http://goo.gl/PXyycQ

KYOTO UNIVERSITY

情報理論
誤り訂正符号③

鹿島久嗣
京都大学 情報学研究科 知能情報学専攻

DEPARTMENT OF INTELLIGENCE SCIENCE AND TECHNOLOGY

概要：BCH符号について学びます

- 準備：ガロア体と体の拡大
- BCH符号：巡回符号の一種
  - BCH符号の生成多項式
  - BCH符号の復号

ガロア体

ガロア体（有限体）：加減乗除できる有限集合

- 体： 以下が成り立つ集合
  - 加法と乗法について閉じ、結合法則・分配法則、可換性が成り立つ
  - 以下が存在：
    - 零元（加法）： $x + 0 = 0 + x = x$
    - 単位元（乗法）： $x \cdot 1 = 1 \cdot x = x$
    - 逆元の存在
      - $x + (-x) = (-x) + x = 0$ となる $-x$
      - $x \cdot (x^{-1}) = (x^{-1}) \cdot x = 1$ となる x^{-1}
- ガロア体 $GF(q)$：q 個（位数）の元をもつ有限体
  - $q = p^m$ （p：素数、m：正整数）のときのみ存在

素体：素数個の元をもつガロア体

- ガロア体 $GF(q)$：q 個（位数）の元をもつ有限体
  - $q = p^m$ （p：素数、m：正整数）のときのみ存在
- 素体： $m = 1$ の場合 （ $m > 1$ の場合 拡大体）
  - p 個の整数 $\{ 0, 1, 2, \ldots, p\text{-}1 \}$ の集合
  - mod p の加算・乗算
  - 減算 b - a： b に a の加法に関する逆元 -a を加える
    - $(-a) + a = 0$ mod p を満たす $-a = 0$ (a=0のとき) or p-a
  - 除算 b / a： b に a の乗法に関する逆元 a^{-1} を掛ける
    - $a^{-1}\, a = 1$ mod p を満たす a^{-1} （ユークリッドの互除法等）

素体上の演算例：$GF(2)$ と $GF(3)$ 上の計算

- $GF(2)$：

＋	0	1
0	0	1
1	1	0

×	0	1
0	0	0
1	0	1

−	0	1
0	0	1
1	1	0

／	0	1
0	-	0
1	-	1

- $GF(3)$：

＋	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

×	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

−	0	1	2
0	0	2	1
1	1	0	2
2	2	1	0

／	0	1	2
0	-	0	0
1	-	1	2
2	-	2	1

逆元もここからわかる

拡大体：
素数の2乗以上の位数をもつガロア体の構成

- 位数 $q = p^m$ （$m>1$）のガロア体は mod p の加算・乗算では構成できない（例： $q = 2^2$ で 2 の逆元 2^{-1}がない）
- 拡大体 $GF(p^m)$：素体 $GF(p)$上のひとつの m次原始多項式の根のひとつ α を $GF(p)$ に加えて体をつくったもの
  - 原始多項式：
    周期がちょうど p^m-1の（$G(x) \mid x^{p^m-1} - 1$） m次の多項式
  - イメージは実数体 → 虚数体 への拡大
    - 実数体上の多項式 $x^2 +1 = 0$ の根のひとつ（i）を実数体に加え、体となるために必要な元を加えたもの

拡大体の例：
$GF(2^2)$ を $GF(2)$ の拡大によって構成

- $GF(2)$ 上の多項式 $x^2 + x + 1$ の根 α を$GF(2)$ に付加
- 0, 1, α に加え α のべきは全て含むはず
  - $\alpha^0 = 1, \alpha^1 = \alpha, \alpha^2 = \alpha+1, \alpha^3 = \alpha^2 +\alpha = 1, \ldots.$ 以下同じもの
    - $\alpha^2 + \alpha + 1 = 0$ を利用する
  - 全ての $a_1\alpha+a_0$ のパターンが出尽しており加算について閉じている

+	0	1	α	α^2
0	**0**	1	α	α^2
1	1	**0**	α^2	α
α	α	α^2	**0**	1
α^2	α^2	α	1	**0**

×	0	1	α	α^2
0	0	0	0	0
1	0	**1**	α	α^2
α	0	α	α^2	**1**
α^2	0	α^2	**1**	α

逆元の存在も確認

拡大体の演算：
拡大体の構成に用いた原始多項式を利用

- 素体 $GF(2)$ の m次の拡大体 $GF(2^m)$ は 0 と m次原始多項式
  $F(x) = x^m + f_{m-1}x^{m-1} + \ldots + f_1 x + 1$
  の根 α のべき $\alpha^0, \alpha^1, \ldots, \alpha^{2^m-1}$ によって構成できる
  - $\alpha^{2^m-1} = 1$ (2^m-1は非零のm次多項式の数)
- 積の計算： $\alpha^i \alpha^j = \alpha^{i+j \bmod 2^m-1}$
- 逆元： $\alpha^{-i} = \alpha^{2^m-1-i \bmod 2^m-1}$
- 加算：$F(\alpha) = 0$ より $\alpha^m = f_{m-1}\alpha^{m-1} + \ldots + f_1\alpha + 1$ を用いて、任意の $\alpha^i = a_{m-1}\alpha^{m-1} + \ldots + a_1\alpha + 1$ として表せるので、ベクトル表現 $(a_{m-1}, a_{m-1}, \ldots, a_1)$ しておくと便利
  - 係数同志の加算によって、$\alpha^i + \alpha^j$ を計算できる

ベクトル表現の例：
拡大体$GF(2^4)$ のベクトル表現

- $GF(2^4)$ を $x^4 + x + 1$ の根 α からつくる （$\alpha^{15}=1$）
- 計算例：

$$\alpha^3\underbrace{(\alpha^7+\alpha^5)}_{\text{ベクトル表現のち加算}}{}^3 + \frac{\alpha^9+\alpha^3}{1+\alpha^{10}}$$

$$= \alpha^3\underbrace{(\alpha^{13})^3}_{\bmod 15} + \frac{\alpha}{\alpha^5}$$

逆元

$$= \alpha^3 \cdot \alpha^9 + \alpha \cdot \alpha^{10}$$

$$= \alpha^{12} + \alpha^{11}$$

$$= 1$$

べき表現	展開	ベクトル表現
0	0	0000
1	1	0001
α	α	0010
α^2	α^2	0100
α^3	α^3	1000
α^4	$\alpha + 1$	0011
α^5	$\alpha^2 + \alpha$	0110
α^6	$\alpha^3 + \alpha^2$	1100
α^7	$\alpha^3 + \alpha + 1$	1011
α^8	$\alpha^2 + 1$	0101
α^9	$\alpha^3 + \alpha$	1010
α^{10}	$\alpha^2 + \alpha + 1$	0111
α^{11}	$\alpha^3 + \alpha^2 + \alpha$	1110
α^{12}	$\alpha^3 + \alpha^2 + \alpha + 1$	1111
α^{13}	$\alpha^3 + \alpha^2 + 1$	1101
α^{14}	$\alpha^3 + 1$	1001

BCH符号

BCH符号：
巡回符号の一種

- ブロック長や誤り訂正をカスタマイズ可能な巡回符号の一種
  - 符号化は生成多項式 $G(x)$ を用いて行う
  - 復号化はシンドロームに基づいて比較的簡単に行える
- m と t をパラメータとして
  - 符号長： $n = 2^m - 1$
  - 情報ビット数：$k \geq 2^m - 1 - mt$
    （誤り訂正に最大mt ビット使用）
  - 誤り訂正能力： $t_0 \geq t$

  をもつ

BCH符号の定義：原始多項式の根のべきを根にもつ生成多項式を用いる

- BCH符号：$GF(2^m)$ の原始元 α として、$\alpha, \alpha^2, \ldots, \alpha^{2t}$ のすべてを根とする最小次数の$GF(2)$上の多項式を生成多項式 $G(x)$ として用いる巡回符号
- 実は $\alpha, \alpha^3, \ldots, \alpha^{2t\text{-}1}$ の t 個を根とする最小次数の多項式でよい
  - 理由： $F(x) = f_m x^m + f_{m\text{-}1} x^{m\text{-}1} + \ldots + f_1 x + f_0$ に対して、$[F(x)]^2 = F(x^2)$ であるから α^i が $F(x)$ の根なら α^{2i} もまた根
  - このような多項式の次数は mt 以下
- BCH符号の能力：最小距離は $d = 2t + 1$ 以上
  （d をBCH限界と呼ぶ）

BCH符号の生成多項式の例：連立方程式を解き生成多項式の係数を求める

- 原始多項式 $x^4 + x + 1$ $(m=4)$； $t=2$ ；符号長 $n= 15$
- 生成多項式の次数 $mt=8$ なので
  $G(x) = g_8 x^8 + g_7 x^7 + \ldots + g_1 x + 1$ とおく
- $G(x)$ は α と $\alpha^{2t\text{-}1} = \alpha^3$ を根にもつので、連立方程式：
  - $G(\alpha) = g_8 \alpha^8 + g_7 \alpha^7 + \ldots + g_1 \alpha + 1 = 0$
  - $G(\alpha^3) = g_8 x^{24} + g_7 x^{21} + \ldots + g_1 x^3 + 1 = 0$

  を解く（次頁）
- 解は $(g_8, g_7, \ldots, g_1) = (1, 1, 1, 0, 1, 0, 0, 0)$
  生成多項式は $G(x) = x^8 + x^7 + x^6 + x^4 + 1$

連立方程式の例：
p.9 のベクトル表現をもとに連立方程式を構成

$$G(\alpha) = g_8\alpha^8 + g_7\alpha^7 + \ldots + g_1\alpha + 1 = 0$$

$$G(\alpha^3) = g_8x^{24} + g_7x^{21} + \ldots + g_1x^3 + 1 = 0$$

α^8 のベクトル表現

ひとつめの式に対応 $\alpha^8,\ldots,\alpha$

ふたつめの式に対応 $\alpha^{24},\ldots,\alpha^3$

$$\begin{pmatrix} 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} g_8 \\ g_7 \\ g_6 \\ g_5 \\ g_4 \\ g_3 \\ g_2 \\ g_1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

BCH符号の復号

BCH符号の誤り検出：
シンドロームを計算して誤りを検出する

- 受信語を $Y(x) = y_{n\text{-}1}\, x^{n\text{-}1} + y_{n\text{-}2}\, x^{n\text{-}2} + \ldots + y_1\, x + y_0$ として：
  - 符号多項式 $V(x) = v_{n\text{-}1}\, x^{n\text{-}1} + v_{n\text{-}2}\, x^{n\text{-}2} + \ldots + v_1\, x + v_0$
  - 誤りパターン $E(x) = e_{n\text{-}1}\, x^{n\text{-}1} + e_{n\text{-}2}\, x^{n\text{-}2} + \ldots + e_1\, x + e_0$

  とすると、$Y(x) = V(x) + E(x)$ ならびに $V(\alpha^i) = 0$ より

  シンドロームが $S_i = Y(\alpha^i) = E(\alpha^i)$ （ i=1,2,…,2t ）
  - なお $Y(x^2) = [Y(x)]^2 \to S_{2i} = (S_i)^2$ より
    偶数番目のシンドロームは他から計算可能
- シンドローム $\{S_i\}_i$ が全て零であれば、誤りがないと判断する

BCH符号の誤り訂正：
誤り位置方程式を解く

- l 個の誤り位置を $j_1, j_2, \ldots, j_l$ とする
- 誤り位置方程式 ：$\sigma(x) = (1\text{-}\alpha^{j1}z)\,(1\text{-}\alpha^{j2}z)\cdots(1\text{-}\alpha^{jl}z)$ を考える
  - $\sigma(x)$ の根は $\alpha^{-j1}, \alpha^{-j2}, \ldots, \alpha^{-jl}$
- このような $\sigma(x)$ が得られたとすると、
  $\sigma(x)$ に $1, \alpha, \alpha^2, \ldots$ と代入していくことで誤り位置を調べる
  - $\sigma(\alpha^i) = 0$ になったとすると、i の逆元 $-i$ が誤り位置
- 注意：誤り位置方程式の構成は自明ではない

誤り位置方程式の構成：
誤りが 2個 (t = 2) の場合

- 誤り位置方程式 ：
  $\sigma(x) = (1 - \alpha^{j1}z)\,(1 - \alpha^{j2}z) = 1 + (\alpha^{j1} + \alpha^{j2})z + \alpha^{j1}\alpha^{j2}z^2$
  - 根は $\alpha^{-j1}, \alpha^{-j2}$
- シンドロームを計算する：
  - $S_1 = E(\alpha) = \alpha^{j1} + \alpha^{j2}$
  - $S_3 = E(\alpha^3) = \alpha^{3j1} + \alpha^{3j2}$
- $S_1{}^3 = (\alpha^{j1} + \alpha^{j2})^3 = \alpha^{3j1} + \alpha^{3j2} + \alpha^{j1}\alpha^{j2}(\alpha^{j1} + \alpha^{j2}) = S_3 + \alpha^{j1}\alpha^{j2} S_1$
  より $\alpha^{j1}\alpha^{j2} = (S_1{}^3+S_3)\,S_1{}^{-1}$
- $\sigma(x) = 1+ S_1z + (S_1{}^3 + S_3)\,S_1{}^{-1}z^2$

BCH符号による誤り訂正の例：
誤りが 2個 (t = 2) の場合

- 受信語： (000100010000000) の多項式 $Y(x) = x^{11}+ x^7$
- シンドロームの計算：
  - $S_1 = Y(\alpha) = \alpha^{11}+\alpha^7 = \alpha^8$,
  - $S_3 = Y(\alpha^3) = \alpha^{33}+\alpha^{21} = \alpha^2$

  より $\sigma(x) = 1+ \alpha^8 z + (\alpha^{24}+\alpha^2)\,\alpha^{-8}z^2 = 1+ \alpha^8 z + \alpha^3 z^2$
- $\sigma(1), \sigma(\alpha), \sigma(\alpha^2), \ldots$ を調べていくと $\alpha^4 = \alpha^{-11}, \alpha^8 = \alpha^{-7}$ が根
  → 誤り位置は 11, 7 番目
- 符号語は 000….0 とわかる