MATHEMATICS OF COMPUTATION
VOLUME 63, NUMBER 208
OCTOBER 1994, PAGES 759–765

PRIMITIVE NORMAL POLYNOMIALS OVER FINITE FIELDS

ILENE H. MORGAN AND GARY L. MULLEN

ABSTRACT. In this note we significantly extend the range of published tables of primitive normal polynomials over finite fields. For each $p^n < 10^{50}$ with $p \leq 97$, we provide a primitive normal polynomial of degree n over F_p. Moreover, each polynomial has the minimal number of nonzero coefficients among all primitive normal polynomials of degree n over F_p. The roots of such a polynomial generate a primitive normal basis of F_{p^n} over F_p, and so are of importance in many computational problems. We also raise several conjectures concerning the distribution of such primitive normal polynomials, including a refinement of the primitive normal basis theorem.

1. INTRODUCTION

For q a prime power and $n \geq 2$ an integer, let F_q denote the finite field of order q. It is well known that F_{q^n} can be viewed as a vector space of dimension n over F_q. A basis of F_{q^n} over F_q of the form $\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}$ is called a normal basis, and if α is also a primitive element of F_{q^n}, i.e., if α generates the multiplicative group $F_{q^n}^*$, then the basis is said to be a primitive normal basis.

Normal and primitive normal bases are of great importance in many computational problems involving finite fields, and so there has been considerable effort directed to discussing various methods of obtaining such elements. It is well known that for any prime power q and any integer $n \geq 2$, F_{q^n} contains a normal basis over F_q; see for example Lidl and Niederreiter [17, Theorem 3.73]. In [7], Davenport showed that if $q = p$ is a prime, then for each $n \geq 2$, F_{p^n} contains a primitive element α that generates a primitive normal basis of F_{p^n} over F_p, and in [4], Carlitz showed that for sufficiently large q^n, F_{q^n} contains a primitive element that generates a primitive normal basis over F_q. Recently, Lenstra and Schoof [15] showed that for every prime power q and every integer $n \geq 2$, F_{q^n} contains a primitive normal basis over F_q. This result completely settled the question of the existence of primitive normal bases over finite fields, although the above methods are all nonconstructive. Hachenberger [11] gives an alternative proof of the primitive normal basis theorem, which at least theoretically provides a method to determine all primitive normal elements.

Received by the editor August 23, 1993.
1991 *Mathematics Subject Classification.* Primary 11T06; Secondary 11T30.
Key words and phrases. Finite field, primitive normal basis.
We would like to thank the National Security Agency for partial support under the second author's grant agreement #MDA904-92-H-3044.

0025-5718/94 $1.00 + $.25 per page

For the more practical matter of finding a primitive normal element, Stepanov and Shparlinski [26] give an upper bound N so that if $\beta \in F_{q^n}$ is a fixed primitive element, then the sequence $\beta, \beta^2, \ldots, \beta^N$ must contain an element that generates a primitive normal basis. In [9] von zur Gathen and Giesbrecht provide a probabilistic polynomial-time algorithm for the determination of a primitive normal element. Shoup [24] considers the problem of how to deterministically generate in polynomial time a subset of F_{p^n} that contains a primitive element. See also Menezes [18, Chapters 4–5] and Shparlinski [25, Chapters 2–5] for discussions of various algorithms and theoretical results concerning the distribution of primitive normal elements. For a discussion of various other kinds of bases, see for example [8, 14, 19, 21–23]. We also refer to Lidl [16, §3] for a discussion of a number of recent results related to various types of bases over finite fields, and we refer to [1] for a discussion of algorithmic computations involving primitive and normal elements in the field F_{2^m}. In [20], Niederreiter shows that normal bases are useful in the problem of factoring polynomials over finite fields.

A monic polynomial $f(x)$ of degree n over F_q is called a primitive (resp. normal) polynomial if it is the minimal polynomial of a primitive element of F_{q^n} (resp. it is the minimal polynomial of an element which generates a normal basis of F_{q^n} over F_q). Alternatively, $f(x)$ is primitive if $q^n - 1$ is the smallest positive integer s such that $f(x)$ divides $x^s - 1$, and it is normal if any root of $f(x)$ generates a normal basis of F_{q^n} over F_q. Thus, $f(x)$ is normal if $f(x)$ belongs to the linearized polynomial $x^{q^n} - x$ so that the monic linearized polynomial of least degree satisfied by a root of $f(x)$ is the linearized polynomial $x^{q^n} - x$. Recall that a linearized polynomial is a polynomial of the form $\sum_{i=0}^{n-1} a_i x^{q^i}$ with $a_i \in F_{q^n}$. In the terminology of Beard and West [3], a primitive (resp. normal) polynomial is said to be of the first (resp. second) kind, and a polynomial which is both primitive and normal is said to be of the third kind. We will however use the more natural terms of primitive (resp. normal) polynomials and simply say that a polynomial is a primitive normal polynomial if it is both primitive and normal.

It is known that there are $\phi(q^n - 1)/n$ primitive polynomials of degree n over F_q, where ϕ denotes Euler's totient function from elementary number theory; see [17, Theorem 3.5]. Moreover, there are $\Phi_q(x^n - 1)/n$ normal polynomials of degree n over F_q, where Φ_q denotes the Euler function defined on the ring $F_q[x]$; see [17, §3.4]. Very recently, Akbik [2] has obtained an apparently different formula for the number of normal basis generators of F_{p^n} over F_p with p prime, although that formula is, in reality, just a different way of rewriting the standard formula $\Phi_q(x^n - 1)/n$.

While there is no known closed formula for the number of primitive normal polynomials of degree n over F_q, Carlitz [4] obtained the asymptotic bound that there are N'/n primitive normal polynomials over F_q of degree n, where

$$N' = \phi(q^n - 1)\Phi_q(x^n - 1)/q^n + O(q^{n(1/2+\epsilon)}),$$

the implied constant depending only upon ϵ.

For each p, d, and n satisfying $p < 10^2$, $p^d < 10^3$, and $p^{dn} < 10^6$, Beard and West [3] provided a primitive normal polynomial of degree n over F_{p^d}. Very recently, Gulliver, Serra, and Bhargava [10] gave lists of primitive normal

polynomials of small degrees over F_q for $q \leq 19$ except for $q = 9$. (It should be pointed out that their polynomial 11000002 over F_{17} cannot be primitive since -2 is not a primitive element in F_{17}; see Theorem 1 below. A primitive normal polynomial is 11000007.)

The purpose of this paper is to significantly extend the range of published tables of primitive normal polynomials over prime fields. The range of our tables is $p^n < 10^{50}$ with $p \leq 97$. Moreover, each of our polynomials has at most five nonzero coefficients. Such polynomials with small Hamming weight provide for easy implementation of the corresponding extension field arithmetic, and so our tables are intended to provide the practitioner with an easily accessible collection of primitive normal polynomials for use in various applications.

While extensive tables of primitive polynomials are available, see for example Hansen and Mullen [12], most of those polynomials are not normal since their trace coefficients are 0, and thus they cannot be used to generate a normal basis of F_{p^n} over F_p.

The following results from Lidl and Niederreiter [17, Theorem 3.18 and Corollary 2.39] provide algorithms for testing whether a given polynomial $f(x)$ of degree n over F_q is primitive and normal.

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* mod $f(x)$ *to some element of F_q is $r = (q^n - 1)/(q - 1)$.*

Theorem 2. *For $\alpha \in F_{q^n}$, $\{\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}\}$ is a normal basis of F_{q^n} over F_q if and only if the polynomials $x^n - 1$ and $\alpha x^{n-1} + \alpha^q x^{n-2} + \cdots + \alpha^{q^{n-2}} x + \alpha^{q^{n-1}}$ in $F_{q^n}[x]$ are relatively prime.*

2. Tables

The methods of Hansen and Mullen [12] provide the starting point for our search. Because of the availability of software programs used in [12], we have used the following strategy in searching for a primitive normal polynomial over F_p, even though some of the methods discussed in §1 at least theoretically provide faster algorithms. We first locate a primitive polynomial of degree n over F_p, as in [12], using Theorem 1. If a polynomial is primitive by Theorem 1, then the Euclidean algorithm is used to test a root α of the polynomial against Theorem 2 in order to determine whether the polynomial is a normal polynomial, and hence whether its roots generate a normal basis of F_{p^n} over F_p.

For ease of implementation of extension field arithmetic by a practitioner, our search has focused on polynomials of low Hamming weight, i.e., on polynomials with a small number of nonzero coefficients. In particular, for each p and n, the polynomial which we have listed has the minimal weight among all primitive normal polynomials of degree n over F_p. In addition, the given polynomial is the first primitive normal polynomial obtained among all polynomials of that weight which were tested in the following natural order as in [12]. 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 polynomials of the same weight, $f(x)$ was tested before $g(x)$ if $N_f < N_g$. Subject to this ordering, the

first primitive normal polynomial obtained is listed in the table. (Note that any normal polynomial must have nonzero trace coefficient, i.e., the coefficient of x^{n-1} must be nonzero.) An asterisk denotes the fact that for the given polynomial $f(x)$, the reciprocal polynomial $f(x)^* = x^n f(1/x)$ is also primitive normal. The reciprocal of a primitive polynomial is of course always primitive, but the reciprocal of a normal polynomial is not always normal.

In the Supplement section at the end of this issue we provide tables of the primitive normal polynomials obtained using the procedure described above. For each $p^n < 10^{50}$ with $p \leq 97$, we provide a primitive normal polynomial of degree n over F_p. As in [12], only the nonzero coefficients are listed so that, for example, the polynomial $x^8 + x^7 + 3$ over F_7 is listed as 8:1, 7:1, 0:3. Copies of the tables either in hardcopy or electronic form are available from the authors.

3. Conjectures

In this section we raise several conjectures concerning the distribution of primitive normal polynomials over finite fields. We remind the reader that if $n \geq 2$, the trace function is defined from F_{q^n} to F_q by $\mathrm{TR}(\gamma) = \gamma + \gamma^q + \gamma^{q^2} + \cdots + \gamma^{q^{n-1}}$, and that, if γ has degree n over F_q, 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. We first recall that in [5] Cohen showed that, except for several necessary exceptions, there is for every prime power q and every integer $n \geq 2$, a primitive polynomial of degree n over F_q with an arbitrarily specified trace coefficient. More specifically, he proved:

Theorem 3. *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.*

Based upon computer evidence and several special cases below, we propose the following refinement of the primitive normal basis theorem of Lenstra and Schoof [15] as well as the above result of Cohen:

Conjecture 1. *Let $n \geq 2$ and let $a \in F_q$ with $a \neq 0$. Then there exists a primitive normal polynomial of degree n over F_q with trace a.*

We note that Cohen [6, p. 53] alludes to a special case of Conjecture 1 and also briefly discusses a possible method of attack. If a denotes the trace coefficient of a normal polynomial $f(x)$ of degree n, then clearly a cannot be zero; otherwise, the roots of f would not be independent, and hence they could not form a basis of F_{q^n} over F_q. Conjecture 1 is thus clearly true for $q = 2$, and it follows from Hachenberger [11, p. 146] and Theorem 3, that the conjecture is also true for $n = 2$ and any prime power q.

Theorem 4. *If every prime factor of $q - 1$ divides n, then for every nonzero element $b \in F_q$ there is a primitive normal polynomial with trace coefficient b.*

Proof. Let α be a primitive normal element in F_{q^n}. We just need to check that $b\alpha$ is also a primitive normal element for every nonzero element $b \in F_q$. Clearly, $b\alpha$ is a normal element. Let $w = (q^n - 1)/(q - 1)$, and let $a = \alpha^w$ be the norm of α over F_q. Then a is primitive in F_q and $b = a^t$ for some

$0 < t \leq q-2$. Moreover, $b\alpha = \alpha^{wt+1}$ and $b\alpha$ is primitive if and only if

$$1 = \gcd(wt+1, q^n-1) = \gcd(wt+1, q-1) = \gcd(nt+1, q-1).$$

Since every prime factor of $q-1$ is a divisor of n, we have

$$\gcd(nt+1, q-1) = 1.$$

Thus, $b\alpha$ is primitive for every nonzero $b \in F_q$ and the proof is complete. □

Corollary 5. *Conjecture* 1 *is true whenever* n *is a multiple of* $q-1$.

The following elementary argument provides a class of values of q for which Conjecture 1 is also true. Assume that $f(x) = x^n + bx^{n-1} + \cdots + b_1x + b_0$ with $b \neq 0$ is a primitive normal polynomial over F_q, $\alpha \in F_{q^n}$ is a root of $f(x)$, and that $\mathrm{TR}(\alpha) = -b$. If $c \neq 0 \in F_q$, then clearly $c\alpha$ also generates a normal basis of F_{q^n} over F_q, and moreover, $\mathrm{TR}(c\alpha) = -cb$. Since α is a primitive element of F_{q^n}, we may write $c \in F_q$ as $c = \alpha^{k(q^{n-1}+q^{n-2}+\cdots+q+1)}$, $0 \leq k < q-1$. Thus, the order of $c\alpha$ is $\frac{q^n-1}{\gcd(q^n-1, k(q^{n-1}+q^{n-2}+\cdots+q+1)+1)}$. As a result, Conjecture 1 will be true if $c\alpha$ is a primitive element for each $c \neq 0 \in F_q$, i.e., if $\gcd(q-1, k(q^{n-1}+q^{n-2}+\cdots+q+1)+1) = 1$, for $k = 0, 1, \ldots, q-2$.

If Conjecture 1 fails, it is most likely to fail for small values of q and n. However, it has been verified by machine calculation to be true for all prime powers $q \leq 97$ with $n \leq 6$.

We also propose the following conjecture, which is a refinement of the analogous conjecture of Hansen and Mullen [13, p. 434] for primitives over a field with a prime number of elements.

Conjecture 2. (1) *For each prime* p *and each* $n \geq 2$ *there exists a primitive normal polynomial of degree* n *over* F_p *with at most five nonzero coefficients.*

(2) *If* $p \geq 11$, *then there is a primitive normal polynomial of degree* n *over* F_p *with at most four nonzero coefficients.*

It may be that (2) holds for $p > 3$ except for $p = 5$, $n = 32$ and $p = 7$, $n = 24$.

The following algorithm can be used to construct a primitive (normal) polynomial of degree n over a nonprime field F_{p^m} of order p^m. Let f be a primitive polynomial of degree mn over F_p, taken for example from [12]. Choose an element $\beta \in F_{p^{mn}}$ whose order is equal to $p^{mn}-1$ so that β is a primitive element in $F_{p^{mn}}$. Calculate the minimal polynomial $M_\beta(x)$ of β over $F_{p^m} = F_q$ as $M_\beta(x) = \prod_{i=0}^{n-1}(x - \beta^{q^i})$, which according to [17, Corollary 2.19] is a primitive polynomial of degree n over F_{p^m}. In order to check whether β generates a normal basis of $F_{p^{mn}}$ over F_{p^m}, we now simply apply Theorem 2. This technique was in fact used to verify Conjecture 1 for all prime powers $q \leq 97$ with $n \leq 6$.

As an illustration of this technique, as in Table A of [17], assume that $F_{2^4}^*$ is multiplicatively generated by a root α of the primitive polynomial $x^4 + x^3 + 1$ over F_2. Let $\beta = \alpha$ so that β and β^4 form a primitive normal basis of F_{16} over F_4. Consequently, the minimal polynomial $M_\beta(x)$ of β over F_4 given by $(x-\beta)(x-\beta^4) = x^2 + \alpha^5x + \alpha^5$ is a primitive polynomial of degree 2 over F_4. Similarly, if $\gamma = \alpha^2$, then γ and γ^4 form a primitive normal basis, and the minimal polynomial $M_\gamma(x) = x^2 + \alpha^{10}x + \alpha^{10}$ is primitive

normal. Analogously, if $\delta = \alpha^7$ and $\epsilon = \alpha^{11}$, then $M_\delta(x) = x^2 + x + \alpha^5$ and $M_\epsilon(x) = x^2 + x + \alpha^{10}$ are also primitive normal polynomials over F_4. Moreover, $x^4 + x^3 + 1 = M_\beta(x)M_\gamma(x)$ and $x^4 + x + 1 = M_\delta(x)M_\epsilon(x)$.

Alternatively, one could proceed as follows to construct a primitive (normal) polynomial of degree n over a nonprime field F_{p^m}. As above, let f be a primitive polynomial of degree mn over F_p. Then by [17, Theorem 3.46], f factors over F_{p^m} into m irreducibles, each of degree n. Moreover, from [17, Corollary 2.19], each irreducible factor is a primitive polynomial of degree n over F_{p^m}. As above, Theorem 2 can then be applied to determine whether a root of such a primitive polynomial generates a normal basis.

Acknowledgment

We would like to thank the PSU Mathematics Department for use of its network of SUN workstations. Special thanks are due Tom Hansen for use of several programs from [12] and Gerry McKenna for use and technical support of his finite field software package as well as a number of helpful comments. Without their assistance, this project would not have been undertaken. Finally, we thank Shuhong Gao for his proof of Theorem 4, and the referee for pointing out several misprints in an earlier version.

Bibliography

1. G. B. Agnew, T. Beth, R. C. Mullin, and S. A. Vanstone, *Arithmetic operations in* $GF(2^m)$, J. Cryptology **6** (1993), 3–13.
2. S. Akbik, *Normal generators over finite fields*, J. Number Theory **41** (1992), 146–149.
3. J. T. Beard and K. I. West, *Some primitive polynomials of the third kind*, Math. Comp. **28** (1974), 1166–1167.
4. L. Carlitz, *Primitive roots in a finite field*, Trans. Amer. Math. Soc. **73** (1952), 373–382.
5. S. D. Cohen, *Primitive elements and polynomials with arbitrary trace*, Discrete Math. **83** (1990), 1–7.
6. S. D. Cohen, *Primitive elements and polynomials: existence results*, Finite Fields, Coding Theory, and Advances in Communications and Computing (G. L. Mullen and P. J.-S. Shiue, eds.), Lecture Notes in Pure and Appl. Math., vol. 141, Marcel Dekker, New York, 1993, pp. 43–55.
7. H. Davenport, *Bases for finite fields*, J. London Math. Soc. **43** (1968), 21–39; Addendum, *ibid.* **44** (1969), 378.
8. S. Gao and H. W. Lenstra, Jr., *Optimal normal bases*, Des. Codes Cryptog. **2** (1992), 315–323.
9. J. von zur Gathen and M. Giesbrecht, *Constructing normal bases in finite fields*, J. Symbolic Comput. **10** (1990), 547–570.
10. T. A. Gulliver, M. Serra, and V. K. Bhargava, *The generation of primitive polynomials in* $GF(q)$ *with independent roots and their applications for power residue codes, VLSI testing and finite field multipliers using normal basis*, Internat. J. Electron. **71** (1991), 559–576.
11. D. Hachenberger, *On primitive and free roots in a finite field*, Appl. Alg. Eng., Comm. Computing **3** (1992), 139–150.
12. T. Hansen and G. L. Mullen, *Primitive polynomials over finite fields*, Math. Comp. **59** (1992), 639–643; Supplement: **59** (1992), S47–S50.
13. ———, *Primitive polynomials of low weight*, Finite Fields, Coding Theory, and Advances in Communications and Computing (G. L. Mullen and P. J.-S. Shiue, eds.), Lecture Notes in Pure and Appl. Math., vol. 141, Marcel Dekker, New York, 1993, p. 434.
14. D. Jungnickel, *Finite fields*, Bibliographisches Institut, Mannheim, Germany, 1993.

15. H. W. Lenstra and R. J. Schoof, *Primitive normal bases over finite fields*, Math. Comp. **48** (1987), 217–231.

16. R. Lidl, *Computational problems in the theory of finite fields*, Appl. Alg. Eng., Comm. Computing **2** (1991), 81–89.

17. R. Lidl and H. Niederreiter, *Finite fields*, Encyclopedia Math. Appl., Vol. 20, Addison-Wesley, Reading, MA, 1983. (Now distributed by Cambridge Univ. Press.)

18. A. J. Menezes, ed., *Applications of finite fields*, Kluwer, Dordrecht, 1993.

19. R. C. Mullin, I. M. Onyszchuk, S. A. Vanstone, and R. M. Wilson, *Optimal normal bases in* $GF(p^n)$, Discrete Appl. Math. **22** (1988/89), 149–161.

20. H. Niederreiter, *Factoring polynomials over finite fields using differential equations and normal bases*, Math. Comp. **62** (1994), 819–830.

21. S. Schwarz, *Irreducible polynomials over finite fields with linearly independent roots*, Math. Slovaca **38** (1988), 147–158.

22. ———, *Construction of normal bases in cyclic extensions of a field*, Czechoslovak Math. J. **38** (1988), 291–312.

23. I. A. Semaev, *Construction of polynomials irreducible over a finite field with linearly independent roots*, Math. USSR-Sb. **63** (1989), 507–519.

24. V. Shoup, *Searching for primitive roots in finite fields*, Math. Comp. **58** (1992), 369–380.

25. I. E. Shparlinski, *Computational and algorithmic problems in finite fields*, Math. Appl., Kluwer, Dordrecht, 1992.

26. S. A. Stepanov and I. E. Shparlinski, *On construction of a primitive normal basis of a finite field*, Mat. Sbornik **180** (1989), 1067–1072; English transl. in Math. USSR-Sb. **67** (1990), 527–533.

27. ———, *On the construction of primitive elements and primitive normal bases in a finite field*, Computational Number Theory (Proc. Colloq. on Comput. Number Theory, Hungary), de Gruyter, Berlin, 1991, pp. 1–14.

Department of Mathematics and Statistics, University of Missouri-Rolla, Rolla, Missouri 65401-0249

E-mail address: imorgan@umr.edu

Department of Mathematics, The Pennsylvania State University, University Park, Pennsylvania 16802

E-mail address: mullen@math.psu.edu