hw4-proofs-and-sets

CSE20S24

Due: 5/14/24 at 5pm (no penalty late submission until 8am next morning)

In this assignment, you will use propositional and predicate logic to evaluate statements and arguments. You will analyze statements and determine if they are true or false using valid proof strategies. You will also determine if candidate arguments are valid.

Relevant class material: Weeks 4,5,6.

You will submit this assignment via Gradescope (https://www.gradescope.com) in the assignment called "hw4-proofs-and-sets".

For all HW assignments: These homework assignments may be done individually or in groups of up to 3 students. Please ensure your name(s) and PID(s) are clearly visible on the first page of your homework submission, start each question on a new page, and upload the PDF to Gradescope. If you're working in a group, *submit only one submission per group*: one partner uploads the submission through their Gradescope account and then adds the other group member(s) to the Gradescope submission by selecting their name(s) in the "Add Group Members" dialog box. You will need to re-add your group member(s) every time you resubmit a new version of your assignment.

Each homework question will be graded either for **correctness** (including clear and precise explanations and justifications of all answers) or **fair effort completeness**. You may collaborate on "graded for correctness" questions only with CSE 20 students in your group; if your group has questions about a problem, you may ask in drop-in help hours or post a private post (visible only to the Instructors) on Piazza. For "graded for completeness" questions: collaboration is allowed with any CSE 20 students this quarter; if your group has questions about a problem, you may ask in drop-in help hours or post a public post on Piazza.

All submitted homework for this class must be typed. You can use a word processing editor if you like (Microsoft Word, Open Office, Notepad, Vim, Google Docs, etc.) but you might find it useful to take this opportunity to learn LaTeX. LaTeX is a markup language used widely in computer science and mathematics. The homework assignments are typed using LaTeX and you can use the source files as templates for typesetting your solutions.

Integrity reminders

- Problems should be solved together, not divided up between the partners. The homework is designed to give you practice with the main concepts and techniques of the course, while getting to know and learn from your classmates.

- You may not collaborate on homework questions graded for correctness with anyone other than your group members. You may ask questions about the homework in office hours (of the instructor, TAs, and/or tutors) and on Piazza (as private notes viewable only to the Instructors). You *cannot* use any online resources about the course content other than the class material from this quarter – this is primarily to ensure that we all use consistent notation and definitions (aligned with the textbook) and also to protect the learning experience you will have when the 'aha' moments of solving the problem authentically happen.

- Do not share written solutions or partial solutions for homework with other students in the class who are not in your group. Doing so would dilute their learning experience and detract from their success in the class.

In your proofs and disproofs of statements below, justify each step by reference to a component of the following proof strategies we have discussed so far, and/or to relevant definitions and calculations.

- A counterexample can be used to prove that $\forall x P(x)$ is **false**.

- A witness can be used to prove that $\exists x P(x)$ is **true**.

- **Proof of universal by exhaustion**: To prove that $\forall x\, P(x)$ is true when P has a finite domain, evaluate the predicate at **each** domain element to confirm that it is always T.

- **Proof by universal generalization**: To prove that $\forall x\, P(x)$ is true, we can take an arbitrary element e from the domain and show that $P(e)$ is true, without making any assumptions about e other than that it comes from the domain.

- To prove that $\exists x P(x)$ is **false**, write the universal statement that is logically equivalent to its negation and then prove it true using universal generalization.

- **Strategies for conjunction**: To prove that $p \wedge q$ is true, have two subgoals: subgoal (1) prove p is true; and, subgoal (2) prove q is true. To prove that $p \wedge q$ is false, it's enough to prove that p is false. To prove that $p \wedge q$ is false, it's enough to prove that q is false.

- **Proof of Conditional by Direct Proof**: To prove that the implication $p \to q$ is true, we can assume p is true and use that assumption to show q is true.

- **Proof of Conditional by Contrapositive Proof**: To prove that the implication $p \to q$ is true, we can assume $\neg q$ is true and use that assumption to show $\neg p$ is true.

- **Proof by Cases**: To prove q when we know $p_1 \vee p_2$, show that $p_1 \to q$ and $p_2 \to q$.

Assigned questions

1. Evaluating predicates. Consider the following predicates, each of which has as its domain the set of all bitstrings whose leftmost bit is 1

   $E(x)$ is T exactly when $(x)_2$ is even, and is F otherwise

   $L(x)$ is T exactly when $(x)_2 < 15$, and is F otherwise

   $M(x)$ is T exactly when $(x)_2 > 2$ and is F otherwise.

   Sample response that can be used as reference for the detail expected in your answer: To prove that the statement
   $$\forall x\ L(x)$$
   is false, we can use the counterexample $x = 1111$, which is a bitstring whose leftmost bit is 1 (so is in the domain). Applying the definition of $L(x)$, since $(1111)_2 = 1 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0 = 8 + 4 + 2 + 1 = 15$ which is not (strictly) less than 15, we have that $L(1111) = F$ and so the universal statement is false.

   (a) (*Graded for correctness*) [1] Use a counterexample to prove that the statement
   $$\forall x(\ L(x) \rightarrow E(x)\ )$$
   is false.

   (b) (*Graded for correctness*) Use a witness to prove that the statement
   $$\exists x(\ L(x) \wedge M(x)\ )$$
   is true.

   (c) (*Graded for completeness*) [2] Translate each of the statements in the previous two parts to English.

   ---

   [1]This means your solution will be evaluated not only on the correctness of your answers, but on your ability to present your ideas clearly and logically. You should explain how you arrived at your conclusions, using mathematically sound reasoning. Whether you use formal proof techniques or write a more informal argument for why something is true, your answers should always be well-supported. Your goal should be to convince the reader that your results and methods are sound.

   [2]This means you will get full credit so long as your submission demonstrates honest effort to answer the question. You will not be penalized for incorrect answers. To demonstrate your honest effort in answering the question, we expect you to include your attempt to answer *each* part of the question. If you get stuck with your attempt, you can still demonstrate your effort by explaining where you got stuck and what you did to try to get unstuck.

2. Set properties. Let $W = \mathcal{P}(\{1, 2, 3, 4, 5\})$.

Sample response that can be used as reference for the detail expected in your answer for parts (a) and (b) below:

To give an example element in the set $\{X \in W \mid 1 \in X\} \cap \{X \in W \mid 2 \in X\}$, consider $\{1, 2\}$. To prove that this is in the set, by definition of intersection, we need to show that $\{1, 2\} \in \{X \in W \mid 1 \in X\}$ and that $\{1, 2\} \in \{X \in W \mid 2 \in X\}$.

- By set builder notation, elements in $\{X \in W \mid 1 \in X\}$ have to be elements of W which have 1 as an element. By definition of power set, elements of W are subsets of $\{1, 2, 3, 4, 5\}$. Since each element in $\{1, 2\}$ is an element of $\{1, 2, 3, 4, 5\}$, $\{1, 2\}$ is a subset of $\{1, 2, 3, 4, 5\}$ and hence is an element of W. Also, by roster method, $1 \in \{1, 2\}$. Thus, $\{1, 2\}$ satisfies the conditions for membership in $\{X \in W \mid 1 \in X\}$.

- Similarly, by set builder notation, elements in $\{X \in W \mid 2 \in X\}$ have to be elements of W which have 2 as an element. By definition of power set, elements of W are subsets of $\{1, 2, 3, 4, 5\}$. Since each element in $\{1, 2\}$ is an element of $\{1, 2, 3, 4, 5\}$, $\{1, 2\}$ is a subset of $\{1, 2, 3, 4, 5\}$ and hence is an element of W. Also, by roster method, $2 \in \{1, 2\}$. Thus, $\{1, 2\}$ satisfies the conditions for membership in $\{X \in W \mid 2 \in X\}$.

(a) (*Graded for correctness*) Give two (different) example elements in

$$W \times \mathcal{P}(W)$$

Justify your examples by explanations that include references to the relevant definitions.

(b) (*Graded for correctness*) Give one example element in

$$\{X \in W \mid (1 \in X) \wedge (X \cap \{3, 4\} = \emptyset)\}$$

Justify your example by explanations that include references to the relevant definitions.

(c) (*Graded for completeness*) Consider the following statement and attempted proof:

$$\forall A \in W \; \forall B \in W \; (\; ((A \cap B) \subseteq A) \to (A \subseteq B) \;)$$

(1) Towards a universal generalization argument, **choose arbitrary** $A \in W, B \in W$.
(2) We need **to show** $((A \cap B) \subseteq A) \to (A \subseteq B)$.
(3) Towards a proof of the conditional by the contrapositive, **assume** $A \subseteq B$, and we need **to show** that $(A \cap B) \subseteq A$.
(4) By definition of subset inclusion, this means we need **to show** $\forall x \; (x \in A \cap B \to x \in A \;)$.
(5) Towards a universal generalization, **choose arbitrary** x; we need **to show** that
$x \in A \cap B \to x \in A$.

(6) Towards a direct proof, **assume** $x \in A \cap B$, and we need **to show** $x \in A$.

(7) By definition of set intersection and set builder notation, we have that $x \in A \wedge x \in B$.

(8) By the definition of conjunction, $x \in A$, which is what we needed to show. QED

Demonstrate that this attempted proof is invalid by providing and justifying a **counterexample** (disproving the statement). Then, explain why this attempted proof is invalid by identifying in which step a definition or proof strategy is used incorrectly, and describing how the definition or proof strategy was misused.

(d) (*Graded for completeness*) A Venn diagram is a chart of overlapping regions that illustrates the similarities differences of a collection of sets. You may have seen some examples in memes, including these (from a web search):
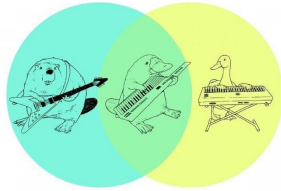

Mostly we see Venn Diagrams with 2 or 3 circles (or other shapes). In this question, we consider how to draw a Venn Diagram with 4 regions.

  i. Here is a Venn Diagram with 2 circles. Each region is labelled (encoded) with a binary string with 2 bits. Notice that there are four regions: the region outside of the two circles, the region inside the left circle and not the right circle, the region inside the right circle and not the left circle, and the region inside both circles.
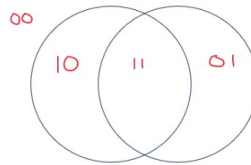

Generalize this encoding by encoding each region in this 3 circle Venn Diagram with a unique binary string with 3 bits.
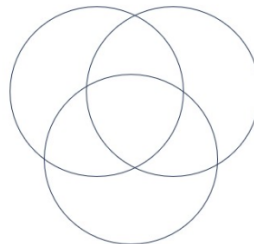
  ii. Give an alternate representation of the regions in the 2 circle and 3 circle Venn Diagrams by labelling each circle with a letter (X, Y, Z, or A, B, C, for example) and then

expressing each region as the result of combining these with set operations (like union, intersection, and set difference).

iii. Here are two attempts at a Venn Diagram with 4 shapes, one with circles and the other with ellipses.
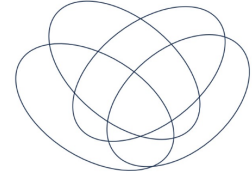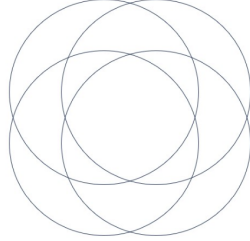
Is there anything missing from either diagram? (How many regions are there? How many regions should there be in order to use each 4 bit binary string exactly once in a generalization of the encoding we saw before?) If you had to choose one of these diagrams, which would you choose, and why?

(This question is adapted from one created by Miles Jones and is used with permission.)

3. Number properties. Consider the predicate $F(\,(a,b)\,)=$ "a is a factor of b" over the domain $\mathbb{Z}^{\neq 0} \times \mathbb{Z}$. Consider the following quantified statements

(i) $\forall x \in \mathbb{Z}\ (F(\,(1,x)\,))$

(ii) $\forall x \in \mathbb{Z}^{\neq 0}\ (F(\,(x,1)\,))$

(iii) $\exists x \in \mathbb{Z}\ (F(\,(1,x)\,))$

(iv) $\exists x \in \mathbb{Z}^{\neq 0}\ (F(\,(x,1)\,))$

(v) $\forall x \in \mathbb{Z}^{\neq 0}\ \exists y \in \mathbb{Z}\ (F(\,(x,y)\,))$

(vi) $\exists x \in \mathbb{Z}^{\neq 0}\ \forall y \in \mathbb{Z}\ (F(\,(x,y)\,))$

(vii) $\forall y \in \mathbb{Z}\ \exists x \in \mathbb{Z}^{\neq 0}\ (F(\,(x,y)\,))$

(viii) $\exists y \in \mathbb{Z}\ \forall x \in \mathbb{Z}^{\neq 0}\ (F(\,(x,y)\,))$

(a) (*Graded for completeness*) Which of the statements (i) - (viii) is being **proved** by the following proof:

> By universal generalization, **choose** e to be an **arbitrary** integer. We need to show that $F(\,(1,e)\,)$. By definition of the predicate F, we can rewrite this goal as $\exists c \in \mathbb{Z}\ (e = c \cdot 1)$. We pick the **witness** $c = e$, which is an integer and therefore in the domain. Calculating, $c \cdot 1 = e \cdot 1 = e$, as required. Since the predicate $F(1,e)$ evaluates to true for the arbitrary integer e, the claim has been proved. $\square$

Hint: it may be useful to identify the key words in the proof that indicate proof strategies.

(b) (*Graded for completeness*) Which of the statements (i) - (viii) is being **disproved** by the following proof:

> To disprove the statement, we need to find a counterexample. We choose 2, a nonzero integer so in the domain. We need to show that $\neg F(\,(2,1)\,)$. By definition of the predicate F, we can rewrite this goal as $1 \bmod 2 \neq 0$. By definition of integer division, since $1 = 0 \cdot 2 + 1$ (and $0 \leq 1 < 2$), $1 \bmod 2 = 1$ which is nonzero so the counterexample works to disprove the original statement. $\square$

Hint: it may be useful to identify the key words in the proof that indicate proof strategies.

(c) (*Graded for correctness of evaluation of statement (is it true or false?) and fair effort completeness of the translation and proof*) Translate the statement to English, state whether is it true or false, and then justify your answer (by proving the statement or its negation).

$$\exists x \in \mathbb{Z}^{\neq 0} \ \exists y \in \mathbb{Z}^{\neq 0} \ (\ \neg(x = y) \wedge F(\ (x, y) \ ) \wedge F(\ (y, x) \ ) \ )$$

(d) (*Graded for correctness of evaluation of statement (is it true or false?) and fair effort completeness of the translation and of the proof*) Translate the statement to English, state whether is it true or false, and then justify your answer (by proving the statement or its negation).

$$\forall x \in \mathbb{Z}^{\neq 0} \ \forall y \in \mathbb{Z}^{\neq 0} \ (\ F(\ (x, y) \ ) \rightarrow \neg F(\ (y, x) \ ) \ )$$

(e) (*Graded for correctness of evaluation of statement (is it true or false?) and fair effort completeness of the translation and of the proof*) Translate the statement to English, state whether is it true or false, and then justify your answer (by proving the statement or its negation).

$$\exists x \in \mathbb{Z}^{\neq 0} \ \exists y \in \mathbb{Z} \ (\ F(\ (x, y) \ ) \wedge F(\ (x + 1, y) \ ) \wedge F(\ (x + 2, y) \ ) \ )$$

(f) (*Graded for correctness of evaluation of statement (is it true or false?) and fair effort completeness of the translation and of the proof*) Translate the statement to English, state whether is it true or false, and then justify your answer (by proving the statement or its negation).

$$\forall x \in \mathbb{Z}^{\neq 0} \ (\ F(\ (x, x^2) \ ) \wedge F(\ (x, x^3) \ ) \ )$$

4. Structural induction. Recall that we define the set of bases as $B = \{\text{A}, \text{C}, \text{U}, \text{G}\}$. The set of RNA strands S is defined (recursively) by:

$$\begin{array}{ll} \text{Basis Step:} & \text{A} \in S, \text{C} \in S, \text{U} \in S, \text{G} \in S \\ \text{Recursive Step:} & \text{If } s \in S \text{ and } b \in B, \text{ then } sb \in S \end{array}$$

where sb is string concatenation. The function *rnalen* that computes the length of RNA strands in S is defined recursively by $rnalen : S \rightarrow \mathbb{Z}^+$

Basis step: If $b \in B$ then $rnalen(b) = 1$

Recursive step: If $s \in S$ and $b \in B$, then $rnalen(sb) = 1 + rnalen(s)$

The function *basecount* that computes the number of a given base b appearing in a RNA strand s is defined recursively:

$$basecount : S \times B \rightarrow \mathbb{N}$$

$$\text{Basis Step:} \quad \text{If } b_1 \in B, b_2 \in B \quad basecount(\ (b_1, b_2) \ ) = \begin{cases} 1 & \text{when } b_1 = b_2 \\ 0 & \text{when } b_1 \neq b_2 \end{cases}$$

$$\text{Recursive Step:} \quad \text{If } s \in S, b_1 \in B, b_2 \in B \quad basecount(\ (sb_1, b_2) \ ) = \begin{cases} 1 + basecount(\ (s, b_2) \ ) & \text{when } b_1 = b_2 \\ basecount(\ (s, b_2) \ ) & \text{when } b_1 \neq b_2 \end{cases}$$

(a) (*Graded for correctness of evaluation of statement (is it true or false?) and fair effort completeness of the translation and proof*) Translate the statement to English, state whether is it true or false, and then justify your answer (by proving the statement or its negation).

$$\forall b \in B \; \exists s \in S \; (\; rnalen(s) = basecount(\; (s, b) \;) \;)$$

(b) (*Graded for correctness of evaluation of statement (is it true or false?) and fair effort completeness of the translation and of the proof*) Translate the statement to English, state whether is it true or false, and then justify your answer (by proving the statement or its negation).

$$\forall s \in S \; (rnalen(s) > basecount(\; (s, \texttt{A}) \;))$$

(c) (*Graded for correctness of evaluation of statement (is it true or false?) and fair effort completeness of the translation and of the proof*) Translate the statement to English, state whether is it true or false, and then justify your answer (by proving the statement or its negation).

$$\forall s \in S \; \forall b \in B \; (basecount(\; (s, b) \;) > 0)$$