Projective DeBruijn 系列を係数に持つ多項式の原始既約性の判定

佐藤 春菜　(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の排他的論理和 (XOR) を取ることで暗号化され，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，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「Projective DeBruijn 系列を係数に持つ原始多項式が存在する」ことを確かめるため，小さなパラメータでの原始多項式の割合を調べた．

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)* と呼ぶ．

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

$$f(t)=t^n+a_{n-1}t^{n-1}+\cdots+a_1t+a_0$$

の係数から作られる漸化式

$$x_{n+i}+a_{n-1}x_{n+i-1}+\cdots+a_0x_i=0$$

で生成される，周期 q^n-1 の数列 $x_0x_1x_2\cdots$ である．

$$C:=\{x_ix_{i+1}\cdots x_{i+n-1}\mid i=0,1,\cdots,q^n-1\}$$

とおくと，$C=F_q^n\backslash\{\mathbf{0}\}$ となる．

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

$$a_0a_1a_2a_3\cdots,\quad a_i=a_{N+i},\quad a_j\in X$$

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．

F_q 上 n 次の m 系列は，周期 q^n-1 で，Definition4,5 より $(q^n-1,n,1)$ECS である．

3　Projective 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，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

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

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$\dfrac{q^n-1}{q-1}$ 個であるから，s をなるべく小さくするには，この最大値を考えればよいので，$n+s=\dfrac{q^n-1}{q-1}$ とする．このとき，行列 A の一行目を 1 つの周期とする数列を考えると，行列 A のどの列も周期の中でちょうど 1 回ずつ，連続する s 文字として現れていることがわかる．

Definition 6 (Projective Debruijn 系列) s 次の *Projective DeBruijn* 系列とは，F_q 上の周期 $\dfrac{q^s-1}{q-1}$ の数列であり，連続する s 個を見ると，周期の中で全て *0* の列以外のどのパターンもちょうど *1* 回ずつ出ている数列である．ただし，$k\in F_q\backslash\{0\}$ について $(x_1x_2\cdots x_s)=k(x_1x_2\cdots x_s)$ とする．

Theorem 1 $f(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$ を F_q 上 s 次の *Projective DeBruijn* 系列を係数に持つ多項式とする．ただし $n=\frac{q^s-1}{q-1}-s$ である．この $f(x)$ からm系列を作ると，$(q^n-1,n+s,3)$*ECS* となる．

「Projective DeBruijn 系列を係数に持つ多項式」とは，$s-1$ 個の 0 が連続する部分を除き，その次の数から順に係数とした多項式である．これは $\frac{q^s-1}{q-1}-s$ 次式になる．

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

$$\frac{(q!)^{\frac{q^{s-1}-1}{q-1}}}{q^{s-1}}$$

個である.

Conjecture 1 $F_q(q \geq 3)$ 上の *Projective 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，$\left(q^{\frac{q^s-1}{q-1}-s}-1, \frac{q^s-1}{q-1}, 3\right)$ *ECS* が存在する.

$F = F_2$ の場合については，この予想は成り立たず，代わりに $(2^{2^n-n-1}-1, 2^n-2, 3)$ECS が存在すると予想されている．この予想については，DeBruijn 系列と呼ばれる列を係数とする原始多項式の存在を仮定すれば正しいことが示されていて，その存在性については先行研究があるので，本研究では q が奇数の場合を考察した.

4 既約多項式の原始性の判定

Definition 7 (原始多項式) $f(x)$ を F_q 上の n 次式とする．$x, x^2, x^3, \cdots, x^{q^n-1}$ を $f(x)$ で割ったときの余りが全て異なるとき，$f(x)$ を原始多項式という.

本研究では，すでに既約多項式であると判定された多項式を以下のような方法で原始多項式かどうかを調べた.

F_q 上の n 次式を考え，k を $x^k = 1$ となる最初の k とすると，$x, x^2, x^3, \cdots$ は周期 k の周期列となる．既約な多項式は $x^{q^n-1} = 1$ であるので，$k \mid q^n - 1$ が成り立つ.

定義より，$k = q^n - 1$ なら原始既約である.
$q^n - 1$ と k がそれぞれ次のように分解できたとする.

$$q^n - 1 = q_1^{e_1} q_2^{e_2} \cdots q_l^{e_l}$$
$$k = q_1^{d_1} q_2^{d_2} \cdots q_l^{d_l}$$

$k < q^n - 1$ とすると，$d_i < e_i$ となる i が存在し，$k \mid \frac{q^n-1}{q_i}$ が成り立つ.
$x^k = 1$ ならば $x^{\frac{q^n-1}{q_i}} = 1$ なので，$q^n - 1$ の全ての素因数 q_i について $x^{\frac{q^n-1}{q_i}} \neq 1$ ならば原始既約であるといえる.

5 Projective DeBruijn 原始多項式の存在性

F_3 上の 3 次と 4 次の Projective DeBruijn 系列に関しての結果は以下のようになった.

	3 次 $(n = 10)$	4 次 $(n = 36)$
ProjectiveDeBruijn の数 (調べた数)	144 (144)	6510819 (2000)
既約多項式の数	12	64
原始多項式の数	0	28
$a_n = 1, a_0 \neq 0$ の多項式の総数	39366	約 1.00×10^{17}
原始多項式の総数	2640	約 1.19×10^{15}

3 次の Projective DeBruijn 系列では原始多項式は存在しなかった．これは Conjecture1 の反例となる結果である.

また，4 次の結果から,「一般の多項式の中の原始多項式の割合」と「Projective DeBruijn 系列から作った多項式の中の原始多項式の割合」を比較してみると，以下のようになる.

$$\frac{F_3 \text{上の } 36 \text{ 次の原始多項式の個数}}{F_3 \text{上の } 36 \text{ 次式の個数}} = \frac{\phi(3^{36}-1)/36}{2 \cdot 3^{35}} = 0.00399\cdots$$

$$\frac{\text{Projective DeBruijn 原始多項式の個数}}{\text{Projective DeBruijn 多項式の個数}} = \frac{28}{2000} = 0.014$$

このように，Projective DeBruijn 系列から作った多項式の方が原始多項式の割合が高いと期待できる結果となった．Projective DeBruijn 系列から作った多項式の方がランダムに係数を選んだ多項式よりも原始多項式になりやすいと仮定すると，Projective DeBruijn 系列を係数とする原始多項式の個数の期待値は,

$$(F_3 \text{上4 次の Projective DeBruijn 系列の個数}) \times \frac{F_3 \text{上 36 次の原始多項式の個数}}{F_3 \text{上 36 次の多項式の個数}} = \frac{(q!)^{\frac{q^{s-1}-1}{q-1}}}{q^{s-1}} \cdot \frac{\phi(q^n-1)/n}{(q-1)q^{n-1}}$$

個以上となり，$q = 3$ の 3 次 $(s = 3, n = 10)$ 以外では存在すると期待できる.

6 まとめと今後の課題

F_3 上の 3 次と 4 次の Projective DeBruijn 系列の係数から作った多項式について，それぞれの原始多項式の割合を調べた.

今後は，F_3 上の 4 次の多項式について，より統計的な精度を出すようにプログラムを改良すること，また，F_5 上の Projective DeBruijn 系列についても同様に調べていきたい.

参考文献

[1] Mariko Hagita, Makoto Matsumoto, Fumio Natsu, Yuki Ohtsuka: "Error Correcting Sequence and Projective De Bruijn Graph"
Graphs and Combinatorics(2008)24:185-194