4 元体 $\mathbb{F}_4$ の演算対応表

$+$	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

$\times$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

同様にして 8 元体 $\mathbb{F}_8$ の対応表を作れ。

. . . . . .

有限体の標数は素数である。標数とは乗法単位元 1 をその個数だけ足すと 0 になる数のことである。4 元体も 8 元体も標数は 2 であるので、$1+1=0$ であり、同じ者同士の和が 0 になる。

2 元体 $\mathbb{F}_2$ は $\mathbb{F}_2=\{0,1\}$ であり、その演算は整数の加法乗法と同じであり、$2=0$ という規則を付け加えたものになる。

4 元体は 1 変数多項式の加法乗法と同じであり、標数 $2(2=0)$ と $x^2=x+1$ を付け加えたものになる。

$$\mathbb{F}_4=\{0,1,x,1+x\} \tag{1}$$

この $\mathbb{F}_4$ の演算が多項式の加法と乗法であり、2 が出てくると 0 に置き換え、x^2 が出てくると $x+1$ に置き換えることで体になる。対応表では $a=x,\ b=1+x$ としたものと同じである。

8 元体 $\mathbb{F}_8$ は 4 元体 $\mathbb{F}_4$ の規則 $x^2=x+1$ を $x^3=x+1$ に変えたものになる。

$$\mathbb{F}_8=\{0,1,x,x+1,x^2,x^2+1,x^2+x,x^2+x+1\} \tag{2}$$

これに多項式としての加法と乗法を当てはめ、2 が出てくると 0 に置き換え、x^3 が出てくると $x+1$ に置き換える。

例えば、x^2+1 と x^2+x+1 をかけると次のようになる。

$$\begin{aligned}(x^2+1)\times(x^2+x+1)&=x^4+x^3+2x^2+x+1 &(3)\\ &=x(x+1)+(x+1)+x+1 &(4)\\ &=x^2+x+x+1+x+1 &(5)\\ &=x^2+x &(6)\end{aligned}$$

$\mathbb{F}_8$ の元は $a = x,\ b = x+1,\ c = x^2,\ d = x^2+1,\ e = x^2+x,\ f = x^2+x+1$ と表記すると次のようになる。

$+$	0	1	a	b	c	d	e	f
0	0	1	a	b	c	d	e	f
1	1	0	b	a	d	c	f	e
a	a	b	0	1	e	f	c	d
b	b	a	1	0	f	e	d	c
c	c	d	e	f	0	1	a	b
d	d	c	f	e	1	0	b	a
e	e	f	c	d	a	b	0	1
f	f	e	d	c	b	a	1	0

$\times$	0	1	a	b	c	d	e	f
0	0	0	0	0	0	0	0	0
1	0	1	a	b	c	d	e	f
a	0	a	c	e	b	1	f	d
b	0	b	e	d	f	c	1	a
c	0	c	b	f	e	a	d	1
d	0	d	1	c	a	f	b	e
e	0	e	f	1	d	b	a	c
f	0	f	d	a	1	e	c	b

有限体は多項式環を既約多項式で割ったものと同型になる。

$$4\text{ 元体}：\mathbb{F}_2[X]/(x^2+x+1) \qquad 8\text{ 元体}：\mathbb{F}_2[X]/(x^3+x+1) \tag{7}$$

G, H を群とする。G の演算を $\bullet_G$ とし、H の演算を $\bullet_H$ とする。直積集合 $G \times H$ に演算 $\bullet_{G\times H}$ を次のように成分ごとの演算で定義する。

$$(g_1, h_1) \bullet_{G\times H} (g_2, h_2) = (g_1 \bullet_G g_2, h_1 \bullet_H h_2) \tag{8}$$

$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ と $\mathbb{Z}/9\mathbb{Z}$ は同型か否かを判定せよ。

.....

剰余類群は次のような集合である。

$$\mathbb{Z}/3\mathbb{Z} = \{0, 1, 2\}, \quad \mathbb{Z}/9\mathbb{Z} = \{0, 1, 2, 3, 4, 5, 6, 7, 8\} \tag{9}$$

位数 3 の群は次のような演算が定義される。

	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

つまり、$e = 0, a = 1, b = 2$ である加法群と同型なものしか存在しない為、$\mathbb{Z}/3\mathbb{Z}$ と同型である。

$\mathbb{Z}/9\mathbb{Z}$ を剰余類群とすると、整数を 9 で割った余りの集合となる。この為、演算は整数の加法で行い、9 が現れると 0 に置き換えることで群となる。

$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ の元は (n_1, n_2) となるが、$(0, 0)$ 以外の元は 3 回足すと $(0, 0)$ になる。

$$(0, 2) + (0, 2) + (0, 2) = (0, 6) = (0, 0) \tag{10}$$
$$(1, 1) + (1, 1) + (1, 1) = (3, 3) = (0, 0) \tag{11}$$

つまり、$(0, 0)$ は位数 1 であり、それ以外の元は位数 3 である。しかし、$\mathbb{Z}/9\mathbb{Z}$ の元 1 は位数 9 である。

よって、位数の異なるものに準同型写像が対応を取れないため同型写像が存在しない。これにより $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ と $\mathbb{Z}/9\mathbb{Z}$ は同型ではない。

送信者は 2 ビットのビット列 S を送ろうとしている。通信経路にて高々 2 ビットのノイズが入ることが想定される。

このビット列 S に 6 ビットの訂正列を加えた 8 ビットを送ることで誤り訂正が可能である。この手順を構成し説明せよ。

.....

高々 2 ビットのエラーが含まれる事を考え、送信者が送るビット列のそれぞれのハミング距離は 4 以上ないといけない。

例えば、送るデータ列を次のようにする。

$$a = (0,0,\ 0,0,0,0,0,0) \tag{12}$$
$$b = (0,1,\ 0,0,0,1,1,1) \tag{13}$$
$$c = (1,0,\ 1,1,1,0,0,0) \tag{14}$$
$$d = (1,1,\ 1,1,1,1,1,1) \tag{15}$$

これらのハミング距離 d_H は次のようになる。

$$d_H(a,b) = 4 \qquad d_H(a,c) = 4 \qquad d_H(a,d) = 8 \tag{16}$$
$$d_H(b,c) = 8 \qquad d_H(b,d) = 4 \qquad d_H(c,d) = 4 \tag{17}$$

ハミング距離は 2 つの文字列の異なる箇所の個数で定義する。

エラーが高々 2 ビットしか含まれないのであれば受信したデータとハミング距離が最も小さいものが送られたと考えられる。

これにより送信するデータ列 a, b, c, d からみてハミング距離が 2 以内の受信データはそのデータが送られたものとして扱うことで誤り訂正が可能である。

以下のような誤り訂正・検出の手順を考える。

1. 送信者は 100 ビットの情報列を 10×10 の正方形に並べる
2. 正方形の各列各行についてそこに含まれる 10 個の数の和を求める。(2 元体上)
3. すべての数の総和を求める。(2 元体上)
4. 2 及び 3 で得られた 21 個の数を並べ、訂正列として付加して送信する。

この方式 (垂直水平パリティ符号) を誤り訂正符号として用いた場合、誤りが何ビットまでなら確実に訂正できるか。また、誤り検出符号として用いた場合、誤りが何ビットまでなら確実に検出できるか。

.....

- 1 ビットの誤りがあるとそのビットを含む行と列の和が合わなくなる。この行と列からエラーの含まれるビットが特定できるため、1 ビットの誤りは訂正が可能である。
- 2 ビットの誤りがあると行の和が合わない場所が 2 行、列の和が合わない場所が 2 列発生する場合がある。この場合はエラーを含むビットを絞ることは出来るが、特定は出来ない。
- 3 ビットの誤りがあると他の情報列と 1 ビットの誤りと区別がつかない。
- 4 ビットの誤りがあると他の情報列と一致する場合がある。

以上により、1 ビットの誤りは訂正が可能である。検出だけであれば 3 ビットの誤りまで検出可能である。