

2010 年度春期

# 応用数学Ⅰ

(数学科)

# 情報数学特論

(理工学専攻情報学領域)

(Information Mathematics)

(担当: 角皆)

## 本講義の概要 (Course Description)

- **情報通信の数理 (Math. in Communication)**
  - ★ 情報理論 (Information Theory)
  - ★ 符号理論 (Coding Theory)
  - ★ 暗号理論 (Cryptography)
- **土台の数学 (Mathematical background)**
  - ★ 有限体とその上の線型代数・Galois 理論 (Finite fields, Linear algebra, Galois theory)
  - ★ 計算量の理論 (Theory of Complexity)

## 情報通信を行なう際の要請

### (What is required in communication ?)

- 効率的に (efficiently)  
→ 情報理論 (Information Theory)
- 確実に (certainly)  
→ 符号理論 (Coding Theory)
- 安全に (safely)  
→ 暗号理論 (Cryptography)

## 情報通信を行なう際の要請

### (What is required in communication ?)

- 効率的に (efficiently)  
→ 情報理論 (Information Theory)
- 確実に (certainly)  
→ 符号理論 (Coding Theory)
- 安全に (safely)  
→ 暗号理論 (Cryptography)

## 情報理論 (情報源符号化・情報量の理論)

### (Information Theory, Source coding)

- 伝えるべき情報をより効率良く伝えるには  
(How to communicate more efficiently)

- 「効率の良さ」を計る  
(quantify (formulate) “efficiency”)

- ★ 伝えるべき「情報の量」を計る  
(quantify “information”)

- ★ 伝える為の「手間」を計る  
(quantify “cost to transmit”)

→ Shannon

「情報の量は伝えるのに必要な手間と一致」  
(“quantity of information = minimum cost”)

## 情報理論 (情報源符号化・情報量の理論)

### (Information Theory, Source coding)

- 伝えるべき情報をより効率良く伝えるには  
(How to communicate more efficiently)
- 「効率の良さ」を計る  
(quantify (formulate) “efficiency”)
  - ★ 伝えるべき「情報の量」を計る  
(quantify “information”)
  - ★ 伝える為の「手間」を計る  
(quantify “cost to transmit”)

→ Shannon

「情報の量は伝えるのに必要な手間と一致」  
(“quantity of information = minimum cost”)

## 情報理論 (情報源符号化・情報量の理論)

### (Information Theory, Source coding)

- 伝えるべき情報をより効率良く伝えるには  
(How to communicate more efficiently)
- 「効率の良さ」を計る  
(quantify (formulate) “efficiency”)
  - ★ 伝えるべき「情報の量」を計る  
(quantify “information”)
  - ★ 伝える為の「手間」を計る  
(quantify “cost to transmit”)

→ Shannon

「情報の量は伝えるのに必要な手間と一致」  
(“quantity of information = minimum cost”)

## 符号理論 (誤り訂正符号)

### (Coding theory, Error-correcting codes)

- 通信路での雑音による誤りを  
検出・訂正するための符号方式  
(Coding system to detect/correct errors  
caused by noise in transmission)

- ★ 「冗長性」を持たせる (Add “redundancy”)
- ★ しかしなるべく効率良く (Keep efficiency)

→ 効率の良い符号の構成のために  
様々な代数的性質を利用  
(線型符号・代数幾何符号など)  
(Use various algebraic properties)



## 符号理論 (誤り訂正符号)

### (Coding theory, Error-correcting codes)

- 通信路での雑音による誤りを  
検出・訂正するための符号方式  
(Coding system to detect/correct errors  
caused by noise in transmission)
  - ★ 「冗長性」を持たせる (Add “redundancy”)
  - ★ しかしなるべく効率良く (Keep efficiency)

→ 効率の良い符号の構成のために  
様々な代数的性質を利用  
(線型符号・代数幾何符号など)  
(Use various algebraic properties)

## 符号理論 (誤り訂正符号)

### (Coding theory, Error-correcting codes)

- 通信路での雑音による誤りを  
検出・訂正するための符号方式  
(Coding system to detect/correct errors  
caused by noise in transmission)
    - ★ 「冗長性」を持たせる (Add “redundancy”)
    - ★ しかしなるべく効率良く (Keep efficiency)
- 効率の良い符号の構成のために  
様々な代数的性質を利用  
(線型符号・代数幾何符号など)  
(Use various algebraic properties)

## 暗号理論 (共通鍵・公開鍵暗号)

### (Cryptography (Secret Key / Public Key))

- 安全な情報生活の為に  
(For secure communication)
  - ★ 秘密通信 (secret communication)
  - ★ デジタル認証・署名 (digital signature)
  - ★ 秘密分散 (secret sharing)
  - ★ 鍵共有 (key exchange)
- 安全な暗号の実現 (RSA 暗号・楕円曲線暗号等)  
(Construction of secure cryptosystem)
- 「安全さ」を計る (計算量の理論)  
(quantify “security” (Theory of Complexity))

## 暗号理論 (共通鍵・公開鍵暗号)

### (Cryptography (Secret Key / Public Key))

- 安全な情報生活の為に  
(For secure communication)
  - ★ 秘密通信 (secret communication)
  - ★ デジタル認証・署名 (digital signature)
  - ★ 秘密分散 (secret sharing)
  - ★ 鍵共有 (key exchange)
- 安全な暗号の実現 (RSA 暗号・楕円曲線暗号等)  
(Construction of secure cryptosystem)
- 「安全さ」を計る (計算量の理論)  
(quantify “security” (Theory of Complexity))

## 基礎となる数理の予備知識

代表的には、例えば次のような事柄

	基礎編	初級編
情報理論	微分積分・線型代数・確率論	
符号理論	有限体上の 線型代数	整数論・群論・ 代数幾何の初歩
暗号理論	初等整数論 (素数の話)	

他に、計算の理論 (計算可能性・計算量) など

## 情報通信を行なう際の要請

(What is required in communication ?)

- 効率的に (efficiently)  
→ 情報理論 (Information Theory)
- 確実に (certainly)  
→ 符号理論 (Coding Theory)
- 安全に (safely)  
→ 暗号理論 (Cryptography)

## 情報理論 (情報源符号化・情報量の理論)

### (Information Theory, Source coding)

- 伝えるべき情報をより効率良く伝えるには  
(How to communicate more efficiently)
- 「効率の良さ」を計る  
(quantify (formulate) “efficiency”)
  - ★ 伝えるべき「情報の量」を計る  
(quantify “information”)
  - ★ 伝える為の「手間」を計る  
(quantify “cost to transmit”)

→ Shannon

「情報の量は伝えるのに必要な手間と一致」  
(“quantity of information = minimum cost”)

## 情報の符号化 (Coding)

**Analog data (continuous data)**

⇓ **sampling**

**Digital data (discrete, finite)**

↑ “情報 (information)” to be treated here  
(情報源, source)

⇓ ← “符号化 (coding)” to be treated here

**Digital data for transmission (伝送用データ)**

… 特定 (一般には少数) の種類の文字の列  
(a sequence of specific alphabets)



## 情報の符号化 (Coding)

**Analog data (continuous data)**

⇓ **sampling**

**Digital data (discrete, finite)**

↑ “**情報 (information)**” to be treated here  
(**情報源, source**)

⇓ ← “**符号化 (coding)**” to be treated here

**Digital data for transmission (伝送用データ)**

… 特定 (一般には少数) の種類の文字の列  
(**a sequence of specific alphabets**)

## 文字 (characters) → ASCII code

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	(control characters)															
1	(control characters)															
2	!	"	#	\$	%	&	'	(	)	*	+	,	-	.	/	
3	0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?
4	@	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
5	P	Q	R	S	T	U	V	W	X	Y	Z	[	\	]	^	_
6	'	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
7	p	q	r	s	t	u	v	w	x	y	z	{		}	~	

**7 bits for each character**

**(8 bits in actual implementation)**

## ASCII code

<b>A</b>	01000001	<b>J</b>	01001010	<b>S</b>	01010011
<b>B</b>	01000010	<b>K</b>	01001011	<b>T</b>	01010100
<b>C</b>	01000011	<b>L</b>	01001100	<b>U</b>	01010101
<b>D</b>	01000100	<b>M</b>	01001101	<b>V</b>	01010110
<b>E</b>	01000101	<b>N</b>	01001110	<b>W</b>	01010111
<b>F</b>	01000110	<b>O</b>	01001111	<b>X</b>	01011000
<b>G</b>	01000111	<b>P</b>	01010000	<b>Y</b>	01011001
<b>H</b>	01001000	<b>Q</b>	01010001	<b>Z</b>	01011010
<b>I</b>	01001001	<b>R</b>	01010010		

## モールス符号 (Morse code)

A	· -
B	- ...
C	- · - ·
D	- ..
E	·
F	.. - ·
G	- - ·
H	....
I	..

J	· - - -
K	- · -
L	· - ..
M	- -
N	- ·
O	- - -
P	· - - ·
Q	- - · -
R	· - ·

S	...
T	-
U	.. -
V	... -
W	· - -
X	- .. -
Y	- · - -
Z	- - ..

# モールス符号 (Morse code)

## 1 文字のための符号長が区々 (various length for each character)

← 頻度の高い文字は短く、低い文字は長く  
(Shorter if frequent, longer if rare)

→ 頻度まで考慮して符号長の期待値を短く  
(Shorten the expectation length)

… 頻度 (出現確率) も考慮した符号効率の定式化  
(Formulate efficiency considering frequency)

## モールス符号 (Morse code)

1 文字のための符号長が区々  
(various length for each character)

← 頻度の高い文字は短く、低い文字は長く  
(Shorter if frequent, longer if rare)

→ 頻度まで考慮して符号長の期待値を短く  
(Shorten the expectation length)

… 頻度 (出現確率) も考慮した符号効率の定式化  
(Formulate efficiency considering frequency)

## モールス符号 (Morse code)

1 文字のための符号長が区々  
(various length for each character)

← 頻度の高い文字は短く、低い文字は長く  
(Shorter if frequent, longer if rare)

→ 頻度まで考慮して符号長の期待値を短く  
(Shorten the expectation length)

… 頻度 (出現確率) も考慮した符号効率の定式化  
(Formulate efficiency considering frequency)

## モールス符号 (Morse code)

1 文字のための符号長が区々  
(various length for each character)

← 頻度の高い文字は短く、低い文字は長く  
(Shorter if frequent, longer if rare)

→ 頻度まで考慮して符号長の期待値を短く  
(Shorten the expectation length)

… 頻度 (出現確率) も考慮した符号効率の定式化  
(Formulate efficiency considering frequency)



## モールス符号 (Morse code)

1 文字のための符号長が区々  
(various length for each character)

→ 1 文字毎の区切りは判るのか？  
(Can one detect an end of each character ?)

→ 実はモールス符号では、  
文字間・単語間の送信間隔が定められている  
(The interval between characters are fixed.)

## モールス符号 (Morse code)

1 文字のための符号長が区々  
(various length for each character)

→ 1 文字毎の区切りは判るのか？  
(Can one detect an end of each character ?)

→ 実はモールス符号では、  
文字間・単語間の送信間隔が定められている  
(The interval between characters are fixed.)

A	· -
B	- ...
C	- · - ·
D	- ..
E	·
F	.. - ·
G	- - ·

H	....
I	..
J	· - - -
K	- · -
L	· - ..
M	- -
N	- ·

O	- - -
P	· - - ·
Q	- - · -
R	· - ·
S	...
T	-

U	.. -
V	... -
W	· - -
X	- .. -
Y	- · - -
Z	- - ..

**Ex. the cat and the dog**

- .... ·                      - · - ·                      · -                      -                      · -  
 - ·                      - ..                      - ....                      ·                      - ..                      - - -  
 - - ·

( is a space (interval) with length as one · )

→ - と · と   とを用いて符号化している

(Coding with -, ·, and )

## 情報源符号化の定式化

### (Formulation of source coding)

**source alphabet**  $S$  : a finite set

$S^+ := \bigsqcup_{n \geq 1} S^n$  :  $S$  の元の 1 個以上の列全体

$\varepsilon$  : 空語 (the empty word),  $S^0 := \{\varepsilon\}$

$S^* := \bigsqcup_{n \geq 0} S^n$  :  $S$  の元の 0 個以上の列全体

$$= S^+ \sqcup \{\varepsilon\}$$

$w \in S^n$  に対し、 $|w| := n$

(the length of a sequence)