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

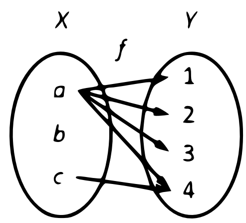
   (iv) $\forall x_1 \in X\ \forall x_2 \in X\ \forall y \in Y\ x_1 \neq x_2 \rightarrow \big((x_1, y) \notin f \vee (x_2, y) \notin f\big)$.

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

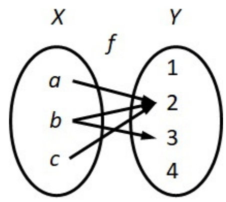
Solution:

(a) There are infinitely many correct answers for each part.

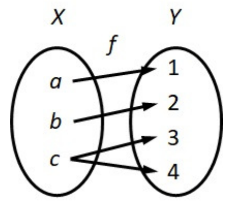
(i) $\exists x \in X\ \forall y \in Y\ (x, y) \in f$.
$f = \{(a, 1), (a, 2), (a, 3), (a, 4), (c, 4)\}$.



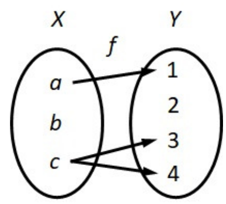
(ii)* $\exists y \in Y\ \forall x \in X\ (x, y) \in f$.
$f = \{(a, 2), (b, 2), (b, 3), (c, 2)\}$.



(iii)* $\forall y \in Y\ \exists x \in X\ (x, y) \in f$.
$f = \{(a, 1), (b, 2), (c, 3), (c, 4)\}$.



(iv) $\forall x_1 \in X\ \forall x_2 \in X\ \forall y \in Y\ x_1 \neq x_2 \rightarrow \big((x_1, y) \notin f \vee (x_2, y) \notin f\big)$.
$f = \{(a, 1), (c, 3), (c, 4)\}$.



(b) All the f's above are not functions.

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

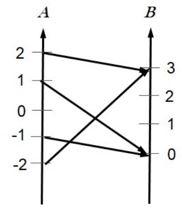
(a) Suppose $A = \{-2, -1, 0, 1, 2\}$ and $B = \{0, 1, 2, 3\}$. Is R a function $A \to B$?

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

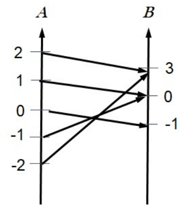
(c) Suppose $B = \{0, 1, 2, 3\}$.
Give an example of A such that $A \subseteq C$ and R is an injective function $A \to B$.

Solution: $C = \{-4, -3, -2, -1, 0, 1, 2, 3, 4\}$, $A \subseteq C$, $B \subseteq C$, and $R = \{(x, y) \in A \times B : y = x^2 - 1\}$.

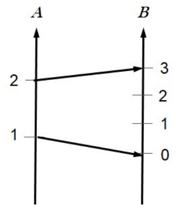
(a) $A = \{-2, -1, 0, 1, 2\}$,
$B = \{0, 1, 2, 3\}$.
Not a function, since
$(0, y) \notin R$ for any $y \in B$.



(b) $A = \{-2, -1, 0, 1, 2\}$.
Setting $B = \{-1, 0, 3\}$ makes
f a surjective function $A \to B$.
No other choice of B works.



(c) $B = \{0, 1, 2, 3\}$.
Setting $A = \{1, 2\}$ makes
f an injective function $A \to B$.
Alternatives: $A = \varnothing$, $A = \{-1\}$, etc.



3. Recall that saying a function $f\colon X \to Y$ 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".

Solution: injective function: $\forall x_1 \in X\ \forall x_2 \in X\ f(x_1) = f(x_2) \to x_1 = x_2$

(a)* "for any x_1 and x_2 in X, $f(x_1) = f(x_2)$ whenever $x_1 = x_2$"
$\forall x_1 \in X\ \forall x_2 \in X\ x_1 = x_2 \to f(x_1) = f(x_2)$ — converse (**not** equivalent)
This statement is true for all functions f: if $x_1 = x_2$, then of course $f(x_1) = f(x_2)$.

(b)* "for every x_1 and x_2 in X, $f(x_1) \neq f(x_2)$ whenever $x_1 \neq x_2$"
$\forall x_1 \in X\ \forall x_2 \in X\ x_1 \neq x_2 \to f(x_1) \neq f(x_2)$ — contrapositive (equivalent)

(c) "there are no elements x_1 and x_2 in X such that $x_1 \neq x_2$ and $f(x_1) = f(x_2)$"
$\sim\exists x_1 \in X\ \exists x_2 \in X\ x_1 \neq x_2 \wedge f(x_1) = f(x_2)\ \equiv\ \forall x_1 \in X\ \forall x_2 \in X\ x_1 = x_2 \vee f(x_1) \neq f(x_2)$
$\equiv\ \forall x_1 \in X\ \forall x_2 \in X\ f(x_1) = f(x_2) \to x_1 = x_2$ — equivalent

(d) "$x_1 \neq x_2$ and $f(x_1) = f(x_2)$ for some x_1 and x_2 in X"
$\exists x_1 \in X\ \exists x_2 \in X\ x_1 \neq x_2 \wedge f(x_1) = f(x_2)$ — negation (**not** equivalent)

4. Recall that saying a function $f\colon X \to Y$ 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".

Solution: surjective function: $\forall y \in Y\ \exists x \in X\ y = f(x)$

(a)* "for every x in X, there is y in Y such that $y = f(x)$"
$\forall x \in X\ \exists y \in Y\ y = f(x)$ — **not** equivalent
(Actually, this is F1. So it is satisfied by all function, but not all functions are surjective.)

(b)* "there is x in X such that $y = f(x)$ for any y in Y"
$\exists x \in X\ \forall y \in Y\ y = f(x)$ — **not** equivalent
(For example, $\mathrm{id}_{\{1,2\}}$ is a surjective function, but it does not satisfy this condition.)

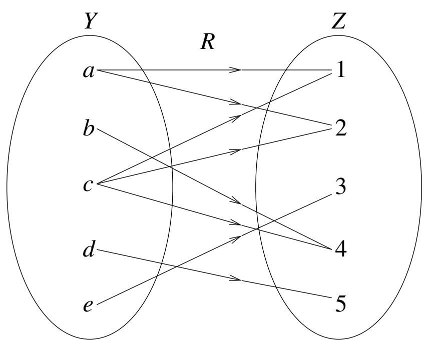
(c)* "there is some y in Y such that $y = f(x)$ for some x in X"
$\exists y \in Y\ \exists x \in X\ y = f(x)$ — **not** equivalent
(For example, the function $f\colon \{1\} \to \{0,1\}$ satisfying $f(1) = 1$ is not surjective, but it satisfies this condition.)

(d) "there is some y in Y such that $y = f(x)$ for any x in X"
$\exists y \in Y\ \forall x \in X\ y = f(x)$ — **not** equivalent
(For example, the function $f\colon \{1\} \to \{0,1\}$ satisfying $f(1) = 1$ is not surjective, but it satisfies this condition.)

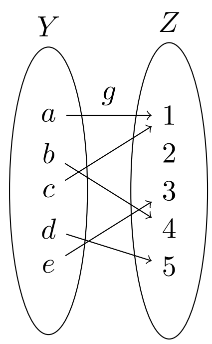
(e) "there is no y in Y such that $y \neq f(x)$ for any x in X"
$\sim\exists y \in Y\ \forall x \in X\ y \neq f(x)\ \equiv\ \forall y \in Y\ \exists x \in X\ y = f(x)$ — equivalent

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 $Y \to Z$ but it is neither injective nor surjective.

Solution:

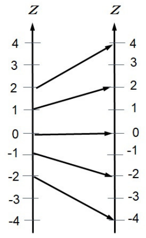


For example, the arrow diagram on the right represents a function $g\colon Y \to Z$ that is neither injective nor surjective.



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.

Solution:



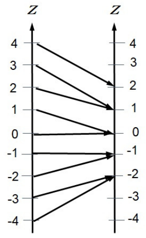
f

<u>inj.</u>

$f(n) = f(k)$
$\Rightarrow 2n = 2k$
$\Rightarrow n = k$

<u>not</u> surj.

$f(n) \neq 1$
for any $n \in \mathbb{Z}$



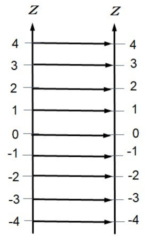
g

<u>not</u> inj.

$g(0) = 0$
$= g(1)$

<u>surj.</u>

Given $y \in \mathbb{Z}$,
let $x = 2y$;
then
$g(x) = \lfloor \frac{x}{2} \rfloor$
$= \lfloor y \rfloor$
$= y$



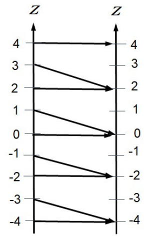
$g \circ f$

<u>inj.</u>

$(g \circ f)(n) = (g \circ f)(k)$
$\Rightarrow g(2n) = g(2k)$
$\Rightarrow \lfloor \frac{2n}{2} \rfloor = \lfloor \frac{2k}{2} \rfloor$
$\Rightarrow n = k$

<u>surj.</u>

Given $y \in \mathbb{Z}$,
let $x = y$;
then
$(g \circ f)(x) = g(f(x))$
$= g(2x) = \lfloor \frac{2x}{2} \rfloor = x$



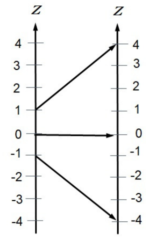
$f \circ g$

<u>not</u> inj.

$(f \circ g)(0) = 0$
$= (f \circ g)(1)$

<u>not</u> surj.

$(f \circ g)(n) \neq 1$
for any $n \in \mathbb{Z}$



$f \circ f$

<u>inj.</u>

$(f \circ f)(n) = (f \circ f)(k)$
$\Rightarrow f(2n) = f(2k)$
$\Rightarrow 4n = 4k$
$\Rightarrow n = k$

<u>not</u> surj.

$(f \circ f)(n) \neq 1$
for any $n \in \mathbb{Z}$

range$(f) = \{2n : n \in \mathbb{Z}\}$, range$(g) = \mathbb{Z}$, range$(g \circ f) = \mathbb{Z}$,
range$(f \circ g) = \{2n : n \in \mathbb{Z}\}$, range$(f \circ f) = \{4n : n \in \mathbb{Z}\}$.

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) $g(p,q,r) = (p \vee q) \rightarrow {\sim}r$.

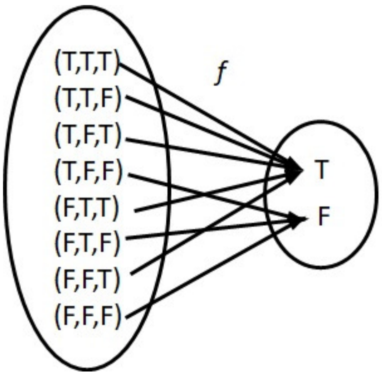
(a) Draw arrow diagrams for f and g.

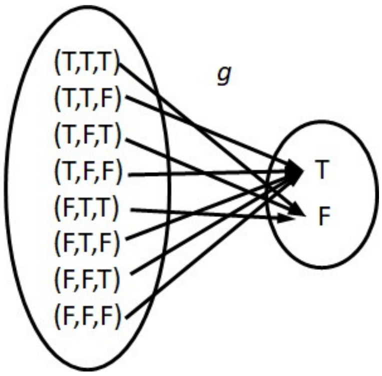
(b) Using only $\sim$ and $\wedge$, define Boolean functions f^* and g^* such that $f = f^*$ and $g = g^*$.

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

Solution:

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





(b) (i) $(p \wedge q) \vee r \equiv {\sim}{\sim}((p \wedge q) \vee r) \equiv {\sim}({\sim}(p \wedge q) \wedge {\sim}r) \stackrel{\text{def}}{=\!=} f^*(p,q,r)$

(ii) $(p \vee q) \rightarrow {\sim}r \equiv {\sim}{\sim}(({\sim}p \wedge {\sim}q) \vee {\sim}r) \equiv {\sim}({\sim}({\sim}p \wedge {\sim}q) \wedge r) \stackrel{\text{def}}{=\!=} g^*(p,q,r)$

(c) Since f is not surjective, either $\forall \alpha \in \{\mathrm{T},\mathrm{F}\}^n\ f(\alpha) = \mathrm{T}$ or $\forall \alpha \in \{\mathrm{T},\mathrm{F}\}^n\ f(\alpha) = \mathrm{F}$, i.e., either Q is a tautology, or Q is a contradiction.

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

Solution: Assume f is surjective. Suppose $y_1, y_2 \in Y$ such that $g(y_1) = g(y_2)$.
Use the surjectivity of f to find $x_1, x_2 \in X$ such that $y_1 = f(x_1)$ and $y_2 = f(x_2)$. Then

$$x_1 = \mathrm{id}_X(x_1) = (g \circ f)(x_1) = g(f(x_1)) = g(y_1) = g(y_2) = g(f(x_2)) = (g \circ f)(x_2) = \mathrm{id}_X(x_2) = x_2.$$

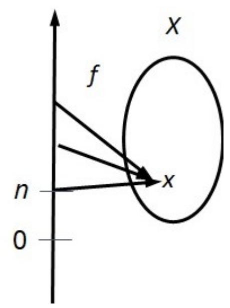
So $y_1 = f(x_1) = f(x_2) = y_2$.
Since $g(y_1) = g(y_2)$ implies $y_1 = y_2$ for all $y_1, y_2 \in Y$, we know that g is injective.

9.* Let X be a nonempty set. Consider any surjective function $f\colon \mathbb{Z}_{\geqslant 0} \to X$. Define a function $g\colon X \to \mathbb{Z}_{\geqslant 0}$ 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

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

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

Solution: A surjective function $f\colon \mathbb{Z}_{\geqslant 0} \to X$,
$g = \{(x, n) \in X \times \mathbb{Z}_{\geqslant 0} : n \text{ is the smallest integer such that } f(n) = x\}$.



Let $x \in X$. Define $N_x = \{n \in \mathbb{Z}_{\geqslant 0} : f(n) = x\}$.
Note that $N_x \subseteq \mathbb{Z}$. Since f is surjective, $N_x \neq \varnothing$.
Also N_x is bounded below by 0, i.e., $\forall n \in N_x\ n \geqslant 0$.
By the Well-Ordering Principle, N_x has a smallest element.
Let n_x be this smallest element, so that $\forall n \in N_x\ n \geqslant n_x$.
Then $(x, n_x) \in g$.
(F1: $\forall x \in X\ \exists n_x \in \mathbb{Z}_{\geqslant 0}\ (x, n_x) \in g$.)

Suppose $(x, n_x) \in g$ and $(x, n_x^*) \in g$.
Then $f(n_x) = x$ and $f(n_x^*) = x$ by the definition of g.
Also $n_x \geqslant n_x^*$ and $n_x^* \geqslant n_x$ by the definition of g. Thus $n_x = n_x^*$.
(F2: $\forall x \in X\ \forall n_x \in \mathbb{Z}_{\geqslant 0}\ \forall n_x^* \in \mathbb{Z}_{\geqslant 0}\ (x, n_x) \in g \wedge (x, n_x^*) \in g \to n_x = n_x^*$.)

Hence g is a function.
Moreover, for any $x \in X$, if we let $g(x) = n_x$, then $f(n_x) = x$ by the definition of g, and so $(f \circ g)(x) = f(g(x)) = f(n_x) = x = \mathrm{id}_X(x)$. Thus $f \circ g = \mathrm{id}_X$.

These demonstrate how one can construct an "inverse" g for any surjective function $f\colon \mathbb{Z}_{\geqslant 0} \to X$, in the sense that $f \circ g = \mathrm{id}_X$.
However, the following shows that this "inverse" may not satisfy $g \circ f = \mathrm{id}_{\mathbb{Z}_{\geqslant 0}}$.

Consider any f that is not injective.
(For example, one can take $f\colon \mathbb{Z}_{\geqslant 0} \to \mathbb{Z}_{\geqslant 0}$ where $f(n) = \lfloor \frac{n}{2} \rfloor$ for all $n \in \mathbb{Z}_{\geqslant 0}$.)
Take $n, n^* \in \mathbb{Z}_{\geqslant 0}$ such that $n \neq n^*$ and $f(n) = f(n^*) = x$, say. If $g \circ f = \mathrm{id}_{\mathbb{Z}_{\geqslant 0}}$, then

$$n = \mathrm{id}_{\mathbb{Z}_{\geqslant 0}}(n) = (g \circ f)(n) = g(f(n)) = g(x) = g(f(n^*)) = (g \circ f)(n^*) = \mathrm{id}_{\mathbb{Z}_{\geqslant 0}}(n^*) = n^*,$$

contradicting $n \neq n^*$. Therefore, $g \circ f \neq \mathrm{id}_{\mathbb{Z}_{\geqslant 0}}$ if f is not injective.

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:

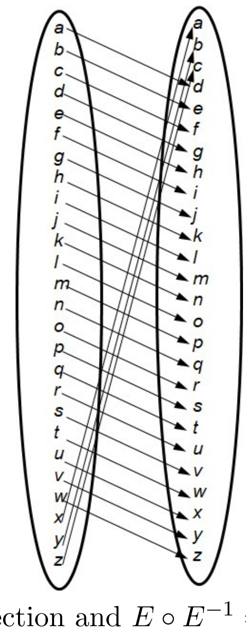
c	o	l	a	t
b	d	e	f	g
h	i	j	k	m
n	p	q	r	s
u	v	w	x	y
z				

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_{coolcat} and E_{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 $f\colon X \to Y$ and $g\colon Y \to X$ such that $g \circ f = \mathrm{id}_X$ but $f \circ g \neq \mathrm{id}_Y$.

Solution:

(a) The following is an arrow diagram for E:



This E is bijective. So E^{-1} is a bijection and $E \circ E^{-1} = \mathrm{id} = E^{-1} \circ E$.

(b) Define $E(\alpha) = \beta$ and $D(\beta) = \alpha$, whenever α and β are in the same position in the respective tables below.

α

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

$\xrightarrow{E}$

β

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				

(c) In Problem 6, $g \circ f = \mathrm{id}_X$, but $f \circ g \neq \mathrm{id}_Y$. So $g \neq f^{-1}$. (In fact, f^{-1} is not a function.)

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.]

Error: $S \setminus \{x, y\}$ may be empty, i.e., the argument fails when S has exactly 2 students.
Indeed, the induction step is bogus when S consists of one male and one female.