MATHEMATICS OF COMPUTATION
VOLUME 59, NUMBER 200
OCTOBER 1992, PAGES 639-643

PRIMITIVE POLYNOMIALS OVER FINITE FIELDS

TOM HANSEN AND GARY L. MULLEN

ABSTRACT. In this note we extend the range of previously published tables of primitive polynomials over finite fields. For each $p^n < 10^{50}$ with $p \leq 97$ we provide a primitive polynomial of degree n over F_p. Moreover, each polynomial has the minimal number of nonzero coefficients among all primitives of degree n over F_p.

1. INTRODUCTION

Let F_q denote the finite field of order $q = p^n$, where p is prime and $n \geq 1$. The multiplicative group F_q^* of nonzero elements of F_q is cyclic and a generator of F_q^* is called a primitive element. Moreover, a monic irreducible polynomial whose roots are primitive elements is called a primitive polynomial. It is well known that the field F_q can be constructed as $F_p[x]/(f(x))$, where $f(x)$ is an irreducible polynomial of degree n over F_p and, in addition, if $f(x)$ is primitive, then F_q^* is generated multiplicatively by any root of $f(x)$. With the recent availability of faster machines there is a need to significantly extend the range of published tables of primitive polynomials so as to be able to implement the arithmetic of larger fields for various applications in a variety of areas. In this note we exhibit for each prime power $p^n < 10^{50}$ with $p \leq 97$ a primitive polynomial of degree n over F_p. Moreover, for each such p and n we have listed a primitive of degree n over F_p with the minimal number of nonzero coefficients among all primitives of degree n over F_p. In addition to the tables presented in §4 we propose in §5 two conjectures concerning the distribution of primitive and irreducible polynomials over finite fields.

2. PUBLISHED TABLES

Table F of Lidl and Niederreiter [9], which is taken from Alanen and Knuth [1], lists one primitive of degree n over F_p for $p^n < 10^9$ with $p \leq 47$. Sugimoto [14] extended this for the same primes p to the range $p^n < 10^{19}$. Because of applications in a variety of areas, including information theory, tables with larger ranges are available for $p = 2$. In particular, Watson [15] gives for $n \leq 100$ one primitive of degree n over F_2, and Stahnke [13] lists for each $n \leq 168$ a primitive with a minimum number of nonzero coefficients.

Received by the editor February 7, 1991 and, in revised form, October 8, 1991.
1991 *Mathematics Subject Classification*. Primary 11T06.
Key words and phrases. Finite field, primitive polynomial.
The authors would like to thank the NSA for partial support under the second author's grant agreement #MDA904-87-H-2023.

Zierler and Brillhart [17, 18] greatly extended this work by listing all primitive trinomials of degree n over F_2 with $n \leq 1000$. The tables of [17,18] also give all irreducible trinomials of degree $n \leq 1000$ and their orders. Green and Taylor [8] list one primitive over F_q of degree n with $q = 4$, $n \leq 11$; $q = 8$, $n \leq 7$; $q = 9$, $n \leq 7$; and $q = 16$, $n \leq 5$. Beard and West [3] study special types of primitive polynomials over F_q, and Peterson and Weldon [12] give all irreducibles over F_2 with $n \leq 16$. For $17 \leq n \leq 34$ they give a primitive with a minimum number of nonzero coefficients and an irreducible belonging to each possible order.

3. Primitive polynomials

Given a monic polynomial of degree n over F_q, the following provides an algorithm to test for primitivity, see Lidl and Niederreiter [9, Theorem 3.18].

Theorem 1. *The monic polynomial $f \in F_q[x]$ of degree $n \geq 1$ is a primitive polynomial over F_q if and only if $(-1)^n f(0)$ is a primitive element of F_q and the least positive integer r for which x^r is congruent* $\bmod f(x)$ *to some element of F_q is $r = (q^n - 1)/(q-1)$. If $f(x)$ is primitive over F_q, then $x^r \equiv (-1)^n f(0)$* $(\bmod f(x))$.

The following algorithm, which is a simplified version of Theorem 1, was implemented on a SUN 460 workstation to test a polynomial $f(x)$ of degree n over F_p for primitivity. As a precomputation, for a given p and n, the prime factorization of $p^n - 1$ was obtained using the computer programs Mathematica [16], PARI [2], a General Factorization and Primality Testing Program [4], and the tables from the Cunningham Project [5].

Only those $f(x)$ for which $(-1)^n f(0)$ is a primitive element in F_p need be considered. First, $f(\theta)$ is calculated for each $\theta \in F_p^*$ to eliminate those f's with linear factors. Then the rank of the Berlekamp matrix is calculated to eliminate reducible polynomials for which the rank is of course less than $n - 1$, see [9, §4.1].

The residue of $x^{(p^n-1)/(p-1)}$ $(\bmod f(x))$ is calculated, and if $x^{(p^n-1)/(p-1)} \not\equiv (-1)^n f(0)$ $(\bmod f(x))$, then $f(x)$ is not primitive. If $x^{(p^n-1)/(p-1)} \equiv (-1)^n f(0)$ $(\bmod f(x))$, we proceed as follows. For each prime factor s of $(p^n - 1)/(p-1)$ such that s does not divide $p - 1$, the residue of $x^{(p^n-1)/((p-1)s)}$ $(\bmod f(x))$ is calculated. If, for one such s we have $x^{(p^n-1)/((p-1)s)} \equiv b$ $(\bmod f(x))$ with $b \in F_q$, then $f(x)$ is not primitive. If for all such s, $x^{(p^n-1)/((p-1)s)} \not\equiv b$ $(\bmod f(x))$ with $b \in F_q$, then $f(x)$ is a primitive polynomial of degree n over F_p.

4. Tables

In the Supplement section at the end of this issue we provide tables of the primitive polynomials obtained from the calculations described in §3. For each $p^n < 10^{50}$ with $p \leq 97$, we provide a primitive polynomial of degree n over F_p. Moreover, each polynomial has the minimal number of nonzero coefficients (minimal Hamming weight) among all primitives of degree n over F_p.

In our search procedure, for a given p and n, we first tried to locate a primitive trinomial of degree n over F_p. Failing this, a search was conducted among polynomials of Hamming weight four, then five, etc. Among those polynomials of a given weight, say among trinomials for example, polynomials were tested for primitivity in the following order. Consider $f(x) = x^n + \sum_{i=0}^{n-1} a_i x^i$ of degree n over F_p. Let $N_f = p^n + \sum_{i=0}^{n-1} a_i p^i$ be the corresponding number in base p. Thus, among the trinomials of degree n over F_p, $f(x)$ was tested for primitivity before $g(x)$ if $N_f < N_g$. Subject to this ordering, the first primitive polynomial obtained is listed in the table.

Each polynomial has minimal Hamming weight among all primitives of degree n over F_p. Primitive 5-nomials were of minimal weight for some values of n in the $p = 2$ case, and for $p = 3$ with $n = 48, 72, 96$. In all other cases we have a primitive of degree n with weight at most 4.

In the tables only the nonzero terms are represented, so that for example over F_7, the polynomial $x^{14} + 2x^5 + 3$ is represented as $14:1,\ 5:2,\ 0:3$. Copies of the tables and/or programs, either in electronic or hardcopy form, are available upon request from the authors.

5. Two conjectures

Before closing, we raise two conjectures concerning the distribution of primitive and irreducible polynomials over finite fields. We also provide some evidence for each of the conjectures.

Conjecture A. *Let $a \in F_q$, let $n \geq 2$ and fix $0 \leq j < n$. Then there exists a primitive polynomial $f(x) = x^n + \sum_{k=0}^{n-1} a_k x^k$ of degree n over F_q with $a_j = a$ except when*

- (A1) *q arbitrary, $j = 0$, and $a \neq (-1)^n \alpha$, where $\alpha \in F_q$ is a primitive element;*
- (A2) *q arbitrary, $n = 2$, $j = 1$, and $a = 0$;*
- (A3) *$q = 4$, $n = 3$, $j = 2$, and $a = 0$;*
- (A4) *$q = 4$, $n = 3$, $j = 1$, and $a = 0$;*
- (A5) *$q = 2$, $n = 4$, $j = 2$, and $a = 1$.*

Theorem 1 implies that the constant term of a primitive polynomial must be of the form $(-1)^n \alpha$ with α primitive in F_q, and hence (A1) is a necessary exception. Clearly, $x^2 + a$ cannot be primitive over F_q, and so we have (A2). From [8, Table 1] we deduce the exceptions (A3) and (A4). Exceptions (A3) and (A4) will also be excluded as a result of Theorem 2 below. Exception (A5) arises from Table F of [9].

Conjecture A states that with the five necessary exceptions, there exists a primitive polynomial of degree n over F_q with the coefficient of any fixed power of x prescribed in advance.

For irreducible polynomials we propose:

Conjecture B. *Let $a \in F_q$, let $n \geq 2$ and fix $0 \leq j < n$. Then there exists an irreducible polynomial $f(x) = x^n + \sum_{k=0}^{n-1} a_k x^k$ over F_q with $a_j = a$ except when*

- (B1) *q arbitrary and $j = a = 0$;*
- (B2) *$q = 2^m$, $n = 2$, $j = 1$, and $a = 0$.*

Clearly, (B1) must be an exception, for otherwise $f(x)$ is divisible by x. As for (B2), in characteristic two, every element of F_q is a square, and so $x^2 + a = (x+b)^2$ is reducible. Conditions (A3) and (A4) for primitivity may now be removed because such irreducibles exist by [8, Table 1]. Similarly, (A5) may be removed because of Table F of [9].

As evidence for Conjectures A and B we first note that Table F of [9] supports both conjectures for small p and n, and Tables 1–4 of [8] support the conjectures for small n and nonprime q. The chief theoretical result in this direction is the following result of Cohen [7, Theorem 1]. We remind the reader that, if $n \geq 2$, the trace function is defined from F_{q^n} to F_q by $\mathrm{TR}(\gamma) = \gamma + \gamma^q + \gamma^{q^2} + \cdots + \gamma^{q^{n-1}}$.

Theorem 2. *Let $n \geq 2$ and let $a \in F_q$ with $a \neq 0$ if $n = 2$ or if $n = 3$ and $q = 4$. Then there exists a primitive polynomial of degree n over F_q with trace a.*

Cohen [7] proved that F_{q^n} contains a primitive element γ with $\mathrm{TR}(\gamma) = a$ over F_q, where the trace of γ is of course the negative of the coefficient of x^{n-1} in the minimal polynomial of γ over F_q. Cohen's theorem explains the exceptions (A2) and (A3) and indirectly (A4), since if $f(x)$ is primitive, so is the reciprocal polynomial $f^*(x)$ of $f(x)$, namely, $f^*(x) = x^n f(1/x)$, which accounts for (A4). His result proves that among the primitives of degree n, the coefficients of x^{n-1} satisfy Conjecture A, and since every primitive is irreducible, Conjecture B as well.

We now show that the constant terms of the primitive and irreducible polynomials satisfy Conjectures A and B. For Conjecture A, let α be a primitive element in F_{q^n} and let $f_\alpha(x)$ be the minimal polynomial of α over F_q with constant term $(-1)^n a$, where by Theorem 1, a is a primitive element in F_q and moreover, $a = \alpha^{(q^n-1)/(q-1)}$. Let b be a primitive element in F_q and let $b = a^l$ with $1 \leq l \leq q-2$. Choose k so that $(k, q^n - 1) = 1$ and $k \equiv l \pmod{q-1}$. Then α^k is primitive in F_{q^n} and hence the minimal polynomial $g(x)$ of α^k is a monic primitive of degree n over F_q and, moreover, the constant term of $g(x)$ is $(-1)^n \alpha^{k(q^n-1)/(q-1)} = (-1)^n a^k = (-1)^n a^l = (-1)^n b$.

For Conjecture B, let $c \neq 0 \in F_q$, so $c = a^m$ with $0 \leq m \leq q-2$. The element α^m cannot be in any proper subfield of F_{q^n}, for otherwise $\alpha^{m(q^t-1)} = 1$ with $t|n$, a contradiction, since α has order $q^n - 1$. Hence, the minimal polynomial $h(x)$ of α^m is a monic irreducible of degree n over F_q with constant term $(-1)^n \alpha^{m(q^n-1)/(q-1)} = (-1)^n c$. Thus, the constant terms indeed satisfy Conjectures A and B.

From the above discussion we see that Conjectures A and B hold for polynomials of degree two. We also note that if $f(x)$ is irreducible, so is $f(x+e)$ for $e \in F_q$, and if a primitive (irreducible) polynomial $f(x)$ has 0 coefficient of x^{n-k} for $1 \leq k < n$, then the primitive (irreducible) polynomial $(1/f(0))f^*(x)$ has 0 coefficient of x^k, where $f^*(x)$ is the reciprocal of $f(x)$. Finally, if $f(x)$ is irreducible of degree n over F_q, then $f^Q(x) = x^n f(x + 1/x)$ is irreducible if and only if $x^2 - \beta x + 1$ is irreducible over F_{q^n}, where β is any root of $f(x)$, see Meyn [10, Lemma 5], also Niederreiter [11] and Cohen [6] for related results. These simple transformations can of course be repeatedly applied to obtain further evidence for the conjectures.

If Conjectures A and B are true, then the primitive and irreducible polynomials of fixed degree over F_q are in a limited way rather uniformly distributed over F_q.

ACKNOWLEDGMENT

We would like to thank C. Batut, D. Bernardi, H. Cohen, and M. Olivier for providing a copy of PARI and D. M. Bressoud for providing a copy of A General Factorization and Primality Testing Program that were extremely helpful in our calculations. Thanks are also due J. V. Brawley and W.-S. Chou for helpful discussions.

BIBLIOGRAPHY

1. J. D. Alanen and D. E. Knuth, *Tables of finite fields*, Sankhyā Ser. A **26** (1964), 305–328.
2. C. Batut, D. Bernardi, H. Cohen, and M. Olivier, *PARI*, Version 1.32, 1989, 1990.
3. J. T. B. Beard, Jr. and K. I. West, *Some primitive polynomials of the third kind*, Math. Comp. **28** (1974), 1166–1167.
4. D. M. Bressoud, *A general factorization and primality testing program*, The Pennsylvania State University, 1988.
5. J. Brillhart, D. H. Lehmer, J. L. Selfridge, B. Tuckerman, and S. S. Wagstaff, Jr., *Factorizations of* $b^n \pm 1$, $b = 2, 3, 5, 6, 7, 10, 11, 12$ *up to high powers*, Contemp. Math., Vol. 22, Amer. Math. Soc., Providence, R. I., 1983.
6. S. D. Cohen, *On irreducible polynomials of certain types in finite fields*, Proc. Cambridge Philos. Soc. **66** (1969), 335–344.
7. ——, *Primitive elements and polynomials with arbitrary trace*, Discrete Math. **83** (1990), 1–7.
8. D. H. Green and I. S. Taylor, *Irreducible polynomials over composite Galois fields and their applications in coding techniques*, Proc. IEE **121** (1974), 935–939.
9. R. Lidl and H. Niederreiter, *Finite fields*, Encyclopedia Math. Appl., Vol. 20, Addison-Wesley, Reading, Mass., 1983 (Now distributed by Cambridge Univ. Press).
10. H. Meyn, *On the construction of irreducible self-reciprocal polynomials over finite fields*, Applicable Algebra in Eng., Comm. and Comp. **1** (1990), 43–53.
11. H. Niederreiter, *An enumeration formula for certain irreducible polynomials with an application to the construction of irreducible polynomials over the binary field*, Applicable Algebra in Eng., Comm. and Comp. **1** (1990), 119–124..
12. W. W. Peterson and E. J. Weldon, Jr., *Error-correcting codes*, 2nd ed., M.I.T. Press, Cambridge Mass., 1972.
13. W. Stahnke, *Primitive binary polynomials*, Math. Comp. **27** (1973), 977–980.
14. E. Sugimoto, *A short note on new indexing polynomials of finite fields*, Inform. and Control **41** (1979), 243–246.
15. E. J. Watson, *Primitive polynomials* $\pmod 2$, Math. Comp. **16** (1962), 368–369.
16. S. Wolfram, Mathematica (sun 3.68881) 1.2, 1988, 1989.
17. N. Zierler and J. Brillhart, *On primitive trinomials* $\pmod 2$, Inform. and Control **13** (1968), 541–554.
18. ——, *On primitive trinomials* $\pmod 2$, II, Inform. and Control **14** (1969), 566–569.

DEPARTMENT OF MATHEMATICS, THE PENNSYLVANIA STATE UNIVERSITY, UNIVERSITY PARK, PENNSYLVANIA 16802

E-mail address, G. L. Mullen: mullen@math.psu.edu

E-mail address, T. Hansen: pho3@math.psu.edu