教育課題演習　第 6 回　線形符号

１．巡回符号をベクトルで表す

	x_1	x_2	x_3	c_1	c_2	c_3	c_4
u_0	0	0	0	0	0	0	0
u_1	0	0	1	0	1	1	1
u_2	0	1	0	1	1	1	0
u_3	1	0	1	1	1	0	0
u_4	0	1	1	1	0	0	1
u_5	1	1	1	0	0	1	0
u_6	1	1	0	0	1	0	1
u_7	1	0	0	1	0	1	1

u_0～u_7 を 7 個の要素 x_1，x_2，x_3，c_1，c_2，c_3，c_4 からなるベクトルとみなし，２つのベクトル u, v に対し成分ごとに⊕の和を取ったものを $u⊕v$ で表す。

Note. 第 4 回の巡回符号と同じ表であるが，u_1~u_8 の番号を 1 だけ減らした。

例　$u_1⊕u_2$=(0⊕0, 0⊕1, 1⊕0, 0⊕1, 1⊕1, 1⊕1, 1⊕0)= (0, 1, 1, 1, 0, 0, 1)=u_4

$u_i⊕u_j$

＼	u_1	u_2	u_3	u_4	u_5	u_6	u_7
u_1		u_4					
u_2							
u_3							
u_4							
u_5							
u_6							
u_7							

問題 1

u と v のハミング距離（異なる要素の個数）を d(u, v)で表す。　　d…distance

また，v の 0 でない要素の個数を w(v)で表す。　　w…weight

w(u_1)=w(u_2)=…=w(u_7)=4 と上の表とから，$i≠j$ のとき d(u_i, u_j)=4 であることが導かれる。なぜか？

ヒント　w($u_i⊕u_j$)は何か？

２．巡回符号を多項式で表す

GF(2)の要素からなる符号 a_0, a_1, …, 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。

たとえば，$a_{n-1}x^n= a_{n-1}+ a_{n-1}$ (x^n-1)なので，$a_{n-1}x^n \equiv a_{n-1} \pmod{x^n-1}$

合同式　a, b を k で割った余りが等しいことを $a \equiv b$（mod k）で表す。

前ページの u_3 は　$G(x) = 1+x^2+x^3+x^4$ で表される。7 ビットの符号なので，$x^7=1$ として計算する。

問題 2

(1)　$u_1 \sim u_7$ を $x^kG(x)$の形で表せ。

(2)　$u_0 \sim u_7$ を$(a_0+a_1x+a_2x^2)\ G(x)$ $(a_0, a_1, a_2 \in \mathrm{GF}(2))$の形に表せ。

ヒント　$u_i \oplus u_j$ の表が利用できる

(3)　$G(x)$を因数分解せよ。

ヒント　$G(1)=0$ だから $G(x)$は $x+1$ で割り切れる。