IRREDUCIBLE POLYNOMIALS USED IN INFORMATIONS TRANSMISION SAFETY

Constantin BOCHIȚOIU, Nicolae JULA, Ciprian RĂCUCIU

Technical Military Academy, Bd. G. Coşbuc, 83-85, Bucharest, Romania

Abstract. The work provides a matricial method to test and obtain irreducible polynomials. The method can be applied by a PC for high-degree polynomials. Such polynomials and the corresponding fields are used in codes making

Key-words: eigenvalues, field, cyclic group.

INTRODUCTION

As known [1] every finite p-characteristic field has p^n elements. Such a field, noted G_f, can be obtained by an irreducible polynomial $f = X^n + a_1 X^{n-1} + ... + a_{n-1} X + a_n ; a_i \in Z_p$ and: $G_f = \left| u = \alpha_0 + \alpha_1 \theta + \alpha_2 \theta^2 + ... + \alpha_{n-1} \theta^{n-1} ; \alpha_i \in Z_p , f(\theta) = 0 \right|$ .The field operations are the usual polynomial addition and their modulo f multiplication.

For all irreducible n-degree polynomials f the fields G_f are isomorphic and for this reason on note G_{p^n} instead of G_f when the polynomial f isn't used.

The elements of the field G_{p^n} are the roots of all irreducible polynomials those degree divide n and consequently, $p^n = \sum_{m/n} m \cdot N(m)$ where $N(m)$ is the number of m-degree irreducible polynomials. As a result we obtain the recurrence formula:

$$N(n) = \frac{1}{n} \cdot \left(p^n - \sum_{\substack{m/n \\ m<n}} m \cdot N(m) \right)$$

For example, in case $p=3$, the 1-degree irreducible polynomials are the three polynomials $X+a$; $a=0, 1, 2$ that is, $N(1) = 3$. The formula gives: $N(2) = 3$, $N(3) = 8$, $N(4) = 18$, and so on.

The multiplicative group $G^*_{p^n}$ is a cyclic one and, as a result,

$$X^{p^n} - X = \prod_{\substack{f\text{ - irred}\\ \deg. f/n}} f$$

Moreover, $G_{p^m} \subset G_{p^n} \Leftrightarrow m/n$ and in this case, $G_{p^m} = \left\{ u \in G_{p^n}; u^{p^m} = u \right\}$

§1. THE MATRIX A_f

For each polynomial $f = X^n + a_1 X^{n-1} + ... + a_{n-1}X + a_n; a_i \in Z_p$ the matrix:

$$A_f = \begin{pmatrix} 0 & 0 & 0 & ... & 0 & (-1)^{n-1}a_n \\ 1 & 0 & 0 & ... & 0 & (-1)^{n-1}a_{n-1} \\ 0 & 1 & 0 & ... & 0 & (-1)^{n-1}a_{n-2} \\ ... & ... & ... & ... & ... & ... \\ 0 & 0 & 0 & ... & 0 & (-1)^{n-1}a_2 \\ 0 & 0 & 0 & ... & 1 & (-1)^{n-1}a_1 \end{pmatrix}$$

has *f* as characteristic polynomial.

§2. TESTING THE IRREDUCIBILITY OF POLYNOMIALS

We note $K = G_{p^{n!}}$. This field can be obtained by an *n!*-degree irreducible polynomial which not need to mention. The field *K* plays the role of an algebraic closure [2]. It contains all the roots of all *m*-degree polynomials for $m \leq n$.

In testing the irreducibility of an *n*-degree polynomial *f* we can suppose *f* has no multiple factors. They can be obtained from the polynomial *(f, f')*.

The distinct roots $\lambda_1, \lambda_2, ..., \lambda_n$ of *f* in the field *K* are the eigenvalues of the matrix A_f.. Consequently, there is an invertible matrix *T* having the elements in *K,* such that:

$$A_f = T \cdot \begin{pmatrix} \lambda_1 & 0 & ... & 0 \\ 0 & \lambda_2 & ... & 0 \\ ... & ... & ... & ... \\ 0 & 0 & ... & \lambda_n \end{pmatrix} \cdot T^{-1}$$

and for each natural number *k* we have:

$$A_f^k = T \cdot \begin{pmatrix} \lambda_1^k & 0 & ... & 0 \\ 0 & \lambda_2^k & ... & 0 \\ ... & ... & ... & ... \\ 0 & 0 & ... & \lambda_n^k \end{pmatrix} \cdot T^{-1}$$

THEOREM

The n-degree polynomial f is irreducible if and only if:

$$1. A_f^{p^n} = A_f$$

$$2. rang\left(A_f^{p^m} - A_f \right) = n \text{ for } m = 1, 2, ..., \left[\frac{n}{2} \right]$$

PROOF. Let f be irreducible. Then the roots of f vanish the polynomial $X^{p^n} - X$ and consequently,

$$A_f^{p^n} = T \cdot \begin{pmatrix} \lambda_1^{p^n} & 0 & ... & 0 \\ 0 & \lambda_2^{p^n} & ... & 0 \\ ... & ... & ... & ... \\ 0 & 0 & ... & \lambda_n^{p^n} \end{pmatrix} \cdot T^{-1} = T \cdot \begin{pmatrix} \lambda_1 & 0 & ... & 0 \\ 0 & \lambda_2 & ... & 0 \\ ... & ... & ... & ... \\ 0 & 0 & ... & \lambda_n \end{pmatrix} \cdot T^{-1} = A_f,$$

that is, the first condition. For the second, from the relations:

$$A_f^{p^m} - A_f = T \cdot \begin{pmatrix} \lambda_1^{p^m} & 0 & ... & 0 \\ 0 & \lambda_2^{p^m} & ... & 0 \\ ... & ... & ... & ... \\ 0 & 0 & ... & \lambda_n^{p^m} \end{pmatrix} \cdot T^{-1} - T \cdot \begin{pmatrix} \lambda_1 & 0 & ... & 0 \\ 0 & \lambda_2 & ... & 0 \\ ... & ... & ... & ... \\ 0 & 0 & ... & \lambda_n \end{pmatrix} \cdot T^{-1} =$$

$$= T \cdot \begin{pmatrix} \lambda_1^{p^m} - \lambda_1 & 0 & ... & 0 \\ 0 & \lambda_2^{p^m} - \lambda_2 & ... & 0 \\ ... & ... & ... & ... \\ 0 & 0 & ... & \lambda_n^{p^m} - \lambda_n \end{pmatrix} \cdot T^{-1}$$

we infer that the number $n - rang\left(A_f^{p^m} - A_f \right)$ is exactly the number of $\lambda_i; \lambda_i^{p^m} - \lambda_i = 0$. But such roots vanish an irreducible m-degree polynomial; $m<n$ and then f is reducible.

Conversely, the first condition means that $\lambda_1, \lambda_2, ..., \lambda_n$ are roots of irreducible polynomials those degree are divisors of n. The second condition assures that these degrees are not less then n. Q.E.D.

3. **REMARK**

The theorem provides the following algorithm to test the irreducibility of an n-degree polynomial f: for $m = 1, 2, ..., \frac{n}{2}$ is to calculate $A_f^{p^m} = \left(A_f^{p^{m-1}} \right)^p ; r_m = rang\left(A_f^{p^m} - A_f \right)$.If all the numbers r_m are equal to n we deduce f is irreducible. Otherwise, if m is the first number having $r_m<n$ then f has m-degree irreducible factors. Their number is $\frac{1}{m}(n - r_m)$.

For $p=2$ the algorithm is simpler: it consists from successive squaring of matrices starting with A_f.

4. CONCLUSIONS

The method use matricial calculus to test the irreducibility of polynomials, used in making the codes. The most used case is $p=2$ for which the algorithm is simpler. One can test the irreducibility of large degree polynomials with an ordinary PC.

REFERENCES

[1] S. LANG *Algebra*, Addison Wesley Publishing Company, New York, 1969

[2] C. DOCHIȚOIU, *Algebraic closure of a finite field,* Proceedings of the SSM Conference, Craiova, 1999.