

2008 年度春期

応用数学Ⅰ

(数学科)

応用数学特別講義Ⅰ

(数学専攻)

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
 - ★ 計算量の理論

情報通信を行なう際の要請

- 効率的に → 情報理論
- 確実に → 符号理論
- 安全に → 暗号理論

情報通信を行なう際の要請

- 効率的に → 情報理論
- 確実に → 符号理論
- 安全に → 暗号理論

情報理論 (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

→ **Shannon**

「情報の量は伝えるのに必要な手間と一致」

情報理論 (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

→ Shannon

「情報の量は伝えるのに必要な手間と一致」

情報理論 (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

→ **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)

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)

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)
- 安全性を計る (計算量の理論)

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)
- 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ことから

	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