DeBruijn 系列から作られる多項式について

松木　みなみ　(指導教員：萩田真理子)

1　はじめに

ストリーム暗号の多くは、鍵から生成した擬似乱数列と平文を XOR して暗号化され、復号時には再び暗号文と擬似乱数列を XOR する。このとき、暗号化した時と同じ位置で XOR しなければならないため、送信者と受信者の間で同期を取る必要がある。そのため、送信者が周期的な数列を単位時間に 1 ビットずつ送り続けたとき、受信者の側で受け取った数列の一部分を見れば、たとえそれが誤りを含む列でも、それを訂正して相手の送った数列を知り、同期を取ることができる誤り訂正符号系列が必要とされている。このような誤り訂正符号系列は、F_2 上では DeBruijn 系列、$F_q(q \geq 3)$ 上では Projective DeBruijn 系列を係数に持つ原始多項式が存在すれば、これを用いて m 系列を作ると性質の良いものが得られる。本研究では F_2 上の 4 次以下の多項式から作られる行列が何行まで行を増やせばどの 2 列も独立になるか確認した。どの 2 列も独立になるように増やす行数が少なくて済む多項式からm系列を生成すると効率良く誤り訂正できる符号が得られるためである。多項式によって必要な行数にどの程度差があるのか調べた。

2　誤り訂正符号とm系列

Definition 1 (ハミング距離) F^n の任意の 2 つの元 $\boldsymbol{x} = (x_1, \cdots, x_n)$ と $\boldsymbol{y} = (y_1, \cdots, y_n)$ に対して，$x_i \neq y_i$ である座標 i の数を $\boldsymbol{x}$ と $\boldsymbol{y}$ のハミング距離といい，$d(\boldsymbol{x},\boldsymbol{y})$ と書く.

Definition 2 (最小距離)　$C(\subset F^n)$ を符号とする.C の任意の 2 つの符号語のハミング距離の最小値

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

を符号 C の最小距離という.

Definition 3 (e-誤り訂正符号) e ビット以内の誤りを正確に復号することが出来る符号を e-誤り訂正符号 *(e-error correcting code)* と呼び，e をこの符号の誤り訂正能力という.

符号 C の最小距離 d が $d \geq 2e+1$ を満たすとき，C は e-誤り訂正符号となる.

Definition 4 (m 系列) F_q 上の n 次のm系列とは，原始多項式

$$f(t) = t^n + a_{n-1}t^{n-1} + \cdots + a_1 t + a_0$$

の係数から作られる漸化式

$$x_{n+i} + a_{n-1}x_{n+i-1} + \cdots + a_0 x_i = 0$$

で生成される，周期 $q^n - 1$ の数列

$$C := x_i x_{i+1} \cdots x_{i+m-1} (i = 0, 1, \cdots, q^n - 1)$$

である.

Definition 5 (error-correcting sequence) X 上の (N, k, d)*error-correcting sequcnce(ECS)* とは，周期 N の数列

$$a_0 a_1 a_2 \cdots a_{N-1} \qquad a_i = a_{N+i}, \quad a_j \in X$$

であり，どの連続する k 個も異なり，最小距離

$$d := \min_{0 \leq s < t \leq N-1} \sum_{i=0}^{k-1} \delta(a_{i+s}, a_{i+t}) \text{ ただし}$$

$$\delta(x, y) = \begin{cases} 1 & (x \neq y) \\ 0 & (x = y) \end{cases}$$

の *error-correcting code* をなすものをいう.

例：m 系列は，周期 $q^n - 1$ で，連続する n 個を見たときの最小距離が 1 であるから，$(q^n - 1, n, 1)$ECS である.

3　DeBruijn 系列

2 章より，e 個の誤り訂正をするための最小距離 d は $d \geq 2e+1$ であることから，1 個の誤りを訂正するには d は 3 以上でなくてはならないことが分かる. しかしm系列は $(q^n - 1, n, 1)$ECS，すなわち $d = 1$ であるため，誤りを訂正することができない.
そこで，$d \geq 3$ とするため，$(q^n - 1, n + s, d)$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

$$A = \begin{pmatrix} a_0 & a_1 & \cdots & a_{n-1} & 1 & 0 & \cdots & 0 \\ 0 & a_0 & a_1 & \cdots & a_{n-1} & 1 & \cdots & 0 \\ & & \ddots & \ddots & & \ddots & & \\ 0 & \cdots & 0 & a_0 & a_1 & \cdots & a_{n-1} & 1 \end{pmatrix}$$

を $s \times (n+s)$ の行列とすると，$A\boldsymbol{x} = 0$ を満たす，全て 0 以外のベクトル$\boldsymbol{x}$の全体である.$d \geq 3$ にするためには，行列 A のどの 2 つの列も線型独立でなくてはならない. 線型独立な列の個数は高々 $\dfrac{q^s - 1}{q - 1}$ 個であるから，$n + s \leq \dfrac{q^s - 1}{q - 1}$ とわかる. 本研究では $q = 2$ とし、s が小さくなるための条件を考える。

Definition 6 (Debruijn 系列) s 次の *DeBruijn* 系列とは，F_2 上の周期 2^s の数列であり，連続する s 個を見ると，周期の中でどのパターンもちょうど *1* 回ずつ出ている数列である.

Theorem 1 F_2 上の *DeBruijn* 系列を係数に持つ多項式からm系列を作ると，$n + s = 2^s - 2$ の $(2^n - 1, n + s, 3)$*ECS* となる. ただし s 次の *DeBruijn* 系列を係数に持つ多項式とは、*DeBruijn* 系列の 0 が s 個連続する部分の次からその s 個の前までの列から，1 が s 個連続する部分の 1 つの 1 を除いた列を係数列とする多項式である.

Theorem 2 (DeBruijn 系列の個数) F_q 上の s 次の *DeBruijn* 系列の個数は

$$2^{2s-1-s}$$

個である.

Conjecture 1 F_2 上の *DeBruijn* 系列を係数に持つ多項式の中には，原始既約であるものが存在する.

この予想が成り立てば，次の予想も成り立つ.

Conjecture 2 *Conjecture1* が正しければ，各 s で $\left(2^{2^s-s-2}, 2^s-2, 3\right)$ *ECS* が存在する.

4 多項式の選択による行数の差異

Definition 7 多項式

$$f(x) = a_0x^n + a_1x^{n-1} \cdots + a^{n-1}x + a_n$$

から作られる行列を

$$A = \begin{pmatrix} a_0 & a_1 & \cdots & a_{n-1} & a_n & 0 & \cdots & 0 \\ 0 & a_0 & a_1 & \cdots & a_{n-1} & a_n & \cdots & 0 \\ & & \ddots & \ddots & \ddots & & & \\ 0 & \cdots & 0 & a_0 & a_1 & \cdots & a_{n-1} & a_n \end{pmatrix}$$

とする。この $s \times (n+s)$ 行列 A を行数 s の行列と呼ぶ。

本研究においては, 多項式から作られる行数を何行まで増やせばどの２列も独立になるか、４次以下の多項式について調べた。

Definition 8 多項式 $f(x)$ がどの k 列も独立になるために必要な行の数を $r_k(f(x))$ とし、
その差を $d_k = r_{k+1} - r_k$ とする。

それぞれの多項式の r_2, r_3, d_2 の値は次のようになった。特に４次の場合、r_2 の値が３から８と大きな差があることがわかった。また、$r_2(f_1(x)) \leq r_2(f_2(x))$ のときに $r_k(f_1(x)) \leq r_k(f_2(x))$ となると予想していたが、ならない場合もあることがわかった。

表 1: １次の多項式

	r_2	r_3	d_2
$x+1$	2	3	1

表 2: ２次の多項式

	r_2	r_3	d_2
x^2+1	4	6	2
x^2+x+1	3	4	1

表 3: ３次の多項式

	r_2	r_3	d_2
x^3+1	6	9	3
x^3+x+1	3	5	2
x^3+x^2+1	3	4	1
x^3+x^2+x+1	4	5	1

表 4: ４次の多項式

	r_2	r_3	d_2
x^4+1	8	12	4
x^4+x+1	4	6	2
x^4+x^2+1	6	8	2
x^4+x^2+x+1	3	7	4
x^4+x^3+1	4	6	2
x^4+x^3+x+1	5	8	3
$x^4+x^3+x^2+1$	3	7	4
$x^4+x^3+x^2+x+1$	5	6	1

5 ４次多項式の r_2 が最小の例と最大の例

行数 r_2 が一番少なかった例１：x^4+x^2+x+1

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

行数 r_2 が一番少なかった例２：$x^4+x^3+x^2+1$

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

行数 r_2 が一番多かった例：x^4+1

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

6 まとめと今後の課題

多項式の選び方によってどの２列も独立になるために必要な行の数が大きく異なることが確認された。一般の k についてどの k 列も線形独立になるために必要な行の数 $r_k(f(x))$ についても調べていきたい。また、$r_2(f_1(x)) < r_2(f_2(x))$ のときに $r_3(f_1(x)) > r_3(f_2(x))$ となる例が確認されたが、一般の k について $r_k(f_1(x)) < r_k(f_2(x))$ となるための条件や、DeBruijn 系列から作った多項式の r_2, r_3, d_2 の値について考えていきたい。