Construction and Determination of Irreducible Polynomials in Galois fields, $GF(2^m)$.

Abraham Aidoo[1], Kwasi Baah Gyamfi[1]

1. *Department of Mathematics, Kwame Nkrumah University of Science and Technology, Kumasi, Ghana.*

Email:*abramkhems09@gmail.com, kwasibaahgyamfi1@gmail.com*

Abstract
This work is about Construction of Irreducible Polynomials in Finite fields. We defined some terms in the Galois field that led us to the construction of the polynomials in the $GF(2^m)$. We discussed the following in the text; irreducible polynomials, monic polynomial, primitive polynomials, field, Galois field or finite fields, and the order of a finite field. We found all the polynomials in $F_2[x]$ that is, $P(x) = \sum_{i=1}^{m} a_i x^i : a_i \in F_2$ with $a_m \neq 0$ for some degree m which led us to determine the number of irreducible polynomials generally at any degree in $F_2[x]$.

Mathematics Subject Classification: 20D99
Keywords: Irreducible polynomials,Field, Finite fields.

1 Introduction

In arithmetic, a polynomial of the form $a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1} + a_nx^n$, is an expression such as variables and coefficients that entails most effective the operations of addition, subtraction, multiplication, and non-negative integer exponents. Polynomials are used in the various areas of mathematics and science,[6].

In advanced mathematics, polynomials are used in rings, critical concepts in algebra and algebraic geometry. In this study, we show how polynomials are developed in the Galois fields. Galois' notion about finite fields are; the order or number of elements of a finite field is of the form p^m, where p is a prime number and $m \in Z^+$, he used naming scheme $GF(p^m)$ to specify the order of the field where $m = 1$ (prime field) or $m > 1$ (field extension). He also said Finite field exists for every p^m elements and any two finite fields with the same elements are isomorphic,[5].

The construction of $N-$polynomials over any finite field is a challenging mathematical problem. Especially in the field of mathematical theory and coding theory. However, many Researchers have done credibly in this area of study using different approaches to construct polynomials in the field Fq but hardly have they determined the number of irreducible polynomials in every degree of polynomials in $F_{2^m}[x]$. The construction of normal basis of F_p over F_{p^m} is another challenging area. In this thesis, a computationally simple construction of polynomials and the general rule for determining the number of irreducible polynomials over $F_{2^m}[x]$ is presented.

2 Preliminary Definitions And Basic Theorems

In this chapter we tried to define some terms and its supporting theorems and proofs while giving examples where necessary.

2.1 Irreducible Polynomial

2.1.1 Definition

A polynomial $f(x)$ is irreducible in GF(q) if $f(x)$ cannot be factored into a product of lower-degree polynomials in GF(q)[x], [2].

1. A polynomial may be irreducible in one ring of polynomials, but reducible in another.

2. In fact, every polynomial is reducible in some ring of polynomials. The term irreducible must thus be used only with respect to a specific ring of polynomials.

3. In GF(2)[x], if $f(x)$ has degree > 1 and has an even number of terms, then it can't be irreducible. Because 1 is its root, and hence $x + 1$ is one of its factor.

2.1.1 Lemma
A field of prime power order p^m is a splitting field over F_p of $x^{p^m} - x$, [3].

Proof: Let F be a field of order p^m. F carries a sub-field isomorphic to $Z/(p) = F_p$. Explicitly, the subring of F produced by means of 1 is a field of order q. Every $t \in F$ satisfies $t^{p^m} = t$: if $t \neq 0$ then $t^{p^m} - 1 = 1$ since $F^* = F - \{0\}$ is a multiplicative group of order $p^m - 1$, after which multiplying through via t gives us $t^{p^m} = t$, which is also proper whilst $t = 0$. The polynomial $x^{p^m} - x$ has every detail of F as a root, so F is a splitting field of $x^{p^m} - x$ over the field F_p. □

2.1.2 Theorem
Any polynomial $\pi(x)$ which is irreducible in $F_p[x]$ of degree m divides $x^{p^m} - x$ and is separable, [3].

Proof: The field $F_p[x]/(\pi(x))$ has order p^n, so $t^{p^n} = t$ for all t in $F_p[x]/(\pi(x))$ (see the proof of Lemma 2.1.1). In particular, $x^{p^n} \equiv x mod \pi(x)$, so $\pi(x) \mid (x^{p^n} - x)$ in $F_p[x]$ and its factor $\pi(x)$ is separable. □

2.2 Field

A field is one of the fundamental algebraic structures used in abstract algebra. It is a commutative ring in which the non-zero elements have an inverse or equivalently a ring whose non-zero elements form an abelian group,that is, $\forall\ a, b \in R$, $ab = ba$ under multiplication, [2].

Theorem: For $f \in F[x]$, the residue class ring $F[x]/(f)$ is a field if and only if f is irreducible over F, [3].

Proof: Assuming $f(x)$ is irreducible over F. This implies that the quotient ring $F[x]/(f(x))$ is a prime ideal and therefore a maximal ideal. But all maximal ideals are fields hence $F[x]/(f)$ is a field. The converse is obvious. If d is an irreducible polynomial in Z/pZ of degree m, then $Z/pZ(d)$ is a field with exactly p^m elements. p, prime, is the characteristic of the sub-field Z_p.

2.3 Finite Field or Galois Field

A field is said to be a Galois field if it contains finite number of elements. As with any field, a finite field is set on which the operations of multiplication, addition, subtraction and division are defined and satisfied under certain basic rule, [3]. The most common examples of finite fields are given by the integer $mod p$ when p is a prime number.

Lemma: A field of prime power order p^m is a splitting field over F_p of $x^{p^m} - x$, [3].

Proof: Let F be a field of order p^m. F carries a sub-field isomorphic to $Z/(p) = F_p$. Explicitly, the subring of F produced by means of 1 is a field of order q. Every $t \in F$ satisfies $t^{p^m} = t$: if $t \neq 0$ then $t^{p^m} - 1 = 1$ since $F^* = F - \{0\}$ is a multiplicative group of order $p^m - 1$, after which multiplying through via t gives us $t^{p^m} = t$, which is also proper whilst $t = 0$. The polynomial $x^{p^m} - x$ has every detail of F as a root, so F is a splitting field of $x^{p^m} - x$ over the field F_p.

2.4 Order of Finite Fields

The number of elements of a finite field is known as its order. A finite field of order q exists if and most effective if the order q is a prime power p^k (p is a prime number and k is a positive integer).

Theorem: Any finite field has prime power order, [1].

Proof: For every commutative ring R there is a unique ring homomorphism $Z \longrightarrow R$, given by $m \longmapsto \begin{cases} 1+1+\cdots+1, & \text{if} \quad m \geq 0, \\ m \quad \text{times} \\ -(1+1+\cdots+1), & \text{if} \quad m < 0. \\ \quad \mid m \mid \quad \text{times} \end{cases}$
We apply this to the case when $R = F$ is a finite field. The kernel of $Z \longrightarrow F$ is nonzero since Z is infinite and F is finite. Write the kernel as $(m) = mZ$ for an integer $m > 0$, so $Z/(m)$ embeds as a subring of F. Any subring of a field is a domain, so m has to be a prime number, say $m = p$. Therefore there is an embedding $Z/(p) \hookrightarrow F$. Viewing F as a vector space over $Z/(p)$, it is finite-dimensional since F is finite. Letting $n = dim_{Z/(p)}(F)$ and picking a basis $\{e_1, \cdots, e_n\}$ for F over $Z/(p)$, elements of F can be written uniquely as $c_1e_1 + \cdots + c_ne_n$, $c_i \in Z/(p)$: Each coefficient has p choices, so $\sharp F = p^n$, [4]. $\square$

3 Main Result

3.1 Overview

In this chapter we presented how irreducible polynomials are determined, and how polynomials are constructed in $GF(2^m)$.

3.1.1 Construction Of Polynomials In $F_2[x]$

$F_2[x]$ is basically a field of polynomials with coefficients of the polynomials in F_2 with elements $(0, 1)$. We determine or construct all the possible polynomials of various degree, particularly, degree 1,2,3,4,5, and 6 within the field F_2, find how to determine the number of polynomials of a particular degree in F_2 and the number of irreducible polynomials associated with them.

3.2 Polynomial of degree one

This has the form $a_1x + a_0$, where $a_1 = 1$ and $a_0 = 0$ (or) 1. So by construct, we have two polynomials; x, $x + 1$, which are both irreducible.

3.3 Polynomial of degree two

This takes the form $a_2x^2 + a_1x + a_0$, where $a_2 = 1$ and $a_1, a_0 = 0$ (or) 1. We therefore, have the following four polynomials; x^2, $x^2 + 1$, $x^2 + x$, and $x^2 + x + 1$ with one irreducible polynomial.

3.4 Polynomial of degree three

The form of this polynomial is $a_3x^3 + a_2x^2 + a_1x + a_0$ with $a_3 \neq 0$ and $a_0, a_1, a_2 = \begin{cases} 0 \\ 1 \end{cases}$. This yields eight polynomials with two irreducible polynomials;

x^3, $x^3 + x^2$, $x^3 + x$, $x^3 + x^2 + x$, $x^3 + x^2 + 1$, $x^3 + x + 1$, $x^3 + 1$, $x^3 + x^2 + x + 1$.

3.5 Polynomial of degree four

This has the form $a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$ with $a_4 \neq 0$ and $a_0, a_1, a_2, a_3 = \begin{cases} 0 \\ 1 \end{cases}$ and yields sixteen polynomials with four being irreducible in $F_2[x]$;

x^4, $x^4 + 1$, $x^4 + x^3$, $x^4 + x^2$, $x^4 + x$, $x^4 + x^3 + x^2$, $x^4 + x^3 + x$, $x^4 + x^2 + x$, $x^4 + x^3 + 1$, $x^4 + x^2 + 1$, $x^4 + x + 1$, $x^4 + x^3 + x^2 + x$, $x^4 + x^2 + x + 1$, $x^4 + x^3 + x + 1$, $x^4 + x^3 + x^2 + 1$, $x^4 + x^3 + x^2 + x + 1$.

3.6 Polynomial of degree five

The form of such polynomials is $a_5x^5+a_4x^4+a_3x^3+a_2x^2+a_1x+a_0$, where $a_5 \neq 0$, while $a_0, a_1, a_2, a_3, a_4 = \begin{cases} 0 \\ 1 \end{cases}$. We have thirty-two polynomials with eight being irreducible;

x^5, x^5+1, x^5+x^4, x^5+x^3, x^5+x^2, x^5+x, x^5+x+1, x^5+x^2+1, x^5+x^3+1, x^5+x^4+1, x^5+x^2+x+1, x^5+x^3+x+1, x^5+x^4+x+1, $x^5+x^4+x^3$, $x^5+x^4+x^2$, $x^5+x^3+x^2$, $x^5+x^4+x^3+x^2$, x^5+x^3+x, $x^5+x^4+x^3+x^2+1$, $x^5+x^4+x^3+1$, $x^5+x^4+x^2+1$, $x^5+x^3+x^2+1$, $x^5+x^3+x^2+x+1$, $x^5+x^4+x^2+x+1$, $x^5+x^4+x^3+x$, $x^5+x^4+x^3+x^2+x+1$, x^5+x^2+x, x^5+x^4+x, $x^5+x^4+x^2+x$, $x^5+x^4+x^3+x^2+x$, $x^5+x^4+x^3+x+1$, $x^5+x^3+x^2+x$.

3.7 Polynomial of degree six

This takes the form $a_6x^6+a_5x^5+a_4x^4+a_3x^3+a_2x^2+a_1x+a_0$, where $a_6 \neq 0$, while $a_0, a_1, a_2, a_3, a_4, a_5 = \begin{cases} 0 \\ 1 \end{cases}$ which produces sixty-four polynomials with sixteen being irreducible;

x^6, $x^6+x^5+x^4+x^3+x^2+x+1$, $x^6+x^5+x^4+x^3+x^2+x$, $x^6+x^5+x^4+x^3+x^2$,$x^6+x^5+x^4+x^3$, $x^6+x^5+x^4$, x^6+x^5, x^6+x^4, x^6+x^3, x^6+x^2, x^6+x, x^6+1, $x^6+x^5+x^4+x^3+x^2+1$, $x^6+x^5+x^4+x^3+x+1$, $x^6+x^5+x^4+x^2+x+1$, $x^6+x^5+x^3+x^2+x+1$, $x^6+x^4+x^3+x^2+x+1$, $x^6+x^5+x^4+x^3+1$, $x^6+x^5+x^4+x^2+1$, $x^6+x^5+x^3+x^2+1$, $x^6+x^4+x^3+x^2+1$, $x^6+x^5+x^4+x+1$, $x^6+x^5+x^3+x+1$, $x^6+x^4+x^3+x+1$, x^6+x^5+x+1, x^6+x^4+x+1, x^6+x^3+x+1, x^6+x^2+x+1, x^6+x^5+1, x^6+x^4+1, x^6+x^3+1, x^6+x^2+1, x^6+x+1, $x^6+x^5+x^4+1$, $x^6+x^5+x^3+1$, $x^6+x^5+x^2+1$, x^6+x^5+x+1, $x^6+x^3+x^2+x+1$, $x^6+x^5+x^3$, $x^6+x^5+x^2$, x^6+x^5+x, $x^6+x^5+x^4+x^2$, $x^6+x^5+x^4+x$, $x^6+x^5+x^3+x^2+x$, $x^6+x^4+x^2$, x^6+x^3+x, x^6+x^4+x, x^6+x^3+x, x^6+x^2+x, $x^6+x^4+x^3$, $x^6+x^3+x^2$, $x^6+x^3+x^2+x$, $x^6+x^4+x^3+x^2+x$, $x^6+x^4+x^2+1$, $x^6+x^4+x^2+x+1$, $x^6+x^5+x^2+x+1$, $x^6+x^4+x^3+1$, $x^6+x^5+x^3+x^2$, $x^6+x^5+x^2+x$, $x^6+x^5+x^2+x+1$, $x^6+x^4+x^3+x$, $x^6+x^4+x^2+x$, $x^6+x^5+x^3+x$, $x^6+x^4+x^3+x^2+x$.

From the above, the general form of the polynomials in $F_2[x] = \sum_{i=0}^{m} a_i x^i : a_i \in F_2$ with $a_m \neq 0$ for some degree m. Also, we see that the number of irreducible polynomials and the degree of polynomials in $F_2[x]$ are given by $2^{(m-2)}$ for $m \geq 2$ and 2^m respectively.

4 Conclusion

In the nut shell, polynomials from Galois fields, $GF2^m$ have been constructed. Following the trend, we were able to determine the number of irreducible polynomials in the degrees of $F_{2^m}[x]$ as well as the general rule. These irreducible polynomials are very essential in the construction of Galois field since some of them are primitive polynomials. Therefore, this piece of work would contribute much to ease burdens of many Researchers in this field of Mathematics.

References

[1] Anthony Y. Aidoo, Kwasi Baah-Gyamfi, Joseph Ackora-Prah, *Explicit construction of finite fields using normal bases*, International Journal of Pure and Applied Mathematics, Volume 70 No. 4 2011 (2011), 559-569.

[2] Rotman, J. J., *A first course in abstract algebra with application,* (3/E), Pearson Education, Inc., 2006.

[3] Lidl, R., and Niederreiter, H., *Introduction to Finite Fields and their applications,* Cambridge University Press, 1997.

[4] Conrad, K. finite fields:, *http://www.math.uconn.edu/ kconrad/blurbs/galoistheory/ finitefields.pdf*

[5] Mahmood Alizadeh, Saeid Mehrabi, *Construction of self-reciprocal normal polynomials over finite fields of even characteristic,* Turkish Journal of Mathematics ht tp://journals.tubitak.gov.t r/ma th/ (2015).

[6] Edwards, H. M., *The construction of solvable polynomials,* Bulletin(New Series) of the American Mathematical Society Volume 46, Number 3 (2009), Pages 397-411.