入学年度	学部	学 科	組	番 号	検	フリガナ	
						氏 名	

BCH 符号とは，誤り訂正符号の一種で，実際に衛星通信や移動通信に用いられる実用性の高い符号である． BCH 符号では情報のブロックの長さや誤り訂正能力を目的に応じてカスタマイズできる．

数学的には， BCH 符号では 0 と 1 の並びであるデータを $GF(2) = \mathbf{F}_2 = \{0, 1\}$ を係数とする多項式と捉え，それを送受信すると考える． $GF(2^q)$ を用いる BCH 符号では， $(2^q - 1)$bit の情報を $(2^q - 2)$ 次多項式と捉え，その中に送りたいデータ（情報語という）と誤り訂正用のデータ（検査語という）を詰め込んで，それを送受信する．

受信したデータの誤りを訂正して必要な情報を取り出すこと（復号という）は「シンドローム」と呼ばれる値の組を計算することによって行われる．シンドロームがすべて零ならば誤りなしと判定し，非零のときは，シンドロームから誤り位置を同定し，それを訂正する．

QR コードの中にも BCH 符号が一部使われており， 5 bit の情報を間違いなく送るために 10 bit の検査 bit を加えて 15 bit とし， 3 つまでの誤りを訂正出来るようにしたものである．このため， 16 個の元を持つ数の体系 $GF(2^4) = \mathbf{F}_{16}$ を用いる．

ここでは最も簡単な場合である， $GF(2^3) = \mathbf{F}_8$ を用い，誤り訂正能力が 1 である BCH 符号について，具体例を用いて詳しく見ることにする．

$GF(2^3) = \mathbf{F}_8$ は $GF(2) = \mathbf{F}_2$ に $\alpha^3 + \alpha + 1 = 0$ をみたす数 α を加えて得られる数の体系であった． $GF(2^3)$ の元はすべて α の 2 次以下の多項式として表され（加法表示）， 0 を除く 7 個の元は α^k $(0 \leq k \leq 6)$ と表せる（乗法表示）のであった．まず，加法表示と乗法表示の間の対応を思い出しておく．

$\alpha^0 =$　　$\alpha^4 =$

$\alpha^1 =$　　$\alpha^5 =$

$\alpha^2 =$　　$\alpha^6 =$

$\alpha^3 =$　　$\alpha^7 =$

BCH 符号では 0 と 1 の列であるデータを多項式として扱う．例えば， 1011011 という 7 bit のデータは，左端が最高次 6 次の係数，右端が定数項として，

$$\begin{aligned} 1011011 \quad &\longmapsto \quad 1 \cdot x^6 + 0 \cdot x^5 + 1 \cdot x^4 + 1 \cdot x^3 + 0 \cdot x^2 + 1 \cdot x + 1 \\ &= x^6 + x^4 + x^3 + x + 1 \end{aligned}$$

というように 6 次の多項式で表される．

問. 01100101 を多項式として表せ．

ここでは， 1 つの誤りが訂正可能な $(7, 4)$ 型と呼ばれる BCH 符号を見てみる． $(7, 4)$ の 7 は送受信の bit 数， 4 は情報語の bit 数を表している． BCH 符号で重要になるのは「生成多項式」と呼ばれる多項式で，この場合は $g(x) = x^3 + x + 1$ とする．すぐにわかるのは， $g(\alpha) = \alpha^3 + \alpha + 1 = 0$ となることである．

情報語は次の手順によって送信される．

1. 送りたい 4bit の情報語を 3 次の情報多項式 $q(x)$ に変換する．
2. 生成多項式 $g(x)$ を用いて，送信多項式 $u(x)$ を次のように作る．

$$u(x) = q(x)x^3 + \big(q(x)x^3 \text{ を } g(x) \text{ で割った余り}\big)$$

こうして作られた $u(x)$ は $g(x)$ で割り切れる．なぜなら， $u(x)$ を $g(x)$ で割ると余りは $\big(q(x)x^3$ を $g(x)$ で割った余り $\big)$ の 2 倍になるが， $2 = 0$ なので余りは 0 となるからである．したがって， $u(x) = g(x)m(x)$ の形に書ける．これより， $u(\alpha) = g(\alpha)m(\alpha) = 0 \cdot m(\alpha) = 0$ となることがわかる．

1 情報語 1101 を送信したい．

a) 1101 を情報多項式 $q(x)$ に直せ．

$q(x) =$

b) $q(x)x^3$ を $g(x)$ で割った余りを求めよ．

$q(x)x^3$ を $g(x)$ で割った余り $=$

c) これより送信多項式 $u(x)$ を作れ．

$u(x) =$

d) 送信多項式を 0, 1 の列に直した送信語を求めよ．

送信語 $=$

さて，送信語が通信経路を通って受信されたとき，まずそのデータ（受信語）を受信多項式 $r(x)$ に変換する．通信経路で誤りが起こったとするとそれは $r(x)$ と $u(x)$ の差に他ならない．そこで，

$$r(x) = u(x) + e(x)$$

と置く．この $e(x)$ は誤差多項式と呼ばれる．

さて，ここで，送信語と受信語は高々 1bit しか相違していないと仮定する．すると，

$$e(x) = 0 \quad \text{または} \quad e(x) = x^k$$

という形をしている．

【裏に続く】

いま，送信多項式 $u(x)$ に α を代入すると $u(\alpha)=0$ となるのであったから，受信多項式 $r(x)$ に α を代入すると

$$r(\alpha)=u(\alpha)+e(\alpha)=0+e(\alpha)=e(\alpha)=0 \text{ または } \alpha^k$$

が成り立つ．これより，$r(\alpha)$ を計算することにより誤りがあるかないかが判定できるので，$r(\alpha)$ を「シンドローム」と呼び，s で表す．

シンドローム $s=e(\alpha)$ は，0 または α^k に等しく，

- $s=0$ なら誤りなし，
- $s\neq 0$ なら，s を情報表示し $s=\alpha^k$ の形にすると，$r(x)$ と $u(x)$ は k 次の項が異なることを示す．すなわち，受信語の右から $k+1$ 番目の bit に誤りがあったことがわかる．

2 いま，$(7,4)$ 型の BCH 符号で 1011011 という語を受信したとする．誤りは高々 1 個であるという仮定の下に送信語を求めたい．

a) 受信多項式 $r(x)$ を求めよ．

$r(x)=$

b) シンドローム $s=r(\alpha)$ を計算せよ．

$s=$

c) シンドローム s を $s=\alpha^k$ の形に表し，誤り位置を求めよ．（最初に求めた，加法表示と乗法表示の対照表を利用するとよい．）

d) 情報語を求めよ．

3 $(7,4)$ 型の BCH 符号で 01010010 という語を受信したとする．誤りは高々 1 個であるという仮定の下に情報語を求めよ．

担当：鍬田 政人 (kuwata.04f@g.chuo-u.ac.jp)