Homework 1

CS 70, Summer 2024

Due by Friday, June 28th at 11:59 PM

This content is protected and may not be shared, uploaded, or distributed.

Instructions. Start each problem on a separate page. The subparts of each problem can be on the same page. Every answer should contain a calculation or reasoning. Your answers should be clear, organized, and legible—your final submission should not include scratch work or failed attempts. You must always commit to a final answer; if multiple answers are provided, the most incorrect one will be graded.

If you are completing the homework using LaTeX, you may use the templates. Homeworks must be submitted through Gradescope. See the end of the homework for submission instructions.

Sundry. Before you start writing your final homework submission, state briefly how you worked on it (e.g., if you went to office hours, how frequently you worked on it, etc.). If you worked on the assignment in a group with other students, list their names and email addresses.

1 The Boolean Algebra

We have seen that we are able to prove tautological truth and tautological equivalence using truth tables. However, the truth table algorithm is exponential in the number of inputs: if there are n variables in the propositional form, there will be 2^n rows in our truth table. This motivates us to find an alternate method for showing truth and equivalence in propositional logic.

The *Boolean algebra* provides us a base set of tautological truths and tautological equivalences which we can use to simplify most propositional forms. The Boolean algebra consists of the following tautological equivalences. The laws for conjunction and disjunction come in pairs. There is only one law for negation and only one law for implication.

Name	Conjunctive Rule	Disjunctive Rule
identity law	$\mathrm{T} \wedge P \equiv P$	$\mathrm{F} \vee P \equiv P$
annihilation law	$\mathrm{F} \wedge P \equiv \mathrm{F}$	$\mathrm{T} \vee P \equiv \mathrm{T}$
idempotent law	$P \wedge P \equiv P$	$P \vee P \equiv P$
inverse law	$P \wedge \neg P \equiv \mathrm{F}$	$P \vee \neg P \equiv \mathrm{T}$
commutative law	$P \wedge Q \equiv Q \wedge P$	$P \vee Q \equiv Q \vee P$
associative law	$(P \wedge Q) \wedge R \equiv P \wedge (Q \wedge R)$	$(P \vee Q) \vee R \equiv P \vee (Q \vee R)$
distributive law	$P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R)$	$P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R)$
absorption law	$P \wedge (P \vee Q) \equiv P$	$P \vee (P \wedge Q) \equiv P$
De Morgan's law	$\neg(P \wedge Q) \equiv \neg P \vee \neg Q$	$\neg(P \vee Q) \equiv \neg P \wedge \neg Q$

Name	Rule
double negation	$\neg\neg P \equiv P$

Name	Rule
modus tollens	$(P \implies Q) \equiv \neg Q \implies \neg P$

The remaining laws in the Boolean algebra are tautological truths. Note that the first is just the inverse law for disjunctions, and that the last is just proof by contradiction.

Name	Tautology
law of the excluded middle	$P \vee \neg P$
conjunction elimination	$(P \wedge Q) \implies P$
modus ponens	$\big((P \implies Q) \wedge P\big) \implies Q$
proof by cases	$\big((P \vee Q) \wedge (P \implies R) \wedge (Q \implies R)\big) \implies R$
reductio ad absurdum	$(\neg P \implies \mathrm{F}) \implies P$

(a) We have already proved many of these equivalences and truths in the class so far. We will now prove some more. You may not use the Boolean algebra in any of these proofs.

(i) Prove that *reductio ad absurdum* is tautologically true.

(ii) Prove the tautological equivalence in the absorption law for conjunction.

(iii) Prove that the proof by cases law is tautologically true.

(b) Let's use the Boolean algebra to prove that different propositional forms are tautologically equivalent. We can do this by chaining equivalence laws together.

Here's an example.

Example 1. $(B \wedge A) \vee A \equiv A \wedge (B \vee A)$.

$$\begin{aligned}
(B \wedge A) \vee A &\equiv A \vee (B \wedge A) && \text{(commutation)} \\
&\equiv (A \vee B) \wedge (A \vee A) && \text{(distribution)} \\
&\equiv (A \vee B) \wedge A && \text{(idempotence)} \\
&\equiv A \wedge (A \vee B). && \text{(commutation)}
\end{aligned}$$

Use the Boolean algebra to prove that each of the following pairs of propositional forms are equivalent. You may not use truth tables in your proofs. Justify each line of your proof with a law from the Boolean algebra.

(i) $(A \vee B) \wedge C \wedge (\neg(\neg B \wedge \neg A) \vee B)$ and $(A \vee B) \wedge C$.

(ii) $(A \wedge B) \vee (A \wedge C)$ and $A \wedge (B \vee A) \wedge (A \vee C) \wedge (B \vee C)$.

(c) In this part, we will use the Boolean algebra to prove propositional forms are tautologically true without using truth tables.

The last law needed to use the Boolean algebra is the law of *substitution*. This is the rule that if two propositional formulas are equivalent, then we can substitute them for one another in expressions without changing the truth value of the expression.

Here's an example of how to prove something is tautologically true using the Boolean algebra.

Example 2. $\neg(P \vee Q) \implies \neg P$.

(1) By De Morgan's law, $\neg(P \vee Q) \equiv \neg P \wedge \neg Q$.

(2) By conjunction elimination, $(\neg P \wedge \neg Q) \implies \neg P$.

(3) By (1), we can substitute $\neg P \wedge \neg Q$ with $\neg(P \vee Q)$ in (2). So $\neg(P \vee Q) \implies \neg P$.

In the proof, we used the conjunction elimination tautology and the De Morgan's law equivalence to show that $\neg(P \vee Q) \implies \neg P$ is also a tautology.

Here is another example of proving a tautology using the Boolean algebra.

Example 3. $\big((B \wedge A) \vee A\big) \implies A$.

(1) By **Example 1**, $(B \wedge A) \vee A \equiv A \wedge (A \vee B)$.

(2) By conjunction elimination, $\big(A \wedge (A \vee B)\big) \implies A$.

(3) By (1), we can substitute $A \wedge (A \vee B)$ with $(B \wedge A) \vee A$ in (2). So $\big((B \wedge A) \vee A\big) \implies A$.

Use the Boolean algebra to prove that each of the following are tautologically true. You may not use truth tables in your proof. Justify each line of your proof.

(i) $\big((A \wedge B) \vee (A \wedge C)\big) \implies A$.

(ii) The *disjunctive syllogism*: $\big((P \vee Q) \wedge \neg P\big) \implies Q$.

2 Binary Relationships

Let R be a binary predicate such that the following are true.

(1) $\forall x \forall y \big(R(x, y) \implies R(y, x)\big)$.

(2) $\exists x \forall y R(x, y)$.

(a) Prove or disprove whether each of the following are logically implied by conditions (1) and (2).

(i) $\forall x \exists y R(x, y)$.

(ii) $\forall x R(x, x)$.

(iii) $\exists y \forall x R(x, y)$.

(iv) $\forall x \forall y (R(x, y) \vee R(y, x))$.

(b) Consider the natural numbers with the binary predicate $R(x, y)$ as "$x \cdot y = 0$."

(i) Check that the conditions (1) and (2) are true of R in this setting.

(ii) Translate conditions (1) and (2), when applied to this setting, into simple English sentences.

3 Prime Factorization

In this problem, we will prove the fundamental theorem of arithmetic: any integer $n \geq 2$ can be factorized as a product of powers of its prime factors. That is, for any integer $n \geq 2$, we can write

$$n = p_1^{q_1} \cdot p_2^{q_2} \cdot \ldots \cdot p_m^{q_m},$$

where $p_1, p_2, \ldots, p_m$ are prime numbers and $q_1, q_2, \ldots, q_m$ are positive integers.

(a) We first consider the case where n is prime. Show that the fundamental theorem of arithmetic holds when n is itself a prime number.

(b) Now we consider the case when n is not prime; that is, n is composite. By the definition of a composite number, there exists a positive integer d such that $d \mid n$ and $1 < d < n$. We call d a *nontrivial divisor* of n.

Prove that if d and n/d can be factorized as a product of powers of its prime factors, then n can also be factorized as a product of powers of its prime factors.

(c) Using induction and the two parts above, prove the fundamental theorem of arithmetic.

4 Induction or Contradiction?

In this problem, we will learn a proof technique which is equivalent to induction. We will use the motivating example of proving Bernoulli's inequality: $(1 + x)^n \geq nx + 1$ for all $n \in \mathbb{N}$ and all $x \in \mathbb{R}$ such that $1 + x > 0$

(a) Suppose there exists some natural number such that Bernoulli's inequality is false. Let $k \in \mathbb{N}$ be the smallest number which is a counterexample to Bernoulli's inequality: $(1 + x)^k < kx + 1$.

Explain why $k \neq 0$.

(b) Continuing from part **(a)**, prove we must have $(1 + x)^{k-1} \geq (k - 1)x + 1$. Do not use induction.

(c) Continuing from parts **(a)** and **(b)**, multiply $(1 + x)$ on both sides of the inequality $(1 + x)^{k-1} \geq (k - 1)x + 1$ from part **(b)**. Observe what occurs and use your observation to complete the proof of Bernoulli's inequality.

(d) Now, prove Bernoulli's inequality using the principle of induction instead.

Once you're done, take a moment to think about the difference between the proof by contradiction in parts **(a)**, **(b)**, and **(c)** and the proof by induction. In particular, consider which step of the proof by contradiction is equivalent to the principle of induction. You don't need to include these thoughts and considerations in your answers.

5 Quick Proofs

Prove each of the following statements.

(a) For $a, b, c \in \mathbb{N}$, if $a \mid b$ and $b \mid c$, then $a \mid c$.

(b) If the sum of digits of $n \in \mathbb{N}$ is divisible by 9, then n is divisible by 9.

(c) If $a + b < c + d$, then $a < c$ or $b < d$.

(d) $\forall x, y \in \mathbb{R}$, $\min(x, y) = (x + y - |x - y|)/2$.

You may use without proof the fact that the absolute value of a real number z is defined as

$$|z| = \begin{cases} z & z \geq 0, \\ -z & z < 0. \end{cases}$$

6 Card Game

Azibo is playing with a deck of $n \geq 1$ cards. The front sides of the cards are labeled with the numbers 1 through n; we'll refer to them as Card 1 through Card n. The back sides of the cards contain an instruction to go to another card in the deck.

Azibo picks one of the n cards as his starting card. Let this card's number be c_1. Azibo follows the instruction on the back side to visit a new card, whose number we will call c_2. Then he follows the instruction on the back side of the new card to visit yet another card number c_3. And so on.

For example, consider the $n = 3$ cards given below, where the top halves represent the front sides of the cards and the bottom halves represent the back sides of the cards.

Card 1	Card 2	Card 3
Go to 3	Go to 1	Go to 3

If Azibo picks Card 2 as his first card, he will make the following steps: Card 2 to Card 1, and then Card 1 to Card 3, and then Card 3 to Card 3, and so on. This yields $c_1 = 2, c_2 = 1, c_3 = 3, c_4 = 3, \ldots$

We say that the cards have a *loop* if there is a sequence of at least two cards which return to the first card of the sequence. More formally, we say that the cards have a loop if we can pick a starting card c_1 such that for some $\ell > 1$, the cards $c_1, \ldots, c_\ell$ are all distinct and $c_{\ell+1} = c_1$. For example, the earlier three cards do not have a loop. Note that a card which goes to itself is not a loop.

The below deck of $n = 4$ cards has a loop.

Card 1	Card 2	Card 3	Card 4
Go to 3	Go to 3	Go to 4	Go to 2

The loop is the sequence with starting card $c_1 = 2$ and $\ell = 3$:

$$c_1 = 2, \quad c_2 = 3, \quad c_3 = 4, \quad c_4 = 2.$$

(a) Prove or disprove: if there is a card in the deck which goes to itself, then there are no loops.

(b) Prove or disprove: if there are no loops in the deck, there there must be some card which goes to itself.

(c) Suppose that Azibo's cards have no loop and that Card 1 is the only card which goes to itself. Prove that no matter which card Azibo starts with, the number of the n^{th} card that Azibo visits, c_n, is always the same. Determine the card number c_n of the n^{th} card Azibo visits.

Submission. Homeworks must be submitted through Gradescope. If you are completing your homeworks on paper, please scan the pages of your homework into a PDF using any scanner or phone application such as CamScanner. **It is your responsibility to ensure that all the work on the scanned pages is legible.**

Once you upload your submission to the Gradescope assignment, you will be prompted to select pages. **It is your responsibility to correctly select the pages of your homework corresponding to each question.** If you are having difficulties scanning, uploading, or submitting your homework, post a follow-up on the main thread corresponding to this homework on Ed.