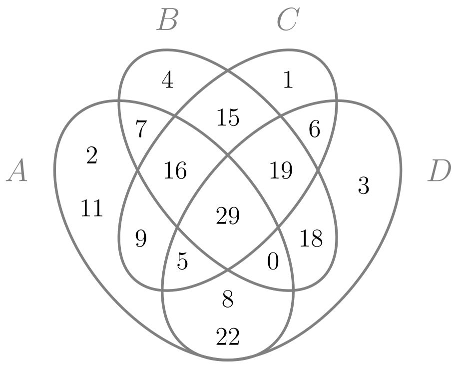
Homework 3

Discrete Structures
Due Tuesday, January 26, 2021

Submit each question separately in .pdf format only

---

1. (a) Given the Venn diagram on the left, write all the elements of the sets on the right.



$(A \cap C) \setminus (D \cap B)$	$\{16, 9, 5\}$
$\overline{(\overline{A} \cup D)} \cap B$	$\{7, 16\}$
$(C \oplus D) \cap \overline{(D \oplus B)}$	$\{9, 1, 0, 18\}$
$\overline{(D \cap B \cap C)} \oplus (D \cup B \cup C)$	$\{29, 16, 2, 11\}$

(b) Describe the following sets using A, B, C, D from above and set operations on them.

$$E = \{16, 29, 0\} \qquad F = \{6, 7, 16, 19\} \qquad G = \{3, 18, 0, 4, 7\}$$

$$E = (A \cap B) \setminus \overline{(C \cup D)} \qquad F = ((A \cap B) \setminus D) \cup ((C \cup D) \setminus A) \qquad G = (D \cup B) \setminus (C \cup (A \setminus B))$$

(c) Simplify the following sets as much as possible. That is, rewrite them without using the union $\cup$ or intersection $\cap$ symbols.

$$X = \bigcup_{i=0}^{\infty} [i, i+1] \qquad Y = \bigcap_{n=1}^{\infty} \left[0, \frac{1}{n}\right] \qquad Z = \bigcap_{n=1}^{\infty} \left\{ \frac{n}{x} \ : \ x \in \mathbf{Z}_{\geqslant n} \right\}$$

$$X = \mathbf{R}_{\geqslant 0} \qquad Y = \{0\} \qquad Z = \left\{ \frac{1}{n} \ : \ n \in \mathbf{N} \right\}$$

2. Let A, B, C be sets, and let $f\colon A \to B$ and $g\colon B \to C$ be functions.

(a) Using logical symbols, express the following statements.

i. g is injective when restriced to the range of f

$\forall\ b_1, b_2 \in f(A)\ ((g(b_1) = g(b_2)) \ \rightarrow \ (b_1 = b_2))$ □

ii. there exists an element in C whose preimage in g is not $f(a)$ for any a in A

$\exists\ c \in C\ (\forall\ a \in A\ (g^{-1}(c) \neq a))$ □

(b) If f and g are injective, prove that $g \circ f$ is injective.

Let $a_1, a_2 \in A$ and suppose that $g(f(a_1)) = g(f(a_2))$. Since the codomain of f is B, $f(a_1), f(a_2) \in B$. Since g is injective and $g(f(a_1)) = g(f(a_2))$, it must be that $f(a_1) = f(a_2)$. Since f is injective and $f(a_1) = f(a_2)$, it must be that $a_1 = a_2$. Hence $g \circ f$ is injective. □

(c) If $g \circ f$ is surjective, prove that g must be surjective.

Suppose that g is not surjective. That is, suppose that there exists some $c \in C$ with $c \notin g(B)$. Since $f(A) \subseteq B$, it follows that $c \notin g(f(A))$. Since $g \circ f$ is surjective, we have that $C = (g \circ f)(A) = g(f(A))$. This is a contradiction, as $c \in C$, but $c \notin g(f(A))$. Hence our initial assumption was false, and so g is surjective. $\square$

3. Let A, B, C be arbitrary sets in the same universe U. Prove or disprove the following statements:

(a) $(B \cup C) - A = (B - C) \cup (C - A)$.

The set identity is false; see the comparison of the left side and the right side in Figure 1. Consider elements that belong to A and B, but not C $((A \cap B) - C)$. They do not belong to the left side, but they do belong to the right side. Therefore this identity is not valid for arbitrary sets. (For certain sets having $(A \cap B) - C = \varnothing$ it is true, but these are special cases only.)

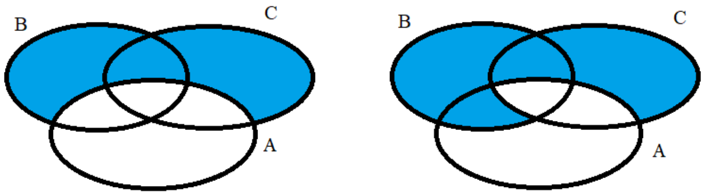


Figure 1: Illustration that, in general, $(B \cup C) - A \neq (B - C) \cup (C - A)$.

$\square$

(b) $(B \oplus C) - A = (B - A) \oplus (C - A)$.

The set identity is true.
The left side contains elements that belong just to one of the sets B or C (namely, $B - (A \cup C)$ or $C - (A \cup B)$).
And the right side also contains exactly those elements. See Figure 2.

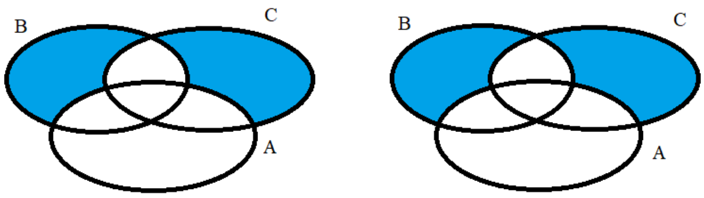


Figure 2: Illustration that $(B \oplus C) - A = (B - A) \oplus (C - A)$.

$\square$

(c) $\overline{A} \times \overline{(B \cup C)} = \overline{A \times (B \cup C)}$.

The set identity is false.
The right side of the equality contains pairs (x, y), where (x, y) is outside the Cartesian product $A \times (B \cup C)$ (i.e. $x \notin A$ **or** $y \notin (B \cup C)$). The left side of the expression requires that both x and y belong to the complements ($x \notin A$ **and** $y \notin (B \cup C)$).

For example, if the universe of all A, B, C is the set of all integers $\mathbf{Z}$, and we define:

- A – all integers divisible by 2,
- B – all integers divisible by 3,
- C – all integers divisible by 5.

In this case, the left side $\overline{A} \times \overline{(B \cup C)}$ contains just those $(x, y) \in \mathbf{Z} \times \mathbf{Z}$ for which **both** x is odd (not divisible by 2); **and** y is not divisible either by 3 or 5.

On the other hand, $\overline{A \times (B \cup C)}$ also contains elements such as $(x, y) = (2, 1)$ (where x is divisible by 2, but y is not divisible either by 3 or 5), and also $(x, y) = (1, 3)$ (where x is not divisible by 2, but y is divisible by 3 or 5). □

4. Prove or disprove the following statements about power sets.

(a) There is a set X such that its powerset $\mathcal{P}(X)$ equals

$$\{\varnothing, \{a\}, \{\varnothing\}, \{a, \{\varnothing\}\}\}. \tag{1}$$

Answer. The set cannot be a powerset of any set X.
Let us assume by contradiction, that there is some X such that (1) is $\mathcal{P}(X)$. Since any X it is a subset of itself (and thus $X \in \mathcal{P}$), the set X must appear as one of the elements in $\mathcal{P}$.
Case 1. If $X = \{a, \{\varnothing\}\}$, one of its subsets is the set containing a single element $\{\varnothing\} \in X$. Thus $\{\{\varnothing\}\} \subseteq X$ and $\{\{\varnothing\}\} \in \mathcal{P}(X)$. But we can see that the set (1) does not contain such an element. It does contain a different element: $\{\varnothing\}$ (which should not be there). Surrounding it with an extra pair of parentheses would create a set that is the powerset of X as in (2).

$$\{\varnothing, \{a\}, \{\{\varnothing\}\}, \{a, \{\varnothing\}\}\}. \tag{2}$$

Case 2. If X is $\varnothing$, or $\{a\}$, or $\{\varnothing\}$, then $\mathcal{P}(X)$ cannot equal the expression (1), since these are 0-element or 1-element sets, and their powersets cannot have 4 elements as (1) does.

□

(b) There is a set X such that its powerset $\mathcal{P}(X)$ equals

$$\{\varnothing, \{\varnothing\}, \{\{a\}\}, \{\{a, b\}\}, \{\varnothing, \{a\}\}, \{\varnothing, \{a, b\}\}, \{\{a\}, \{a, b\}\}, \{\varnothing, \{a\}, \{a, b\}\}\}. \tag{3}$$

Answer. The set $X = \{\varnothing, \{a\}, \{a, b\}\}$ is such that $\mathcal{P}(X)$ equals (3).
This 3-element set X has these subsets:
1 set with zero elements: $\varnothing$,
3 sets with one element: $\{\varnothing\}, \{\{a\}\}, \{\{a, b\}\}$,

3 sets with two elements: $\{\varnothing, \{a\}\}, \{\varnothing, \{a,b\}\}, \{\{a\}, \{a,b\}\}$,
1 set with three elements (X itself): $\{\varnothing, \{a\}, \{a,b\}\}$.
We can check that all these sets (and nothing else) is in (3).

$\square$

(c) For any two sets A and B, $\mathcal{P}(A) \subseteq \mathcal{P}(B)$ iff $A \subseteq B$.

The statement is true. Since it contains biconditional "iff", the proof has two parts:
Part 1. $A \subseteq B \to \mathcal{P}(A) \subseteq \mathcal{P}(B)$.
Assume that $A \subseteq B$; let us prove that $\mathcal{P}(A) \subseteq \mathcal{P}(B)$. Namely, let $X \in \mathcal{P}(A)$ be any element in $\mathcal{P}(A)$; and it means that X is a subset of A. Since $A \subseteq B$, X is also a subset of B. So we also must have $X \subseteq \mathcal{P}(B)$.
Part 2. $\mathcal{P}(A) \subseteq \mathcal{P}(B) \to A \subseteq B$.
By contradiction, assume that $A \not\subseteq B$. In this case there should be element $a \in A$ (and $a \notin B$). Then the set $\{a\}$ is in $\mathcal{P}(A)$, but at the same time $\{a\}$ is not in $\mathcal{P}(B)$, because $\{a\}$ is not a subset of B. This is a contradiciton, since the assumption was $\mathcal{P}(A) \subseteq \mathcal{P}(B)$; but we just found a counterexample. Therefore A must be a subset of B whenever $\mathcal{P}(A)$ is a subset of $\mathcal{P}(B)$.

$\square$

5. Prove the following three tautologies using Coq. Submit your file `tautology.v` as the solution for your Problem 5.

```
Lemma Sample5A: forall P Q:Prop, ~(~P /\ ~Q) -> P \/ Q.
Proof.
  (* Place your proof here *)
Qed.

Lemma Sample5B: forall P Q:Prop, (P -> Q) -> (~P \/ Q).
Proof.
  (* Place your proof here *)
Qed.

Lemma Sample5C: forall P Q:Prop, (P -> Q) <-> (~Q -> ~P).
Proof.
  (* Place your proof here *)
Qed.
```

Note. Most lemmas in the non-constructive mathematics are proven using some tautology as an axiom. Either the "NNPP axiom" ($\neg\neg A \to A$, double negation elimination) or the "classic axiom" ($A \vee \neg A$, the law of the Excluded Middle). See the link *Week3 > Two Nonconstructive Proofs of the Same Lemma* in ORTUS. You can try out whichever method you want. For these axioms to work the first line in your proof should be:
`Require Import Classical_Prop.`

A sample answer file `tautology.v` with full proofs is provided below; there are certainly many other ways to prove these 3 tautologies. Please note that every lemma uses some classical result (in our case `NNPP` or `classic`).

```
Require Import Classical_Prop.

Lemma Sample5A: forall P Q: Prop, ~(~P /\ ~Q) -> P \/ Q.
Proof.
  intros P Q.
  intros H.
  apply NNPP.
  unfold not.
  intros H2.
  unfold not in H.
  apply H.
  split.
  intros H3.
  apply H2.
  left; exact H3.
  intros H4.
  apply H2.
  right; exact H4.
Qed.

Lemma Sample5B: forall P Q: Prop, (P -> Q) -> (~P \/ Q).
Proof.
  intros P Q.
  intros H.
  destruct (classic P) as [H2|H3].
  right.
  apply (H H2).
  left.
  exact H3.
Qed.

Lemma Sample5C: forall P Q: Prop, (P -> Q) <-> (~Q -> ~P).
Proof.
  intros P Q.
  split.
  - intros H.
    intros H2.
    intros H3.
    contradiction (H2 (H H3)).
  - intros H4.
    intros H5.
    apply NNPP.
    intros H6.
    contradiction ((H4 H6) H5).
Qed.
```