ハミング符号と多項式

原田　剛

1　はじめに

現代社会において通信の安定性は極めて重要な問題である．例えば，ある場所から離れた場所に花の画像を送ろうとした場合，花の画像を小さな部分の集まりと考えて，それぞれの部分の位置，色，明るさ等を決まった方法で数値に置き換えて，その数値を記号列とみなして送る．その記号列を受信して元の情報に復元することができれば，花の画像を見ることができる．このようにある情報を決まった方法で数値に変換することを符号化といい，その数値を記号列とみなしたもの全体を符号といい，符号の元を符号語という．技術の進歩と共に情報を記憶する媒体も紙に書かれた表からブルーレイディスク等に進化していき，記憶する媒体に合わせて符号も進化してきた．

ひとことに符号と言ってもさまざまな符号がある．通信の正確さを高めようと考えた時，記号列の長さを長くすれば良いが，通信そのものに時間がかかってしまう．そこで，どのくらい状態の悪い通信路を用いて，どのような種類の情報をやり取りするかで，適切な符号を選ぶ必要がある．情報を送ろうとするとき，通信経路内で雑音（人の手によるミス，落雷，導線の熱膨張等）を拾うことがある．即ち，通信の状態の良くない通信路において情報を送った時，情報をそのままの形で送られるとは限らない．そこで，余分な情報を送りたい情報に加えることで，限られた範囲の誤りが起きてもそれを訂正して正しい情報を受信したり，誤りが生じていることを伝えたりするのが，誤り訂正符号である．

また，送られてきた情報は雑音の影響を受けているので，記号列に誤り訂正を施さなければ，もとの情報を取り出すことができない．そこで，記号列の長さ，誤り訂正をするための情報量が第 2 節で説明するハミング限界式の等号を満たすような符号を用いることが考えられる．このように理想的状態の符号を完全符号という．その完全符号の一つにハミング符号がある．

符号が q 個の元を持つ有限体 F 上のベクトル空間の部分空間である場合，即ち線形符号を考える．符号語の成分を一つずらしても再び符号語となる線形符号を巡回符号という．この符号の性質は多項式環 $F[x]$ をイデアル (x^n-1) で割った剰余環 $F[x]/(x^n-1)$ を用いて考えることができ，符号語を剰余環 $F[x]/(x^n-1)$ の元とみなすことができる．$q=2$ の時，原始多項式の理論を用いることにより，巡回符号の枠組みの中でハミング符号を考えること（定理 4.15）ができる．

符号を $F[x]$ の $n-1$ 次以下の多項式の成すベクトル空間の部分空間としても考えることができる．原始多項式を用いることにより，多項式の成す符号においてもハミング符号を生成することができる．

この論文では，符号を第 4 節においては剰余環 $F[x]/(x^n-1)$ の部分空間として，第 5 節においては $F[x]$ の $n-1$ 次以下の多項式の成すベクトル空間の部分空間として考える．$q=2$ に対して，異なる符号の作り方をしても原始多項式を用いることにより，同じハミング符号を作ることができること（定理 4.17 と系

5.8）を紹介することがこの論文の目的の一つである．この論文においてのもう一つの目的は，F 上の既約多項式から F 上のハミング符号を構成するための必要十分条件（定理 5.9）を紹介し，実際に既約多項式からハミング符号を構成すること（例 5.12）である．上述の定理（定理 5.9）は A. S. Barashko [5] の仕事である．

以下，この論文の構成を簡単に説明する．第 2 節において符号の一般論（ハミング限界式，完全符号，線形符号，符号の同値関係）を紹介し，第 3 節においては，ハミング符号の作り方を紹介する．具体的には，有限体上のベクトル空間をスカラー倍の作用により軌道分解を行い，各軌道の代表元から符号の検査行列を構成する．この検査行列からハミング符号を作る．第 4 節において巡回符号の作り方とその性質を説明する．具体的には，巡回符号を多項式環の性質を用いて構成し，有限体 F_2 上のハミング符号との関係を論じる．第 5 節においては，A. S. Barashko [5] の仕事である有限体 F 上のハミング符号と原始多項式との関係を述べる．

第 2 節は 2007 年度後期，2008 年度前期に開かれた桂利行先生，川北素子先生による集中講義を参考にした．第 3，4 節は R. Hill [2] のハミング符号，巡回符号の解説を参考にし，第 5 節では A. S. Barashko [5] の論文に基づいてハミング符号と多項式との関係を解説した．ハミング符号 · 巡回符号と多項式との関係は様々な論文，テキストなどで紹介されており，特に J. H. van Lint [3] と F. J. MacWilliams and N. J. A. Sloane [4] は論文を書く上で参考にした．また，符号理論での専門用語の日本語訳は内田興二 [1] を参考にした．

2　符号理論入門

情報を数値化して，通信路を通して伝えやすい記号列にすることを符号化，符号化されたものを符号語という．送られてきた符号語を受信ベクトルという．但し，通信路に雑音が入るため受信ベクトルは必ずしも符号語とは限らない．受信ベクトルを誤り訂正した符号にすることを復号化，復号化されたものを復号語という．

情報のやり取りを図示すると以下のようにして表すことができる．

$$\text{送信情報} \xrightarrow{\text{符号化}} \text{符号語} \xrightarrow[\uparrow]{\text{通信}} \text{受信ベクトル} \xrightarrow{\text{復号化}} \text{復号語} \longrightarrow \text{受信情報}$$
$$\text{雑音}$$

2.1　符号理論入門

$X = \{\lambda_1, \ldots, \lambda_q\}$ を q 個の元を持つ集合とする．直積 X^n の元を括弧などを用いずに羅列して $x = x_1 \ldots x_n$ と書くことにする．

定義 2.1. 有限集合 X^n の部分集合 C を長さ n の q 元符号という．符号 C の元を符号語という．

定義 2.2. X^n 上に関数 d を

$$d : X^n \times X^n \to \mathbb{N},$$

$$d(x,y) = \#\{i \ ; \ x_i \neq y_i \ (1 \leq i \leq n)\}, \quad x = x_1 \dots x_n, \ y = y_1 \dots y_n \in X^n$$

のように定める．但し，$\mathbb{N} = \{$ 零以上の整数 $\}$ とする．関数 d は距離の公理を満たす．この距離をハミング距離という．

定義 2.3. 符号 C に対して最小距離 $d(C)$ を

$$d(C) = \min\{d(x,y) \ ; \ x, y \in C, x \neq y\}$$

で定める．

定義 2.4. 符号 C の長さが n であり，符号語の総数が $M = \#C$, 最小距離が $d(C) = d$ である時 C を (n, M, d) 符号という．

定理 2.5. 符号 C に対して最小距離 $d(C) = d$ が不等式 $d \geq 2t+1$ を満たせば，どの符号語も t 個までの誤りを訂正することができる．つまり，x を符号語 y を受信ベクトルとする時 $d(x,y) \leq t$ ならば $d(x',y) \leq t$ となる符号語 x' は他にないので y から x を復号化できる．

任意の $u \in X^n$ と整数 $r \geq 0$ に対して半径 r 中心 u の球 $S(u,r)$ を

$$S(u,r) = \{v \in X^n \ ; \ d(u,v) \leq r\}$$

で定める．

定理 2.6. q 元 $(n, M, 2t+1)$ 符号に対して不等式

$$M \left\{ \binom{n}{0} + \binom{n}{1}(q-1) + \cdots + \binom{n}{t}(q-1)^t \right\} \leq q^n \tag{2.1}$$

が成り立つ．但し，$\binom{n}{m}$ は二項係数である．

この不等式 (2.1) をハミング限界式という．

定義 2.7. ハミング限界式において等号が成立する符号を完全符号という．

符号 C が q 元 $(n, M, 2t+1)$ 完全符号であることと

$$\bigsqcup_{x \in C} S(x,t) = X^n$$

が成り立つことは同値である．これを言い換えると任意の $y \in X^n$ に対して $d(x,y) \leq t$ となる $x \in C$ が一意的に存在することを意味している．

2.2 線形符号入門１

素数のベキ $q \geq 2$ を取り，q 個の元を持つ有限体を F とする．元の個数を強調するために F_q と書くこともある．有限体 F 上の n 次元行ベクトル全体の空間を $F^n = \{(x_1, \ldots, x_n)\ ;\ x_i \in F\}$ で表し，ベクトル空間 F^n の元 $(x_1, \ldots, x_n)$ を $x_1 \ldots x_n$ で表す．

定義 2.8. ベクトル空間 F^n の部分空間を有限体 F 上の線形符号 C という．線形符号 C が F^n の k 次元部分空間である時，C を $[n, k]$ 符号といい，最小距離 $d(C) = d$ の時 C を $[n, k, d]$ 符号という．

注意 2.9. 線形符号には $0 = 0 \ldots 0$ が自動的に含まれている．

線形符号 C を $[n, k]$ 符号とし，C の基底を $v_1, \ldots, v_k$ とする．符号語 x は $x = a_1 v_1 + \cdots + a_k v_k \quad (a_i \in F,\ 1 \leq i \leq k)$ と一意的に表すことができる．

注意 2.10. 線形符号 C が q 元 $[n, k, d]$ 符号ならば C は q 元 (n, q^k, d) 符号である．

定義 2.11. ベクトル空間 F^n の元 $x = x_1 \ldots x_n$ の重み $w(x)$ を

$$w(x) = \#\{i\ ;\ x_i \neq 0\}$$

で定める．符号 C に対して C の最小重み $w(C)$ を

$$w(C) = \min\{w(x)\ ;\ x \in C\}$$

で定める．

命題 2.12. 線形符号 C に対して $d(C) = w(C)$ となる．

定義 2.13. 線形符号 C を $[n, k]$ 符号とする．符号 C の基底 $v_1, \ldots, v_k$ を並べた行列 $G \in M(k, n : F)$

$$G = \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_k \end{pmatrix}$$

を C の生成行列という．v_i は行ベクトルであった．

2.3 線形符号の同値関係

符号は線形符号を扱い，$k \leq n$ とする．

定義 2.14. 二つの線形符号 C_1, C_2 が同値であるとは以下の (1), (2) の操作により C_1 から C_2 を得ることができることである．

(1) 成分の並べ換え．

(2) ある固定した成分に零でない定数倍を施す．

定理 2.15. 二つの階数 k の行列 $G_1, G_2 \in M(k, n : F)$ に対して G_1 が次の操作 (R1) から (R3) の行基本変形と (C1) から (C2) の列基本変形を施すことで G_2 になる時，G_1, G_2 により生成された符号 C_1, C_2 は F 上の同値な $[n, k]$ 符号である．

(R1) 行ベクトルの入れ換え．

(R2) 零でないスカラー倍を行ベクトルに施す．

(R3) ある行ベクトルに他の行ベクトルの定数倍を加える．

(C1) 列ベクトルの入れ換え．

(C2) 零でないスカラー倍を列ベクトルに施す．

定理 2.16. $[n, k]$ 符号の生成行列 G を定理 2.15 の操作で $[I_k, A]$ の形に変形することができる．但し，I_k は k 次単位行列，$A \in M(k, n-k : F)$ である．

定義 2.17. $[n, k]$ 符号の生成行列 G を定理 2.15 の操作で変形した行列 $[I_k, A]$ を G の標準形という．

注意 2.18. 生成行列 G を行基本変形 (R1) から (R3) のみで標準形 G' に変形した場合，G' は G と同一の符号を生成する．

注意 2.19. 生成行列の標準形は必ずしも一意的ではない．

2.4 線形符号入門２

ベクトル空間 F^n に内積 $*$ を

$$u * v = u_1 v_1 + \cdots + u_n v_n \quad (u = u_1 \ldots u_n,\ v = v_1 \ldots v_n \in F^n)$$

で定める．$u * v = 0$ となる時 u, v は直交するという．

定義 2.20. 符号 C を $[n, k]$ 符号とする．符号 C の双対符号 $C^\perp$ を

$$C^\perp = \{v \in F^n \ ;\ v * u = 0,\ u \in C\}$$

で定める．

定理 2.21. 符号 C を $[n, k]$ 符号とする時，双対符号 $C^\perp$ は $[n, n-k]$ 符号である．

証明. 双対符号 $C^\perp$ は線形符号であることを示す．$v_1, v_2 \in C^\perp$, $a, b \in F$ とする．任意の $u \in C$ に対して

$$(av_1 + bv_2) * u = a(v_1 * u) + b(v_2 * u) = 0$$

となるので $av_1 + bv_2 \in C^\perp$ である．

次元が $n-k$ であることを示す．符号 C の生成行列を $G = (g_{ij})$ とする．任意の $1 \leq i \leq k$ に対して $x_1 \ldots x_n \in C^\perp$ は $\sum_{j=1}^{n} g_{ij} x_j = 0$ を満足する．また，符号 C_1, C_2 が同値ならば $C_1^\perp, C_2^\perp$ も同値であるので，

符号 C の生成行列 G を標準形

$$G' = \left(\begin{array}{ccccc|ccc} 1 & 0 & \dots & 0 & 0 & a_{11} & \dots & a_{1(n-k)} \\ 0 & 1 & \dots & 0 & 0 & a_{21} & \dots & a_{2(n-k)} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & 1 & 0 & a_{(k-1)1} & \dots & a_{(k-1)(n-k)} \\ 0 & 0 & \dots & 0 & 1 & a_{k1} & \dots & a_{k(n-k)} \end{array}\right)$$

に変形し，G' を生成行列とする C と同値な符号 C' について考えればよい．この時，双対符号 $C'^{\perp}$ は

$$C'^{\perp} = \{x_1 \dots x_n \in F^n \ ; \ x_i + \sum_{j=1}^{n-k} a_{ij} x_{k+j} = 0 \ (1 \leq i \leq k)\}$$

となる．$x_{k+1}, \dots, x_n$ の選び方は q^{n-k} 通りあるので $\#C'^{\perp} = q^{n-k}$ である．つまり双対符号 $C'^{\perp}$ の次元は $n-k$ である． □

定理 2.22. 任意の $[n,k]$ 符号 C に対して $(C^{\perp})^{\perp} = C$ が成り立つ．

証明. 符号 C の任意の元は $C^{\perp}$ の任意の元と直交しているので $C \subset (C^{\perp})^{\perp}$ となる．また

$$\dim(C^{\perp})^{\perp} = n - (n-k) = k = \dim C$$

なので，$(C^{\perp})^{\perp} = C$ である． □

定義 2.23. 符号 C を $[n,k]$ 符号とする時，双対符号 $C^{\perp}$ の生成行列 $H \in M(n-k, n : F)$ を符号 C の検査行列という．

符号 C の生成行列 G と検査行列 H に対して $GH^T = 0$ が成り立つ．但し，H^T は H の転置行列とする．

注意 2.24. 定理 2.22 より $(C^{\perp})^{\perp} = C$ が成り立つので，符号 C は

$$C = \{x \in F^n \ ; \ xH^T = 0\}$$

のように表すことができる．このように任意の線形符号は検査行列により定まる．また，行列 $H \in M(n-k, n : F)$ が線形符号の検査行列であるための条件は行列 H の階数が $n-k$ となることである．

定理 2.25. 符号 C を $[n,k]$ 符号とし，C の検査行列 H を $H = (h_1, \dots, h_n)$ とする．但し，h_i は列ベクトルとする．この時，最小距離 $d(C) = d$ となる必要十分条件は，任意の番号 $i_1, \dots, i_{d-1}$ $(1 \leq i_1 < \dots < i_{d-1} \leq n)$ に対して $h_{i_1}, \dots, h_{i_{d-1}}$ は線形独立であり，$h_{j_1}, \dots, h_{j_d}$ が線形従属となる番号 $j_1, \dots j_d$ $(1 \leq j_1 < \dots < j_d \leq n)$ が存在することである．

証明. 符号 C の最小距離 $d(C) = d$ とする．線形符号なので $d(C) = w(C) = d$ となる．F^n の元 $x = x_1 \dots x_n$ に対して x が符号語であるための必要十分条件は $xH^T = 0$ である．つまり，

$$x \in C \iff x_1 h_1 + \dots + x_n h_n = 0 \tag{2.2}$$

である．$w(C)=d$ なので $w(x)=d$ となる $x\in C$ が存在する．つまり，$x_{j_1},\dots,x_{j_d}$ は零ではなく，残りの x_j はすべて零となる番号 $j_1,\dots,j_d$ が存在する．必要十分条件 (2.2) により $x_{j_1}h_{j_1}+\cdots+x_{j_d}h_{j_d}=0$ となる．よって $h_{j_1},\dots,h_{j_d}$ は線形従属である．一方，任意の番号 $i_1,\dots,i_{d-1}$ $(1\le i_1<\cdots<i_{d-1}\le n)$ に対して $x_{i_1}h_{i_1}+\cdots+x_{i_{d-1}}h_{i_{d-1}}=0$ とする．この時，$x=0\dots0x_{i_1}0\dots0x_{i_{d-1}}0\dots0$ とおくと

$$xH^T=x_{i_1}h_{i_1}+\cdots+x_{i_{d-1}}h_{i_{d-1}}=0$$

となる．但し，x_k は k 番目の要素である．線形符号 C に対して $w(x)\le d-1$ となるので $x=0$ でなければならない．よって，$h_{i_1},\dots,h_{i_{d-1}}$ は線形独立である． □

3 ハミング符号

有限体 F に対して F の可逆元全体を F^* と表す.

ベクトル空間 F^r には群 F^* が自然にスカラー倍で作用している．この作用によりベクトル空間 F^r は自明な軌道 $\{0\}$ とそれ以外の $n=\dfrac{q^r-1}{q-1}$ 個の軌道に分解しており，

$$F^r=\{0\}\sqcup A_1\sqcup\cdots\sqcup A_n \tag{3.1}$$

となる．$\{0\}$ 以外の軌道 $A_1,\dots,A_n$ はすべて $q-1$ 個の元から成っている．ここで，各軌道 A_i の代表元 $c_i\in A_i$ $(1\le i\le n)$ を選んでできる行列

$$H=(c_1,\dots,c_n)\in M(r,n:F),\quad c_i\in A_i\ (1\le i\le n)$$

を考える．但し，c_i は列ベクトルである．番号 i,j が異なれば基本ベクトル e_i,e_j は互いに異なる軌道に含まれる．よって，適当に番号を付け替えることにより，$e_i\in A_i$ $(1\le i\le r)$ として良い．従って

$$H=\left(\begin{array}{ccccc|ccc}
a_1 & 0 & \dots & 0 & 0 & b_{11} & \dots & b_{1(n-k)}\\
0 & a_2 & \dots & 0 & 0 & b_{21} & \dots & b_{2(n-k)}\\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & & \vdots\\
0 & 0 & \dots & a_{r-1} & 0 & b_{(k-1)1} & \dots & b_{(k-1)(n-k)}\\
0 & 0 & \dots & 0 & a_r & b_{k1} & \dots & b_{k(n-k)}
\end{array}\right)$$

とすることができる．但し，$a_1,\dots,a_r$ は零ではない．よって，行列 H の階数は r である．注意 2.24 により行列 H はある符号の検査行列になっている．

定義 3.1. このような行列 H を検査行列とする符号をハミング符号という．また，検査行列 H の階数は r であるので，ハミング符号は $[n,n-r]$ 符号である．

注意 3.2. 上述の構成法により得られる符号の同値類は軌道の代表元の取り方には依らない.

任意の i, j $(i \neq j)$ に対して c_i, c_j は線形独立である．一方 c_1, c_2, c_3 を

$$c_1 = e_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad c_2 = e_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad c_3 = e_1 + e_2 = \begin{pmatrix} 1 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

のように取る．この時， $c_1 + c_2 - c_3 = 0$ である．上述の 2 つのことから定理 2.25 より $d(C) = 3$ となる．従って，ハミング符号は $[n, n-r, 3]$ 符号である．即ち 1 誤り訂正符号である．また，ハミング符号の各パラメータは $n = \dfrac{q^r - 1}{q - 1}$, $M = q^{n-r}$, $t = 1$ で与えられるのでハミング限界式 (2.1)

$$q^{n-r}\left\{\binom{n}{0} + \binom{n}{1}(q-1)\right\} = q^{n-r}\left(1 + \frac{q^r - 1}{q-1}(q-1)\right) = q^n$$

において等号が成り立つ．このことから，ハミング符号は 1 誤り訂正完全符号であることがわかる．

4 巡回符号

4.1 巡回符号の性質

定義 4.1. 長さ n の符号 C が巡回符号であるとは以下の (1), (2) を満たすことである．

(1) 線形符号である．

(2) 符号語 $a_0 a_1 \ldots a_{n-1} \in C$ ならば $a_1 \ldots a_{n-1} a_0 \in C$ である．

例 4.2. (1) $\{000, 101, 011, 110\}$ は F_2 上の巡回符号である．

(2) $C_1 = \{0000, 1001, 0110, 1111\}$ と $C_2 = \{0000, 1010, 0101, 1111\}$ とは同値な F_2 上の符号である．しかし，C_1 は巡回符号ではなく C_2 は巡回符号である．

符号語 $a_0 a_1 \ldots a_{n-1} \in F^n$ と $a(x) = a_0 + a_1 \overline{x} + \cdots + a_{n-1} \overline{x}^{n-1} \in F[x]/(x^n - 1)$ を同一視することにより F^n の部分空間である符号 C を $F[x]/(x^n - 1)$ の部分空間とみなすことができる．また，混乱の恐れがない場合に限り $n-1$ 次以下の多項式と剰余類とを同一視し $a(x) = a_0 + a_1 \overline{x} + \cdots + a_{n-1} \overline{x}^{n-1}$ を $a(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}$ と書くことにする．これにより C の元と $n-1$ 次以下の多項式とを同一視する．

命題 4.3. 長さ n の符号 C が巡回符号である必要十分条件は以下の (1), (2) を満たすことである．

(1) 符号語 $a(x), b(x) \in C$ ならば $a(x) + b(x) \in C$ である．

(2) 符号語 $a(x) \in C, r(x) \in F[x]/(x^n - 1)$ ならば $a(x) r(x) \in C$ である．

証明. $a(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}$, $b(x) = b_0 + b_1 x \cdots + b_{n-1} x^{n-1} \in C$ とすると，

$$a(x) + b(x) = (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_{n-1} + b_{n-1}) x^{n-1} \in C$$

になる．このことは符号 C が線形であることと同値である．また，巡回符号の仮定により

$$xa(x) = a_0x + a_1x^2 + \cdots + a_{n-2}x^{n-1} + a_n \in C \tag{4.1}$$

となるので $r(x) = r_0 + r_1x + \cdots + r_{n-1}x^{n-1} \in F[x]/(x^n - 1)$ に対して

$$r(x)a(x) = r_0a(x) + r_1xa(x) + \cdots + r_{n-1}x^{n-1}a(x) \in C$$

である．逆に (2) が成立すれば式 (4.1) より符号 C が巡回符号であることがわかる． □

任意の $f(x) \in F[x]/(x^n - 1)$ に対して $f(x)$ で生成されたイデアルを

$$(f(x)) = \{r(x)f(x)\ ;\ r(x) \in F[x]/(x^n - 1)\}$$

で表す．任意の $f(x) \in F[x]/(x^n - 1)$ に対して命題 4.3 により $(f(x))$ は巡回符号である．この時，巡回符号 $(f(x))$ は $f(x)$ で生成されるという．

例 4.4. 符号 $C = (1 + x^2) \subset F_2[x]/(x^3 - 1)$ を考える．この時，C の符号語は以下のようになる．

$$C = \{0, 1 + x, 1 + x^2, x + x^2\} = \{000, 011, 101, 110\}.$$

次の定理 4.5 により任意の巡回符号は多項式により生成されることがわかる．

定理 4.5. 長さ n の零でない巡回符号を C とする．この時，以下の (1) から (3) が成り立つ．
(1) 次数が最小となるモニック多項式 $g(x) \in C$ が一意に存在する．
(2) 符号 C は $g(x)$ により生成される．
(3) (1) の $g(x)$ は $x^n - 1$ の因子である．

証明. (1) 巡回符号 C は $F[x]$ の $n-1$ 次以下の多項式のなす部分空間と同一視すると，零でない C を考えているので次数が最小となるモニック多項式 $g(x)$ が存在する．符号 C において次数最小の相異なるモニック多項式を $g(x), h(x)$ とする．$g(x) - h(x) \in C$ なので $\deg(g(x) - h(x)) < \deg g(x), \deg h(x)$ となり，零でない定数倍して $g(x) - h(x)$ をモニックにすると C において次数最小となるので仮定に矛盾する．よって $g(x), h(x)$ は一致して一意に存在する．

(2) 符号語 $a(x) \in C$ を多項式 $F[x]$ において $g(x)$ で割り，商を $q(x)$ ，余りを $r(x)$ とする．つまり $a(x) = g(x)q(x) + r(x)$ $\deg r(x) < \deg g(x)$ となる．余り $r(x)$ は $r(x) = a(x) - g(x)q(x) \in C$ となるが $\deg g(x)$ は C において次数最小なので $\deg r(x) = 0$ であり $r(x) = 0$ である．つまり，$a(x) = g(x)q(x)$ となる．

(3) 多項式 $F[x]$ において x^n-1 を $g(x)$ で割り，商を $q(x)$ ，余りを $r(x)$ とする．つまり $x^n-1 = g(x)q(x)+r(x)$ $\deg r(x) < \deg g(x)$ となる．余り $r(x)$ は $r(x) = x^n - 1 - g(x)q(x)$ となるので $r(x) \equiv -g(x)q(x) \pmod{x^n - 1}$ となる．また，$\deg g(x)$ は C のなかで最小なので $\deg r(x) = 0$ であり $r(x) = 0$ である．つまり，$x^n - 1 = g(x)q(x)$ となる． □

定義 4.6. 定理 4.5 で与えた多項式 $g(x)$ を符号 C の生成多項式という．

注意 4.7. 生成多項式を用いなくても符号を生成することができる．例 4.4 においては生成多項式は $1+x$ であるが実際には $1+x^2$ で符号を生成することができた．

補題 4.8. 多項式 $g(x)=g_0+g_1x+\cdots+g_rx^r$ が符号 C の生成多項式となるとき $g_0\neq 0$ である．

証明. $g_0=0$ と仮定する．符号語 $x^{n-1}g(x)\equiv g_1+\cdots+g_rx^{r-1} \pmod{x^n-1}$ となる．多項式 $g_1+\cdots+g_rx^{r-1}$ は次数 $r-1$ となるので $g(x)$ が C において次数最小であることに反する． □

定理 4.9. 巡回符号 C に対して，C の生成多項式を $g(x)=g_0+g_1x+\cdots+g_rx^r$ とする．この時，符号 C の次元は $n-r$ であり，符号 C の生成行列 $G\in M(n-r,n:F)$ として

$$G=\begin{pmatrix} g_0 & g_1 & \dots & g_r & 0 & \dots & 0 \\ 0 & g_0 & \dots & g_{r-1} & g_r & \dots & 0 \\ \vdots & \vdots & \ddots & & & \ddots & \vdots \\ 0 & 0 & \dots & g_0 & g_1 & \dots & g_r \end{pmatrix}$$

が取れる．

証明. $g_0\neq 0$ なので行列 G の各 $n-r$ 行は線形独立である．各 $n-r$ 行は符号語 $g(x),xg(x),\dots,x^{n-r-1}g(x)$ を表している．符号 C の符号語すべてがこれらの線形結合によって表すことができることを示せば良い．定理 4.5 により符号語 $a(x)$ に対して $a(x)\equiv q(x)g(x) \pmod{x^n-1}$ となる $q(x)\in F[x]$ が存在する．定理 4.5 により $g(x)\mid x^n-1$ なので多項式の中において $a(x)=q'(x)g(x)$ となる $q'(x)\in F[x]$ が存在する．符号語 $a(x)$ の次数は n 未満なので $q'(x)$ の次数は $n-r$ 未満である．$q'(x)=q_0+q_1x+\cdots+q_{n-r-1}x^{n-r-1}$ とすると $q'(x)g(x)$ は

$$q'(x)g(x)=q_0g(x)+q_1xg(x)+\cdots+q_{n-r-1}x^{n-r-1}g(x)$$

のように表すことができ，この式が示したい線形結合の式である． □

定理 4.9 で与えた巡回符号の生成行列は標準形ではなかったので，標準形から検査行列を書き出す方法は巡回符号には当てはまらない．そこで巡回符号に対応した検査行列を考える．

定義 4.10. 巡回符号 C を $[n,k]$ 符号，$g(x)$ を C の生成多項式とする．この時，$g(x)h(x)=x^n-1$ となるモニック多項式 $h(x)$ のことを C の検査多項式 $h(x)$ と言う．

定理 4.9 より生成多項式の次数は $n-k$ なので検査多項式 $h(x)$ の次数は k である．

定理 4.11. 巡回符号 C を $[n,k]$ 符号とする．巡回符号 C の生成多項式を $g(x)$，検査多項式を $h(x)$ とする．この時，$c(x)\in F[x]/(x^n-1)$ が C の符号語であるための必要十分条件は $c(x)h(x)\equiv 0 \pmod{x^n-1}$ で与えられる．

証明. $c(x)$ が符号語の場合を考える．定理 4.5 により $g(x)\mid x^n-1$ なので多項式の中において $c(x)=a(x)g(x)$ となる $a(x)\in F[x]$ が存在する．この時，

$$c(x)h(x)=a(x)g(x)h(x)=a(x)(x^n-1)\equiv 0 \pmod{x^n-1}$$

となる．

逆に $c(x)h(x) \equiv 0 \pmod{x^n-1}$ の場合を考える．巡回符号 C は $[n,k]$ 符号なので，$\deg g(x) = n-k$, $\deg h(x) = k$ である．$c(x)$ を $g(x)$ で割るとき商を $q(x)$ 余りを $r(x)$ とする．次数について，$n-k = \deg g(x) > \deg r(x)$ である．$0 \equiv c(x)h(x) = q(x)g(x)h(x) + r(x)h(x)$ となるので $r(x)h(x) \equiv 0 \pmod{x^n-1}$ である．また，$\deg r(x)h(x) < n-k+k = n$ なので $r(x)h(x) = 0$ である．つまり $r(x) = 0$ であり $c(x) = q(x)g(x)$ は符号語となる． □

定理 4.12. 巡回符号 C を $[n,k]$ 符号，$h(x) = h_0 + h_1x + \cdots + h_kx^k$ を C の検査多項式とする．この時，以下の (1)，(2) が成り立つ．

(1) 行列 $H \in M(n-k, n : F)$

$$H = \begin{pmatrix} h_k & h_{k-1} & \dots & h_0 & 0 & \dots & 0 \\ 0 & h_k & \dots & h_1 & h_0 & \dots & 0 \\ \vdots & \vdots & \ddots & & & \ddots & \vdots \\ 0 & 0 & \dots & h_k & h_{k-1} & \dots & h_0 \end{pmatrix}$$

は符号 C の検査行列になる．

(2) 双対符号 $C^\perp$ は $\overline{h}(x) = h_k + h_{k-1}x + \cdots + h_0x^k$ により生成される巡回符号である．

証明. (1) 多項式 $c(x) = c_0 + c_1x + \cdots + c_{n-1}x^{n-1}$ とおく．定理 4.11 により $c(x)$ が符号語である必要十分条件は $c(x)h(x) \equiv 0 \pmod{x^n-1}$ であった．即ち，$c(x)h(x) = (x^n-1)i(x)$ となる $k-1$ 次以下の多項式 $i(x)$ が存在する．一方

$$\begin{aligned} c(x)h(x) &= (c_0 + c_1x + \cdots + c_{n-1}x^{n-1})(h_0 + h_1x + \cdots + h_kx^k) \\ &= (c_0h_k + \dots c_kh_0)x^k + \cdots + (c_{n-k-1}h_k + \cdots + c_{n-1}h_0)x^{n-1} + (k-1 \text{ 次以下の項}) + (n \text{ 次以上の項}) \end{aligned}$$

である．よって，各 $x^k, \dots, x^{n-1}$ の係数は零でなければならない．即ち

$$\begin{aligned} c_0h_k + c_1h_{k-1} + \cdots + c_kh_0 &= 0, \\ c_1h_k + c_2h_{k-1} + \cdots + c_{k+1}h_0 &= 0, \\ &\vdots \\ c_{n-k-1}h_k + c_{n-k-2}h_{k-1} + \cdots + c_{n-1}h_0 &= 0 \end{aligned}$$

である．第 1 列目は $c_0c_1 \dots c_{n-1} \in C$ は $h_kh_{k-1} \dots h_00 \dots 0 \in F^n$ に直交していることを示しており，第 2 列目は $c_0c_1 \dots c_{n-1} \in C$ は $0h_kh_{k-1} \dots h_00 \dots 0 \in F^n$ に直交していることを示している．以下，各列同様である．よって，行列 H の各行は $C^\perp$ に属している．$h(x)$ は次数 k のモニック多項式であったので $h_k = 1$ である．行列は

$$H = \begin{pmatrix} 1 & h_{k-1} & \dots & h_0 & 0 & \dots & 0 \\ 0 & 1 & \dots & h_1 & h_0 & \dots & 0 \\ \vdots & \vdots & \ddots & & & \ddots & \vdots \\ 0 & 0 & \dots & 1 & h_{k-1} & \dots & h_0 \end{pmatrix}$$

のような形になるので各行とも線形独立である．定理 2.21 により双対符号 $C^\perp$ の次元は $n-k$ であり，行の数は $n-k$ でもあったので行列 H は双対符号 $C^\perp$ の生成行列である．つまり行列 H は符号 C の検査行列である．

(2) 定理 4.5 により $\overline{h}(x) \mid x^n - 1$ を示せば $(\overline{h}(x))$ は巡回符号を生成し，H がその生成行列になる．つまり，$(\overline{h}(x)) = C^\perp$ である．また，

$$\overline{h}(x) = h_k + h_{k-1}x + \cdots + h_0 x^k = x^k(h_0 + \cdots + h_k x^{-k}) = x^k h(x^{-1}),$$

$$x^{n-k}g(x^{-1}) = x^{n-k}(g_0 + g_1 x^{-1} + \cdots + g_{n-k}x^{-n+k}) = g_0 x^{n-k} + g_1 x^{n-k-1} + \cdots + g_{n-k}$$

であり，$h(x^{-1})g(x^{-1}) = (x^{-1})^n - 1$ である．この時

$$x^k h(x^{-1}) x^{n-k} g(x^{-1}) = x^n(x^{-n} - 1) = 1 - x^n$$

となるので $\overline{h}(x)$ は $x^n - 1$ の因子である． □

定義 4.13. 定理 4.12 で与えた $\overline{h}(x)$ を $h(x)$ の相反多項式という．

4.2 巡回符号としてのハミング符号

定義 4.14. 有限体 F の元 α が F の原始元であるとは $\langle\alpha\rangle = F^*$ のことを言う．

定理 4.15. 有限体 F_2 上のハミング符号は巡回符号に同値である．

証明. 次数 r の既約多項式 $p(x) \in F_2[x]$ を取る．この時 $F_2[x]/(p(x))$ は 2^r 個の元を持つ有限体である．この有限体の原始元を $\alpha \in F_2[x]/(p(x))$ とすると

$$F_2[x]/(p(x)) = \{0, 1, \alpha, \ldots, \alpha^{2^r-2}\}$$

と表すことができる．新たに $a_0 + a_1\alpha + \cdots + a_{r-1}\alpha^{r-1} \in F_2[x]/(p(x))$ $(a_i \in F_2)$ と列ベクトルを

$$\begin{array}{ccc} F_2[x]/(p(x)) & \longleftrightarrow & F_2^r \\ a_0 + a_1\alpha + \cdots + a_{r-1}\alpha^{r-1} & \longleftrightarrow & \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{r-1} \end{pmatrix} \end{array}$$

のようにして同一視する．行列 $H \in M(r, 2^r - 1 : F_2)$ を上の同一視により $((F[x]/(p(x)))^*)^{2^r-1}$ の元 $(1, \alpha, \ldots, \alpha^{2^r-2})$ と対応する元

$$\begin{array}{ccc} ((F[x]/(p(x)))^*)^{2^r-1} & \longleftrightarrow & (F_2^r)^{2^r-1} = M(r, 2^r - 1 : F_2) \\ (1, \alpha, \ldots, \alpha^{2^r-2}) & \longleftrightarrow & H \end{array}$$

として考える．行列 H を検査行列とする 2 元線形符号を C とする．行列 H の各列は零でなく，互いに異なる二つの列はスカラー倍ではなく，列の数が代表元の個数と一致しているので，符号 C はハミング符号である．$n = 2^r - 1$ とおくと符号 C は

$$\begin{aligned} C &= \{a_0 a_1 \dots a_{n-1} \in F_2^n \ ; \ a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} = 0\} \\ &= \{f(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} \in F_2[x]/(x^n - 1) \ ; \ F_2[x]/(p(x)) \text{ において } f(\alpha) = 0\} \end{aligned} \tag{4.2}$$

になる．$f(x) \in C,\ r(x) \in F_2[x]/(x^n - 1)$ とすると $r(\alpha)f(\alpha) = 0$ なの $r(x)f(x) \in C$ となる．命題 4.3 により符号 C は巡回符号である． □

定義 4.16. x が有限体 $F_2[x]/(p(x))$ の原始元となる次数 r の既約多項式 $p(x)$ を原始多項式という．

定理 4.17. 有限体 F_2 上の次数 r の原始多項式を $p(x)$ とする．この時，巡回符号 $(p(x)) \subset F_2[x]/(x^n - 1)$ はハミング符号である．但し，$n = 2^r - 1$ とする．

証明. 多項式 $p(x)$ を F_2 上の次数 r の原始多項式とする．この時，ハミング符号 C は (4.2) により

$$\begin{aligned} C &= \{f(x) \in F_2[x]/(x^n - 1) \ ; \ F_2[x]/(p(x)) \text{ において } f(\alpha) = 0\} \\ &= (p(x)) \end{aligned}$$

と表すことができる． □

例 4.18. 有限体 F_2 上の既約多項式 $x^4 + x^3 + 1$ でハミング符号を作る．多項式 $x^4 + x^3 + 1$ の F_2 上での既約性を調べる．多項式 $x^4 + x^3 + 1$ に $x = 0, 1$ を代入すると，共に 1 となる．従って，多項式 $x^4 + x^3 + 1$ は一次因子を持たない．F_2 上での二次の既約多項式は $x^2 + x + 1$ である．既約多項式 $x^2 + x + 1$ を二乗すると $x^4 + x^2 + 1$ になり，多項式 $x^4 + x^3 + 1$ は二次因子を持たない．よって，多項式 $x^4 + x^3 + 1$ は F_2 上で既約である．既約多項式 $x^4 + x^3 + 1$ の一つの根を α とする．この時 $\alpha^4 + \alpha^3 + 1 = 0$ となっている．有限体 $F_2[x]/(x^4 + x^3 + 1)$ は

$$\begin{aligned} F_2[x]/(x^4 + x^3 + 1) = \{&0, 1, \alpha, \alpha + 1, \alpha^2, \alpha^2 + 1, \alpha^2 + \alpha, \alpha^2 + \alpha + 1, \alpha^3, \alpha^3 + 1, \alpha^3 + \alpha, \\ &\alpha^3 + \alpha^2, \alpha^3 + \alpha + 1, \alpha^3 + \alpha^2 + 1, \alpha^3 + \alpha^2 + \alpha, \alpha^3 + \alpha^2 + \alpha + 1\} \end{aligned}$$

である．この時

$$\begin{array}{cccc} \alpha^4 = \alpha^3 + 1, & \alpha^5 = \alpha^3 + \alpha + 1, & \alpha^6 = \alpha^3 + \alpha^2 + \alpha + 1, & \alpha^7 = \alpha^2 + \alpha + 1, \\ \alpha^8 = \alpha^3 + \alpha^2 + \alpha, & \alpha^9 = \alpha^2 + 1, & \alpha^{10} = \alpha^3 + \alpha, & \alpha^{11} = \alpha^3 + \alpha^2 + 1, \\ \alpha^{12} = \alpha + 1, & \alpha^{13} = \alpha^2 + \alpha, & \alpha^{14} = \alpha^3 + \alpha^2, & \alpha^{15} = 1 \end{array}$$

となるので，α は有限体 $F_2[x]/(x^4 + x^3 + 1)$ の原始元である．多項式 $x^4 + x^3 + 1$ は原始多項式である．よって，多項式 $x^4 + x^3 + 1$ は F_2 上の $[15, 11]$ ハミング符号を生成する．生成されるハミング符号の検査行列は

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

のようになる．

5　ハミング符号を生成する多項式

符号語 $c_{n-1}\dots c_1c_0 \in F^n$ と多項式 $c(x)=c_{n-1}x^{n-1}+\cdots+c_1x+c_0$ を同一視することにより F^n の部分空間である符号を $n-1$ 次以下の多項式全体の成すベクトル空間の部分空間として考えることができる．

注意 5.1. この節においては A. S. Barashko [5] に従い，多項式を高ベキの順に表示するので符号語は $c_{n-1}\dots c_1c_0$ と表される．前節では，多項式を低ベキの順に表示していたので，この節での符号語は前節では $c_0c_1\dots c_{n-1}$ と表される．

有限体 F の上の次数 $r\geq 2$ のモニック多項式を $g(x)=x^r+g_{r-1}x^{r-1}+\cdots+g_1x+g_0$ とし，整数 n $(n>r)$ を取る．多項式 $g(x)$ の生成する符号 $C_{g(x)}(n)$ を

$$C_{g(x)}(n)=\{c(x)\in F[x]\ ;\ g(x)\mid c(x),\ \deg c(x)\leq n-1\}$$

で定める．符号語 $c(x)$ に対して $c(x)=g(x)h(x)$ となる次数 $n-r-1$ 以下の多項式 $h(x)$ が存在するので符号 $C_{g(x)}(n)$ は

$$C_{g(x)}(n)=\{c(x)\in F[x]\ ;\ c(x)=g(x)h(x),\ \deg h(x)\leq n-r-1\}$$

として表すこともできる．符号 $C_{g(x)}(n)$ は $[n,n-r]$ 符号である．

以下のような行列 $M_{g(x)}\in M(r,r:F)$ と r 次元の基本ベクトル e_1

$$M_{g(x)}=\begin{pmatrix}0&0&\dots&0&0&-g_0\\1&0&\dots&0&0&-g_1\\0&1&\dots&0&0&-g_2\\\vdots&\vdots&\ddots&\vdots&\vdots&\vdots\\0&0&\dots&1&0&-g_{r-2}\\0&0&\dots&0&1&-g_{r-1}\end{pmatrix},\quad e_1=\begin{pmatrix}1\\0\\0\\\vdots\\0\\0\end{pmatrix}$$

を考える．また，行列単位 $E_{i,j}$ を用いて行列 $M_{g(x)}$ を表すと

$$M_{g(x)}=\sum_{i=1}^{r-1}E_{i+1,i}+\sum_{i=1}^{r}g_{i-1}E_{r,i}$$

になり，固有多項式は $\det(M_{g(x)}-xI)=(-1)^rg(x)$ となることが確かめられる．

ベクトル空間 $F[x]/(g(x))$ と F^r はベクトル空間として同型である．同型写像 θ を以下のような基底の対応

$$\begin{array}{ccc}F[x]/(g(x))&\longrightarrow&F^r\\1&\longrightarrow&e_1\\x&\longrightarrow&e_2=M_{g(x)}e_1\\&\vdots&\\x^{r-1}&\longrightarrow&e_r=M_{g(x)}^{r-1}e_1\end{array}\tag{5.1}$$

により具体的に定める．この時，ベクトル空間 F^r において行列 $M_{g(x)}$ を掛けることは $F[x]/(g(x))$ において x 倍をすることに対応している．つまり，可換図式

$$\begin{array}{ccc} F[x]/(g(x)) & \xrightarrow{\theta} & F^r \\ {\scriptstyle x\text{ 倍}}\downarrow & & \downarrow{\scriptstyle M_{g(x)}\text{倍}} \\ F[x]/(g(x)) & \xrightarrow{\theta} & F^r \end{array}$$

が成り立つ．行列 $H_{g(x)}(n) \in M(r, n : F)$ を

$$H_{g(x)}(n) = (M_{g(x)}^{n-1}e_1, M_{g(x)}^{n-2}e_1, \ldots, M_{g(x)}^{r}e_1 \mid M_{g(x)}^{r-1}e_1, \ldots, M_{g(x)}e_1, e_1)$$

とおく．行列 $H_{g(x)}(n)$ を具体的に表すと

$$H_{g(x)}(n) = \left(\begin{array}{cccc|cccccc} * & \ldots & * & -g_0 & 0 & 0 & \ldots & 0 & 1 \\ * & \ldots & * & -g_1 & 0 & 0 & \ldots & 1 & 0 \\ \vdots & & \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots \\ * & \ldots & * & -g_{r-2} & 0 & 1 & \ldots & 0 & 0 \\ * & \ldots & * & -g_{r-1} & 1 & 0 & \ldots & 0 & 0 \end{array}\right)$$

の形になり，行列 $H_{g(x)}(n)$ の階数は r である．任意の符号語 $c(x) = c_{n-1}x^{n-1} + \cdots + c_1x + c_0 \in C_{g(x)}(n)$ は $F[x]/(g(x))$ の中では

$$c_{n-1}x^{n-1} + \cdots + c_1x + c_0 \equiv 0 \pmod{g(x)}$$

を満たしている．この関係式はベクトル空間 F^r の中では

$$c_{n-1}M_{g(x)}^{n-1}e_1 + \cdots + c_1M_{g(x)}e_1 + c_0e_1 = 0$$

に相当する．即ち

$$H_{g(x)}(n)\begin{pmatrix} c_{n-1} \\ \vdots \\ c_1 \\ c_0 \end{pmatrix} = 0$$

である．よって，行列 $H_{g(x)}(n)$ は符号 $C_{g(x)}(n)$ の検査行列となる．

以下，$T = \dfrac{q^r - 1}{q - 1}$ とおく．$q \geq 2$, $r \geq 2$ なので $T > r$ であることに注意する．

定義 5.2. 多項式 $g(x)$ がハミング符号を生成するとは検査行列 $H_{g(x)}(T)$ において互いに異なる二つの列がスカラー倍ではないことをいう．即ち，$C_{g(x)}(T)$ がハミング符号になることをいう．

定理 5.3. 次数 2 以上の多項式 $g(x)$ が x で割り切れるならば $g(x)$ はハミング符号を生成しない．

証明. 次数 2 以上の多項式 $g(x)$ を x で割り切ることができ，$g(x)$ がハミング符号を生成すると仮定する．この時，$g_0 = 0$ なので $\det M_{g(x)} = 0$ となる．よって固有値 0 の固有ベクトル c が存在する．多項式 $g(x)$ はハミング符号を生成するので $c = \alpha M^i_{g(x)} e_1$ となる $1 \leq i \leq T-1$ と $\alpha(\neq 0) \in F$ が存在する．よって $\alpha M^{i+1}_{g(x)} e_1 = 0$ である．すべての $1 \leq j \leq T-1$ に対して $M^j_{g(x)} e_1 \neq 0$ なので $j = T-1$ でなければならない．つまり $M^T_{g(x)} e_1 = 0$ である．同値なこととして $F[x]/(g(x))$ の中では $x^T \equiv 0 \pmod{g(x)}$ であり，多項式の中では $g(x) = x^r$ であることがわかる．この時，検査行列は

$$H_{g(x)}(T) = (M^{T-1}_{g(x)} e_1, \ldots, M^{r+1}_{g(x)} e_1, 0, e_r, \ldots, e_1)$$

となるので多項式 $g(x)$ はハミング符号を生成しない．これは仮定に矛盾する． □

以下，ハミング符号を生成する多項式 $g(x)$ を考える．従って，多項式 $g(x)$ は x で割り切れないものとして良い．多項式 $g(x)$ について次の記号

$$e_{g(x)} = \min\{n \ ; \ g(x) \mid (x^n - 1)\},$$

$$t_{g(x)} = \min\{n \geq 1 \ ; \ x^n \equiv \alpha \pmod{g(x)} \text{ となる零でない } \alpha \in F \text{ が存在する } \}$$

を導入する．行列式 $\det M_{g(x)} = (-1)^r g(0) \neq 0$ なので $M_{g(x)} \in GL(r:F)$ となる．$GL(r:F)$ は有限群なので $M^n_{g(x)} = I$ となる n が存在する．これを $F[x]/(g(x))$ のなかで考えると $x^n - 1 \equiv 0 \pmod{g(x)}$ となる．即ち，$g(x) \mid x^n - 1$ となる n は存在しているので $e_{g(x)}$ は確かに存在する．このことから $e_{g(x)}$ は

$$e_{g(x)} = \min\{n \geq 1 \ ; \ x^n \equiv 1 \pmod{g(x)}\} \tag{5.2}$$

のように表すことができる．$e_{g(x)}$ の 式 (5.2) の表し方により $t_{g(x)}$ の存在もわかる．

定義 5.4. 多項式 $g(x)$ が原始的であるとは $e_{g(x)} = q^r - 1$ を満足するときをいう．

注意 5.5. 多項式 $g(x)$ が原始的ならば既約なので $q = 2$ の時は定義 4.3 と同じである．

x で生成された巡回群 $\langle x \rangle = G \subset (F[x]/(g(x)))^*$ を考える．部分群 K を

$$K = \{x^i \ ; \ 0 \leq i \leq e_{g(x)} - 1 \ , \ x^i = \alpha \text{ となる零でない } \alpha \in F \text{ が存在する } \}$$

のようにおく．部分群 K は $K = G \cap F^*$ とも表すことができる．$\#K = k_{g(x)}$ とおく．巡回群 G の部分群 K による剰余類群 G/K を考える．相異なる剰余類は $t_{g(x)}$ 個あるので，剰余類群 G/K は

$$G/K = \{K, xK, \ldots, x^{t_{g(x)}-1} K\}$$

のように表すことができる．巡回群 G ，部分群 K ，剰余類群 G/K の各位数 $e_{g(x)}$, $k_{g(x)}$, $t_{g(x)}$ は関係式

$$e_{g(x)} = k_{g(x)} t_{g(x)} \tag{5.3}$$

を満足する．関係式 (5.1) で与えられる同型写像 θ により巡回群 G を

$$G \subset (F[x]/(g(x)))^* \subset F[x]/(g(x)) \longrightarrow F^r$$

のようにしてベクトル空間 F^r の部分集合としてみなすことができる．また，$x^{t_{g(x)}} = \alpha$ となるので，ベクトル空間 F^r において α 倍することは巡回群 G において $x^{t_{g(x)}}$ 倍することに対応している．可換図式

$$\begin{array}{ccc} G & \xrightarrow{\theta} & F^r \\ {\scriptstyle x^{t_{g(x)}}\text{倍}}\downarrow & & \downarrow{\scriptstyle \alpha\text{倍}} \\ G & \xrightarrow{\theta} & F^r \end{array}$$

を満足する．但し，可換図式ベクトル空間 F^r は 等式 (3.1) のように軌道分解している．軌道の一つ A と巡回群 G との共通部分はある i $(0 \leq i \leq t_{g(x)} - 1)$ が存在して剰余類群 G/K の剰余類 x^iK もしくは空集合である．また，ベクトル空間 F^r と巡回群 G との共通部分は

$$G \cap F^r = (G \cap A_1) \sqcup \cdots \sqcup (G \cap A_T)$$

と分解している．よって，剰余類 x^iK を含む軌道 A_j が一意に存在する．上述により，剰余類群 G/K から軌道の集合 $F^r/F^* = \{A_1, \ldots, A_T\}$ への写像 π

$$\begin{array}{ccc} G/K & \longrightarrow & \{A_1, \ldots, A_T\} \\ x^iK & \longrightarrow & A_j \end{array}$$

を考えることができる．写像 π は単射である．写像 π が全射ならばハミング符号を生成することが下述の定理 5.6 により分かる．

定理 5.6. 多項式 $g(x)$ は次数 2 以上で x で割り切れないとし，$T = \dfrac{q^r - 1}{q - 1}$ とおく．この時，$g(x)$ がハミング符号を生成する必要十分条件は $t_{g(x)} = T$ になることである．

証明. 写像 π は単射なので $t_{g(x)} \leq T$ である．

多項式 $g(x)$ がハミング符号を生成すると仮定する．この時，検査行列 $H_{g(x)}(T)$ は

$$H_{g(x)}(T) = (M_{g(x)}^{T-1} e_1, \ldots, M_{g(x)} e_1, e_1)$$

のように表される．同型写像 θ により

$$(M_{g(x)}^{T-1} e_1, \ldots, M_{g(x)} e_1, e_1) \longleftrightarrow (x^{T-1}, \ldots, x, 1)$$

のように考えることができる．$t_{g(x)}$ の定義と x^i, x^j $(i \neq j)$ は互いに他のスカラー倍ではないことにより $t_{g(x)} \geq T$ となる．

$t_{g(x)} = T$ と仮定する．この時，$A_i \cap G = x^{i-1}K$ となるように軌道 A_i に番号 i を付けることができる．各剰余類の代表元と $H_{g(x)}(T)$ の列ベクトルとは対応しているので，$1 \leq i \leq T$ に対して

$$A_i \quad \longleftrightarrow \quad x^{i-1}K \quad \longleftrightarrow \quad M_{g(x)}^{i-1} e_1$$

が成り立っている．行列 $H_{g(x)}(T)$ の互いに相異なる二つの列はスカラー倍ではない．よって $g(x)$ はハミング符号を生成する． □

系 5.7. 多項式 $g(x)$ は次数 2 以上で x で割り切れないとし，$T = e_{g(x)}$ とする．この時，T が素数ならば $g(x)$ はハミング符号を生成する．

証明. 等式 (5.3) により $e_{g(x)} = t_{g(x)}k_{g(x)}$ が成り立ち，$T = e_{g(x)}$ は素数なので $t_{g(x)} = 1$ もしくは $k_{g(x)} = 1$ である．$k_{g(x)} = 1$ の場合を考える．$t_{g(x)} = e_{g(x)} = T$ となるので定理 5.6 より成立する．$t_{g(x)} = 1$ の場合を考える．$x \equiv \alpha \pmod{g(x)}$ となる $\alpha \in F^*$ が存在する．つまり，$x - \alpha = g(x)h(x)$ となる多項式 $h(x)$ が存在する．しかし，$g(x)$ の次数は 2 以上なのでこのような場合は起こらない． □

一般に次数 2 以上の多項式 $g(x)$ に対して

$$t_{g(x)} = \#G/K \leq \frac{q^r - 1}{q - 1} = T,$$

$$k_{g(x)} = \#K = \#(G \cap F^*) \leq \#F^* = q - 1,$$

$$e_{g(x)} = t_{g(x)}k_{g(x)} \leq \frac{q^r - 1}{q - 1}(q - 1) = q^r - 1$$

が成り立っている．

系 5.8. 有限体 F_2 上において多項式 $g(x)$ がハミング符号を生成する必要十分条件はその多項式が原始的であることである．

証明. $q = 2$ なので $T = 2^r - 1,\ e_{g(x)} \leq 2^r - 1,\ t_{g(x)} \leq 2^r - 1$ であり，$k_{g(x)} = 1$ となる．

多項式 $g(x)$ がハミング符号を生成すると仮定する．定理 5.6 より $t_{g(x)} = T = 2^r - 1$ となる．等式 (5.3) により

$$e_{g(x)} = t_{g(x)}k_{g(x)} = 2^r - 1$$

となる．多項式 $g(x)$ は原始的である．

一方，多項式 $g(x)$ が原始的，$e_{g(x)} = 2^r - 1$ と仮定する．等式 (5.3) により

$$t_{g(x)} = e_{g(x)}/k_{g(x)} = 2^r - 1 = T$$

となる．定理 5.6 より多項式 $g(x)$ はハミング符号を生成する． □

定理 4.17 と系 5.8 との関係について考える．第 4 節において符号は $F[x]/(x^n - 1)$ の部分空間として考えており，第 5 節では符号は $n - 1$ 次以下の多項式の成すベクトル空間の部分空間として考えていた．

原始多項式 $g(x)$ の次数を r とし，$q = 2$ とする．この時，第 5 節の符号から第 4 節の符号への写像 ϕ を

$$\begin{array}{ccc} C_{g(x)}(T) & \longrightarrow & F_2[x]/(x^T - 1) \\ c(x) & \longrightarrow & \overline{c(x)} \end{array}$$

とする．但し，$T = 2^r - 1$ である．符号 $C_{g(x)}(T)$ の符号語 $c(x)$ は高々 $T - 1$ 次多項式なので $\ker\phi = \{0\}$ となる．つまり，写像 ϕ は同型写像である．第 5 節の符号語を第 4 節の符号語として

$$\begin{array}{ccc} C_{g(x)}(T) & \longrightarrow & \phi(C_{g(x)}(T)) \\ c(x) = g(x) \text{ の倍数} & \longrightarrow & \overline{c(x)} = \overline{g(x)} \text{の倍数} \end{array}$$

のように解釈することができる．

多項式 $g(x) \in F[x]$ を次数 r のモニックかつ既約な多項式とし，有限体 $F[x]/(g(x))$ の原始元を α とする．この時，$\alpha^k \equiv x \pmod{g(x)}$ となる正の整数 k $(k \leq q-1)$ が存在する．このような正の整数 k を取ると F 上の α^k の最小多項式と $g(x)$ が一致する．符号 $C_{g(x)}(n)$ は

$$C_{g(x)}(n) = \{c(x) \in F[x] \ ; \ c(\alpha^k) = 0, \ \deg c(x) \leq n-1\}$$

のようにして表すことができる．有限体 F に α^k を添加した $F(\alpha^k)$ は有限体 F_{q^r} に一致する．ベクトル空間として $F(\alpha^k)$ と $F[x]/(g(x))$ の間には同型対応

$$\begin{array}{ccc} F[x]/(g(x)) & \longleftrightarrow & F(\alpha^k) \\ x & \longleftrightarrow & \alpha^k \end{array}$$

がある．任意の符号語 $c(x) = c_{n-1}x^{n-1} + \cdots + c_1 x + c_0 \in C_{g(x)}(n)$ は $F[x]/(g(x))$ の中では

$$c_{n-1}x^{n-1} + \cdots + c_1 x + c_0 \equiv 0 \pmod{g(x)}$$

を満たしている．この関係式は $F(\alpha^k)$ の中では

$$c_{n-1}\alpha^{(n-1)k} + \cdots + c_1\alpha^k + c_0 = 0 \tag{5.4}$$

が成り立つ．有限体 F_{q^r} はベクトル空間 F^r に同型なので α^k を F^r の元として，即ち列ベクトルと考えると等式 (5.4) は

$$(\alpha^{(n-1)k}, \ldots, \alpha, 1) \begin{pmatrix} c_{n-1} \\ \vdots \\ c_1 \\ c_0 \end{pmatrix} = 0$$

に対応している．従って，行列 $H_{g(x)}(n)$ は符号 $C_{g(x)}(n)$ の検査行列となる．検査行列 $H_{g(x)}(n)$ は

$$H_{g(x)}(n) = (\alpha^{(n-1)k}, \ldots, \alpha, 1)$$

のように表すことができる．

定理 5.9. 多項式 $g(x) \in F[x]$ を次数 r のモニックかつ既約な多項式とする．有限体 $F[x]/(g(x))$ の原始元を α とし，$T = \dfrac{q^r - 1}{q - 1}$ とする．多項式 $g(x)$ が α^k の最小多項式となるように，正の整数 k $(k \leq q^r - 1)$ を取ることができる．この時，多項式 $g(x)$ が F 上にハミング符号を生成する必要十分条件は k と T が互いに素になることである．

定理 5.9 を示すために二つの補題を用意する．

補題 5.10. 正の整数 m を取り，有限体 F_{q^r} の原始元を α とする．この時，$\alpha^m \in F$ となる必要十分条件は $T \mid m$ である．

証明. 原始元 α の位数は q^r-1 であり，かつ $\beta \in F_{q^r}^*$ に対して $\beta \in F$ である必要十分条件は $\beta^{q-1}=1$ なので，$\alpha^m \in F^*$ となる必要十分条件は $(q^r-1) \mid m(q-1)$ である．$T=\dfrac{q^r-1}{q-1}$ なので $T \mid m$ である． □

補題 5.11. 任意の p $(1 \leq p \leq T-1)$ に対して $T \nmid pk$ であることの必要十分条件は k と T が互いに素になることである．

証明. 十分条件を示す．任意の p $(1 \leq p \leq T-1)$ に対して $T \nmid pk$ かつ k と T が互いに素でないと仮定する．この時 $k=ip$, $T=jp$ となる i,j と $p \geq 2$ が存在する．積 jk は $jk=ijp=iT$ となるので $T \mid jk$ となる．しかし，$j \leq T-1$ なので $T \nmid pk$ に矛盾する．

必要条件を示す．k と T が互いに素であると仮定する．この時 $T \mid pk$ であることの必要十分条件は $T \mid p$ であることである．任意の p $(1 \leq p \leq T-1)$ に対して $T \nmid p$ なので，任意の p $(1 \leq p \leq T-1)$ に対して $T \nmid pk$ である． □

定理 5.9 の証明. 行列 $H_{g(x)}(T)$ がハミング符号の検査行列となる必要十分条件は任意の p $(1 \leq p \leq T-1)$ に対して $\alpha^{pk} \notin F^*$ となることである．補題 5.10 により $H_{g(x)}(T)$ がハミング符号の検査行列となる必要十分条件は任意の p $(1 \leq p \leq T-1)$ に対して $T \nmid pk$ となることである．補題 5.11 により $H_{g(x)}(T)$ がハミング符号の検査行列となる必要十分条件は k と T が互いに素になることである． □

例 5.12. 有限体 F_4 上の既約多項式 x^2+ax+a でハミング符号を作る．有限体 F_2 上の既約多項式 x^2+x+1 による二次の拡大体を $F_4=F_2[x]/(x^2+x+1)$ とする．よって，有限体 F_4 は

$$F_4=\{0,1,a,a+1\}$$

となる．但し，$a, a+1$ は多項式 x^2+x+1 の根である．F_4 上での多項式 x^2+ax+a の既約性を調べる．$x=0,a$ を代入すると a になり，$x=1,a+1$ を代入すると 1 になるので，F_4 において多項式 x^2+ax+a は既約である．有限体 $F_4[x]/(x^2+ax+a)$ を考える．有限体 $F_4[x]/(x^2+ax+a)$ は

$$F_4[x]/(x^2+ax+a)=\{0,1,a,(a+1),x,x+1,x+a,x+(a+1),ax,ax+1,ax+a,ax+(a+1),$$
$$(a+1)x,(a+1)x+1,(a+1)x+a,(a+1)x+(a+1)\}$$

として表すことができる．$\alpha=x+a$ とする．この時

$$\begin{array}{lllll} \alpha^2=ax+1, & \alpha^3=x+1, & \alpha^4=x, & \alpha^5=a, & \alpha^6=ax+(a+1), \\ \alpha^7=(a+1)x+a, & \alpha^8=ax+a, & \alpha^9=ax, & \alpha^{10}=a+1, & \alpha^{11}=(a+1)x+1, \\ \alpha^{12}=x+(a+1), & \alpha^{13}=(a+1)x+(a+1), & \alpha^{14}=(a+1)x, & \alpha^{15}=1 & \end{array}$$

となるので，$\alpha=x+a$ は有限体 $F_4[x]/(x^2+ax+a)$ の原始元である．多項式 x^2+ax+a は $\alpha=x+a$ の最小多項式である．$T=\dfrac{4^2-1}{4-1}=5$ であり，5 と 4 は互いに素である．よって，多項式 x^2+ax+a は F_4 上の $[5,3]$ ハミング符号を生成する．この時，生成されるハミング符号の検査行列 $H_{x^2+ax+a}(5)$ は

$$\begin{aligned} H_{x^2+ax+a}(5) &= \begin{pmatrix} \alpha^{16} & \alpha^{12} & \alpha^8 & \alpha^4 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 1 & a & 0 & 1 \\ a & a+1 & a & 1 & 0 \end{pmatrix} \end{aligned}$$

である．ベクトル空間 F_4^2 は

$$F_4^2 = \left\{ \begin{pmatrix} 0 \\ 0 \end{pmatrix} \right\} \sqcup F_4^* \left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right\} \sqcup F_4^* \left\{ \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\} \sqcup F_4^* \left\{ \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\} \sqcup F_4^* \left\{ \begin{pmatrix} 1 \\ a \end{pmatrix} \right\} \sqcup F_4^* \left\{ \begin{pmatrix} 1 \\ a+1 \end{pmatrix} \right\}$$

の軌道に分解している．確かに，行列 $H_{x^2+ax+a}(5)$ の各列には各軌道の代表元が現れている．

参考文献

[1] 内田　興二．有限体と符号理論．サイエンス社 2000

[2] R. Hill．*A First Course in Coding Theory*．Oxford Uinversity Press 1984

[3] J. H. van Lint．*Introduction to Coding Theory Third Edition*．Springer-Verlag, New York 1998

[4] F. J. MacWilliams and N. J. A. Sloane．*The Theory of Error-Correcting Codes*．North-Holland, Amsterdam 1977

[5] A. S. Barashko．*Polynomials Generating Hamming Codes*．Ukrainian Math. J. 45, no.7, 987-992, 1994