HW7 Function and Relations

CSE20F21

Due: Tuesday, November 30, 2021 at 11:00PM on Gradescope

In this assignment,

You will practice determining and justifying whether statements are true in multiple contexts.

Instructions and academic integrity reminders for all homework assignments in CSE20 this quarter are on the class website and on the hw1-definitions-and-notations assignment.

You will submit this assignment via Gradescope (https://www.gradescope.com) in the assignment called "hw7-functions-and-relations".

Resources: To review the topics you are working with for this assignment, see the class material from Weeks 8 and 9. We will post frequently asked questions and our answers to them in a pinned Piazza post.

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 $p \rightarrow q$ 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 $p \rightarrow q$ is true, we can assume $\neg q$ is true and use that assumption to show $\neg p$ is true.

- **Proof of disjuction using equivalent conditional**: To prove that the disjunction $p \vee q$ is true, we can rewrite it equivalently as $\neg p \rightarrow q$ and then use direct proof or contrapositive proof.

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

- **Proof by Structural Induction**: To prove that $\forall x \in X\, P(x)$ where X is a recursively defined set, prove two cases:

Basis Step:	Show the statement holds for elements specified in the basis step of the definition.
Recursive Step:	Show that if the statement is true for each of the elements used to construct new elements in the recursive step of the definition, the result holds for these new elements.

- **Proof by Mathematical Induction**: To prove a universal quantification over the set of all integers greater than or equal to some base integer b:

Basis Step:	Show the statement holds for b.
Recursive Step:	Consider an arbitrary integer n greater than or equal to b, assume (as the **induction hypothesis**) that the property holds for n, and use this and other facts to prove that the property holds for $n + 1$.

- **Proof by Strong Induction** To prove that a universal quantification over the set of all integers greater than or equal to some base integer b holds, pick a fixed nonnegative integer j and then:

Basis Step:	Show the statement holds for b, $b + 1$, $\ldots$, $b + j$.
Recursive Step:	Consider an arbitrary integer n greater than or equal to $b + j$, assume (as the **strong induction hypothesis**) that the property holds for **each of** b, $b + 1$, $\ldots$, n, and use this and other facts to prove that the property holds for $n + 1$.

- **Proof by Contradiction**

  To prove that a statement p is true, pick another statement r and once we show that $\neg p \rightarrow (r \wedge \neg r)$ then we can conclude that p is true.

  Informally The statement we care about can't possibly be false, so it must be true.

Assigned questions

1. Consider the set $U = \mathcal{P}(\mathbb{R})$.

   (a) (*Translation graded for fair effort completeness; Counterexample graded for correctness*) Translate the statement to English and then give a counterexample that could be used to disprove the statement. You do not need to justify your answer. However, if you include clear explanations, we may be able to give partial credit for an answer with some imprecision.

   Note: your counterexample should specify a value for A and a value for B.

   $$\forall A \in U \; \forall B \in U \; (\; (A \subseteq B \rightarrow \neg(\; |A| \geq |B| \;) \;)$$

   (b) (*Translation graded for fair effort completeness; Counterexample graded for correctness*) Translate the statement to English and then give a counterexample that could be used to disprove the statement. You do not need to justify your answer. However, if you include clear explanations, we may be able to give partial credit for an answer with some imprecision.

   Note: your counterexample should specify a value for X and a value for Y.

   $$\forall X \in U \; \forall Y \in U \; (\; X \subseteq \mathbb{Z} \; \wedge \; Y \subseteq \mathbb{Z} \; \rightarrow \; |X| = |Y| \;)$$

   (c) (*Translation graded for fair effort completeness; Witness graded for correctness*) Translate the statement to English and then give a witness that could be used to prove the statement. You do not need to justify your answer. However, if you include clear explanations, we may be able to give partial credit for an answer with some imprecision.

   Note: your witness should specify a value for X and a value for Y.

   $$\exists X \in U \; \exists Y \in U(\; (\; \mathbb{Z} \subseteq X \;) \wedge (\; \mathbb{Z} \subseteq Y \;) \wedge \neg(|X| = |Y|) \;)$$

2. (*Graded for correctness*[1]) The diagonalization argument constructs, for each function $f : \mathbb{N} \rightarrow \mathcal{P}(\mathbb{N})$, a set D_f defined as

   $$D_f = \{x \in \mathbb{N} \mid x \notin f(x)\}$$

   (a) Define a function g such that D_g is a finite nonempty set, or explain why no such function exists.

   (b) Define a function h such that D_h is an infinite set that is a proper subset of $\mathbb{N}$, or explain why no such function exists.

[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.

(c) Define a function k such that D_k is a proper superset of $\mathbb{N}$ (in other words, $\mathbb{N}$ is a proper subset of D_k), or explain why no such function exists.[2]

3. (*Graded for correctness*) For each part of this question, you do not need to justify your answer. However, if you include clear explanations, we may be able to give partial credit for an answer with some imprecision.

(a) Recall that in a movie recommendation system, each user's ratings of movies is represented as a n-tuple (with the positive integer n being the number of movies in the database), and each component of the n-tuple is an element of the collection $\{-1, 0, 1\}$. Assume there are five movies in the database, so that each user's ratings can be represented as a 5-tuple. We call Rt_5 the set of all ratings 5-tuples. Consider the binary relation on the set of all 5-tuples where each component of the 5-tuple is an element of the collection $\{-1, 0, 1\}$:

$G = \{(u, v) \in Rt_5 \times Rt_5 \mid \text{the number of 0s in } u \text{ is the same as the number of 0s in } v\}$

This is an equivalence relation (you do not need to prove this).

Recall that the **equivalence class** of an element $x \in X$ for an equivalence relation $\sim$ on the set X is the set $\{s \in X | (x, s) \in \sim\}$. We write this as $[x]_\sim$.

i. Find a ratings 5-tuple v such that $[v]_G = \{v\}$.

ii. Find distinct ratings 5-tuples u_1, u_2 ($u_1 \neq u_2$) whose equivalence classes $[u_1]_G$ and $[u_2]_G$ have the same size.

iii. Find distinct ratings 5-tuples w_1, w_2 ($w_1 \neq w_2$) whose equivalence classes $[w_1]_G$ and $[w_2]_G$ have different sizes.

(b) Let $S_{1,2}$ be the set of RNA strands of length 1 or 2, formally

$$S_{1,2} = \{s \in S \mid (rnalen(s) = 1) \vee (rnalen(s) = 2)\}$$

Consider the binary relation on $S_{1,2}$ given by

$P = \{(s, s') \in S_{1,2} \times S_{1,2} \mid s \text{ is a prefix of } s',$
namely either $s = s'$ or there is some base b such that $sb = s'\}$

This is a partial ordering (you do not need to prove this).

Draw the Hasse diagram of P.

(c) Consider the set CP of compound propositions that use propositional variables from the set $\{p, q\}$. We define the logical equivalence binary relation on this set by

$$LE = \{(x, y) \in CP \times CP \mid x \equiv y\}$$

This is an equivalence relation (you do not need to prove this).

[2]For sets A and B, when the relation $A \subseteq B$ holds we say that A is a subset of B and that B is a superset of A. Similarly, when the relation $A \subsetneq B$ holds we say that A is a proper subset of B and that B is a proper superset of A.

i. Give two distinct examples of elements in $[\ (p \wedge \neg p)\ ]_{LE}$

ii. Give two distinct examples of elements in $[\ (p \rightarrow q)\ ]_{LE}$

Bonus - not for credit; do not hand in: Prove that G is an equivalence relation on the set of ratings 5-tuples. Prove that P is a partial ordering on $S_{1,2}$. Prove that LE is an equivalence relation on the set of compound propostions that use propositional variables from the set $\{p, q\}$.

4. Imagine you are playing the role of Alice in the Diffie Hellman key agreement (exchange) protocol. You and Bob have agreed to use the prime $p = 7$ and its primitive root $a = 3$. Your secret integer is $k_1 = 3$.

   (a) (*Graded for fair effort completeness*[3]) Calculate the number you send to Bob, a^{k_1} **mod** p. Use the modular exponentiation algorithm for the calculation. Include a trace of the algorithm in your solution.

Modular Exponentation

```
1   procedure modular exponentiation(b: integer;
2                n = (a_{k-1}a_{k-2}...a_1a_0)_2, m: positive integers)
3   x := 1
4   power := b mod m
5   for i:= 0 to k-1
6     if a_i = 1 then x:= (x · power) mod m
7     power := (power · power) mod m
8   return x {x equals b^n mod m}
```

   (b) (*Graded for fair effort completeness*) Bob sends you the number 5. Compute your shared key, $\left(a^{k_2}\right)^{k_1}$ **mod** p. Hint: a^{k_2} **mod** p is what Bob sent you. Include all relevant calculations, annotated with explanations, for full credit.

   (c) (*Graded for fair effort completeness*) What are some possible values for Bob's secret integer? What algorithm are you using to compute them?

[3]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.