誤り訂正符号系列の存在条件

田中郁美 (指導教員：萩田真理子)

1　はじめに

誤り訂正符号系列の存在条件において、これまでに１個の誤りが訂正できる最小距離 3 の誤り訂正符号系列の存在条件については研究が進んでいて、参考文献 [2][3] などでいくつかの存在条件が示されているが、2 個以上の誤りを訂正できる、最小距離 5 以上の場合についてはまだ研究されていなかった。そこで、本研究では $\mathbb{F}_2$ 上の 10 次の原始多項式を使って、2 誤り訂正符号系列にどのような存在条件があるかを調べた。

2　符号

[符号]
X:有限集合とする時、$C \subset X^n$ を符号という。$\mathbf{x} = (x_1, x_2, \ldots, x_n), \mathbf{y} = (y_1, y_2, \ldots, y_n) \in X^n$ について、$d(\mathbf{x}, \mathbf{y}) = \sharp\{i | x_i \neq y_i\}$ を $\mathbf{x}$ と $\mathbf{y}$ のハミング距離という。

[誤り訂正符号]
符号 C の最小距離 $d = min\{d(\mathbf{x}, \mathbf{y}) | \mathbf{x}, \mathbf{y} \in C, \mathbf{x} \neq \mathbf{y}\} \geq 2e + 1$ の時、送る元が X^n の中の C の元だけだとわかっていれば、C にない元が届いた時に 1 番近い符号に直す事で e 個までの誤りを訂正できる。このような符号を e 誤り訂正符号という。

[線形符号]
$C \subset \mathbb{F}_q^n$ が $\mathbb{F}_q^n$ の k 次元部分空間のときつまり、基底ベクトル $^\exists c_1, c_2, \ldots, c_k \in C$ について $C = \{a_1c_1 + a_2c_2 + \cdots + a_kc_k | a_i \in X\}$ と書ける時、C を線形符号という。この時、C の大きさは q^k である。この符号の最小距離が d の時、(n, k, d) 符号という。

[パリティ検査行列]
C の直交補空間は線形代数の次元公式の定理より、$n-k$ 次元である。つまり、ある行列 H について、$C = \{c \in X^n | Hc = \overrightarrow{0}\}$ とかける。この H をパリティ検査行列という。

以上より、n を固定したとき、送れる情報の割合を大きくするには $|C|$ は大きい方がよい。つまり、$\mathbb{F}_2$ 上の (n, k, d) 符号では $|C| = 2^k$ なので、k が大きい方がよい。また、たくさんの誤りを訂正できるので、e も大きい方がよい。

3　符号の限界式

しかし、k も e も大きくするのは難しい。例えば、以下のシングルトン限界式とハミング限界式を満たさなければならないことが知られている。

[シングルトン限界式]
$\mathbb{F}_q$ 上の符号において、符号語の長さが n であるとき、可能な最大符号語数は q^k。2 つの符号語間の最小ハミング距離を d とする。すると、$q^k \leq q^{n-d+1}$ が成り立つ。$\mathbb{F}_2$ 上の符号では、$q = 2$ で $2^k \leq 2^{n-d+1}$ となる。

[ハミング限界式]
C の元 $\mathbf{x}$ から、距離 e 以下の点の集まりは全て異なる。$\mathbf{x}$ から距離 e 以下の点の数は $1 + \binom{n}{1}(q-1) + \binom{n}{2}(q-1)^2 + \cdots + \binom{n}{e}(q-1)^e$ よって、ハミング限界式は $|C|(1 + \binom{n}{1}(q-1) + \binom{n}{2}(q-1)^2 + \cdots + \binom{n}{e}(q-1)^e) \geq q^n$ と書ける。$\mathbb{F}_2$ 上の符号では、$q = 2$ で $|2^k|(1 + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{e}) \geq 2^n$ となる。

4　誤り符号訂正系列

[誤り訂正符号系列 (error-correcting sequence(ECS))]
X 上の (N, k, d) 誤り訂正符号系列 (ECS) とは、周期 N の数列
$a_0a_1a_2 \ldots a_{N-1} \ldots (a_{i+N} = a_i, a_j \in X)$
であり、どの連続する k 項も異なり、最小距離
$d = min\{\sum_{i=0}^{k-1} \delta(a_{i+s}, a_{i+t}) | 0 \leq s < t \leq N-1\}$
ただし、$\delta(x, y) = \begin{cases} 1(x \neq y) \\ 0(x = y) \end{cases}$
の誤り訂正符号をなすものをいう。

[m 系列]
$\mathbb{F}_2$ 上の n 次の原始多項式 $f(t) = t^n + a_{n-1}t^{n-1} + \cdots + a_1t + a_0$ の係数から作られる漸化式 $x_{n+i} + a_{n-1}x_{n+i-1} + \cdots + a_1x_{i+1} + a_0x_i = 0$ で生成される数列 $x_0x_1x_2x_3 \ldots$ を m 系列という。

m 系列は、周期 $2^n - 1$ で、連続する n 個見た時の最小距離が 1 であるから、$(2^n - 1, n, 1)$ECS である。つまり、$d = 1$ となり、誤りを訂正することはできない。

そこで、$d \geq 3$ とするために、$(2^n - 1, n + s, d)$ECS とし、d を大きくするために、見る範囲を $+s$ だけ拡張し、m 系列に現れる連続する $n + s$ 個を見る。これは

$$A = \begin{bmatrix} a_0 & a_1 & \ldots & a_n & 0 & 0 & 0 & \ldots & 0 \\ 0 & a_0 & a_1 & \ldots & a_n & 0 & 0 & \ldots & 0 \\ 0 & 0 & a_0 & a_1 & \ldots & a_n & 0 & \ldots & 0 \\ & & \ddots & & & & \ddots & & \\ 0 & 0 & 0 & \ldots & 0 & a_0 & a_1 & \ldots & a_n \end{bmatrix}$$

を $s \times (n + s)$ 行列とすると、$A\mathbf{x} = 0$ を満たす、全て 0 以外のベクトル $\mathbf{x}$ の全体である。$d \geq 3$ にするためには、行列 A のどの 2 列以下の組み合わせも線形独立、$d \geq 5$ にするためには、行列 A のどの 4 列以下の組み合わせも線形独立でなくてはならない。

5　$\mathbb{F}_2$ 上の 10 次の原始多項式の比較

$\mathbb{F}_2$ 上の 10 次の原始多項式の m 系列からパリティ検査行列を作り、以下の 2 つについて調べた。

- 多項式ごとのパリティ検査行列の行数の比較
- 2 列独立になるための行数と 4 列独立になるのための行数の比較

[1 誤り訂正符号系列]
最小距離 $d \geq 3$、つまり、A のどの 2 列以下も線形独立であるパリティ検査行列 A をもつ誤り訂正符号系列を 1 誤り訂正符号系列という。また、ドブライン系列からこの条件を満たす原始多項式が知られている。

[2 誤り訂正符号系列]
最小距離 $d \geq 5$、つまり、A のどの 4 列以下も線形独

立であるパリティ検査行列 A をもつ誤り訂正符号系列を 2 誤り訂正符号系列という。

[比較]

パリティ検査行列を作った時、どの 2 列以下も独立になる行数とどの 4 列以下も独立になる行数を図 1 にまとめた。

原始多項式	2列独立	4列独立	原始多項式	2列独立	4列独立
10011010111	4	15	10000011011	7	12
10001101111	5	10	11101100011	7	12
10100100011	5	12	11001111111	7	16
11110010011	5	10	10000101101	7	14
10111111011	6	11	11011011111	7	12
10100110001	6	13	10100001101	8	11
10111100101	6	15	11111111001	8	12
10100011001	6	10	11101000111	8	11
10110001111	6	11	10111000111	8	13
11011010011	6	11	11010110101	8	12
11101111101	6	12	10000100111	8	15
11001111001	6	11	11000010011	9	11
11000010101	6	10	11101010101	9	13
11010001001	6	11	11100111001	9	12
11101001101	7	13	10000001001	10	20

図 1: 原始多項式 (m 系列表示) の 2 列独立になる行数と 4 列独立になる行数

図 1 から、図 2 のような関係性がわかる。

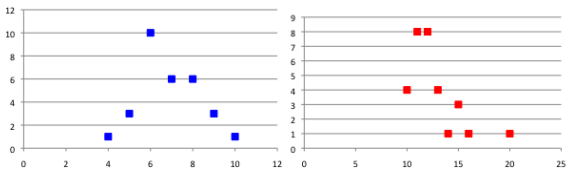

図 2: (左)x 軸:2 列独立になる行数と y 軸:その多項式の数の関係,(右)x 軸:4 列独立になる行数と y 軸:その多項式の数の関係

図 2 から、図 3 のような 2 列独立になる行数と 4 列独立になる行数の関係性がわかる。

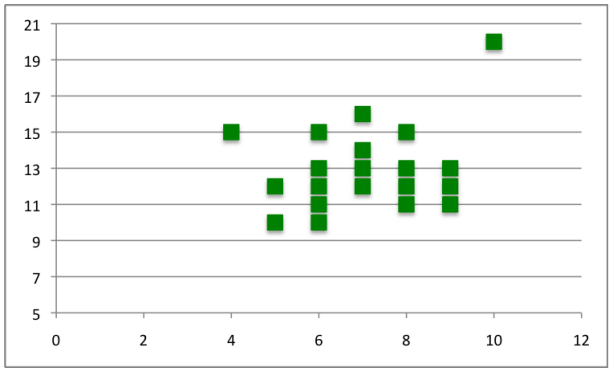

図 3: x 軸:2 列独立になる行数と y 軸:4 列独立になる行数の関係

以上の結果をより正確に分析する為に、相関係数を使う。相関係数とは、2 つの確率変数の間の相関を示す統計学的指標である。

[相関係数]

2 組の数値からなるデータ列 $(x, y) = \{(x_i, y_i)\}(i = 1, 2, \ldots, n)$ があたえられたとき、

$$\frac{\sum_{i=1}^{n}(x_i - \overline{x})(y_i - \overline{y})}{\sqrt{\sum_{i=1}^{n}(x_i - \overline{x})^2}\sqrt{\sum_{i=1}^{n}(y_i - \overline{y})^2}}$$

を相関係数とよぶ。ただし、$\overline{x}, \overline{y}$ はそれぞれデータ $x = x_i, y = y_i$ の相加平均である。これは、各データの平均からのずれを表すベクトル

$$x - \overline{x} = (x_1 - \overline{x}, \ldots, x_n - \overline{x}), y - \overline{y} = (y_1 - \overline{y}, \ldots, y_n - \overline{y})$$

のなす角の余弦である。

相関係数は-1 から 1 の間の実数値をとり、1 に近いときは 2 つの確率変数には正の相関があるといい、-1 に近いときは負の相関があるという。0 に近いときはもとの確率変数の相関は弱いという。

これを計算すると図 3 の相関係数は 0.357297087 で、正の相関があり、やや相関があるといえる。

6 まとめ

図 1 より、以下の存在定理が示された。

[誤り訂正符号系列の存在定理]

誤り訂正符号系列として、1 誤り訂正符号系列は $(2^{10} - 1, 14, 3)ECS$、2 誤り訂正符号系列は $(2^{10} - 1, 20, 5)ECS$ が存在する。

$(2^{10} - 1, 14, 3)ECS$ は $x^{10} + x^7 + x^6 + x^2 + x + 1$ から生成される m 系列であり、$(2^{10} - 1, 20, 5)ECS$ は $x^{10} + x^6 + x^5 + x^3 + x^2 + x + 1$,$x^{10} + x^9 + x^8 + x^7 + x^4 + x + 1$,$x^{10} + x^8 + x^4 + x^3 + 1$,$x^{10} + x^9 + x^4 + x^2 + 1$ から生成される m 系列である。ただし、m 系列から作られる 1 誤り訂正符号系列としては最もよいパラメータを与えた原始多項式 $x^{10} + x^7 + x^6 + x^2 + x + 1$ で作られる m 系列は、2 誤り訂正符号系列としてはあまりよいパラメータとは言えず、$(2^{10} - 1, 25, 5)ECS$ であるが、$k \leq 24$ については $(2^{10} - 1, k, 5)ECS$ でない事がわかった。

7 今後の課題

少ない行数で最小距離 5 以上になるための簡単な条件を見つけ，一般的な次数についての”何行で最小距離 5 になる原始多項式が存在する”というような存在定理を作り、具体的な原始多項式の見つけ方を与えることが今後の課題である。そのために、まずもう少し大きな次数について実験し、最小距離をもっと増やそうとするとよい原始多項式が変わるかどうか調べ、$\mathbb{F}_2$ だけではなく、$\mathbb{F}_3$ など他の体上の m 系列についても調べることを考えている。

参考文献

[1] Oliver Pretzel:Error-Correcting Codes and Finite Fields

[2] 佐藤春菜:”Projective DeBruijn 系列を係数に持つ多項式の原始既約性の判定” 2009 年度お茶の水女子大学修士論文

[3] Mariko Hagita, Makoto Matsumoto, Fumio Natsu, Yuki Ohtsuka: ”Error Correcting Sequence and Projective De Bruijn Graph” Graphs and Combinatorics 24,185-194,2008.