論　文

F_2 上の既約 All One Polynomial を用いた素数次の既約多項式の組織的な生成法

牧田　慶[†]　　野上　保之[††]　　杉村　立夫[†]

Generating Prime Degree Irreducible Polynomials by Using Irreducible All One Polynomial over F_2

Kei MAKITA[†], Yasuyuki NOGAMI[††], and Tatsuo SUGIMURA[†]

あらまし　近年考案されている公開鍵暗号方式には，位数の大きな有限体を定義体とするものが多い．これに対して，ハード化しやすいなどの理由から標数を 2 として高次拡大体を高速実装する研究報告が多く，それに必要となる高次既約多項式の生成法，Optimal Normal Bases（ONB）など高速実装に適した基底の構成法に関する研究報告が多くなされている．高次既約多項式の一生成法として，m 次既約多項式から $2m$ 次の自己相反既約多項式を簡単な多項式変換（自己相反変換と呼ぶ）により生成する手法が知られており，本論文では，その m 次既約多項式の零点集合が正規基底をなす場合には，生成される $2m$ 次自己相反既約多項式の零点集合も正規基底をなすことを示す．続いて自己相反変換において，変換を施される既約多項式と生成される自己相反既約多項式が 1 対 1 の関係にあることを明確に示し，自己相反既約多項式には自己相反変換の逆変換（自己相反逆変換）が行えることを示す．そして自己相反逆変換により，$2m$ 次の自己相反既約多項式から m 次の既約多項式が必ず生成されることを示し，1/2 倍の次数の既約多項式生成につながることを述べる．自己相反逆変換による 1/2 倍の次数の既約多項式生成の応用として，TypeII ONB を零点にもち，かつ素数次の既約多項式を生成する手法を与える．

キーワード　自己相反既約多項式，TypeI/TypeII Optimal Normal Basis，楕円曲線暗号

1. まえがき

現代情報化社会において，様々な機器が端末としてインターネットに接続されるようになり，情報セキュリティ技術の必要性はますます高まってきている．特に電子認証技術の需要は多く，それを可能とする公開鍵暗号技術は必要不可欠である [1]．RSA（Rivest Shamir Adleman）公開鍵暗号方式に代わる次世代の公開鍵暗号方式として注目される楕円曲線暗号など，近年考案されている公開鍵暗号方式の多くが，位数の大きな有限体を定義体とするものである [2]．楕円曲線暗号方式の場合は，その安全性を確保するために 160 ビット以上の位数を有する有限体を定義体とする必要があり [2]，XTR-Elgamal 暗号方式の場合には 340 ビット以上の有限体を必要とする [3], [4]．

このような位数の大きな有限体，より具体的には，そのような有限体における演算を，携帯電話など計算リソースの限られた端末へ実装する場合，プログラムサイズがコンパクトであること，計算処理が高速であることなどが要求される [5]．楕円曲線暗号の分野に限っていうと，定義体に用いる有限体の拡大次数は素数でなければならないなど，安全性の観点から満足しなければならない条件もある [6]．

以上のような要請に対して，ハード化しやすいなどの理由から標数を 2 として高次拡大体を高速実装する研究報告が多い [7], [8]．その際に必要となる高次既約多項式の生成法に関する研究報告も多くなされているが，これら生成法の多くが変数変換を用いるものであり，合成数次数の既約多項式しか生成できないという問題がある [9]～[11]．一方高速実装に関する研究は大きく二つに分類でき，一つは既約 3 項式，既約 All One

[†] 信州大学工学部電気電子工学科，長野市
Faculty of Engineering, Shinshu University, Nagano-shi, 380-0928 Japan
[††] 岡山大学工学部通信ネットワーク工学科，岡山市
Faculty of Engineering, Okayama University, Okayama-shi, 700-8530 Japan

Polynomial（既約 AOP）[12] など法多項式に関するもの，もう一つは Optimal Normal Bases（ONB）[2] など基底に関するものである．ONB は，更に TypeI 及び TypeII の 2 通りに分類でき，既約 AOP の零点 ω の共役元で構成されるのが TypeIONB であり，その零点 ω を用いて $\omega+\omega^{-1}$ のように変換して得られる元の共役元で構成されるのが TypeIIONB である [13], [14]．本論文は，自己相反既約多項式と正規基底の関係を用いて，TypeII ONB を零点にもつ素数次の既約多項式の生成法を提案するものである．

本論文では，既約 AOP が TypeIONB を零点とし，拡大体上演算の高速実装に非常に適した既約多項式であることに加え，自己相反既約多項式の典型的な例でもあるということに着目する．そして，本論文を通して自己相反変換と呼ぶ，m 次多項式から $2m$ 次自己相反多項式を得る多項式変換手法を紹介し，1 次係数が 1 である m 次既約多項式から，$2m$ 次の自己相反既約多項式が生成できる定理を復習する [11]．そして本論文では，自己相反変換を施される m 次既約多項式の零点集合が正規基底を成す場合には，変換により得られる $2m$ 次自己相反既約多項式の零点集合も正規基底を成していることを示す．

続いて前述の自己相反変換において，変換を施される既約多項式と得られる自己相反既約多項式が 1 対 1 の関係にあることを明らかにし，自己相反既約多項式には自己相反変換の逆変換（自己相反逆変換）が行えることを示す．そして自己相反逆変換により，$2m$ 次の自己相反既約多項式から m 次の既約多項式が生成できることを示し，1/2 倍の次数の既約多項式生成につながることを述べる．自己相反逆変換による 1/2 倍の次数の既約多項式生成の応用として，TypeII ONB を零点にもち，かつ素数次の既約多項式を生成する手法を与える．これは $2m$ 次の既約 AOP を簡単な条件判定により生成し，その既約 AOP に自己相反逆変換を施して m 次既約多項式が生成でき，これが TypeII ONB を零点にもち，m が素数ならば素数次の既約多項式の生成にもなるというものである．

以下特に断らない限り p を素数，素数位数 p の有限体を F_p，その m 次拡大体を F_{p^m} のように表し，多項式の零点は ω などのギリシャ文字を用いて表す．

2. 基礎的準備

本章では，自己相反多項式，自己相反既約多項式，高速演算可能な標数 2 の拡大体，及び高次であり素数次の既約多項式の生成について復習する．

2.1 自己相反多項式，自己相反既約多項式

自己相反多項式は，次のように定義されている [15]．

[定義 1] F_2 上の m 次多項式 $f(x)$ を次式で考える．

$$f(x)=\sum_{i=0}^{m} f_i x^i, \quad f_i \in F_2 \tag{1a}$$

上記の $f(x)$ に対して，次式で与えられる多項式 $f^*(x)$ のことを $f(x)$ の相反多項式と呼ぶ．

$$f^*(x)=x^m f(x^{-1})=\sum_{i=0}^{m} f_{m-i} x^i \tag{1b}$$

ここで，特に $f(x)=f^*(x)$ である多項式 $f(x)$ のことを自己相反多項式と呼び，既約である自己相反多項式のことを自己相反既約多項式と呼ぶ． □

式 (1b) から容易に理解できるように，$f(x)$ の零点を仮に ω とすれば $f^*(x)$ の零点は ω^{-1} で与えられる．自己相反多項式とは，ω 及びその逆元 ω^{-1} をともに零点としてもつ多項式として特徴づけられる．本論文で特に重要となる自己相反既約多項式の性質を以下に列挙しておく．これら性質の証明など，詳細については付録 **1.** を参照して頂きたい．

[性質 2] $x+1$ を除くすべての自己相反既約多項式は偶数次数の多項式である． □

[性質 3] 2 次以上の m 次自己相反既約多項式の零点 ω に対して $\omega^{-1}=\omega^{2^{m/2}}$ が成り立つ． □

2.2 高速演算可能な標数 2 の拡大体

標数が 2 であるか否かにかかわらず，拡大体の高速実装に関する研究のほとんどは，法多項式による多項式剰余算を高速に計算する方法を提案するものである．ここでは，標数を 2 とした場合に限定して，これまでに提案されている，多項式剰余算を高速に計算するのに効果的な法多項式などをいくつか紹介する．

2.2.1 既約 3，5 項式

標数を 2 とした拡大体の高速実装に関する研究報告の多くは既約 3，5 項式を用いる方法である [8], [15]．法多項式の項数を少なくすることによって，多項式剰余算をハード的にコンパクトに実装するというものである(注1)．既約 3 項式の方が，既約 5 項式に比べて計算効率が良くなるのはいうまでもないが，任意の次数に対して必ずしも既約 3 項式が存在するわけではない．暗号に用いる程度の高次の次数，より具体的には

(注1)：2，4 項式など，偶数項式は F_2 上で可約であることに注意する．

10000 次までの既約 3，5 項式が，これまでの研究成果として得られている [9].

2.2.2 既約 All One Polynomial と TypeIONB

次式で与えられるような，係数がすべて 1 である多項式を All One Polynomial（AOP）と呼ぶ [12].

$$f(x) = (x^{m+1} - 1)/(x - 1) \tag{2}$$

既約である場合には既約 AOP と呼ぶ．式 (2) の $f(x)$ を m 次既約 AOP とし，これを法多項式として F_{2^m} を高速実装する従来法 [12] では，$f(x)$ の零点 α により構成できる式 (3a) の正規基底及び式 (3b) の擬多項式基底が等価なものであることを利用し，式 (2) より成り立つ関係式 $\alpha^{m+1} = 1$ を効果的に用いて，拡大体上乗算及び文献 [16] のアルゴリズムを用いた逆元算出を実装している．

$$\{\alpha, \alpha^2, \alpha^{2^2}, \cdots, \alpha^{2^{m-1}}\} \tag{3a}$$

$$\{\alpha, \alpha^2, \alpha^3, \cdots, \alpha^m\} \tag{3b}$$

式 (3a) に示される既約 AOP の零点による正規基底が TypeIONB であり，上述のように拡大体上演算の高速実装に適している．本論文では，この既約 AOP が自己相反既約多項式のスペシャルケースであることに加えて，付録 **2.** に示すような非常に簡単な条件判定により得られることを利用する．

2.2.3 TypeIIONB [14]

2.1 の性質 2 で示したように，$x+1$ を除く自己相反既約多項式は，すべて偶数次数である．すなわち，2 次以上の既約 AOP はすべて偶数次数となり，このことに注意しながら，式 (3a) で与えられる TypeIONB に対して次式のような集合を考える．

$$\{\alpha + \alpha^{2^{m/2}}, \alpha^2 + \alpha^{2^{m/2+1}}, \cdots, \alpha^{2^{m/2-1}} + \alpha^{2^{m-1}}\} \tag{4a}$$

式 (3a)，式 (3b) 及び性質 3 を考慮すれば，式 (4a) は次式で与えられる集合と等価である．

$$\{\alpha + \alpha^{-1}, \alpha^2 + \alpha^{-2}, \cdots, \alpha^{m/2} + \alpha^{-m/2}\} \tag{4b}$$

ここで式 (4a) は，F_{2^m} の部分体 $F_{2^{m/2}}$ において正規基底をなし，かつ式 (4b) と等価になるということを用いて $F_{2^{m/2}}$ における演算を高速に実装することができ，これを用いた拡大体の高速実装に関する研究報告がなされている [14]．そして式 (4a) の正規基底は，TypeIIONB と呼ばれている．

2.3 素数次既約多項式の生成

1. にも述べたように，F_2 上の高次既約多項式の組織的な生成法に関する研究が広く行われている．これら従来研究の多くは変数変換を用いるものであり [10]，その問題点として合成数次の既約多項式しか生成できないということがある．一方暗号の分野においては，安全の確保のために素数次拡大体を定義体として用いるようにとの指摘もあり [6], [17]，高次でありかつ素数次である既約多項式の組織的な生成法が希求されている．このような要求に対しては，所望の素数次数の多項式をランダムに生成して，それを既約判定するという操作を，既約多項式が得られるまで繰り返して行うというのが現状である．

3. 自己相反変換と正規基底

本章ではまず，自己相反変換と呼ぶ多項式変換を紹介し，これを用いて 1 次係数が 1 である既約多項式から 2 倍の次数の自己相反既約多項式を生成する手法を紹介する [11], [18]．そして，自己相反変換を施される既約多項式の零点の共役集合が正規基底をなす場合は，変換により得られる自己相反既約多項式の零点の共役集合も正規基底を成すことを示す．

3.1 自己相反変換 [11]

次式で示されるような m 次多項式 $f(x)$ から $2m$ 次多項式 $F(x)$ への多項式変換 ψ を考え，

$$\psi : f(x) \to F(x) = x^m f(x + x^{-1}) \tag{5}$$

この変換 ψ を自己相反変換と呼ぶこととする．以下の議論を分かりやすくするために，式 (5) に示すように，自己相反変換を施される前の多項式をアルファベット小文字を用いて表し，それに対応する大文字を用いて変換後の多項式を表すこととする．例えば，自己相反変換を施される多項式 $f(x)$ を次のように考えれば，

$$f(x) = \sum_{i=0}^{m} f_i x^i, \quad f_i \in F_2 \tag{6a}$$

変換により得られる多項式 $F(x)$ は次のようになる．

$$F(x) = \sum_{i=0}^{m} f_i x^m (x + x^{-1})^i = \sum_{i=0}^{m} f_i x^{m-i} (x^2 + 1)^i \tag{6b}$$

式 (5) のように定義した自己相反変換 ψ に関して，次のような性質が成り立つ [11].

[性質 4] $f(x)$ の零点を ω としたとき，$\omega=\gamma+\gamma^{-1}$ を満たす γ は $F(x)$ の零点であり，逆に $F(x)$ の零点を γ とすると，$\omega=\gamma+\gamma^{-1}$ は $f(x)$ の零点となる．□

[性質 5] $F(x)$ はその零点 γ に対して γ^{-1} も零点としてもつことから，自己相反多項式となる．□

本論文で変換 ψ を自己相反変換と呼ぶ理由は，この変換 ψ に関して性質 5 が成り立つためである．自己相反変換により 2 倍の次数の自己相反既約多項式を生成する次の定理が知られている [11].

[定理 6] F_2 上の m 次既約多項式 $f(x)$ に対し，その自己相反変換後の多項式 $F(x)$ を次式で考える．

$$F(x)=x^m f(x+x^{-1}) \tag{7}$$

ここで $f(x)$ の 1 次係数が 1 であるときのみ，$F(x)$ は $2m$ 次自己相反既約多項式となる．□

定理 6 を用いた自己相反既約多項式の生成例を示す．

[例 7] 次式で与えられる F_2 上の 2 次既約多項式 $f(x)$ に対して，

$$f(x)=x^2+x+1 \tag{8}$$

次式の自己相反既約多項式 $F(x)$ が得られる．

$$F(x)=x^4+x^3+x^2+x+1 \tag{9}$$

この場合，$f(x), F(x)$ はともに既約 AOP である．□

例 7 からも分かるように，定理 6 を用いて生成される 2 倍の次数の自己相反既約多項式を，拡大体の高速実装を目的に法多項式として用いることは，例えば既約 3，5 項式のように項数が少なくなるとも限らないため，必ずしも得策であるとはいいがたい．

3.2 正規基底との関係

既約 AOP は自己相反既約多項式のスペシャルケースである．そこで既約 AOP が，TypeIONB という拡大体の高速実装の適した正規基底を零点にもつということに注目し，提案法により生成される自己相反既約多項式と正規基底の関係について考察した結果，次の補題が得られた．

[補題 8] 定理 6 を用いて生成される自己相反既約多項式 $F(x)$ の零点の共役集合が正規基底をなすことと，変換前の既約多項式 $f(x)$ の零点の共役集合が正規基底をなすことは必要十分条件である．□

詳しい証明については付録 **3.** を参照されたい．文献 [18] には自己相反変換により無限個の自己相反既約多項式を生成する定理が示されており，この定理と補題 8 を組み合わせることにより，正規基底を零点にもつ無限個の自己相反既約多項式が生成できることとなる．例 7 で用いた既約多項式 x^2+x+1 は零点の共役集合が正規基底をなしており，生成された自己相反既約多項式 $F(x)$ も正規基底を零点にもつ自己相反既約多項式となっている．この場合の $f(x), F(x)$ は，ともに既約 AOP であり TypeIONB を零点にもつ．

4. 自己相反逆変換と TypeIIONB

1 次の自己相反既約多項式 $x+1$ を除く，すべての自己相反既約多項式は偶数次数である．そして $x+1$ 以外のすべての自己相反既約多項式には **3.1** で定義した自己相反変換の逆変換（以下，自己相反逆変換）が可能であり，本章ではまずこれを示すことによって，自己相反変換前の既約多項式 $f(x)$ と変換後の自己相反既約多項式 $F(x)$ が 1 対 1 の関係にあることを述べ，これと併せて自己相反逆変換の具体的なアルゴリズムを示す．そして既約 AOP に対して自己相反逆変換を施すことにより，TypeIIONB を零点にもつ既約多項式の導出，更には素数次既約多項式の生成などが行えることを示す．これら応用を考えるのは，自己相反逆変換を施す自己相反既約多項式として既約 AOP を考えるからであり，既約 AOP を考えるのは，**2.2.2** 及び付録 **2.** から分かるように既約 AOP の生成に大した計算を要さないためである．

4.1 自己相反逆変換とそのアルゴリズム

詳しい証明は付録 **4.** に譲ることとして，すべての $2m$ 次自己相反既約多項式 $F(x)$ は，それに対応する m 次既約多項式 $f(x)$ に式 (5) の自己相反変換 ψ を施して生成できる．すなわち，$f(x)$ と $F(x)$ が自己相反変換に関して 1 対 1 の関係にあり，自己相反既約多項式 $F(x)$ に自己相反逆変換 ψ'：

$$\psi' : F(x)=x^m f(x+x^{-1}) \to f(x) \tag{10}$$

を施せば自己相反変換前の既約多項式 $f(x)$ が求められる．まず式 (6b) に注目すれば，$F(x)$ から $f(x)$ を求めるには，式 (6b) の係数情報 f_i が求まればよいことが分かる．10 進数を 2 進数に変換する方法に着想を得て，式 (6b) が x^2+1 を基底とする表現であると考えれば，以下のような自己相反逆変換のアルゴリズムを考えることができる．

【自己相反逆変換アルゴリズム】

Input: F_2 上の $2m$ 次自己相反既約多項式 $F(x)$

Output: F_2 上の m 次既約多項式 $f(x)$
Step1: $A(x) \leftarrow F(x)$, $R(x) \leftarrow 0$, $i \leftarrow 0$
Step2: $R(x) \leftarrow A(x) \pmod{x^2+1}$
Step3: $R(x) = 0$ ならば $f_i \leftarrow 0$ とし，それ以外であるならば $f_i \leftarrow 1$ とする．
Step4: $A(x) \leftarrow (A(x) - f_i x^{m-i})/(x^2+1)$
Step5: $i \leftarrow i+1$
Step6: $i < m$ ならば Step2，$i = m$ ならば終了．

上記アルゴリズムについて若干説明すると，例えばアルゴリズムを $i = s < m$ まで回した後の Step2 における $A(x)$ は次のような形になる．

$$A(x) = \sum_{i=s+1}^{m} f_i x^{m-i}(x^2+1)^i + f_s x^{m-s} \quad (11)$$

すなわち，Step2 で x^2+1 で剰余をとることにより式 (11) 右辺の第 1 項が消え，$f_s x^{m-s} \pmod{x^2+1}$ の値が $R(x)$ に代入されることとなる．これに以下の関係を踏まえることにより，Step3 のようにして係数情報 f_s が得られることとなる．

$$x^{m-s} \pmod{x^2+1} = \begin{cases} 1 & m-s: \text{偶数} \\ x & m-s: \text{奇数} \end{cases} \quad (12)$$

付録 **4.** に示したように自己相反変換が 1 対 1 変換であり，自己相反逆変換の操作を上記のような過程で行うことから，Step3 における $R(x)$ は $x+1$ には決してならない．そして補題 8 により，自己相反既約多項式 $F(x)$ が正規基底を零点にもつ場合には，これに自己相反逆変換を施して求められる既約多項式 $f(x)$ も正規基底を零点としてもつ．

4.2 TypeII ONB を零点にもつ既約多項式

ここでは，TypeIIONB を零点にもつ既約多項式の導出について考える．これは造作のないことで，既約 AOP に自己相反逆変換を施すだけである．例を用いて説明すると，10 次既約 AOP：

$$F(x) = (x^{11}-1)/(x-1) \quad (13a)$$

に前節で提案したアルゴリズムを用い自己相反逆変換して，以下のように 5 次既約多項式 $f(x)$ を得る．

$$f(x) = x^5 + x^4 + x^2 + x + 1 \quad (13b)$$

$F(x)$ 及び $f(x)$ の零点集合を考えれば，$F(x)$ の一つの零点を γ として，以下に示す γ の F_2 に関する共役集合は TypeIONB をなす．

$$\{\gamma, \gamma^2, \cdots, \gamma^{2^9}\} \quad (14a)$$

これに対して $f(x)$ の一つの零点を ω として，以下に示されるような関係が成り立ち，ω の F_2 に関する共役集合が TypeIIONB をなすこととなる．

$$\begin{aligned} &\{\omega, \omega^2, \cdots, \omega^{2^4}\} \\ &= \{\gamma+\gamma^{2^5}, \gamma^2+\gamma^{2^6}, \cdots, \gamma^{2^4}+\gamma^{2^9}\} \\ &= \{\gamma+\gamma^{-1}, \gamma^2+\gamma^{-2}, \cdots, \gamma^{2^4}+\gamma^{-2^4}\} \end{aligned} \quad (14b)$$

従来の TypeIIONB を用いた拡大体上演算の高速実装に関する研究は，**2.2.3** で示した式 (4a) と式 (4b) が等価である関係を用いるものばかりである [2], [14]．本論文により TypeIIONB を零点にもつ既約多項式が求められることにより，文献 [19] の手法のような TypeI 及び TypeIIONB を併用するような実装研究に対しての更なる高速化が期待できる．

4.3 素数次既約多項式の生成

素数次既約多項式の生成であるが，先に示した 10 次既約 AOP に対する自己相反逆変換の例から分かるように，この例では式 (13b) に示される 5 次既約多項式が生成できている．既約 AOP は自己相反既約多項式であるから偶数次数であり，これを $2m$ とすれば，自己相反逆変換により m 次の既約多項式が生成され，もし仮に m が素数であるとすれば素数次既約多項式の生成になるというものである．したがって，生成される素数次の既約多項式の零点は，前節の議論より TypeII ONB をなすこととなる．

表 1 に，五つの素数次数を具体的に設定し，一つの素数次既約多項式を得るのに必要となる平均の計算時間を，**2.3** で紹介した既約判定を用いる場合と，提案法を用いる場合とで比較した結果を示す．図 1 は表 1 の結果をグラフにしたものである．計算機には PentiumIII (2.66 GHz) を用い，プログラミングには Visual C++を用いた．既約判定には，NTL (A Library for

表 1 素数次数の既約多項式の生成に要する計算時間 [単位：ms]
Table 1 Computation time for generating a prime degree irreducible polynomial [unit:ms].

degree	DDF	proposed method
113	2.66	0.62
233	11.1	1.38
293	22.5	2.01
509	73.1	4.95
641	187.5	7.26

* CPU：PentiumIII (2.66 GHz)

表 2　生成可能な素数次数
Table 2　Possible prime degree.

range	possible prime degree
10 ～	29, 41, 53, 89
100 ～	113, 173, 233, 281, 293, 509, 593, 641, 653, 761, 809, 953
1000 ～	1013, 1049, 1229, 1289, 1409, 1481, 1601, 1733, 1889, 1901, 1973, 2069, 2129, ···
10000 ～	10061, 10253, 10313, 10529, 10589, 10613, 10709, 10733, 10781, 11321, 11369, ···

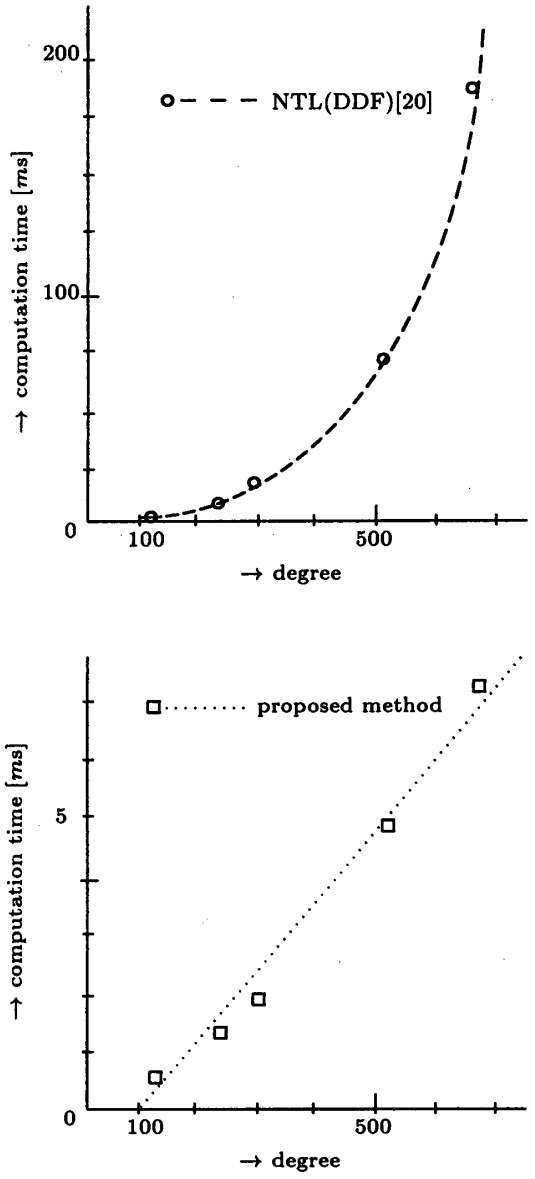


図 1　素数次数の既約多項式の生成に要する計算時間
Fig. 1　Computation time for generating a prime degree irreducible polynomial.

doing Number Theory) [20] にある既約判定関数を用いた．なお NTL の既約判定関数は，DDF (Distinct Degree Factorisation) [21], [22] をベースにしている．

これらのデータから，本論文の提案法の方が，高次かつ素数次の既約多項式を高速に生成できることが分かる．既約判定を用いた場合は，次数が上がるにつれて指数関数的に必要となる計算時間が増えていくのに対し，提案法はそのようなことはなく，次数が高いほど提案法の方が優れていることが分かる．本論文を通して繰り返し述べていることではあるが，既約 AOP は付録 **2.** に示すような非常に簡単な条件判定により得られるため，素数次でありかつ高次の既約多項式を生成する上で，提案法は有効な手段となる．

最後に，既約 AOP に自己相反逆変換を施すことによって得られる素数次の既約多項式の例を，表 2 に示す．なお，これら素数次の既約多項式についても，その零点の共役集合が TypeIIONB になることに注意して頂きたい．

5. むすび

本論文では，既約 AOP が TypeIONB を零点とする拡大体上演算の高速実装に非常に適した既約多項式であることに加え，自己相反既約多項式でもあるということに着目した．そして，m 次多項式から $2m$ 次自己相反多項式を得る変換手法（自己相反変換）を紹介し，1 次係数が 1 である m 次既約多項式から，$2m$ 次の自己相反既約多項式を生成する定理を復習した．そして本論文では，自己相反変換を施される m 次既約多項式の零点集合が正規基底をなす場合には，変換により得られる $2m$ 次自己相反既約多項式の零点集合も正規基底をなしていることを示した．

続いて自己相反変換において，変換を施される既約多項式と得られる自己相反既約多項式が 1 対 1 の関係にあることを明らかにし，自己相反既約多項式には自己相反変換の逆変換（自己相反逆変換）が行えることを示した．そして自己相反逆変換により，$2m$ 次の自己相反既約多項式から m 次の既約多項式が必ず生成されることを示し，1/2 倍の次数の既約多項式生成につながることを述べた．自己相反逆変換による 1/2 倍の次数の既約多項式生成の応用として，$2m$ 次の既約 AOP を簡単な条件判定により生成し，これに自己相反逆変換を施すことにより，TypeII ONB を零点にも

つ既約多項式，及び素数次の既約多項式を生成する手法を与えた．

文　献

[1] P. Loshin, 暗号化によるセキュリティ対策ガイド，翔泳社，1999.

[2] I. Blake, G. Seroussi, and N. Smart, Elliptic Curves in Cryptography, LNS 265, Cambridge University Press, 1999.

[3] A. Lenstra and E. Verheul, "The XTR public key system," Proc. Crypto 2000, LNCS 1880, pp.1–20, 2000.

[4] D. Han, K. Yoon, Y. Park, C. Kim, and J. Lim, "Optimal extension fields for XTR," Proc. SAC2002, LNCS 2595, pp.369–384, 2003.

[5] T. Kobayashi, K. Aoki, and F. Hoshino, "OEF using a successive extension," Proc. 2000 Symposium on Cryptography and Information Security, no.B02, 2000.

[6] C. Diem, "The GHS-attack in odd characteristic," Preprint,2002. http://www.exp-math.uni-essen.de/~diem

[7] C. Paar and P.S. Rodriguez, "Fast arithmetic architectures for public-key algorithms over galois fields $GF((2^n)^m)$," Proc. Eurocrypto '97, LNCS 1233, pp.363–378, 1997.

[8] D. Hankerson, J.L. Hernandez, and A. Menezes, "Software implementation of elliptic curve cryptography over binary fields," CT-RSA 2001, Lecture Notes in Computer Science, pp.250–265, 2001.

[9] G. Seroussi, "Table of low-weight binary irreducible polynomials," HPL-98-135, Hewlett Packard, 1998.

[10] 野上保之，田中　清，杉村立夫，大下眞二郎，"変数変換 $x^P - x + s$ による無限個の既約多項式の導出，" 信学論 (A)，vol.J82-A, no.4, pp.587–590, April 1999.

[11] H. Meyn, "On the construction of irreducible self-reciprocal polynomials over finite fields," Appl. Alg. in Eng., Commun. and Comput., vol.1, pp.43–53, 1990.

[12] Y. Nogami, A. Saito, and Y. Morikawa, "Finite extension field with modulus of all-one polynomial and representation of its elements for fast arithmetic operations," IEICE Trans. Fundamentals, vol.E86-A, no.9, pp.2376–2387, Sept. 2003.

[13] J. Silverman, "Fast multiplication in finite fields GF(2^N)," CHES'99, pp.122–134, 1999.

[14] B. Sunar and C. Koc, "An efficient optimal normal basis type II multiplier," IEEE Trans. Comput., vol.50, no.1, pp.83–87, 2001.

[15] R. Lidl and H. Niederreiter, Finite Field, Encyclopedia of Mathematics and Its Applications, Cambridge University Press, 1984.

[16] T. Itoh and S. Tsujii, "A fast algorithm for computing multiplicative inverses in $GF(2^m)$ using normal bases," Inf. Comput., vol.78, pp.171–177, 1988.

[17] M. Ciet, J. Quisquater, and F. Sica, "A secure family of composite finite fields suitable for fast implementation of elliptic curve cryptography," INDOCRYPT 2001, pp.108–116, 2001.

[18] A. Menezes (ed), Applications of Finite Fields, Kluwer Academic Press, 1993.

[19] 藤井吉弘，野上保之，森川良孝，"楕円曲線暗号への利用を目的とした拡大体 F_{2m} の高速実装，" 2003 年暗号と情報セキュリティシンポジウム (SCIS2003) 予稿集 vol.II of II, pp.765–770, 2003.

[20] A Library for doing Number Theory. http://www.shoup.net/ntl/

[21] S. Gao, "Deterministic distinct-degree factorisation of polynomials over finite fields," J. Symbolic Computation. http://www4.ncsu.edu/ kalto-fen/bibliography/01/GKL01.pdf

[22] S. Gao, "On the deterministic complexity of factoring polynomials," J. Symbolic Computation. http://citeseer.nj.nec.com/gao99deterministic.html

[23] 杉村立夫，末次康徳，"既約多項式の導出に関する一考察，" 信学技報，IT89-61, 1989.

[24] 杉村立夫，笠原正雄，滑川敏彦，"加法表を用いた有限体上における加法演算に関する考察，" 信学論 (A)，vol.J64-A, no.12, pp.1034–1041, Dec. 1981.

[25] 杉村立夫，末次康徳，"既約円周等分多項式に関する考察，" 信学論 (A)，vol.J73-A, no.12, pp.1929–1935, Dec. 1990.

[26] R. Mullin, I. Onyszchuk, S. Vanstone, and R. Wilson, "Optimal normal basis in $GF(p^n)$," Discrete Applied Math., vol.22, pp.149–161, 1988/1989.

付　録

1. 自己相反既約多項式の性質の証明

性質 2 については，奇数次の自己相反既約多項式 $f(x)$ を考えた場合，自己相反でありかつ奇数次であることから係数が非零である項の数は偶数となる．すなわち，標数が 2 であることに注意すれば，$f(1) = 0$ が成り立ち，$f(x)$ が $x-1$ を因数にもつこととなるから，$f(x)$ が既約であることに矛盾する．したがって，自己相反既約多項式は偶数次でなければならない．

続いて性質 3 については，m 次自己相反既約多項式 $f(x)$ の零点 ω に対して，ω^{-1} も $f(x)$ の零点となるから ω^{-1} は ω の共役元となるので，次式のように書くことができる．

$$\omega^{-1} = \omega^{2^n}, \quad 0 \le n \le m-1. \qquad \text{(A·1)}$$

今 $n \neq m/2$ と仮定する．ここで，性質 2 より m が偶数であることに注意して頂きたい．式 (A·1) の関係を用いれば，ω^{-1} の 2^n 乗は次式に示すように ω にならなければならない．

$$\left(\omega^{-1}\right)^{2^n} = \left(\omega^{2^n}\right)^{-1} = \left(\omega^{-1}\right)^{-1} = \omega \qquad \text{(A·2)}$$

しかし式 (A·1) 右辺の ω^{2^n} の 2^n 乗を考えると，以下に示すように ω にはならない．

$$\left(\omega^{2^n}\right)^{2^n} = \omega^{2^{2n}} \neq \omega, \qquad \text{(A·3)}$$
$$0 \leq 2n \neq m \leq 2m-2$$

以上より，$n = m/2$，すなわち $\omega^{-1} = \omega^{2^{m/2}}$ となる．なお，自己相反既約多項式の厳密な個数に関しては，文献 [24] の付録を参照されたい．

2. 任意次数の AOP に対する既約判定

任意次数の AOP に対し，それが既約であるか否かを判定する方法について，まず文献 [25], [26] にある次の定理を引用して紹介することとする．

[定理 9] p 及び $m+1$ を相異なる素数であるとする．このとき F_{m+1} において非零元 p が原始元となることは，F_p 上の m 次 AOP：

$$(x^{m+1}-1)/(x-1) \qquad \text{(A·4)}$$

が既約であることの必要十分条件である． □

本論文で取り扱うのは標数 p が 2 である場合であり，式 (A·4) の m 次 AOP が既約となるためには，素数 $m+1$ を法として 2 の位数を求め，これが m になればよいこととなる．この条件判定は複雑な計算を要さずに行えるため，任意次数の AOP に対する既約判定法として十分に実用的と考える．

3. 補題 8 の証明

まず，m 次既約多項式 $f(x)$ の零点を ω として，ω の F_2 に関する共役集合：

$$\{\omega, \omega^2, \cdots, \omega^{2^{m-1}}\} \qquad \text{(A·5)}$$

が正規基底をなす場合について考える．なお，$f(x)$ の 1 次係数は定理 6 の条件を満たすように 1 であるものとする．このとき，$f(x)$ に自己相反変換を施して得られる $2m$ 次の自己相反既約多項式 $F(x)$ の零点を γ とすれば，ω 及び γ は性質 4 の関係を満たす．そして，$F(x)$ の零点 γ の共役集合：

$$\{\gamma, \gamma^2, \cdots, \gamma^{2^{2m-1}}\} \qquad \text{(A·6)}$$

が正規基底をなすか否かについて考えてみる．仮に正規基底をなさない場合，式 (A·6) の共役集合に対して 1 次従属な関係が成り立つこととなり，次式を満たす非零の係数 c_i が存在することとなる．

$$\sum_{i=0}^{2m-1} c_i \gamma^{2^i} = 0, \quad c_i \in F_2 \qquad \text{(A·7)}$$

上式を 2^m 乗することで次式を得る．

$$\sum_{i=0}^{m-1} c_{i+m} \gamma^{2^i} + \sum_{i=m}^{2m-1} c_{i-m} \gamma^{2^i} = 0 \qquad \text{(A·8)}$$

ここで $\gamma^{2^{2m}} = \gamma$ であることに注意する．式 (A·7) 及び式 (A·8) を辺々加え合わせ，性質 3 及び性質 4 の関係を用いれば次式が得られる．

$$\sum_{i=0}^{m-1} (c_i + c_{i+m}) \omega^{2^i} = 0 \qquad \text{(A·9)}$$

ここで $\omega^{2^m} = \omega$ であることに注意する．上式を満たすためには，標数が 2 である拡大体を取り扱っていること，ω の共役集合が正規基底をなすと仮定していることに注意して，次式が成り立つ必要がある．

$$c_i = c_{i+m}, \quad i = 0, 1, \cdots, m-1 \qquad \text{(A·10)}$$

式 (A·10) の関係を式 (A·7) に代入して次式を得る．

$$\sum_{i=0}^{m-1} c_i (\gamma^{2^i} + \gamma^{2^{i+m}}) = 0 \qquad \text{(A·11)}$$

ここで $F(x)$ が自己相反既約多項式であることに注意すれば，性質 3 及び性質 4 より次式が成り立ち，

$$\gamma^{2^i} + \gamma^{2^{i+m}} = \gamma^{2^i} + \gamma^{-2^i} = \omega^{2^i} \qquad \text{(A·12)}$$

これを式 (A·11) に代入して次式が成り立つことから，

$$\sum_{i=0}^{m-1} c_i \omega^{2^i} = 0 \qquad \text{(A·13)}$$

式 (A·10) の関係を用いていることに注意をすれば，式 (A·13) は正規基底をなすと仮定している ω の共役集合に 1 次従属な関係が成り立つことを示す式であり矛盾となる．すなわち，生成される自己相反既約多項式 $F(x)$ の零点 γ の共役集合もまた正規基底をなす．

なお，この逆の証明については，ω の共役集合が 1 次従属であることを仮定すれば，γ の共役集合も 1 次従属となることを簡単に示すことができる．また付録 **3.** の冒頭で式 (A·5) が正規基底の場合としているが，これは ω の F_2 に関するトレースの値が 1 であることの十分条件である [15]．

4. 自己相反既約多項式に対する自己相反逆変換

すべての $2m$ 次自己相反既約多項式 $F(x)$ には，式 (10) に示される自己相反変換の逆変換 ψ' ができることを示す．まず，$F(x)$ が自己相反既約多項式であることから，その零点 γ の共役集合を用いて次のような式展開が行える．式展開には性質 3 を用いた．

$$\begin{aligned} F(x) &= \prod_{i=0}^{2m-1}(x-\gamma^{2^i}) \\ &= \prod_{i=0}^{m-1}(x-\gamma^{2^i})(x-\gamma^{2^{m+i}}) \\ &= \prod_{i=0}^{m-1}(x-\gamma^{2^i})(x-\gamma^{-2^i}) \\ &= \prod_{i=0}^{m-1}\{x^2-(\gamma^{2^i}+\gamma^{-2^i})x+1\} \end{aligned} \quad \text{(A·14)}$$

式 (A·14) に $\omega=\gamma+\gamma^{-1}$ を代入して次式を得る．

$$F(x)=x^m\prod_{i=0}^{m-1}(x+x^{-1}-\omega^{2^i}) \quad \text{(A·15)}$$

$F(x)$ は $2m$ 次自己相反既約多項式であり，性質 3 を用いて次式が得られるから，ω は F_{2^m} の元である．

$$\begin{aligned} \omega^{2^m} &= (\gamma+\gamma^{-1})^{2^m} \\ &= (\gamma+\gamma^{2^m})^{2^m} \\ &= \gamma^{2^m}+\gamma \\ &= \gamma^{-1}+\gamma=\omega \end{aligned} \quad \text{(A·16)}$$

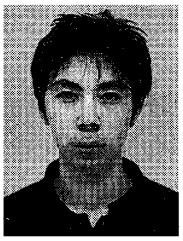
ここで ω を F_{2^m} の真部分体の元であると仮定すると，式 (A·15) に ω の共役集合が複数回含まれることとなり，$F(x)$ が既約であることに矛盾する．すなわち，ω は F_{2^m} の真部分体には属さない．したがって，ω の最小多項式は F_2 上の適当な m 次既約多項式であり，これを $f(x)$ とすれば，式 (A·15) より次式を得る．

$$F(x)=x^m f(x+x^{-1}) \quad \text{(A·17)}$$

以上より，$2m$ 次の自己相反既約多項式 $F(x)$ に逆変換 ψ' が行えるとともに，その結果が $\omega=\gamma+\gamma^{-1}$ を零点にもつ m 次既約多項式 $f(x)$ になることが分かる．

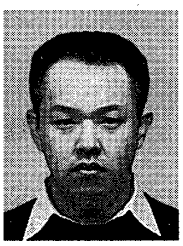
なお，式 (A·17) を満たす $2m$ 次の自己相反既約多項式 $F(x)$ と m 次既約多項式 $f(x)$ が 1 対 1 の関係にあることは，次のように理解できる．まず $F(x)$ は，$f(x)$ に対して変数変換を施すことにより一意に求まる多項式である．一方 $f(x)$ は，$F(x)$ の零点 γ に対して一意に計算される元 $\omega=\gamma+\gamma^{-1}$ の最小多項式であり，$F(x)$ に対して一意に決まる多項式である．

（平成 15 年 5 月 12 日受付，12 月 4 日再受付，
16 年 3 月 18 日最終原稿受付）



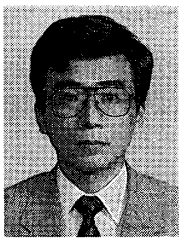
牧田　慶

2002 信州大・工・電気電子卒．同年，同大大学院博士前期課程入学．有限体理論に関する研究に従事．



野上　保之　（正員）

1994 信州大・工・電気電子卒．1999 同大大学院博士後期課程了．同年，岡山大学工学部助手．博士（工学）．有限体基礎理論，情報セキュリティに関する研究に従事．IEEE，情報理論とその応用学会各会員．



杉村　立夫　（正員）

昭 51 阪大・工・通信卒．昭 57 同大大学院博士後期課程了．工博．同年松下電器産業(株)入社．昭 60 福岡工大助教授．平 3 信州大・工・電気電子工学科助教授，現在，同教授．誤り訂正符号の構成及びその応用，有限体理論，情報セキュリティに関する研究に従事．情報理論とその応用学会，IEEE 各会員．