Recap and announcements

Section A3: Relations and functions (cont)

Properties of functions: injective

Let $f : A \to B$ be a function. We say that f is **one-to-one** or f is **injective** or f is an **injection** when

$$\forall a_1, a_2 \in A \; (a_1 \neq a_2) \Rightarrow (f(a_1) \neq f(a_2))$$

So f is injective if whenever the inputs are different, the outputs are different.

When proving that a function is injective, it is often easier to prove the contrapositive; that is

$$\forall a_1, a_2 \in A \; (f(a_1) = f(a_2)) \Rightarrow (a_1 = a_2)$$

EXAMPLE: Let $f : \mathbb{N} \to \mathbb{N}$ be defined by $f(n) = n^2$. Is f injective?

EXAMPLE: Let $f : \mathbb{N} \to \mathbb{N}$ be defined by $f(n) = n^2$. Is f injective?

A: Yes. To show this we follow three steps:

1. Clearly identify the logical structure of the statement to be proved
2. Write the structural part of a proof that responds to the logical structure of the statement
3. Try to complete “the middle” of the proof.

EXAMPLE: Let $f : \mathbb{N} \to \mathbb{N}$ be defined by $f(n) = n^2$. Is f injective?

A: Yes. To show this we show that

$$\forall n_1, n_2 \in \mathbb{N} \;\; ((f(n_1) = f(n_2)) \Rightarrow (n_1 = n_2)).$$

EXAMPLE: Let $f : \mathbb{N} \to \mathbb{N}$ be defined by $f(n) = n^2$. Is f injective?

A: Yes. To show this we show that

$$\forall n_1, n_2 \in \mathbb{N} \ \ ((f(n_1) = f(n_2)) \Rightarrow (n_1 = n_2)).$$

Let $n_1, n_2 \in \mathbb{N}$**. Suppose that** $f(n_1) = f(n_2)$**.**

Hence $n_1 = n_2$**.** $\square$

EXAMPLE: Let $f : \mathbb{N} \to \mathbb{N}$ be defined by $f(n) = n^2$. Is f injective?

A: Yes. To show this we show that

$$\forall n_1, n_2 \in \mathbb{N} \ \ ((f(n_1) = f(n_2)) \Rightarrow (n_1 = n_2)).$$

Let $n_1, n_2 \in \mathbb{N}$**. Suppose** $f(n_1) = f(n_2)$**.** Then

$$\begin{aligned} & f(n_1) = f(n_1) \\ \Rightarrow & n_1^2 = n_2^2 \\ \Rightarrow & n_1^2 - n_2^2 = 0 \\ \Rightarrow & (n_1 - n_2)(n_1 + n_2) = 0 \\ \Rightarrow & (n_1 - n_2) = 0 \vee (n_1 + n_2) = 0 \\ & \text{(When a product is zero, one of the factors must be zero.)} \end{aligned}$$

Since n_1, n_2 are both positive, $n_1 + n_2 > 0$. It follows that $n_1 - n_2 = 0$.
Hence $n_1 = n_2$**.** $\square$

EXAMPLE: Let $g : \mathbb{Z} \to \mathbb{Z}$ be defined by $g(n) = n^2$. Is g injective?

EXAMPLE: Let $g : \mathbb{Z} \to \mathbb{Z}$ be defined by $g(n) = n^2$. Is g injective?

A: No. Let's plan...

EXAMPLE: Let $g : \mathbb{Z} \to \mathbb{Z}$ be defined by $g(n) = n^2$. Is g injective?

A: No. Let's plan...
We want to disprove

$$\forall n_1, n_2 \in \mathbb{Z} \ \ ((f(n_1) = f(n_2)) \Rightarrow (n_1 = n_2)).$$

Thus we wish to prove:

$$\begin{aligned} &\neg\forall n_1, n_2 \in \mathbb{Z} \ \ ((f(n_1) = f(n_2)) \Rightarrow (n_1 = n_2) \\ \equiv &\exists n_1, n_2 \in \mathbb{Z} \ \ \neg((f(n_1) = f(n_2)) \Rightarrow (n_1 = n_2) \\ \equiv &\exists n_1, n_2 \in \mathbb{Z} \ \ ((f(n_1) = f(n_2)) \wedge \neg(n_1 = n_2) \\ \equiv &\exists n_1, n_2 \in \mathbb{Z} \ \ ((f(n_1) = f(n_2)) \wedge (n_1 \neq n_2) \end{aligned}$$

Therefore, to show that g is not injective, we need to exhibit two different inputs that give the same output. Now, let's write our answer.

EXAMPLE: Let $g : \mathbb{Z} \to \mathbb{Z}$ be defined by $g(n) = n^2$. Is g injective?

A: No. Since $g(2) = g(-2) = 4$, g is not injective.

Properties of functions: surjective

Let $f : A \to B$ be a function. We say that f is **onto** or f **maps onto** B or f is **surjective** or f is a **surjection** when

$$\forall b \in B \; \exists a \in A \; f(a) = b.$$

So f is surjective when its codomain and range are equal; f is surjective when every element of the codomain is an actual output of the function).

EXAMPLE: Let $h : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ be defined by $h(n) = (n, n+1)$. Is h surjective?

EXAMPLE: Let $h : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ be defined by $h(n) = (n, n+1)$. Is h surjective?

A: No. We note that $(1, 4)$ is not of the form $(n, n+1)$. Since $(1, 4)$ is in the codomain, but no input maps to $(1, 4)$, h is not surjective.

EXAMPLE: Let $j : \mathbb{N} \to \mathbb{Z}$ defined by

$$j(n) = \begin{cases} \frac{n}{2} - 1 & \text{if } n \text{ is even,} \\ \frac{-(n+1)}{2} & \text{if } n \text{ is odd.} \end{cases}$$

Is j surjective?

EXAMPLE: Let $j : \mathbb{N} \to \mathbb{Z}$ defined by

$$j(n) = \begin{cases} \frac{n}{2} - 1 & \text{if } n \text{ is even,} \\ \frac{-(n+1)}{2} & \text{if } n \text{ is odd.} \end{cases}$$

Is j surjective?

Plan:

1. We identify the logical structure of the statement to be considered.
2. We consider its negation.
3. We decide whether we want to prove the statement or its negation. To do this, we try inputting some values from the domain to see what happens.
4. Write the structural part of a proof that responds to the logical structure of what we are proving.
5. Try to complete "the middle" of the proof.

EXAMPLE: Let $j : \mathbb{N} \to \mathbb{Z}$ defined by

$$j(n) = \begin{cases} \frac{n}{2} - 1 & \text{if } n \text{ is even,} \\ \frac{-(n+1)}{2} & \text{if } n \text{ is odd.} \end{cases}$$

Is j surjective?

EXAMPLE: Let $j : \mathbb{N} \to \mathbb{Z}$ defined by

$$j(n) = \begin{cases} \frac{n}{2} - 1 & \text{if } n \text{ is even,} \\ \frac{-(n+1)}{2} & \text{if } n \text{ is odd.} \end{cases}$$

Is j surjective?

The statement is

$$\forall z \in \mathbb{Z} \;\; \exists n \in \mathbb{N} \;\; j(n) = z.$$

Its negation has the form

$$\exists z \in \mathbb{Z} \;\; \forall n \in \mathbb{N} \;\; j(n) \neq z.$$

First compute $j(1), j(2), j(3), j(4), \ldots$ to build intuition for what the function does...

$$j(1) = -1, j(2) = 0, j(3) = -2, j(4) = 1, j(5) = -3, j(6) = 2, \ldots$$

decide we will prove the original statement.

EXAMPLE: Let $j : \mathbb{N} \to \mathbb{Z}$ defined by

$$j(n) = \begin{cases} \frac{n}{2} - 1 & \text{if } n \text{ is even,} \\ \frac{-(n+1)}{2} & \text{if } n \text{ is odd.} \end{cases}$$

Is j surjective?

EXAMPLE: Let $j : \mathbb{N} \to \mathbb{Z}$ defined by

$$j(n) = \begin{cases} \frac{n}{2} - 1 & \text{if } n \text{ is even,} \\ \frac{-(n+1)}{2} & \text{if } n \text{ is odd.} \end{cases}$$

Is j surjective?

A: Yes. **Let $z \in \mathbb{Z}$.**

Hence there exists an input that maps to z.

EXAMPLE: Let $j : \mathbb{N} \to \mathbb{Z}$ defined by

$$j(n) = \begin{cases} \frac{n}{2} - 1 & \text{if } n \text{ is even,} \\ \frac{-(n+1)}{2} & \text{if } n \text{ is odd.} \end{cases}$$

Is j surjective?

A: Yes. **Let $z \in \mathbb{Z}$. We consider cases.**
Case $z \geq 0$:

Case $z < 0$:

In all cases, there exists an input that maps to z.

EXAMPLE: Let $j : \mathbb{N} \to \mathbb{Z}$ defined by

$$j(n) = \begin{cases} \frac{n}{2} - 1 & \text{if } n \text{ is even,} \\ \frac{-(n+1)}{2} & \text{if } n \text{ is odd.} \end{cases}$$

Is j surjective?

A: Yes. **Let $z \in \mathbb{Z}$. We consider cases.**
Case $z \geq 0$: Let $n = 2(z+1)$. Then $n \in \mathbb{N}$ and n is even, so

$$j(n) = \frac{2(z+1)}{2} - 1 = (z+1) - 1 = z.$$

Case $z < 0$: Let $n = -(1+2z)$. Then $n \in \mathbb{N}$ and n is odd, so

$$j(n) = \frac{-(-(1+2z)+1)}{2} = \frac{-(-2z)}{2} = \frac{2z}{2} = z.$$

In all cases, there exists an input that maps to z.

Codomain matters

To determine whether or not a function in surjective, the codomain must be explicitly understood.

EXAMPLE: Consider the function f that takes any integer as input, and outputs the absolute value of the input. Then f is surjective if the codomain is $\mathbb{N}$, but not surjective if the codomain is $\mathbb{Z}$.

Properties of functions: bijective

Let $f : A \to B$ be a function. We say that f is **bijective** or f is a **bijection** when f is injective and surjective.

We say that A and B are in one-to-one correspondence when there exists a bijection $f : A \to B$.

Composition

Let A, B and C be subsets of a universe U. If $f : A \to B$ and $g : B \to C$ are functions, then the rule $a \mapsto g(f(a))$ defines a function called the **composition of g and f** and denoted $g \circ f$. Note

$$(g \circ f)(a) = g(f(a)).$$

The order of composition matters...

Order matters

Let $A = \{\text{cat}, \text{dog}, \text{chicken}\}$ and let $f : A \to \mathbb{N}$ be defined by the rule

$$\begin{aligned} & f \\ \text{cat} &\mapsto 70 \\ \text{dog} &\mapsto 90 \\ \text{chicken} &\mapsto 50, \end{aligned}$$

and let $g : \mathbb{N} \to \mathbb{N}$ be defined by the rule

$$g(z) = 3z.$$

Then $g \circ f$ is defined, but $f \circ g$ is undefined.

Inverse function

Let A, B be subsets of a universe U. Recall that if R is a relation from A to B, then the inverse relation R^{-1} from B to A is determined by the rule

$$aRb \Leftrightarrow bR^{-1}a.$$

Theorem: Let A, B be subsets of a universe U, and let $f : A \to B$ be a function. The inverse relation f^{-1} is a function from B to A (called the **inverse of** f) if only if f is a bijection.

If f and f^{-1} are both functions, we call them **inverse functions** and we say that f is **invertible**.

Inverse functions and identity functions

For any set A, the identity function on A is the function $i_A : A \to A$ defined by the rule $a \mapsto a$.

If $f : A \to B$ is a bijection, then $f^{-1} \circ f = i_A$ and $f \circ f^{-1} = i_B$.

Example

Let's unpack something written using the vocabulary we have defined above.

Let $B = \{0, 1\}$ and $n \in \mathbb{N}$. We define a set

$$B_n = \underbrace{B \times B \times \cdots \times B}_{n \text{ times}},$$

and a function $H_n : B_n \times B_n \to \mathbb{Z}_{\geq 0}$ by the rule

$$H_n(s,t) = \text{ the number of coordinate (bit) positions where } s \text{ and } t \text{ differ.}$$

Q: Explain, in your own words, what has been defined by the above.

Example (cont.)

An infinite number of sets $B_1, B_2, B_3, \ldots$ and functions $H_1, H_2, H_3, \ldots$ (called the **Hamming functions**) have been defined. For each positive integer n, B_n is the set of n-tuples of binary digits (bits). So, for example, $(0, 1, 1, 0, 0, 1) \in B_6$.

The function H_n takes as input two n-tuples of bits (in the form of an ordered pair), compares them to see in which places they agree, and outputs the number of coordinates in which they disgree. For example,

$$H_5((0, 0, 0, 1, 1), (1, 0, 1, 0, 1)) = 3$$

because the n-tuples given disagree in the first, third and fourth coordinates.

Challenge

Describe, if possible, a way to arrange the elements of B_n around a circle so that $H_n(s, t) = 1$ whenever s and t are adjacent in your arrangement.