QR コード—誤り訂正

渋谷　憲政

(久留米工業大学)

目 次

1　BCH 符号の作り方

1.1　誤り訂正の基本的な考え方

誤り訂正の基本的な考え方を述べます.

Example 1.
0 と 1 の数字を 2 個並べた列を考えます．これを 2 bit と言います．全部で 4 通りあります.

$$F = \{00, 01, 10, 11\}$$

とおきます．相手にこの 4 つの中から 1 個だけ選んでもらって，そのデータを 1 bit だけ変更してもらいます．例えば，10 を選んで，11 に変更したとします．でもその変更を目撃していない限り，データを変更したかどうかはわかりません.
次のような場合はどうでしょう.

$$C = \{00, 11\}$$

とおきます．C は F の部分集合です．今度はこの 2 つの中から 1 個選んでもらって 1 bit だけ変更してもらいます．例えば，11 を選んで．01 に変更したとします．すると集合 $C = \{00, 11\}$ の中に 01 が入ってないからデータが変更されたことがわかります．でもどの場所を変更したかはわかりません．01 は 00 を変更したものかも知れないからです．　□

Example 2.
4 bit の列を考えます．全部で 16 通りあります.

$$F = \{0000, 0001, 0010, \ldots, 1111\}$$

$$C = \{0011, 0101, 1001, 0110, 1010, 1100\}$$

とおきます．C の中から 1 個選んでもらって 1 bit だけ変更してもらいます．例えば，0011 を選んで．0010 に変更したとします．すると 1 の数が減っているのでデータが変更されたことがわかります．C には 1 の数が 2 個のものしか入っていないからです．誤りがあったかどうかだけの判定なら，この方法で何 bit でもできます．でも誤りの場所まではわかりません．　□

Example 3.
3 bit の列を考えます．全部で 8 通りあります.

$$F = \{000, 001, 010, 011, 100, 101, 110, 111\}$$

$$C = \{000, 111\}$$

とおきます．C の中から 1 個選んでもらって 1 bit だけ変更してもらいます．例えば，000 を選んで．001 に変更したとします．すると 3 番目が変更されたことがわかります．これはあまりにも簡単ですが，この場合は間違いの場所までわかります.

C の元は特殊で散らばっていることがわかります．C の元を 1 bit だけ変更しても C の元にはなりません．3ヶ所変更すれば，C の元になります．このように2つの元が何ヶ所違っているかをその2つの元の距離と言います．000 と 111 の距離は 3 です．距離を計算するには bit 同士をたし算すればよいことがわかります．1+1=0 (mod 2) などのたし算です．今，変更されたデータが 001 ですから，C のすべての元との距離を計算します．

001 と 000 の距離は 1 です．

001 と 111 の距離は 2 です．

C の中で 001 に1番近いものは1個しかありません．ですから，001 は 000 を変更したものだということがわかります．

なお，Example 2 では 01 と 00 の距離は 1 で，01 と 11 との距離も 1 です．ですから，どちらが変更前のものか判定できません．　□

誤り訂正の基本的な考え方は以上に尽きます．全体集合 F とその部分集合 C を考えます．C をいかにうまくつくるかが符号理論 (coding theory) の中心テーマです．

この部分集合 C のことを誤り訂正符号と言います．この言葉は C の要素を呼ぶときにも用いられますが，部分集合であることを強調した方がいいと思います．

部分集合 C で特に有名なものが BCH 符号とリード・ソロモン符号です．BCH は Bose-Chaudhuri-Hocquenghem の略です．

Example 4. (BCH 符号)
15 bit の列を考えます．全部で $2^{15} = 32,768$ 通りあります．

$$F = \{000000000000000, 000000000000001, \ldots, 111111111111111\}$$

とおきます．次のような F の部分集合 C を考えます．

$$\begin{aligned} C = \{&000000000000000,\ 000010100110111,\ 000101001101110,\ 000111101011001,\\ &001000111101011,\ 001010011011100,\ 001101110000101,\ 001111010110010,\\ &010001111010110,\ 010011011100001,\ 010100110111000,\ 010110010001111,\\ &011001000111101,\ 011011100001010,\ 011100001010011,\ 011110101100100,\\ &100001010011011,\ 100011110101100,\ 100100011110101,\ 100110111000010,\\ &101001101110000,\ 101011001000111,\ 101100100011110,\ 101110000101001,\\ &110000101001101,\ 110010001111010,\ 110101100100011,\ 110111000010100,\\ &111000010100110,\ 111010110010001,\ 111101011001000,\ 111111111111111\} \end{aligned}$$

C の要素の個数は 32 個あります．この C を BCH 符号と言います．C から1個選んでもらって 3 ヶ所変更してもらいます．例えば，

001010011011100

を選んで

$$001110010001100$$

に変更したとします．すると変更した場所

$$001 * 1001 * 0 * 1100$$

を当てることができます．原理は簡単です．C の 2 つの元の距離を全部計算してみてください．距離は 7 か 8 になります．000000000000000 と 111111111111111 の距離だけ 15 になりますが，これは特殊で省いてもいいくらいです．C は散らばって作られていることがわかります．

今，$x = 001110010001100$ が与えられたデータですから，これと C のすべての元との距離を計算します．$x = 001110010001100$ と $a = 001010011011100$ の距離だけが 3 になって他はこれより長くなります．最短距離は 1 個しかありません．なぜなら，距離 3 のものが他にあったとします．今それを b とします．すると a から x を経由して b に行けば 6 bit の変更で行けます．これは矛盾です．C がうまく散らばって作られている，というのがミソです．

このことから，4 ヶ所の変更は判定できないことがわかります．3 ヶ所以下なら OK です．15 bit のうち 3 bit ですから，20 %の復元能力があると言えます．

なお，C の元の個数が多くなると距離の計算は大変ですから，シンドロームなどの計算で誤り判定をします． □

1.2 多項式の計算

まず次の多項式を展開してみます．

$$(ax + b)(cx + d) = acx^2 + (ad + bc)x + bd$$

多項式の係数を見ると係数同士の積や和があります．割り算はどうでしょう．

$$(x^2 + 2x - 15) \div (5x - 15) = 5^{-1}x + 1$$

となって係数の割り算 (乗法の逆元 5^{-1}) が必要になります．従って，多項式の加減乗除をするとき，係数の加減乗除が必要になります．加減乗除が自由にできる集合を体といいます．多項式の係数は体を考えます．

Example 5. GF(2)

$$\mathrm{GF}(2) = \{0, 1\}$$

とおきます．GF は Galoa Field の略です．一般に GF(q) は要素の個数が q 個の有限体を表します．GF(2) の場合，0 と 1 しかありませんから，和と積は

$$0 + 0 = 0,\ 0 + 1 = 1,\ 1 + 0 = 1,\ 1 + 1 = 0,\ 0 \cdot 0 = 0,\ 0 \cdot 1 = 0,\ 1 \cdot 0 = 0,\ 1 \cdot 1 = 1$$

となります．GF(2) はこの和と積について体になります．$-1 = 1, 1^{-1} = 1$ ですから引き算，割り算もできるという意味です．

GF(q) は $q = p^m$ の形でないと体にはならないことが知られています．p は素数，m は自然数です．この形は後で出てきます．GF(2^4) と GF(2^8) です．要素の個数が 16 個の有限体 GF(16) と 256 個の有限体 GF(256) です．　□

Example 6. (多項式の積)
4bit の 0, 1 の列を考えます．

$$F = \{0000, 0001, 0010, 0011, 0100, 0101, \cdots, 1111\}$$

とおきます．要素の個数は 16 個あります．F の元に対して四則演算を定義するのが目的です．この Example 6 では多項式の積の練習だけをします．

和は簡単です．成分同士の和をとればいい．$-1 = 1$ だから引き算もできます．積はどうでしよう．積はいろいろな場面で難しいことが多いものです．F の元を次のような多項式で表します．

$r_3r_2r_1r_0 \in F$ に対して ($r_i \in \{0, 1\}$),

$$r_3x^3 + r_2x^2 + r_1x + r_0$$

を対応させます．x が何であるかを考える必要はなく，単なる記号と考えます．多項式の係数は 0,1 しか取りませんから，このような多項式を体 GF(2) 上の多項式と言います．和は多項式の和，積は多項式の積で定義します．和は成分同士の和になります．多項式の積の練習をしてみます．

$$(x + 1)^2 = x^2 + x + x + 1 = x^2 + 1$$

となります．なぜなら，$x + x = (1 + 1)x = 0$ だからです．一般に GF(2) 上の多項式 a, b に対して

$$(a + b)^2 = a^2 + b^2$$

が成立します,

$$(a + b + c)^2 = a^2 + b^2 + c^2$$

も同様です．また,

$$(a + b)^4 = (a^2 + b^2)^2 = a^4 + b^4$$

です.

$$(a + b + c)^4 = a^4 + b^4 + c^4$$

も同様です．偶数乗はいつもこうなります．奇数乗は

$$(a + b)^3 = (a^2 + b^2)(a + b) = a^3 + a^2b + ab^2 + b^3$$

となって，$a^3 + b^3$ にはなりません．以下のような４次の多項式の因数分解が成立します．右辺を展開して左辺になることを確かめてください．４次の多項式は全部で 16 個あります．

$$x^4 = x^4, \quad x^4 + 1 = (x + 1)^4, \quad x^4 + x = x(x + 1)(x^2 + x + 1),$$

$$x^4+x+1 : \text{因数分解できない},$$

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

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

$$x^4+x^3+1 : \text{因数分解できない},$$

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

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

$$x^4+x^3+x^2+x+1 : \text{因数分解できない} \quad \square$$

多項式を体にするところまでは説明してませんが，一応ここまでで BCH 符号は作れます．

1.3 BCH 符号の作り方

5 bit の 0, 1 の列があったとします．この後に 10 bit の列を付け加えて 15 bit の符号をつくります．全体集合は

$$F=\{000000000000000, 000000000000001, \ldots, 111111111111111\}$$

で，要素の個数は $2^{15}=32,768$ 個あります．F は

$$F=\{r_{14}r_{13}r_{12}r_{11}r_{10}r_9r_8r_7r_6r_5r_4r_3r_2r_1r_0;\ r_j \text{ は } 0 \text{ または } 1\ \}$$

と書けます．任意の元 $\boldsymbol{y}\in F$ は

$$\boldsymbol{y}=Y(x)=r_{14}x^{14}+r_{13}x^{13}+r_{12}x^{12}+r_{11}x^{11}+r_{10}x^{10}+r_9x^9+r_8x^8$$

$$+r_7x^7+r_6x^6+r_5x^5+r_4x^4+r_3x^3+r_2x^2+r_1x+r_0$$

のように x の 14 次以下の多項式と同一視することができます．先頭の 5 bit

$$r_{14}r_{13}r_{12}r_{11}r_{10}$$

を情報ビットといい，残りの 10 bit

$$r_9r_8r_7r_6r_5r_4r_3r_2r_1r_0$$

を誤り訂正ビットと言います．情報ビットが１つ与えられたとき，誤り訂正ビットを一意に定め，それを付け加えて 15 bit の列をつくります．この集合が C です．C の元の個数は情報ビットの個数ですから，$2^5=32$ 個しかありません．３万個もある bit 列の中で 32 個の bit 列しか使わないのです．誤り訂正はもったいない？

例題で C の作り方を説明します．

Example 7.

情報ビット：00101

とします．00101 は先頭の 5 bit ですから

$$I(x) = 0 \cdot x^{14} + 0 \cdot x^{13} + 1 \cdot x^{12} + 0 \cdot x^{11} + 1 \cdot x^{10} = x^{12} + x^{10}$$

と同一視できます．

生成多項式と呼ばれる次の多項式 $g(x)$ を考えます．

$$g(x) = x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1$$

$I(x)$ を $g(x)$ で割り，余り $R(x)$ を求めます．割り算を知らなくても右辺を展開して左辺になることは確認できます．

$$x^{12} + x^{10} = x^2(x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1) + x^7 + x^6 + x^4 + x^3 + x^2$$

となります．$x^7 + x^7 = 0$ などを使います．

$$I(x) = h(x)g(x) + R(x)$$

です．この余り $R(x)$ が誤り訂正ビットです．$x^7 + x^7 = 0$ より $-x^7 = x^7$ などですから余りを左辺に移すと

$$x^{12} + x^{10} + x^7 + x^6 + x^4 + x^3 + x^2 = x^2(x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1)$$

となります．つまり，$I(x)+R(x) = h(x)g(x)$ です．$I(x)$ に $R(x)$ をつなげた多項式$Y(x) = I(x) + R(x)$ が誤り訂正付き符号です．次のような 15 bit の列が得られます．

$$001010011011100$$

誤り訂正付符号はすべて，$g(x)$ の多項式倍になっています．つまり，符号は $g(x)$ から作られるので，$g(x)$ は生成多項式と呼ばれています．他の場合も同様に求められます．C のすべての元は Example 4 に書いてあります．この C を BCH 符号と言います．　□

注．生成多項式 $g(x)$ は次のように因数分解できます．

$$g(x) = (x^2 + x + 1)(x^4 + x^3 + x^2 + x + 1)(x^4 + x + 1)$$

2　リード・ソロモン符号の作り方

リード・ソロモン符号の作り方には少し長い説明が必要になります.

2.1　4 bit を体にする

Example 8. (4 bit を体にする)
Example 6 と同じ F を考えます．4bit の列です.

$$F = \{0000, 0001, 0010, 0011, 0100, 0101, \cdots, 1111\}$$

です．$F = \mathrm{GF}(2^4) = \mathrm{GF}(16)$ のように F を体にすることが目的です.
F の元を多項式と同一視して，F での積を多項式の積で定義します．ところが

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

となって，3 次の多項式ではないので，F の元にはなりません．こんなときは $x^4 = 1$ などの条件をつけて，3 次以下に落としてやります．$x^4 = 1$ を代入して

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

となります．この曖昧な式は後でもっと正確にしますが，感覚的にはわかると思います．bit で書くと

$$(1000) \cdot (0101) = (1010)$$

となり，かけ算ができます．また，$x^4 = 1$ を代入せずに，$x^4 - 1$ で割って余りを求める方法もあります.

$$x^5 + x^3 = x(x^4 - 1) + x^3 + x$$

従って，余り $x^3 + x$ です．こちらの方が正統派です．余りだけが欲しいので

$$x^5 + x^3 = x + x^3 \qquad (\mathrm{mod}\ x^4 - 1)$$

と書きます.

$$a(x) = b(x) \qquad (\mathrm{mod}\ x^4 - 1)$$

とは

$$a(x) - b(x) = h(x)(x^4 - 1)$$

のように差が $x^4 - 1$ の多項式倍になっていることを意味します.
では割り算はどうでしょう．$(x+1)^{-1}$ を求めてみます.

$$(x+1)f(x) = 1 \qquad (\mathrm{mod}\ x^4 - 1)$$

となる $f(x)$ を探します．つまり，

$$(x+1)f(x) - h(x)(x^4 - 1) = 1$$

となる多項式 $f(x), h(x)$ を探します．$x^4 - 1 = (x-1)(x^3 + x^2 + x + 1)$ と因数分解できますが，$-1 = 1$ ですから $x^4 - 1 = x^4 + 1 = (x+1)(x^3 + x^2 + x + 1)$ となります．従って，左辺は

$$(x+1)\{f(x) - h(x)(x^3 + x^2 + x + 1)\} = 1$$

と因数分解できます．$x+1$ の多項式倍は決して 1 にならないので，このような $f(x), h(x)$ は存在しません．$(x+1)^{-1}$ が存在しないので割り算ができません．従って，F は体にはなりません．この原因は

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

と因数分解できたことにあります．因数分解できる多項式だと，いつでもこのようなことが起こり，F を体にすることはできません．それで因数分解できない多項式 (既約多項式) を考えます．GF(2) 上の４次の多項式で因数分解できないものは次の３つしかありませんでした (Cf. Example 6).

$$x^4 + x^3 + x^2 + x + 1, \quad x^4 + x^3 + 1, \quad x^4 + x + 1$$

の３つです．このどれを使っても多項式を体にすることができます．ここでは

$$g(x) = x^4 + x + 1$$

を選んでおきます．0,1 を係数にもつ多項式 $a(x), b(x)$ に対して，

$$a(x) = b(x) \qquad (\mathrm{mod}\ x^4 + x + 1)$$

と定義します．積は

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

のようになります．つまり，

$$x^3(x^2 + 1) = x^3 + x^2 + x \qquad (\mathrm{mod}\ x^4 + x + 1)$$

です．bit で書くと

$$(1000) \cdot (0101) = (1110)$$

となります．先程とは別の積を考えていることになります．この積なら $(x+1)^{-1}$ も存在します．

$$(x+1)f(x) = 1 \qquad (\mathrm{mod}\ x^4 + x + 1)$$

となる $f(x)$ を探すと $f(x) = x^3 + x^2 + x$ となります．これはユークリッドの互除法で求めることができます．

$$(x+1)(x^3 + x^2 + x) = 1 \qquad (\mathrm{mod}\ x^4 + x + 1)$$

を確認するのも簡単です．bit で書くと

$$(0011)^{-1} = (1110)$$

となります．つまり，4 bit の世界で割り算もできます．

$$g(x) = x^4 + x + 1$$

が因数分解できないことから，３次以下のどんな多項式とも互いに素になって，乗法の逆元が存在します．従って，4 bit の列の集合 F は体になります．要素の個数が 16 の有限体ですから，

$$F = \mathrm{GF}(2^4) = \mathrm{GF}(16)$$

と書きます．一般に $\mathrm{GF}(p^m)$ を体にする方法も同様です．　□

4bit の世界 GF(16) で積が定義できましたが，積を実際に計算するのは bit 数が増えてくると大変です．積を簡単に計算する方法を考えます．いきなりですが，

$$x^4 + x + 1 = 0$$

の１つの根 α を考えます．

$$\alpha^4 + \alpha + 1 = 0$$

です．そんな α が存在するのか，と思われるかも知れませんが，複素数の虚数単位 i を考えれば納得できます．虚数単位 i は $x^2 + 1 = 0$ の根の１つで，

$$i^2 + 1 = 0$$

を満たします．この条件だけで，すべての計算をします．i だけ付け加えれば複素数の世界ができます．矛盾なく計算が行えて，それが役に立つものなら使ってみる価値はあります．従って，新しい数 α を考えます．GF(16) のすべての元をこの α を用いて表示します．虚数単位 i を用いた複素数表示のようなものです．GF(16) は α を用いて次のように書けます．

$$\mathrm{GF}(2^4) = \mathrm{GF}(16) = \{r_3\alpha^3 + r_2\alpha^2 + r_1\alpha + r_0;\ r_j \text{ は } 0 \text{ または } 1\ \}$$

何のことはない，x の多項式で書いたのと少しも変わりません．

$$\alpha^4 + \alpha + 1 = 0$$

を明確にしたにすぎません．でもこの式があれば，$\alpha^4 = \alpha + 1$ を代入できます．以前，$x^4 = 1$ を代入してと書きましたが，この α を使えば明確になります．計算練習をしてみます．GF(16) は体ですから，２つの元の積もまた GF(16) の元です．$\alpha \in \mathrm{GF}(16)$ ですから，その２乗，３乗,... もすべて GF(16) の元です．計算してみます．$\alpha^4 = \alpha + 1$ です．bit で言えば 0011 です．

$$\alpha^5 = \alpha \cdot \alpha^4 = \alpha(\alpha + 1) = \alpha^2 + \alpha$$

bit で言えば 0110 です．$\alpha^4 = \alpha + 1$ を代入しましたが，α^5 を $\alpha^4 + \alpha + 1$ で割って余りを求めてもできます．全部計算したものは表１にあります．α^{15} だけ計算してみます．

$$\alpha^{16} = (\alpha^4)^4 = (\alpha + 1)^4 = \alpha^4 + 1 = \alpha$$

となります．偶数乗の公式を使いました．両辺を α で割れば

$$\alpha^{15} = 1$$

を得ます．α^{15} を $\alpha^4 + \alpha + 1$ で割って余りを求めた方が素直かも知れません．Excel で求めるなら α^j すべてが欲しいわけですから，$\alpha^4, \alpha^5, \cdots$ のように前のものを使って次々に求める方が楽です．表を見ると $1, \alpha, \alpha^2, \cdots \alpha^{14}$ で 4 bit のすべてが出てきているのがわかります．おっと，0 を忘れていました．0 は指数では書けないので，これだけ別に付け加えます．$\alpha^{15} = 1$ ですから，α^{16} 以上はまた同じことが繰り返されます．例えば，$\alpha^{20} = \alpha^5$ になります．また，割り算もできます．$\alpha^{-3} = \alpha^{12}$ などです．

表1. 指数を 4 bit に直す

j	α^j	α の 3 次以下の多項式	4 bit
	0	0	0000
0	α^0	1	0001
1	α^1	α	0010
2	α^2	α^2	0100
3	α^3	α^3	1000
4	α^4	$\alpha + 1$	0011
5	α^5	$\alpha^2 + \alpha$	0110
6	α^6	$\alpha^3 + \alpha^2$	1100
7	α^7	$\alpha^3 + \alpha + 1$	1011
8	α^8	$\alpha^2 + 1$	0101
9	α^9	$\alpha^3 + \alpha$	1010
10	α^{10}	$\alpha^2 + \alpha + 1$	0111
11	α^{11}	$\alpha^3 + \alpha^2 + \alpha$	1110
12	α^{12}	$\alpha^3 + \alpha^2 + \alpha + 1$	1111
13	α^{13}	$\alpha^3 + \alpha^2$+!	1101
14	α^{14}	$\alpha^3 + 1$	1001

ここで，$1, \alpha, \alpha^2, \cdots \alpha^{14}$ で 4 bit のすべてが出てくるということを説明します．$\alpha^{15} = 1$ ですから α は

$$x^{15} - 1 = 0$$

の根です．$x^{15} - 1$ を因数分解してみます．

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

です．因数分解は難しいですが，右辺を展開して左辺になることは確認できます．この因数の中に $x^4 + x + 1$ が入っています．従って，$\alpha^{15} = 1$ になります．この因数に 4 次の既約多項式 3 つがすべて入っています．

$$x^4 + x^3 + x^2 + x + 1 = 0$$

の１つの根を α として同じ議論ができますが，まずいことがあります．

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

ですから，$\alpha^5 = 1$ となります．$1, \alpha, \alpha^2, \alpha^3, \alpha^4$ の繰り返しになりますから，16 個の 4bit は指数で表示できません．$x^4 + x^3 + 1$ を選ぶことはできます．これを選んでも同様の議論ができます．結局，4 bit の集合は

$$\mathrm{GF}(2^4) = \{0, 1, \alpha, \alpha^2, \alpha^3, \cdots, \alpha^{14}\}$$

と書けます．ただし，α は $x^4 + x + 1 = 0$ の根です．一般に $\mathrm{GF}(p^m)$ の場合，$x^4 + x + 1$ のような既約多項式が存在して，$\mathrm{GF}(p^m)$ の任意の元は α^j で表されることが知られています．0 は別に加えます．

注．4 bit を指数に対応させる表は 4 bit と 0〜14 を対応させていることになります (ゼロ元は除く)．２進数も 4 bit と 0〜15 を対応させるものの１つと考えることができます．

Example 9. (4 bit の四則演算)
$a = (1011)$ と $b = (1101)$ の積 $a \cdot b$ を求めてみます．
表より $a = (1011) = \alpha^7,\ b = (1101) = \alpha^{13}$ です．

$$a \cdot b = \alpha^7 \cdot \alpha^{13} = \alpha^{20} = \alpha^5 = \alpha^2 + \alpha = (0110)$$

となります．従って，

$$(1011) \cdot (1101) = (0110)$$

です．

次に $\alpha^8 + \alpha^{11}$ を求めてみます．

指数は乗除に強く加減に弱い

です．いきなりは足せません．指数を bit に直します．$\alpha^8 = \alpha^2 + 1 = (0101)$，$\alpha^{11} = \alpha^3 + \alpha^2 + \alpha = (1110)$ です．従って，

$$\alpha^8 + \alpha^{11} = (0101) + (1110) = (1011)$$

これをまた表を見て指数に直します．$(1011) = \alpha^7$ です．最終的に

$$\alpha^8 + \alpha^{11} = \alpha^7$$

となります．なかなか面倒ですね．でもこれをリード・ソロモンで使います．割り算は $\alpha^{-6} = \alpha^9$ などですから同様にできます．　□

2.2 GF(256)

GF(16) の説明を長くしたので，GF(256) は簡単に説明します．QR コードは 8 bit 単位でしたから，$\mathrm{GF}(2^8) = \mathrm{GF}(256)$ が必要になります．８次の多項式

$$g(x) = x^8 + x^4 + x^3 + x^2 + 1$$

を考えます．$g(x)$ は因数分解ができず (既約多項式)，GF(256) のすべての元を指数で表すことができる多項式です．

0,1 を係数にもつ多項式 $a(x), b(x)$ に対して，

$$a(x) = b(x) \qquad (\mathrm{mod}\ x^8 + x^4 + x^3 + x^2 + 1)$$

によって多項式が等しいことを定義します．すると積が定義されて GF(256) は体になります．

α を $x^8 + x^4 + x^3 + x^2 + 1 = 0$ の根の 1 つとします．すなわち，

$$\alpha^8 + \alpha^4 + \alpha^3 + \alpha^2 + 1 = 0$$

とします．8bit の列

$$(r_7 r_6 r_5 r_4 r_3 r_2 r_1 r_0) \in \mathrm{GF}(2^8)$$

に対して，

$$r_7\alpha^7 + r_6\alpha^6 + r_5\alpha^5 + r_4\alpha^4 + r_3\alpha^3 + r_2\alpha^2 + r_1\alpha + r_0$$

を対応させます．ただし，$r_i \in \{0, 1\}$ です．

$\mathrm{GF}(2^4) = \mathrm{GF}(16)$ と同様に $\alpha^8, \alpha^9, \alpha^{10}, \cdots, \alpha^{254}$ が計算できます．少しやってみます．

$$\alpha^8 = \alpha^4 + \alpha^3 + \alpha^2 + 1$$

です．

$$\alpha^9 = \alpha \cdot \alpha^8 = \alpha(\alpha^4 + \alpha^3 + \alpha^2 + 1)$$
$$= \alpha^5 + \alpha^4 + \alpha^3 + \alpha$$

となります．以下，次々に求めていきます．Excel で求めることができます．256 個すべてを書くのは大変ですから，そのいくつかを表にしておきます．$\alpha^{255} = 1$ に注意します．

表2. 指数を 8 bit に直す

j	α^j	α の 7 次以下の多項式	8 bit
	0	0	00000000
0	α^0	1	00000001
1	α^1	α	00000010
2	α^2	α^2	00000100
3	α^3	α^3	00001000
4	α^4	α^4	00010000
5	α^5	α^5	00100000
6	α^6	α^6	01000000
7	α^7	α^7	10000000
8	α^8	$\alpha^4+\alpha^3+\alpha^2+1$	00011101
9	α^9	$\alpha^5+\alpha^4+\alpha^3+\alpha$	00111010
10	α^{10}	$\alpha^6+\alpha^5+\alpha^4+\alpha^2$	01110100
11	α^{11}	$\alpha^7+\alpha^6+\alpha^5+\alpha^3$	11101000
12	α^{12}	$\alpha^7+\alpha^6+\alpha^3+\alpha^2+1$	11001101
13	α^{13}	$\alpha^7+\alpha^2+\alpha+1$	10000111
...	...	長いので途中省略	...
254	α^{254}	$\alpha^7+\alpha^3+\alpha^2+\alpha$	10001110

注. これも 8 bit と 0〜254 の対応表ということになります (ゼロ元は除く).

この表を使って，$\mathrm{GF}(2^8)=\mathrm{GF}(256)$ における四則演算ができます.

2.3 リード・ソロモン符号の作り方

1-L 型の QR コードのリード・ソロモン符号の作り方を述べます．1-L 型ではデータコード語数 19，誤り訂正コード語数 7 でした．8 bit 列を 19 個与えて，8 bit 列を 7 個作り出します．8 bit を表現するのに $\mathrm{GF}(2^8) = \mathrm{GF}(256)$ を使います．次の例で説明します．

Example 10. (リード・ソロモン符号の作り方)
I Love You の QR コードを作るときの例で説明します．I Love You を 0,1 に直し，埋め草コード語 1,2 などを入れて 8 bit のコード語を 19 個つくりました．最初のいくつかを書いてみます．

$$01000000, \quad 10100100, \quad 10010010$$

などです．01000000 は GF(256) の元ですから，α^j の形に書けます．表 2 です．表 2 はほとんど省略していますから，確認することはできません．

$$(01000000) = \alpha^6, \quad (10100100) = \alpha^{149}, \quad (10010010) = \alpha^{153}$$

となります．19 コード語は表 3 のようになります．

表3. 8 bit を指数に直す

	8 bit	α^j
1	01000000	α^6
2	01000000	α^{149}
3	10010010	α^{153}
4	00000100	α^2
5	11000110	α^{164}
6	11110111	α^{232}
7	01100110	α^{126}
8	01010010	α^{148}
9	00000101	α^{50}
10	10010110	α^{180}
11	11110111	α^{232}
12	01010000	α^{54}
13	11101100	α^{122}
14	00010001	α^{100}
15	11101100	α^{122}
16	00010001	α^{100}
17	11101100	α^{122}
18	00010001	α^{100}
19	11101100	α^{122}

この 19 コード語は次の 25 次の多項式と同一視できます．

$$I(x) = \alpha^6 \cdot x^{25} + \alpha^{149} \cdot x^{24} + \alpha^{153} \cdot x^{23} + \cdots + \alpha^{122} \cdot x^7$$

係数は GF(256) の元から成る多項式です.

生成多項式と呼ばれる次の 7 次の多項式 $g(x)$ を考えます.

$$g(x) = x^7 + \alpha^{87} \cdot x^6 + \alpha^{229} \cdot x^5 + \alpha^{146} \cdot x^4 + \alpha^{149} \cdot x^3 + \alpha^{238} \cdot x^2 + \alpha^{102} \cdot x + \alpha^{21}$$

これは 1-L 型の場合です．1-M 型，2-L 型などそれぞれの型に対して，生成多項式は定められています.

$I(x)$ を $g(x)$ で割り，余り $R(x)$ を求めます．この割り算に GF(256) での四則演算を使います．例えば，$\alpha^{87} + \alpha^{235}$ を計算するには表 2 をみて，指数を 8 bit に直し，それを足して，また表 2 をみて α^j の形に戻します．このようにして余り $R(x)$ を求めることができます.

$$R(x) = \alpha^{135} \cdot x^6 + \alpha^{31} \cdot x^5 + \alpha^{200} \cdot x^4 + \alpha^{215} \cdot x^3 + \alpha^{100} \cdot x^2 + \alpha^{236} \cdot x + \alpha^{224}$$

となります．得られた $\alpha^{135}, \alpha^{31}, \alpha^{200}, \alpha^{215}, \alpha^{100}, \alpha^{236}, \alpha^{224}$ をまた表を使って 8 bit に直せば，誤り訂正コード語 7 個が得られます．表 4 を見て下さい.

表4. 誤り訂正コード語 7 個

	x^i の i	α^j	8 bit
1	6	α^{135}	10101001
2	5	α^{31}	11000000
3	4	α^{200}	00011100
4	3	α^{215}	11110111
5	2	α^{100}	00010001
6	1	α^{236}	11001011
7	0	α^{224}	00010010

注１．生成多項式

$$g(x) = x^7 + \alpha^{87} \cdot x^6 + \alpha^{229} \cdot x^5 + \alpha^{146} \cdot x^4 + \alpha^{149} \cdot x^3 + \alpha^{238} \cdot x^2 + \alpha^{102} \cdot x + \alpha^{21}$$

は

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

と因数分解できます．他の型の生成多項式も同様です．例えば，誤り訂正コード語 10 個の場合の生成多項式は

$$g(x) = (x-1)(x-\alpha)(x-\alpha^2)(x-\alpha^3)(x-\alpha^4)(x-\alpha^5)(x-\alpha^6)(x-\alpha^7)(x-\alpha^8)(x-\alpha^9)$$

となります．展開して整理したものを表 5 に載せておきます．たくさんあるので一部分だけです．ただし，1 型，2 型で使用される生成多項式は書いておくことにします.

表5. リード・ソロモン生成多項式

r	生成多項式
7	$x^7+\alpha^{87}x^6+\alpha^{229}x^5+\alpha^{146}x^4+\alpha^{149}x^3+\alpha^{238}x^2+\alpha^{102}x+\alpha^{21}$
10	$x^{10}+\alpha^{251}x^9+\alpha^{67}x^8+\alpha^{61}x^6+\alpha^{118}x^5+\alpha^{70}x^4+\alpha^{64}x^3+\alpha^{94}x^2+\alpha^{32}x+\alpha^{45}$
13	$x^{13}+\alpha^{74}x^{12}+\alpha^{152}x^{11}+\alpha^{176}x^{10}+\alpha^{100}x^9+\alpha^{86}x^8+\alpha^{100}x^7+\alpha^{106}x^6+\alpha^{104}x^5+\alpha^{130}x^4+\alpha^{218}x^3+\alpha^{206}x^2+\alpha^{140}x+\alpha^{78}$
15	$x^{15}+\alpha^8x^{14}+\alpha^{183}x^{13}+\alpha^{61}x^{12}+\alpha^{91}x^{11}+\alpha^{202}x^{10}+\alpha^{37}x^9+\alpha^{51}x^8+\alpha^{58}x^7+\alpha^{58}x^6+\alpha^{237}x^5+\alpha^{140}x^4+\alpha^{124}x^3+\alpha^5x^2+\alpha^{99}x+\alpha^{105}$
16	$x^{16}+\alpha^{120}x^{15}+\alpha^{104}x^{14}+\alpha^{107}x^{13}+\alpha^{109}x^{12}+\alpha^{102}x^{11}+\alpha^{161}x^{10}+\alpha^{76}x^9+\alpha^3x^8+\alpha^{91}x^7+\alpha^{191}x^6+\alpha^{147}x^5+\alpha^{169}x^4+\alpha^{182}x^3+\alpha^{194}x^2+\alpha^{225}x+\alpha^{120}$
17	$x^{17}+\alpha^{43}x^{16}+\alpha^{139}x^{15}+\alpha^{206}x^{14}+\alpha^{78}x^{13}+\alpha^{43}x^{12}+\alpha^{239}x^{11}+\alpha^{123}x^{10}+\alpha^{206}x^9+\alpha^{214}x^8+\alpha^{147}x^7+\alpha^{24}x^6+\alpha^{99}x^5+\alpha^{150}x^4+\alpha^{39}x^3+\alpha^{243}x^2+\alpha^{163}x+\alpha^{136}$
18	$x^{18}+\alpha^{215}x^{17}+\alpha^{234}x^{16}+\alpha^{158}x^{15}+\alpha^{94}x^{14}+\alpha^{184}x^{13}+\alpha^{97}x^{12}+\alpha^{118}x^{11}+\alpha^{170}x^{10}+\alpha^{79}x^9+\alpha^{187}x^8+\alpha^{152}x^7+\alpha^{148}x^6+\alpha^{252}x^5+\alpha^{179}x^4+\alpha^5x^3+\alpha^{98}x^2+\alpha^{96}x+\alpha^{153}$
22	$x^{22}+\alpha^{210}x^{21}+\alpha^{171}x^{20}+\alpha^{247}x^{19}+\alpha^{242}x^{18}+\alpha^{93}x^{17}+\alpha^{230}x^{16}+\alpha^{14}x^{15}+\alpha^{109}x^{14}+\alpha^{221}x^{13}+\alpha^{53}x^{12}+\alpha^{200}x^{11}+\alpha^{74}x^{10}+\alpha^8x^9+\alpha^{172}x^8+\alpha^{98}x^7+\alpha^{80}x^6+\alpha^{219}x^5+\alpha^{134}x^4+\alpha^{160}x^3+\alpha^{105}x^2+\alpha^{165}x+\alpha^{231}$
28	$x^{28}+\alpha^{168}x^{27}+\alpha^{223}x^{26}+\alpha^{200}x^{25}+\alpha^{104}x^{24}+\alpha^{224}x^{23}+\alpha^{234}x^{22}+\alpha^{108}x^{21}+\alpha^{180}x^{20}+\alpha^{110}x^{19}+\alpha^{190}x^{18}+\alpha^{195}x^{17}+\alpha^{147}x^{16}+\alpha^{205}x^{15}+\alpha^{27}x^{14}+\alpha^{232}x^{13}+\alpha^{201}x^{12}+\alpha^{21}x^{11}+\alpha^{43}x^{10}+\alpha^{245}x^9+\alpha^{87}x^8+\alpha^{42}x^7+\alpha^{195}x^6+\alpha^{212}x^5+\alpha^{119}x^4+\alpha^{242}x^3+\alpha^{37}x^2+\alpha^9x+\alpha^{123}$
...	
...	途中略
...	
68	$x^{68}+\alpha^{247}x^{67}+\alpha^{159}x^{66}+\alpha^{223}x^{65}+\alpha^{33}x^{64}+\alpha^{224}x^{63}+\alpha^{93}x^{62}+\alpha^{77}x^{61}+\alpha^{70}x^{60}+\alpha^{90}x^{59}+\alpha^{160}x^{58}+\alpha^{32}x^{57}+\alpha^{254}x^{56}+\alpha^{43}x^{55}+\alpha^{150}x^{54}+\alpha^{84}x^{53}+\alpha^{101}x^{52}+\alpha^{190}x^{51}+\alpha^{205}x^{50}+\alpha^{133}x^{49}+\alpha^{52}x^{48}+\alpha^{60}x^{47}+\alpha^{202}x^{46}+\alpha^{165}x^{45}+\alpha^{220}x^{44}+\alpha^{203}x^{43}+\alpha^{151}x^{42}+\alpha^{93}x^{41}+\alpha^{84}x^{40}+\alpha^{15}x^{39}+\alpha^{84}x^{38}+\alpha^{253}x^{37}+\alpha^{173}x^{36}+\alpha^{160}x^{35}+\alpha^{89}x^{34}+\alpha^{227}x^{33}+\alpha^{52}x^{32}+\alpha^{199}x^{31}+\alpha^{97}x^{30}+\alpha^{95}x^{29}+\alpha^{231}x^{28}+\alpha^{52}x^{27}+\alpha^{177}x^{26}+\alpha^{41}x^{25}+\alpha^{125}x^{24}+\alpha^{137}x^{23}+\alpha^{241}x^{22}+\alpha^{166}x^{21}+\alpha^{225}x^{20}+\alpha^{118}x^{19}+\alpha^2x^{18}+\alpha^{54}x^{17}+\alpha^{32}x^{16}+\alpha^{82}x^{15}+\alpha^{215}x^{14}+\alpha^{175}x^{13}+\alpha^{198}x^{12}+\alpha^{43}x^{11}+\alpha^{238}x^{10}+\alpha^{235}x^9+\alpha^{27}x^8+\alpha^{101}x^7+\alpha^{184}x^6+\alpha^{127}x^5+\alpha^3x^4+\alpha^5x^3+\alpha^8x^2+\alpha^{163}x+\alpha^{238}$

r：誤り訂正コード語数

3　誤り訂正の仕組み

以下の説明は少し数学的になります.
多項式はすべて，0,1 を係数にもつ多項式を考えます (体 GF(2) 上の多項式).

3.1　なぜ最小距離が 7 以上になるのか

Example 4 の 15 bit の BCH 符号をみると，お互いの距離の最小値は 7 でした．なぜこんなにうまく作られているのでしょうか．ここではそのしくみを考えます.

長さ n で情報ビットが k の符号を次のように定義します.
Definition 1.
n, k $(n > k)$ を自然数とし，$g(x)$ を $n-k$ 次の多項式とする.

$$C = \{f(x);\ f(x) = h(x)g(x),\ h(x) \text{ は } (k-1) \text{ 次以下の任意の多項式 }\}$$

とおく．C を $g(x)$ によって生成される (n, k) コード，あるいは (n, k) 符号という．$g(x)$ をこの符号の生成多項式という．　□
注１．$f(x)$ は $n-1$ 次以下の多項式です.
注２．全体集合 F は n bit の列全体で,

$$F = \{r_{n-1}r_{n-2}\cdots r_2r_1r_0;\ r_j \text{ は } 0 \text{ または } 1 \ \}$$

です．C は F の部分集合です．F を体 GF(2^n) と考える必要はありません．n 次以上の多項式が出てこないようにしていますから，F の中で積が定義されていなくても問題ありません．上の定義は部分集合 C の作り方を述べているだけです．F は体ではありませんが，F の中で和が定義されていて，0,1 倍 (スカラー倍) も定義されていますから，F はベクトル空間になります.
注３．今，n 次以上の多項式は出てこないと書きましが，巡回符号を考えるとき，$x^n = 1$ の条件をつけて n 次以上の多項式を考える場合があります.
注４．$\mathbf{0} \in \mathbf{C}$ です．以下で述べるように，$C \subset F$ は部分空間になります.

Lemma 1.
C を (n, k) 符号とする．　このとき，$\boldsymbol{x}, \boldsymbol{y} \in C$ ならば，$\boldsymbol{x} + \boldsymbol{y} \in C$ である.
Proof.
$\boldsymbol{x} = f_1(x) = h_1(x)g(x),\ \ \boldsymbol{y} = f_2(x) = h_2(x)g(x) \in C$ のとき,

$$\boldsymbol{x} + \boldsymbol{y} = f_1(x) + f_2(x) = (h_1(x) + h_2(x))g(x) \in C \quad \square$$

$a \in \{0, 1\}$ に対して，明らかに $a \cdot f(x) \in C$ です．従って，$C \subset F$ は部分空間になります.

Example 4 の 15 bit の BCH 符号 C を見て下さい．C はうまく散らばって作られていて，その最小距離は 7 でした．C の元をよく見ると 1 の個数は 7 か 8 か 15 で

$\mathbf{0}$=(000000000000000) を除いてその最小値は 7 です．このように最小距離とその符号に出てくる 1 の個数の間に関係があります．それが次の Lemma 2 です．

$\boldsymbol{z} \in C$ に対して，$w(\boldsymbol{z})$ を $\boldsymbol{z}$ の中の 1 の個数とします．

Lemma 2.

任意の $\boldsymbol{x}, \boldsymbol{y} \in C$ の最小距離を d_0 とする．このとき，任意の $\boldsymbol{z} \in C, \boldsymbol{z} \neq \mathbf{0}$ に対して，$w(\boldsymbol{z})$ の最小値は d_0 である．また，その逆も成立する．

Proof.

最小距離が d_0 である $\boldsymbol{x}, \boldsymbol{y} \in C$ を考える．$\boldsymbol{x}$ と $\boldsymbol{y}$ は d_0 個の場所で異なっているから，$\boldsymbol{x}+\boldsymbol{y}$ の 1 の個数は d_0 個である．ゆえに $w(\boldsymbol{x}+\boldsymbol{y}) = d_0$．$\boldsymbol{x}+\boldsymbol{y} \in C$ だから，1 の個数が d_0 個のものが存在する．また，任意の $\boldsymbol{z} \in C, \boldsymbol{z} \neq \mathbf{0}$ を考えると仮定より，$\boldsymbol{z}$ と $\mathbf{0}$ との距離は d_0 以上だから $w(\boldsymbol{z}) \geq d_0$．よって，$w(\boldsymbol{z})$ の最小値は d_0 である．

$w(\boldsymbol{z})$ の最小値を d_0 とする．もし，$\boldsymbol{x}, \boldsymbol{y} \in C$ の最小距離が $d_1 \neq d_0$ なら，上のことより，$w(\boldsymbol{z})$ の最小値は d_1 になる．これは矛盾である．よって，$\boldsymbol{x}, \boldsymbol{y} \in C$ の最小距離は d_0 である． □

それでは 15 bit の BCH 符号に出てくる 1 の個数が 7 以上になるしくみは何でしょう．そのしくみは生成多項式 $g(x)$ の作り方にあります．$x^4+x+1=0$ の根の 1 つを α とすると $g(x)=0$ は $\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6$ を根に持ちます (Cf. Example 11)．この連続した根の個数が 6 個ですから，1 の個数は 7 以上になるというのです．証明してみます．

簡単のために (111111000000000) $\notin C$ を示します．これは 1 の数が 6 個のものです．(001010110100100) など，1 がどこにあっても証明できますが，証明をわかりやすくするためです．1 の場所を決めただけです．

$$Y(x) = r_{14}x^{14} + r_{13}x^{13} + r_{12}x^{12} + r_{11}x^{11} + r_{10}x^{10} + r_9x^9 \in C$$

とします．この形は (110101000000000) など 1 の個数が 6 個以下のものも含んでいます．$Y(x) = h(x)g(x)$ ですから，$Y(x)=0$ は $\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6$ を根を持ちます．$Y(\alpha)=0$ より，

$$r_{14}\alpha^{14} + r_{13}\alpha^{13} + r_{12}\alpha^{12} + r_{11}\alpha^{11} + r_{10}\alpha^{10} + r_9\alpha^9 = 0$$

$Y(\alpha^2)=0$ より，

$$r_{14}\alpha^{28} + r_{13}\alpha^{26} + r_{12}\alpha^{24} + r_{11}\alpha^{22} + r_{10}\alpha^{20} + r_9\alpha^{18} = 0$$

です．

$$a=\alpha^{14},\ b=\alpha^{13},\ c=\alpha^{12},\ d=\alpha^{11},\ e=\alpha^{10},\ f=\alpha^9$$

とおくと

$$a\cdot r_{14} + b\cdot r_{13} + c\cdot r_{12} + d\cdot r_{11} + e\cdot r_{10} + f\cdot r_9 = 0$$

と

$$a^2\cdot r_{14} + b^2\cdot r_{13} + c^2\cdot r_{12} + d^2\cdot r_{11} + e^2\cdot r_{10} + f^2\cdot r_9 = 0$$

を得ます．同様に $\alpha^3, \alpha^4, \alpha^5, \alpha^6$ が根であることより

$$a^3\cdot r_{14} + b^3\cdot r_{13} + c^3\cdot r_{12} + d^3\cdot r_{11} + e^3\cdot r_{10} + f^3\cdot r_9 = 0$$

$$a^4 \cdot r_{14} + b^4 \cdot r_{13} + c^4 \cdot r_{12} + d^4 \cdot r_{11} + e^4 \cdot r_{10} + f^4 \cdot r_9 = 0$$
$$a^5 \cdot r_{14} + b^5 \cdot r_{13} + c^5 \cdot r_{12} + d^5 \cdot r_{11} + e^5 \cdot r_{10} + f^5 \cdot r_9 = 0$$
$$a^6 \cdot r_{14} + b^6 \cdot r_{13} + c^6 \cdot r_{12} + d^6 \cdot r_{11} + e^6 \cdot r_{10} + f^6 \cdot r_9 = 0$$

を得ます．この 6 つの式を $r_{14},\ r_{13},\ r_{12},\ r_{11},\ r_{10},\ r_9$ に対する連立 1 次方程式と考えて解きます．係数の行列式を考えると

$$|A| = \begin{vmatrix} a & b & c & d & e & f \\ a^2 & b^2 & c^2 & d^2 & e^2 & f^2 \\ a^3 & b^3 & c^3 & d^3 & e^3 & f^3 \\ a^4 & b^4 & c^4 & d^4 & e^4 & f^4 \\ a^5 & b^5 & c^5 & d^5 & e^5 & f^5 \\ a^6 & b^6 & c^6 & d^6 & e^6 & f^6 \end{vmatrix} = abcdef \begin{vmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ a & b & c & d & e & f \\ a^2 & b^2 & c^2 & d^2 & e^2 & f^2 \\ a^3 & b^3 & c^3 & d^3 & e^3 & f^3 \\ a^4 & b^4 & c^4 & d^4 & e^4 & f^4 \\ a^5 & b^5 & c^5 & d^5 & e^5 & f^5 \end{vmatrix} \neq 0$$

となります．最後の行列式は Vandermonde の行列式として知られています．a, b, c, d, e, f はゼロでなく，すべて異なりますから $|A| \neq 0$ です．従って，

$$r_{14} = 0,\ r_{13} = 0,\ r_{12} = 0,\ r_{11} = 0,\ r_{10} = 0,\ r_9 = 0$$

になります．よって，$Y(x) = 0$ です．つまり，ゼロ元を除いて 1 の個数が 6 個以下のものは C の中に存在しないことがわかります．

一般の証明も同じです．(001010110100100) の場合は a, b, c, d, e, f の取り方が変わるだけです．また，連続した解 6 個であれば $\alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7, \alpha^8$ などでもよいことがわかります．

Example 11.
$x^4 + x + 1 = 0$ の 1 つの根を α とすると

$$\mathrm{GF}(2^4) = \{0, 1, \alpha, \alpha^2, \alpha^3, \cdots, \alpha^{14}\}$$

と書けました．これらがどんな方程式の解になっているか調べておきます．
$\alpha^{15} = 1$ です．$(\alpha^j)^{15} = (\alpha^{15})^j = 1$ だから，α^j はすべて $x^{15} - 1 = 0$ の根になります．0 も入れるなら，$\mathrm{GF}(2^4)$ の元はすべて $x^{16} - x = 0$ の根になります．$x^{16} - x$ の因数分解は

$$x^{16} - x = x(x+1)(x^2 + x + 1)(x^4 + x^3 + x^2 + x + 1)(x^4 + x^3 + 1)(x^4 + x + 1)$$

です．$\alpha^4 + \alpha + 1 = 0$ ですが，偶数乗の公式より

$$(\alpha^2)^4 + \alpha^2 + 1 = (\alpha^4)^2 + \alpha^2 + 1 = (\alpha^4 + \alpha + 1)^2 = 0$$

となり，α^2 もまた $x^4 + x + 1 = 0$ の解になります．これは 一般に成立します．β を $f(x) = 0$ の解とすると β^2 もまた $f(x) = 0$ の解になります．従って，$\alpha, \alpha^2, \alpha^4, \alpha^8, \alpha^{16}, \cdots$ は $x^4 + x + 1 = 0$ の解になります．$\alpha^{16} = \alpha$ で元に戻りますから，

$$\alpha, \alpha^2, \alpha^4, \alpha^8 \quad \text{は} \quad x^4 + x + 1 = 0 \quad \text{の解}$$

になります．α^3 がどの因数の解になるかを調べます．$x^4+x^3+x^2+x+1=0$ の解になります．従って，$\alpha^3, \alpha^6, \alpha^{12}, \alpha^{24}=\alpha^9$ も解であることがわかります．以下同様にして

$$\alpha^3, \alpha^6, \alpha^9, \alpha^{12} \quad \text{は} \quad x^4+x^3+x^2+x+1=0 \quad \text{の解}$$

$$\alpha^7, \alpha^{11}, \alpha^{13}, \alpha^{14} \quad \text{は} \quad x^4+x^3+1=0 \quad \text{の解}$$

$$\alpha^5, \alpha^{10} \quad \text{は} \quad x^2+x+1=0 \quad \text{の解}$$

であることがわかります．従って，

$$g(x)=(x^2+x+1)(x^4+x^3+x^2+x+1)(x^4+x+1)=0$$

は $\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6$ を根に持ちます．　□

3.2　BCH 符号の定義

15 bit の BCH 符号がなぜ，GF(2^4) と関係しているのでしょうか．それは BCH 符号が長さ $n=2^m-1$ に対してだけ，定義されているからです．(n,k) 符号の長さ n は何でもよかったのですが，BCH 符号の長さは $n=1,3,7,15,31,63,\cdots$ だけです．6bit の BCH 符号はありません．従って，$n=15=2^4-1$ は GF(2^4) と関係があります．

m を与えます (長さ $n=2^m-1$ を与える)．もう 1 つ，誤り訂正の個数 t を与える必要があります．15 bit の BCH 符号の場合，3 ヶ所の誤りまで訂正できますから $t=3$ です．この場合，最小距離を $2t+1=7$ 以上にする必要がありました．そのためには生成多項式 $g(x)$ が $\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6$ を根に持つことが必要です．一般に t 個の誤りを検出するには $g(x)$ が $\alpha, \alpha^2, \alpha^3, \cdots, \alpha^{2t-1}, \alpha^{2t}$ を根に持つことが必要です．こうして，次の BCH 符号の定義に至ります．

Definition 2. (BCH 符号の定義)
自然数 m に対して，$n=2^m-1$ とおく．また，$2t<n$ なる自然数 t を考える．α を GF(2^m) の原始元とする．$p_i(x)$ を α^i を根としてもつ既約多項式とする．

$$g(x)=\mathrm{LCM}(p_1(x)p_2(x)p_3(x)p_4(x)\cdots p_{2t}(x))$$

とおく．$g(x)$ の次数を r とし，$k=n-r$ とおく．C を $g(x)$ によって生成される (n,k) コードとする．このとき，C を $t-$ 誤り訂正 BCH 符号という．　□

注 1．LCM は最小公倍多項式です．

注 2．原始元の定義はしてませんが，m 次の既約多項式の根で，GF(2^m) が α^j の形に書ける α のことです．

注 3．$g(x)=0$ は $\alpha, \alpha^2, \alpha^3, \cdots, \alpha^{2t-1}, \alpha^{2t}$ を解に持ちます．$g(x)$ はそのように作られていることがわかります．

注 4．k は情報ビットの bit 数になります．

注 5．$n=1$ は $2t<n$ なる t が存在しないので省きます．$n=3,7,15,31,63,127,\cdots$ です．次節で $n=3,7,15$ の場合の例題を考えます．

巡回符号

Example 4 の BCH 符号をよくみると，101011001000111 と 010110010001111 の２つのパターンしかないことがわかります．他のものはこれらを左にどんどんシフトしていって得られます．先頭 bit は１番最後にもってきます.

C の元を左にシフトしてもまた C の元になるとき，C を巡回符号と言います.

BCH 符号は巡回符号になります．一般の (n, k) 符号は巡回符号になるとは限りません．Example 4 の BCH 符号で証明してみます.

$$\boldsymbol{y} = r_{14}r_{13}r_{12}r_{11}r_{10}\cdots r_2r_1r_0 \in C$$

のとき,

$$r_{13}r_{12}r_{11}r_{10}r_9\cdots r_1r_0r_{14} \in C$$

であることを示します．$\boldsymbol{y}$ を

$$\boldsymbol{y} = Y(x) = r_{14}x^{14} + r_{13}x^{13} + r_{12}x^{12} + \cdots + r_2x^2 + r_1x + r_0 \in C$$

なる多項式と同一視します．$\boldsymbol{y} \in C$ より，$Y(x) = h(x)g(x)$ と書けます．ただし，$h(x)$ は４次以下の多項式，$g(x)$ は生成多項式で

$$g(x) = x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1$$

です．$xY(x)$ を考えます.

$$r_{14}x^{15} + r_{13}x^{14} + r_{12}x^{13} + \cdots + r_1x^2 + r_0x = xh(x)g(x)$$

となります.

$$r_{14}(x^{15} - 1) + r_{13}x^{14} + r_{12}x^{13} + \cdots + r_1x^2 + r_0x + r_{14} = xh(x)g(x)$$

ここで，$x^{15} - 1$ は $g(x)$ で割り切れます.

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

従って

$$r_{13}x^{14} + r_{12}x^{13} + \cdots + r_1x^2 + r_0x + r_{14} = (xh(x) - r_{14}(x + 1)(x^4 + x^3 + 1))g(x)$$

$$= h_1(x)g(x)$$

$r_{14} = 0$ のとき，$h(x)$ は３次以下の多項式ですから，$h_1(x)$ は４次以下の多項式です．$r_{14} = 1$ のとき，５次の項が消えますから，やはり $h_1(x)$ は４次以下の多項式です．従って,

$$r_{13}r_{12}r_{11}r_{10}r_9\cdots r_1r_0r_{14} \in C$$

を得ます．　□

以上のことから，単純に $x^{15} = 1$ として計算してよいことがわかります．一般の場合も同様です．符号の長さ n の BCH 符号においては $x^n = 1$ とおいて計算できます．こうしておけば何次の多項式でも扱えます.

Example 4 の BCH 符号の場合，000010100110111 をシフトしたものは 15 個あります．この 15 個を［000010100110111］と書くことにします．すると Example 4 の C は

$C = \{000000000000000,\ [000010100110111],\ [010110010001111], 111111111111111\}$

と書けます．こう書くとパターンがよく見えてきます．1 の個数が 7 個の［000010100110111］と 8 個の［010110010001111］です．それぞれ 15 個あり，あと自明な符号が 2 個ありますから，全部で 32 個あります．

3.3 BCH 符号の例

BCH 符号の例題を考えますが，最初にまとめを書いておきます．詳しくは Example を見てください．

表6. 15bit 以下の BCH 符号

m	長さ n	情報ビット k	誤り訂正 t	$g(x)$ の次数 r	C の元の個数 ℓ	備考
2	3	1	1	2	2	Ex.3,12
3	7	4	1	3	16	Ex.13
3	7	1	2	6	2	Ex.14
3	7	1	3	6	2	Ex.14
4	15	11	1	4	2048	Ex.15
4	15	7	2	8	128	Ex.16
4	15	5	3	10	32	Ex.17
4	15	1	4	14	2	Ex.18
4	15	1	5	14	2	Ex.18
4	15	1	6	14	2	Ex.18
4	15	1	7	14	2	Ex.18

説明

自然数 m と t を与えます．ただし，$2t < 2^m - 1$．すると符号の長さ $n = 2^m - 1$ と生成多項式の次数 r が定まります．関係式

$$n = 2^m - 1, \quad k = n - r, \quad \ell = 2^k, \quad 2t < n.$$

より，k と ℓ が得られます．意味のある BCH 符号は

$$(n, k) = (7, 4), \quad (15, 11), \quad (15, 7), \quad (15, 5)$$

の場合だけです．他は自明な符号ばかりです． □

Example 12. ($m = 2,\ t = 1$ の場合)

符号の長さは $n = 2^2 - 1 = 3$ です．GF(2^2) は 4 個の元をもつ有限体ですが，$x^2 + x + 1 = 0$ の 1 つの解を α とすると

$$\mathrm{GF}(2^2) = \{0, 1, \alpha, \alpha^2\}$$

と書けます．$t = 1$ ですから，誤り訂正は 1 ヶ所です．α, α^2 を解にもつ生成多項式を求めます．$\alpha^2 + \alpha + 1 = 0$ ですが，偶数乗の公式より

$$(\alpha^2)^2 + \alpha^2 + 1 = (\alpha^2 + \alpha + 1)^2 = 0$$

となり，α^2 もまた $x^2 + x + 1 = 0$ の解になります．従って $p_1(x) = p_2(x) = x^2 + x + 1$ です．よって，生成多項式は

$$g(x) = \mathrm{LCM}(p_1(x)p_2(x)) = p_1(x) = x^2 + x + 1$$

です．生成多項式の次数 $r = 2$ ですから，情報ビットは $k = n - r = 1$ bit です．3 bit は 2 次の多項式で書けますから，$0 \cdot x^2$ と $1 \cdot x^2$ を $x^2 + x + 1$ で割って余りを求めると 00 と 11 を得ます．従って，BCH 符号は

$$C = \{000,\ 111\}$$

となります．自明な符号しか得られません． □

次に 7 bit の例を考えてみます．

Example 13. ($m = 3,\ t = 1$ の場合)

符号の長さは $n = 2^3 - 1 = 7$ です．GF(2^3) は 8 個の元をもつ有限体ですが，$x^3 + x + 1 = 0$ の 1 つの解を α とすると

$$\mathrm{GF}(2^3) = \{0, 1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6\}$$

と書けます．$t = 1$ ですから，誤り訂正は 1 ヶ所です．α, α^2 を解にもつ生成多項式を求めます．α は $x^3 + x + 1 = 0$ の根ですが，偶数乗の公式より α^2 もまた根になります．従って，$p_1(x) = p_2(x) = x^3 + x + 1$ です．よって，生成多項式は

$$g(x) = \mathrm{LCM}(p_1(x)p_2(x)) = p_1(x) = x^3 + x + 1$$

です．生成多項式の次数 $r = 3$ ですから，情報ビットは $k = n - r = 4$ bit です．BCH 符号 C の元の個数は $2^4 = 16$ 個です．これは個数が少ないので全部書いてみます．

$$C = \{0000000,\ 0001011,\ 0010110,\ 0011101,\ 0100111,\ 0101100,\ 0110001,\ 0111010,$$

$$1000101,\ 1001110,\ 1010011,\ 1011000,\ 1100010,\ 1101001,\ 1110100,\ 1111111\}$$

となります．どれか 1 つ計算してみます．(1001110) を計算してみます．7 bit は 6 次の多項式で表されるので，情報ビットの多項式は $(1001) = x^6 + x^3$ です．これを $g(x) = x^3 + x + 1$ で割って余りを求めます．

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

よって，余りは $x^2 + x = (110)$ になります．これを情報ビットにつなげて，(1001110) を得ます．C は巡回符号なので

$$C = \{0000000,\ [0001011],\ [0100111],\ 1111111\}$$

と書けます．1 の個数が 3 個である `[0001011]` と 4 個である `[0100111]`．それぞれ 7 個あり，あと自明な符号が 2 個ありますから，全部で 16 個です．最小距離は 3 であることがわかります．従って，1 ヶ所の誤りを判定することができます． □

Example 14. ($m = 3,\ t = 2$ の場合)

Example 13 と同様です．$t = 2$ ですから，$\alpha, \alpha^2, \alpha^3, \alpha^4$ を解にもつ生成多項式を求めます．

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

と因数分解できます．α^3 は $x^3+x^2+1=0$ の解になります．従って，

$$g(x) = \mathrm{LCM}(p_1(x)p_2(x)p_3(x)p_4(x)) = p_1(x)p_3(x)$$

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

となります．$k=n-r=1$ となり，情報ビットが 1bit, 長さ 7 bit の BCH 符号 C が得られます．

$$C = \{0000000,\ 1111111\}$$

です．自明な符号しか得られません．$t=3$ の場合も同じ C になります． □

次に 15 bit の例を考えてみます．

Example 15. ($m=4,\ t=1$ の場合)
符号の長さは $n=2^4-1=15$ です．$x^4+x+1=0$ の１つの解を α とします．
$t=1$ ですから，誤り訂正は１ヶ所です．α, α^2 を解にもつ生成多項式を求めます．

$$g(x) = \mathrm{LCM}(p_1(x)p_2(x))$$

$p_1(x)=p_2(x)=x^4+x+1$ ですから

$$g(x) = x^4+x+1$$

を得ます．$k=n-r=11$ となり，情報ビットが 11bit, 長さ 15 bit の BCH 符号が得られます．C の元の個数は $2^{11}=2,048$ 個あります．数が多いので書きませんが，C の元を見ると 1 の個数は $3,4,5,\cdots,12,15$ で，最小距離が 3 であることがわかります．従って，１ヶ所の誤りを判定することができます． □

Example 16. ($m=4,\ t=2$ の場合)
$t=2$ ですから，$\alpha, \alpha^2, \alpha^3, \alpha^4$ を解にもつ生成多項式を求めます．

$$g(x) = \mathrm{LCM}(p_1(x)p_2(x)p_3(x)p_4(x))$$

$p_1(x)=p_2(x)=p_4(x)=x^4+x+1$ ですから

$$g(x) = p_1(x)p_3(x) = (x^4+x+1)(x^4+x^3+x^2+x+1)$$

$$= x^8+x^7+x^6+x^4+1$$

です．$k=n-r=7$ となり，情報ビットが 7，長さ 15 の BCH 符号が得られます．C の元の個数は $2^7=128$ 個あります．

$$C = \{000000000000000,\ [010001000000111],\ [010010101000011],\ [001100000100111],$$

$$[000010100110111],\ [010110010001111],\ [001011010101111],\ [011000110011111],$$

$$[000101110111111],\ *001001001001001*,\ *011011011011011*,\ 111111111111111\}$$

です．$*001001001001001*$ は 3 回の巡回で元に戻るものを表しています．C の元を見ると 1 の個数は 5,6,7,8,9,10 か 15 で，最小距離が 5 であることがわかります．従って，2ヶ所以内の誤りを判定することができます． □

Example 17. ($m = 4,\ t = 3$ の場合)
$t = 3$ ですから，$\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6$ を根に持つ生成多項式 $g(x)$ を求めます．α^2, α^4 は $p_1(x) = x^4 + x + 1 = 0$ の解ですから，$p_1(x) = p_2(x) = p_4(x) = x^4 + x + 1$ です．同様に $p_3(x) = p_6(x) = x^4 + x^3 + x^2 + x + 1$ です．α^5 は $p_5(x) = x^2 + x + 1 = 0$ の解です．従って，生成多項式 $g(x)$ は

$$g(x) = \mathrm{LCM}(p_1(x)p_2(x)p_3(x)p_4(x)p_5(x)p_6(x))$$

$$= p_1(x)p_3(x)p_5(x) = (x^4 + x + 1)(x^4 + x^3 + x^2 + x + 1)(x^2 + x + 1)$$

$$= x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1$$

となります．これは Example 7 で考えた生成多項式になっています．
$g(x)$ が 10 次の多項式ですから，$k = n - r = 5$ となり，情報ビットが 5bit, 長さ 15 bit の BCH 符号が得られます． □

Example 18. ($m = 4,\ t = 4$ の場合)
$t = 4$ ですから，$\alpha, \alpha^2, \alpha^3, \alpha^4, \cdots, \alpha^8$ を解にもつ生成多項式を求めます．

$$g(x) = \mathrm{LCM}(p_1(x)p_2(x)p_3(x)p_4(x)\cdots p_8(x))$$

$$= p_1(x)p_3(x)p_5(x)p_7(x)$$

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

$$= x^{14} + x^{13} + x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$$

です．$k = n - r = 1$ となり，情報ビットが 1bit, 長さ 15 bit の BCH 符号 C が得られます．

$$C = \{000000000000000,\ 111111111111111\}$$

自明な符号しか得られません．$t = 5, 6, 7$ の場合も同じ C になります． □

4　誤り訂正方法

誤り訂正は距離の計算でできますが，C の元の個数が多くなると時間がかかります．また，C の元すべてを書いておくのも大変です．一般にはシンドロームなどの計算で誤り判定をします.

4.1　誤り位置を探す

15 bit の 3-誤り訂正 BCH 符号 C を考えます (Example 4,7,17).

$$\boldsymbol{y} = r_{14}r_{13}r_{12}r_{11}r_{10}r_9r_8r_7r_6r_5r_4r_3r_2r_1r_0 \in F$$

が与えられたとします.

$$Y(x) = r_{14}x^{14} + r_{13}x^{13} + r_{12}x^{12} + r_{11}x^{11} + r_{10}x^{10} + r_9x^9 + r_8x^8$$

$$+r_7x^7 + r_6x^6 + r_5x^5 + r_4x^4 + r_3x^3 + r_2x^2 + r_1x + r_0$$

とおきます．今，$\boldsymbol{y}_0$ を正しい符号とし，$\boldsymbol{y}$ が $\boldsymbol{y}_0$ と 9 次と 7 次と 4 次の項だけ違っていたとします．すると，その項だけに 1 を足せば (誤りを修正すれば)，それは正しい符号になりますから,

$$\boldsymbol{y}_0 = r_{14}r_{13}r_{12}r_{11}r_{10}(r_9+1)r_8(r_7+1)r_6r_5(r_4+1)r_3r_2r_1r_0 \in C$$

です.

$$Y_0(x) = r_{14}x^{14} + r_{13}x^{13} + r_{12}x^{12} + r_{11}x^{11} + r_{10}x^{10} + (r_9+1)r_9x^9 + r_8x^8$$

$$+(r_7+1)x^7 + r_6x^6 + r_5x^5 + (r_4+1)x^4 + r_3x^3 + r_2x^2 + r_1x + r_0$$

とおくと，$Y_0(x) = Y(x) + x^9 + x^7 + x^4$ です．$Y_0(x)$ は正しい符号です．移行すれば

$$Y(x) = Y_0(x) + x^9 + x^7 + x^4$$

となります．$Y(x)$ が与えられたとき，誤り位置 9,7,4 を求めることが問題です.

一般に p, q, r の場所が間違っていたとします．３ヶ所の誤り訂正を考えます.

$$Y(x) = Y_0(x) + x^p + x^q + x^r$$

です．ただし，p, q, r はすべて異なるとし，$p, q, r = 0, 1, 2, \cdots, 14$ とします.
$Y(x)$ は与えられているので計算できますが，$Y_0(x)$ と p, q, r は未知です.

$\alpha^4 + \alpha + 1 = 0$ を満たす α を考えます．$Y_0(x) \in C$ なので,

$$Y_0(x) = h(x)g(x)$$

と書けます．生成多項式 $g(x)$ の作り方から，$g(x)=0$ は $\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6$ を根に持ちます．従って，

$$Y_0(\alpha)=Y_0(\alpha^2)=Y_0(\alpha^3)=Y_0(\alpha^4)=Y_0(\alpha^5)=Y_0(\alpha^6)=0$$

です．$Y_0(\alpha)=0$ より，$Y(\alpha)=\alpha^p+\alpha^q+\alpha^r$，$Y_0(\alpha^2)=0$ より，$Y(\alpha^2)=\alpha^{2p}+\alpha^{2q}+\alpha^{2r}$ となります．$\alpha^p,\ \alpha^q,\ \alpha^r$ は煩雑なので

$$u=\alpha^p, \quad v=\alpha^q, \quad w=\alpha^r$$

とおきます．すると

$$Y(\alpha)=u+v+w$$
$$Y(\alpha^2)=u^2+v^2+w^2$$

同様に

$$Y(\alpha^3)=u^3+v^3+w^3$$
$$Y(\alpha^4)=u^4+v^4+w^4$$
$$Y(\alpha^5)=u^5+v^5+w^5$$
$$Y(\alpha^6)=u^6+v^6+w^6$$

となります．$Y(\alpha^i),\ i=1,2,3,4,5,6$ は計算できますが，u,v,w は未知です．$Y(\alpha^i)$ が計算できるという意味は $Y(\alpha^i)\in \mathrm{GF}(2^4)$ ですから $Y(\alpha^i)=\alpha^j$ の形になるということです．α を使って計算できるという意味です．

$$S_1(\alpha)=Y(\alpha),\ S_2(\alpha)=Y(\alpha^2),\ S_3(\alpha)=Y(\alpha^3),$$

$$S_4(\alpha)=Y(\alpha^4),\ S_5(\alpha)=Y(\alpha^5),\ S_6(\alpha)=Y(\alpha^6)$$

とおき，$S_1(\alpha), S_2(\alpha), S_3(\alpha), S_4(\alpha), S_5(\alpha), S_6(\alpha)$ をシンドローム (Syndrome) と言います．シンドロームは症候群，行動の型の意味です．以下では α を省略してシンドロームを $S_1,\ S_2,\ S_3,\ S_4,\ S_5,\ S_6$ と書くことにします．

$$S_2=Y(\alpha^2)=(Y(\alpha))^2=(S_1)^2,$$

$$S_4=Y(\alpha^4)=(Y(\alpha))^4=(S_1)^4,$$
$$S_6=Y(\alpha^6)=(Y(\alpha^3))^2=(S_3)^2$$

ですから，本質的な量は $S_1,\ S_3,\ S_5$ だけになります．

u,v,w を直接求めることはできないので，誤り位置多項式と呼ばれる次の 3 次の多項式 $E(x)$ を求めます．

$$E(x)=(x-u)(x-v)(x-w)$$

ただし，$E(x)$ は α^j を係数に持ちます．今，仮に $E(x)$ が求まったとします．このとき，
$\alpha^0,\ \alpha^1,\ \alpha^2,\ \alpha^3,\cdots,\alpha^{14}$ を $E(x)$ に代入し，$E(\alpha^j)=0$ を得るならば j が誤り位置です．このような j は 3 つあります．こうして 3 ヶ所の誤りを訂正することができます．

4.2　誤り位置多項式

$$E(x) = (x-u)(x-v)(x-w)$$

でした．$E(x)$ を展開した３次の多項式を

$$E(x) = x^3 + \sigma_1 x^2 + \sigma_2 x + \sigma_3$$

とします．根と係数の関係から，

$$\sigma_1 = u+v+w, \quad \sigma_2 = uv+vw+wu, \quad \sigma_3 = uvw$$

です．また，シンドロームと u, v, w の関係は

$$S_1 = u+v+w, \quad S_2 = u^2+v^2+w^2, \quad S_3 = u^3+v^3+w^3$$

$$S_4 = u^4+v^4+w^4, \quad S_5 = u^5+v^5+w^5, \quad S_6 = u^6+v^6+w^6$$

でした．問題は S_1, S_2, S_3, S_4, S_5 が与えられたとき，u, v, w を消去して，$\sigma_1,\ \sigma_2,\ \sigma_3$ を求めることです．

明らかに $\sigma_1 = u+v+w = S_1$ です．u, v, w は

$$E(x) = x^3 + \sigma_1 x^2 + \sigma_2 x + \sigma_3 = 0$$

の根ですから

$$(1)\begin{cases} u^3+\sigma_1 u^2+\sigma_2 u+\sigma_3 &= 0 & \cdots(\mathrm{i}) \\ v^3+\sigma_1 v^2+\sigma_2 v+\sigma_3 &= 0 & \cdots(\mathrm{ii}) \\ w^3+\sigma_1 w^2+\sigma_2 w+\sigma_3 &= 0 & \cdots(\mathrm{iii}) \end{cases}$$

を得ます．辺々たし算すると

$$u^3+v^3+w^3+(u^2+v^2+w^2)\sigma_1+(u+v+w)\sigma_1+\sigma_3 = 0$$

です．従って，

$$S_3 + S_2\sigma_1 + S_1\sigma_2 + \sigma_3 = 0$$

を得ます．もう一つ式が必要です．(1)-(i) を u 倍，(ii) を v 倍，(iii) を w 倍して加えると

$$u^4+v^4+w^4+(u^3+v^3+w^3)\sigma_1+(u^2+v^2+w^2)\sigma_1+(u+v+w)\sigma_3 = 0$$

を得ます．すなわち，

$$S_4 + S_3\sigma_1 + S_2\sigma_2 + S_1\sigma_3 = 0$$

です．この２つの式を $\sigma_2,\ \sigma_3$ に対する連立１次方程式とみると係数の行列式は

$$(S_1)^2 - S_2 = 0$$

となります．よってこの２つの式は独立ではありません．独立な式を得るために (1)-(i) を u^2 倍，(ii) を v^2 倍，(iii) を w^2 倍して加えます．

$$u^5+v^5+w^5+(u^4+v^4+w^4)\sigma_1+(u^3+v^3+w^3)\sigma_1+(u^2+v^2+w^2)\sigma_3 = 0$$

すなわち,

$$S_5 + S_4\sigma_1 + S_3\sigma_2 + S_2\sigma_3 = 0$$

を得ます．今度は係数の行列式は

$$S_1S_2 + S_3 \neq 0$$

となります (Cf. Lemma 3)．従って，$\sigma_1,\ \sigma_2,\ \sigma_3$ に対する連立１次方程式は

$$(2)\begin{cases} S_1 + \sigma_1 & = & 0 & \cdots(\mathrm{i}) \\ S_3 + S_2\sigma_1 + S_1\sigma_2 + \sigma_3 & = & 0 & \cdots(\mathrm{ii}) \\ S_5 + S_4\sigma_1 + S_3\sigma_2 + S_2\sigma_3 & = & 0 & \cdots(\mathrm{iii}) \end{cases}$$

となります．この連立１次方程式を解いて，$\sigma_1,\ \sigma_2,\ \sigma_3$ を求め，$E(x)$ をつくるとこれが誤り位置多項式になります．また，2 個以下の誤りもこの $E(x)$ で判定できます.

Lemma 3.

$$S_1 = u + v + w, \quad S_2 = u^2 + v^2 + w^2, \quad S_3 = u^3 + v^3 + w^3$$

とおく．u, v, w がすべて異なるとき，$S_3 - S_1S_2 \neq 0$ である．

Proof.

$$S_3 - S_1S_2 = u^3 + v^3 + w^3 - (u + v + w)(u^2 + v^2 + w^2)$$

$$= uv^2 + uw^2 + vu^2 + vw^2 + wu^2 + wv^2 = (u + v)(v + w)(w + u) \neq 0 \quad \square$$

4.3　シンドロームの計算

15 bit のデータ

$$\boldsymbol{y} = r_{14}r_{13}r_{12}r_{11}r_{10}r_9r_8r_7r_6r_5r_4r_3r_2r_1r_0$$

が与えられたとします.

$$Y(x) = r_0 + r_1x + r_2x^2 + r_3x^3 + r_4x^4 + r_5x^5 + r_6x^6 + r_7x^7$$

$$+r_8x^8 + r_9x^9 + r_{10}x^{10} + r_{11}x^{11} + r_{12}x^{12} + r_{13}x^{13} + r_{14}x^{14}$$

とおきます.

α を $x^4 + x + 1 = 0$ の１つの根としたとき，シンドロームは

$$S_1(\alpha) = Y(\alpha), \quad S_2(\alpha) = (S_1(\alpha))^2, \quad S_3(\alpha) = Y(\alpha^3),$$

$$S_4(\alpha) = (S_1(\alpha))^4, \quad S_5(\alpha) = Y(\alpha^5)$$

でした．シンドロームは $GF(2^4)$ の元ですから α の３次以下の多項式で書けます．これを計算してみます．表１を使って，α^4 以上を α^3 以下に落としてやればできます．結果だけを書くと次のようになります.

$$S_1(\alpha) = r_0 + r_4 + r_7 + r_8 + r_{10} + r_{12} + r_{13} + r_{14} + (r_1 + r_4 + r_5 + r_7 + r_9 + r_{10} + r_{11} + r_{12})\alpha$$

$$+(r_2+r_5+r_6+r_8+r_{10}+r_{11}+r_{12}+r_{13})\alpha^2+(r_3+r_6+r_7+r_9+r_{11}+r_{12}+r_{13}+r_{14})\alpha^3$$

$$S_3(\alpha)=r_0+r_4+r_5+r_9+r_{10}+r_{14}+(r_3+r_4+r_8+r_9+r_{13}+r_{14})\alpha$$

$$+(r_2+r_4+r_7+r_9+r_{12}+r_{14})\alpha^2+(r_1+r_2+r_3+r_4+r_6+r_7+r_8+r_9+r_{11}+r_{12}+r_{13}+r_{14})\alpha^3$$

$$S_5(\alpha)=r_0+r_2+r_3+r_5+r_6+r_8+r_9+r_{11}+r_{12}+r_{14}$$

$$+(r_1+r_2+r_4+r_5+r_7+r_8+r_{10}+r_{11}+r_{13}+r_{14})\alpha$$

$$+(r_1+r_2+r_4+r_5+r_7+r_8+r_{10}+r_{11}+r_{13}+r_{14})\alpha^2$$

シンドロームは $r_{14},\cdots,r_1,r_0$ が与えられると計算できるということです.

S_2,S_4 は $S_2=(S_1)^2,S_4=(S_1)^4$ より求めることができますが，成分で書くと次のようになります.

$$S_2(\alpha)=k_0+k_2+k_2\alpha+(k_1+k_3)\alpha^2+k_3\alpha^3$$

ただし，k_i は $S_1(\alpha)$ の係数.

$$S_4(\alpha)=k_0+k_1+k_2+k_3+(k_1+k_3)\alpha+(k_2+k_3)\alpha^2+k_3\alpha^3$$

また，3次以下の多項式は α^j $(0\le j\le 14)$ の形に書けるので，シンドロームは α^j $(0\le j\le 14)$ の形に書けます．ただし，シンドロームが 0 になることもあります.

4.4 誤り訂正の手順

15 bit のデータ

$$\boldsymbol{y}=r_{14}r_{13}r_{12}r_{11}r_{10}r_9r_8r_7r_6r_5r_4r_3r_2r_1r_0$$

が与えられたとします．3 ヶ所以内の誤りを訂正する手順は次のようになります.

手順１．　(シンドロームを計算する)

$$S_1,\ S_2,\ S_3,\ S_4,\ S_5$$

を計算する．シンドロームは 0 か α^j $(0\le j\le 14)$ の形になる.

注．S_6 は後の計算に必要ないので省きました.

手順２．　($\sigma_1,\ \sigma_2,\ \sigma_3$ を求める)

$\sigma_1,\ \sigma_2,\ \sigma_3$ に対する連立１次方程式

$$(2)\begin{cases} S_1+\sigma_1 & = & 0 & \cdots(\mathrm{i}) \\ S_3+S_2\sigma_1+S_1\sigma_2+\sigma_3 & = & 0 & \cdots(\mathrm{ii}) \\ S_5+S_4\sigma_1+S_3\sigma_2+S_2\sigma_3 & = & 0 & \cdots(\mathrm{iii}) \end{cases}$$

を解いて，$\sigma_1,\ \sigma_2,\ \sigma_3$ を求める．これらは 0 か α^j $(0\le j\le 14)$ の形になる.

ただし，連立１次方程式が無数の解をもつときは解 0 を取るものとする.

手順３．　(誤り位置多項式を求める)
上の $\sigma_1,\ \sigma_2,\ \sigma_3$ を代入して，誤り位置多項式

$$E(x) = x^3 + \sigma_1 x^2 + \sigma_2 x + \sigma_3$$

を求める．係数は 0 か α^j $(0 \leq j \leq 14)$ の形になる．

手順４．　(誤り判定を行う)
$1 = \alpha^0,\ \alpha^1,\ \alpha^2,\ \alpha^3, \cdots, \alpha^{14}$ を $E(x)$ に代入し，

$$E(\alpha^j) = 0$$

となる j を求める．この j が誤り位置である．j が３つあるときは３ヶ所の誤りを訂正する．２つのときは２ヶ所，１つのときは１ヶ所の誤りを訂正する．このような j が存在しないとき，$\boldsymbol{y}$ は正しい符号である．　□

３個の誤り訂正の説明はしましたが，２個以下の誤り訂正の説明はしてません．以下の例題でそれを説明します．結局，２個以下の誤り訂正は３個の誤り訂正において，$w = 0$ あるいは $v = w = 0$ とおいたものだということがわかります．

Example 18. (誤りが 0 ヶ所の場合)

$$\boldsymbol{y} = r_{14}r_{13}r_{12}r_{11}r_{10}r_9r_8r_7r_6r_5r_4r_3r_2r_1r_0 \in C$$

を正しい符号とします．このとき，シンドロームはすべて 0 になります．連立１次方程式

$$(2)\begin{cases} S_1 + \sigma_1 & = & 0 & \cdots(\mathrm{i}) \\ S_3 + S_2\sigma_1 + S_1\sigma_2 + \sigma_3 & = & 0 & \cdots(\mathrm{ii}) \\ S_5 + S_4\sigma_1 + S_3\sigma_2 + S_2\sigma_3 & = & 0 & \cdots(\mathrm{iii}) \end{cases}$$

は無数の解をもつので，$\sigma_1 = \sigma_2 = \sigma_3 = 0$ に取ります．すると誤り位置多項式は

$$E(x) = x^3$$

となります．$E(x) = 0$ の解は $x = 0$ のみです．従って，$x = \alpha^0,\ \alpha^1,\ \alpha^2, \cdots, \alpha^{14}$ を代入しても $E(x)$ は 0 にはなりません．従って，$\boldsymbol{y}$ は正しい符号であると判定できます．　□

Example 19. (誤りが 1 ヶ所の場合)
誤りが１ヶ所であるデータ

$$\boldsymbol{y} = r_{14}r_{13}r_{12}r_{11}r_{10}r_9r_8r_7r_6r_5r_4r_3r_2r_1r_0$$

が与えられたとします．p 次の項だけに誤りがあったとします．

$$Y(x) = Y_0(x) + x^p$$

でから，$Y(\alpha)=\alpha^p=u$ です．誤りが 3 ヶ所あるときの $v=w=0$ の場合になっています．従って，シンドロームは

$$S_1=u,\ S_2=u^2,\ S_3=u^3,\ S_4=u^4,\ S_5=u^5$$

となります．$\sigma_1=S_1=u$ です．連立 1 次方程式

$$(2)\begin{cases} S_1+\sigma_1 & = & 0 & \cdots(\mathrm{i}) \\ S_3+S_2\sigma_1+S_1\sigma_2+\sigma_3 & = & 0 & \cdots(\mathrm{ii}) \\ S_5+S_4\sigma_1+S_3\sigma_2+S_2\sigma_3 & = & 0 & \cdots(\mathrm{iii}) \end{cases}$$

の $\sigma_2,\ \sigma_3$ に対する行列式は

$$S_1S_2-S_3=u\cdot u^2-u^3=0$$

ですから無数の解を持ちます．よって，$\sigma_2=\sigma_3=0$ に取ります．すると誤り位置多項式は

$$E(x)=x^3+ux^2=x^2(x+u)$$

となります．$E(x)=0$ の解は $x=0$ と $x=u$ です．従って，$x=u=\alpha^p$ を $E(x)$ に代入したときだけ $E(x)$ は 0 になります．よって，1 ヶ所の誤り判定ができます．　□

Example 20. (誤りが 2 ヶ所の場合)
誤りが 2 ヶ所あるデータ

$$\boldsymbol{y}=r_{14}r_{13}r_{12}r_{11}r_{10}r_9r_8r_7r_6r_5r_4r_3r_2r_1r_0$$

が与えられたとします．p 次と q 次の項だけ誤りがあったとします．

$$Y(x)=Y_0(x)+x^p+x^q$$

でから，$Y(\alpha)=\alpha^p+\alpha^q=u+v$ です．誤りが 3 ヶ所あるときの $w=0$ の場合になっています．従って，シンドロームは

$$S_1=u+v,\ S_2=u^2+v^2,\ S_3=u^3+v^3,\ S_4=u^4+v^4,\ S_5=u^5+v^5$$

となります．$\sigma_1=S_1=u+v$ です．連立 1 次方程式

$$(2)\begin{cases} S_1+\sigma_1 & = & 0 & \cdots(\mathrm{i}) \\ S_3+S_2\sigma_1+S_1\sigma_2+\sigma_3 & = & 0 & \cdots(\mathrm{ii}) \\ S_5+S_4\sigma_1+S_3\sigma_2+S_2\sigma_3 & = & 0 & \cdots(\mathrm{iii}) \end{cases}$$

において，$\sigma_3=0$ であることを示します．

$$S_3+S_2S_1=u^3+v^3+(u^2+v^2)(u+v)=uv(u+v)=uvS_1$$

$$S_5+S_4S_1=u^5+v^5+(u^4+v^4)(u+v)=uv(u^3+v^3)=uvS_3$$

ですから，(2)-(ii) を S_3 倍，(2)-(iii) ををを S_1 倍して加えると

$$(S_3 + S_2S_1)\sigma_3 = 0$$

となります．Lemma 3 より，$S_3 + S_2S_1 = (u+v)(v+w)(w+u)$．今の場合 $w = 0$ ですから，$S_3 + S_2S_1 = uv(u+v) \neq 0$ を得ます．従って，$\sigma_3 = 0$ です．σ_2 は連立 1 次方程式 (2)-(ii) から求めます．$S_1 = u + v \neq 0$ であり，$S_3 + S_2S_1 = uvS_1$ ですから，$\sigma_2 = uv$ を得ます．従って，誤り位置多項式は

$$E(x) = x^3 + (u+v)x^2 + uvx = x(x+u)(x+v)$$

となります．$E(x) = 0$ の解は $x = 0, u, v$ です．従って，2 ヶ所の誤り判定ができます． □

5 付録

5.1 体の定義

Definition 3. (体，Field, Körper)

集合 F がある．任意の $x, y \in F$ に対してその和 $x + y \in F$ と積 $x \cdot y \in F$ が定義されていて，次の (1)〜(9) をみたすとき，F を体 (たい) という．$x, y, z \in F$ とする．

(1) $(x + y) + z = x + (y + z)$ (加法の結合法則)

(2) $x + y = y + x$ (加法の交換法則)

(3) $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ (乗法の結合法則)

(4) $x \cdot y = y \cdot x$ (乗法の交換法則)

(5) $x \cdot (y + z) = x \cdot y + x \cdot z$ (分配法則)

(6) $x + 0 = x$ (for 任意の $x \in F$) となる $0 \in F$ が存在する．(加法の単位元)

(7) 任意の $x \in F$ に対して，$x + (-x) = 0$ となる $-x \in F$ が存在する．(加法の逆元)

(8) $1 \cdot x = x$ (for 任意の $x \in F$) となる $1 \in F$ が存在する．(乗法の単位元)

(9) 任意の $x \in F$，$x \neq 0$ に対して，$x \cdot x^{-1} = 1$ となる $x^{-1} \in F$ が存在する．
(乗法の逆元)