International Electronic Journal of Pure and Applied Mathematics
Volume 4 No. 2 2012, 59-70

A NOTE ON IDENTIFICATION OF IRREDUCIBLE POLYNOMIALS OF OVER $\mathbb{F}_2$

R.K. Sharma[1], Wagish Shukla[2], S. Ramasamy[3] §
[(1,2,3)]Department of Mathematics
IIT Delhi
New Delhi, 110016, INDIA

Abstract: We study the structure of $\mathbb{F}_{2^n}$ visualized in [3] and completely characterize the elements of the structure. We devise a method to identify irreducible polynomials of degree n as an application and show that large structure can be split into small parts for the purpose of identifying irreducible polynomials.

AMS Subject Classification: 11T06
Key Words: finite field, irreducible polynomials, trace, conjugate

1. Introduction

This paper is organized in the following manner. In this section, we give some preliminary concepts. In Section 2, we completely characterize the structure introduced in [3] and devise a method to identify irreducible polynomials of degree n. Section 3 concludes the paper.

1.1. Preliminaries

Irreducible polynomial plays an important role in determination of extension fields and designing of cryptographic algorithms. A polynomial $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ is said to be irreducible over a field K if it can not be factored into two non-constant polynomials, that is , whenever $f(x) = g(x)h(x)$ with $g, h \in K[x]$, then either g or h is a constant polynomial. If $a_n = 1$, then $f(x)$ is called a monic irreducible polynomial.

Received: May 24, 2011

§Correspondence author

International Electronic Journal of Pure and Applied Mathematics – IEJPAM, Volume 4, No. 2 (2012)

If L, considered as a vector space over K, is finite-dimensional, then L is called a finite extension of K. The dimension of the vector space L over K is then called the degree of L over K and denoted by $[L : K]$. If L is a finite extension of K and M is a finite extension of L, then M is a finite extension of K with $[M : K] = [M : L][L : K]$.

Let K be any subfield of a finite field F. Then K and F can be denoted by $K = \mathbb{F}_q$ and $F = \mathbb{F}_{q^m} = K[x]/(f(x))$ where $f(x)$ is an irreducible polynomial of degree m for some positive integer m. m is called the degree of F over K treating K and F as vector spaces and is denoted by $m = [F : K]$. If q is prime, then K is called a prime field and K and F are said to be of characteristic q.

Let $\mathbb{F}_q^*$ be any finite field. Then generator of the cyclic group $\mathbb{F}_q^*$ is called a primitive element of $\mathbb{F}_q$. If F is an extension field of K of degree m, then a basis of F over K of the form $\{\alpha, \alpha^q, \alpha^{q^2} \cdots \alpha^{q^{m-1}}\}$, consisting of a suitable element $\alpha \in F$ and its *conjugates* $\alpha, \alpha^q, \alpha^{q^2}, \alpha^{q^3}, \cdots, \alpha^{q^{m-1}}$ with respect to K, is called normal basis of F over K. If α is a root of an irreducible polynomial of degree m over K, then $\{1, \alpha, \alpha^2, \cdots \alpha^{m-1}\}$ is called a polynomial basis of F over K with respect to α. We can directly construct polynomial basis from a root of irreducible polynomial and normal basis from a root of *suitable* irreducible polynomial. For details on finite fields and definitions on related concepts, see [1] and for details on cryptographic algorithms, see [2] and [4].

For β in F, the trace of β, denoted by $Tr_{F/K}(\beta)$, is defined as $Tr_{F/K}(\beta) = \beta + \beta^q + \beta^{q^2} + \beta^{q^3} \cdots + \beta^{q^{m-1}}$. All the roots of an irreducible polynomial have the same trace value.

For details on vector space, dimension, basis, etc., see [**?**]. For definition and details on finite fields, see [1].

1.2. On Structure

The following structure is due to [3].

1.2.1. Structure of Nonzero Elements of $\mathbb{F}_{2^n}^*$

For any fixed primitive element α of $\mathbb{F}_{2^n}$, the following array gives a structure of nonzero elements of $\mathbb{F}_{2^n}^*$.

α															
α^2								α^3							
α^{2^2}				α^5				α^6				α^7			
α^{2^3}		α^9		α^{10}		α^{11}		α^{12}		α^{13}		α^{14}		α^{15}	
α^{2^4}	α^{17}	α^{18}	α^{19}	α^{20}	α^{21}	α^{22}	α^{23}	α^{24}	α^{25}	α^{26}	α^{27}	α^{28}	α^{29}	α^{30}	α^{31}
α^{32}	$\cdots$	$\cdots$	$\cdots$												

Figure 1: Structure of $\mathbb{F}_{2^n}^*$

$\vdots$

For the structure of the elements of $\mathbb{F}_{3^n}^*$ in terms of their traces over $\mathbb{F}_3$, see [3]

International Electronic Journal of Pure and Applied Mathematics – IEJPAM, Volume 4, No. 2 (2012)

Notation (see [3]) Let $\mathbb{F}_{2^t}$ be any finite field and let $n \in \mathbb{N}$ be such that $n < 2^t$ and $2^m + 1 \leq n \leq 2^m + 2^m$, let $n = n_0 + R$ where $n_0 = 2^m$ for some unique $m \in \mathbb{N}$.

Let $X_i(m)$ denote the set of all columns of length i (Number of elements in column i) in [1, $2^m - 1$]. Let $X_i^{'}$ denote the set of all columns of length i in [1, $2^m + R - 1$],

let $X(m)$ denote the set of all columns (of possible length) in [1, $2^m - 1$] and let $X^{'}$ denote the set of all columns (of possible length) in [1, $2^m + R - 1$].

For a real number $s \geq 0$, let $\lfloor s \rfloor$ denote the integral part of s.

Theorem 1.1. (see [3]) *(i) For* $1 \leq i \leq m-1$, $\mid X_i^{'} \mid = \mid X_i(m) \mid + \lfloor \frac{R-1+2^{i-1}}{2^i} \rfloor - \lfloor \frac{R-1+2^i}{2^{i+1}} \rfloor$ *for* $1 \leq R \leq 2^m$.

(ii) For $m \leq i \leq m+1$, $\mid X_i^{'} \mid = \mid X_i(m') \mid + \lfloor \frac{R-1+2^{i-1}}{2^i} \rfloor - \lfloor \frac{R-1+2^i}{2^{i+1}} \rfloor$ *for* $1 \leq R \leq 2^m$.

We have already introduced an idea of identifying some irreducible polynomials in [3]. As an improved version, we have completely characterized the elements of the finite field $\mathbb{F}_{2^n}^*$ and we show in this paper that it is possible to identify all irreducible polynomials of degree n over $\mathbb{F}_2$.

It is easily seen that "conjugate" is an equivalence relation. Similarly, we define a relation with the condition that that two elements are related if and only if both the elements are in the same column. Classes in the latter case are called "column class" or "column". We fix α as mentioned in the structure and use $[\alpha^k]$ and $[[k]]$ interchangeably to denote the conjugate class $[\alpha^k]$. Let $[[[i]]]$ denote the column containing α^i.

The notations $[[k]]$ and $[[[i]]]$ are used instead of $[k]$ and $[i]$ to avoid confusion with "reference citation". Note that $\alpha^{t \times 2^i}$ is a conjugate of α^t for any integer $i \geq 0$ and $[\alpha^t] = [[t]] = [[t \times 2^i]] = [\alpha^{t \times 2^i}]$ for $i \geq 0$. Note also that $[[0]] = [[2^n - 1]]$ and $[[-i]] = [[2^n - 1 - i]]$.

Hereafter, we take i and j as nonnegative integers until otherwise stated.

2. Characterization of Elements of the Structure

In Section 2.1, we show the correspondence of elements of the n^{th} row from the beginning starting from $\alpha^{2^{n-1}}$ onwards with the elements of various other rows. In Section 2.2, we show the correspondence of elements of the n^{th} row from the end starting from $\alpha^{2^n} - 1$ in the reverse order with the elements of various other rows. In Section 2.3, we show the correspondence of elements at each column with the elements of n^{th} row.

International Electronic Journal of Pure and Applied Mathematics – IEJPAM, Volume 4, No. 2 (2012)

2.1. Conjugates of Elements in the n^{th} row from the beginning

We consider the n^{th} row and link values of the trace of the elements with different columns. This links all the new columns introduced up to the $(n-1)^{th}$ row and gives conjugates of every element in the n^{th} row.

Proposition 2.1.

$$\alpha^{2^{n-1}+r} \text{ and } \alpha^{2r+1} \text{ are in the same conjugate class,} \tag{1}$$

for any non-negative integer $r = 0, 1, 2, 3, \cdots, 2^{n-1} - 1$.

Proof. $[\alpha^{2^{n-1}+r}] = [(\alpha^{2^{n-1}+r})^2] = [\alpha^{2^n+2r}] = [\alpha^{2^n}\alpha^{2r}] = [\alpha^{2r+1}]$.
This completes the proof. □

This proposition shows that n^{th} row covers all the columns, that is, n^{th} row alone can describe the entire structure. This result is true for any integer $r \geq 0$. However, the result for the values $r = 0, 1, 2, 3, \cdots, 2^{n-1} - 1$ itself links all the elements of the structure.

Classes of type $[[2^{n-1} + r]]$ for $r = 1, 2, \cdots, 2^{n-1} - 1$: For the sake of clarity, we use α initially in the classes and then we use the equivalent notation. From the above result, we get the conjugates of every element in the n^{th} row in the following way.

When $r = 0$, $[\alpha^{2^{n-1}}] = [\alpha^1] = [\alpha^{2^n}]$.
The length of $[[[1]]]$ is n and there are n conjugates of $\alpha^{2^{n-1}}$ in $[[[1]]]$.
When $r = 1$, $[\alpha^{2^{n-1}+1}] = [\alpha^3] = [\alpha^{2^{n-1}+2^{n-2}}]$.
The length of $[[[3]]]$ is $n-1$ and there are $n-1$ conjugates of $\alpha^{2^{n-1}+1}$ in $[[[3]]]$.
When $r = 2$, $[\alpha^{2^{n-1}+2}] = [\alpha^5] = [\alpha^{2^{n-1}+2^{n-3}}]$.
The length of $[[[5]]]$ is $n-2$ and there are $n-2$ conjugates of $\alpha^{2^{n-1}+2}$ in $[[[5]]]$.
When $r = 3$, $[\alpha^{2^{n-1}+3}] = [\alpha^7] = [\alpha^{2^2+2^1+1}] = [\alpha^{2^{n-1}+2^{n-2}+2^{n-3}}]$.
The length of $[[[7]]]$ is $n-2$ and there are $n-2$ conjugates of $\alpha^{2^{n-1}+3}$ in $[[[7]]]$.
When $r = 4$, $[[2^{n-1}+4]] = [[9]] = [[2^3+1]] = [[2^{n-1}+2^{n-4}]]$.
The length of $[[[9]]]$ is $n-3$ and there are $n-3$ conjugates of $\alpha^{2^{n-1}+4}$ in $[[[9]]]$.
When $r = 5$, $[[2^{n-1}+5]] = [[11]] = [[2^3+2^1+1]] = [[2^{n-1}+2^{n-3}+2^{n-4}]]$.
The length of $[[[11]]]$ is $n-3$ and there are $n-3$ conjugates of $\alpha^{2^{n-1}+5}$ in $[[[11]]]$.
When $r = 6$, $[[2^{n-1}+6]] = [[13]] = [[2^3+2^2+1]] = [[2^{n-1}+2^{n-2}+2^{n-4}]]$.
The length of $[[[13]]]$ is $n-3$ and there are $n-3$ conjugates of $\alpha^{2^{n-1}+6}$ in $[[[13]]]$.
$\vdots$
When $r = 2^{n-2} - 1$, $[[2^{n-1}+2^{n-2}-1]] = [[2^{n-1}-2+1]] = [[2^{n-1}-1]]$.
It is easily seen that the length of $[[[2^{n-1}-1]]]$ is $n - \lfloor log_2(2^{n-1}-1) \rfloor = 2$.
There are 2 conjugates of $\alpha^{2^{n-1}+2^{n-2}-1}$ in $[[[2^{n-1}-1]]]$.
$\vdots$
When $r = 2^{n-1} - 2$, $[[2^{n-1}+2^{n-1}-2]] = [[2^n-4+1]] = [[2^n-3]]$.

International Electronic Journal of Pure and Applied Mathematics – IEJPAM, Volume 4, No. 2 (2012)

It is easily seen that the length of $[[[2^n-3]]]$ is $n-\lfloor log_2(2^n-3)\rfloor = 1$.
The element in the column $[[[2^n-3]]]$ is a conjugate of $\alpha^{2^{n-1}+2^{n-1}-2}$.
When $r = 2^{n-1}-1$, $[[2^{n-1}+2^{n-1}-1]] = [[2^n-2+1]] = [[2^n-1]]$.
It is easily seen that the length of $[[[2^n-1]]]$ is $n-\lfloor log_2(2^n-1)\rfloor = 1$.
The element in the column $[[[2^n-1]]]$ is a conjugate to itself.

In general, the length of any column $[[[2r+1]]]$ corresponding to class $[[2^{n-1}+r]]$ is $n-\lfloor log_2(2r+1)\rfloor$ where $log_2(x)$ denotes logarithmic value of any positive real number x to the base 2 and $\lfloor s\rfloor$ denotes the greatest nonnegative integer less than or equal to the nonnegative real number s.

2.1.1. Characterization of Irreducible Polynomials of Same Degree over $\mathbb{F}_2$

Illustration-Identifying the irreducible polynomials of degree 6 over $\mathbb{F}_2$

We use Proposition 2.1 to identify all the irreducible polynomials of degree 6 over $\mathbb{F}_2$ directly from the structure of $\mathbb{F}_{2^6}^*$.

α															
α^2								α^3							
α^{2^2}				α^5				α^6				α^7			
α^{2^3}		α^9		α^{10}		α^{11}		α^{12}		α^{13}		α^{14}		α^{15}	
α^{2^4}	α^{17}	α^{18}	α^{19}	α^{20}	α^{21}	α^{22}	α^{23}	α^{24}	α^{25}	α^{26}	α^{27}	α^{28}	α^{29}	α^{30}	α^{31}
α^{32}	α^{33}	α^{34}	α^{35}	α^{36}	α^{37}	α^{38}	α^{39}	α^{40}	α^{41}	α^{42}	α^{43}	α^{44}	α^{45}	α^{46}	α^{47}
α^{48}	α^{49}	α^{50}	α^{51}	α^{52}	α^{53}	α^{54}	α^{55}	α^{56}	α^{57}	α^{58}	α^{59}	α^{60}	α^{61}	α^{62}	α^{63}
(0)	(1)	(2)	(3)	()	(4)	(5)	(6)	(2)	(5)	()	(7)	(4)	()	(7)	(8)
(1)	(3)	(4)	(6)	(5)	(7)	()	(8)	(3)	(6)	(7)	(8)	(6)	(8)	(8)	()

Figure 2: Structure of $\mathbb{F}_{2^6}^*$

The symbol "()" for "empty bracket" indicates that there is no irreducible polynomial of degree 6 formed using the column above "()".
Following are the all irreducible polynomials of degree 6 over $\mathbb{F}_2$.

$$f_0(x) = \prod_{i=0}^{5}(x-\alpha^{2^i}),\ \ f_1(x) = (x-\alpha^{33})\prod_{i=0}^{4}(x-\alpha^{3\times 2^i}),\ \ f_2(x) = \prod_{i=0}^{1}(x-\alpha^{17\times 2^i})\prod_{j=0}^{3}(x-\alpha^{5\times 2^j}),$$

$$f_3(x) = (x-\alpha^{35})(x-\alpha^{49})\prod_{i=0}^{3}(x-\alpha^{7\times 2^i}),\ \ f_4(x) = (x-\alpha^{37})\prod_{i=0}^{2}(x-\alpha^{11\times 2^i})\prod_{j=0}^{1}(x-\alpha^{25\times 2^j}),$$

$$f_5(x) = \prod_{i=0}^{1}(x-\alpha^{19\times 2^i})(x-\alpha^{41})\prod_{j=0}^{2}(x-\alpha^{13\times 2^j}),\ \ f_6(x) = (x-\alpha^{39})(x-\alpha^{51})(x-\alpha^{57})\prod_{i=0}^{2}(x-\alpha^{15\times 2^i}),$$

$$f_7(x) = (x-\alpha^{43})\prod_{i=0}^{1}(x-\alpha^{23\times 2^i})(x-\alpha^{53})\prod_{j=0}^{1}(x-\alpha^{29\times 2^j}) \text{ and}$$

$$f_8(x) = (x-\alpha^{47})(x-\alpha^{55})(x-\alpha^{59})(x-\alpha^{61})\prod_{i=0}^{1}(x-\alpha^{31\times 2^i})$$

International Electronic Journal of Pure and Applied Mathematics – IEJPAM, Volume 4, No. 2 (2012)

Illustration-Identifying the irreducible polynomials of degree 7 over $\mathbb{F}_2$

Now we use the Proposition 2.1 and compute all irreducible polynomials of degree 7 over $\mathbb{F}_2$ by considering elements from the beginning of n^{th} row of $\mathbb{F}_{2^7}^*$ in the structure. As the figure is very large, we split the figure into four parts and identify irreducible polynomials by considering all the four figures together.

α															
α^2															
α^4															
α^8								α^9							
α^{16}				α^{17}				α^{18}				α^{19}			
α^{32}		α^{33}		α^{34}		α^{35}		α^{36}		α^{37}		α^{38}		α^{39}	
α^{64}	α^{65}	α^{66}	α^{67}	α^{68}	α^{69}	α^{70}	α^{71}	α^{72}	α^{73}	α^{74}	α^{75}	α^{76}	α^{77}	α^{78}	α^{79}
(0)	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(4)	(8)	(9)	(10)	(8)	(11)	(12)	(13)

Figure 3: Structure of $\mathbb{F}_{2^7}^* - part(1)$

α^5															
α^{10}								α^{11}							
α^{20}				α^{21}				α^{22}				α^{23}			
α^{40}		α^{41}		α^{42}		α^{43}		α^{44}		α^{45}		α^{46}		α^{47}	
α^{80}	α^{81}	α^{82}	α^{83}	α^{84}	α^{85}	α^{86}	α^{87}	α^{88}	α^{89}	α^{90}	α^{91}	α^{92}	α^{93}	α^{94}	α^{95}
(2)	(6)	(9)	(12)	(9)	(14)	(14)	(15)	(5)	(11)	(14)	(16)	(10)	(16)	(15)	(17)

Figure 4: Structure of $\mathbb{F}_{2^7}^* - part(2)$

α^3															
α^6								α^{13}							
α^{12}				α^{25}				α^{26}				α^{27}			
α^{24}		α^{49}		α^{50}		α^{51}		α^{52}		α^{53}		α^{54}		α^{55}	
α^{48}		α^{98}		α^{100}		α^{102}		α^{104}		α^{106}		α^{108}		α^{110}	
α^{96}	α^{97}	α^{98}	α^{99}	α^{100}	α^{101}	α^{102}	α^{103}	α^{104}	α^{105}	α^{106}	α^{107}	α^{108}	α^{109}	α^{110}	α^{111}
(1)	(3)	(5)	(7)	(8)	(10)	(11)	(13)	(6)	(12)	(14)	(15)	(11)	(16)	(16)	(17)

Figure 5: Structure of $\mathbb{F}_{2^7}^* - part(3)$

International Electronic Journal of Pure and Applied Mathematics – IEJPAM, Volume 4, No. 2 (2012)

α^7								α^{15}							
α^{14}								α^{30}				α^{31}			
α^{28}				α^{29}				α^{60}		α^{61}		α^{62}		α^{63}	
α^{56}		α^{57}		α^{58}		α^{59}		α^{120}		α^{122}		α^{124}		α^{126}	α^{127}
α^{112}	α^{113}	α^{114}	α^{115}	α^{116}	α^{117}	α^{118}	α^{119}	α^{121}		α^{123}		α^{125}			
(3)	(7)	(10)	(13)	(12)	(15)	(16)	(17)	(7)	(13)	(15)	(17)	(13)	(17)	(17)	()

Figure 6: Structure of $\mathbb{F}_{2^7}^* - part(4)$

Following are the all irreducible polynomials directly identified from the structure.

$$f_0(x) = \prod_{i=0}^{6}(x-\alpha^{2^i}),\ \ f_1(x) = (x-\alpha^{65})\prod_{i=0}^{5}(x-\alpha^{3\times 2^i}),\ \ f_2(x) = \prod_{i=0}^{1}(x-\alpha^{33\times 2^i})\prod_{j=0}^{4}(x-\alpha^{5\times 2^j}),$$

$$f_3(x) = (x-\alpha^{67})(x-\alpha^{97})\prod_{i=0}^{4}(x-\alpha^{7\times 2^i}),\ \ f_4(x) = \prod_{i=0}^{2}(x-\alpha^{17\times 2^i})\prod_{j=0}^{3}(x-\alpha^{9\times 2^j}),$$

$$f_5(x) = (x-\alpha^{69})\prod_{i=0}^{3}(x-\alpha^{11\times 2^i})\prod_{j=0}^{1}(x-\alpha^{49\times 2^j}),\ \ f_6(x) = \prod_{i=0}^{1}(x-\alpha^{35\times 2^i})(x-\alpha^{81})\prod_{j=0}^{3}(x-\alpha^{13\times 2^j}),$$

$$f_7(x) = (x-\alpha^{71})(x-\alpha^{99})(x-\alpha^{113})\prod_{i=0}^{3}(x-\alpha^{15\times 2^i}),$$

$$f_8(x) = (x-\alpha^{73})\prod_{i=0}^{2}(x-\alpha^{19\times 2^i})\prod_{j=0}^{2}(x-\alpha^{25\times 2^j}),$$

$$f_9(x) = \prod_{i=0}^{1}(x-\alpha^{37\times 2^i})\prod_{j=0}^{1}(x-\alpha^{41\times 2^j})\prod_{k=0}^{2}(x-\alpha^{21\times 2^k}),$$

$$f_{10}(x) = (x-\alpha^{75})\prod_{i=0}^{2}(x-\alpha^{23\times 2^i})(x-\alpha^{101})\prod_{j=0}^{1}(x-\alpha^{57\times 2^j}),$$

$$f_{11}(x) = (x-\alpha^{77})(x-\alpha^{89})\prod_{i=0}^{1}(x-\alpha^{51\times 2^i})\prod_{j=0}^{2}(x-\alpha^{27\times 2^j}),$$

$$f_{12}(x) = \prod_{i=0}^{1}(x-\alpha^{39\times 2^i})(x-\alpha^{83})(x-\alpha^{105})\prod_{j=0}^{2}(x-\alpha^{29\times 2^j}),$$

$$f_{13}(x) = (x-\alpha^{79})(x-\alpha^{103})(x-\alpha^{115})(x-\alpha^{121})\prod_{i=0}^{2}(x-\alpha^{31\times 2^i}),$$

$$f_{14}(x) = (x-\alpha^{85})\prod_{i=0}^{1}(x-\alpha^{43\times 2^i})\prod_{j=0}^{1}(x-\alpha^{45\times 2^j})\prod_{k=0}^{1}(x-\alpha^{53\times 2^k}),$$

$$f_{15}(x) = (x-\alpha^{87})\prod_{i=0}^{1}(x-\alpha^{47\times 2^i})(x-\alpha^{107})(x-\alpha^{117})\prod_{j=0}^{1}(x-\alpha^{61\times 2^j}),$$

$$f_{16}(x) = (x-\alpha^{91})(x-\alpha^{93})(x-\alpha^{109})\prod_{i=0}^{1}(x-\alpha^{55\times 2^i})\prod_{j=0}^{1}(x-\alpha^{59\times 2^j}) \text{ and}$$

International Electronic Journal of Pure and Applied Mathematics – IEJPAM, Volume 4, No. 2 (2012)

$$f_{17}(x) = (x-\alpha^{95})(x-\alpha^{111})(x-\alpha^{119})(x-\alpha^{123})(x-\alpha^{125})\prod_{i=0}^{1}(x-\alpha^{63\times 2^i}).$$

In this section itself, we have completely characterized the structure. However, we describe the characterization of the structure from different angle in the next section.

2.2. Conjugates of elements in the n^{th} row from the end

Proposition 2.2. *If $\beta = \alpha^{2^n-k}$ then*

$$\beta^2 = \alpha^{2^n-(2k-1)} \tag{2}$$

$$\text{for } k = 1, 2, 3, \cdots, 2^{n-1}$$

Proof. $\beta^2 = \alpha^{2^{n+1}-2k} = \alpha^{2^n+2^n-2k} = \alpha\alpha^{2^n-2k} = \alpha^{2^n-(2k-1)}$. □

We prove the following important proposition and use it to calculate the trace of elements of n^{th} row starting from the end in reverse order.

Proposition 2.3. *Let $l_1, l_2, l_3, \cdots, l_t$ be positive integers such that $l_1 > l_2 > l_3 > \cdots > l_t \geq 0$ and $r + l_1 \leq n-2$ where r is a nonnegative integer. Then conjugate of*
$\alpha^{2^n-(2^{r+l_1}+2^{r+l_2}+2^{r+l_3}+\cdots+2^{r+l_t}+1)}$ *is* $\alpha^{2^n-(2^{r+l_1+1}+2^{r+l_2+1}+2^{r+l_3+1}+\cdots+2^{r+l_t+1}+1)}$
and $[[2^n-(2^{l_1}+2^{l_2}+2^{l_3}+\cdots+2^{l_t}+1)]]$
$$= [[2^n-(2^{l_1+1}+2^{l_2+1}+2^{l_3+1}+\cdots+2^{l_t+1}+1)]]$$
$$= [[2^n-(2^{l_1+2}+2^{l_2+2}+2^{l_3+2}+\cdots+2^{l_t+2}+1)]] = \cdots$$

Proof.

$$(\alpha^{2^n-(2^{r+l_1}+2^{r+l_2}+2^{r+l_3}+\cdots+2^{r+l_t}+1)})^2 = \alpha^{2^{n+1}-(2^{r+l_1+1}+2^{r+l_2+1}+2^{r+l_3+1}+\cdots+2^{r+l_t+1}+2)}$$
$$= \alpha^{2^n+1-(2^{r+l_1+1}+2^{r+l_2+1}+2^{r+l_3+1}+\cdots+2^{r+l_t+1}+2)}$$
$$= \alpha^{2^n-(2^{r+l_1+1}+2^{r+l_2+1}+2^{r+l_3+1}+\cdots+2^{r+l_t+1}+1)}.$$

This completes the proof of first part. Now we prove the second part.

$$[[2^n-(2^{l_1}+2^{l_2}+2^{l_3}+\cdots+2^{l_t}+1)]] = [[2^n-(2(2^{l_1}+2^{l_2}+2^{l_3}+\cdots+2^{l_t}+1)-1)]]$$
$$= [[2^n-((2^{l_1+1}+2^{l_2+1}+2^{l_3+1}+\cdots+2^{l_t+1}+2)-1)]]$$
$$= [[2^n-(2^{l_1+1}+2^{l_2+1}+2^{l_3+1}+\cdots+2^{l_t+1}+1)]].$$

This completes the proof. □

We may note that any odd positive integer less than 2^{n-1} can be expressed in the format $2^{r+l_1}+2^{r+l_2}+2^{r+l_3}+\cdots+2^{r+l_t}+1$ with the non-negative integers $l_1, l_2, l_3, \cdots, l_t$ such that $l_1 > l_2 > l_3 > \cdots > l_t \geq 0$ and $r + l_1 \leq n-2$ where r is a non-negative integer.

International Electronic Journal of Pure and Applied Mathematics – IEJPAM, Volume 4, No. 2 (2012)

We now illustrate the above proposition with some special cases:

Class of Type $\alpha^{2^n-(2^r+1)}$: By Proposition 2.3, $\alpha^{2^n-(2^r+1)}$ for $r = 0, 1, 2, 3, \cdots, n-2$ in the last row are conjugates of α^{2^n-2}. For example, they are $[[2^n-2]] = [[2^n-3]] = [[2^n-5]] = [[2^n-9]] = [[2^n-17]] = \cdots = [[2^n-2^{n-2}-1]] = [[2^{n-1}+2^{n-2}-1]]$.

Example. Consider the elements of the form $\alpha^{2^n-(2^r+1)}$ for $r = 0, 1, 2, \cdots$
Let $\beta = \alpha^{2^n-(2^r+1)}$ for $r = 0$.

By (2), $\beta^2 = \alpha^{2^n-3} = \alpha^{2^n-(2^r+1)}$ where $r = 1$ $\beta^{2^2} = \alpha^{2^n-5} = \alpha^{2^n-(2^r+1)}$ where $r = 2 \ldots$
$\beta^{2^{n-2}} = \alpha^{2^n-(2^{n-2}+1)} = \alpha^{2^n-(2^r+1)}$ where $r = n-2$
$\beta^{2^{n-1}} = \alpha^{2^{n-1}-1} = \alpha^{2^n-(2^r+1)}$ where $r = n-1$
The irreducible polynomial is

$$\prod_{r=0}^{n-1}\left(x - \alpha^{2^n-(2^r+1)}\right)$$

In the similar manner, we get the following irreducible polynomials.

Class of type $\alpha^{2^n-(2^{r+1}+2^r+1)}$: Using the Proposition 2.3, we get the irreducible polynomial

$$\prod_{r=0}^{n-1}\left(x - \alpha^{2^n-(2^{r+1}+2^r+1)}\right)$$

Class of type $\alpha^{2^n-(2^{r+2}+2^r+1)}$:

Using the Proposition 2.3, we get the irreducible polynomial

$$\prod_{r=0}^{n-1}\left(x - \alpha^{2^n-(2^{r+2}+2^r+1)}\right)$$

Class of type $\alpha^{2^n-(2^{r+3}+2^r+1)}$: Using the Proposition 2.3, we get the irreducible polynomial

$$\prod_{r=0}^{n-1}\left(x - \alpha^{2^n-(2^{r+3}+2^r+1)}\right)$$

Class of type $\alpha^{2^n-(2^{r+4}+2^r+1)}$: Using the Proposition 2.3, we get the irreducible polynomial

$$\prod_{r=0}^{n-1}\left(x - \alpha^{2^n-(2^{r+4}+2^r+1)}\right)$$

2.2.1. Characterization of Irreducible Polynomials of Same Degree over $\mathbb{F}_2$

Illustration-Identifying all the irreducible polynomials of degree 5 over $\mathbb{F}_2$:

We use the Proposition 2.2 and compute all irreducible polynomials of degree 5 over $\mathbb{F}_2$ by considering elements from the end of 5^{th} row of $\mathbb{F}_{2^5}$ in the structure.

International Electronic Journal of Pure and Applied Mathematics – IEJPAM, Volume 4, No. 2 (2012)

α															
α^2								α^3							
α^{2^2}				α^5				α^6				α^7			
α^{2^3}		α^9		α^{10}		α^{11}		α^{12}		α^{13}		α^{14}		α^{15}	
α^{2^4}	α^{17}	α^{18}	α^{19}	α^{20}	α^{21}	α^{22}	α^{23}	α^{24}	α^{25}	α^{26}	α^{27}	α^{28}	α^{29}	α^{30}	α^{31}
(0)	(4)	(5)	(2)	(5)	(3)	(3)	(1)	(4)	(2)	(3)	(1)	(2)	(1)	(1)	()

Figure 7: Structure of $\mathbb{F}^*_{2^5}$

The symbol empty bracket "()" indicates that there is no irreducible polynomial of degree 5 formed using the column above "()". Therefore, all the six irreducible polynomials of degree 5 are

$$f_0(x) = \prod_{i=0}^{4}(x-\alpha^{2^i}),\ \ f_1(x) = (x-\alpha^{23})(x-\alpha^{27})(x-\alpha^{29})\prod_{i=0}^{1}(x-\alpha^{15\times 2^i}),$$

$$f_2(x) = (x-\alpha^{19})(x-\alpha^{25})\prod_{i=0}^{2}(x-\alpha^{7\times 2^i}),\ \ f_3(x) = (x-\alpha^{21})\prod_{i=0}^{1}(x-\alpha^{11\times 2^i})\prod_{j=0}^{1}(x-\alpha^{13\times 2^j}),$$

$$f_4(x) = (x-\alpha^{17})\prod_{i=0}^{3}(x-\alpha^{3\times 2^i}) \text{ and } f_5(x) = \prod_{i=0}^{1}(x-\alpha^{9\times 2^i})\prod_{i=0}^{2}(x-\alpha^{5\times 2^i})$$

In the next subsection, we approach the elements of the structure from rows and columns in some order.

2.3. Correspondence between Elements at Each Column and the Elements of n^{th} Row

First we start with α which is in first row.
For $i \geq 2$, element in every i^{th} row introducing new column is of the form $\alpha(i,j) = \alpha^{2^{i-1}+2j-1}$ for the integer $j = 1, 2, \cdots, 2^{i-2}$
Now we link $\alpha^{2^{i-1}+2j-1}$ with elements in n^{th} row
For $i = 1$, no new element is introduced and

$$[[1]] = [[2^1]] = [[2^2]] = [[2^2]] = \cdots = [[2^{n-1}]]$$

$[[[1]]]$ has length n

For $i = 2$ and $j = 1$, $2^{i-1} + 2j - 1 = 3$ and $[\alpha^{2^1+2\times 1-1}] = [[2^1+1]] = \cdots = [[2^{n-1}+2^{n-2}]]$

$[[[2^1+1]]]$ has length $n-1$

For $i = 3$, there are two values for j, that is, $j = 1, 2$
When $j = 1$, $2^{i-1} + 2j - 1 = 2^2 + 1 = 5$ and $[\alpha^{2^2+1}] = [[2^2+1]] = [[2^{n-1}+2^{n-3}]]$

$[[[2^2+1]]]$ has length $n-2$

When $j = 2$, $2^{i-1} + 2j - 1 = 2^2 + 2^1 + 1 = 7$ and $[\alpha^{2^2+2^1+1}] = \cdots = [[2^{n-1}+2^{n-2}+2^{n-3}]]$

$[[[2^2+2^1+1]]]$ has length $n-2$

International Electronic Journal of Pure and Applied Mathematics – IEJPAM, Volume 4, No. 2 (2012)

In this way, we can proceed up to $i = n$.

We have completely characterized all the elements of the structure from n^{th} row and from the columns of each row. A few examples are given to identify irreducible polynomials of degree n

1. Example
   First column contains the n distinct conjugates $\alpha, \alpha^2, \alpha^{2^2}, \alpha^{2^3}, \alpha^{2^4}, \cdots, \alpha^{2^{n-1}}$ and hence the corresponding irreducible polynomial (the minimal polynomial of α) of degree n is
   $$\prod_{k=0}^{n-1} \left(x - \alpha^{2^k}\right)$$
2. Example
   Consider the column containing distinct $n-1$ conjugates $\alpha^3, \alpha^{3\times 2}, \alpha^{3\times 2^2}, \alpha^{3\times 2^3}, \alpha^{3\times 2^4}, \cdots, \alpha^{3\times 2^{n-2}}$.
   The remaining one more conjugate is $\alpha^{3\times 2^{n-1}} = \alpha^{(2+1)\times 2^{n-1}} = \alpha\alpha^{2^{n-1}} = \alpha^{2^{n-1}+1}$
   Therefore, the corresponding irreducible polynomial of degree n is
   $$\prod_{k=0}^{n-1} \left(x - \alpha^{3\times 2^k}\right)$$
3. Example
   Consider the column $\alpha^{5\times 2^i} = \alpha^{(2^2+1)\times 2^i} = \alpha^{((2^2)\times 2^i)+2^i}$ for $i = 0$ to $n-3$.
   There are $n-2$ elements and two more elements are to be determined.
   The remaining two conjugates are $\alpha^{2^{n-2}+1}$ and $\alpha^{2\times(2^{n-2}+1)}$
   Therefore, the corresponding irreducible polynomial of degree n is
   $$\prod_{k=0}^{n-1} \left(x - \alpha^{5\times 2^k}\right)$$

We can construct irreducible polynomials this way.

3. Conclusion

We have completely characterized the structure which was visualized in [3]. As an application of the structure, we have shown that we can identify *all* the irreducible polynomials of degree n over $\mathbb{F}_2$ for a given positive integer n.

Acknowledgments

The authors thank the referees for having spared time to read the manuscript with care.

References

[1] Rudolf Lidl, Harald Niederreiter, *Finite Fields*, Cambridge University Press (1997).

[2] Alfred J. Menezes, Paul C. VanOorschot, Scott A.Vanstone, *Handbook of Applied Cryptography*, CRC Press LLC (1997).

[3] R.K. Sharma, Wagish Shukla, S. Ramasamy, On trace structure of $\mathbb{F}_{2^n}$, *Journal of Communication and Computer*, **8** (2011), 329-334.

[4] Douglas R. Stinson, *Cryptography (Theory and Practice)*, Chapman and Hall, (2006).