Homework 1

CS 70, Summer 2024

Due by Friday, June 28$^{\text{th}}$ at 11:59 PM

1 The Boolean Algebra

(a) To prove that two propositional forms are tautologically equivalent, or that a propositional form is tautologically true, we must use truth tables.

(i) The truth table below shows that *reductio ad absurdum* is tautologically true, since it always evaluates to true.

P	$(\neg P$	$\implies$	F)	$\implies$	P
T	F	T	F	T	T
F	T	F	F	T	F

(ii) The truth table below shows that $P \land (P \lor Q)$ is tautologically equivalent to P since two propositional forms always have the same truth values.

P	Q	P	$\land$	$(P$	$\lor$	$Q)$	P
T	T	T	T	T	T	T	T
T	F	T	T	T	T	F	T
F	T	F	F	F	T	T	F
F	T	F	F	F	F	F	F

(iii) The truth table below shows that the proof by cases law is tautologically true, since it always evaluates to true. The order in which the columns are evaluated is indicated by the colors: first, the three gray columns; followed by the red column; then the blue column; and then the final green column.

P	Q	R	$((P$	$\lor$	$Q)$	$\land$	$(P$	$\implies$	$R)$	$\land$	$(Q$	$\implies$	$R))$	$\implies$	R
T	T	T	T	T	T	T	T	T	T	T	T	T	T	T	T
T	T	F	T	T	T	F	T	F	F	F	T	F	F	T	F
T	F	T	T	T	F	T	T	T	T	T	F	T	T	T	T
T	F	F	T	T	F	F	T	F	F	F	F	T	F	T	F
F	T	T	F	T	T	T	F	T	T	T	T	T	T	T	T
F	T	F	F	T	T	T	F	T	F	F	T	F	F	T	F
F	F	T	F	F	F	F	F	T	T	F	F	T	T	T	T
F	F	F	F	F	F	F	F	T	F	F	F	T	F	T	F

(b) **(i)** Start with De Morgan's laws, and simplify using the double negation rule, as well as the conjunction and disjunction rules.

$$\begin{aligned}
(A \lor B) \land C \land (\neg(\neg B \land \neg A) \lor B) &\equiv (A \lor B) \land C \land ((\neg\neg B \lor \neg\neg A) \lor B) && \text{(De Morgan's)} \\
&\equiv (A \lor B) \land C \land ((B \lor A) \lor B) && \text{(double negation)} \\
&\equiv (A \lor B) \land C \land (B \lor (B \lor A)) && \text{(commutation)} \\
&\equiv (A \lor B) \land C \land ((B \lor B) \lor A) && \text{(association)} \\
&\equiv (A \lor B) \land C \land (B \lor A) && \text{(idempotence)} \\
&\equiv (A \lor B) \land C \land (A \lor B) && \text{(commutation)} \\
&\equiv (A \lor B) \land (A \lor B) \land C && \text{(commutation)} \\
&\equiv (A \lor B) \land C. && \text{(idempotence)}
\end{aligned}$$

(ii) Apply the distribution laws.

$$\begin{aligned}(A \land B) \lor (A \land C) &\equiv ((A \land B) \lor A) \land ((A \land B) \lor C) && \text{(distribution)}\\ &\equiv (A \lor (A \land B)) \land (C \lor (A \land B)) && \text{(commutation)}\\ &\equiv \big((A \lor A) \land (A \lor B)\big) \land \big((C \lor A) \land (C \lor B)\big) && \text{(distribution)}\\ &\equiv \big(A \land (A \lor B)\big) \land \big((C \lor A) \land (C \lor B)\big) && \text{(idempotence)}\\ &\equiv \big(A \land (B \lor A)\big) \land \big((A \lor C) \land (B \lor C)\big) && \text{(commutation)}\\ &\equiv A \land (B \lor A) \land (A \lor C) \land (B \lor C). && \text{(association)}\end{aligned}$$

(c) **(i)** We mimic the proof in **Example 3**.

(1) By **(a)(ii)**, we have that $(A \land B) \lor (A \land C) \equiv A \land (B \lor A) \land (A \lor C) \land (B \lor C)$.

(2) By conjunction elimination, $A \land (B \lor A) \land (A \lor C) \land (B \lor C) \implies A$.

(3) By (1), we can substitute $(A \land B) \lor (A \land C)$ with $A \land (B \lor A) \land (A \lor C) \land (B \lor C)$ in (2). So $(A \land B) \lor (A \land C) \implies A$.

(ii) First we simplify the left-hand side into an equivalent expression.

$$\begin{aligned}\big((P \lor Q) \land \neg P\big) &\equiv (\neg P \land (P \lor Q)) && \text{(commutation)}\\ &\equiv (\neg P \land P) \lor (\neg P \land Q) && \text{(distribution)}\\ &\equiv \mathrm{F} \lor (\neg P \land Q) && \text{(inverse)}\\ &\equiv \neg P \land Q && \text{(annihilation)}\\ &\equiv Q \land \neg P. && \text{(commutation)}\end{aligned}$$

So $\big((P \lor Q) \land \neg P\big) \equiv Q \land \neg P$. Therefore we can use conjunction elimination to get the implication of Q. Again, we mimic the proof of **Example 3**.

(1) By the above, we have that $\big((P \lor Q) \land \neg P\big) \equiv Q \land \neg P$.

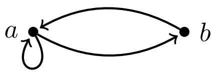
(2) By conjunction elimination, $Q \land \neg P \implies Q$.

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

2 Binary Relationships

(a) **(i)** This is logically implied. Let a be an arbitrary element. We must show that $\exists y R(a, y)$. By condition (2), there is some element b such that $\forall y R(b, y)$. In particular, $R(b, a)$. By applying condition (1) in the case of b and a, $R(b, a) \implies R(a, b)$. Together, $R(b, a)$ and $R(b, a) \implies R(a, b)$ means we have that $R(a, b)$. So $\exists y R(a, y)$. But a was chosen arbitrarily, so we have that $\forall x \exists y R(x, y)$.

(ii) This is not logically implied. Consider the following counterexample with domain $\mathfrak{D} = \{a, b\}$ and $R(x, y)$ defined as "x points to y."



In the above model, a satisfies the existential claim $\exists x \forall y R(x, y)$ since $R(a, a)$ and $R(a, b)$.

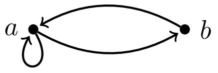
The first condition is also satisfied.

- For a and b, we have that $R(a, b)$ and $R(b, a)$, so $R(a, b) \implies R(b, a)$ and $R(b, a) \implies R(a, b)$ are both true.
- For a and a, we have that $R(a, a)$, so $R(a, a) \implies R(a, a)$ is true. Its converse is identical to itself, so the converse is also true.
- For b and b, $R(b, b)$ is false, so $R(b, b) \implies R(b, b)$ and its converse are both vacuously true.

However, it is not the case that $\forall x R(x, x)$. We can show this by demonstrating that the negation $\exists x \neg R(x, x)$ is true. In particular the model makes $\neg R(b, b)$, so it makes $\exists x \neg R(x, x)$ true.

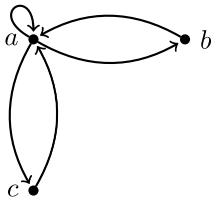
(iii) This is logically implied. By applying (2), we have some object a such that $\forall y R(a, y)$. Let b be an arbitrary element. By applying $\forall y R(a, y)$, we know that $R(a, b)$. By applying (1) in the case of a and b, we have that $R(a, b) \implies R(b, a)$, so we know that $R(b, a)$. But b was arbitrary, so we have $\forall x R(x, a)$. Therefore we have $\exists y \forall x R(x, y)$.

(iv) This is not logically implied. Consider the following counterexample.



We have already seen that this model satisfies the two conditions. However, it does not make the condition $\forall x \forall y(R(x,y) \lor R(y,x))$ true. We demonstrate that the negation $\exists x \exists y(\neg R(x,y) \land \neg R(y,x))$ is true. In particular, we have that $\neg R(b,b) \land \neg R(b,b)$, so $\exists x \exists y(\neg R(x,y) \land \neg R(y,x))$.

Another counterexample is the following model. Note that $\neg R(b,c) \land \neg R(c,b)$.



(b) **(i)** (1) For any two natural numbers $x, y \in \mathbb{N}$, suppose that $x \cdot y = 0$. By commutativity of multiplication, we have that $y \cdot x = 0$. So for any $x, y \in \mathbb{N}$, $R(x,y) \implies R(y,x)$.

(2) For any $y \in \mathbb{N}$, $0 \cdot y = 0$. So there exists some element such x such that for all y, $R(x,y)$.

(ii) (1) For any two natural numbers x and y, if $x \cdot y$ equals 0, then so does $y \cdot x$.

(2) There is a natural number such that its product with any natural number is 0.

3 Prime Factorization

(a) If n is prime, its only prime factor is itself, by definition. We can write $n = n^1$ to factorize it as a product of the powers of its prime factors.

(b) By assumption, we have the following factorizations of d and n/d:

$$d = p_1^{q_1} \cdot \ldots \cdot p_m^{q_m} \qquad\qquad n/d = r_1^{s_1} \cdot \ldots \cdot r_k^{s_k},$$

where $p_1, \ldots, p_m$ and $r_1, \ldots, r_k$ are prime numbers and $q_1, \ldots, q_m$ and $s_1, \ldots, s_k$ are positive integers.

Therefore

$$\begin{aligned} n &= d \cdot n/d \\ &= \left(p_1^{q_1} \cdot \ldots \cdot p_m^{q_m}\right) \cdot \left(r_1^{s_1} \cdot \ldots \cdot r_k^{s_k}\right) \\ &= p_1^{q_1} \cdot \ldots \cdot p_m^{q_m} \cdot r_1^{s_1} \cdot \ldots \cdot r_k^{s_k}, \end{aligned}$$

where $p_1, \ldots, p_m, r_1, \ldots, r_k$ are prime numbers and $q_1, \ldots, q_m, s_1, \ldots, s_k$ are positive integers. Note that the prime numbers $p_1, \ldots, p_m, r_1, \ldots, r_k$ are not necessarily distinct.

(c) By induction.

Base case. $n = 2$. We can write $n = 2 = 2^1$.

Induction case.

Induction hypothesis. Suppose that for all $2 \leq k \leq n-1$, k can be factorized as a product of powers of its prime factors.

Induction case. We now consider the claim for n. Either n is prime or composite.

(1) If n is prime, we have a prime factorization by part **(a)**.

(2) If n is composite, we have a nontrivial divisor $d \in \mathbb{Z}^+$ such that $d \mid n$ and $1 < d < n$. Since $d \mid n$, n/d is also an integer. Moreover, since $d \neq n$, $n/d \neq 1$, and thus $n/d \geq 2$.

By the induction hypothesis, since $d \geq 2$ and $n/d \geq 2$, we have prime factorizations of d and n/d. Therefore we have a prime factorization for n by part **(b)**.

By the principle of mathematical induction, we have shown that for all integers $n \geq 2$, the claim holds.

4 Induction or Contradiction?

(a) For $k = 0$, we have that $(1 + x)^0 = 1 \not< 1 = 0 \cdot x + 1$. So $k = 0$ cannot be the counterexample to the rule.

(b) Suppose for contradiction that $(1 + x)^{k-1} < (k - 1)x + 1$. So $k - 1$ contradicts Bernoulli's inequality. But $k - 1 < k$. This contradicts the fact that n is the smallest counterexample to Bernoulli's inequality, so our assumption that $(1 + x)^{k-1} < (k - 1)x + 1$ must be incorrect. Instead, it must be that $(1 + x)^{k-1} \geq (k - x)x + 1$.

(c) Multiplying both sides by $(1 + x)$ yields

$$\begin{aligned}(1 + x)^{k-1}(1 + x) &\geq ((k - 1)x + 1)(1 + x)\\ (1 + x)^k &\geq (k - 1)x + 1 + (k - 1)x^2 + x\\ &= kx + 1 + (k - 1)x^2\\ &\geq kx + 1.\end{aligned}$$

But this contradicts our assumption that k is a counterexample with $(1+x)^k < kx+1$. Therefore our assumption that there existed a counterexample to Bernoulli's inequality must be incorrect.

(d) As directed, we use induction.

Base case. $n = 0$. By **(a)**, the claim holds.

Induction case.

Induction hypothesis. Suppose that for some $n \in \mathbb{N}$, we have that $(1 + x)^n \geq nx + 1$.

Induction step. We now consider the claim for $n + 1$.

$$\begin{aligned}(1 + x)^{n+1} &= (1 + x)^n(1 + x)\\ &\geq (nx + 1)(1 + x)\\ &= nx + 1 + nx^2 + x\\ &= (n + 1)x + 1 + nx^2\\ &\geq (n + 1)x + 1.\end{aligned}$$

Thus we have shown that $(1 + x)^n \geq nx + 1 \implies (1 + x)^{n+1} \geq (n + 1)x + 1$.

By the principle of mathematical induction, we have that for all $n \in \mathbb{N}$, the claim $(1 + x)^n \geq nx + 1$ holds.

Note that the proofs are quite similar. In the contradiction proof, we use that fact that $(1 + x)^n \geq nx + 1 \implies (1+x)^{n+1} \geq (n+1)x+1$ to prove that there cannot exist a counterexample to Bernoulli's inequality. In the induction proof, we use the same fact to show that prove that Bernoulli's inequality holds for all elements. In some sense, the contradiction proof is disproving the negation of the claim, while the induction proof is proving the claim directly.

The contradiction proof uses the *well-ordering principle*, which is equivalent to the principle of induction. The well-ordering principle states that every subset of the natural numbers has a smallest element; we invoked this principle when we used the smallest element of the subset corresponding to the counterexamples to Bernoulli's inequality.

5 Quick Proofs

(a) By definition, if $a \mid b$, there is some $k \in \mathbb{Z}$ such that $b = ak$. Similarly, there is some $m \in \mathbb{Z}$ such that $c = bm$.

Then $c = bm = akm$, where $km = \ell \in Z$ since the integers are closed under multiplication. So $c = a\ell$ for some $\ell \in \mathbb{Z}$. By definition, this means that $a \mid c$.

(b) Let the digits of n be $n_0, n_1, \ldots, n_k \in \{0, \ldots, 9\}$. Then

$$n = n_0 + 10n_1 + \ldots + 100^k n_k = \sum_{i=0}^{k} 10^i n_i$$

Suppose that the sum of the digits of n are divisible by 9: that is, for some $k \in \mathbb{Z}$,

$$\sum_{i=0}^{k} n_i = 9k.$$

Note that we can write

$$n = \sum_{i=0}^{k} 10^i n_i = \sum_{i=0}^{k} ((10^i - 1)n_i + n_i) = \sum_{i=0}^{k} (10^i - 1)n_i + \sum_{i=0}^{k} n_i = \sum_{i=0}^{k} (10^i - 1)n_i + 9k.$$

We claim that $9 \mid (10^i - 1)$. To show this, we will show that for any $i \in \mathbb{N}$,

$$10^i - 1 = 9 \sum_{j=0}^{i-1} 10^j.$$

By the finite geometric series, for any $i \in \mathbb{N}$,

$$9 \sum_{j=0}^{i-1} 10^j = 9 \left(\frac{1 - 10^i}{1 - 10} \right) = 9 \left(\frac{10^i - 1}{10 - 1} \right) = 9 \left(\frac{10^i - 1}{9} \right) = 10^i - 1.$$

Therefore $9 \mid (10^i - 1)$, as desired, and so we can write $10^i - 1 = 9k_i$ for some $k_i \in \mathbb{Z}$. Therefore

$$n = \sum_{i=0}^{k} 9k_i n_i + 9k = 9 \left(\sum_{i=0}^{k} k_i n_i + k \right).$$

Thus $9 \mid n$, as desired.

(c) By contraposition. Suppose that $a \geq c$ and $b \geq d$. Then $a + b \geq c + d$.

(d) There are two cases. Either $x \geq y$ or $x < y$.

(1) $x \geq y$. Then $\min(x, y) = y$ and $x - y \geq 0$. So $|x - y| = x - y$. Then

$$\frac{x + y - |x - y|}{2} = \frac{x + y - (x - y)}{2} = \frac{2y}{2} = y = \min(x, y).$$

(2) $x < y$. Then $\min(x, y) = x$ and $x - y < 0$. So $|x - y| = -(x - y) = y - x$. Then

$$\frac{x + y - (y - x)}{2} = \frac{2x}{2} = x = \min(x, y).$$

In either case, $\min(x, y) = (x + y - |x - y|)/2$. So the claim holds in general.

6 Card Game

(a) Playing around with a few small decks of cards quickly yields a counterexample. Consider the following deck.

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

This deck has a card which goes to itself—Card 3—but it also has a loop: for $c_1 = 1$, we get $c_2 = 2$, $c_3 = 1$. This is a loop with $\ell = 2$.

(b) By contraposition. Suppose that no card goes to itself. Starting with Card 1, follow the next n instructions. After this, Azibo will have visited $n + 1$ cards. Since there are only n cards, by the pigeonhole principle, Azibo must have visited one card at least twice. Let k be the index at which that card is visited for the first time and $k + \ell + 1$ be the index at which that card is visited for the second time, so that $c_k = c_{k+\ell+1}$.

Since no card in the deck goes to itself, the card cannot have been visited in consecutive turns. That is, $k+\ell+1 > k+1$. Then we have found a loop with $\ell > 1$: it starts with card c_k and ends with the card $c_{k+\ell}$. In particular, if Azibo starts at card c_k, we get the sequence of cards $c_1 = c_k, \ldots, c_\ell, c_{\ell+1} = c_{k+\ell+1} = c_k$. Therefore there is a loop.

(c) No matter where Azibo starts, he will have that $c_n = 1$, the first card. There are two cases: either Azibo starts with Card 1 or he starts with some other card.

(1) If Azibo starts with Card 1, then he will always stay at Card 1, and so $c_n = 1$.

(2) If Azibo starts with any other card and takes $n-1$ steps, he will have visited n cards.

Suppose for contradiction that Azibo never visits Card 1. Then there are only $n-1$ possible cards that he could have visited: Cards $2, \ldots, n$. By the pigeonhole principle, Azibo must have visited one of those cards twice. But as we saw in **(b)**, this allows us to construct a loop, which is a contradiction to the assumption that there are no loops in the deck.

Therefore Azibo must have visited Card 1 at some point in his $n-1$ turns. But once Azibo visits Card 1, he stays at Card 1 for all future steps. Therefore $c_n = 1$.

Regardless of whether Azibo starts at Card 1 or some other card, he has that $c_n = 1$.