2009 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)

(担当: 角皆)

本講義の概要

- **情報通信の数理**
  - ⋆ 情報理論
  - ⋆ 符号理論
  - ⋆ 暗号理論
- **それを支える数学**
  - ⋆ 有限体とその上の線型代数・Galois 理論
  - ⋆ 情報量の理論・計算量の理論

情報通信を行なう際の要請

- **効率的に** $\longrightarrow$ **情報理論**
- **確実に** $\longrightarrow$ **符号理論**
- **安全に** $\longrightarrow$ **暗号理論**

情報理論 (情報源符号化・情報量の理論)

- 伝えるべき情報をより効率良く伝えるには

- 「効率の良さ」を計る
  - ⋆ 伝えるべき「情報の量」を計る
  - ⋆ 伝える為の「手間」を計る

$\longrightarrow$ Shannon
「情報の量は伝えるのに必要な手間と一致」

符号理論 (誤り訂正符号)

- **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

- **誤りを検出・訂正するには**
  - ⋆ **「冗長性」を持たせる**
  - ⋆ **しかしなるべく効率良く**

⟶ 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)

暗号理論 (共通鍵・公開鍵暗号)

- 安全な情報生活の為に
  - ⋆ 秘密通信
  - ⋆ ディジタル認証・署名
  - ⋆ 秘密分散
  - ⋆ 鍵共有
- 安全な暗号の実現
  (RSA 暗号・楕円曲線暗号など)
- 安全性を計る (計算量の理論)

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

<table>
<tr><th></th><th>基礎編</th><th>初級編</th></tr>
<tr><td>情報理論</td><td colspan="2">微分積分・線型代数・確率論</td></tr>
<tr><td>符号理論</td><td>有限体上の
線型代数</td><td rowspan="3">整数論・群論・
代数幾何の初歩</td></tr>
<tr><td>暗号理論</td><td>初等整数論
(素数の話)</td></tr>
</table>

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

- **効率的に** $\longrightarrow$ **情報理論**
- **確実に** $\longrightarrow$ **符号理論**
- **安全に** $\longrightarrow$ **暗号理論**

情報理論 (情報源符号化・情報量の理論)

- 伝えるべき情報をより効率良く伝えるには

- 「効率の良さ」を計る
  - ⋆ 伝えるべき「情報の量」を計る
  - ⋆ 伝える為の「手間」を計る

$\longrightarrow$ Shannon
「情報の量は伝えるのに必要な手間と一致」

情報の符号化

アナログデータ (連続データ)

⇓ サンプリングなど

ディジタルデータ (離散・有限データ)
↑ ここで扱う “情報” (元データ・情報源)

⇓ ⟵ ここで扱う “符号化”

通信用の形式のディジタルデータ
(特定 (一般には少数) の種類の文字の列)

文字データ $\longrightarrow$ 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 bit で 1 文字を表す (実装上は 8 bit にする)

ASCII code

A	01000001
B	01000010
C	01000011
D	01000100
E	01000101
F	01000110
G	01000111
H	01001000
I	01001001

J	01001010
K	01001011
L	01001100
M	01001101
N	01001110
O	01001111
P	01010000
Q	01010001
R	01010010

S	01010011
T	01010100
U	01010101
V	01010110
W	01010111
X	01011000
Y	01011001
Z	01011010

モールス符号 (Morse code)

A	・ ー
B	ー ・・・
C	ー ・ ー ・
D	ー ・・
E	・
F	・・ ー ・
G	ー ー ・
H	・・・・
I	・・

J	・ ー ー ー
K	ー ・ ー
L	・ ー ・・
M	ー ー
N	ー ・
O	ー ー ー
P	・ ー ー ・
Q	ー ー ・ ー
R	・ ー ・

S	・・・
T	ー
U	・・ ー
V	・・・ ー
W	・ ー ー
X	ー ・・ ー
Y	ー ・ ー ー
Z	ー ー ・・