A Search of all of the irreducible polynomials of degree *m* over $GF(2)$

W. C. Chen. 陳爲志
Department of Electronic Engineering,
Kaohsiung County, Taiwan
I-Shou University.
m865015m@csa500.isu.edu.tw

J. H. Jeng 鄭志宏
Department of Information Engineering,
Kaohsiung County, Taiwan
I-Shou University.
jjeng@csa500.isu.edu.tw

Abstract

A fast method for finding irreducible polynomial of degree m over $GF(2)$ is proposed in this paper. Given an arbitrary irreducible polynomial of degree m and any proper primitive element, the finite field $GF(2^m)$ is generated. From this finite field, one can generate all the irreducible polynomials over $GF(2)$ with degree less than or equal to m. These irreducible polynomials are useful in constructing finite fields for applications in error correcting code, cryptography and other related subjects.

Index terms: *irreducible polynomial, finite field, primitive element, minimal polynomial.*

Introduction:

Finite fields have important applications in error correcting code and cryptography [1, 2]. An irreducible polynomial of degree *m* together with a primitive element can be used to construct the finite field $GF(2^m)$. For special basis, such as normal basis, a proper irreducible polynomial can be chosen so that the normal basis has a convenient form. Constructions of these special bases will reduce the hardware complexity of multiplication and exponentiation of elements in $GF(2^m)$. Various of algorithms are derived to find the irreducible polynomials [3-6]. In this paper, a fast algorithm is proposed.

The constructed finite fields can be used to generate irreducible polynomials. In other words, if $f(x)$ is an irreducible polynomial of degree *m* and α is an arbitrary element. We will use them to construct $GF(2^m)$. If it is successful, we can obtain 2^m different elements in $GF(2^m)$. And this α is called a primitive element of $GF(2^m)$. For any given β in $GF(2^m)$, the conjugates of β can be computed. From the conjugates, we can also generate minimal polynomials over $GF(2)$. These minimal polynomials are irreducible. Thus by this concept, as long as a finite field $GF(2^m)$ is constructed, then all the irreducible polynomials of degree less than or equal to *m* can be found. A Maple program is written to implement the algorithm.

Background theorems:

The theorems below are provided without proof to describe the characteristics of irreducible polynomials, which are used to generate irreducible polynomials. Theorems 1 is from Williams and Sloane [7].

Theorem 1: $x^{2^m}+x=$ product of all monic polynomials, irreducible over $GF(2)$ whose degree divides m.

For *m*=4, by theorem 1, one has

$$x^{2^4}+x = x(x+1)\ (x^2+x+1)\ (x^4+x^3+1)\ (x^4+x+1)\ (x^4+x^3+x^2+x+1)$$ where x,

$(x+1)$, (x^2+x+1), (x^4+x^3+1), (x^4+x+1) $(x^4+x^3+x^2+x+1)$ are polynomials of degree 1, 2 and 4. And these degrees can divide 4. Hence they all are irreducible polynomials over $GF(2)$. The following definition and theorem 2 are from Shu Lin [5].

Definition: The minimal polynomial over $GF(2)$ of β is the lowest degree monic polynomial $M(x)$ say with coefficients from $GF(2)$ such that $M(\beta)=0$.

Theorem 2: Let β be an element in $GF(2^m)$ and e be the smallest nonnegative integer such that $\beta^{2^e}=\beta$ then $f(x)=\prod_{i=0}^{e-1}(x+\beta^{2^i})$ is an irreducible polynomials over $GF(2)$.

An efficient algorithm for finding the irreducible polynomials:

The fast method for finding irreducible polynomials of degree divides m proposed in this paper is based on the theorems above. The algorithm is divided into four steps as follows:

1. Given an irreducible polynomial $f(x)$ of degree m and any primitive element β.
2. Construct $GF(2^m)$, using $f(x)$ and β.
3. Dividing these 2^m elements into non-overlapping partitions, each partition is of the form $[\beta^{2^0}, \beta^{2^0}, \ldots\ldots, \beta^{2^{l-1}}]$ where $\beta \in GF(2^m)$ and l is the smallest integer, such that $\beta^{2^l}=\beta$.
4. For each partition, generate the polynomial which has the elements in the partition as roots.

To illustrate the above steps, let $f(x)=\sum_{i=0}^{m} a_i x^i$ be an monic irreducible polynomial of degree m over $GF(2)$ and $\alpha=\sum_{j=0}^{m-1} c_j x^j$ be a primitive element, where $c_i \in GF(2)$. Also let $n=2^m-1$. From $f(x)$ and α, the finite field $GF(2^m)$ is built, which has 2^m elements. We can take $\beta=\alpha^i$ to construct conjugate partitions, where $0 \le i \le n-1$. In order to get much efficiency, we only use i of the power of α to operate, by using $i=i+i$ (mod n) to build the partition in step3. Step4 can be implemented by $M(x)=\sum_{j=0}^{2^l-1}(x+\beta^i)$, which is exactly the minimal polynomial as defined above. By theorem 2, $M(x)$ is irreducible. The product all the minimal polynomial generated from the non-overlapping partition is of degree x^{2^m}, thus by theorem 1, these minimal polynomials are the all irreducible polynomials of degree divides m.

Example:

Given an irreducible polynomial $f(x)=x^4+x+1$ and $\alpha=[0,0,1,0]$. The finite field $GF(2^4)$ is built, which is of the form $\{0\} \cup \{\alpha^j : j=0,\ldots\ldots,14\}$. The 16 elements in $GF(2^4)$ can be divided into six non-overlapping partitions, i.e, [0], [1], $[\alpha^1, \alpha^2, \alpha^4, \alpha^8]$, $[\alpha^3, \alpha^6, \alpha^{12}, \alpha^9]$, $[\alpha^5, \alpha^{10}]$, $[\alpha^7, \alpha^{14}, \alpha^{13}, \alpha^{11}]$.

In each partition, a polynomial can be generated using all the elements as its roots. For the partition $[\alpha^1, \alpha^2, \alpha^4, \alpha^8]$, the minimal polynomial $M(x)$ is generated by $M(x)=(x+\alpha^1)\ (x+\alpha^2)\ (x+\alpha^4)\ (x+\alpha^8)\ =x^4+x+1$. By theorem 2, it is an irreducible polynomial. Other related minimal polynomials are computed in table 1.

Table 1. All minimal polynomials generated from each partition.

partition	Minimal polynomial
0	x
1	$M^0(x)=x+1$
$\alpha^1,\alpha^2,\alpha^4,\alpha^8$	$M^{(1)}=M^{(2)}=M^{(4)}=M^{(8)}$ $=x^4+x+1$

$\alpha^3, \alpha^6, \alpha^{12}, \alpha^9$	$M^{(3)} = M^{(6)} = M^{(9)} = M^{(12)}$ $= x^4 + x^3 + x^2 + x + 1$
$\alpha^5,\ \alpha^{10}$	$M^{(5)} = M^{(10)}$ $= x^2 + x + 1$
$\alpha^7, \alpha^{14}, \alpha^{13}, \alpha^{11}$	$M^{(7)} = M^{(14)} = M^{(13)} = M^{(11)}$ $= x^4 + x^3 + 1$

since the product of the irreducible polynomials $x,\ M^0(x), \ldots\ldots, M^7(x)$ equals $x^{2^4} + x$, by theorem 1, these are all the irreducible polynomials of degree divides *m*. The numbers of all irreducible polynomials of degree *m* equals to the numbers of all irreducible polynomials of degree less than *m* and divides *m*. In the above example, the number of all irreducible polynomials of degree 4 is 6-2-1=3.

Reference:

[1] Alfred J. Menezes Editor, *Applications of finite fields*, Kluwer Academic, 1993.

[2] Stephen B. Wicker, *Error control systems for Digital Communication and Storage*, Prentice Hall, 1995.

[3] M.Z. Wang, 'Algorithm for recursively generating irreducible polynomials', *Electronic. Lett.*, *v.*32,*n.*20, pp.1875, Sep. 1996.

[4] Victor Shoup, 'New algorithms for finding irreducible polynomials over finite fields', *Math. Comp.* v*54, n189*, pp. 435-447, 1990.

[5] Shu Lin, Daniel J. and Costello, J. *Error control coding fundamentals and applications*, Prentice-Hall, 1983.

[6] W. Wesley Peterson, E. J. Weldon, *Error correcting codes*, Colonia Press, 1972.

[7] F.J. Mac Williams and N.J.A. Sloane, *The Theory of Error Correcting Codes*, North-Holland, pp. 81-124, 1976.