Cryptography

Cunsheng DING

HKUST, Hong Kong

COMP3631

Lecture 05: Linear and Nonlinear Functions

The Outline of This Lecture

1. The objective of this lecture.
2. Abelian groups.
3. Linear and nonlinear functions.
4. The need of linear and nonlinear functions in cryptography.

Part 1: The Objective of This Lecture

The Objective of This Lecture

In Lecture 4, we did the following:

- We defined one-key block ciphers and talked about their security issues in general.
- We discussed simple substitution ciphers, and realized that they are not secure.
- We saw that the one-time pad is secure in the information-theoretic sense but impractical.

The objective of this lecture: To introduce two types of building blocks for constructing both **secure** and **efficient** one-key block ciphers: linear and nonlinear functions.

Part 2: Abelian Groups

Abelian Groups

Abelian group: An Abelian group is a set A associated with a binary operation $+$ that satisfies the following five conditions:

- $x + y \in A$ for any pair of x and y in A (A is closed under $+$).
- $x + y = y + x$ for any pair of x and y in A ("+" is commutative).
- $(x + y) + z = x + (y + z)$ for any x, y and z in A ("+" is associative).
- There is a special element $0 \in A$ such that $0 + x = x$ for all $x \in A$ (identity element).
- For any $x \in A$ there is an element $y \in A$ such that $x + y = 0$ (y is the inverse of x with respect to $+$).

If A is a finite set, $(A, +)$ is called a finite Abelian group. In this course, we need only finite Abelian groups.

The First Example of Abelian Groups

Example of Abelian groups: Let $\mathbf{Z}$ denote the set of all integers and $+$ denote the integer addition. Then $(\mathbf{Z}, +)$ is an Abelian group with infinitely many elements.

Question: What is the identity element of $(\mathbf{Z}, +)$?

Question: How do you prove that $(\mathbf{Z}, +)$ is an Abelian group?

Answer: You prove that the five conditions in the definition are satisfied.

Remark: School students encounter this Abelian group.

The Second Example of Abelian Groups

The set of all rational numbers:

$$\mathbf{R} = \left\{ \frac{n}{m} : n \in \mathbf{Z},\ 0 \neq m \in \mathbf{Z} \right\}.$$

Example of Abelian groups: Let $\mathbf{R}$ denote the set of all rational numbers and $+$ denote the addition of rational numbers. Then $(\mathbf{R}, +)$ is an Abelian group with infinitely many elements.

Question: What is the identity element of $(\mathbf{R}, +)$?

Question: How do you prove that $(\mathbf{R}, +)$ is an Abelian group?

Remark: Secondary school students encounter this Abelian group.

The Third Example of Abelian Groups

The set of all rational numbers:

$$\mathbf{R} = \left\{ \frac{n}{m} : n \in \mathbf{Z},\ 0 \neq m \in \mathbf{Z} \right\}.$$

Example of Abelian groups: Let $\mathbf{R}^\times = \mathbf{R} \setminus \{0\}$ denote the set of all nonzero rational numbers and $\times$ denote the multiplication of rational numbers. Then $(\mathbf{R}^\times, \times)$ is an Abelian group with infinitely many elements.

Question: What is the identity element of $(\mathbf{R}^\times, \times)$?

Question: How do you prove that $(\mathbf{R}^\times, \times)$ is an Abelian group?

Remark: Secondary school students encounter this Abelian group.

Two More Examples of Abelian Groups

Example of Abelian groups: $(\mathbf{Z}_p, \oplus_p)$ is a finite Abelian group with p elements, where $\oplus_p$ denotes the modulo-p addition, p is any prime, and $\mathbf{Z}_p = \{0, 1, 2, \ldots, p-1\}$.

Question: What is the identity element of $(\mathbf{Z}_p, \oplus_p)$?

Example of Abelian groups: $(\mathbf{Z}_p^\times, \otimes_p)$ is a finite Abelian group with $p-1$ elements, where $\otimes_p$ denotes the modulo-p multiplication, p is any prime and $\mathbf{Z}_p^\times = \{1, 2, \cdots, p-1\}$.

Question: What is the identity element of $(\mathbf{Z}_p^\times, \otimes_p)$?

Remark: The finite field $\mathbf{Z}_p$ has two Abelian groups: the additive group $(\mathbf{Z}_p, \oplus_p)$, and the multiplicative group $(\mathbf{Z}_p^\times, \otimes_p)$.

The Abelian Group $(\mathbf{Z}_m^n, +)$

Definition: Let $m \geq 2$ and $n \geq 1$ be integers. Let

$$\mathbf{Z}_m^n = \mathbf{Z}_m \times \mathbf{Z}_m \times \cdots \times \mathbf{Z}_m \ (n\text{-ary Cartesian product of } \mathbf{Z}_m).$$

For any two elements

$$x = (x_1, x_2, \cdots, x_n) \in \mathbf{Z}_m^n, \ y = (y_1, y_2, \cdots, y_n) \in \mathbf{Z}_m^n,$$

define

$$x + y = (x_1 \oplus_m y_1, x_2 \oplus_m y_2, \ldots, x_n \oplus_m y_n) \in \mathbf{Z}_m^n,$$

where $\oplus_m$ denotes the modulo-m addition.

Proposition: $(\mathbf{Z}_m^n, +)$ is an Abelian group with m^n elements.

Remark: This Abelian group is employed in many cryptographic systems.

Part 3: Linear and Nonlinear Functions

Linear Functions

Definition: A function f from an Abelian group $(A, +)$ to an Abelian group $(B, +)$ is called a **homomorphism** if $f(x + y) = f(x) + f(y)$ for all $x, y \in A$.

Remark: No confusion using symbol $+$ to denote two different operations.

Definition: A function $g : A \to B$ is **linear** if and only if $g = f + b$ for a homomorphism $f : A \to B$ and a constant $b \in B$. Equivalently, g is linear if and only if $g + b'$ is a homomorphism for some $b' \in B$. (b' the inverse of b.)

Remark: A homomorphism is a special linear function by definition, as $f(x) = f(x) + 0$ is linear by definition for every homomorphism $f(x)$.

Example: Let $f(x) = x_1 + x_2 + \cdots + x_n$, where $x = (x_1, \cdots, x_n) \in \mathbf{Z}_2^n$ and $x_i \in \mathbf{Z}_2$. Then f is a linear function (homomorphism) from $(\mathbf{Z}_2^n, +)$ to $(\mathbf{Z}_2, +)$. The function $f(x) + 1$ is a linear function from $(\mathbf{Z}_2^n, +)$ to $(\mathbf{Z}_2, +)$.

The Constant Linear Functions

The zero function: From an Abelian group $(A, +)$ to an Abelian group $(B, +)$, the **zero function** is defined as $L_0(x) = 0$ for all $x \in A$, where 0 is the identity element of $(B, +)$.

Proposition: The zero function is a linear function (homomorphism) from Abelian group $(A, +)$ to Abelian group $(B, +)$.

Proof: For any x and y in A, by definition we have

$$L_0(x + y) = 0 = 0 + 0 = L_0(x) + L_0(y).$$

The constant linear functions: From an Abelian group $(A, +)$ to an Abelian group $(B, +)$, the **constant linear functions** are defined as $L_b(x) = L_0(x) + b = b$ for all $x \in A$, where b is any fixed element of B.

The Composition of Two Linear Functions

Proposition: Let f be a linear function from Abelian group $(A, +)$ to Abelian group $(B, +)$ and g be a linear function from Abelian group $(B, +)$ to Abelian group $(C, +)$. Then $g \circ f$ is a linear function from Abelian group $(A, +)$ to Abelian group $(C, +)$

Proof: Left as an offline exercise.

Comment: The composition of two linear functions is still a linear function.

A Special Type of Linear Functions

Definition: Let P be a permutation of the set $\{1, \cdots, n\}$. Define a function L_P from $(\mathbf{Z}_2^n, +)$ to itself by

$$L_P((x_1, x_2, \cdots, x_n)) = (x_{P(1)}, x_{P(2)}, \cdots, x_{P(n)})$$

for any $x = (x_1, x_2, \ldots, x_n) \in \mathbf{Z}_2^n$.

Proposition: The function L_P is a linear function (homomorphism) from $(\mathbf{Z}_2^n, +)$ to $(\mathbf{Z}_2^n, +)$.

Remark: L_P is used in some one-key block ciphers.

Linear Functions: Example

Proposition: Let P be a permutation of the set $\{1, \cdots, n\}$. Define a function L_P from $(\mathbf{Z}_2^n, +)$ to itself by

$$L_P((x_1, x_2, \cdots, x_n)) = (x_{P(1)}, x_{P(2)}, \cdots, x_{P(n)})$$

for any $x = (x_1, x_2, \ldots, x_n) \in \mathbf{Z}_2^n$. The function L_P is a linear function (homomorphism) from $(\mathbf{Z}_2^n, +)$ to $(\mathbf{Z}_2^n, +)$.

Proof: For any $x = (x_1, x_2, \ldots, x_n) \in \mathbf{Z}_2^n$ and $y = (y_1, y_2, \ldots, y_n) \in \mathbf{Z}_2^n$,

$$\begin{aligned} L_P(x+y) &= L_P((x_1+y_1, \ldots, x_n+y_n)) = L_P(((x+y)_1, \ldots, (x+y)_n)) \\ &= ((x+y)_{P(1)}, \ldots, (x+y)_{P(n)}) \\ &= (x_{P(1)} + y_{P(1)}, \ldots, x_{P(n)} + y_{P(n)}) \\ &= (x_{P(1)}, x_{P(2)}, \ldots, x_{P(n)}) + (y_{P(1)}, y_{P(2)}, \ldots, y_{P(n)}) \\ &= L_P(x) + L_P(y). \end{aligned}$$

Nonlinear Functions

Definition: A function that is not linear is called a **nonlinear function**.

Remark: To prove that a function f from an Abelian group $(A, +)$ to an Abelian group $(B, +)$ is nonlinear, by definition you need to prove that $f(x) + b$ is not a homomorphism for each fixed $b \in B$.

Example: The following function from $(\mathbf{Z}_2^4, +)$ to $(\mathbf{Z}_2, +)$ is nonlinear:

$$f((x_1, x_2, x_3, x_4)) = x_1 + x_2 + x_3 + x_4 + x_1 \times x_2 \times x_3 \times x_4,$$

where the $+$ and $\times$ are the modulo-2 addition and modulo-2 multiplication.

Question: How do you prove that f is nonlinear.

Answer: Prove that both $f(x)$ and $1 + f(x)$ are not homomorphisms using the definition of homomorphisms.

Nonlinear Functions

Example: The following function from $(\mathbf{Z}_2^4, +)$ to $(\mathbf{Z}_2, +)$ is nonlinear:

$$f((x_1, x_2, x_3, x_4)) = x_1 + x_2 + x_3 + x_4 + x_1 \times x_2 \times x_3 \times x_4.$$

Proof: Note that $f((x_1, x_2, x_3, x_4))$ is not a homomorphism, as we have

$$1 = f((1, 1, 1, 1)) = f(x + y) \neq f(x) + f(y) = 0 + 0 = 0,$$

where $x = (1, 1, 0, 0)$, $y = (0, 0, 1, 1)$ and $x + y = (1, 1, 1, 1)$.

Let $f_1((x_1, x_2, x_3, x_4)) = f((x_1, x_2, x_3, x_4)) + 1$. Then we have

$$1 = f_1((0, 0, 0, 0)) = f_1(x' + y') \neq f_1(x') + f_1(y') = 0 + 0 = 0,$$

where $x' = y' = (1, 1, 1, 1)$. Hence, $f_1((x_1, x_2, x_3, x_4))$ is not a homomorphism either.

Consequently, $f((x_1, x_2, x_3, x_4))$ is nonlinear by definition.

Part 4: The Need of Linear and Nonlinear Functions in Cryptography

Linear and Nonlinear Functions

Question: Why are we interested in linear and nonlinear functions?

Answer: Both linear and nonlinear functions are needed in many cryptographic systems as basic building blocks.

Later, we will use both linear and nonlinear functions to construct some ciphers.