Computer Security

Cunsheng DING, HKUST

COMP4631

Lecture 03: Mathematical Foundations I

Outline of this Lecture

1. To recall sets.
2. To recall functions.
3. To explain why functions are important in security systems.

Definition of Sets

Definition: A set is a collection of (distinct) objects.

Example: $A = \{x, y, z\}$

Example: $B = \{1, 2\}$.

Example: $C = \{1, 2, x\}$.

Example: Z the set of all integers.

Example: $S = \{x \in Z : x > 0\}$.

Membership: We write $a \in A$ if a is an element of A.

The Number of Elements in a Set

Example: $|A| = |\{x, y, z\}| = 3$

Example: $|B| = |\{1, 2\}| = 2.$

Example: $|C| = |\{1, 2, x\}| = 3.$

Cartesian Product of Sets

Definition: The Cartesian product of two sets A and B is defined as

$$A \times B = \{(a, b) : a \in A,\ b \in B\}.$$

Example: Let $A = \{x, y, z\}$ and $B = \{1, 2\}$. Then

$$A \times B = \{(x, 1), (x, 2), (y, 1), (y, 2), (z, 1), (z, 2)\}.$$

Question: For the sets A and B above, what is $B \times A$?

Definition of Functions

Definition: A function f from A to B is a *mapping* such that f mapps every element $a \in A$ to a **unique** element, denoted $f(a)$, in B.

Example: Let $A = \{x, y, z\}$ and $B = \{1, 2\}$. Is the mapping

$$x \mapsto 1, \;\; x \mapsto 2, \;\; y \mapsto 2, \;\; z \mapsto 2$$

a function from A to B? Why?

Example: Let $A = \{x, y, z\}$ and $B = \{1, 2\}$. Is the mapping

$$x \mapsto 2, \;\; y \mapsto 2, \;\; z \mapsto 2$$

a function from A to B? Why?

The Number of Functions from A to B

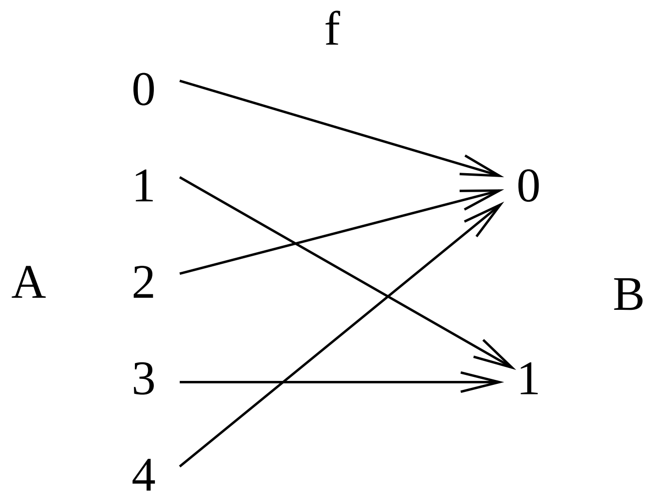
Question: Let $|A| = m$ and $|B| = n$. What is the total number of functions from A to B?

How to Describe Functions

Formula Description: Let $A = \{0, 1, 2, 3, 4\}$ and $B = \{0, 1\}$. Define

$$f(x) = x \bmod 2$$

Pictorial Description: For the f above,



Remark: These are school approaches. There are other approaches.

Onto Functions

Definition: A function f from A to B is *onto* if there is at least one $a \in A$ such that $f(a) = b$ for every $b \in B$.

Example: Let $A = \{0, 1, 2, 3, 4\}$ and $B = \{0, 1\}$. Is the function

$$f(x) = x \bmod 2$$

onto? Why?

Example: Let $A = \{x, y, z\}$ and $B = \{1, 2\}$. Is the function

$$x \mapsto 2, \;\; y \mapsto 2, \;\; z \mapsto 2$$

onto? Why?

Question: Let $|A| = m$ and $|B| = n$, where $m \geq n$. What is the total number of onto functions from A to B?

Onto Functions

Question: Let $|A| = m$ and $|B| = n$, where $m \geq n$. What is the total number of onto functions from A to B?

Solution: It is

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} (n-k)^m.$$

You need to use the Inclusion-Exclusion Principle to get this result.

One-to-one Functions

Definition: A function f from A to B is *one-to-one* if $f(a_1) \neq f(a_2)$ for every pair (a_1, a_2) of distinct elements in A.

Example: Let $A = \{0, 1, 2, 3, 4\}$ and $B = \{0, 1\}$. Is the function

$$f(x) = x \bmod 2$$

one-to-one? Why?

Example: Let $A = \{x, y\}$ and $B = \{1, 2\}$. Is the function

$$x \mapsto 1, \quad y \mapsto 2$$

one-to-one? Why?

Question: Let $|A| = m$ and $|B| = n$, where $m \leq n$. What is the total number of one-to-one functions from A to B?

One-to-one Functions

Question: Let $|A| = m$ and $|B| = n$, where $m \le n$. What is the total number of one-to-one functions from A to B?

Answer: It is

$$m!\binom{n}{m} = \frac{n!}{(n-m)!} = n(n-1)(n-2)\cdots(n-(m-1)).$$

One-to-one Correspondences

Definition: A function f from A to B is a *one-to-one correspondence* if it is both onto and one-to-one.

Example: Let $A = \{0, 1, 2, 3, 4\}$ and $B = \{0, 1\}$. Is the function

$$f(x) = x \bmod 2$$

a one-to-one correspondence? Why?

Example: Let $A = \{x, y\}$ and $B = \{1, 2\}$. Is the function

$$x \mapsto 1, \quad y \mapsto 2$$

a one-to-one correspondence? Why?

Inverse Functions

Definition: Let f be a one-to-one correspondence from A to B. The inverse of f, denoted by f^{-1}, is defined by

$$f^{-1}(b) = a \text{ if and only if } f(a) = b.$$

Conclusion: f^{-1} is a one-to-one correspondence from B to A.

Example: Let $A = \{x, y\}$ and $B = \{1, 2\}$ and

$$f : x \mapsto 1, \ y \mapsto 2.$$

Then

$$f^{-1} : 1 \mapsto x, \ 2 \mapsto y.$$

The Identity Function

Definition: The *identity function* I_A from A to A is defined by

$$I_A(a) = a \text{ for every element } a \in A.$$

Conclusion: I_A is a one-to-one correspondence from A to A.

Example: Let $A = \{x, y\}$.

$$I_A : x \mapsto x,\ \ y \mapsto y.$$

Conclusion: The inverse of I_A is itself.

Function Composition

Definition: Let f be a function from A to B, and g a function from B to C. The *composition* of f and g, denoted by $g \circ f$, is a function from A to C defined as

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

for all $a \in A$

Example: Let $A = \{x, y\}$, $B = \{1, 2\}$, $C = \{u, v\}$,

$$f : x \mapsto 1,\ \ y \mapsto 2$$

$$g : 1 \mapsto u,\ \ 2 \mapsto u.$$

Then

$$g \circ f : x \mapsto u,\ \ y \mapsto u.$$

Function Composition - ctd.

Question: Let $A = B = C$, be the set of integers.

$$f(x) = x + 1 \text{ and } g(x) = x^2 + x.$$

What is $g \circ f$?

Conclusion: Let f be a one-to-one correspondence from A to B. Then

$$f^{-1} \circ f = I_A.$$

This allows for correct decryption!

Permutations

Definition: A *permutation* f of A is a one-to-one correspondence from A to A.

Example: Let $A = \{0, 1, 2\}$ and $f(x) = (x + 1) \bmod 3$.

Conclusion: Every permutation f of A has the inverse f^{-1}. Clearly f^{-1} is also a permutation of A.

Example: Let $A = \{0, 1, 2\}$ and f be the same as above. Then

$$f^{-1}(x) = (x + 2) \bmod 3.$$

Question: What is the total number of permutations of A with n elements?

Permutations as One-dimensional Arrays

Conclusion: Any permutation of $A = \{1, 2, \ldots, n\}$ can be expressed as an array

$$f[1]f[2]\cdots f[n].$$

Example: Let $A = \{0, 1, 2\}$ and

$$f(x) = (x + 1) \bmod 3.$$

Then f can be expressed as the array

$$120.$$

Permutations as Two-dimensional Arrays

Conclusion: Let $A = \{1, 2, \cdots, n\}$. If $n = lm$, then a permutation f of A can also be defined as a two-dimensional array

$$
\begin{array}{llll}
f[1] & f[2] & \cdots & f[l] \\
f[1+l] & f[2+l] & \cdots & f[2l] \\
f[1+2l] & f[2+2l] & \cdots & f[3l] \\
\vdots & \vdots & & \vdots \\
f[1+(m-1)l] & f[2+(m-1)l] & \cdots & f[ml]
\end{array}
$$

Permutations as Two-dimensional Arrays - ctd.

Example: Let $n = 6 = 3 \times 2$. Then the following two-dimensional array (table)

$$\begin{array}{ccc} 6 & 2 & 5 \\ 1 & 3 & 4 \end{array}$$

defines a permutation of $A = \{1, 2, 3, 4, 5, 6\}$.

Question: Find f^{-1} and express it in the same form.

The Importance of Functions in Security Systems

Summary: Almost every building block in a cryptographic system is a function.