第9章

誤り訂正

無線でのデータ伝送では，誤り訂正の技術が不可欠です．誤り訂正技術がなければ，今日の通信のディジタル化は難しかったでしょう．もっとも簡単なハミング符号から，最近のターボ符号までさまざまな方法が使われています．ここではすべてを説明することはできません．詳しく説明すると誤り訂正だけで1冊の本になってしまうので，ここではその中の一つを代表として説明します．もっと詳しく基礎から勉強したい方は参考文献(59)を読んでください．

先に勉強したガロア体の代数を使うブロック符号のBCH符号について説明します．BCH符号は，現在使われているブロック符号にもっとも多く使われているアルゴリズムです．その中には，ハミング符号や，リード・ソロモン符号も含まれます．これを理解できれば実際の応用も広がるでしょう．ただし，第2章など前のほうで説明したガロア体の代数に関して理解していないと，なかなか理解できないかもしれません．残念ながら，数学的計算抜きには理解できません．

ここで取り上げるBCH符号の誤り訂正方法は，ピーターソン法を使って説明します．そのほかももっと実践的に使われるバレカンプ・マーシー法(BM法)などもありますが，紙面の関係で説明を参考文献(59)に譲ることにします．

9-1　BCH符号

ハミング符号は，符号語間のハミング距離3で誤り訂正が1個しかできません．それでも，そもそもの開発目的のコンピュータ・メモリの信頼性向上には充分ですが，そのほかのたとえば信頼性が低い無線伝送路などの応用では，回線の誤り率に対して誤り訂正能力が充分ではありません．そこで，複数の誤りも訂正できるように考えられた符号の一つにBCH符号があります．

この符号は1959年にHocquenghemによって，また1960年にBoseとChaudhuriによってそれぞれ独立に発見されたものです．それぞれの頭文字をとってBCH符号と呼ばれています．ハミング符号もBCH符号の一種だと考えることができます．BCH符号も大きく分けて，符号語の多項式の係数が2元すなわち$GF(2)$の場合と，ガロア拡大体$GF(2^M)$の場合があります．実際に使われるほとんどの巡

回ブロック符号はBCH符号の一種で，とても応用の幅が広い符号です．ここでは，その中のデータが1/0のみで構成される2元BCH符号について説明します．拡大体の多元BCH符号は，発見者にちなんでリード・ソロモン符号と呼ばれています．

BCH符号は純粋に，数学を使って展開された符号なので，数式を使った説明なしには残念ながら理解はできません．ただし最終的に得られた結果は，直感的に理解できるものです．ある程度式を理解した後，具体例をじっくり理解することにより，確かな直感とイメージがつかめると思います．

9-2　t個の誤りを訂正するBCH符号

ブロック符号の特徴として，生成された符号$F(X)$は必ず生成多項式$G(X)$で割り切れます．この際に計算は，その符号が定義されたガロア拡大体$GF(2^M)$上で行われます．すなわち，受信側でこの符号を受信し$G(X)$で割ったときに完全に割り切れれば，誤りがなかったことがわかります．

伝送路上で，誤りが発生した場合は，ゼロになりません．この受信符号を$G(X)$で割った余りをシンドロームと呼んでいます．誤り訂正では，このシンドロームを使って計算し誤りの訂正を行います．シンドロームは符号を作る前の情報ビット列の組み合わせにはまったく影響を受けません．ただ伝送路での誤りのパターンのみで一意に決まります．この生成多項式の性質によって，どれくらいの誤り訂正能力があるかがわかります．

BCH符号の一種であるハミング符号は，1個の誤りを訂正できる能力があります．これを一般化したt個の誤りを訂正するBCH符号は，どのような生成多項式をしているのでしょうか．

$$G(X)=(X+\alpha)(X+\alpha^2)(X+\alpha^3)\cdots(X+\alpha^{2t})F(X) \quad \cdots\cdots (9\text{-}1)$$

一般的に$GF(2^M)$上の原始元をαとするとき，上式を符号生成多項式とするものをBCH符号と呼んでいます．$G(X)=0$は式のように，αから連続した，α^{2t}までのαのベキ乗を根にもちます．$GF(2^4)$のハミング符号では，

$$G(X)=X^4+X+1=(X+\alpha)(X+\alpha^2)F(X) \qquad \text{ただし，} F(X)=(X+\alpha^4)(X+\alpha^8) \quad \cdots\cdots (9\text{-}2)$$

$2t=2$ですから，1個の誤りを訂正可能なBCH符号といえます．2個の誤りを訂正できるBCH符号では，

$$\begin{aligned} G(X)&=(X^4+X+1)(X^4+X^3+X^2+X+1)\\ &=(X+\alpha)(X+\alpha^2)(X+\alpha^3)(X+\alpha^4)F(X) \qquad \cdots\cdots (9\text{-}3)\\ &\text{ただし}\quad F(X)=(X+\alpha^6)(X+\alpha^8)(X+\alpha^{12})(X+\alpha^9) \end{aligned}$$

です．$2t=4$として，4個の$G(X)=0$の根がαのべき乗として連続していることがわかると思います．しかしここで注意することは，2元符号の多項式係数としてαのままでは具体的にシフト・レジスタなどを実現できません．そこで，BCH生成多項式として直接必要のない共役根を含め，生成多項式のすべての係数にαが現れないようにしなければなりません．そのため$F(X)$の項が必要になります．これはむだに生成多項式の次数を大きくすることです．できるだけ$F(X)$の次数を小さく設計したものが効率の良い符号となります．

すなわち1個の誤り訂正には，αを根にもつ最小多項式（共役根をもち係数にαを含まない最小次数

多項式），2個の場合はαとα^3，3個の場合はα，α^3，α^5をそれぞれ根にもつ最小多項式の積になります．このように共役関係にない根を，生成多項式に新たに加えることによって，誤りを訂正できる数が増えていきます．

具体的に$GF(2^4)$の場合の根と最小多項式の関係を下に書き直します．

$$\left.\begin{aligned}
&\alpha \rightarrow X^4+X+1\\
&\alpha^3 \rightarrow X^4+X^3+X^2+X+1\\
&\alpha^5 \rightarrow X^2+X+1\\
&\alpha^7 \rightarrow X^4+X^3+1
\end{aligned}\right\} \quad \cdots\cdots (9\text{-}4)$$

そこで，これらを使っていろいろな生成多項式を計算します．

$$\left.\begin{aligned}
&\text{1個エラー} \quad G(X)=(X+\alpha)(X+\alpha^2)F(X)\\
&\qquad\qquad =X^4+X+1\\
&\text{2個エラー} \quad G(X)=(X+\alpha)(X+\alpha^2)(X+\alpha^3)(X+\alpha^4)F(X)\\
&\qquad\qquad =(X^4+X+1)(X^4+X^3+X^2+X+1)\\
&\qquad\qquad =X^8+X^7+X^6+X^4+1\\
&\text{3個エラー} \quad G(X)=(X+\alpha)(X+\alpha^2)(X+\alpha^3)(X+\alpha^4)(X+\alpha^5)(X+\alpha^6)F(X)\\
&\qquad\qquad =(X^4+X+1)(X^4+X^3+X^2+X+1)(X^2+X+1)\\
&\qquad\qquad =(X^8+X^7+X^6+X^4+1)(X^2+X+1)\\
&\qquad\qquad =X^{10}+X^8+X^5+X^4+X^2+X+1
\end{aligned}\right\} \quad \cdots\cdots (9\text{-}5)$$

ここでは$GF(2^4)$の話でした．そのほかのガロア拡大体に対しても，最少多項式が決まり，その組み合わせで同じ方法でBCH符号の生成多項式が求められます．

9-3　BCH符号の復号

抽象的な話ではなかなかわかりにくいので，具体的な例題を使って説明します．$GF(2^4)$における(15, 5)のBCH符号を使って話を進めます．

● シンドロームの計算

まずはシンドロームの計算をします．ここでは，もっと具体的に説明していきます．

(15, 5)のBCH符号の生成多項式は，

$$\left.\begin{aligned}
&\text{3個エラー} \quad G(X)=(X+\alpha)(X+\alpha^2)(X+\alpha^3)(X+\alpha^4)(X+\alpha^5)(X+\alpha^6)F(X)\\
&\qquad\qquad =(X^4+X+1)(X^4+X^3+X^2+X+1)(X^2+X+1)\\
&\qquad\qquad =(X^8+X^7+X^6+X^4+1)(X^2+X+1)\\
&\qquad\qquad =X^{10}+X^8+X^5+X^4+X^2+X+1
\end{aligned}\right\} \quad \cdots\cdots (9\text{-}6)$$

でした．符号語は$G(X)$で割り切れるはずです．したがって，下記のように表せます．

$$R(X)=I(X)\,G(X) \quad \cdots\cdots (9\text{-}7)$$

そのため$R(X)$は$G(X)=0$と同じ根をもつことは明らかです．そこで，