CSE215
Foundations of Computer Science

Instructor: Zhoulai Fu

State University of New York, Korea

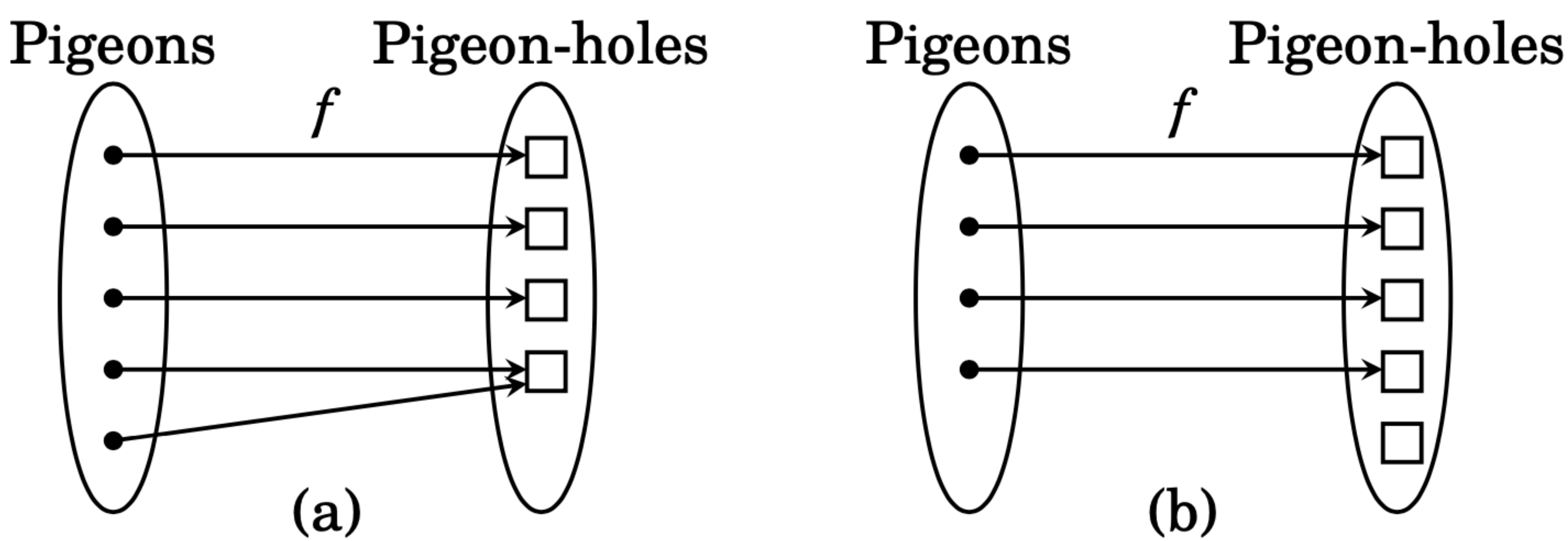
Agenda

- Pigeonhole principle
- Inverse functions

The Pigeonhole Principle

Intuition

- Imagine there is a set A of pigeons and a set B of pigeonholes, and all the pigeons fly into the pigeonholes. You can think of this as describing a function $f : A \to B$, where pigeon X flies into pigeonhole $f(X)$.



The Pigeonhole Principle (function version)

Suppose A and B are finite sets and $f : A \to B$ is any function. Then:

- If $|A| > |B|$, then f is not injective.

Example 1

- Prove the following statement: There are at least two people in Incheon with the same number of hairs on their heads.

- We accept two facts. First, the population of Incheon is around 3 million. Second, it is a biological fact that every human head has fewer than one million hairs.

Solution

- Let A be the set of all people of Incheon and let B = {0,1,2,3,4,…,1000000}. Let $f : A \to B$ be the function for which $f(x)$ equals the number of hairs on the head of x. Since $|A| > |B|$, the pigeonhole principle asserts that f is not injective. Thus there are two people of Incheon x and y for whom $f(x) = f(y)$, meaning that they have the same number of hairs on their heads.

Example 2

- Prove the following statement: If A is any set of 10 integers between 1 and 100, then there exist two different subsets $X \subseteq A$ and $Y \subseteq A$ for which the sum of elements in X equals the sum of elements in Y .

- Prove the following statement: If A is any set of 10 integers between 1 and 100, then there exist two different subsets X ⊆ A and Y ⊆ A for which the sum of elements in X equals the sum of elements in Y .

To illustrate what this proposition is saying, consider the random set

$$A = \{5, 7, 12, 11, 17, 50, 51, 80, 90, 100\}$$

of 10 integers between 1 and 100. Notice that A has subsets $X = \{5, 80\}$ and $Y = \{7, 11, 17, 50\}$ for which the sum of the elements in X equals the sum of those in Y. If we tried to "mess up" A by changing the 5 to a 6, we get

$$A = \{6, 7, 12, 11, 17, 50, 51, 80, 90, 100\}$$

which has subsets $X = \{7, 12, 17, 50\}$ and $Y = \{6, 80\}$ both of whose elements add up to the same number (86). The proposition asserts that this is always possible, no matter what A is. Here is a proof:

Solution

Proof. Suppose $A \subseteq \{1,2,3,4,\ldots,99,100\}$ and $|A| = 10$, as stated. Notice that if $X \subseteq A$, then X has no more than 10 elements, each between 1 and 100, and therefore the sum of all the elements of X is less than $100 \cdot 10 = 1000$. Consider the function

$$f : \mathscr{P}(A) \to \{0,1,2,3,4,\ldots,1000\}$$

where $f(X)$ is the sum of the elements in X. (Examples: $f\left(\{3,7,50\}\right) = 60$; $f\left(\{1,70,80,95\}\right) = 246$.) As $|\mathscr{P}(A)| = 2^{10} = 1024 > 1001 = \left|\{0,1,2,3,\ldots,1000\}\right|$, it follows from the pigeonhole principle that f is not injective. Therefore there are two unequal sets $X, Y \in \mathscr{P}(A)$ for which $f(X) = f(Y)$. In other words, there are subsets $X \subseteq A$ and $Y \subseteq A$ for which the sum of elements in X equals the sum of elements in Y. ■

Exercise 1

- Prove that if six numbers are chosen at random, then at least two of them have the same remainder when divided by 5.

Solution

- Suppose we randomly choose 6 integers.
- Let A be the set of the six integers.
- Let B the the set {0,1,2,3,4}
- Let f: A -> B be the function defined as f(a) = a mod 5
- Then f cannot be one-to-one because |A|>|B|
- Therefore there exists a1, a2 of A such that f(a1) = f(a2)

Exercise 2

- Prove that if a is a natural number, then there exist two unequal natural numbers k and l for which a^k – a^l is divisible by 10.

Solution

- Suppose we randomly choose a natural number “a”.
- Let f: N -> {0,1,2,…,9} be a function defined as f(k) = last digit of a^k
- Following the pigeonhole principle, f cannot be injective.
- Thus there exists k and l such that f(k) = f(l)
- Thus a^k and a^l have the same last digit. Thus a^k - a^l is a multiple of 10.

One-to-one correspondence (or bijective functions)

Important Note

- No need to know how to prove bijectivity, although it helps
- But we we need to be able to determine if a function is bijective

One-to-one correspondences

Definition

- A one-to-one correspondence (or bijection) from a set X to a set Y is a function $F : X \to Y$ that is both one-to-one and onto.

Example

Problem

- Define $F : \mathbb{R} \times \mathbb{R} \to \mathbb{R} \times \mathbb{R}$ by the rule $F(x, y) = (x + y, x - y)$ for all $(x, y) \in \mathbb{R} \times \mathbb{R}$. Is F a one-to-one correspondence? Prove or give a counterexample.

Proof

To show that F is a one-to-one correspondence, we need to show that:

1. F is one-to-one.
2. F is onto.

Proof (continued)

- Proof that F is one-to-one.

  Suppose that (x_1, y_1) and (x_2, y_2) are any ordered pairs in $\mathbb{R}\times\mathbb{R}$ such that $F(x_1, y_1) = F(x_2, y_2)$.

  $\implies (x_1 + y_1, x_1 - y_1) = (x_2 + y_2, x_2 - y_2)$

  ($\because$ Defn. of F)

  $\implies x_1 + y_1 = x_2 + y_2$ and $x_1 - y_1 = x_2 - y_2$

  ($\because$ Defn. of equality of ordered pairs)

  $\implies x_1 = x_2$ and $y_1 = y_2$

  ($\because$ Solve the two simultaneous equations)

  $\implies (x_1, y_1) = (x_2, y_2)$

  ($\because$ Defn. of equality of ordered pairs)

  Hence, F is one-to-one.

Proof (continued)

- Proof that F is onto.

  Suppose (u, v) is any ordered pair in the co-domain of F. We will show that there is an ordered pair in the domain of F that is sent to (u, v) by F.

  Let $r = \frac{u+v}{2}$ and $s = \frac{u-v}{2}$. The ordered pair (r, s) belongs to $\mathbb{R} \times \mathbb{R}$. Also,

  $F(r, s)$

  $= F(\frac{u+v}{2}, \frac{u-v}{2}) \qquad (\because \text{Defn. of } F)$

  $= (\frac{u+v}{2} + \frac{u-v}{2}, \frac{u+v}{2} - \frac{u-v}{2}) \qquad (\because \text{Substitution})$

  $= (u, v) \qquad (\because \text{Simplify})$

  Hence, F is onto.

Exercises

Exercise 1

Problem 3. [5 points]

Let $X = \{1, 2, 3\}$, $Y = \{1, 2, 3, 4\}$ and $Z = \{1, 2\}$. Use arrow diagrams to define functions.

1. Define a function $f : X \to Y$ that is one-to-one but not onto.
2. Define a function $g : X \to Z$ that is onto but not one-to-one.
3. Define a function $h : X \to X$ that is neither one-to-one nor onto.
4. Define a function $k : X \to X$ that is one-to-one and onto but is not the identity function on X.

Exercise 2

A function $f : Z \times Z \to Z \times Z$ is defined as $f(m, n) = (m + n, 2m + n)$.

Check if the function f is bijective

Exercise 3

- Consider the function $\theta : \{0,1\} \times \mathbb{N} \to \mathbb{Z}$ defined as $\theta(a,b) = (-1)^a b$. Is θ injective? Is it surjective?