MATHEMATICS OF COMPUTATION
Volume 67, Number 221, January 1998, Pages 337–341
S 0025-5718(98)00904-1

DISTRIBUTION OF IRREDUCIBLE POLYNOMIALS OF SMALL DEGREES OVER FINITE FIELDS

KIE H. HAM AND GARY L. MULLEN

ABSTRACT. D. Wan very recently proved an asymptotic version of a conjecture of Hansen and Mullen concerning the distribution of irreducible polynomials over finite fields. In this note we prove that the conjecture is true in general by using machine calculation to verify the open cases remaining after Wan's work.

For a prime power q let F_q denote the finite field of order q. Hansen and Mullen in [4, p. 641] raise

Conjecture B. *Let $a \in F_q$ and let $n \geq 2$ be a positive integer. Fix an integer j with $0 \leq j < n$. 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 $x^2 + a_0 = (x+b)^2$ is reducible.

Using character sum estimates, in [6, Cor. 5.8] Wan provides an asymptotic version of Conjecture B by proving:

Theorem 1. *If either $q > 19$ or $n \geq 36$, then Conjecture B is true.*

As Wan indicates in [6, p. 1197], "Actually the number of possible exceptions is much smaller. It should be quite realistic to completely settle Conjecture B by detailed arguments with perhaps some computer calculations." The purpose of this note is to point out that Conjecture B is indeed true in general.

We begin by first noting that Corollary 5.6 (and Corollary 5.3 for $q = 2$) of Wan [6] actually provide a smaller list of possible exceptions. We state these refinements as

Theorem 2. *Conjecture B is true for $a \neq 0 \in F_q$ if*
(i) *$q^{n-j-2} \geq (j+1)^4$ or $q^{j-1} \geq (n-j+1)^4$; (if $q = 2, 2^{n-j} \geq (j+1)^4$ or $2^{j-1} \geq (n-j+1)^4$);*
(ii) *For $a = 0$, if $q^{n-j-1} \geq (j+1)^4$ or $q^{j-1} \geq (n-j+1)^4$.*

By machine calculation each of the exceptions from Theorem 2 was checked and indeed an irreducible with the specified conditions to satisfy Conjecture B was found. However rather than listing all of these polynomials, we have provided in

Received by the editor May 20, 1996 and, in revised form, October 7, 1996.
1991 *Mathematics Subject Classification.* Primary 11T06.

Table A a collection of irreducibles, which along with use of the elementary fact that if a polynomial $f(x)$ is irreducible over F_q, then so is the reciprocal polynomial $f^*(x) = x^n f(1/x)$, shows that in all of the exceptional cases, there is indeed an irreducible with the specified property.

The following conventions have been used in listing the various polynomials. The coefficients of a polynomial are listed from highest degree on the left, to lowest degree on the right. In addition, capital letters $A, B, \ldots, I$ are used to denote the numbers $10, 11, \ldots, 18$. Thus for $q = 19$ and $n = 3$, the polynomial $x^3+3x^2+11x+1$ is represented by $13B1$.

For each non-prime value of q, in addition to the values of $q = p^m$ and the degree n, we have also listed a primitive polynomial $f(x)$ of degree m over F_p. Hence any root α of $f(x)$ multiplicatively generates the non-zero elements of F_q. Define $*$ by $\alpha^* = 0$. Then for $j = *, 0, 1, \ldots, q-2$, we list the element $\alpha^j \in F_q$ by j. Thus for the case $q = 2^2$, $n = 3$, and $f(x) = x^2 + x + 1$, the irreducible polynomial $x^3 + 0x^2 + \alpha x + 1$ of degree 3 over F_4 is listed as $0 * 10$.

TABLE A

$q = 2\ (n)$

(4)	(6)	(9)	(12)	(15)
11001	1000011	1101100001	1000000001001	1000000011100111
11111	1101101	(10)	1000001111011	(16)
(5)	(7)	10010000001	(13)	10000100000000111
101001	11110001	10100111101	10010001111111	10000000111000111
	(8)	(11)	(14)	(17)
	101100011	100011000011	100010000001011	100000000111000001
	100011101		100000011101011	

(18)	(19)	(20)	(21)
1000000000000001001	10000000001100100001	100000001000000010011	1000000000011000010001
1000000001111000101		100000000011100000001	

(22)	(23)	(24)
10000000001000000000111	100000000000100000111011	1000000000000000000011011
10000000000110000011101		1000000000001000000001101

$q = 3\ (n)$

(3)	(5)	(7)	(9)	(11)	(13)
1211	110111	10001111	1000011011	100000110011	10000001100121
(4)	101221	10002211	1000022021	100000221121	10000002200101
10012	(6)	(8)	(10)	(12)	(14)
12112	1000012	100000102	10002001021	1000000010011	100000000000111
11222	1001122	100011022	10000111111	1000001101111	100000011000121
	1102202	100022012	10000222021	1000002201101	100000022000201

(15)	(16)	(17)
1000000011000001	10000000020000121	100000002100000211
1000000022002021	10000000110000001	
	10000000220000021	

(18)	(19)
1000000000000000211	10000000021000002101
1000000001000001221	
1000000002000000001	

$q = 5\ (n)$

(3)	(4)	14331	111231	1001101	(7)	(8)	100033041
1011	11041	11441	103441	1012221	10040001	100000241	100044031
1021	10111	(5)	(6)	1003301	10012121	100011131	
1341	10221	100041	1000111	1004441	10034001	100022021	

(9)	10000000221	(11)
1000120011	10000100301	100001201111
1000340311	10000200131	100003400231
(10)	10000300121	
	10000400121	

$q = 7\ (n)$

(3)	(4)	11331	(5)	(6)	1003341	(7)	(8)	100030041
1151	10011	13441	100031	1000021	1004461	10012011	100000021	100040151
1261	10111	11551	101231	1001111	1005531	10034011	100010061	100050011
1341	13221	14661	103431	1002221	1006611	10056001	100020041	100060011
			105601					

(9)
1000120151
1000340251
1000560021

$q = 11\ (n)$

(3)	1392	(4)	10331	13771	(5)	105621	(6)	1003041	1007011
1171	1463	10041	10441	13881	101211	107861	1000111	1004111	1008051
12A3	1581	15111	13551	10991	103461	109A71	1001041	1005001	1009081
		11221	11661	11AA1			1002011	1006011	100A031

(7)	10056001
10012051	10078061
10034041	1009A021

$q = 13\ (n)$

(3)	1761	(4)	14441	11991	(5)	107831	(6)	1004051	1009061
1181	19C1	160A1	14551	10A21	101201	109A01	1000021	1005031	100A061
1321	1BA1	11111	15661	18BB1	103451	10BC51	1001041	1006081	100B031
1541		10221	10771	15CC1	105641		1002011	1007011	100C011
		10331	13881				1003231	1008041	

(7)	10078001
10012021	1009A041
10034001	100BC051
10056121	

$q = 17\ (n)$

(3)	14A1	18B1	(4)	10221	10521	10861	10B11	10E51	(5)	105601
1131	1591	13G1	10031	10331	10621	10921	10C11	10F21	101251	107851
1261	17C1	1EF1	10131	10431	10721	10A11	10D41	10G31	103411	109A21

10BC31
10DE61
10FG01

$q = 19\ (n)$

(3)	14C1	18G1	(4)	10311	10721	10B21	10F81	(5)	107841	10FG11
11H1	15I1	19E1	10091	10411	10861	10C21	10G21	101291	109A11	10HI01
12D1	16A1		10141	10551	10931	10D71	10H11	103411	10BC01	
13B1	17F1		10211	10611	10A11	12E01	10I61	105601	11DE21	

$q = 4\ (n) \quad x^2 + x + 1$

(3)	(4)	(5)	0 * 00021	0 * 112210	0 * * * 22 * 00	(10)
0 * 00	00 * 10	0 * *0 * 0	0 * 011 * 1	(8)	(9)	0 * * * * * 2 * *10
0 * 10	0 * 010	0 * 1220	0 * 12211	0 * * * *2 * 10	0 * * * *0 * * * 0	0 * * * *00 * 100
0 * 20	00100	(6)	(7)	0 * * * 00010	0 * * * 12 * *20	0 * * * *11 * 010
	01220	0 * 0 * *01	0 * * * 0000	0 * * * 11 * 00		0 * * * *22 * 210

	(12)	
(11)	0 * * * * * *2 * *0 * 0	(13)
0 * * * * * 0 * *110	0 * * * * * 00 * * * 10	0 * * * * * *0 * * * 100
0 * * * *12 * 1 * 10	0 * * * * * 11 * * * 20	0 * * * * * 12 * * * *20
	0 * * * * * 22 * * * 10	

$$q = 8\ (n) \quad x^3 + x + 1$$

(3)	(4)		(5)	(6)		(7)	(8)
0010	0 * *00	04330	0 * *0 * 0	0 * * * *30	0 * *3350	0 * *01 * 00	0 * * * *0030
0230	00000	01440	0 * 12 * 0	0 * 30020	0 * *4410	0 * *23020	0 * * * 00 * 00
0450	01110	02550	0 * 3440	0 * *1120	0 * *5560	0 * *45 * 10	0 * * * 100 * 0
0260	02220	01660	0 * 5640	0 * *2240	0 * *6630	0 * * * 6 * *0	0 * * * 200 * 0

	(9)
0 * * * 30 * 40	0 * * * 01 * *40
0 * * * 400 * 0	0 * * * 23 * * * 0
0 * * * 50 * 20	0 * * * 45 * *20
0 * * * 60 * 10	0 * * * *6 * * * 0

$$q = 9\ (n) \quad x^2 + 2x + 2$$

(3)	0270	(4)	0 * 110	02440	00770	0 * 23 * 0	(6)	0 * *1 * 50	0 * *4210
0030	0460	00 * 00	0 * 220	00550	(5)	0 * 4500	0 * * * 230	0 * *2200	0 * *5 * 10
0150		01000	0 * 330	0 * 660	0 * 0120	0 * 6720	0 * *0230	0 * *3 * 70	0 * *6220

0 * *7 * 30	0 * *23 * *0
(7)	0 * *45050
0 * *01130	0 * *67120

$$q = 16\ (n) \quad x^4 + x + 1$$

(3)	0260	09A0	(4)	0 * 100	0 * 400	0 * 750	0 * A10	0 * D50	0 * 0100
0080	0350	0BC0	00 * 30	0 * 200	0 * 510	0 * 800	0 * B30	0 * E30	0 * 2300
0170	0040	0DE0	0 * 030	0 * 300	0 * 600	0 * 900	0 * C00	(5)	0 * 45 * 0

0 * 67 * 0	0 * CD00	0 * *C * 0
0 * 8960	0 * *E30	0 * *D04
0 * AB * 0	0 * *B07	0 * *E02

Theorem 3. *Conjecture B is true.*

It seems quite natural to ask to what extent one can more generally specify several coefficients in advance; perhaps some function of n say like $\log n$?

Since every primitive polynomial over F_q is irreducible over F_q, we also briefly discuss the following conjecture concerning the distribution of primitive polynomials. Along with use of tables of irreducibles such as Table C of Lidl and Niederreiter [5], the motivation for Conjecture B initially arose from the main result of Cohen [1]. Cohen proved in [1] that if $n \geq 2$ and $a \in F_q$ 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. As a generalization of Cohen's result, we also state the following conjecture from [4] concerning the distribution of primitive polynomials:

Conjecture A. *Let a, n, j be as in Conjecture B. 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 $a = 1$.*

Conjecture A states that with five exceptions, there exists a primitive polynomial of degree n over F_q with the coefficient of any fixed power of x prescribed in advance. The five exceptions are indeed necessary because in those cases, there are no polynomials with the desired property. Once again one can ask to what extent one can specify more than one coefficient in advance. For example Cohen asks in [2] whether there is some function $c(n)$ (such as $\log n$, $\sqrt{n}$, or $n/4$) so that there is a primitive with $\lfloor c(n) \rfloor$ coefficients specified in advance, where $\lfloor\rfloor$ denotes the greatest integer function. For a recent partial result in this direction, we refer to Han [3] who shows that for $n \geq 7$, there is a primitive polynomial of degree n over F_q with the coefficents of both x^{n-1} and x^{n-2} specified in advance.

Acknowledgment

We would like to thank Daqing Wan for providing us with a number of very helpful ideas.

References

1. S. D. Cohen, *Primitive elements and polynomials with arbitrary trace*, Discrete Math. **83** (1990), 1-7. MR **91h:**11143
2. S. D. Cohen, Primitive elements and polynomials: existence results, In: Finite Fields, Coding Theory, and Advances in Communications and Computing, (G. L. Mullen and P. J.-S. Shiue, Eds.), Lect. Notes in Pure & Appl. Math., Vol. 141(1993), Marcel Dekker, New York, pp. 43-55. MR **93k:**11113
3. W. B. Han, *The coefficients of primitive polynomials over finite fields*, Math. Comp. **65** (1996), 331-340. MR **96d:**11128
4. T. Hansen and G. L. Mullen, *Primitive polynomials over finite fields*, Math. Comp. **59** (1992), 639-643; Supplement S47-S50. MR **93a:**11101
5. R. Lidl and H. Niederreiter, Finite Fields, Encyclo. Math. Appl., Vol. 20, Addison-Wesley, Reading, MA, 1983 (Now distributed by Camb. Univ. Press). MR **86c:**11106
6. D. Wan, *Generators and irreducible polynomials over finite fields*, Math. Comp. **66** (1997), 1195–1212. CMP 96:16

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

E-mail address: `csh102@psu.edu`

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

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