http://goo.gl/PXyycQ

KYOTO UNIVERSITY

情報理論
誤り訂正符号②

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

符号の多項式表現

符号語の多項式表現：
ひとつの符号語はブール多項式の係数として表現できる

- 符号多項式： 符号語 $v = (v_0, v_1, \ldots, v_{n\text{-}1})$ を
  多項式 $V(x) = v_{n\text{-}1}\, x^{n\text{-}1} + v_{n\text{-}2}\, x^{n\text{-}2} + \ldots + v_1\, x + v_0$ に対応させる
  – ただし、v_i, $x_i \in \{0, 1\}$
- 例： $v = (1,0,1,0,0,1,1) \to V(x) = x^6 + x^4 + x + 1$

ブール多項式の加減乗除：
「ビット毎の演算」が原則（繰り上げ・繰り下げなし）

- 「ビット毎の演算」が原則（繰り上げ・繰り下げなし）
- $G(x) = x^4 + x^3 + x^2 + 1$
- $A(x) = x^2 + x + 1$
- $G(x)\ A(x) = x^6 + x^4 + x + 1$
- $X'(x) = x^6 + x^4 = (x^4 + x^3 + x^2 + 1)(x^2 + x + 1) + x + 1$

ブール多項式の周期：
x^p-1 を割り切る最小の p

- 多項式$G(x)$が多項式$H(x)$を割り切るとき $G(x) \mid H(x)$ とかく
- 周期：$G(x) \mid x^p-1$となる最小のpを$G(x)$の周期と呼ぶ
- 例：$G(x) = x^4 + x^3 + x^2 + 1$ の周期は7
  - $G(x)$ は x^7-1 を割り切るが x^l-1 $(l = 1,2,\ldots,6)$ は割り切らない

巡回符号

巡回符号：生成多項式から作られる線形符号

- 生成多項式 (m次)： $G(x) = x^m + g_{m-1} x^{m-1} + \ldots + g_1 x + 1$
  - 注：0次とm次のビットは1
- 巡回符号：n-1次以下の符号多項式
  $V(x) = v_{n-1} x^{n-1} + v_{n-2} x^{n-2} + \ldots + v_1 x + v_0$ で表現される符号で、$G(x)$ で割り切れるもの
  - $V(x) = G(x)\, A(x)$ となる （ $A(x)$ は n-m-1 次）
- 線形性： $V_1(x) + V_2(x)$ も符号多項式
- なにが「巡回」なのかはしばらく忘れる

巡回符号の符号化（準備）：情報ビットの右側に数個の 0 を付与し符号多項式表現

- 生成多項式 $G(x)$ を考える
  - 例： m=4, $G(x) = x^4 + x^3 + x^2 + 1$
- 情報ビット（k ビット）を符号多項式として表す：
  $X(x) = x_{k-1} x^{k-1} + x_{k-2} x^{k-2} + \ldots + x_1 x + x_0$
  - 例：k = 3, (1,0,1) ⇔ $X(x) = x^2 + 1$
- $X(x)$ に x^m を掛ける：
  $x^m X(x) = x_{k-1} x^{k+m-1} + x_{k-2} x^{k+m-2} + \ldots + x_1 x^{m+1} + x_0 x^m$
  - 右側に m個の 0 を付加する操作 （→ 後に検査ビットになる）
  - 例：$x^4 X(x) = x^6 + x^4$ ⇔ (1,0,1,$\underline{0,0,0,0}$)

巡回符号の符号化（検査ビットの生成準備）：生成多項式で割った余りを検査ビットとする

- $x^m\, X(x)$ を$G(x)$で割った余り$C(x)$を$x^m\, X(x)$に加える：
- 符号多項式は $V(x) = x^m\, X(x) + C(x)$
  - $x^m\, X(x) = G(x)\, A(x) + C(x)$
    - 例： $x^4 X(x) = x^6 + x^4 = (x^4 + x^3 + x^2 + 1)(x^2 + x + 1) + x + 1$
      - $A(x) = x^2 + x + 1,\ C(x) = x + 1 \Leftrightarrow (0,0,1,1)$
  - $C(x)$ は m-1次以下なので末尾に付加した0を置き換える
    - 例： $(1,0,1,\underline{0,0,0,0}) + C(x) = (1,0,1,\underline{0,0,1,1})$
  - 符号多項式は $G(x)A(x)$ と捉えてもよい（計算上は↑が有利）
    - $V(x) = x^m\, X(x) + C(x) = G(x)A(x)$

巡回符号の誤り訂正・検出：生成多項式で割る

- 誤り訂正：
  - 予め1ビットだけ1であるとベクトル $(0,\ldots,0,1,0,..,0)$ に対して、$G(x)$で割った余りを計算してシンドロームの表を作っておく
  - 検出時には受信した符号を$G(x)$で割った余りを表に当てはめる
- 誤り検出：
  - 受信した符号を$G(x)$で割ってみて、余りが出なければ誤りなしと判断
  - 符号語は $V(x) = G(x)A(x)$ を満たす筈

巡回符号の性質

巡回符号の符号長の制限：誤り訂正を保証するためには符号長は周期以下にする

- 符号長 n は 生成多項式 $G(x)$ の周期 p 以下にする必要がある
  - $n > p$ のとき、1ビットの誤り訂正が保証されない
    - 理由：
      - $G(x) \mid x^p - 1$ より $x^p - 1 = G(x)A(x)$
        $n > p$ のとき、これは符号多項式になる
      - $x^p - 1$を符号にすると $(0,\ldots,0,1,0,..,0,1,\underline{0,\ldots,0})$ という形になる
      - この符号の重みは2なので、最小距離は2以下になる
  - 例：$G(x) = x^4 + x^3 + x^2 + 1$ の周期は 7 で、
    前述の符号の符号長は7 （周期と符号長が一致）

巡回符号の「巡回」性：
符号語を巡回置換してもまた符号語になる

- 符号多項式 $V(x) = v_{n\text{-}1}\, x^{n\text{-}1} + v_{n\text{-}2}\, x^{n\text{-}2} + \ldots + v_1\, x + v_0$ に対して
  $$V'(x) = v_{n\text{-}2}\, x^{n\text{-}1} + v_{n\text{-}1}\, x^{n\text{-}2} + \ldots + v_0\, x + v_{n\text{-}1}$$
  $$= x\ V(x) + v_{n\text{-}1}\,(\, x^n\ \text{-}1)$$
  を考える
  - 係数を「ひとつ回した」もの
  - $G(x) \mid x^n$ -1 ならば $V'(x)$ も符号多項式
    - $G(x)$ の周期を p とすると、n=p とすればよい
- 巡回符号：符号語を何回「回して」も符号語になるもの