } (\neg -, 3, 4) \\
(6) & (\neg p) \to (\neg q) \vdash q \to p & \text{by } (\to +, 5)
\end{array}$$

Exercise 33. *Show that* $(p \wedge (\neg q)) \to r, (\neg r), p \vdash q$.

Solution:

$$\begin{array}{lcl}
(1) & (p \wedge \neg q) \to r, \neg r, p, \neg q \vdash p & \text{by } (\in) \\
(2) & (p \wedge \neg q) \to r, \neg r, p, \neg q \vdash \neg q & \text{by } (\in) \\
(3) & (p \wedge \neg q) \to r, \neg r, p, \neg q \vdash (p \wedge \neg q) & \text{by } (\wedge +, 1, 2) \\
(4) & (p \wedge \neg q) \to r, \neg r, p, \neg q \vdash (p \wedge \neg q) \to r & \text{by } (\in) \\
(5) & (p \wedge \neg q) \to r, \neg r, p, \neg q \vdash r & \text{by } (\to -, 3, 4) \\
(6) & (p \wedge \neg q) \to r, \neg r, p, \neg q \vdash (\neg r) & \text{by } (\in) \\
(7) & (p \wedge \neg q) \to r, \neg r, p \vdash q & \text{by } (\neg -, 5, 6)
\end{array}$$

Exercise 34. *Show that* $(p \vee q), (\neg p) \vdash q$.

Solution:

(1)	$\neg p, p, \neg q \vdash p$	by $(\in)$
(2)	$\neg p, p, \neg q \vdash \neg p$	by $(\in)$
(3)	$\neg p, p \vdash q$	by $(\neg -, 1, 2)$
(4)	$\neg p, q \vdash q$	by $(\in)$
(5)	$\neg p, p \vee q \vdash q$	by $(\vee -, 3, 4)$

Exercise 35. *Show that* $\emptyset \vdash (\neg p) \to (p \to (p \to q))$.

Solution:

(1)	$\neg p, p, \neg(p \to q) \vdash p$	by $(\in)$
(2)	$\neg p, p, \neg(p \to q) \vdash \neg p$	by $(\in)$
(3)	$\neg p, p \vdash p \to q$	by $(\neg -, 1, 2)$
(4)	$\neg p \vdash p \to (p \to q)$	by $(\to +, 3)$
(5)	$\emptyset \vdash (\neg p) \to (p \to (p \to q))$	by $(\to +, 4)$

1.9.8 Putting them together!

Exercise 36. *(De Morgan's Law) Show that* $(\neg(a \vee b)) \vdash ((\neg a) \wedge (\neg b))$.

Solution:

(1)	$\neg(a \vee b), a \vdash \neg(a \vee b)$	by $(\in)$
(2)	$\neg(a \vee b), a \vdash a$	by $(\in)$
(3)	$\neg(a \vee b), a \vdash (a \vee b)$	by $(\vee+, 2)$
(4)	$\neg(a \vee b), b \vdash \neg(a \vee b)$	by $(\in)$
(5)	$\neg(a \vee b), b \vdash b$	by $(\in)$
(6)	$\neg(a \vee b), b \vdash (a \vee b)$	by $(\vee+, 5)$
(7)	$\neg(a \vee b) \vdash \neg a$	by $(\wedge+, 1, 3)$
(8)	$\neg(a \vee b) \vdash \neg b$	by $(\wedge+, 4, 6)$
(9)	$\neg(a \vee b) \vdash \neg a \wedge \neg b$	by $(\wedge+, 7, 8)$

Exercise 37. *(De Morgan's Law) Show that* $((\neg a) \wedge (\neg b)) \vdash (\neg(a \vee b))$.

Solution:

(1)	$\neg a \wedge \neg b, a, \neg q \vdash \neg a \wedge \neg b$	by $(\in)$
(2)	$\neg a \wedge \neg b, a, \neg q \vdash \neg a$	by $(\wedge-, 1)$
(3)	$\neg a \wedge \neg b, a, \neg q \vdash a$	by $(\in)$
(4)	$\neg a \wedge \neg b, a \vdash q$	by $(\neg-, 2, 3)$
(5)	$\neg a \wedge \neg b, b, \neg q \vdash \neg a \wedge \neg b$	by $(\in)$
(6)	$\neg a \wedge \neg b, b, \neg q \vdash \neg b$	by $(\wedge-, 5)$
(7)	$\neg a \wedge \neg b, b, \neg q \vdash b$	by $(\in)$
(8)	$\neg a \wedge \neg b, b \vdash q$	by $(\neg-, 6, 7)$
(9)	$\neg a \wedge \neg b, a \vee b \vdash q$	by $(\vee-, 4, 8)$
(10)	$\neg a \wedge \neg b, a, q \vdash \neg a \wedge \neg b$	by $(\in)$
(11)	$\neg a \wedge \neg b, a, q \vdash \neg a$	by $(\wedge-, 10)$
(12)	$\neg a \wedge \neg b, a, q \vdash a$	by $(\in)$
(13)	$\neg a \wedge \neg b, a \vdash \neg q$	by $(\neg+, 11, 12)$
(14)	$\neg a \wedge \neg b, b, q \vdash \neg a \wedge \neg b$	by $(\in)$
(15)	$\neg a \wedge \neg b, b, q \vdash \neg b$	by $(\wedge-, 14)$
(16)	$\neg a \wedge \neg b, b, q \vdash b$	by $(\in)$
(17)	$\neg a \wedge \neg b, b \vdash \neg q$	by $(\neg+, 15, 16)$
(18)	$\neg a \wedge \neg b, a \vee b \vdash \neg q$	by $(\vee-, 13, 18)$
(19)	$\neg a \wedge \neg b \vdash \neg(a \vee b)$	by $(\wedge+, 8, 18)$

Exercise 38. *(De Morgan's Law) Show that* $((\neg a) \vee (\neg b)) \vdash (\neg(a \wedge b))$.

Solution:

(1)	$\neg b, (a \wedge b) \vdash a \wedge b$	by $(\in)$
(2)	$\neg b, (a \wedge b) \vdash \neg b$	by $(\in)$
(3)	$\neg b, (a \wedge b) \vdash b$	by $(\wedge-, 1)$
(4)	$\neg b \vdash \neg(a \wedge b)$	by $(\neg+, 2, 3)$
(5)	$\neg a, (a \wedge b) \vdash a \wedge b$	by $(\in)$
(6)	$\neg a, (a \wedge b) \vdash \neg a$	by $(\in)$
(7)	$\neg a, (a \wedge b) \vdash a$	by $(\wedge-, 5)$
(8)	$\neg a \vdash \neg(a \wedge b)$	by $(\neg+, 6, 7)$
(9)	$\neg a \vee \neg b \vdash \neg(a \wedge b)$	by $(\vee-, 4, 8)$

Exercise 39. *(De Morgan's Law) Show that* $(a \vee b) \vdash (\neg((\neg a) \wedge (\neg b)))$.

Solution:

(1)	$\neg a \wedge \neg b, a \vdash \neg a \wedge \neg b$	by $(\in)$
(2)	$\neg a \wedge \neg b, a \vdash \neg a$	by $(\wedge-, 1)$
(3)	$\neg a \wedge \neg b, a \vdash a$	by $(\in)$
(4)	$\neg a \wedge \neg b, b \vdash \neg a \wedge \neg b$	by $(\in)$
(5)	$\neg a \wedge \neg b, b \vdash \neg b$	by $(\wedge-, 4)$
(6)	$\neg a \wedge \neg b, b \vdash b$	by $(\in)$
(7)	$a \vdash \neg(\neg a \wedge \neg b)$	by $(\neg+, 2, 3)$
(8)	$b \vdash \neg(\neg a \wedge \neg b)$	by $(\neg+, 5, 6)$
(9)	$a \vee b \vdash \neg(\neg a \wedge \neg b)$	by $(\vee-, 7, 8)$

Exercise 40. *(De Morgan's Law) Show that* $(\neg(a \wedge b)) \vdash ((\neg a) \vee (\neg b))$*.*

Solution:

Exercise 41. *Show that* $(\neg(p \to q)) \vdash (q \to p)$*.*

Solution:

Exercise 42. *(Law of excluded middle)* $\emptyset \vdash (a \vee (\neg a))$.

Solution: Solution 1:

(1)	$\neg(a \vee (\neg a)), a \vdash a$	by $(\in)$
(2)	$\neg(a \vee (\neg a)), a \vdash \neg(a \vee (\neg a))$	by $(\in)$
(3)	$\neg(a \vee (\neg a)), a \vdash a \vee (\neg a)$	by $(\vee+, 1)$
(4)	$\neg(a \vee (\neg a)) \vdash \neg a$	by $(\neg+, 2, 3)$
(5)	$\neg(a \vee (\neg a)) \vdash \neg(a \vee (\neg a))$	by $(\in)$
(6)	$\neg(a \vee (\neg a)) \vdash a \vee (\neg a)$	by $(\vee+, 4)$
(7)	$\emptyset \vdash a \vee (\neg a)$	by $(\neg-, 5, 6)$

Solution 2:

(1)	$\neg(a \vee (\neg a)), \neg a \vdash \neg a$	by $(\in)$
(2)	$\neg(a \vee (\neg a)), \neg a \vdash \neg(a \vee (\neg a))$	by $(\in)$
(3)	$\neg(a \vee (\neg a)), \neg a \vdash a \vee (\neg a)$	by $(\vee+, 1)$
(4)	$\neg(a \vee (\neg a)) \vdash a$	by $(\neg-, 2, 3)$
(5)	$\neg(a \vee (\neg a)) \vdash \neg(a \vee (\neg a))$	by $(\in)$
(6)	$\neg(a \vee (\neg a)) \vdash a \vee (\neg a)$	by $(\vee+, 4)$
(7)	$\emptyset \vdash a \vee (\neg a)$	by $(\neg-, 5, 6)$

1.9.9 Putting them together: Additional exercises

Exercise 43. $(\neg(p \to q)) \vdash p$.

Exercise 44. $((p \to q) \to p) \vdash p$.

Exercise 45. $((p \to q) \to q) \vdash ((\neg q) \to p)$.

Exercise 46. $\emptyset \vdash ((p \to q) \lor (q \to r))$

Exercise 47. $(p \to (q \lor r)) \vdash ((p \to q) \lor (p \to r))$.

1.9.10 Other problems

Exercise 48. *E4 Exercise 4: Prove that for any set of propositional formulas* Σ *and any propositional variables* p *and* q*, if* $\Sigma \vdash p$*, then* $\Sigma \vdash ((\neg p) \to q)$*.*

Solution:

Proof. Let Σ be a set of propositional formulas and let p and q be propositional variables. Assume that $\Sigma \vdash p$. This means that the following proof exists.

(1)	$\Sigma \vdash p$	by assumption

Using the above proof, we will construct a formal deduction proof for $\Sigma \vdash ((\neg p) \to q)$.

(1)	$\Sigma \vdash p$	by assumption
(2)	$\Sigma, \neg p, \neg q \vdash p$	by $(+, 1)$
(3)	$\Sigma, \neg p, \neg q \vdash \neg p$	by $(\in)$
(4)	$\Sigma, \neg p \vdash q$	by $(\neg -, 2, 3)$
(5)	$\Sigma \vdash (\neg p) \to q$	by $(\to +, 4)$

Therefore, $\Sigma \vdash ((\neg p) \to q)$ holds. □

1.10 Soundness and Completeness of Formal Deduction

1.10.1 The soundness of inference rules

Exercise 49. *The following inference rule is called Disjunctive syllogism.*

$$\begin{aligned} \textit{if}\ &\Sigma \vdash \neg A, \\ &\Sigma \vdash A \vee B, \\ \textit{then}\ &\Sigma \vdash B. \end{aligned}$$

where A and B are well-formed propositional formulas.

Prove that this inference rule is sound. That is, prove that if $\Sigma \models \neg A$ and $\Sigma \models A \vee B$, then $\Sigma \models B$.
You must use **the definition of tautological consequence** *to write your proof. Do not use any other technique such as truth table, valuation tree, logical identities, formal deduction, soundness, or completeness.*

Solution:

Proof. Consider a truth valuation t under which $\Sigma^t = 1$. Since $\Sigma \models (\neg A)$ and $\Sigma \models A \vee B$, we have that $(\neg A)^t = 1$ and $(A \vee B)^t = 1$. We need to show that $B^t = 1$.
By the truth table of $\neg$, since $(\neg A)^t = 1$, $A^t = 0$.
By the truth table of $\vee$, since $(A \vee B)^t = 1$, at least one of A and B is true under t. Since $A^t = 0$, then $B^t = 1$.
Therefore, $\Sigma \models B$ holds. □

Remark 2. *To prove that a tautological consequence holds, we need to consider all truth valuations under which all of the premises are true. For each such truth valuation, we need to show that the conclusion is true.*

The proof typically looks like the following.

- *Consider a truth valuation t under which all of the premises are true.*
- *If premise 1 is true under t, then A must be ... under t and B must be ... under t. If premise 2 is true under t, then ...*
- *There are ... cases that we need to consider.*
- *Case 1: this case is impossible because .../... the conclusion is true under t.*
- *Case 2: ...*
- *The conclusion is true in every case. Therefore, the tautological consequence holds.*

Exercise 50. *Consider the following inference rule:*

$$\frac{(A \to B)}{(B \to A)} \textit{ Flip the implication}$$

where A and B are well-formed propositional formulas.

Prove that this inference rule is NOT sound. That is, prove the following statement:

$$\{(A \to B)\} \not\models (B \to A)$$

You must use **the definition of tautological consequence** *to write your proof. Do not use any other technique such as truth table, valuation tree, logical identities, formal deduction, soundness, or completeness.*

Solution:

Remark 3. *To prove that a tautological consequence does not hold, we need to find a concrete counterexample, which shows that, there is a truth valuation t under which all of the premises are true and the conclusion is false.*

A concrete counterexample consist of the following:

- *Choose concrete formulas for A and B. In the following proof, we let A be p and B be q where p and q are propositional variables.*
- *Choose a truth valuation t such that all the premises are true and the conclusion is false.*

Choosing a concrete formula for each symbol is important. In the proof below, if we do not assign concrete formulas to A and B, then we cannot make claims about their truth values under t. We want to find a truth valuation under which B is true and A is false. This is not possible if B is $(r \wedge (\neg r))$ and A is $(r \vee (\neg r))$.

The difficult part is coming up with a counterexample that works. After that, writing up the proof is straightforward.

Proof. To prove that the tautological consequence does not hold, we need to find one counterexample.

Let p and q be two propositional variables. Let A be p and let B be q. Consider a truth valuation t under which $p^t = 0$ and $q^t = 1$.

Under t, the premise is true. $(A \to B)^t = (p \to q)^t = 1$.
Under t, the conclusion is false. $(B \to A)^t = (q \to p)^t = 0$.

We found a truth valuation under which the premise is true and the conclusion is false. Thus, the tautological consequence does not hold. □

1.10.2 Soundness and Completeness of Formal Deduction

Exercise 51. *Prove or disprove this statement: If $\{a, b\} \vdash c$, then $\emptyset \vDash ((a \wedge b) \to c)$. a, b, and c are well-formed propositional formulas.*

Solution:

Remark 4. *The statement is an implication, and the premise and the conclusion of the implication differ in two ways. The premise is about the existence of a formal deduction proof, whereas the conclusion is about a tautological consequence. Moreover, the premise has a and b on the left hand side, whereas the conclusion has everything on the right hand side. Thus, there are two ways for us to transform the premise into the conclusion.*

Approach 1:

A visual representation of approach 1:

$$\{a, b\} \vdash c \quad \to \quad \{a, b\} \vDash c \quad \to \quad \emptyset \vDash ((a \wedge b) \to c)$$

First, we transform $\{a, b\} \vdash c$ (the existence of a proof) to $\{a, b\} \vDash c$ (a tautological consequence) by using the soundness of formal deduction.

Then, we move a and b from the left hand side to the right hand side by proving that $\{a, b\} \vDash c$ are $\emptyset \vDash ((a \wedge b) \to c)$ equivalent by the definition of tautological consequence.

Approach 2:

A visual representation of approach 2:

$$\{a, b\} \vdash c \quad \to \quad \emptyset \vdash ((a \wedge b) \to c) \quad \to \quad \emptyset \vDash ((a \wedge b) \to c)$$

First, we move a and b from the left hand side to the right hand side by proving that $\{a, b\} \vdash c$ and $\emptyset \vdash ((a \wedge b) \to c)$ are equivalent.

Then, we transform $\emptyset \vdash ((a \wedge b) \to c)$ (the existence of a proof) to $\emptyset \vDash ((a \wedge b) \to c)$ (a tautological consequence) by the soundness of formal deduction.

See the two proofs on the following page.

Proof 1. We will prove the statement.

Assume $\{a, b\} \vdash c$ holds.

By the soundness of formal deduction, the tautological consequence $\{a, b\} \vDash c$ holds.

Consider a truth valuation t under which $a^t = 1$ and $b^t = 1$. We know that $c^t = 1$ by $\{a, b\} \vDash c$. Therefore, by the definition of an implication, we know that $((a \wedge b) \to c)$ is a tautology.

Consider a truth valuation t. There is no formula in $\emptyset$. Thus, t satisfies $\emptyset$. t also satisfies $((a \wedge b) \to c)$ since $((a \wedge b) \to c)$ is a tautology. Therefore, the tautological consequence $\emptyset \vDash ((a \wedge b) \to c)$ holds.

□

Proof 2. We will prove the statement.

Assume $\{a, b\} \vdash c$ holds. Thus, there is a formal deduction proof which starts with a and b as the premises and ends with c.

1.	a	premise
2.	b	premise
3.	...	...
4.	c	...

We construct a formal deduction proof for $\emptyset \vdash ((a \wedge b) \to c)$ as follows.

1.	$(a \wedge b)$	assumption
2.	a	$\wedge$e: 1
3.	b	$\wedge$e: 1
4.	...	...
5.	c	...
6.	$((a \wedge b) \to c)$	$\to$i: 1-5

This proof shows that $\emptyset \vdash ((a \wedge b) \to c)$ holds.

By the soundness of formal deduction, the tautological consequence $\emptyset \vDash ((a \wedge b) \to c)$ holds.

□

Exercise 52. *Prove or disprove this statement: If $\{A\} \vDash B$, then $\emptyset \vdash (B \to A)$. A and B are well-formed propositional formulas.*

Solution:

Remark 5. *To show that the implication is false, we need to choose concrete formulas for A and B such that the premise is true and the conclusion is false.*

By inspecting the premise and the conclusion, we see that the concrete formulas need to make sure that A entails B, but B does not entail A.

Choosing A to be p and B to be $(p \vee q)$ satisfy both requirements.

Proof. We will disprove the statement.

Let p and q be two propositional variables. Let A be p and let B be $(p \vee q)$.

First, we prove that $\{A\} \vDash B$ holds. Consider a truth valuation t under which A is true. This means that $p^t = 1$. Under t, B is true because $(p \vee q)^t = 1$. Therefore, the tautological consequence $\{A\} \vDash B$ holds.

Now, we prove that $\emptyset \nvdash (B \to A)$ holds. To show that such a proof does not exist, it suffices to show that the corresponding tautological consequence $\emptyset \vDash (B \to A)$ does not hold. Then by the contrapositive of the soundness of formal deduction, we have that $\emptyset \nvdash (B \to A)$ holds.

To prove that $\emptyset \nvDash (B \to A)$ (or $\emptyset \nvDash ((p \vee q) \to p)$), we consider a truth valuation t such that $p^t = 0$ and $q^t = 1$. Under t, $B^t = (p \vee q)^t = 1$ and $A^t = p^t = 0$. Therefore, $\emptyset \nvDash (B \to A)$ holds.

□

1.11 Proving the Completeness Theorem

Exercise 53. *Prove that the following two definitions of a consistent set are equivalent.*

1. *There exists a formula A such that $\Sigma \nvdash A$.*
2. *For every formula A, if $\Sigma \vdash A$, then $\Sigma \nvdash (\neg A)$.*

Exercise 54. *Let* Σ_1 *and* Σ_2 *be sets of propositional formulas. Let* $\Sigma_1 \subseteq \Sigma_2$. *Prove or disprove the statement below: If* Σ_1 *is consistent, then* Σ_2 *is consistent.*

Exercise 55. *Let* Σ_1 *and* Σ_2 *be sets of propositional formulas. Let* $\Sigma_1 \subseteq \Sigma_2$. *Prove or disprove the statement below: If* Σ_2 *is consistent, then* Σ_1 *is consistent.*

Prove that the following two definitions of a maximally consistent set are equivalent. Assume that Σ is consistent.

1. For every propositional formula B, if $\Sigma \nvdash B$ then $\Sigma \cup \{B\}$ is inconsistent.
2. For every propositional formula A, $\Sigma \vdash A$ or $\Sigma \vdash (\neg A)$.

Solution: Question: Is the OR in definition 2 an exclusive OR?
Answer: Yes, it has to be. If for every propositional formula A, $\Sigma \vdash A$ and $\Sigma \vdash (\neg A)$, then A has to be inconsistent, which contradicts with our assumption that Σ is consistent.

Part (a) Prove that if a set Σ satisfies definition 1, then it also satisfies definition 2.

Proof Sketch:
To show that Σ satisfies definition 2, we need to show that for every propositional formula A, $\Sigma \vdash A$ or $\Sigma \vdash (\neg A)$. If at least one of $\Sigma \vdash A$ and $\Sigma \vdash (\neg A)$ is true, then we are done. However, it is unlikely that we can prove that one of them is always true. Therefore, it must be the case that one is true in some scenarios and the other one is true in other scenarios.

A common approach for proving a disjunction is to divide into several cases. It must be true that either $\Sigma \vdash A$ or $\Sigma \nvdash A$. In fact, these two cases are mutually exclusive and exhaustive. Therefore, we will consider two cases. In each case, we will need to prove that $\Sigma \vdash A$ and $\Sigma \vdash (\neg A)$.

Here is a sketch of the proof.
Assume that Σ satisfies definition 1.
Consider any propositional formula A.
Case (1): Assume that $\Sigma \vdash A$.
We need to prove that $\Sigma \vdash A$ or $\Sigma \vdash (\neg A)$.
Case (2): Assume that $\Sigma \nvdash A$.
We need to prove that $\Sigma \vdash A$ or $\Sigma \vdash (\neg A)$.

Part (b) Prove that if a set Σ satisfies definition 2, then it also satisfies definition 1.
Proof sketch:

2 Predicate Logic

2.1 Translations

Exercise 56. *Let the domain be the set of animals. Let $B(x)$ mean that x is a bear. Let $H(x)$ mean that x likes honey.*

Translate "every bear likes honey" into predicate logic.

Solution: People often come up with the following two translations. See the formulas and the corresponding explanations below.

- $(\forall x\ (B(x) \wedge H(x)))$

  This formula says that every animal x is a bear and likes honey.

  This formula is an incorrect translation. The original sentence does not require every animal to be a bear. The sentence simply ignores any animal that is not a bear and focuses on animals that are bears.

- $(\forall x\ (B(x) \to H(x)))$

  This formula says that for every animal x, if x is a bear, then x likes honey.

  This is a correct translation. If an animal is a bear, then it must like honey as required by the original sentence. If an animal is not a bear, then the premise of the implication is false, which means that the implication is vacuously true. (In other words, we don't care about animals that are not bears.)

To differentiate between two predicate formulas, it is often a useful exercise to come up with a domain for which one formula is true and the other formula is false.

Consider a domain, which contains a bear A who likes honey and a rabbit B.

- For this domain, the first formula is false. When x is rabbit B, x is not a bear.
- For this domain, the second formula is true. When x is bear A, it likes honey, so the implication is true. When x is rabbit B, it is not a bear, so the implication is vacuously true. Since the implication is true for every element of the domain, the formula is true.

In general, consider a domain D and a predicate $P(x)$.
The following sentence

> "All <things in D for which P is true> have the property Q."

translates into the formula

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

Exercise 57. *Let the domain be the set of animals. Let $B(x)$ mean that x is a bear. Let $H(x)$ mean that x likes honey.*

Translate "some bear likes honey" into predicate logic.

Solution: People often come up with the following two translations. See the formulas and the corresponding explanations below.

- $(\exists x\ (B(x) \wedge H(x)))$

  This formula says that there is an animal x, which is a bear and likes honey.

  This formula is the correct translation. The original sentence requires that there is a bear in the domain. Furthermore, it requires that there is a bear in the domain that likes honey. This formula guarantees both.

- $(\exists x\ (B(x) \to H(x)))$

  This formula says that there is an animal x, which is either not a bear, or is a bear and likes honey.

  This sentence is an incorrect translation, although many people think that it makes intuitive sense. The problem with this formula comes from the fact that the implication is vacuously true when the premise is false. This formula does not guarantee that there has to be a bear in the domain. As soon as we find an animal that is not a bear in the domain, the premise of the implication is false and the implication is vacuously true. This does not correspond to the original sentence, which requires that there is a bear in the domain.

To differentiate these two formulas, let's consider a domain, which contains a rabbit B. For this domain, the original sentence should be false because there is no bear.

- For this domain, the first formula is false. We cannot find a bear in the domain, which is required by the formula.
- For this domain, the second formula is true. When x is rabbit B, B is not a bear, so the premise of the implication is false. Thus, the implication is vacuously true. Since we have found an animal which makes the implication true, the formula is true.

In general, consider a domain D and a predicate $P(x)$.
The following sentence

> "Some <thing in D for which P is true> have the property Q."

translates into the formula

$$(\exists x\ (P(x) \wedge Q(x))).$$

Based on the two exercises above, could you summarize the general patterns of translations? Which binary connectives usually go with the universal and the existential quantifiers?

As a general rule of thumb, the universal quantifier is often used in conjunction with the implication ($\rightarrow$), and the existential quantifier is often used in conjunction with the conjunction ($\wedge$). We've seen examples of both above.

The universal quantifier

- $\forall$ and $\rightarrow$: This universal quantifier pairs well with the implication. This combination is used to make a statement about a subset of the domain. Therefore, we use the premise of the implication to restrict our attention to this subset. We don't have to worry about any element that is not in this subset because the implication is vacuously true for any such element.
- $\forall$ and $\wedge$: This combination is not impossible. However, it is a very strong statement. This combination is claiming that every element of the domain must satisfy the properties connected by the $\wedge$. If this is what you meant to express, then go ahead and use this combination.

The existential quantifier

- $\exists$ and $\wedge$: The existential quantifier pairs well with the conjunction. This combination can be used to express the fact that there exists an element of domain which has the two properties connected by the conjunction.
- $\exists$ and $\rightarrow$: This combination does not make sense logically. The main reason is that it is too easy to make such a formula true. As soon as we find an element of the domain, which makes the premise of the implication false, the implication is vacuously true and the formula is true as well.

Exercise 58. *Translate the following sentences into predicate formulas.*

Let the domain contain the set of all students and courses. Define the following predicates:
$C(x)$: x is a course.
$S(x)$: x is a student.
$T(x, y)$: student x has taken course y.

1. Every student has taken some course.

   Solution: $(\forall x\ (S(x) \to (\exists y\ (C(y) \wedge T(x, y)))))$

2. A student has taken a course.

   Solution: $(\exists x\ (S(x) \wedge (\exists y\ (C(y) \wedge T(x, y)))))$

3. No student has taken every course.

   Solution: $(\neg(\exists x\ (S(x) \wedge (\forall y\ (C(y) \to T(x, y))))))$

4. Some student has not taken any course.

   Solution: $(\exists x\ (S(x) \wedge (\forall y\ (C(y) \to (\neg T(x, y))))))$

5. Every student has taken every course.

   Solution: $(\forall x\ (S(x) \to (\forall y\ (C(y) \to T(x, y)))))$

Exercise 59. *Translating "at least", "at most", and "exactly". Translate the following sentences into predicate formulas.*

- There is at least one bear.

  Solution:

  $$(\exists x\ B(x))$$

- There are at least two bears.

  Solution:

  $$(\exists x\ (\exists y\ ((B(x) \wedge B(y)) \wedge (x \neq y))))$$

  The formula says: there are two bears x and y, and x and y must be different. Note that, if we don't have $(x \neq y)$, the formula only guarantees that there exists one bear because x and y could refer to the same animal in the domain.

- There is at most one bear.

  Solution:

  $$(\neg(\exists x\ (\exists y\ ((B(x) \wedge B(y)) \wedge (x \neq y)))))$$

  The negation of "at most one" is "at least two". Therefore, the sentence is equivalent to "It is not the case that there exist two different bears".

  Using the generalized De Morgan's laws, we can show that the above formula is logically equivalent to the formula below.

  $$(\forall x\ (\forall y\ ((B(x) \wedge B(y)) \rightarrow (x = y))))$$

  This formula says that: If we can find two bears x and y, then x and y must refer to the same bear. To understand this formula, imagine that I made the claim that there is at most one bear. Then your goal is to disprove my claim. You find two bears in the domain and show them to me. For my claim to be true, I have to be able to prove that the two bears you found are actually the same bear. I have to be able to do this no matter which two bears you show to me.

  Yet another translation is that: ((there is no bear) or (there is exactly one bear)). We can use any translation of "there is exactly one bear" on the next page.

  $$((\forall x\ (\neg B(x))) \vee (\exists y\ (B(y) \wedge (\forall z\ (B(z) \rightarrow (y = z))))))$$

- There is exactly one bear.

  Solution: One translation is: there is at least one bear and there is at most one bear.

  $$((\exists z\ B(z)) \wedge ((\neg(\exists x\ (\exists y\ ((B(x) \wedge B(y)) \wedge (x \neq y)))))))$$

  Another translation: there is at least one bear and if there is another bear, then the two bears must be the same.

  $$(\exists x\ (B(x) \wedge (\forall y\ (B(y) \rightarrow (x = y)))))$$

2.2 Semantics of Predicate Formulas

Consider this language of predicate logic:

- Individual constant symbols: a, b, c
- Free Variable Symbols: u, v, w
- Bound Variable symbols: x, y, z
- Function symbols: f is a unary function, g is a binary function.
- Predicate/Relation symbols: P is a unary predicate, Q is a binary predicate.

2.2.1 Evaluating Formulas with No Variables

Exercise 60. *Give a valuation v such that $Q(f(c), a)^v = 1$ where $D = \{1, 2, 3\}$.*

Solution:

Remark 6. *We only need to define the components of the valuation that appear in the formula. This means, we only need to define a^v, c^v, f^v, and Q^v.*
I don't like to work with weird functions. So let's fix the function f to something simple first. Let f^v be $f^v(x) = x, \forall x \in D$. Given this, we simplify the formula below.

$$f(c)^v = f^v(c^v) = c^v \tag{98}$$

$$Q(f(c), a)^v = Q(c, a)^v \tag{99}$$

I like to deal with the predicates last. So let's assign meanings to the individual constant symbols. Let $c^v = 1$ and $a^v = 2$. Then, we have that $Q(c, a)^v$ is true if and only if $\langle 1, 2\rangle \in Q^v$.

Finally, let's define Q^v. Above the above analysis, at a minimum, we need $\langle 1, 2\rangle \in Q^v$. We could include other tuples in Q^v if we like, but they don't affect the truth value of this formula. Thus, let $Q^v = \{\langle 1, 2\rangle\}$.

Solution Text: The valuation v is given below.

- $D = \{1, 2, 3\}$.
- $a^v = 2, c^v = 1$.
- $f^v(x) = x, \forall x \in D$.
- $Q^v = \{\langle 1, 2\rangle\}$.

Therefore, $Q(f(c), a)^v = 1$ since all of the following hold:

$$f(c)^v = f^v(1) = 1 \tag{100}$$

$$a^v = 2 \tag{101}$$

$$\langle 1, 2\rangle \in Q^v. \tag{102}$$

Exercise 61. *Give a valuation v such that $Q(f(c), a)^v = 0$.*

Solution:

Remark 7. *All we need to do is make one small adjustment to the interpretation in exercise 60.*

To make the formula false, we need to make sure the tuple $\langle 1, 2\rangle \notin Q^v$. Let Q^v be the empty set.

Solution Text: The valuation v is given below.

- $D = \{1, 2, 3\}$.
- $a^v = 2, c^v = 1$.
- $f^v(x) = x, \forall x \in D$.
- $Q^v = \emptyset$.

Therefore, $Q(f(c), a)^v = 0$ since all of the following hold:

$$f(c)^v = f^v(1) = 1 \tag{103}$$

$$a^v = 2 \tag{104}$$

$$\langle 1, 2\rangle \notin Q^v. \tag{105}$$

2.2.2 Evaluating Formulas without Bound Variables

Exercise 62. *Give a valuation v such that $Q(f(u), a)^v = 1$.*

Solution:

Remark 8. *Let's start with the valuation in the solution to exercise 60. We simplify the formula below.*

$$f(u)^v = f^v(u^v) = u^v, a^v = 2.$$

Thus, the formula is true if and only if $\langle u^v, 2\rangle \in Q^v$.

The only tuple in Q^v is $\langle 1, 2\rangle$. Thus, it is sufficient to let $u^v = 1$.

Solution Text: The valuation v is given below. $D = \{1, 2, 3\}$, $a^v = 2$, $u^v = 1$, $f^v(x) = x, \forall x \in D$, $Q^v = \{\langle 1, 2\rangle\}$.
Given v, we can show that $Q(f(x), a)^v = 1$ because

$$u^v = 1, f(u)^v = f^v(1) = 1, a^v = 2, \langle 1, 2\rangle \in Q^v.$$

Exercise 63. *Give a valuation v such that $Q(f(x), a)^v = 0$.*

Solution:

Remark 9. *Let's start with the valuation in the solution to exercise 62, and modify Q^v to be the empty set. Under v, the formula is false, using similar reasoning as exercise 61.*

Solution Text: The valuation v are given below.

$$D = \{1, 2, 3\}, a^v = 2, u^v = 1, f^v(x) = x, \forall x \in D, Q^v = \{\langle 1, 2\rangle\}.$$

Given v, we can show that $Q(f(x), a)^v = 0$ because

$$u^v = 1, f(x)^v = f^v(1) = 1, a^v = 2, \langle 1, 2\rangle \notin Q^v.$$

2.2.3 Evaluating Formulas with Free and Bound Variables

Exercise 64. *Give a valuation v such that $(\exists x\ Q(x, u))^v = 1$. Assume that the domain is $D = \{1, 2, 3\}$.*

Solution:

Remark 10. *Here is more explanation to help you understand how I came up with the valuation v above.*
u is a free variable in the formula. Let's arbitrarily define $u^v = 2$.

To make the formula true, there must be at least one tuple in Q^v and the second value in the tuple (the value of u in the tuple) must be 2 because $u^v = 2$. Let $Q^v = \{\langle 1, 2\rangle\}$.

Solution Text: The valuation v is shown below.

$$D = \{1, 2, 3\}, u^v = 2, Q^v = \{\langle 1, 2\rangle\}.$$

Given the v above, we know that $Q(u, w)^{v(u/1)} = 1$ because all of the following hold:

$$\langle u, w\rangle^{v(u/1)(w/2)} = \langle 1, 2\rangle \in Q^v \qquad (106)$$

Hence, by the $\exists$-satisfaction rule, $(\exists x\ Q(x, y))^v = 1$.

Exercise 65. *Give a valuation v such that $(\forall x\ Q(x, u))^v = 1$. Assume that the domain is $D = \{1, 2, 3\}$.*

Solution:

Remark 11. *Let's start with the valuation v in exercise 64.*

We will modify Q^v. To make the formula true, we must be able to replace x by any value in the domain. Furthermore, for each tuple in Q^v, the second value in the tuple must be 2 because the environment maps y to 2. Thus, let $Q^v = \{\langle 1, 2\rangle, \langle 2, 2\rangle, \langle 3, 2\rangle\}$.

Solution Text: The valuation is shown below.

- $D = \{1, 2, 3\}$.
- $a^v = 2, b^v = 1, c^v = 1$.
- $f^v(x) = x, \forall x \in D$, $g^v(x) = 1, \forall x \in D$.
- $Q^v = \{\langle 1, 2\rangle, \langle 2, 2\rangle, \langle 3, 2\rangle\}$, $P^v = \emptyset$.

The environment E is $E(x) = 1, E(y) = 2, E(z) = 1$.

We will prove that $(\forall x\ Q(x, y))^v = 1$. Consider all possible values of x. By the definition of Q^v, the following statements hold.

- $[x \mapsto 1]$: $Q(x, y)^{(I, E[x \mapsto 1])} = 1$ because all of the following hold.

$$\begin{aligned}&E[x \mapsto 1](x) = 1\\&E[x \mapsto 1](y) = 2\\&\langle 1, 2\rangle \in Q^v.\end{aligned}$$

- $[x \mapsto 2]$: $Q(x, y)^{(I, E[x \mapsto 2])} = 1$ because all of the following hold.

$$\begin{aligned}&E[x \mapsto 2](x) = 2\\&E[x \mapsto 2](y) = 2\\&\langle 2, 2\rangle \in Q^v.\end{aligned}$$

- $[x \mapsto 3]$: $Q(x, y)^{(I, E[x \mapsto 3])} = 1$ because all of the following hold.

$$\begin{aligned}&E[x \mapsto 3](x) = 3\\&E[x \mapsto 3](y) = 2\\&\langle 3, 2\rangle \in Q^v.\end{aligned}$$

Therefore, by the satisfaction rules for $\forall$, $(\forall x\ Q(x, y))^v = 1$.

2.2.4 Evaluating Formulas with Bound Variables Only

Exercise 66. *Give an interpretation I and an environment E such that $(\exists x(\forall y\ Q(x,y)))^v = 1$. Start with the domain $D = \{1,2,3\}$.*

Solution:

Remark 12. *To make the formula true, there must be at least 3 tuples in Q^v because y (the second value of each tuple) could take any of the 3 possible values in the domain.*

The first element of all three tuples must be the same because there must be one value for x that makes $Q(x,y)$ true.

Note that, when choosing the value of x, we do not know the value of y yet. Our choice of value for x cannot depend on the value of y.

One definition of Q^v that satisfies all these requirements is $Q^v = \{\langle 1,1\rangle, \langle 1,2\rangle, \langle 1,3\rangle\}$.

Solution Text: The interpretation I is given below.

- $D = \{1,2,3\}$.
- $a^v = 2, b^v = 1, c^v = 1$.
- $f^v(x) = x, \forall x \in D$, $g^v(x) = 1, \forall x \in D$.
- $Q^v = \{\langle 1,1\rangle, \langle 1,2\rangle, \langle 1,3\rangle\}$, $P^v = \emptyset$.

Let E be an arbitrary environment.

We will prove that $(\exists x(\forall y\ Q(x,y)))^v = 1$.

By the satisfaction rules of $\exists$, we need to show that $(\forall y\ Q(x,y))^{(I,E[x\mapsto d_x])} = 1$ for some $d_x in D$.
Consider $d_x = 1$. We now need to show that $Q(x,y)^{(I,E[x\mapsto d_x][y\mapsto d_y)} = 1$ for every $d_y \in D$. Consider all possible values of y.

- $[y \mapsto 1]$: $Q(x,y)^{(I,E[x\mapsto 1][y\mapsto 1])} = 1$ because all of the following hold.

$$E[x \mapsto 1][y \mapsto 1](x) = 1 \tag{107}$$
$$E[x \mapsto 1][y \mapsto 1](y) = 1 \tag{108}$$
$$\langle E[x \mapsto 1][y \mapsto 1](x), E[x \mapsto 1][y \mapsto 1](y)\rangle = \langle 1,1\rangle \in Q^v. \tag{109}$$

- $[y \mapsto 2]$: $Q(x,y)^{(I,E[x\mapsto 1][y\mapsto 2])} = 1$ because all of the following hold.

$$E[x \mapsto 1][y \mapsto 2](x) = 1 \tag{110}$$
$$E[x \mapsto 1][y \mapsto 2](y) = 2 \tag{111}$$
$$\langle E[x \mapsto 1][y \mapsto 2](x), E[x \mapsto 1][y \mapsto 2](y)\rangle = \langle 1,2\rangle \in Q^v. \tag{112}$$

- $[y \mapsto 3]$: $Q(x,y)^{(I,E[x\mapsto 1][y\mapsto 3])} = 1$ because all of the following hold.

$$E[x \mapsto 1][y \mapsto 3](x) = 1 \tag{113}$$
$$E[x \mapsto 1][y \mapsto 3](y) = 3 \tag{114}$$
$$\langle E[x \mapsto 1][y \mapsto 3](x), E[x \mapsto 1][y \mapsto 3](y)\rangle = \langle 1, 3\rangle \in Q^v. \tag{115}$$

By the satisfaction rules of $\forall$, $(\exists x(\forall y\ Q(x,y)))^{(I,E[x\mapsto 1])} = 1$ holds. By the definition of $\exists$, $(\exists x(\forall y\ Q(x,y)))^v = 1$ holds.

Exercise 67. *Give an interpretation I and an environment E such that $(\exists x(\forall y\ Q(x,y)))^v = 0$. Start with the domain $D = \{1, 2, 3\}$.*

Solution:

Remark 13. *The formula has no free variables. The bound variables get their meanings through the quantifiers. Thus, there is no need to define an environment. We only need to define an interpretation to evaluate the formula.*

There are many ways to make the formula false. An easy solution is to let Q^v be the empty set. Then, $Q^v(x, y)$ is always false and the formula must be false as well.

If there are tuples in Q^v, we need to make sure that Q^v does not have three tuples such that the first value of all three tuples are the same and the second value in all three tuples are all different.

Solution Text:
The interpretation I is shown below.

- $D = \{1, 2, 3\}$.
- $a^v = 2, b^v = 1, c^v = 1$.
- $f^v(x) = x, \forall x \in D$, $g^v(x) = 1, \forall x \in D$.
- $Q^v = \{\langle 1, 1\rangle, \langle 2, 2\rangle, \langle 3, 3\rangle\}$, $P^v = \emptyset$.

Let E be an arbitrary environment.

We will prove that $(\exists x(\forall y\ Q(x, y)))^v = 0$.

By the satisfaction rules for $\exists$, we need to show that $(\forall y\ Q(x, y))^{(I,E[x\mapsto d_x])} = 0$ holds for every $d_x \in D$.

Consider all possible values of x.

- $[x \mapsto 1]$:

  By the rules of satisfaction for $\forall$, to prove that $(\forall y\ Q(x, y))^{(I,E[x\mapsto 1])} = 0$, we need to prove that $Q(x, y)^{(I,E[x\mapsto 1][y\mapsto d_y])} = 0$ for some $d_y \in D$.

  $Q(x, y)^{(I,E[x\mapsto 1][y\mapsto 2])} = 0$ holds since all of the following statements hold.

  $$E[x \mapsto 1][y \mapsto 2](x) = 1 \tag{116}$$
  $$E[x \mapsto 1][y \mapsto 2](y) = 2 \tag{117}$$
  $$\langle E[x \mapsto 1][y \mapsto 2](x), E[x \mapsto 1][y \mapsto 2](y)\rangle = \langle 1, 2\rangle \notin Q^v \tag{118}$$

  Therefore, $Q(x, y)^{(I,E[x\mapsto 1][y\mapsto 2])} = 0$ holds, which means that $(\forall y\ Q(x, y))^{(I,E[x\mapsto 1])} = 0$ holds.

- $[x \mapsto 2]$:

  $Q(x, y)^{(I, E[x \mapsto 2][y \mapsto 1])} = 0$ holds because all of the following statements hold.

  $$E[x \mapsto 2][y \mapsto 1](x) = 2 \tag{119}$$
  $$E[x \mapsto 2][y \mapsto 1](y) = 1 \tag{120}$$
  $$\langle E[x \mapsto 2][y \mapsto 1](x), E[x \mapsto 2][y \mapsto 1](y) \rangle = \langle 2, 1 \rangle \notin Q^v \tag{121}$$

  Therefore, $(\forall y\ Q(x, y))^{(I, E[x \mapsto 2])} = 0$ holds.

- $[x \mapsto 3]$:

  $Q(x, y)^{(I, E[x \mapsto 3][y \mapsto 1])} = 0$ holds because all of the following statements hold.

  $$E[x \mapsto 3][y \mapsto 1](x) = 3 \tag{122}$$
  $$E[x \mapsto 3][y \mapsto 1](y) = 1 \tag{123}$$
  $$\langle E[x \mapsto 3][y \mapsto 1](x), E[x \mapsto 3][y \mapsto 1](y) \rangle = \langle 3, 1 \rangle \notin Q^v \tag{124}$$

  Therefore, $(\forall y\ Q(x, y))^{(I, E[x \mapsto 3])} = 0$ holds.

By the satisfaction rules of $\exists$, we have proven that $(\exists x(\forall y\ Q(x, y)))^v = 0$.

2.3 Tautological Consequence

Collected Wisdom:

- **Tautological consequence and formal deduction are two ways of proving the same argument.** Did you notice that Q1a of assignment 6 is the same as Q2d of assignment 7 (in Spring 2018)? We asked you prove the same argument, once with tautological consequence and once with formal deduction. **If you have trouble proving a statement using tautological consequence, you may want to try formal deduction first, and then convert it to a tautological consequence argument.**

Exercise 68. *Show that* $\{(\forall x\ P(x))\} \models (\exists x\ P(x))$.

Solution:

Proof. Consider an interpretation I such that $(\forall x\, P(x))^v = 1$. We will prove that $(\exists x\, P(x))^v = 1$.

Consider an arbitrary environment E. Let $d_1 \in D$ be a domain element.

By the satisfaction rules for $\forall$, $P(x)^{(I, E[x \mapsto d_1])} = 1$. Therefore, $E[x \mapsto d_1](x) = d_1 \in P^v$.

By the satisfaction rules for $\exists$, $(\exists x\ P(x))^v = 1$. □

Exercise 69. *Show that* $\{(\exists x\ P(x))\} \not\models (\forall x\ P(x))$.

Solution:

Proof. To prove that the tautological consequence does hold, we need to find an interpretation I such that $(\exists x\ P(x))^v = 1$ and $(\forall x\ P(x))^v = 0$.

Consider the interpretation I below.

- $D = \{1, 2\}$.
- $P^v = \{1\}$.

Let E be an arbitrary environment.

$P(x)^{(I, E[x \mapsto 1])} = 1$ holds since $E[x \mapsto 1](x) = 1 \in P^v$. By the satisfaction rules for $\exists$, $(\exists x\ P(x))^v = 1$.

$P(x)^{(I, E[x \mapsto 2])} = 0$ holds since $E[x \mapsto 2](x) = 2 \notin P^v$. By the satisfaction rules for $\forall$, $(\forall x\ P(x))^v = 0$ holds. □

Exercise 70. *Show that* $\{(\forall x\ (A \to B))\} \vDash ((\forall x\ A) \to (\forall x\ B))$*, where* x *is a variable symbol and* A *and* B *are well-formed predicate formulas.*

Solution:

Proof. Consider an interpretation I and an environment E such that $(\forall x\ (A \to B))^v = 1$. We will prove that $((\forall x\ A) \to (\forall x\ B))^v = 1$.

To show that $((\forall x\ A) \to (\forall x\ B))^v = 1$, we assume that $(\forall x\ A)^v = 1$.

By the satisfaction rule for $\forall$, we have that

$$A^{(I,E[x \mapsto d])} = 1 \text{ for every } d \in D.$$

By our assumption, $(\forall x\ (A \to B))^v = 1$. By the satisfaction rule for $\forall$, we have that

$$(A \to B)^{(I,E[x \mapsto d])} = 1 \text{ for every } d \in D.$$

By the satisfaction rule for an implication, we have that

$$B^{(I,E[x \mapsto d])} = 1 \text{ for every } d \in D.$$

By the satisfaction rule for $\forall$, we have that

$$(\forall x\ B)^v = 1.$$

Thus, the tautological consequence holds. □

Exercise 71. *Show that* $\{((\forall x\ A) \to (\forall x\ B))\} \not\models (\forall x\ (A \to B))$*, where* x *is a variable symbol and* A *and* B *are well-formed predicate formulas.*

Solution:

Remark 14. *The most important step for the proof below is to come up with the concrete example such that the premises are all true and the conclusion is false.*

I first chose concrete formulas for A *and* B*. This step is important. Without doing so, I may not be able to make claims about whether* A *and* B *are true or false under a particular interpretation.*

Next, I construct an interpretation to satisfy the two requirements. I start by picking a domain containing two elements. It is small enough to be manageable and large enough to give me a few possibilities to experiment with.

Then, I try to find definitions for P^v *and* Q^v *to satisfy the two requirements.*

First, I want to make the conclusion $(\forall x\ (P(x) \to Q(x)))$ *false. To do this, it is sufficient to make* P *to be true and* Q *to be false for one value of* x *(so that the implication* $(P(x) \to Q(x))$ *is false). I used* $x = 2$ *for this case and made sure that* $2 \in P^v$ *and* $2 \notin Q^v$*.*

Next, I want to make the premise true. Since $2 \notin Q^v$*, then* $(\forall x\ Q(x))$ *is false. So the conclusion of the premise is false. To make the premise true, I have to make the premise of the premise false. This means that, I need to make sure at least one domain element is not in* P^v*. Therefore, I defined* P^v *such that* $1 \notin P^v$*.*

Proof. Let A be $P(x)$ and let B be $Q(x)$, where P and Q are unary predicates. Consider the following interpretation:

- $D = \{1, 2\}$
- $P^v = \{2\}$ and $Q^v = \{1\}$

We need to show that $((\forall x\ P(x)) \to (\forall x\ Q(x)))^v = 1$ and $(\forall x\ (P(x) \to Q(x)))^v = 0$. Let E be an arbitrary environment.

First, we will show that $((\forall x\ P(x)) \to (\forall x\ Q(x)))^v = 1$.
$P(x)^{(I, E[x \mapsto 1])} = 0$ because $E[x \mapsto 1](x) = 1 \notin P^v$. By the satisfaction rule for ∀, $(\forall x\ P(x))^v = 0$.

By the satisfaction rule for an implication, $((\forall x\ P(x)) \to (\forall x\ Q(x)))^v = 1$ because $(\forall x\ P(x))^v = 0$.

Next, we will show that $(\forall x\ (P(x) \to Q(x)))^v = 0$.
$(P(x) \to Q(x))^{(I, E[x \mapsto 2])} = 0$ because $E[x \mapsto 2](x) = 2 \in P^v$ and $E[x \mapsto 2](x) = 2 \notin Q^v$.
By the satisfaction rule for ∀, $(\forall x\ (P(x) \to Q(x)))^v = 0$.

In summary, the tautological consequence does not hold.

□

Exercise 72. *Show that* $\{(\exists y\ (\forall x\ Q(x,y)))\} \vDash (\forall x\ (\exists y\ Q(x,y)))$.

Solution:

Proof. Consider an interpretation I such that $(\exists y\ (\forall x\ Q(x,y)))^v = 1$. We will prove that $(\forall x\ (\exists y\ Q(x,y)))^v = 1$. Let E be an arbitrary environment.

By the satisfaction rules for $\exists$, we have

$$(\forall x\ Q(x,y))^{(I,E[y \mapsto d_y])} = 1 \text{ for some } d_y \in D.$$

By the satisfaction rules for $\forall$, we have

$$Q(x,y)^{(I,E[y \mapsto d_y][x \mapsto d])} = 1, \text{ for some } d_y \in D \text{ and for every } d \in D.$$

Note that in the environment $E[y \mapsto d_y][x \mapsto d]$, the value of d_y was chosen first and does not depend on the value of d. Thus, the environment $E[y \mapsto d_y][x \mapsto d]$ is equivalent to the environment $E[x \mapsto d][y \mapsto d_y]$. It does not matter whether we chose the value for x or the value for y first. Therefore, we rewrite the formula above as follows.

$$Q(x,y)^{(I,E[x \mapsto d][y \mapsto d_y])} = 1, \text{ for every } d \in D \text{ and for some } d_y \in D.$$

By the satisfaction rule for $\exists$, we have

$$(\exists y\ Q(x,y))^{(I,E[x \mapsto d])} = 1 \text{ for every } d \in D.$$

By the satisfaction rule for $\forall$, we have that

$$(\forall x\ (\exists y\ Q(x,y)))^v = 1.$$

□

Exercise 73. *Show that* $\{(\forall x\ (\exists y\ Q(x,y)))\} \not\models (\exists y\ (\forall x\ Q(x,y)))$.

Solution:

Remark 15. *If I attempt to prove the tautological consequence, what would happen?*

By the satisfaction rules for $\forall$*, we have*

$$(\exists y\ Q(x,y))^{(I,E[x\mapsto d_x])} = 1 \textit{ for every } d_x \in D.$$

By the satisfaction rules for $\exists$*, we have*

$$Q(x,y)^{(I,E[x\mapsto d_x][y\mapsto d_y])} = 1$$

for every $d \in D$ *and for some* $d_y \in D$ *where the value of* d_y *may depend on the value of* d_x*. Note that the value of* d_y *may depend on the value of* d_x*. In other words, for every value of* d_x*, we may choose a different value of* d_y *to satisfy the formula. Therefore, we CANNOT switch the two overrides in the environment. The following formula is FALSE.*

$$\textit{A false formula: } Q(x,y)^{(I,E[y\mapsto d_y][x\mapsto d_x])} = 1$$

for some $d_y \in D$ *and for every* $d_x \in D$*.*

Proof. To prove that the tautological consequence does not hold, we need to find an interpretation I such that $(\forall x\ (\exists y\ Q(x,y)))^v = 1$ and $(\exists y\ (\forall x\ Q(x,y)))^v = 0$.

Consider the interpretation I below.

- $D = \{1,2\}$.
- $Q^v = \{\langle 1,1\rangle, \langle 2,2\rangle\}$.

First, we will show that $(\forall x\ (\exists y\ Q(x,y)))^v = 1$. Let E be an arbitrary environment. Consider all possible values of x.

- $[x\mapsto 1]$: $Q(x,y)^{(I,E[x\mapsto 1][y\mapsto 1])} = 1$ because

  $$\langle E[x\mapsto 1][y\mapsto 1](x), E[x\mapsto 1][y\mapsto 1](y)\rangle = \langle 1,1\rangle \in Q^v.$$

  By the satisfaction rule for $\exists$, $(\exists y\ Q(x,y))^{(I,E[x\mapsto 1])} = 1$.

- $[x\mapsto 2]$: $Q(x,y)^{(I,E[x\mapsto 2][y\mapsto 2])} = 1$ because

  $$\langle E[x\mapsto 2][y\mapsto 2](x), E[x\mapsto 2][y\mapsto 2](y)\rangle = \langle 2,2\rangle \in Q^v.$$

  By the satisfaction rule for $\exists$, $(\exists y\ Q(x,y))^{(I,E[x\mapsto 2])} = 1$.

Thus, by the satisfaction rule for ∀, $(\forall x\ (\exists y\ Q(x, y)))^v = 1$.

Next, we will show that $(\exists y\ (\forall x\ Q(x, y)))^v = 0$. Let E be an arbitrary environment. Consider all possible values of y.

- $[y \mapsto 1]$: $Q(x, y)^{(I, E[x \mapsto 2][y \mapsto 1])} = 0$ because
$$\langle E[x \mapsto 2][y \mapsto 1](x), E[x \mapsto 2][y \mapsto 1](y)\rangle = \langle 2, 1\rangle \notin Q^v.$$
By the satisfaction rule for ∃, $(\forall x\ Q(x, y))^{(I, E[y \mapsto 1])} = 0$.

- $[y \mapsto 2]$: $Q(x, y)^{(I, E[x \mapsto 1][y \mapsto 2])} = 0$ because
$$\langle E[x \mapsto 1][y \mapsto 2](x), E[x \mapsto 1][y \mapsto 2](y)\rangle = \langle 1, 2\rangle \notin Q^v.$$
By the satisfaction rule for ∀, $(\forall x\ Q(x, y))^{(I, E[y \mapsto 2])} = 0$.

Thus, by the satisfaction rule for ∀, $(\exists y\ (\forall x\ Q(x, y)))^v = 0$.

Hence, the tautological consequence does not hold. □

Exercise 74. *Show that* $\{(\forall x\ (\exists y\ (P(x) \lor Q(y))))\} \vDash (\exists y\ (\forall x\ (P(x) \lor Q(y))))$.

Remark 16. *Wait a second! In exercise 73, didn't we just show that this tautological consequence does NOT hold? Not quite. In exercise 73, we dealt with a generic predicate formula* $Q(x, y)$ *without knowing any additional information about the predicate. In this question, we are working with a much more concrete predicate formula* $(P(x) \lor Q(y))$*. It turns out that, having this concrete predicate formula allows us to prove the tautological consequence.*

Remark 17. *Let's write out a proof sketch first.*

To prove that the conclusion is true, we need to find one value $d_y \in D$ *for* y *such that* $(P(x) \lor Q(y))$ *is true for every possible value for* x*. The value of* y *only influences the* $Q(y)$ *part of the formula. Does there exist a value for* y *such that* $Q(y)$ *is true?*

Let's suppose that we know that there is some $d_y \in D$ *for* y *such that* $Q(y)$ *is true. Would this help us prove the conclusion? For sure. If* $Q(y)$ *is true for* $y = d_y$*, then* $(P(x) \lor Q(y))$ *must be true for* $y = d_y$ *regardless of the value of* x*. We just found a value for* y *which will make the conclusion true.*

We know how to prove the conclusion for the case when $Q(y)$ *for at least one value of* y*. What if* $Q(y)$ *is always false? Let's look at the premise. If* $Q(y)$ *is always false, for the premise to be true,* $P(x)$ *must be true for every possible value of* x*. If* $P(x)$ *is true for every possible value of* x*, then to prove that the conclusion is true, we could choose any value for* y*. For any value of* y*,* $P(x)$ *is true for any value of* x*, so* $(P(x) \lor Q(y))$ *must be true.*

2.3.1 Semantic Entailment - Additional Exercises

Exercise 75. $\{((\forall x\ P(x)) \vee (\forall x\ Q(x)))\} \vDash (\forall x\,(P(x) \vee Q(x)))$.

Exercise 76. $\{(\exists x\,(P(x) \to Q(x))), (\forall y\ P(y))\} \vDash (\exists x\ Q(x))$

Exercise 77. $\{((\exists x\ P(x)) \vee (\exists x\ Q(x)))\} \vDash (\exists x\,(P(x) \vee Q(x)))$.

2.4 Formal Deduction

$\forall$-introduction ($\forall+$)

if $\Sigma \vdash A(u)$, u not occurring in Σ,
then $\Sigma \vdash \forall x\, A(x)$.

$\forall$-elimination ($\forall-$)

if $\Sigma \vdash \forall x\, A(x)$,
then $\Sigma \vdash A(t)$.

Comments:

- $\forall-$ is analogous to $\wedge-$.
- $\forall+$ is analogous to $\wedge+$.

  Intuitively, this rule means that: from "any member u of the set has a certain property" we can deduce that "every member of the set has this property". The arbitrariness of u means that the choice of u is independent of the premises in Σ. This point is expressed by "u not occurring in Σ".

  We know nothing about u except that u is a domain element. If u is special, our conclusion may not be valid.

$\exists$-introduction ($\exists+$)

if $\Sigma \vdash A(t)$,
then $\Sigma \vdash \exists x\, A(x)$.

where $A(x)$ results by replacing some (not necessarily all) occurrences of t in $A(t)$ by x.

$\exists$-elimination ($\exists-$)

if $\Sigma, A(u) \vdash B, u$ not occurring in Σ or B,
then $\Sigma, \exists x\, A(x) \vdash B$.

Comments:

- $\exists-$ is analogous to $\vee-$.
  - Proof by cases.
  - The conclusion may have nothing to do with the starting formula.
- $\exists+$ is analogous to $\vee+$.

2.4.1 Forall-elimination

Exercise 78. *Show that* $\{P(u), \forall x\ (P(x) \rightarrow (\neg Q(x)))\} \vdash (\neg Q(u))$.

Solution:

$$\begin{array}{lll}
(1) & P(u), \forall x\ (P(x) \rightarrow (\neg Q(x))) \vdash (\forall x\ (P(x) \rightarrow (\neg Q(x)))) & \text{by } ((\in)) \\
(2) & P(u), \forall x\ (P(x) \rightarrow (\neg Q(x))) \vdash P(u) & \text{by } ((\in)) \\
(3) & P(u), \forall x\ (P(x) \rightarrow (\neg Q(x))) \vdash P(u) \rightarrow \neg Q(u) & \text{by } ((\forall -), (1)) \\
(4) & P(u), \forall x\ (P(x) \rightarrow (\neg Q(x))) \vdash \neg Q(u) & \text{by } ((\rightarrow -), (2), (3))
\end{array}$$

2.4.2 Exists-introduction

Exercise 79. *Show that* $\{(\neg P(v))\} \vdash (\exists x\ (P(x) \rightarrow Q(v)))$.

Solution:

$$\begin{array}{lrl}
(1) & (\neg P(v)), P(v), \neg Q(v) \vdash P(v) & \text{by } (\in) \\
(2) & (\neg P(v)), P(v), \neg Q(v) \vdash \neg P(v) & \text{by } (+, 1) \\
(3) & (\neg P(v)), P(v) \vdash Q(v) & \text{by } (\neg -, 1, 2) \\
(4) & (\neg P(v)) \vdash (P(v) \rightarrow Q(v)) & \text{by } (\rightarrow +, 3) \\
(5) & (\neg P(v)) \vdash (\exists x\ (P(x) \rightarrow Q(v))) & \text{by } (\exists +, 4)
\end{array}$$

Exercise 80. *Show that* $\{(\forall x\ P(x))\} \vdash (\exists y\ P(y))$.

Solution:

$$\begin{array}{lll}
(1) & (\forall x\ P(x)) \vdash (\forall x\ P(x)) & \text{by } (\in) \\
(2) & (\forall x\ P(x)) \vdash P(u) & \text{by } (\forall -, 1) \\
(3) & (\forall x\ P(x)) \vdash (\exists y\ P(y)) & \text{by } (\exists +, 2)
\end{array}$$

2.4.3 Forall-introduction

Exercise 81. *Show that* $\{(\forall x\ P(x))\} \vdash (\forall y\ P(y))$.

Solution:

$$\begin{array}{lll}
(1) & (\forall x\ P(x)) \vdash (\forall x\ P(x)) & \text{by } (\in) \\
(2) & (\forall x\ P(x)) \vdash P(u) & \text{by } (\forall -, 1) \\
(3) & (\forall x\ P(x)) \vdash (\forall y\ P(y)) & \text{by } (\forall +, 2)
\end{array}$$

Exercise 82. *Show that* $(\forall x\ (P(x) \to Q(x))) \vdash ((\forall x\ P(x)) \to (\forall y\ Q(y)))$.

Solution:

$$\begin{array}{lrl}
(1) & (\forall x\ (P(x) \to Q(x))), (\forall x\ P(x)) \vdash (\forall x\ P(x)) & \text{by } (\in) \\
(2) & (\forall x\ (P(x) \to Q(x))), (\forall x\ P(x)) \vdash (\forall x\ (P(x) \to Q(x))) & \text{by } (\in) \\
(3) & (\forall x\ (P(x) \to Q(x))), (\forall x\ P(x)) \vdash P(u) & \text{by } (\forall -, 1) \\
(4) & (\forall x\ (P(x) \to Q(x))), (\forall x\ P(x)) \vdash P(u) \to Q(u) & \text{by } (\forall -, 2) \\
(5) & (\forall x\ (P(x) \to Q(x))), (\forall x\ P(x)) \vdash Q(u) & \text{by } (\to -, 3, 4) \\
(6) & (\forall x\ (P(x) \to Q(x))), (\forall x\ P(x)) \vdash (\forall y\ Q(y)) & \text{by } (\forall +, 5) \\
(7) & (\forall x\ (P(x) \to Q(x))) \vdash ((\forall x\ P(x)) \to (\forall y\ Q(y))) & \text{by } (\to +, 6)
\end{array}$$

2.4.4 Forall-introduction - Additional Exercises

Exercise 83. $\{(\forall x\,(\forall y\; P(x,y)))\} \vdash (\forall y\,(\forall x\; P(x,y)))$.

Exercise 84. $\{(\forall x\,((\neg P(x)) \wedge Q(x)))\} \vdash (\forall x\,(P(x) \to Q(x)))$.

Exercise 85. $\{(\forall x\,(P(x) \wedge Q(x)))\} \vdash (\forall x\,(P(x) \to Q(x)))$.

Exercise 86. $\{(\forall x\,(P(x) \wedge Q(x)))\} \vdash ((\forall x\; P(x)) \wedge (\forall x\; Q(x)))$.

Exercise 87. $\{((\forall x\; P(x)) \vee (\forall x\; Q(x)))\} \vdash (\forall x\,(P(x) \vee Q(x)))$.

Exercise 88. $\{(\forall x\,(P(x) \to Q(x)))\} \vdash ((\forall x\,(\neg Q(x))) \to (\forall x\,(\neg P(x))))$.

Exercise 89. $\{(\forall x\,(\forall y\,(R(x,y) \to R(y,x))))\} \vdash (\forall x\,(\forall y\,(R(y,x) \to R(x,y))))$.

Exercise 90. $\{(\forall x\,(\forall y\,(\forall z\,((R(x,y) \wedge R(y,z)) \to R(x,z))))), (\forall x\,(\neg R(x,x)))\}$
$\vdash (\forall x\,(\forall y\,(\forall z\,(\neg((R(x,y) \wedge R(y,z)) \wedge R(z,x))))))$.

Exercise 91. $\{(\forall x\,(\forall y\,(\forall z\,((R(x,y) \wedge R(x,z)) \to R(y,z))))), (\forall x\; R(x,x))\}$
$\vdash (\forall x\,(\forall y\,(\forall z\,((R(x,y) \wedge R(y,z)) \to R(x,z)))))$.

2.4.5 Exists-elimination

Exercise 92. $(\exists x\ P(x)) \vdash (\exists y\ P(y))$.

Solution:

(1)	$P(u) \vdash P(u)$	by $(\in)$
(2)	$P(u) \vdash (\exists y\ P(y))$	by $((\exists+), (1))$
(3)	$(\exists x\ P(x)) \vdash (\exists y\ P(y))$	by $((\exists-), (2))$

Exercise 93. $\exists x\ (P(x) \wedge Q(x)) \vdash (\exists x\ P(x) \wedge (\exists x\ Q(x))$.

Solution:

(1)	$P(u) \vdash P(u)$	by $((\in))$
(2)	$P(u) \vdash (\exists x\, P(x))$	by $((\exists+), (1))$
(3)	$Q(u) \vdash Q(u)$	by $((\in))$
(4)	$Q(u) \vdash (\exists x\, Q(x))$	by $((\exists+), (3))$
(5)	$P(u) \vdash (\exists x\, P(x)) \vee (\exists x\, Q(x))$	by $((\vee+), (2))$
(6)	$Q(u) \vdash (\exists x\, P(x)) \vee (\exists x\, Q(x))$	by $((\vee+), (4))$
(7)	$P(u) \vee Q(u) \vdash (\exists x\, P(x)) \vee (\exists x\, Q(x))$	by $((\vee-), (5), (6))$
(8)	$\exists x(P(x) \vee Q(x)) \vdash (\exists x\, P(x)) \vee (\exists x\, Q(x))$	by $((\exists-), (7))$

Exercise 94. $((\exists x\ P(x)) \vee (\exists x\ Q(x))) \vdash (\exists x\, (P(x) \vee Q(x)))$.

Exercise 95. *Show that* $(\forall x\ (P(x) \to Q(x))), (\exists x\ P(x)) \vdash (\exists x\ Q(x))$.

Solution:

(1)	$(\forall x\ (P(x) \to Q(x))), P(u) \vdash (\forall x\ (P(x) \to Q(x)))$	by $(\in)$
(2)	$(\forall x\ (P(x) \to Q(x))), P(u) \vdash P(u)$	by $(\in)$
(3)	$(\forall x\ (P(x) \to Q(x))), P(u) \vdash P(u) \to Q(u)$	by $(\forall -, 1)$
(4)	$(\forall x\ (P(x) \to Q(x))), P(u) \vdash Q(u)$	by $(\to -, 2, 3)$
(5)	$(\forall x\ (P(x) \to Q(x))), P(u) \vdash (\exists x\ Q(x))$	by $(\exists +, 4)$
(6)	$(\forall x\ (P(x) \to Q(x))), (\exists x\ P(x)) \vdash (\exists x\ Q(x))$	by $(\exists -, 2)$

Exercise 96. *Show that* $(\forall x\ (Q(x) \to R(x))), (\exists x\ (P(x) \land Q(x))) \vdash (\exists x\ (P(x) \land R(x)))$.

Solution:

1.	$(\forall x\ (Q(x) \to R(x)))$	premise
2.	$(\exists x\ (P(x) \land Q(x)))$	premise
3.	$(P(u) \land Q(u))$, u fresh	assumption
4.	$P(u)$	$\land$e: 3
5.	$Q(u)$	$\land$e: 3
6.	$(Q(u) \to R(u))$	$\forall$e: 1
7.	$R(u)$	$\to$e: 5, 6
8.	$(P(u) \land R(u))$	$\land$i: 4, 7
9.	$(\exists x\ (P(x) \land R(x)))$	$\exists$i: 8
10.	$(\exists x\ (P(x) \land R(x)))$	$\exists$e: 2, 3-9

2.4.6 Exists-Elimination - Additional Exercises

Exercise 97. $\{(\exists x\,(P(x) \rightarrow Q(x))), (\forall y\ P(y))\} \vdash (\exists x\ Q(x))$

Exercise 98. $\{(\exists x\,(\exists y\ P(x, y)))\} \vdash (\exists y\,(\exists x\ P(x, y)))$.

Exercise 99. $\{(\exists x\,((\neg P(x)) \wedge (\neg Q(x))))\} \vdash (\exists x\,(\neg(P(x) \wedge Q(x))))$.

Exercise 100. $\{(\exists x\,((\neg P(x)) \vee Q(x)))\} \vdash (\exists x\,(\neg(P(x) \wedge (\neg Q(x)))))$.

2.4.7 Putting them together

Exercise 101. *Show that* $(\exists y\ (\forall x\ P(x,y))) \vdash (\forall x\ (\exists y\ P(x,y)))$.

Solution: There are two different solutions, depending whether we apply $\forall+$ last or apply $\exists-$ last.
Applying $\exists-$ last:

$$\begin{array}{lrll}
(1) & (\forall x\ P(x,v)) & \vdash (\forall x\ P(x,v)) & \text{by } (\in) \\
(2) & (\forall x\ P(x,v)) & \vdash P(u,v) & \text{by } (\forall-, 1) \\
(3) & (\forall x\ P(x,v)) & \vdash (\exists y\ P(u,y)) & \text{by } (\exists+, 2) \\
(4) & (\forall x\ P(x,v)) & \vdash (\forall x\ (\exists y\ P(x,y))) & \text{by } (\forall+, 3) \\
(5) & (\exists y\ (\forall x\ P(x,y))) & \vdash (\forall x\ (\exists y\ P(x,y))) & \text{by } (\exists-, 4)
\end{array}$$

Applying $\forall+$ last:

$$\begin{array}{lrll}
(1) & (\forall x\ P(x,v)) & \vdash (\forall x\ P(x,v)) & \text{by } (\in) \\
(2) & (\forall x\ P(x,v)) & \vdash P(u,v) & \text{by } (\forall-, 1) \\
(3) & (\forall x\ P(x,v)) & \vdash (\exists y\ P(u,y)) & \text{by } (\exists+, 2) \\
(4) & (\exists y\ (\forall x\ P(x,y))) & \vdash (\exists y\ P(u,y)) & \text{by } (\exists-, 3) \\
(5) & (\exists y\ (\forall x\ P(x,y))) & \vdash (\forall x\ (\exists y\ P(x,y))) & \text{by } (\forall+, 4)
\end{array}$$

Exercise 102. *Show that* $\{(\exists x\ P(x)), (\forall x\ (\forall y\ (P(x) \to Q(y))))\} \vdash (\forall y\ Q(y))$.

Solution: There are two different solutions, depending whether we apply $\forall+$ last or apply $\exists-$ last.

$$\begin{array}{lrll}
(1) & P(u), (\forall x\ (\forall y\ (P(x) \to Q(y)))) & \vdash (\forall x\ (\forall y\ (P(x) \to Q(y)))) & \text{by } (\in) \\
(2) & P(u), (\forall x\ (\forall y\ (P(x) \to Q(y)))) & \vdash (\forall y\ (P(u) \to Q(y))) & \text{by } (\forall-, 1) \\
(3) & P(u), (\forall x\ (\forall y\ (P(x) \to Q(y)))) & \vdash (P(u) \to Q(v)) & \text{by } (\forall-, 2) \\
(4) & P(u), (\forall x\ (\forall y\ (P(x) \to Q(y)))) & \vdash P(u) & \text{by } (\in) \\
(5) & P(u), (\forall x\ (\forall y\ (P(x) \to Q(y)))) & \vdash Q(v) & \text{by } (\to -, 3, 4) \\
(6) & (\exists x\ P(x)), (\forall x\ (\forall y\ (P(x) \to Q(y)))) & \vdash Q(v) & \text{by } (\exists-, 5) \\
(7) & (\exists x\ P(x)), (\forall x\ (\forall y\ (P(x) \to Q(y)))) & \vdash (\forall y\ Q(y)) & \text{by } (\forall+, 6)
\end{array}$$

$$\begin{array}{lrll}
(1) & P(u), (\forall x\ (\forall y\ (P(x) \to Q(y)))) & \vdash (\forall x\ (\forall y\ (P(x) \to Q(y)))) & \text{by } (\in) \\
(2) & P(u), (\forall x\ (\forall y\ (P(x) \to Q(y)))) & \vdash (\forall y\ (P(u) \to Q(y))) & \text{by } (\forall-, 1) \\
(3) & P(u), (\forall x\ (\forall y\ (P(x) \to Q(y)))) & \vdash (P(u) \to Q(v)) & \text{by } (\forall-, 2) \\
(4) & P(u), (\forall x\ (\forall y\ (P(x) \to Q(y)))) & \vdash P(u) & \text{by } (\in) \\
(5) & P(u), (\forall x\ (\forall y\ (P(x) \to Q(y)))) & \vdash Q(v) & \text{by } (\to -, 3, 4) \\
(6) & P(u), (\forall x\ (\forall y\ (P(x) \to Q(y)))) & \vdash (\forall y\ Q(y)) & \text{by } (\forall+, 5) \\
(7) & (\exists x\ P(x)), (\forall x\ (\forall y\ (P(x) \to Q(y)))) & \vdash (\forall y\ Q(y)) & \text{by } (\exists-, 6)
\end{array}$$

Exercise 103. *Show that* $\{(\neg(\exists x\ P(x)))\} \vdash (\forall x\ (\neg P(x)))$. *(De Morgan)*

Solution:

$$\begin{array}{lcl}
(1) & (\neg(\exists x\ P(x))), P(u) \vdash P(u) & \text{by } (\in) \\
(2) & (\neg(\exists x\ P(x))), P(u) \vdash (\exists x\ P(x)) & \text{by } (\exists+, 1) \\
(3) & (\neg(\exists x\ P(x))), P(u) \vdash (\neg(\exists x\ P(x))) & \text{by } (\in) \\
(4) & (\neg(\exists x\ P(x))) \vdash (\neg P(u)) & \text{by } (\neg+, 2, 3) \\
(5) & (\neg(\exists x\ P(x))) \vdash (\forall x\ (\neg P(x))) & \text{by } (\forall+, 4)
\end{array}$$

Exercise 104. *Show that* $\{(\forall x\ (\neg P(x)))\} \vdash (\neg(\exists x\ P(x)))$. *(De Morgan)*

Solution:

$$\begin{array}{lcl}
(1) & (\forall x\ (\neg P(x))), P(u), \neg Q(v) \vdash (\forall x\ (\neg P(x))) & \text{by } (\in) \\
(2) & (\forall x\ (\neg P(x))), P(u), \neg Q(v) \vdash \neg P(u) & \text{by } (\forall-, 1) \\
(3) & (\forall x\ (\neg P(x))), P(u), \neg Q(v) \vdash P(u) & \text{by } (\in) \\
(4) & (\forall x\ (\neg P(x))), P(u) \vdash Q(v) & \text{by } (\neg-, 2, 3) \\
(5) & (\forall x\ (\neg P(x))), (\exists x\ P(x)) \vdash Q(v) & \text{by } (\exists-, 4) \\
(6) & (\forall x\ (\neg P(x))), P(u), Q(v) \vdash (\forall x\ (\neg P(x))) & \text{by } (\in) \\
(7) & (\forall x\ (\neg P(x))), P(u), Q(v) \vdash \neg P(u) & \text{by } (\forall-, 6) \\
(8) & (\forall x\ (\neg P(x))), P(u), Q(v) \vdash P(u) & \text{by } (\in) \\
(9) & (\forall x\ (\neg P(x))), P(u) \vdash \neg Q(v) & \text{by } (\neg+, 7, 8) \\
(10) & (\forall x\ (\neg P(x))), (\exists x\ P(x)) \vdash \neg Q(v) & \text{by } (\exists-, 9) \\
(11) & (\forall x\ (\neg P(x))) \vdash (\neg(\exists x\ P(x))) & \text{by } (\neg+, 5, 10)
\end{array}$$

Exercise 105. *Show that* $\{(\exists x\ (\neg P(x)))\} \vdash (\neg(\forall x\ P(x)))$. *(De Morgan)*

Solution:

1.	$(\exists x\ (\neg P(x)))$	premise
2.	$(\forall x\ P(x))$	assumption
3.	$(\neg P(u))$, u fresh	assumption
4.	$P(u)$	$\forall$e: 2
5.	$\bot$	$\bot$i: 3, 4
6.	$\bot$	$\exists$e: 1, 3-5
7.	$(\neg(\forall x\ P(x)))$	$\neg$i: 2-6

Exercise 106. *Show that* $\{(\neg(\forall x\ P(x)))\} \vdash (\exists x\ (\neg P(x)))$. *(De Morgan)*

Solution:

1.	$(\neg(\forall x\ P(x)))$	premise
2.	$(\neg(\exists x\ (\neg P(x))))$	assumption
3.	u fresh	assumption
4.	$(\neg P(u))$	assumption
5.	$(\exists x\ (\neg P(x)))$	$\exists$i: 4
6.	$\bot$	2, 5
7.	$P(u)$	PBC: 4-6
8.	$(\forall x\ P(x))$	$\forall$i: 3-7
9.	$\bot$	$\bot$i: 1, 8
10.	$(\exists x\ (\neg P(x)))$	PBC: 2-9

2.4.8 Putting them together - Additional Exercises

Exercise 107. $\{(\forall x\,(P(x) \to (\neg Q(x))))\} \vdash (\neg(\exists x\,(P(x) \wedge Q(x))))$.

Exercise 108. $\{(\forall x\,(P(x) \vee Q(x)))\} \vdash ((\forall x\ P(x)) \vee (\exists x\ Q(x)))$.

Exercise 109. $\{(\forall x\,(P(x) \to (Q(x) \vee R(x)))), (\neg(\exists x\,(P(x) \wedge R(x))))\} \vdash (\forall x\,(P(x) \to Q(x)))$.

Exercise 110. $\{(\exists x\,(P(x) \wedge Q(x))), (\forall x\,(P(x) \to R(x)))\} \vdash (\exists x\,(R(x) \wedge Q(x)))$.

Exercise 111. $\{(\exists x\,(\exists y\,(S(x,y) \vee S(y,x))))\} \vdash (\exists x\,(\exists y\ S(x,y)))$.

Exercise 112. $\{(\forall x\,(\exists y\ R(x,y)))\} \vdash (\neg(\forall x\ R(x,x)))$.
This is false. Can you prove it?

Exercise 113. $\{(\forall x\,(\exists y\ R(x,y)))\} \vdash (\forall x\,(\exists y\,(\exists z\,(R(x,y) \wedge R(x,z)))))$.

Exercise 114. $\{(\forall x\,(P(x) \vee Q(x))), (\exists x\,(\neg Q(x))), (\forall x\,(R(x) \to (\neg P(x))))\} \vdash (\exists x\,(\neg R(x)))$.

Exercise 115. $\emptyset \vdash (\exists y\,(R(y) \to (\forall x\ R(x))))$.

Exercise 116. $\{(\forall x\,(\exists y\,(P(x) \vee Q(y))))\} \vdash (\exists y\,(\forall x\,(P(x) \vee Q(y))))$.

Exercise 117. $\{(\forall x\,((\exists y\ P(y)) \to Q(x)))\} \vdash (\forall x\,(\exists y\,(P(y) \to Q(x))))$.

Exercise 118. $\{(\forall x\,(P(x,x) \vee (\forall y\ Q(x,y))))\} \vdash (\forall x\,((\exists y\ P(x,y)) \vee Q(x,x)))$.

Exercise 119. $\vdash ((\forall x\,(\exists y\ R(x,y))) \vee (\neg(\forall x\ R(x,x))))$.

2.5 Soundness and Completeness of Natural Deduction

2.5.1 Proving that an inference rule is sound or not sound

Lemma 1. *Let t be a predicate term. Let I be an interpretation with domain D. Let E be an environment. Then we have that*

$$t^v \in D.$$

Lemma 2. *Let A be a well-formed predicate formula. Let t be a predicate term. Let I and E be an interpretation and environment. Let x be a variable. Then we have that*

$$A[t/x]^v = A^{(I, E[x \mapsto t^v])}.$$

Exercise 120. *Prove that the $\forall e$ inference rule is sound. That is, prove that the tautological consequence holds:*

$$\{(\forall x\ A)\} \vDash A[t/x] \tag{125}$$

where A be a Predicate formula, x is a variable, and t is a Predicate term.

The proof sketch below is like an outline or a master plan. I will lay down the plan first. Then I will fill in the missing details.

Proof Sketch. Consider an interpretation and environment (I, E) such that $(\forall x\ A)^v = 1$. We need to show that $A[t/x]^v = 1$.

$(\forall x\ A)^v = 1$ holds because ...

$A^{(I, E[x \mapsto t^v])} = 1$ holds because ...

$A[t/x]^v = 1$ holds because ...

Thus, the tautological consequence holds and the inference rule is sound. □

Solution: Let (I, E) be an interpretation and environment such that $(\forall x\ A)^v = 1$.

By the satisfaction rule for $\forall$, we have that $A^{(I, E[x \mapsto d])} = 1$, for every $d \in D$.

By Lemma 1, t^v is some domain element. Thus, we have that $A^{(I, E[x \mapsto t^v])} = 1$.

By Lemma 2, we have that $A[t/x]^v = A^{(I, E[x \mapsto t^v])}$. Thus, we have that $A[t/x]^v = 1$.

Exercise 121. *Prove that the $\exists i$ inference rule is sound. That is, prove that the tautological consequence holds:*

$$\{A[t/x]\} \models (\exists x\ A) \tag{126}$$

where A is a predicate formula, t is a predicate term, and x is a variable.

Proof Sketch. Consider an interpretation and environment (I, E) such that $A[t/x]^v = 1$. We need to show that $(\exists x\ A)^v = 1$.

$A[t/x]^v = 1$ holds because ...

$A^{(I, E[x \mapsto t^v])} = 1$ holds because ...

$(\exists x\ A)^v = 1$ holds because ...

Thus, the tautological consequence holds and the inference rule is sound. □

Solution: Let (I, E) be an interpretation and environment such that $A[t/x]^v = 1$.

By Lemma 2, we have that $A[t/x]^v = A^{(I, E[x \mapsto t^v])}$. Thus, we have that $A^{(I, E[x \mapsto t^v])} = 1$.

By Lemma 1, t^v is some domain element. Thus, by the satisfaction rule for $\exists$, we have that $(\exists x\ A)^v = 1$.

Exercise 122. *Prove that the following inference rule is NOT sound.*

$$\frac{A[t/x]}{(\forall x\ A)}\ \forall i* \tag{127}$$

where A is a predicate formula, t is a predicate term, and x is a variable.

Proof Sketch. Define the symbols in the language of Predicate logic that we consider.

Choose A to be a concrete Predicate formula. Choose t to be a concrete Predicate term.

Define an interpretation and an environment (I, E).

Show that $A[t/x]^v = 1$.

Show that $(\forall x\ A)^v = 0$. □

Solution:

Remark 18. *How did I come up with the interpretation and the environment below? Given the definition of D, E, and A and t, we can simplify the premise and the conclusion.*

The premise becomes $A[t/x] = P(x)[y/x] = P(y)$.

The conclusion becomes $(\forall x\ P(x))$.

To make the premise true, we need to define $E(y)$ and P^v such that $P(y)$ is true. If we choose $E(y) = 1$, then we need $1 \in P^v$. If we choose $E(y) = 2$, then we need $2 \in P^v$. In the solution below, I chose $E(y) = 1$ and $1 \in P^v$.

To make the conclusion false, we need to make sure that $P(x)$ is false for one element of the domain. By the above definition, we already know that $P(x)$ is true when x is 1. The only other element of the domain is 2. So we need to make sure that $P(x)$ is false when x is 2, which means that $2 \notin P^v$.

Solution Text:

We need to provide an interpretation I and an environment E such that $A[t/x]^v = 1$ and $(\forall x\ A)^v = 0$.

Consider the language of predicate logic where $P^{(1)}$ is a unary predicate and x and y are variables.

Let A be $P(x)$ and let t be y. Let the interpretation I be defined below.

- $D = \{1, 2\}$
- $P^v = \{1\}$

Let the environment E be defined by $E(x) = 1$ and $E(y) = 1$.

First, we show that $A[t/x]^v = 1$. By Lemma 2, $A[t/x]^v = A^{(I, E[x \mapsto t^v])}$. By the definition of the term t, $t^v = y^v = E(y) = 1$. Thus, $A[t/x]^v = A^{(I, E[x \mapsto 1])} = P(x)^{(I, E[x \mapsto 1])} = 1$ because $E[x \mapsto 1](x) = 1 \in P^v$.

Next, we show that $(\forall x\ A)^v = 0$. By the satisfaction rule for $\forall$, we need to show that $A^{(I, E[x \mapsto d])} = 0$ for at least one $d \in D$. We have that $A^{(I, E[x \mapsto 2])} = P(x)^{(I, E[x \mapsto 2])} = 0$ because $E[x \mapsto 2](x) = 2 \notin P^v$.

Exercise 123. *Prove that the following inference rule is NOT sound.*

$$\frac{(\exists x\ A)}{A[t/x]}\ \exists e* \tag{128}$$

where A is a predicate formula, t is a predicate term, and x is a variable.

Proof Sketch. Define the symbols in the language of Predicate logic that we consider.

Choose A to be a concrete Predicate formula. Choose t to be a concrete Predicate term.

Define an interpretation and an environment (I, E).

Show that $(\exists x\ A)^v = 1$.

Show that $A[t/x]^v = 0$. □

Solution: We need to provide an interpretation I and an environment E such that $(\exists x\ A)^v = 1$ and $A[t/x]^v = 0$.

Consider the language of predicate logic where $P^{(1)}$ is a unary predicate and x and y are variables.

Let A be $P(x)$ and let t be y. Let the interpretation I be defined below.

- $D = \{1, 2\}$
- $P^v = \{1\}$

Let the environment E be defined by $E(x) = 1$ and $E(y) = 2$.

First, we show that $(\exists x\ A)^v = 1$.
By the definition of P^v, we have that

$$A^{(I, E[x \mapsto 1])} = 1$$

because $E[x \mapsto 1](x) = 1 \in P^v$.
By the satisfaction rule for $\exists$, we have that

$$(\exists x\ A)^v = 1.$$

Second, we show that $A[t/x]^v = 0$.
By Lemma 2, we have that

$$A[t/x]^v = A^{(I, E[x \mapsto t^v])}.$$

We need to prove that

$$A^{(I, E[x \mapsto t^v])} = 0.$$

By Lemma 1, t^v is a domain element. By the definitions of t, I, and E, we have that

$$t^v = y^v = E(y) = 2.$$

By the definition of P^v, we have that

$$A^{(I,E[x \mapsto t^v])} = A^{(I,E[x \mapsto 2])} = 0$$

because $E[x \mapsto 2](x) = 2 \notin P^v$.
Therefore, we have that $A^{(I,E[x \mapsto t^v])} = 0$.
The tautological consequence does not hold and the inference rule is not sound.

2.5.2 Additional Exercises

Exercise 124. *Prove that the following inference rule is sound.*

$$\frac{(\forall x(A \to B)) \quad A[t/x]}{B[t/x]}\ \forall e1 \tag{129}$$

where A and B are predicate formulas, t is a predicate term, and x is a variable.

Exercise 125. *Prove that the following inference rule is sound.*

$$\frac{(\forall x(A \to B)) \quad (\neg B[t/x])}{(\neg A[t/x])}\ \forall e2 \tag{130}$$

where A and B are predicate formulas, t is a predicate term, and x is a variable.

Exercise 126. *Prove that the following inference rule is NOT sound.*

$$\frac{(\forall x(A \to B)) \quad B[t/x]}{A[t/x]}\ \forall e3 \tag{131}$$

where A and B are predicate formulas, t is a predicate term, and x is a variable.

Exercise 127. *Prove that the following inference rule is NOT sound.*

$$\frac{(\forall x(A \to B)) \quad (\neg A[t/x])}{(\neg B[t/x])}\ \forall e4 \tag{132}$$

where A and B are predicate formulas, t is a predicate term, and x is a variable.

2.5.3 Proofs using the soundness and completeness theorems

Exercise 128. *Let Σ be a set of Predicate formulas and let A be a Predicate formula. If $\Sigma \cup \{(\neg A)\}$ is unsatisfiable, then $\Sigma \vdash A$.*

Proof Sketch. Assume that $\Sigma \cup \{(\neg A)\}$ is unsatisfiable. This means that, for any interpretation and environment (I, E), at least one formula in $\Sigma \cup \{(\neg A)\}$ is false.

Prove that $\Sigma \vDash A$. Consider an interpretation and environment (I, E). Assume that every formula in Σ is true under (I, E). Prove that A is true under (I, E).

We have $\Sigma \vdash A$ by the completeness of Natural Deduction. □

Solution:

Remark 19. *What does it mean for a set of formula Σ to be unsatisfiable?*

- *It means that "for every (I, E), at least one formula in Σ is false."*

  Example 1: The set $\{P(x), (\neg P(x))\}$ is unsatisfiable. Under any (I, E), if $P(x)$ is true, then $(\neg P(x))$ must be false. If $(\neg P(x))$ is true, then $P(x)$ must be false.

- *It DOES NOT mean that " for every (I, E), at least one formula in Σ is a contradiction."*

  Example 2: The set $\{(P(x) \wedge (\neg P(x)))\}$ is unsatisfiable. Under any (I, E), $(P(x) \wedge (\neg P(x)))$ is always false. Note that this is only one type of unsatisfiable set.

- *It DOES NOT mean that "for one pair (I, E), at least one formula in Σ is false."*

When proving the tautological consequence $\Sigma \vDash A$, why do we only consider the cases when every formula in Σ is true?

By the definition of tautological consequence, we only need to verify that A is true in the case when every formula in Σ is true under an (I, E). Thus, we do not need to consider the case when a formula in Σ is false under an (I, E).

Solution Text: Assume that $\Sigma \cup \{(\neg A)\}$ is unsatisfiable. This means that, for any interpretation and environment (I, E), at least one formula in $\Sigma \cup \{(\neg A)\}$ is false.

We need to prove that $\Sigma \vDash A$. Consider an interpretation and environment (I, E). Assume that every formula in Σ is true under (I, E). We need to prove that A is true under (I, E).

Under the (I, E) we are considering, every formula in Σ is true and at least one formula in $\Sigma \cup \{(\neg A)\}$ is false. Therefore, it must be that $(\neg A)^v = 0$. By the definition of $\neg$, $A^v = 1$. Therefore, the tautological consequence $\Sigma \vDash A$ holds.

$\Sigma \vdash A$ holds by the completeness of Natural Deduction.

Exercise 129. *Let Σ be a set of Predicate formulas and let A be a Predicate formula. If $\Sigma \vdash A$, then $\Sigma \cup \{(\neg A)\}$ is unsatisfiable.*

Exercise 130. *Show that there is no formal deduction proof for $\{(\exists x\ P(x))\} \vdash P(t)$, where P is a unary predicate, t is a term and x is a variable.*

3 Program Verification

3.1 Partial and Total Correctness

Exercise 131. *Consider the Hoare triple* $\llparenthesis\, (x > 0) \,\rrparenthesis\ C_1\ \llparenthesis\, ((y * y) < x) \,\rrparenthesis$.

If we run C_1 *starting with the state* $(x = 5), (y = 5)$, C_1 *terminates in the state* $(x = 5), (y = 0)$.

Is the Hoare triple satisfied under partial correctness?

Solution: The answer is ‘not enough information to tell.”

The definition of partial correctness has an implication in it: If a starting state satisfies the precondition and the program terminates when run with this starting state, then the terminating state satisfies the postcondition.

For the given example, the starting state $(x = 5)$ satisfies the precondition $x > 0$, the program terminates, and the terminating state $((x = 5), (y = 0))$ satisfies the postcondition since $y * y = 0 < 5 = 5$. Therefore, this example satisfies the implication in the definition of partial correctness.

However, to verify partial correctness, we need to consider all possible starting states which satisfy the precondition, e.g. $(x = 1)$, $(x = 2)$, etc. We do not know the terminating states for the other possible starting states. Therefore, we do not have enough information to determine the answer.

Exercise 132. *Consider the Hoare triple* $\llparenthesis\, (x > 0) \,\rrparenthesis\ C_2\ \llparenthesis\, ((y * y) < x) \,\rrparenthesis$.

If we run C_2 *starting with the state* $(x = 5), (y = 5)$, C_2 *terminates in the state* $(x = 5), (y = 3)$.

Is the Hoare triple satisfied under partial correctness?

Solution: The answer is NO.

The definition of partial correctness has an implication in it: If a starting state satisfies the precondition and the program terminates when run with this starting state, then the terminating state satisfies the postcondition.

For the given example, the starting state $x = 5$ satisfies the precondition $x > 0$, and the terminating state $(x = 5, y = 3)$ does NOT satisfy the postcondition $y * y = 0 < 5 = 5$. Therefore, this example does not satisfy this implication in the definition of partial correctness.

To verify that partial correctness is not satisfied, it is sufficient to find one counterexample as shown above. Therefore, the triple is NOT satisfied under partial correctness.

Exercise 133. *Consider the Hoare triple* $\llparenthesis\, (x > 0) \,\rrparenthesis \;\; C_3 \;\; \llparenthesis\, ((y * y) < x) \,\rrparenthesis$.

If we run C_3 *starting with the state* $(x = -3), (y = 5)$*,* C_3 *terminates in the state* $(x = -3), (y = 0)$.

Is the Hoare triple satisfied under partial correctness?

Solution: The answer is “not enough information to tell”.

For the given example, the starting state $x = -3$ does not satisfy the precondition.

To verify partial correctness, we only need to consider starting states that satisfy the precondition. Therefore, the example is irrelevant for us.

Since we do not know how the program behaves for starting states that satisfy the precondition, we do not have enough information to determine the answer.

Exercise 134. *Consider the Hoare triple* $\llparenthesis\, (x > 0) \,\rrparenthesis \;\; C_4 \;\; \llparenthesis\, ((y * y) < x) \,\rrparenthesis$.

If we run C_4 *starting with the state* $(x = 2), (y = 5)$*,* C_4 *does not terminate.*

Is the Hoare triple satisfied under partial correctness?

Solution: The answer is “not enough information to tell”.

The definition of partial correctness has an implication in it: If a starting state satisfies the precondition and the program terminates when run with this starting state, then the terminating state satisfies the postcondition.

For the given example, the starting state $x = 2$ satisfies the precondition but the program does not terminate. Note that, program termination is a premise of the implication in the definition of partial correctness. Therefore, this example satisfies the implication in the definition of partial correctness.

However, to verify partial correctness, we need to consider all possible starting states that satisfy the precondition. Since we do not know how the program behaves for other possible starting states, we do not have enough information to determine the answer.

Exercise 135. *Is the following Hoare triple satisfied under partial and/or total correctness?*

$\llparenthesis\, (x = 1) \,\rrparenthesis$

```
while (1) {
   x = 0
};
```

$\llparenthesis\, (y = 1) \,\rrparenthesis$

Solution: The triple is satisfied under partial correctness, and it is not satisfied under total correctness.

The program does not terminate for any starting state. Therefore, partial correctness is automatically satisfied. (If the program does not terminate for a starting state, then the premise of the implication is false and the implication is vacuously true.)

The program does not terminate for any starting state. Therefore, total correctness is NOT satisfied.

The key difference between partial and total correctness is that partial correctness does not require program termination, whereas total correctness does.

Exercise 136. *Is the following Hoare triple satisfied under partial and/or total correctness?*

$\llparenthesis\, true \,\rrparenthesis$

```
y = 1;
z = 0;
while (z != x) {
   z = z + 1;
   y = y * z;
}
```

$\llparenthesis\, (y = x!) \,\rrparenthesis$

Solution: The triple is satisfied under partial correctness, and it is NOT satisfied under total correctness.

The precondition is true. This means that there is no required precondition. In other words, any starting state satisfies the precondition.

If the starting state has $x \geq 0$, we can verify that the program terminates and computes $y = x!$ correctly. (We are not able to prove this yet because we haven't learned the techniques to construct the proof. However, we could verify this on a case-by-case basis.) Therefore, for this case, partial and total correctness are both satisfied.

If the starting state has $x < 0$, the while loop runs forever and does not terminate. Therefore, for this case, only partial correctness is satisfied. Total correctness is not satisfied because the program does not terminate.

In summary, partial correctness is satisfied because it is satisfied in both cases. Total correctness is NOT satisfied because the program does not terminate for some starting states where $x < 0$.

3.2 Assignment Statements

Complete the following annotations.

$\llparenthesis \qquad\qquad \rrparenthesis$
x = 2;
$\llparenthesis\, (x = 2) \,\rrparenthesis$

Solution:

$\llparenthesis\, (2 = 2) \,\rrparenthesis$
x = 2;
$\llparenthesis\, (x = 2) \,\rrparenthesis$ assignment

$\llparenthesis \qquad\qquad \rrparenthesis$
x = 2;
$\llparenthesis\, (x = y) \,\rrparenthesis$

Solution:

$\llparenthesis\, (2 = y) \,\rrparenthesis$
x = 2;
$\llparenthesis\, (x = y) \,\rrparenthesis$ assignment

$\llparenthesis \qquad\qquad \rrparenthesis$
x = 2;
$\llparenthesis\, (x = 0) \,\rrparenthesis$

Solution:

$\llparenthesis\, (2 = 0) \,\rrparenthesis$
x = 2;
$\llparenthesis\, (x = 0) \,\rrparenthesis$ assignment

$\llparenthesis \qquad\qquad\qquad\qquad \rrparenthesis$

x = x + 1;

$\llparenthesis\, (x = (n+1)) \,\rrparenthesis$

Solution:

$\llparenthesis\, ((x+1) = (n+1)) \,\rrparenthesis$

x = x + 1;

$\llparenthesis\, (x = (n+1)) \,\rrparenthesis$ assignment

$\llparenthesis \qquad\qquad\qquad\qquad \rrparenthesis$

x = y;

$\llparenthesis\, ((2 * x) = (x + y)) \,\rrparenthesis$

Solution:

$\llparenthesis\, ((2 * y) = (y + y)) \,\rrparenthesis$

x = y;

$\llparenthesis\, ((2 * x) = (x + y)) \,\rrparenthesis$ assignment

Exercise 137. *Show that the following triple is satisfied under partial correctness.*

$\llparenthesis\, (y = 6)\, \rrparenthesis$
x = y + 1;
$\llparenthesis\, (x = 7)\, \rrparenthesis$

Solution:

$\llparenthesis\, (y = 6)\, \rrparenthesis$
$\llparenthesis\, ((y + 1) = 7)\, \rrparenthesis$ implied (A)
x = y + 1;
$\llparenthesis\, (x = 7)\, \rrparenthesis$ assignment

Proof of implied (A):
Assume that $y = 6$. Adding 1 to both sides, we get $y + 1 = 6 + 1 = 7$.

Exercise 138. *Show that the following triple is satisfied under partial correctness.*

$\llparenthesis\, ((x = x_0) \wedge (y = y_0))\, \rrparenthesis$
t = x;
x = y;
y = t;
$\llparenthesis\, ((x = y_0) \wedge (y = x_0))\, \rrparenthesis$

Solution:

$\llparenthesis\, ((x = x_0) \wedge (y = y_0))\, \rrparenthesis$
$\llparenthesis\, ((y = y_0) \wedge (x = x_0))\, \rrparenthesis$ implied (A)
t = x;
$\llparenthesis\, ((y = y_0) \wedge (t = x_0))\, \rrparenthesis$ assignment
x = y;
$\llparenthesis\, ((x = y_0) \wedge (t = x_0))\, \rrparenthesis$ assignment
y = t;
$\llparenthesis\, ((x = y_0) \wedge (y = x_0))\, \rrparenthesis$ assignment

Proof of implied (A):
Assume that $((x = x_0) \wedge (y = y_0))$ is true. By the definition of $\wedge$, $x = x_0$ and $y = y_0$ are both true. By the definition of $\wedge$, $((y = y_0) \wedge (x = x_0))$ is true.

3.3 Conditional Statements

Exercise 139. *Show that the following triple is satisfied under partial correctness.*

```
$\llparenthesis\, true \,\rrparenthesis$
if (x > y) {
   max = x;
} else {
   max = y;
}
$\llparenthesis\, (((x > y) \wedge (max = x)) \vee ((x \leq y) \wedge (max = y))) \,\rrparenthesis$
```

Solution:

```
$\llparenthesis\, true \,\rrparenthesis$
if (x > y) {
   $\llparenthesis\, (x > y) \,\rrparenthesis$                                                   if-then-else
   $\llparenthesis\, (((x > y) \wedge (x = x)) \vee ((x \leq y) \wedge (x = y))) \,\rrparenthesis$          implied (A)
   max = x;
   $\llparenthesis\, (((x > y) \wedge (max = x)) \vee ((x \leq y) \wedge (max = y))) \,\rrparenthesis$    assignment
} else {
   $\llparenthesis\, (\neg(x > y)) \,\rrparenthesis$                                                if-then-else
   $\llparenthesis\, (((x > y) \wedge (y = x)) \vee ((x \leq y) \wedge (y = y))) \,\rrparenthesis$          implied (B)
   max = y;
   $\llparenthesis\, (((x > y) \wedge (max = x)) \vee ((x \leq y) \wedge (max = y))) \,\rrparenthesis$    assignment
}
$\llparenthesis\, (((x > y) \wedge (max = x)) \vee ((x \leq y) \wedge (max = y))) \,\rrparenthesis$        if-then-else
```

Proof of implied (A)
Assume that $(x > y)$. By the definition of $=$, $x = x$ is true. By the definition of $\wedge$, $((x > y) \wedge (x = x))$ is true. By the definition of $\vee$, $(((x > y) \wedge (x = x)) \vee ((x \leq y) \wedge (x = y)))$ is true.

Proof of implied (B)
Assume that $(\neg(x > y))$ is true. By the definition of $>$, $(x \leq y)$ is true. By the definition of $=$, $y = y$ is true. By the definition of $\wedge$, $((x \leq y) \wedge (y = y))$ is true. By the definition of $\vee$, $(((x > y) \wedge (y = x)) \vee ((x \leq y) \wedge (y = y)))$ is true.

Exercise 140. *Show that the following triple is satisfied under partial correctness.*

```
$\llparenthesis\, (x = 3) \,\rrparenthesis$
if (x > 0) {
   x = 1;
} else {
   x = 0;
}
$\llparenthesis\, (x \geq 0) \,\rrparenthesis$
```

Solution:

```
$\llparenthesis\, (x = 3) \,\rrparenthesis$
if (x > 0) {
   $\llparenthesis\, ((x = 3) \wedge (x > 0)) \,\rrparenthesis$          if-then-else
   $\llparenthesis\, (1 \geq 0) \,\rrparenthesis$                       implied (A)
   x = 1;
   $\llparenthesis\, (x \geq 0) \,\rrparenthesis$                       assignment
} else {
   $\llparenthesis\, ((x = 3) \wedge (\neg(x > 0))) \,\rrparenthesis$      if-then-else
   $\llparenthesis\, (0 \geq 0) \,\rrparenthesis$                       implied (B)
   x = 0;
   $\llparenthesis\, (x \geq 0) \,\rrparenthesis$                       assignment
}
$\llparenthesis\, (x \geq 0) \,\rrparenthesis$                          if-then-else
```

Proof of implied (A) $(((x = 3) \wedge (x > 0)) \rightarrow (1 \geq 0))$
Assume that $((x = 3) \wedge (x > 0))$ is true. $1 \geq 0$ is true by the definition of $\geq$.

Proof of implied (B) $(((x = 3) \wedge (\neg(x > 0))) \rightarrow (0 \geq 0))$
The premise $((x = 3) \wedge (\neg(x > 0)))$ is false. $(x = 3)$ means that x is positive. $(\neg(x > 0))$ means that x is not positive. These two formulas contradict each other and cannot be true at the same time. Therefore, $((x = 3) \wedge (\neg(x > 0)))$ is false by the property of $\wedge$. The implication is vacuously true.

Exercise 141. *Show that the following triple is satisfied under partial correctness.*

```
⦇ $true$ ⦈
if (max < x) {
   max = x;
}
⦇ $(max \geq x)$ ⦈
```

Solution:

```
⦇ $true$ ⦈
if (max < x) {
   ⦇ $(max < x)$ ⦈        if-then
   ⦇ $(x \geq x)$ ⦈        implied (A)
   max = x;
   ⦇ $(max \geq x)$ ⦈        assignment
}
⦇ $(max \geq x)$ ⦈          if-then
                          implied (B) $((\neg(max < x)) \rightarrow (max \geq x))$
```

Proof of implied (A)
Assume that $(max < x)$ is true. $(x \geq x)$ is true by the definition of $\geq$.

Proof of implied (B)
Assume that $(\neg(max < x))$ is true. By the definition of $\neg$ and $<$, $(max \geq x)$ is true.

Exercise 142. *Show that the following triple is satisfied under partial correctness.*

```
$(\!|\, true \,|\!)$
if (x % 2 == 1) {
   x = x + 1;
}
$(\!|\, (\exists u\, (x = (2 * u))) \,|\!)$
```

Solution:

```
$(\!|\, true \,|\!)$
if (x % 2 == 1) {
   $(\!|\, ((x\%2) = 1) \,|\!)$                  if-then
   $(\!|\, (\exists u\ (x + 1 = (2 * u))) \,|\!)$      implied (A)
   x = x + 1;
   $(\!|\, (\exists u\ (x = (2 * u))) \,|\!)$          assignment
}
$(\!|\, (\exists u\ (x = (2 * u))) \,|\!)$             if-then
                                 implied (B) $((\neg(x\%2 = 1)) \to ((\exists u\ (x = (2 * u)))))$
```

Proof of implied (A)
Assume that $((x\%2) = 1)$ is true. This means that x is odd. By the definition of an odd integer, there exists an integer u such that $x = 2 * u - 1$ or $x + 1 = 2 * u$. Therefore, $(\exists u\ (x + 1 = (2 * u)))$ is true.

Proof of implied (B)
Assume that $((\neg(x\%2 = 1))$ is true, which meant that x is even. By the definition of an even integer, there exists an integer u such that $x = 2 * u$. Therefore, $((\exists u\ (x = (2 * u))))$ is true.

Exercise 143. *Show that the following triple is satisfied under partial correctness.*

```
$\llparenthesis\, \mathit{true} \,\rrparenthesis$
if (x < 5) {
  r = 0;
} else {
  if (x > 10) {
    r = 0;
  } else {
    r = 1;
  }
}
$\llparenthesis\, ((((x < 5) \vee (x > 10)) \wedge (r = 0)) \vee (((5 \leq x) \wedge (x \leq 10)) \wedge (r = 1))) \,\rrparenthesis$
```

Solution:

```
$\llparenthesis\, \mathit{true} \,\rrparenthesis$
if (x < 5) {
  $\llparenthesis\, \mathit{true} \wedge (x < 5) \,\rrparenthesis$                                                      if−then−else
  $\llparenthesis\, ((((x < 5) \vee (x > 10)) \wedge (0 = 0)) \vee (((5 \leq x) \wedge (x \leq 10)) \wedge (0 = 1))) \,\rrparenthesis$     implied (A)
  r = 0;
  $\llparenthesis\, ((((x < 5) \vee (x > 10)) \wedge (r = 0)) \vee (((5 \leq x) \wedge (x \leq 10)) \wedge (r = 1))) \,\rrparenthesis$     assignment
} else {
  $\llparenthesis\, \mathit{true} \wedge (x \geq 5) \,\rrparenthesis$                                                      if−then−else
  if (x > 10) {
    $\llparenthesis\, \mathit{true} \wedge (x \geq 5) \wedge (x > 10) \,\rrparenthesis$                                  if−then−else
    $\llparenthesis\, ((((x < 5) \vee (x > 10)) \wedge (0 = 0)) \vee (((5 \leq x) \wedge (x \leq 10)) \wedge (0 = 1))) \,\rrparenthesis$   implied (B)
    r = 0;
    $\llparenthesis\, ((((x < 5) \vee (x > 10)) \wedge (r = 0)) \vee (((5 \leq x) \wedge (x \leq 10)) \wedge (r = 1))) \,\rrparenthesis$   assignment
  } else {
    $\llparenthesis\, \mathit{true} \wedge (x \geq 5) \wedge (x \leq 10) \,\rrparenthesis$   if−then−else
    $\llparenthesis\, ((((x < 5) \vee (x > 10)) \wedge (1 = 0)) \vee (((5 \leq x) \wedge (x \leq 10)) \wedge (1 = 1))) \,\rrparenthesis$   implied (C)
    r = 1;
    $\llparenthesis\, ((((x < 5) \vee (x > 10)) \wedge (r = 0)) \vee (((5 \leq x) \wedge (x \leq 10)) \wedge (r = 1))) \,\rrparenthesis$   assignment
  }
  $\llparenthesis\, ((((x < 5) \vee (x > 10)) \wedge (r = 0)) \vee (((5 \leq x) \wedge (x \leq 10)) \wedge (r = 1))) \,\rrparenthesis$       if−then−else
}
$\llparenthesis\, ((((x < 5) \vee (x > 10)) \wedge (r = 0)) \vee (((5 \leq x) \wedge (x \leq 10)) \wedge (r = 1))) \,\rrparenthesis$         if−then−else
```

3.4 Conditional Statements: Additional Exercises

Exercise 144. *Show that the following triple is satisfied under partial correctness.*

```
⦇ true ⦈
x = a * a;
y = b * b;
z = x + y;
if (b > a) {
   z = z + 2 * a * b;
} else {
   z = z - 2 * a * b;
}
⦇ ((∃u (u * u = z)) ⦈
```

3.5 While Loops

Exercise 145. *Show that the following triple is satisfied under partial correctness.*

```
⦇ (x ≥ 0) ⦈
y = 1;
z = 0;
while (z != x) {
  z = z + 1;
  y = y * z;
}
⦇ (y = x!) ⦈
```

Remark 20. *There is a while loop in the program. To complete the proof, we need to come up with an invariant for the while loop. We produce the following table, which contains the values of all the variables in the program whenever the execution reaches the while test* $z! = x$.

Note: We can choose any non-negative value for x*. For the following table, we chose* $x = 5$.

Note: In the table, I wrote y *as a factorial. Doing this is helpful for seeing a relationship between the variables (With this, it is easy to see that* $y = z!$ *in every row of the table). Also, the post-condition says that* y *should be a factorial. If we want to make progress towards that post-condition, then it makes sense that* y *is equal to some factorial at every iteration of the loop.*

x	z	y
5	0	1 = 0!
5	1	1 = 1!
5	2	2 = 2!
5	3	6 = 3!
5	4	24 = 4!
5	5	120 = 5!

Given the table, we can try to come up with relationship between the variables. For the relationship to be an invariant, it has to be true in every row of the truth table.
For example,

- $(\neg(z = x))$ *is NOT an invariant. It is NOT true in the last row of the table.*
- $(z \leq x)$ *IS an invariant. It is true in every row of the table.*
- $(y = z!)$ *IS an invariant. It is true in every row of the table.*
- $(y = x!)$ *is NOT an invariant. It is only true in the last row of the table and not true in any other row.*

- $((z \leq x) \wedge (y = z!))$ *IS an invariant.*

Note: We can combine one or more invariants with an $\wedge$ *to produce new invariants. If* A *and* B *are invariants, then* $(A \wedge B)$ *is an invariant as well.*

So far, we have found three invariants: $(z \leq x)$, $(y = z!)$, *and* $((z \leq x) \wedge (y = z!))$*. Which of these invariants will lead to valid proofs? It turns out that both the second and third invariants will both lead to valid proofs.*

How do I choose an invariant to complete my proof? The only sure way of answering this question is to try completing the proof with the invariant. The proof is valid if and only if we can prove all of the implied conditions using the invariant.

However, there are two strategies to speed up this process of selecting ani nvariant that works.

- **A useful invariant is often similar to the post-condition.** *In our example, both invariants that work (*$(y = z!)$ *and* $((z \leq x) \wedge (y = z!))$*) have the component* $(y = z!)$*, which is similar to the post-condition* $(y = x!)$*.*

  This makes intuitive sense. An invariant describes the progress we are making towards the post-condition at every iteration of the loop. Therefore, it is only natural that the invariant looks similar to the post-condition.

- **The last implied condition (implied C) is often the most difficult to satisfy.** *Thus, to test whether an invariant works, it may be more efficient to try proving implied (C) first.*

See the completed solution below with the invariant $(y = z!)$*.*

Solution:

```
⦇ $(x \geq 0)$ ⦈
⦇ $(1 = 0!)$ ⦈                 implied (A)
y = 1;
⦇ $(y = 0!)$ ⦈                 assignment
z = 0;
⦇ $(y = z!)$ ⦈                 assignment
while (z != x) {
  ⦇ $((y = z!) \wedge (\neg(z = x)))$ ⦈    partial-while
  ⦇ $((y * (z+1)) = (z+1)!)$ ⦈        implied (B)
  z = z + 1;
  ⦇ $((y * z) = z!)$ ⦈                assignment
  y = y * z;
  ⦇ $(y = z!)$ ⦈                      assignment
}
⦇ $((y = z!) \wedge (\neg(\neg(z = x))))$ ⦈  partial-while
⦇ $(y = x!)$ ⦈                          implied (C)
```

Proof of implied (A):
Assume that $(x \geq 0)$ is true. $(1 = 0!)$ is true by the definition of factorial.

Proof of implied (B):
Assume that $(y = z!)$ and $(\neg(z = x))$ are true.
Multiplying $(z + 1)$ on both sides of $(y = z!)$, we get that $y * (z + 1) = (z + 1)!$ is true.

Proof of implied (C):
Assume that $(y = z!)$ and $(\neg(\neg(z = x)))$ are true. By the definition of $\neg$, $(\neg(\neg(z = x)))$ is equivalent to $(z = x)$. Since $(y = z!)$ and $(z = x)$ are both true, we know that $(y = x!)$ must be true.

Exercise 146. *Show that the following triple is satisfied under partial correctness.*

```
$\llparenthesis\, (x \geq 0) \,\rrparenthesis$
y = 1;
z = 0;
while (z < x) {
  z = z + 1;
  y = y * z;
}
$\llparenthesis\, (y = x!) \,\rrparenthesis$
```

Solution:

```
$\llparenthesis\, (x \geq 0) \,\rrparenthesis$
$\llparenthesis\, ((1 = 0!) \wedge (0 \leq x)) \,\rrparenthesis$                implied (A)
y = 1;
$\llparenthesis\, ((y = 0!) \wedge (0 \leq x)) \,\rrparenthesis$                assignment
z = 0;
$\llparenthesis\, ((y = z!) \wedge (z \leq x)) \,\rrparenthesis$                assignment
while (z < x) {
  $\llparenthesis\, (((y = z!) \wedge (z \leq x)) \wedge (z < x)) \,\rrparenthesis$  partial-while
  $\llparenthesis\, (y * (z + 1) = (z + 1)!) \,\rrparenthesis$                implied (B)
  z = z + 1;
  $\llparenthesis\, (y * z = z!) \,\rrparenthesis$                            assignment
  y = y * z;
  $\llparenthesis\, (y = z!) \,\rrparenthesis$                                assignment
}
$\llparenthesis\, (((y = z!) \wedge (z \leq x)) \wedge (\neg(z < x))) \,\rrparenthesis$  partial-while
$\llparenthesis\, (y = x!) \,\rrparenthesis$                                  implied (C)
```

Proof of implied (A):
Assume that $x \geq 0$ is true. Then $(0 \leq x)$ is true by the definitions of $\leq$ and $\geq$. $(1 = 0!)$ is true by the definition of factorial.

Proof of implied (B):
Assume that $(y = z!)$, $(z \leq x)$ and $(z < x)$ are true.
Multiplying $(z + 1)$ on both sides of $(y = z!)$, we get that $y * (z + 1) = (z + 1)!$ is true.

Proof of implied (C):
Assume that $(y = z!)$, $(z \leq x)$ and $(\neg(z < x))$ are true. By the definition of $\neg$, $(\neg(z < x))$ is equivalent to $(z \geq x)$. Since $(z \leq x)$ and $(z \geq x)$, it must be that $(z = x)$. Since $(y = z!)$ and $(z = x)$ are both true, we know that $(y = x!)$ must be true.

3.6 While Loops: Additional Exercises

Exercise 147. *Show that the following triple is satisfied under partial correctness.*

```
$\llparenthesis ((n \geq 0) \wedge (a \geq 0)) \rrparenthesis$
s = 1;
i = 0;
while (i != n) {
   s = s * a;
   i = i + 1;
}
$\llparenthesis (s = a^n) \rrparenthesis$
```

Exercise 148. *Show that the following triple is satisfied under partial correctness.*

```
$\llparenthesis ((n \geq 0) \wedge (a \geq 0)) \rrparenthesis$
s = 1;
i = 0;
while (i < n) {
   s = s * a;
   i = i + 1;
}
$\llparenthesis (s = a^n) \rrparenthesis$
```

3.7 Array Assignments

Exercise 149. *Show that the following triple is satisfied under partial correctness.*

$\llparenthesis\, ((A[x] = x0) \wedge (A[y] = y0))\, \rrparenthesis$

```
t = A[x];
A[x] = A[y];
A[y] = t;
```

$\llparenthesis\, ((A[x] = y0) \wedge (A[y] = x0))\, \rrparenthesis$ *array assignment*

Solution:

$\llparenthesis\, ((A[x] = x0) \wedge (A[y] = y0))\, \rrparenthesis$

$\llparenthesis\, ((A\{x \leftarrow A[y]\}\{y \leftarrow A[x]\}[x] = y0) \wedge (A\{x \leftarrow A[y]\}\{y \leftarrow A[x]\}[y] = x0))\, \rrparenthesis$ implied

```
t = A[x];
```

$\llparenthesis\, ((A\{x \leftarrow A[y]\}\{y \leftarrow t\}[x] = y0) \wedge (A\{x \leftarrow A[y]\}\{y \leftarrow t\}[y] = x0))\, \rrparenthesis$ assignment

```
A[x] = A[y];
```

$\llparenthesis\, ((A\{y \leftarrow t\}[x] = y0) \wedge (A\{y \leftarrow t\}[y] = x0))\, \rrparenthesis$ array assignment

```
A[y] = t;
```

$\llparenthesis\, ((A[x] = y0) \wedge (A[y] = x0))\, \rrparenthesis$ array assignment

Proof of implied:
We will prove that $((A[x] = x0) \wedge (A[y] = y0)) \rightarrow (((A\{x \leftarrow A[y]\}\{y \leftarrow A[x]\}[x] = y0) \wedge (A\{x \leftarrow A[y]\}\{y \leftarrow A[x]\}[y] = x0))$.

Proof. **Case 1: Assume that $x = y$.** Assume that $A[x] = x0$ and $A[y] = y0$ are true.

Since $x = y$, we can re-write the conclusion as follows.

$$\begin{aligned} &A\{x \leftarrow A[y]\}\{y \leftarrow A[x]\}[x] = A\{y \leftarrow A[y]\}\{y \leftarrow A[y]\}[y] = A[y] = y0, \text{ and} \\ &A\{x \leftarrow A[y]\}\{y \leftarrow A[x]\}[y] = A\{x \leftarrow A[x]\}\{x \leftarrow A[x]\}[x] = A[x] = x0. \end{aligned}$$

Case 2: Assume that $x \neq y$. Assume that $A[x] = x0$ and $A[y] = y0$ are true.

Consider the array $A\{x \leftarrow A[y]\}\{y \leftarrow A[x]\}$. The first assignment $\{x \leftarrow A[y]\}$ changes the xth element of the array to $A[y]$. The second assignment $\{y \leftarrow A[x]\}$ changes the yth element of the array to $A[x]$. Since $x \neq y$, the two assignments are modifying two different elements in the array and do not affect each other.

Therefore, we have that

$$A\{x \leftarrow A[y]\}\{y \leftarrow A[x]\}[y] = A[x] = x0.$$

because the second assignment changes the yth element to $A[x]$.

$$A\{x \leftarrow A[y]\}\{y \leftarrow A[x]\}[x] = A[y] = y0.$$

because the first assignment changes the xth element to $A[y]$.

□

3.8 Putting them together

Exercise 150. *(Reversing an array)*
Consider an array R of n integers, $R[1], R[2], ..., R[n]$.
Consider the following program which reverses the elements inside the array R.
Let r_x denote the element at index x in the array R before the program execution.
Prove that the following triple is satisfied under total correctness.

```
$\llparenthesis\, ((\forall x\,(1 \le x \le n \to R[x] = r_x)))\, \rrparenthesis$
j = 1;
while (2*j <= n) {
  t = R[j];
  R[j] = R[n+1-j];
  R[n+1-j] = t;
  j = j + 1;
}
$\llparenthesis\, ((\forall x\,(1 \le x \le n \to R[x] = r_{n+1-x})))\, \rrparenthesis$
```

Solution: Since there is a while loop in the program, we need to come up with an invariant for the while loop.
Consider the following invariant.

$$\begin{aligned} Inv(j) \vDash\dashv\, & (((\forall x\,(1 \le x \le j-1 \to (R[x] = r_{n+1-x} \land R[n+1-x] = r_x))) \\ & \land (\forall x\,(j \le x \le (n+1)/2 \to (R[x] = r_x \land R[n+1-x] = r_{n+1-x})))) \\ & \land (j \le n/2 + 1)) \end{aligned}$$

Using the above invariant, we complete the annotations for the program as shown below.

```
$\llparenthesis\, (\forall x\,(1 \le x \le n \to R[x] = r_x))\, \rrparenthesis$
$\llparenthesis\, Inv(1)\, \rrparenthesis$                    implied (A)
j = 1;
$\llparenthesis\, Inv(j)\, \rrparenthesis$                    assignment
while (2*j <= n) {
  $\llparenthesis\, (Inv(j) \land (2*j \le n))\, \rrparenthesis$ partial-while
  $\llparenthesis\, Inv(j+1)[R\{j \leftarrow R[n+1-j]\}\{n+1-j \leftarrow R[j]\}/R]\, \rrparenthesis$ implied (B)
  t = R[j];
  $\llparenthesis\, Inv(j+1)[R\{j \leftarrow R[n+1-j]\}\{n+1-j \leftarrow t\}/R]\, \rrparenthesis$ assignment
  R[j] = R[n+1-j];
  $\llparenthesis\, Inv(j+1)[R\{n+1-j \leftarrow t\}/R]\, \rrparenthesis$ array assignment
  R[n+1-j] = t;
  $\llparenthesis\, Inv(j+1)\, \rrparenthesis$                        array assignment
  j = j + 1;
  $\llparenthesis\, Inv(j)\, \rrparenthesis$ assignment
}
```

$(\!|\, (Inv(j) \wedge (\neg(2 * j \leq n)))\, |\!)$ partial−**while**
$(\!|\, ((\forall x\, (1 \leq x \leq n \to R[x] = r_{n+1-x})))\, |\!)$ implied (C)

It remains to prove the implied (A), (B), and (C).

To prove implied (C), we first prove Lemma 3 below.

Lemma 3. *The two formulas below are logically equivalent.*

$$\begin{aligned}&(\forall x\, ((1 \leq x \leq (n+1)/2) \to (R[x] = r_x \wedge R[n+1-x] = r_{n+1-x})))) \\ &\vDash\!\!\!\dashv (\forall x\, ((1 \leq x \leq n) \to (R[x] = r_x)))\end{aligned}$$

Proof. Starting with the top formula is logically equivalent to the following formula

$$\begin{aligned}&(\forall x\, (1 \leq x \leq (n+1)/2 \to R[x] = r_x))) \\ &\wedge (\forall x\, (1 \leq x \leq (n+1)/2 \to R[n+1-x] = r_{n+1-x})))\end{aligned} \tag{133}$$

We will transform formula 133 as follows. Let $y = n+1-x$. Then $x = n+1-y$. Plugging $x = n+1-y$ into formula 133, we have

$$\left(\forall x\, \left(1 \leq n+1-y \leq (n+1)/2 \to R[y] = r_y\right)\right))$$

Let's simplify the inequality $1 \leq n+1-y \leq (n+1)/2$.

$$1 \leq n+1-y \to y \leq n$$

$$n+1-y \leq (n+1)/2 \to y \geq (n+1)/2$$

Thus, the inequality becomes:

$$(n+1)/2 \leq y \leq n$$

The formula becomes:

$$\left(\forall x\, \left((n+1)/2 \leq y \leq n \to R[y] = r_y\right)\right))$$

Changing y back into x, we have

$$(\forall x\, ((n+1)/2 \leq x \leq n \to R[x] = r_x)))$$

□

Implied (A):

$$(\forall x\,(1 \leq x \leq n \rightarrow R[x] = r_x)) \rightarrow Inv(1)$$

Proof. Assume that the premise is true. Our goal is to prove that the conclusion is true. Let's simplify the conclusion below.
The conclusion is $Inv(1)$. Take the invariant $Inv(j)$ and plug in $j = 1$, we have

$$\begin{aligned}&(((\forall x\,(1 \leq x \leq 0 \rightarrow (R[x] = r_{n+1-x} \wedge R[n+1-x] = r_x)))\\ &\wedge (\forall x\,(1 \leq x \leq (n+1)/2 \rightarrow (R[x] = r_x \wedge R[n+1-x] = r_{n+1-x}))))\\ &\wedge (1 \leq n/2+1))\end{aligned}$$

$1 \leq x \leq 0$ is always false for any integer x. Thus the first part of the above formula is always true. We can simplify the formula to the following.

$$\begin{aligned}&(\forall x\,(1 \leq x \leq (n+1)/2 \rightarrow (R[x] = r_x \wedge R[n+1-x] = r_{n+1-x}))))\\ &\wedge (1 \leq n/2+1))\end{aligned}$$

We can further simplify $1 \leq n/2 + 1$ and get $0 \leq n$. The formula becomes the following:

$$\begin{aligned}&(\forall x\,(1 \leq x \leq (n+1)/2 \rightarrow (R[x] = r_x \wedge R[n+1-x] = r_{n+1-x}))))\\ &\wedge (0 \leq n))\end{aligned} \tag{134}$$

Note that $0 \leq n$ is true because n is positive. There is an implicit assumption that the array has at least one element. By Lemma 3, formula 134 is logically equivalent to the premise. Therefore, the implied holds. □

To prove implied (C), we first prove Lemma 4 below.

Lemma 4. *Assume that n is odd (The array R has an odd number of elements). The two formulas below are logically equivalent.*

$$(((\forall x\,(1 \leq x \leq (n-1)/2 \rightarrow (R[x] = r_{n+1-x} \wedge R[n+1-x] = r_{x}))) \wedge (R[(n+1)/2] = r_{(n+1)/2})$$

$$\vDash\!\Dashv ((\forall x\,(1 \leq x \leq n \rightarrow R[x] = r_{n+1-x})))$$

Proof. □

Implied (C):

$$(Inv(j) \wedge (\neg(2 * j \leq n))) \rightarrow ((\forall x \, (1 \leq x \leq n \rightarrow R[x] = r_{n+1-x})))$$

Proof. Let's simplify the premise.

$$\begin{gathered}(2j \leq n) \Dashv\vDash (2j > n) \Dashv\vDash (2j \geq n+1) \Dashv\vDash (j \geq (n+1)/2) \\ (j \leq n/2 + 1) \Dashv\vDash (j \leq (n+2)/2)\end{gathered}$$

If n is odd, then $j = (n+1)/2$. If n is even, then $j = (n+2)/2$.

Case 1: n **is even and** $j = (n+2)/2$**.** Plugging in $j = (n+2)/2$ into the premise, we have

$$\begin{aligned}&(((\forall x \, (1 \leq x \leq n/2 \rightarrow (R[x] = r_{n+1-x} \wedge R[n+1-x] = r_x))) \\ &\wedge (\forall x \, ((n+1)/2 \leq x \leq (n+1)/2 \rightarrow (R[x] = r_x \wedge R[n+1-x] = r_{n+1-x})))) \\ &\wedge (j = (n+1)/2).\end{aligned} \tag{135}$$

$(n+1)/2 \leq x \leq (n+1)/2$ is always false. Thus, formula 135 is always true. We can simplify the formula to the following.

$$\begin{aligned}&(((\forall x \, (1 \leq x \leq n/2 \rightarrow (R[x] = r_{n+1-x} \wedge R[n+1-x] = r_x))) \\ &\wedge (j = (n+1)/2).\end{aligned} \tag{136}$$

We can prove that the formula 136 is logically equivalent to the conclusion of implied (C). (The argument is similar to Lemma 3). Therefore, when n is even, if the premise of implied (C) is true, then the conclusion of implied (C) must be true.

Case 2: n **is odd and** $j = (n+1)/2$**.** Plugging in $j = (n+1)/2$ into the premise, we have the following. (I've omitted the $j = (n+1)/2$ part of the formula.

$$\begin{aligned}&(((\forall x \, (1 \leq x \leq (n-1)/2 \rightarrow (R[x] = r_{n+1-x} \wedge R[n+1-x] = r_x))) \\ &\wedge (\forall x \, ((n+1)/2 \leq x \leq (n+1)/2 \rightarrow (R[x] = r_x \wedge R[n+1-x] = r_{n+1-x}))))\end{aligned} \tag{137}$$

In formula 137, x must be equal to $(n+1)/2$. Thus, we can simplify formula 137 as follows.

$$\begin{aligned}&(\forall x \, ((n+1)/2 \leq x \leq (n+1)/2 \rightarrow (R[x] = r_x \wedge R[n+1-x] = r_{n+1-x}))) \\ &\Dashv\vDash \big(R[(n+1)/2] = r_{(n+1)/2} \wedge R[(n+1)/2] = r_{(n+1)/2}\big)) \\ &\Dashv\vDash R[(n+1)/2] = r_{(n+1)/2}\end{aligned}$$

With this simplification, the premise becomes:

$$\begin{aligned}&(((\forall x \, (1 \leq x \leq (n-1)/2 \rightarrow (R[x] = r_{n+1-x} \wedge R[n+1-x] = r_x))) \\ &\wedge (R[(n+1)/2] = r_{(n+1)/2})\end{aligned}$$

By Lemma 4, the above formula is logically equivalent to the conclusion of implied (C). Therefore, when n is odd, if the premise of implied (C) is true, then the conclusion of implied (C) must be true.

□

Implied (B):

$$(Inv(j) \wedge (2 * j \leq n)) \rightarrow Inv(j+1)[R\{j \leftarrow R[n+1-j]\}\{n+1-j \leftarrow R[j]\}/R]$$

Proof. For convenience, let's define $Inv_p(j)$ to be the following formula:

$$(((\forall x\, (1 \leq x \leq j-1 \rightarrow (R[x] = r_{n+1-x} \wedge R[n+1-x] = r_x))) \tag{138}$$
$$\wedge\, (\forall x\, (j \leq x \leq (n+1)/2 \rightarrow (R[x] = r_x \wedge R[n+1-x] = r_{n+1-x})))) \tag{139}$$

The premise of implied (B) becomes

$$Inv_p(j) \wedge (j \leq n/2+1)) \wedge (2j \leq n)$$

For convenience, let R' denote $R\{j \leftarrow R[n+1-j]\}\{n+1-j \leftarrow R[j]\}$. The conclusion of implied (B) becomes

$$\begin{aligned}
&(((\forall x\, (1 \leq x \leq j \rightarrow (R'[x] = r_{n+1-x} \wedge R'[n+1-x] = r_x)))\\
&\wedge\, (\forall x\, (j+1 \leq x \leq (n+1)/2 \rightarrow (R'[x] = r_x \wedge R'[n+1-x] = r_{n+1-x}))))\\
&\wedge\, (j \leq n/2))\\
&\vDash\!\dashv Inv_p(j+1)[R'/R] \wedge (j \leq n/2)
\end{aligned}$$

To prove implied (B), it is sufficient for us to prove the following two implications:

Implication 1: $((j \leq n/2+1)) \wedge (2j \leq n)) \rightarrow (j \leq n/2)$**.**
Proof of implication 1: Assume that $(j \leq n/2+1))$ and $(2j \leq n)$ are true. $(2j \leq n)$ is equivalent to $(j \leq n/2)$. Since $n/2 < n/2+1$, we know that $(j \leq n/2)$, which is the conclusion that we need.

Implication 2: $Inv_p(j) \rightarrow Inv_p(j+1)[R'/R]$**.**
Proof of implication 2: Let's recall that what $Inv_p(j)$ and $Inv_p(j+1)[R'/R]$ are.

$$\begin{aligned}
&Inv_p(j) \vDash\!\dashv (((\forall x\, (1 \leq x \leq j-1 \rightarrow (R[x] = r_{n+1-x} \wedge R[n+1-x] = r_x)))\\
&\wedge\, (\forall x\, (j \leq x \leq (n+1)/2 \rightarrow (R[x] = r_x \wedge R[n+1-x] = r_{n+1-x}))))
\end{aligned}$$

$$\begin{aligned}
&Inv_p(j+1)[R'/R] \vDash\!\dashv (((\forall x\, (1 \leq x \leq j \rightarrow (R'[x] = r_{n+1-x} \wedge R'[n+1-x] = r_x)))\\
&\wedge\, (\forall x\, (j+1 \leq x \leq (n+1)/2 \rightarrow (R'[x] = r_x \wedge R'[n+1-x] = r_{n+1-x}))))
\end{aligned}$$

To prove implication 2, it is sufficient to prove the following implications.

For any $1 \leq x \leq j-1$,

$$(R[x] = r_{n+1-x} \wedge R[n+1-x] = r_x) \rightarrow (R'[x] = r_{n+1-x} \wedge R'[n+1-x] = r_x).$$

Recall that $R' = R\{j \leftarrow R[n+1-j]\}\{n+1-j \leftarrow R[j]\}$. The two assignments only potentially affect the elements at indices j and $n+1-j$. Thus, for any index x where

$1 \leq x \leq j-1$, the element of R is not affected. Thus, for any $1 \leq x \leq j-1$, $R[x] = R'[x]$. Thus, the implication holds.

For $j+1 \leq x \leq (n+1)/2$,

$$\big(R[x] = r_x \land R[n+1-x] = r_{n+1-x}\big) \to \big(R'[x] = r_x \land R'[n+1-x] = r_{n+1-x}\big).$$

Recall that $R' = R\{j \leftarrow R[n+1-j]\}\{n+1-j \leftarrow R[j]\}$. The two assignments only potentially affect the elements at indices j and $n+1-j$. Thus, for any index x where $j+1 \leq x \leq (n+1)/2$, the element of R is not affected. Thus, for any $j+1 \leq x \leq (n+1)/2$, $R[x] = R'[x]$. Thus, the implication holds.

For $x = j$,

$$\big(R[x] = r_x \land R[n+1-x] = r_{n+1-x}\big) \to \big(R'[x] = r_{n+1-x} \land R'[n+1-x] = r_x\big).$$

This is equivalent to the following implication:

$$\big(R[j] = r_j \land R[n+1-j] = r_{n+1-j}\big) \to \big(R'[j] = r_{n+1-j} \land R'[n+1-j] = r_j\big).$$

Since $j < (n+1)/2$, $j \neq n+1-j$. Thus, we have that

$$R'[j] = R\{j \leftarrow R[n+1-j]\}\{n+1-j \leftarrow R[j]\}[j] = R[n+1-j] = r_{n+1-j}.$$

by the first assignment $\{j \leftarrow R[n+1-j]\}$ and by our assumption that $R[n+1-j] = r_{n+1-j}$.

$$R'[n+1-j] = R\{j \leftarrow R[n+1-j]\}\{n+1-j \leftarrow R[j]\}[n+1-j] = R[j] = r_j.$$

by the second assignment$\{n+1-j \leftarrow R[j]\}$ and by our assumption that $R[j] = r_j$.

□

4 Undecidability

4.1 Prove that a problem is decidable

Collected Wisdom:

- When you describe an algorithm, make sure that it terminates. For example, if a set S is infinite, your algorithm cannot iterate through every element of S. For another example, it is okay to draw the truth table of a given formula because the truth table has finite size.

- An algorithm usually considers several cases. Make sure that you clearly indicate the return value of the algorithm in every case.

Exercise 151. *The propositional-satisfiability problem: Is the propositional formula A satisfiable?*
Prove that the propositional-satisfiability problem is decidable.

Solution: We are given the propositional formula A. We will draw the truth table of A. The formula A must have a finite number of propositional variables in it. Therefore, the truth table will have a finite size and we will need a finite amount of time to draw the truth table.

We will go through every cell in the final column of the truth table, where the truth value of A is indicated. If we can find one row of the truth table in which A is true, then A is satisfiable. Otherwise, if A is false in every row of the truth table, then A is not satisfiable.

Exercise 152. *The propositional-tautology problem: Is the propositional formula A a tautology?*
Prove that the propositional-tautology problem is decidable.

4.2 The Halting Problem is Undecidable

Exercise 153. *The Halting Problem: Given a program P and an input I, does P terminate when run with input I?*
Prove that the Halting Problem is undecidable.

Solution: This proof is adapted from a proof by Luwei Zhang. Thanks, Luwei!

Proof by Contradiction. Assume that the halting problem is decidable. There exists an algorithm H such that H takes a program P and an input I for I and returns yes if P terminates when run with input I and no otherwise.
We will construct a program X which takes a program Y as its input. X works as follows.

- X called $H(Y, Y)$ to predict whether program Y will terminate when run with input Y.
- If $H(Y, Y)$ returns yes, X goes into an infinite loop and does not terminate.
- If $H(Y, Y)$ returns no, X terminates immediately.

Now, consider what happens if we run the program X with itself as input.
Suppose that H predicts that X terminates when run with input X. Then by the construction of X, when $H(X, X)$ returns yes, X goes into an infinite loop and does not terminate. H's prediction was wrong.
Suppose that H predicts that X does not terminate when run with input X. Then by the construction of X, when $H(X, X)$ returns no, X terminates immediately. H's prediction was wrong again.
Therefore, H does not correctly predict whether X terminates when run with input X. This contradicts with our assumption that H can decide the Halting Problem.

□

4.3 Prove that a problem is undecidable

Collected Wisdom:

- Suppose that we are trying to prove that problem X is undecidable. In your reduction, make the inputs to the algorithm for solving problem X relate to P and I. After all, we are trying to construct an algorithm to determine whether P terminates when run with input I.

- To verify whether a reduction leads to a valid proof, consider two different cases: (1) P terminates when run with input I. (2) P does not terminate when run with input I. A reduction works if and only if the constructed algorithm gives the correct answer for both cases.

- A few useful constructions:

  1. Construct a program which runs P with input I.
  2. Construct a program which does nothing and terminates immediately.
  3. Construct a program which has an infinite loop and runs forever.
  4. Construct a program, which ignores its input and does one of 1, 2, and 3.

Exercise 154. *The halting-no-input problem: Given a program P that requires no input, does P halt?*
Prove that the halting-no-input problem is undecidable.

Solution:

Proof by Contradiction. Assume that there is an algorithm B which solves the halting-no-input problem. We will construct an algorithm A to solve the halting problem.

Algorithm A takes two inputs a program P and an input I. It works as follows:

- Constructs a program P', which runs P with input I.
- Runs algorithm B with the program P' as the input and returns the result $B(P')$.

By our construction of algorithm A, P' halts if and only if P halts on input I. Therefore, if algorithm B solves the halting-no-input problem for input P', then algorithm A solves the halting problem for inputs P and I.

By our assumption, algorithm B solves the halting-no-input problem. Thus, algorithm A solves the halting problem.

This contradicts the fact that the halting problem is undecidable.

□

Exercise 155. *The both-halt problem: Given two programs $P1$ and $P2$ that take no input, do both programs halt?*
Prove that the both-halt problem is undecidable.

Solution:

Proof by Contradiction. Assume that there is an algorithm B which solves the both-halt problem. We will construct an algorithm A to solve the halting problem.

Algorithm A takes two inputs a program P and an input I. It works as follows:

- Constructs a program P', which runs P with input I.
- Runs algorithm B with the two programs P' and P' as its inputs and returns the result $B(P', P')$.

By our construction of algorithm A, both programs P' and P' halt if and only if P halts on input I. Therefore, if algorithm B solves the both-halt problem for inputs P' and P', then the algorithm A solves the halting problem for inputs P and I.

By our assumption, algorithm B solves the both-halt problem. Thus, algorithm A solves the halting problem.

This contradicts the fact that the halting problem is undecidable.

□

Remark 21. *Other reductions:*

- *Let $P1$ do nothing. Let $P2$ run P with input I. (This works.)*
- *Let $P1$ contain an infinite loop. Let $P2$ run P with input I. (This does NOT work.)*

Remark 22. *A variant of this problem:*
Consider the both-run-forever problem: Given two programs $P1$ and $P2$, do both programs run forever?
Prove that the both-run-forever problem is undecidable.

Exercise 156. *We say that two problems agree on all input if and only if, for every input x, either they both run forever, or they both halt and return the same value.*

The program-agreement problem: Given two programs, do they agree on all inputs?

Prove that the program-agreement problem is undecidable.

Exercise 157. *The total-correctness problem: Given a Hoare triple, is the triple satisfied under total correctness?*
Prove that the total correctness problem is undecidable.

Exercise 158. *The partial-correctness problem: Given a Hoare triple, is the triple satisfied under partial correctness?*
Prove that the partial-correctness problem is undecidable.

Solution:

Proof by Contradiction. Assume that there is an algorithm B which solves the total-correctness problem. We will construct an algorithm A to solve the halting problem.

Algorithm A takes two inputs a program P and an input I. It works as follows:

- Constructs a program P', which runs P with input I.
- Constructs the Hoare triple $\llparenthesis\, true \,\rrparenthesis\ P'\ \llparenthesis\, false \,\rrparenthesis$.
- Runs algorithm B with the Hoare triple $\llparenthesis\, true \,\rrparenthesis\ P'\ \llparenthesis\, false \,\rrparenthesis$ as its input.
- Return the negation of the result $B(\llparenthesis\, true \,\rrparenthesis\ P'\ \llparenthesis\, false \,\rrparenthesis)$. (If B returns true, then A returns false, and vice versa.)

If the program P' terminates, then the triple $\llparenthesis\, true \,\rrparenthesis\ P'\ \llparenthesis\, false \,\rrparenthesis$ is NOT satisfied under partial correctness because the postcondition is false. Therefore, the only way for the triple to be satisfied under partial correctness is when P' does not terminate.

By our construction of algorithm A, P halts on input I if and only if P' halts. P' halts if and only if the triple $\llparenthesis\, true \,\rrparenthesis\ P'\ \llparenthesis\, false \,\rrparenthesis$ is NOT satisfied under partial correctness. Thus, P halts on input I if and only if the triple $\llparenthesis\, true \,\rrparenthesis\ P'\ \llparenthesis\, false \,\rrparenthesis$ is NOT satisfied under partial correctness.

Therefore, if algorithm B solves the partial-correctness problem for input $\llparenthesis\, true \,\rrparenthesis\ P'\ \llparenthesis\, false \,\rrparenthesis$, then the algorithm A solves the halting problem for inputs P and I.

By our assumption, algorithm B solves the partial-correctness problem. Thus, algorithm A solves the halting problem.

This contradicts the fact that the halting problem is undecidable.

□

Exercise 159. *The exists-halting-input problem: Given a program P, does there exist an input I such that P halts with input I?*
Prove that this problem is undecidable.

Exercise 160. *The halt-every-input problem: Given a program P, does P halt for every input?*
Prove that the halt-every-input problem is undecidable.