教育課題演習　第 7 回　巡回符号と多項式

１．符号を多項式で表す

GF(2)の要素からなる符号 $a_0, a_1, \cdots, a_{n-1}$ を多項式 $a_0+a_1x+\cdots+a_{n-1}x^{n-1}$ で表す。符号のベクトル和は多項式の和と一致する。

符号の右シフトを x 倍することで表すために，$x^n=1$ と約束する。

$P(x) = a_0+a_1x+\cdots+a_{n-1}x^{n-1}$ のとき，

$xP(x) = a_0x+a_1x^2+\cdots+a_{n-1}x^n = a_{n-1}+a_0x+a_1x^2+\cdots+ a_{n-2}x^{n-1}$ となるから，

$xP(x)$は，$a_{n-1}, a_0, a_1, \cdots, a_{n-2}$ を表す。

Note.　$x^n=1$ と約束することは，x^n-1 を法とする剰余系で考えることを意味する。

$G(x) = 1+x^2+x^3+x^4$ のとき，$x^kG(x)$ $(k=0,1,2,\cdots,6)$は $(a_0+a_1x+a_2x^2)G(x)$ $(a_0, a_1, a_2\in\mathrm{GF}(2))$ の形に書けた。そのカラクリを探る。

例 1

$x^7-1=(1+x)(1+x+x^3)(1+x^2+x^3)=(1+x+x+x^2+x^3+x^4)\ (1+x^2+x^3)= (1+x^2+x^3)(\ 1+x^2+x^3+x^4)$

なので，$G(x) = 1+x^2+x^3+x^4$ とおくと，$x^7-1= (1+x^2+x^3)G(x)$　だから

$x^3G(x) = (1+x^2)G(x)+(x^7-1)$であり，

$x^3G(x)\equiv(1+x^2)G(x) \pmod{x^7-1}$

$x^4G(x)\equiv xG(x)+x^3G(x)\equiv(1+x+x^2)G(x) \pmod{x^7-1}$

$x^5G(x)\equiv(x+x^2)G(x)+x^3G(x)\equiv(1+x)G(x) \pmod{x^7-1}$

$x^6G(x)\equiv(x+x^2)G(x) \pmod{x^7-1}$

となって，$x^kG(x)$ $(k=0,1,2,\cdots,6)$ は $(a_0+a_1x+a_2x^2)G(x)$ $(a_0, a_1, a_2\in\mathrm{GF}(2))$の形に書ける。

ここでは，合同式 $x^3G(x)\equiv(1+x^2)G(x)$ によって $G(x)$に掛かる x の多項式の次数を減らせることが効いている。

$G(x)$が x^7-1 の因数であることが本質的である。そのことを確認しよう。

問題 1

(1)　$G(x)= 1+x+x^2+x^4$ のとき。$x^7-1= (1+x+x^3)G(x)$である。$x^kG(x)$ $(k=0,1,2,\cdots,6)$ は $(a_0+a_1x+a_2x^2)G(x)$ $(a_0, a_1, a_2\in\mathrm{GF}(2))$の形に書けることを確かめよ。

(2)　$G(x)= 1+x+x^3$ のとき。$x^7-1= (1+x+x^2+x^4)G(x)$である。$x^kG(x)$ $(k=0,1,2,\cdots,6)$は $(a_0+a_1x+a_2x^2+a_3x^3)G(x)$ $(a_0, a_1, a_2, a_3\in\mathrm{GF}(2))$の形に書けることを確かめよ。

(3)　$G(x)= 1+x^2+x^3$ のとき。$x^7-1= (1+x^2+x^3+x^4)G(x)$である。$x^kG(x)$ $(k=0,1,2,\cdots,6)$は $(a_0+a_1x+a_2x^2+a_3x^3)G(x)$ $(a_0, a_1, a_2, a_3\in\mathrm{GF}(2))$の形に書けることを確かめよ。

問題 2

例 1 で $G(x)$が表す符号の 1 でないビットの個数が 4 であることから，$(a_0+a_1x+a_2x^2)G(x)$

$(a_0, a_1, a_2 \in \mathrm{GF}(2))$の形の多項式が表す符号の全体において，異なる符号間のハミング距離が 4 であると結論することができる。その理由を説明せよ。

ヒント　$(a_0+a_1x+a_2x^2)G(x)$ $(a_0, a_1, a_2 \in \mathrm{GF}(2))$の形の符号の和（差）も再びこの形になることと，その全体が巡回符号となっていることのいずれもが結論に寄与している。

u と v のハミング距離（異なる要素の個数）を $\mathrm{d}(u, v)$で表す。

v の 0 でない要素の個数を $\mathrm{w}(v)$で表す。

$\mathrm{w}(u_1)=\mathrm{w}(u_2)=\cdots=\mathrm{w}(u_7)=4$ といえるのはなぜか。

$i \neq j$ のとき $\mathrm{d}(u_i, u_j)=4$ であることが導かれる。なぜか？

例 1 では，$(a_0+a_1x+a_2x^2)G(x)$ $(a_0, a_1, a_2 \in \mathrm{GF}(2))$の非零な要素の全体と，$x^kG(x)$の形の多項式の全体とが一致している。すなわち，$(a_0+a_1x+a_2x^2)G(x)$ $(a_0, a_1, a_2 \in \mathrm{GF}(2))$は，巡回符号を生成している。

問題 3

問題 1 の(1)について，

(1) $(a_0+a_1x+a_2x^2)G(x)$ $(a_0, a_1, a_2 \in \mathrm{GF}(2))$の形の非零な多項式が $x^kG(x)$の形に表せるか，調べなさい。

(2) $(a_0+a_1x+a_2x^2)G(x)$ $(a_0, a_1, a_2 \in \mathrm{GF}(2))$の形の多項式が表す符号の全体において，異なる符号間のハミング距離を求めよ。

(3) 例 1 の符号との違いは何か？

問題 1 の(2)，(3)では，$(a_0+a_1x+a_2x^2+a_3x^3)G(x)$ $(a_0, a_1, a_2, a_3 \in \mathrm{GF}(2))$の形の非零多項式は $2^4-1(=15)$通りあるのに，$x^7=1$ とするから，$x^kG(x)$の形の多項式は 7 通りしかない。$(a_0+a_1x+a_2x^2+a_3x^3)G(x)$ $(a_0, a_1, a_2, a_3 \in \mathrm{GF}(2))$の形の符号の全体についてどんなことがいえるか。