

代数系と符号理論 第1回板書プリント

植松友彦 2007.4.10

注意事項：授業中の食事は禁止する !!

0.1 教科書

イエレン ユステセン、トム ホーホルト著：誤り訂正符号入門、森北出版

0.2 成績の評価法

- 毎回授業中に演習 (30 分間) を行う。
- 中間テスト (40 点) と期末テスト (40 点) を行う。
- 出席点は 20 点あり、演習を 1 回欠席する毎に、出席点を 1 点ずつ減点する。
- 宿題は期限までに必ず提出すること。 m 回分の宿題を期限までに提出しなかった場合、テストと出席点の総和の 60 点を超える部分を 0.5^m 倍する。例えば、テストと出席点で 100 点であったとしても、2 回提出物を出さなかった場合、成績は

$$(100 - 60) * (0.5)^2 + 60 = 70$$

となる。良い点が欲しければ、ひたすら努力するように。

0.3 参考文献

- 宮川、岩垂、今井：符号理論、昭晃堂、1973.
- 笠原、田崎、小倉：情報理論—基礎と応用—、昭晃堂、1985.
- 今井: 符号理論、電子情報通信学会、1990.
- 岩垂: 符号理論入門、昭晃堂、1992.
- 平澤、西島：符号理論入門、培風館、2000.
- 情報理論とその応用学会編: 符号理論とその応用、培風館、2003.
- W. W. Peterson and E. J. Weldon, Jr.: Error-Correcting Codes, MIT Press, 1971.
- R. E. Blahut: Algebraic Codes for Data Transmission, Cambridge, 2003.
- S. Lin and D. J. Costello, Jr. : Error Control Coding, Peason Prentice Hall, 2004.

1 符号理論とは

通信や記録を行う情報に冗長性を付け加えることで、情報通信システムや記録装置で生じた誤りを検出あるいは訂正し、信頼性を高める技術について研究する学問。

1.1 符号理論の広がり

- 情報理論 (通信の限界)
- 通信理論 (変復調方式、物理系)
- 数学 (代数学、確率、組み合わせ論)
- 計算機科学 (アルゴリズム、計算量)
- 計算機ハードウェア (RAID, メモリ構成)

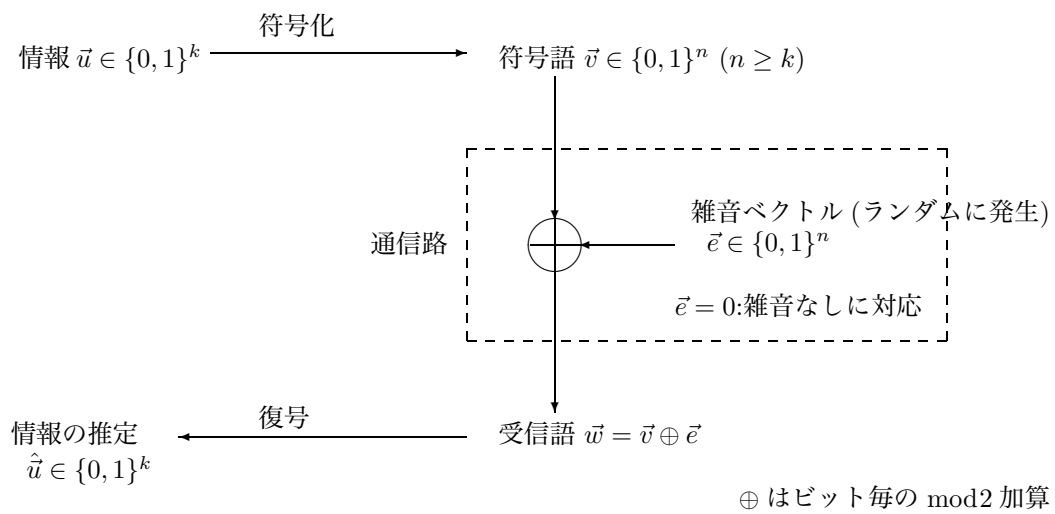
1.2 符号理論の歴史

デジタル情報の様々な通信・記録システムにおいて誤り訂正符号が用いられている。

単一誤り訂正符号	1950	ハミング符号 (唯一個の誤りを訂正できる符号)
複数の誤りを を訂正できる符号	1955	たたみ込み符号 (Elias)
	1959	BCH(Bose-Chaudhuri-Hocquenghem) 符号
	1960	RS(Reed-Solomon) 符号
	1963	Low Density Parity Check(LDPC) 符号 (Gallager)
衛星通信 への応用	1971	Marier 9 号 (火星探査衛星) 双直交符号
	1975	Viking(火星探査衛星) 双直交符号
	1977	Voyager(太陽系探査衛星)
		RS 符号+たたみ込み符号 (NASA の標準技術)
民生機 への応用	1980	音楽用 CD –RS 符号の実用化
	1982	符号化変調方式 (Ungerboeck)
	1985	TV 文字放送 差集合巡回符号 (NHK)
	1988 頃	各種通信用モデム
	1992	MD
	1993	デジタル携帯電話
	1996	CS デジタル放送
	1996	DVD
	1999	1000Base-T (符号化変調方式)
	2004	10GBase-T (LDPC 符号)
新たな符号の発見	⋮	
新たな符号の発見	1993	Turbo 符号 (Berrou, Glavieux ら)
	1996	LDPC 符号の再発見 (MacKay と Neal)

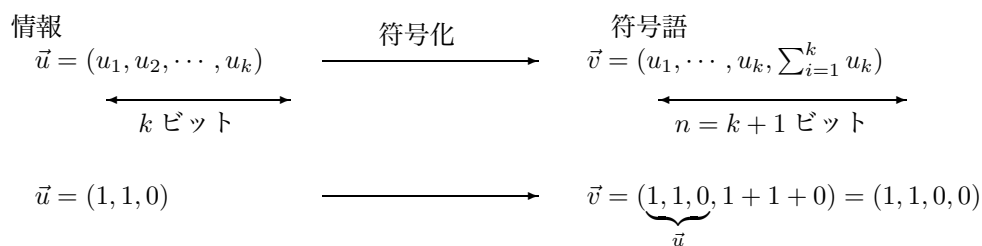
1.3 情報伝送の数学的なモデルの例

情報に冗長性を付け加える操作 : 符号化
誤りの検出や訂正を行なう操作 : 復号化 (復号)



1.4 簡単な誤り検出符号の例

- 単一パリティ検査符号 (Single Parity Check Code)



符号語 $\vec{v} = (1, 1, 0, 0)$ に誤りベクトル $\vec{e} = (1, 0, 0, 0)$ が加わって受信語

$$\vec{w} = \vec{v} + \vec{e} = (1 + 1, 1, 0, 0) = (0, 1, 0, 0)$$

を得る。このとき 1 の個数は奇数なので誤りが生じたことが分かる。受信側では誤りを検出したら送信側に同一符号語の再送を要求する。この操作を誤りを検出しなくなるまで繰り返すことで、符号化を行わないときに比べ信頼の高い通信が行える。

1.5 符号理論の研究テーマ

1. 最良符号はどのような性能を有するか (性能解析)
2. 良い符号はどのように設計法できるか (設計法)
3. そのような符号はどのように復号できるか (復号法)

1.6 線形代数の復習

1) ベクトル空間

集合 V が次の 2 条件を満足するときベクトル空間と呼ぶ。

(I) V の 2 元 x, y に対して和と呼ばれる第三の元 $(x + y)$ が定まり、次の法則が成り立つ。

(1) $(x + y) + z = x + (y + z)$

(2) $x + y = y + x$

(3) ゼロベクトルと呼ばれる特別な元 0 がただ一つ存在し、 V の全ての元 x に対して、 $x + 0 = x$ が成り立つ。

(3) V の全ての元 x に対して、 $x + x' = 0$ となる V の元 x' がただ一つ存在する。

(II) V の任意の元と任意のスカラー a に対し、 x の a 倍とよばれる V の元が定まり、次の法則が成り立つ。

(5) $(a + b)x = ax + bx$

(6) $a(x + y) = ax + ay$

(7) $(ab)x = a(bx)$

(8) $1x = x$ 但し、 1 はスカラーの乗法単位元である。

2) 基底

線形空間 V の有限個のベクトル $e_1, e_2, \dots, e_k$ が次の 2 条件を満足するとき、 $e_1, e_2, \dots, e_k$ は V の基底であるという。また基底ベクトルの個数 k を線形空間 V の次元という。

- (1) $e_1, e_2, \dots, e_k$ は線形独立である。すなわち、

$$a_1 e_1 + a_2 e_2 + \dots + a_k e_k = 0$$

となるようなスカラーの組 $a_1, a_2, \dots, a_k$ は $a_1 = a_2 = \dots = a_k = 0$ に限る。

- (2) V の任意のベクトルは、 $e_1, e_2, \dots, e_k$ の線形結合として書ける。すなわち、任意の $x \in V$ に対して、あるスカラーの組 $a_1, a_2, \dots, a_k$ が存在して、

$$x = a_1 e_1 + a_2 e_2 + \dots + a_k e_k$$

が成り立つ。

3) 部分空間

線形空間 V の部分集合 W が、 V と同じ演算に対して、線形空間になるとき、 W を V の線形部分空間あるいは部分空間と呼ぶ。 W が V の部分空間であるための必要十分条件は、次の 2 条件である。

- (1) 任意の $x, y \in W \implies x + y \in W$
(2) 任意のスカラー a と任意の $x \in W \implies ax \in W$