誤り訂正符号

三谷政昭著,「やり直しのための工業数学」, インターフェース増刊（CQ 出版）2001 年 1 月　第 2 部による。

ハミングの方法

4 ビットのデータ x_1, x_2, x_3, x_4 を送るとき，次式で定められる検査ビット(冗長ビット)c_1, c_2, c_3 を付加した 7 ビットを送る。

$c_1 = x_2 \oplus x_3 \oplus x_4$

$c_2 = x_1 \oplus x_3 \oplus x_4$

$c_3 = x_1 \oplus x_2 \oplus x_4$

ここで，⊕は，mod 2 の加算で，$0 \oplus 0 = 1 \oplus 1 = 0$，$1 \oplus 0 = 0 \oplus 1 = 1$。

伝送時の誤りが 1 ビット以下であれば,

$s_1 = x_4 \oplus c_1 \oplus c_2 \oplus c_3$

$s_2 = x_2 \oplus x_3 \oplus c_2 \oplus c_3$

$s_3 = x_1 \oplus x_3 \oplus c_1 \oplus c_3$

とし，$s = 4s_1 + 2s_2 + s_3$ とすると，

$s = 0$ のとき，誤りなし

$1 \leqq s \leqq 4$ のとき，x_s が誤り

$5 \leqq s$ のとき，c_{s-4} が誤り

と判定できる。

例

1101（$x_1 = 1, x_2 = 1, x_3 = 0, x_4 = 1$）を送るとき，

$c_1 = 1 \oplus 0 \oplus 1 = 0$

$c_2 = 1 \oplus 0 \oplus 1 = 0$

$c_3 = 1 \oplus 1 \oplus 1 = 1$

を付加して送信する。

このとき，誤りなく伝送されれば,

$s_1 = 1 \oplus 0 \oplus 0 \oplus 1 = 0$

$s_2 = 1 \oplus 0 \oplus 0 \oplus 1 = 0$

$s_3 = 1 \oplus 0 \oplus 0 \oplus 1 = 0$,

4 ビットを間違えて $x_4 = 0$ になってしまったとすると,

$s_1 = 0 \oplus 0 \oplus 0 \oplus 1 = 1$

$s_2 = 1 \oplus 0 \oplus 0 \oplus 1 = 0$

$s_3 = 1 \oplus 0 \oplus 0 \oplus 1 = 0$

となって $s = 4 \times 1 + 2 \times 0 + 0 = 4$ より x_4 に誤りがあることが分かる（訂正できる)。

しかし，伝送時の誤りが 2 ビットある場合には，たとえば，x_4 と c_1 を間違えたとき,

$s_1 = 0 \oplus 1 \oplus 0 \oplus 1 = 0$

$s_2 = 1 \oplus 0 \oplus 0 \oplus 1 = 0$

$s_3 = 1 \oplus 0 \oplus 1 \oplus 1 = 1$

となるから，x_1 を間違えたと判断し，元の符号は 0100 であったと判断してしまう。(誤りであることの検出もできない)

巡回符号

	x_1	x_2	x_3	c_1	c_2	c_3	c_4
u_1＝	0	0	0	0	0	0	0
u_2＝	0	0	1	0	1	1	1
u_3＝	0	1	0	1	1	1	0
u_4＝	1	0	1	1	1	0	0
u_5＝	0	1	1	1	0	0	1
u_6＝	1	1	1	0	0	1	0
u_7＝	1	1	0	0	1	0	1
u_8＝	1	0	0	1	0	1	1

はじめの 3 ビット x_1，x_2，x_3 が情報ビット，残りの 4 ビット c_1，c_2，c_3，c_4 が検査ビット。

u_1～u_8 では,

$c_1＝x_1⊕x_2$

$c_2＝x_2⊕x_3$

$c_3＝x_1⊕x_2⊕x_3$

$c_4＝x_1⊕x_3$

となっている。そこで,

$e_1＝c_1⊕x_1⊕x_2$

$e_2＝c_2⊕x_2⊕x_3$

$e_3＝c_3⊕x_1⊕x_2⊕x_3$

$e_4＝c_4⊕x_1⊕x_3$

とおくと，伝送に誤りがなければ e_1～e_4 はすべて 0 となる。

誤りが 1 ビットのみのとき e_1～e_4 のうちの 1 個または 3 個が 1 となる。

c_1～c_4 が誤りのときは，e_1～e_4 のうちの対応する番号のもののみが 1 となる。

x_1 が誤りのとき，e_1，e_3，e_4 が 1 となる。

x_2 が誤りのとき，e_1，e_2，e_3 が 1 となる。

x_3 が誤りのとき，e_2，e_3，e_4 が 1 となる。

誤りが 2 ビットあるとき e_1～e_4 のうちの 2 個または 4 個が 1 となる。

c_1～c_4 が誤りのときは，e_1～e_4 のうちの対応する番号のもの 2 個が 1 となる。

x_1，x_2 が誤りのとき，e_2，e_4 が 1 となる。

x_1，x_3 が誤りのとき，e_1，e_2 が 1 となる。

x_2，x_3 が誤りのとき，e_1，e_4 が 1 となる。

情報ビットと検査ビットが 1 つずつ誤りであるとき e_1～e_4 のうちの 2 個または 4 個が 1。

誤りが 3 ビットあるとき e_1～e_4 のうちの 1 個または 3 個が 1 となる。

なぜなら，e_1～e_4 には，c_1～c_4 が各 1 個，x_1～x_3 が各 3 個含まれる。

だから, 伝送経路での誤りが 2 ビット以下であることが保証されていれば, 誤りの存在が検出できて, しかも, 誤りが 1 ビットであれば訂正可能。

伝送経路での誤りが 3 ビット以下であることしか保証されない場合は，誤りの検出のみ可能（訂正できない）

伝送経路での誤りが 4 ビット以下であることしか保証されない場合は，誤りの検出もできない。

たとえば，x_1，x_2，c_2，c_4 が誤りのとき，e_1～e_4 はすべて 0 となる。

ハミング距離

２つの符号について，符号間の異なるビットの個数をハミング距離という（6.4)。

〔表8.1〕
巡回符号の例

通　報	符　号	
	情報ビット	検査ビット
u_1	0 0 0	0 0 0 0
u_2	0 0 1	0 1 1 1
u_3	0 1 0	1 1 1 0
u_4	1 0 1	1 1 0 0
u_5	0 1 1	1 0 0 1
u_6	1 1 1	0 0 1 0
u_7	1 1 0	0 1 0 1
u_8	1 0 0	1 0 1 1

表 8.1 の巡回符号では，各符号間のハミング距離はすべて 4 である。
だから，伝送経路での誤りが 3 ビット以下であれば誤りの検出が可能である。
また，伝送経路での誤りが 2 ビット以下であれば，誤りの検出と 1 ビットの誤りの訂正が可能。
ハミング距離の調べ方…2 符号の各ビットごとに⊕演算を行った結果の 1 の個数。

巡回符号の多項式表現

符号語 a_0，a_1，a_2，…，a_{n-1} を多項式 $a_0+a_1x+a_2x^2+\cdots+a_{n-1}x^{n-1}$ で表す。係数は 2 を法とする剰余系。
このとき，表 8.1 の符号語は，

$u_1=0$

$u_2=x^2+x^4+x^5+x^6=x^2(1+x^2+x^3+x^4)$

$u_3=x+x^3+x^4+x^5=x(1+x^2+x^3+x^4)$

$u_4=1+x^2+x^3+x^4$

$u_5=x+x^2+x^3+x^6=(x+x^2)(1+x^2+x^3+x^4)$

$u_6=1+x+x^2+x^5=(1+x)(1+x^2+x^3+x^4)$

$u_7=1+x+x^4+x^6=(1+x+x^2)(1+x^2+x^3+x^4)$

$u_8=1+x^3+x^5+x^6=(1+x^2)(1+x^2+x^3+x^4)$

u_4 は生成多項式であるという。
$x^7=1$ として計算する（つまり，x^7-1 を法とする剰余系で考える）と，
$(1+x^2+x^3+x^4)(1+x^2+x^3)=x^7-1=0$ だから，
$x^3(1+x^2+x^3+x^4)=(1+x^2)(1+x^2+x^3+x^4)=u_8$
$x^4(1+x^2+x^3+x^4)=(x+x^3)(1+x^2+x^3+x^4)=(1+x+x^2)(1+x^2+x^3+x^4)=u_7$
$x^5(1+x^2+x^3+x^4)=(x+x^2+x^3)(1+x^2+x^3+x^4)=(1+x)(1+x^2+x^3+x^4)=u_6$
$x^6(1+x^2+x^3+x^4)=(x+x^2)(1+x^2+x^3+x^4)=u_5$
ハミング距離の計算
u_1～u_8 から異なる 2 個を選んで加算(⊕)すると，u_2～u_8 のいずれかになる。だからハミング距離は４。

巡回符号の作り方

$n=k+m$ とする。$G(x)$を x^n-1 を割り切る m 次多項式とする。

このとき，$G(x)$，$xG(x)$，$x^2G(x)$，…，$x^{k-1}G(x)$，および，これらの和の形の 2^k 個の多項式は巡回符号を構成する。

例

k=4，m=3，$G(x)=1+x^2+x^3$ とする。

$x^7=1$ として計算する（つまり，x^7-1 を法とする剰余系で考える）と，

$(1+x^2+x^3+x^4)(1+x^2+x^3)=x^7-1=0$ だから，

$xG(x)$

$x^2G(x)$

$x^3G(x)$

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

$x^5G(x)=x(1+x^2+x^3)\ G(x)=(x+x^3+x^4)\ G(x)=(x+x^3+1+x^2+x^3)\ G(x)=(1+x+x^2)\ G(x)$

$x^6G(x)=x(1+x+x^2)\ G(x)=(x+x^2+x^3)\ G(x)$

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

$H(x)=(1+x^2)\ G(x)\ =\ (1+x^2)(1+x^2+x^3)=1+x^3+x^4+x^5$

$xH(x)=x(1+x^2)\ G(x)=(x+x^3)\ G(x)$

$x^2H(x)=(x^2+x^4)\ G(x)=(1+x^3)\ G(x)$

$x^3H(x)=(x+x^4)\ G(x)=(x+1+x^2+x^3)\ G(x)=(1+x+x^2+x^3)\ G(x)$

$x^4H(x)=(x+x^2+x^3+x^4)\ G(x)\ =(x+x^2+x^3+1+x^2+x^3)\ G(x)\ =(1+x)\ G(x)$

$x^5H(x)=(x+x^2)\ G(x)$

$x^6H(x)=(x^2+x^3)\ G(x)$

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

$(1+x+x^3)\ (1+x^2+x^3)=1+x+x^2+x^3+x^4+x^5+x^6$

上記および0のうち異なる2個を加算すると，上記のいずれかになるから，ハミング距離は3,4,7のいずれか。

すなわち，最小ハミング距離は3。

ガロア体

p が素数であるとき，mod p の剰余系は体。

元の個数が有限の体をガロア体という。

元の個数が q のガロア体を GF(q)で表し，q を位数という。

GF(2)… mod 2 の剰余系

GF(2^m)の構成（$m>1$）

$f(x)$を GF(2)上の m 次の既約多項式とする。

GF(2)に $f(\alpha)=0$ なる元 α を追加する。

$a_1+a_2\alpha+a_3\alpha^2+\cdots+a_m\alpha^{m-1}$（$a_1$，$a_2$，…，$a_m$ は0または1）の全体を考えると，加法および乗法について閉じている。

しかも，すべて異なる。なぜなら，これらのうちに等しいものがあれば，$a_1+a_2\alpha+a_3\alpha^2+\cdots+a_m\alpha^{m-1}=0$（$a_1$，$a_2$，…，$a_m$ のうち少なくとも 1 つは 1）となるが，$g(x)=a_1+a_2x+a_3x^2+\cdots+a_m\ x^{m-1}$ とおくと，$f(x)$と $g(x)$は GF(2)上の多項式とみて互いに素だから，$P(x)f(x)+Q(x)g(x)=1$ となる GF(2)上の多項式 $P(x)$，$Q(x)$

が存在するが，$P(\alpha)f(\alpha)+Q(\alpha)g(\alpha)=1$ は矛盾。
だから，ちょうど 2^m 個の元がある。
$\beta=a_1+a_2\alpha+a_3\alpha^2+\cdots+a_m\alpha^{m-1}$ は逆元を持つ。なぜなら， $f(x)$ と $a_1+a_2x+a_3x^2+\cdots+a_mx^{m-1}$ は GF(2)上の多項式とみて互いに素だから，$P(x)f(x)+(a_1+a_2x+a_3x^2+\cdots+a_mx^{m-1})Q(x)=1$ となる GF(2)上の多項式 $P(x)$，$Q(x)$が存在し，$P(\alpha)f(\alpha)+(a_1+a_2\alpha+a_3\alpha^2+\cdots+a_m\alpha^{m-1})Q(\alpha)=1$ より　$\beta Q(\alpha)=1$。

$m=3$ のとき
$f(x)=1+x+x^3$ は，GF(2)上の既約多項式である。
［なぜなら，3 次式は 1 次式と 2 次式の積の形にしか因数分解できないから，因数分解されれば 1 次の因数をもつのに，$f(0)=f(1)=1$ だから，$f(x)$は 1 次の因数を持たない。］
GF(2)に $1+\alpha+\alpha^3=0$ となる元 α を追加する。
$\alpha^3=1+\alpha$
$\alpha^4=\alpha+\alpha^2$
$\alpha^5=\alpha^2+\alpha^3=1+\alpha+\alpha^2$
$\alpha^6=\alpha+\alpha^2+\alpha^3=1+\alpha^2$
$\alpha^7=\alpha+\alpha^3=1$
GF(2^3)の 0 以外のすべての元は α^n の形になり， $\alpha^7=1$ を利用して乗法に関する逆元の存在がいえる。

$m=4$ のとき
$f(x)=1+x+x^4$ は，GF(2)上の既約多項式である。
［$f(0)=f(1)=1$ だから，1 次の因数を持たない。2 次の既約多項式は $1+x+x^2$ のみだから割ってみる。］
GF(2)に $1+\alpha+\alpha^4=0$ となる元 α を追加する。
$\alpha^4=1+\alpha$
$\alpha^8=(1+\alpha)^2=1+\alpha^2$
$\alpha^{16}=(1+\alpha^2)^2=1+\alpha^4=\alpha$
だから， $\alpha^{15}=1$
その他，表 9.13 参照。

〔表 9.13〕
GF (2^4) の元

べき表現	多項式表現	ベクトル表現
0	0	0 0 0 0
1	1	1 0 0 0
α	α	0 1 0 0
α^2	α^2	0 0 1 0
α^3	α^3	0 0 0 1
α^4	$1+\alpha$	1 1 0 0
α^5	$\alpha+\alpha^2$	0 1 1 0
α^6	$\alpha^2+\alpha^3$	0 0 1 1
α^7	$1+\alpha+\alpha^3$	1 1 0 1
α^8	$1+\alpha^2$	1 0 1 0
α^9	$\alpha+\alpha^3$	0 1 0 1
α^{10}	$1+\alpha+\alpha^2$	1 1 1 0
α^{11}	$\alpha+\alpha^2+\alpha^3$	0 1 1 1
α^{12}	$1+\alpha+\alpha^2+\alpha^3$	1 1 1 1
α^{13}	$1+\alpha^2+\alpha^3$	1 0 1 1
α^{14}	$1+\alpha^3$	1 0 0 1
α^{15}	1	1 0 0 0

（α は x^4+x+1 の根）

GF(2)上で成立する等式
$(a+b)^2=a^2+b^2$
$(a+b)^4=a^4+b^4$
$(a+b)^8=a^8+b^8$
……
$(a+b)^{2^m}=a^{2^m}+b^{2^m}$
$(a+b+c)^{2^m}=a^{2^m}+b^{2^m}+c^{2^m}$
……

最小多項式

GF(2^m)の元βに対する最小多項式とは，βを根にもつ最小次数の GF(2)係数の多項式

最小多項式の求め方

$M(x)$がβの最小多項式であれば，

$M(\beta)=M(\beta^2)=M(\beta^4)=M(\beta^8)=M(\beta^{16})=\cdots\cdots$

となることを利用する。

例 GF(2^3)でα^3の最小多項式を求める。

GF(2^3)で$\alpha^7=1$に注意

α^3，α^6，$\alpha^{12}=\alpha^5$，$\alpha^{24}=\alpha^3$

$M(x)=(x-\alpha^3)(x-\alpha^6)(x-\alpha^5)=x^3-(\alpha^3+\alpha^6+\alpha^5)x^2+(\alpha^3\alpha^6+\alpha^6\alpha^5+\alpha^5\alpha^3)x+\alpha^3\alpha^6\alpha^5$

$=x^3-(\alpha^3+\alpha^6+\alpha^5)x^2+(\alpha^2+\alpha^4+\alpha)x+1=x^3+x^2+1$

最小多項式と誤り訂正符号

GF(2^m)を利用すると，$x^{2^m}-1$の因数分解が得られる。

因数分解ができると，その因数を$G(x)$とおくことにより巡回符号が作れる。

GF(2^3)を利用して

1 → $x+1$

α，α^2，α^4 → x^3+x+1

α^3，α^6，α^5 → x^3+x^2+1

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

GF(2^4)を利用して

1 → $x+1$

α，α^2，α^4，α^8 → x^4+x+1

α^3，α^6，α^{12}，α^9 → $x^4+x^3+x^2+x+1$

α^5，α^{10} → x^2+x+1

α^7，α^{14}，α^{13}，α^{11} → x^4+x^3+1

$x^{15}-1=(x+1)(x^4+x+1)(x^4+x^3+x^2+x+1)(x^2+x+1)(x^4+x^3+1)$

演習問題

Ⅰ　因数分解　$x^{15}-1=(x+1)(x^4+x+1)(x^4+x^3+x^2+x+1)(x^2+x+1)(x^4+x^3+1)$　を利用して 15 ビットの巡回符号を構成する。多項式は $x^{15}-1$ を法とする剰余系で考える（$x^{15}-1=0$ と考える）。

（１）　$G(x)=(x^4+x^3+x^2+x+1)(x^2+x+1)(x^4+x^3+1)$ とし（本稿 p.4 で $n=15$，$k=5$，$m=10$），

$(x+1)(x^4+x+1)=x^5+x^4+x^2+1$ だから，$(x^5+x^4+x^2+1)G(x)=x^{15}-1=0$ に注意すると，

$$x^5G(x)=(x^4+x^2+1)G(x)$$

したがって，$G(x)$を因数にもつ多項式は，

$$(a_0x^4+a_1x^3+a_2x^2+a_3x^1+a_4)\,G(x)\quad（a_i は 0 または 1）\qquad(*)$$

の形になり，全部で $2^5(=32)$個ある。

①　$x^5G(x)$，$x^6G(x)$，$x^7G(x)$，……を(＊)の形に表せ。$x^pG(x)=G(x)$となる最小の自然数 p を求めよ。

②　(＊)の形の多項式のうち，①の形の表せないものがあれば，そのうち次数が最小のもの $G_1(x)$とし，

$x\,G_1(x)$，$x^2\,G_1(x)$，$x^3\,G_1(x)$，……を(＊)の形に表せ。

③　(＊)の形の多項式のうち，①，②の形の表せないものがあれば，そのうち次数が最小のもの $G_2(x)$とし，

$x\,G_2(x)$，$x^2\,G_2(x)$，$x^3\,G_2(x)$，……を(＊)の形に表せ。

④　0 を除くすべての(＊)の形の多項式が①，②，③，…の形に表されるまで，②，③と同様の手続きを繰り返せ。

⑤　最小ハミング距離を求めよ。

（２）（１）と異なる因数をもつ 10 次式を $G(x)$とした場合，どうか。

（３）$G(x)=(x+1)(x^2+x+1)(x^4+x+1)(x^4+x^3+x^2+x+1)$ の場合，どうか。

（４）$G(x)=(x+1)(x^4+x+1)(x^4+x^3+x^2+x+1)$ の場合，どうか。