# HW7 Function and Relations

CSE20F21

Sample Solutions

**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 $B$.

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

   **Solution**: A translation would be "If $A$ and $B$ are sets of real numbers and $A$ is a subset of $B$ then the size of $A$ is not an upper bound for the size of $B$."

   A counterexample would be $A = \mathbb{N}$ and $B = \mathbb{Z}$. Then $A, B \in U$ and $A \subseteq B$ and $|A| = |B|$ so, in particular, $|A| \geq |B|$.

   (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 $Y$.

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

   **Solution**: A translation would be "Any two sets of integers have the same size."

   A counterexample would be $X = \emptyset$ and $B = \mathbb{Z}$. Then $X, Y \in U$ and $X \subseteq \mathbb{Z}$ and $Y \subseteq \mathbb{Z}$ but $|X| \neq |Y|$ because the only set that has the same size as the empty set is itself, and $\mathbb{Z}$ is not empty.

(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 $Y$.

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

**Solution**: A translation would be "There are two sets of real numbers that each have the set of integers as a subset and that do not have the same size."

A witness would be $X = \mathbb{Z}$ and $Y = \mathbb{R}$. Since every set is a subset of itself and since every integer is a real number, we have $X \in U, Y \in U, \mathbb{Z} \subseteq X, \mathbb{Z} \subseteq Y$. However, by the uncountability of the real numbers (see bottom of page in Week 8 Friday notes), $|X| \neq |Y|$.

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

**Solution**: Consider the function $g : \mathbb{N} \to \mathcal{P}(\mathbb{N})$ given by $g(n) = \{x \in \mathbb{N} \mid x \geq 3\}$, the constant function that always outputs the set of integers greater than or equal to 3. Notice that

$$\begin{aligned} 0 &\notin \{x \in \mathbb{N} \mid x \geq 3\} = g(0) \\ 1 &\notin \{x \in \mathbb{N} \mid x \geq 3\} = g(1) \\ 2 &\notin \{x \in \mathbb{N} \mid x \geq 3\} = g(2) \\ 3 &\in \{x \in \mathbb{N} \mid x \geq 3\} = g(3) \end{aligned}$$

And, generalizing,

$$D_g = \{x \in \mathbb{N} \mid x \notin g(x)\} = \{0, 1, 2\}$$

which is a finite, nonempty set.

(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.

**Solution**: Consider the function $h : \mathbb{N} \to \mathcal{P}(\mathbb{N})$ given by $h(n) = \{0\} \cup \{i \in \mathbb{N} \mid i < n\}$ Notice that

$$\begin{aligned} 0 &\in \{0\} = h(0) \\ 1 &\notin \{0\} = h(1) \\ 2 &\notin \{0, 1\} = h(2) \\ 3 &\notin \{0, 1, 2\} = h(3) \end{aligned}$$

And, generalizing,

$$D_g = \{x \in \mathbb{N} \mid x \notin g(x)\} = \mathbb{Z}^+$$

which is an infinite set that is a proper subset of $\mathbb{N}$.

(c) Define a function $k$ such that $D_k$ is a proper superset of $\mathbb{N}$, or explain why no such function exists.

**Solution**: no such function exists because $D_k$ is defined as

$$D_k = \{x \in \mathbb{N} \mid x \notin k(x)\},$$

which (by set builder notation) is guaranteed to be a subset of $\mathbb{N}$.

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 $\{-1, 0, 1\}$:

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

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 $[v]_G = \{v\}$.
**Solution**: Consider $v = (0, 0, 0, 0, 0)$. This is a ratings 5-tuple and

$$\begin{aligned} [v]_G &= \{s \in Rt_5 \mid (\ (0, 0, 0, 0, 0), s\ ) \in G\} \\ &= \{s \in Rt_5 \mid \text{the number of 0s in } (0, 0, 0, 0, 0) \text{ is the same as in } s\} \\ &= \{s \in Rt_5 \mid s \text{ has five 0s}\} = \{(0, 0, 0, 0, 0)\} \end{aligned}$$

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.
**Solution**: When $u_1$ and $u_2$ have the same number of 0s, they are in the same equivalence class so their equivalence classes have the same size. Consider $u_1 = (0, 0, 1, 1, 0)$ and $u_2 = (-1, 1, 0, 0, 0)$, for example.

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.
**Solution**: When $w_1$ and $w_2$ have different numbers of 0s, they are in different equivalence classes and the sizes of the different classes are all different:

- The equivalence class of all ratings 5-tuples that have 5 zeros has 1 element.
- The equivalence class of all ratings 5-tuples that have 4 zeros has 10 elements.
- The equivalence class of all ratings 5-tuples that have 3 zeros has 40 elements.
- The equivalence class of all ratings 5-tuples that have 2 zeros has 80 elements.
- The equivalence class of all ratings 5-tuples that have 1 zeros has 80 elements.
- The equivalence class of all ratings 5-tuples that have 0 zeros has 32 elements.

We can pick examples that are in different sized classes, like $w_1 = (0, 0, 0, 1, 0)$ and $w_2 = (-1, 1, -1, 1, -1)$, for example.

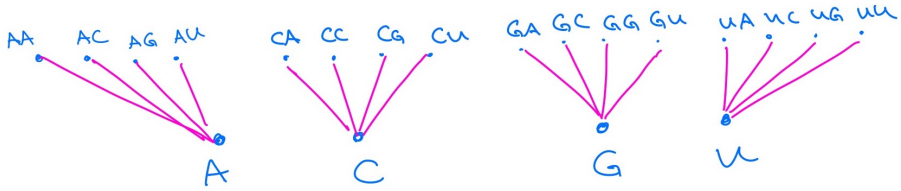
(b) Let $S_{1,2}$ be the set of RNA strands of length 1 or 2, formally

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

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

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

Draw the Hasse diagram of $P$.
**Solution**: The Hasse diagram has 20 nodes and 16 edges. Four nodes are in a single bottom horizontal layer: $A, C, G, U$. Each of these four nodes has an edge to four nodes above it: $A$ has edges to $AA, AC, AG, AU$; $C$ has edges to $CA, CC, CG, CU$; $G$ has edges to $GA, GC, GG, GU$; $U$ has edges to $UA, UC, UG, UU$.




(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

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

i. Give two distinct examples of elements in $[\ (p \wedge \neg p)\ ]_{LE}$
**Solution**: Since every element is in its own equivalence class, $(p \wedge \neg p)$ is one example. A different, logically equivalent, compound proposition is $(q \wedge \neg q)$. Alternatively, we can consider $(p \leftrightarrow \neg p)$.

ii. Give two distinct examples of elements in $[\ (p \rightarrow q)\ ]_{LE}$
**Solution**: Since every element is in its own equivalence class, $(p \rightarrow q)$ is one example. A different, logically equivalent, compound proposition is $(\neg p \vee q)$. Alternatively, we can consider $\neg(p \wedge \neg q)$.

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*[2]) 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}
```

**Solution**: Trace of $3^3$ **mod** 7.

modular exponentiation( b=3, n=3=(11)$_2$, m=7 )
$a_1 a_0$, $k=2$

| X | power | i | $a_i$ |
|---|---|---|---|
| 1 | 3 | 0 | 1 |
| $(1 \cdot 3) \bmod 7 = 3$ | $(3 \cdot 3) \bmod 7 = 2$ | 1 | 1 |
| $(3 \cdot 2) \bmod 7 = 6$ | $(2 \cdot 2) \bmod 7 = 4$ | | |

return 6

Gives 6.

[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.

*Supporting calculations*:

$$3 = 0 \cdot 7 + 3 \text{ so } 3 \textbf{ mod } 7 = 3$$
$$9 = 1 \cdot 7 + 2 \text{ so } 9 \textbf{ mod } 7 = 2$$
$$6 = 0 \cdot 7 + 6 \text{ so } 6 \textbf{ mod } 7 = 6$$
$$4 = 0 \cdot 7 + 4 \text{ so } 4 \textbf{ mod } 7 = 4$$

(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.

**Solution**: We calculate $5^{k_1}$ **mod** $p = 5^3$ **mod** $7 = 6$

modular exponentiation( $\overset{b}{5}$ , $\overset{n}{3} = \overset{a_1 a_0}{(11)_2}$ , $\overset{m}{7}$ )
$k = 2$

| X | power | i | $a_i$ |
|---|---|---|---|
| 1 | 5 | 0 | 1 |
| $(1 \cdot 5) \bmod 7 = 5$ | $(5 \cdot 5) \bmod 7 = 4$ | 1 | 1 |
| $(5 \cdot 4) \bmod 7 = 6$ | $(4 \cdot 4) \bmod 7 = 2$ | | |

return 6

*Supporting calculations*:

$$5 = 0 \cdot 7 + 5 \text{ so } 5 \textbf{ mod } 7 = 5$$
$$25 = 3 \cdot 7 + 4 \text{ so } 25 \textbf{ mod } 7 = 5$$
$$20 = 2 \cdot 7 + 6 \text{ so } 20 \textbf{ mod } 7 = 6$$
$$16 = 2 \cdot 7 + 2 \text{ so } 16 \textbf{ mod } 7 = 2$$

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

**Solution**: We need to find integers such that $3^{k_2}$ **mod** $7 = 5$. We can calculate all the remainders of powers of 3, mod 7:

- $3^0$ **mod** $7 = 1$

- $3^1 \textbf{ mod } 7 = 3$
- $3^2 \textbf{ mod } 7 = 2$
- $3^3 \textbf{ mod } 7 = 6$
- $3^4 \textbf{ mod } 7 = 4$
- $3^5 \textbf{ mod } 7 = 5$
- $3^6 \textbf{ mod } 7 = 1$

and then we notice that the results cycle back. Thus, possible exponents that yield 5 are 5, 11, 17, etc.