連載第3回

数値計算ソフトウェアを用いたアルゴリズム検証

ハミング符号の符号化，復号化の検証

河原崎浩也

CD-ROM 設計データ

光ディスクや，情報通信系の信頼性を高める手段として誤り訂正技術が一般化しています．誤り訂正符号の一つの形式に代数符号があり，代数学のガロア体の理論をもとに構成されています．今回は，それらの理論とともに，もっとも単純なエラー訂正符号であるハミング符号の符号化，復号化のアルゴリズム検証の例を紹介します．

ガロア体

最初に符号理論の基礎をなす「ガロア体理論（Galois Field あるいは有限体：Finite Field）」の入り口を説明します．

ある集合において，加法と乗法の2項演算が定義されていて，その演算について結合則，分配則，交換則が成り立ち，逆元，単位元が存在して代数的に閉じているとき，この集合が**体**（field）をなしているといいます．このときの加法，乗法は普通の算術演算とは限らず，体の条件をみたす演算を加法，乗法と定義します．

体とは，このように順序演算の規則に従って構築された代数的構造です．同様な代数構造に，群，環があります．群（group）は加法のみ定義されて演算が閉じているものです．数学的に重要な体の例として，実数体，複素数体，剰余体，位相体などがあります．体の元の数が有限のとき**ガロア体**といい，記号“GF”で表し符号理論の中心概念となっています．

●剰余体

整数a，bが，ある正の整数$p>1$について$a-b$がpで割り切れるとき，つまり，pで割った剰余が等しいとき，a，bはpを法として合同であるといいます．pについて合同な整数の集合を法mについての**剰余類**といいます．剰余類の集合はp個あり，pが素数であれば体をなしていて，これを**剰余体**といいます．

ここでは，$a<p$である，0，1，2，…，$p-1$までの部分体を問題にします．剰余体の加法と乗法は，算術演算◎の結果に対してある整数pを法とする剰余，

$$z=(x◎y) \bmod p$$

により定義されています．pを体の標数といいます．例として$p=5$とした素体（後述）の加法，乗法の演算表を**表1**に示します．標数pは，かならず素数でなければならず，非素数の場合は乗法の逆元が存在しない場合がでてきます．

さて，符号理論で重要なのは標数$p=2$の体{0,1}です．演算表を**表2**に示します．p=2の体について次のことがいえます．

(1) 加法逆元は自分自身に等しい．したがって，加法と減法は等しい．
(2) 非零の元1に対する乗法逆元は，1自身．
(3) 加法演算は，排他的論理和（EXOR）になっている．
(4) 乗法演算は，論理積（AND）になっている．

〔表1〕加法と乗法の演算表（$p=5$）

(a) 加法　p＝5

＋	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

(b) 乗法　p＝5

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

●拡大体（Extension Field）

前述の，GF(2)，GF(5)のように整数を素数で剰余類展開してつくられた体を**素体**といい，もっとも基本的な有限体です．素体の元{0,1}を係数とする多項式を考えることができ，有限体上の任意の次数までの多項式を元とする体を作ることができます．この体は，元の素体を含んでおり，**拡大体**と呼ばれます．

拡大体は，次数$m-1$を超えない次数のGF(p)上の多項式のすべてをその元として持ちます．多項式の最大次数＋1＝mを拡大次数といいます．多項式の変数xは不定元とよばれ，形式的な変数であり，数値を代表するものではありません．

拡大体は，体である以上，加法，乗法について閉じている必要があります．拡大体の元の演算関係は，素体の演算をもとにして定義されます．以下，GF(2)の例を中心に説明します．

加法は，xについての同じ次数の項どうしを加算（EXOR）します（GF(2)の性質により，加法と減法は同じ）．GF(2)でなくても，各次数の係数を素体の標数pによる剰余とすれば，同様

〔表2〕加法と乗法の演算表（$p=2$）

(a) 加法　p＝2

＋	0	1
0	0	1
1	1	0

(b) 乗法　p＝2

×	0	1
0	0	0
1	0	1

に加算が定義できます.

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

乗法は，既約多項式というものを導入し，これを標数pのかわりに，算術上の積の既約多項式による剰余を求めることを乗法とします．つまり，既約多項式による剰余体です．ここで，**既約多項式**とは，ある拡大次数までの多項式のなかで，1次以上の多項式で因数分解できないものをいいます．もちろん，複素数体上ではすべての多項式は因数分解できますが，ここでは，問題となっている有限体上の多項式を考えます.

既約多項式は同次数のものが複数存在します．代数符号系では乗法を定義する既約多項式を，式の周期がp^m-1となるように選び，これを**原始既約多項式**といいます(pは標数，mは拡大次数).

積＝(式1×式2)mod(原始既約多項式)

除法については，乗法の逆演算なので体の定義から逆元の存在が保証されています．拡大体の演算の例として，GF(2^2)の演算表を**表3**に示します.

●符号多項式と生成多項式

既約多項式は，素体の標数の拡張であり，標数および，既約多項式が有限体の構造を決定します.

符号理論では，符号語のビット列を，有限体上の多項式の係数に対応させて，**符号多項式**というものを考えます．巡回符号では，符号多項式は生成多項式の多項式倍になるという性質があります．**生成多項式**は体の原始既約多項式であり，パリティ・ビットがmビットの**ハミング符号**では，生成多項式はm次で，周期2^m-1をもつものが選ばれます．すべての符号多項式は生成多項式を因数としてもち，代数学の基本定理から，生成多項式の根(変数xに代入すると式がゼロになる数)は同時にすべての符号多項式の根でもあります.

原始既約多項式は，有限体上で既約であることから，体上に根をもちません．しかし，仮想的に根が存在するとすれば，この根は体の原始元であり，これをαとすると，拡大体の元はすべて，αを根としてもち，かつ，αのべき乗順に巡回的に並べることができます．このことを，体がαによって生成されるといいます.

この仮想的な数αは，拡大前の体には存在しない数なので，αを体の他の元の1次結合によって合成することはできません．既約多項式によって演算を定義して体を拡大することは，体の要素にαを添加して拡大することであり，この過程は，実数体に虚数記号iを添加して複素数体を得る過程とよく似ています．ちなみに，虚数記号iは実数体上既約な多項式x^2+1の根です．このような既約多項式の根の添加による体の拡大を**ガロア拡大**といいます.

さて，巡回符号では有限体の元をαのべき乗順に並べてマトリックスを作り，これと情報語を内積演算してパリティ・ビットを生成します．有限体および符号系の演算は定義から明らかに線形演算であり，符号系を線形ベクトル空間と考えて，線形代数学のベクトル空間上の諸定理がほとんどそのまま成り立ちます.

〔表3〕GF(2^2)の演算表

(a) 加算表

+	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	2	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

(b) 乗算表

×	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

線形代数的に考えると，パリティ・ビットは，情報語を変数，有限体を係数とした1次結合となっていることがわかります．符号語は情報語とパリティ・ビット合わせたものであり，符号語は有限体の生成系をベクトル基底として構成されていることになります.

●有限体の基本的性質

素体と拡大体の定義から数学的に導かれる有限体の性質のなかで，基本的かつ符号理論に関係の深いものをあげます.

(1) 拡大体は素体を必ず含み，その位数は，標数pに対してp^nである．ここに，nは拡大次数．体の位数とは，体の元の数をいう.

(2) 同じ位数を持つ二つの有限体は同型である．同型とは，それぞれの体の要素に1対1の対応がつけられ，その演算関係も互いにうつりあうことをいう.

(3) 任意の有限体において，0を除く体の要素からなる乗法群の原始元αが存在する．原始元とは，原始既約多項式の仮想的な根であり，体の標数をpとすると，

$\alpha^0=1,\ \alpha^1=x,\ \cdots,\ \alpha^{p-2}=1+x+x^2,\ \alpha^{p-1}=1$

のように0を除く体の要素をαのべき乗として巡回的に発生させられる数である.

(4) 任意の有限体上で，標数をpとして以下の式が成り立つ.

$(x+y)^p=x^p+y^p$

この式は有限体上の多項式の展開，因数分解によく使用される.

ハミング符号系の構成

ハミング符号は，もっとも単純な誤り訂正符号です．ブロック符号の一種であり，1個の符号語は，もとの情報語にいくつかのパリティ・ビットを付加してつくられます．ハミング符号は，以下の性質があります.

(1) 符号語同士で加算および定数倍の演算を行うと，結果も符号語になる(線形性)

(2) 一つの符号語は(2^{n-1})符号語ビット，情報語(2^n-n-1)ビットで構成される.

(3) 一つの符号語のなかで，1ビットのエラー訂正能力をもつ.