**National University of Singapore**
**Department of Computer Science**

**2021/22 (Sem.1)** **CS1231 Discrete Structures** **Tutorial 6**

1. Let $X = \{a, b, c\}$ and $Y = \{1, 2, 3, 4\}$.

   (a) For each of the following statements, give an example of a relation $f \subseteq X \times Y$ that satisfies it.

   (i) $\exists x \in X\ \forall y \in Y\ (x, y) \in f$.

   (ii)* $\exists y \in Y\ \forall x \in X\ (x, y) \in f$.

   (iii)* $\forall y \in Y\ \exists x \in X\ (x, y) \in f$.

   (iv) $\forall x_1 \in X\ \forall x_2 \in X\ \forall y \in Y\ x_1 \neq x_2 \rightarrow \big((x_1, y) \notin f \vee (x_2, y) \notin f\big)$.

   (b) Are your examples in (a) functions?

2. Let $A$ and $B$ be nonempty subsets of $C$, where $C = \{-4, -3, -2, -1, 0, 1, 2, 3, 4\}$.
   Define $R = \{(x, y) \in A \times B : y = x^2 - 1\}$.

   (a) Suppose $A = \{-2, -1, 0, 1, 2\}$ and $B = \{0, 1, 2, 3\}$. Is $R$ a function $A \rightarrow B$?

   (b) Suppose $A = \{-2, -1, 0, 1, 2\}$.
   Give an example of $B$ such that $B \subseteq C$ and $R$ is a surjective function $A \rightarrow B$.

   (c) Suppose $B = \{0, 1, 2, 3\}$.
   Give an example of $A$ such that $A \subseteq C$ and $R$ is an injective function $A \rightarrow B$.

3. Recall that saying a function $f\colon X \rightarrow Y$ is *injective* means

   "for all $x_1$ and $x_2$ in $X$, $x_1 = x_2$ if $f(x_1) = f(x_2)$".

   Explain the difference (if any) between this condition and

   (a)* "for any $x_1$ and $x_2$ in $X$, $f(x_1) = f(x_2)$ whenever $x_1 = x_2$";

   (b)* "for every $x_1$ and $x_2$ in $X$, $f(x_1) \neq f(x_2)$ whenever $x_1 \neq x_2$";

   (c) "there are no elements $x_1$ and $x_2$ in $X$ such that $x_1 \neq x_2$ and $f(x_1) = f(x_2)$";

   (d) "$x_1 \neq x_2$ and $f(x_1) = f(x_2)$ for some $x_1$ and $x_2$ in $X$".

4. Recall that saying a function $f\colon X \rightarrow Y$ is *surjective* means

   "given any $y$ in $Y$, there is an $x$ in $X$ such that $y = f(x)$".

   Explain the difference (if any) between this condition and

   (a)* "for every $x$ in $X$, there is $y$ in $Y$ such that $y = f(x)$";

   (b)* "there is $x$ in $X$ such that $y = f(x)$ for any $y$ in $Y$";

   (c)* "there is some $y$ in $Y$ such that $y = f(x)$ for some $x$ in $X$";

   (d) "there is some $y$ in $Y$ such that $y = f(x)$ for any $x$ in $X$";

   (e) "there is no $y$ in $Y$ such that $y \neq f(x)$ for any $x$ in $X$".

5.* Consider the sets $Y, Z$ and the relation $R$ from Tutorial 4 Problem 5. Give an example of a subset $g \subseteq R$ such that $g$ is a function $Y \rightarrow Z$ but it is neither injective nor surjective.

6. Consider the functions $f$ and $g$ from $\mathbb{Z}$ to $\mathbb{Z}$ defined by setting $f(n) = 2n$ and $g(n) = \lfloor \frac{n}{2} \rfloor$ for all $n \in \mathbb{Z}$. Which of the functions $f$, $g$, $g \circ f$, $f \circ g$, $f \circ f$ are injective? Which are surjective? Determine the range of each of the two functions.

7. Define Boolean functions $f$ and $g$ from $\{\mathrm{T},\mathrm{F}\}^3$ to $\{\mathrm{T},\mathrm{F}\}$ so that, for all $p$, $q$ and $r$ in $\{\mathrm{T},\mathrm{F}\}$,

   (i)* $f(p,q,r) = (p \wedge q) \vee r$; (ii) $g(p,q,r) = (p \vee q) \rightarrow {\sim}r$.

   (a) Draw arrow diagrams for $f$ and $g$.

   (b) Using only $\sim$ and $\wedge$, define Boolean functions $f^*$ and $g^*$ such that $f = f^*$ and $g = g^*$.

   (c) Let $Q$ is a Boolean expression with $n$ statement variables. Suppose the Boolean function $f\colon \{\mathrm{T},\mathrm{F}\}^n \rightarrow \{\mathrm{T},\mathrm{F}\}$ representing $Q$ is not surjective. What can you say about $Q$?

8. Let $X$ and $Y$ be sets and let $f\colon X \rightarrow Y$ and $g\colon Y \rightarrow X$ such that $g \circ f = \mathrm{id}_X$. Prove that if $f$ is surjective, then $g$ is injective.

9.* Let $X$ be a nonempty set. Consider any surjective function $f\colon \mathbb{Z}_{\geqslant 0} \rightarrow X$. Define a function $g\colon X \rightarrow \mathbb{Z}_{\geqslant 0}$ such that $g(x)$ is the smallest integer $n$ such that $f(n) = x$ for all $x \in X$. Show that $g$ is well defined, i.e., show that

$$\{(x,n) \in X \times \mathbb{Z}_{\geqslant 0} : n \text{ is the smallest integer such that } f(n) = x\} \text{ is a function } X \rightarrow \mathbb{Z}_{\geqslant 0}.$$

   What is $f \circ g$? Is $g \circ f = \mathrm{id}_{\mathbb{Z}_{\geqslant 0}}$?

10.* The concept of an inverse function is central to cryptography.

   (a) Julius Caesar used a cipher that encrypts the message "attack today" as "dwwdfn wrgdb". Define an encryption function $E$ and its decryption function $D$ (i.e., $E^{-1}$) for this cipher.

   (b) The Caesar cipher is easy to break. It can be strengthened with a *key*. For example, if the key is "coolcat", we drop the repeated letters to get "colat", then use it and the rest of the alphabet to construct a rectangle:

| | | | | |
|---|---|---|---|---|
| c | o | l | a | t |
| b | d | e | f | g |
| h | i | j | k | m |
| n | p | q | r | s |
| u | v | w | x | y |
| z | | | | |

   This rectangle can be used to define encryption and decryption functions so that "attack today" is encrypted as "crrchv rqncs". Define $D$ and $E$ for this cipher.
   (The difference now is: Even if you know the encryption method, you still need to know the key to do the decryption; thus $D$ and $E$ here are functions $D_{\text{coolcat}}$ and $E_{\text{coolcat}}$ that depend on the key "coolcat".)

   (c) Actually, we don't need $D = E^{-1}$; we just need $D(E(x)) = x$ for all $x$. Construct two functions $f\colon X \rightarrow Y$ and $g\colon Y \rightarrow X$ such that $g \circ f = \mathrm{id}_X$ but $f \circ g \neq \mathrm{id}_Y$.

11. We will prove that all students have the same sex.

   **Claim.** There is only one sex among any group of $n$ students, for any positive integer $n$.

   *Proof.* By induction on $n$.
   Basis $n = 1$: Since there is only 1 student, there is only 1 sex.
   Induction Hypothesis: Suppose the claim is true if $n = k$, where $k \geqslant 1$.
   Induction Step: Consider any set $S$ of $k+1$ students. Remove one student $x$, so $S \setminus \{x\}$ has $k$ students. By the induction hypothesis, all students in $S \setminus \{x\}$ have the same sex. Now put back the student and remove another student $y$, so $S \setminus \{y\}$ has $k$ students. Again, all students in $S \setminus \{y\}$ have the same sex.

   Thus $x$ and $y$ have the same sex as students in $S \setminus \{x,y\}$, so all students in $S$ have the same sex. □

   What's wrong with this "proof"?

   [The point here is: You can "prove" nonsense with bad logic, even if you stick to the structure provided by a proof technique.]