MATHEMATICS OF COMPUTATION
VOLUME 56, NUMBER 194
APRIL 1991, PAGES 817–821

PRIMITIVE t-NOMIALS $(t = 3, 5)$ OVER $GF(2)$ WHOSE DEGREE IS A MERSENNE EXPONENT ≤ 44497

YOSHIHARU KURITA AND MAKOTO MATSUMOTO

ABSTRACT. All of the primitive trinomials over $GF(2)$ with degree p given by one of the Mersenne exponents 19937, 21701, 23209, and 44497 are presented. Also, one example of a primitive pentanomial over $GF(2)$ is presented for each degree up to 44497 that is a Mersenne exponent. The sieve used is briefly described. A problem is posed which conjectures the number of primitive pentanomials of degree p.

1. INTRODUCTION

A number of authors [3–7] have determined primitive t-nomials (t-term polynomials) over $GF(2)$. Zierler and Brillhart [6] have calculated all irreducible trinomials $(t = 3)$ of degree n, $n \leq 1000$, with the period for some for which the factorization of $2^n - 1$ is known; Stahnke [4] has listed one example of a trinomial or pentanomial $(t = 5)$ for each degree n, $n \leq 168$; Zierler [7] has listed all primitive trinomials for each degree of Mersenne exponent up to 11213.

This note is an extension of these works: let M_n denote the nth Mersenne exponent (for example, $M_{27} = 44497$ and $2^{M_{27}} - 1$ is known to be prime), and let q, q_k $(k = 1, 2, 3)$ be positive integers. Table A lists all primitive trinomials $X^p + X^q + 1$ over $GF(2)$ for which $p = M_n$, $24 \leq n \leq 28$, and $q \leq \lfloor p/2 \rfloor$. Table B lists one example of primitive pentanomials $X^p + X^{q_3} + X^{q_2} + X^{q_1} + 1$ over $GF(2)$ for which $p = M_n$, $8 \leq n \leq 27$, and $p > q_3 > q_2 > q_1$, where q_k is randomly chosen from the interval $[\lfloor p(2k-1)/8 \rfloor : \lfloor p(2k+1)/8 \rfloor]$ to provide some distance between p, q_3, q_2, q_1, and 0.

2. TEST FOR PRIMITIVITY

If $2^p - 1$ is prime, then the primitivity is equivalent to the irreducibility. The test for the primitivity comprises the following three sieves. The first two of these are only necessary condition tests, but they are useful for a prescreening with relatively high speed. The third sieve is a necessary and sufficient test. Let $f(X)$ be a trial t-nomial of degree p, where $t = 3, 5$.

Received January 17, 1990; revised May 1, 1990.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11–04, 11T06, 12–04, 12E05.

0025-5718/91 $1.00 + $.25 per page

Sieve I: mod k *test* ($k = 3, 5, 9$). As stated below in (a)–(c), for some $k > 0$, one can determine very rapidly whether $\gcd(f(X), X^k - 1)$ equals 1 or not. If it equals 1, then $f(X)$ goes forward to the next sieve. About 30% of trials are rejected by this sieve.

(a) For some $k > 0$, there is an irreducible polynomial $h(X)$ with the following two properties: (i) $h(X) \mid X^k - 1$, (ii) every multiple of $h(X)$ with degree $\leq k - 1$ and with the number of terms $\leq t$ is limited to the form $X^l h(X)$, where $0 \leq l \leq k - \deg(h(X)) - 1$. For $t = 3$, and for $k \leq 26$, there are two such $h(X)$: $X^2 + X + 1$ $(k = 3)$, $X^6 + X^3 + 1$ $(k = 9)$. For $t = 5$, and for $k \leq 24$, in addition to the above two, there is: $X^4 + X^3 + X^2 + X + 1$ $(k = 5)$.

(b) Let $r_k(X)$ be the remainder polynomial of the division $f(X)/(X^k - 1)$. This $r_k(X)$ is obtained easily by reducing modulo k the exponent of every term of $f(X)$. It is clear that $\deg(r_k(X)) \leq k - 1$ and the number of terms of $r_k(X)$ is not greater than that of $f(X)$.

(c) From (a) and (b), we get $h(X) \mid f(X)$ if and only if $r_k(X) = X^l h(X)$ for some $l \geq 0$. It is easy to determine whether this last equality holds, and if it holds, then $f(X)$ is rejected.

Sieve II: gcd *test.* This sieve is based on the well-known powerful theorem [2, p. 48]: let $\phi(X)$ be an irreducible polynomial over $GF(2)$ of degree m. Then $\phi(X) \mid X^{2^k} - X$ if and only if $m \mid k$. Thus, by computing $\gcd(f(X), X^{2^k - 1} - 1)$ for $k = 3, 4, \ldots, k_{\max}$ successively, we can see whether $f(X)$ has factors of degree $\leq k$. When $k_{\max} = 12$, approximately 85% of trial polynomials are eliminated by these two sieves.

Sieve III: *necessary and sufficient irreducibility test.* If $f(X)$ survives Sieve II, then we compute $X^N \bmod f(X)$, where $N = 2^p - 1$. The trial t-nomial $f(X)$ is irreducible if and only if the result equals 1. In the actual procedure, we compute successively the sequence X_i from X_0 to X_p, where $X_i = X_{i-1}^2 \bmod f(X)$ over $GF(2)$ and $X_0 = X$.

3. Results

The search for primitive polynomials was done on the SUN-3, -4 for $p \leq 9941$, on the Cray X-MP for $p \geq 11213$ at the AIST computer center (RIPS), Tsukuba. All results and their reciprocals have been verified on all these machines by another independently programmed version of Sieve III. In Tables A and B, only the exponents of the terms are listed. For example, the first line of Table A means that three trinomials exist for $p = 19937$, $q \leq \lfloor p/2 \rfloor$, with $q = 881$, 7083, and 9842. In the first line of Table B, 31, 23, 11, 9 stands for $X^{31} + X^{23} + X^{11} + X^9 + 1$.

Of the entries of Table A, for $p = M_{25} = 21701 = -3 \bmod 8$ and $p = M_{28} = 86243 = 3 \bmod 8$, it is easily found that no primitive trinomial exists as follows: Swan's Corollary [1, p. 170] guarantees that the trinomial $X^p + X^q + 1$ is reducible over $GF(2)$ if $p = \pm 3 \bmod 8$ and if $q \neq 2$. Next we find that by Sieve

III, $X^p + X^2 + 1$ is reducible, where $p = M_{25}$ and M_{28}. Furthermore, in the same way, it is found that there is no primitive trinomial for $p = M_{30} = 216091$ (or more directly, $M_{30} = 3 \bmod 8 = 1 \bmod 3$, hence $X^2+X^1+1 \mid X^{M_{30}}+X^2+1$).

TABLE A
Primitive trinomial

p	q		
19937	881,	7083,	9842
21701	none		
23209	1530,	6619,	9739
44497	8575,	21034	
86243	none		

TABLE B
Primitive pentanomial

p	q_3	q_2	q_1
31	23	11	9
61	43	26	14
89	69	40	20
107	82	57	31
127	83	63	22
521	447	197	86
607	461	307	167
1279	988	630	339
2203	1656	1197	585
2281	1709	1109	577
3217	2381	1621	809
4253	3297	2254	1093
4423	3299	2273	1171
9689	7712	5463	2799
9941	2475	4964	7449
11213	8218	6181	2304
19937	14554	8423	3820
21701	15986	11393	5073
23209	17777	11796	5005
44497	35504	18756	10561

4. PROBABILITY AND PROBLEM

Let p be a prime number. We can obtain the "probability" that a pentanomial of degree p is irreducible as follows. A pentanomial can neither be divided by X nor by $X + 1$. The number of polynomials of degree p which

TABLE C
Observed hit ratio of primitive pentanomial

p	(a) number of trials	(b) number of primitive pentanomials	$p \times$ hit ratio $= p \times$ (b)/(a)	$p \bmod 8$
5	4*	0	0.00	−3
7	20*	0	0.00	−1
13	220*	66	3.90	−3
17	560*	152	4.61	1
19	816*	158	3.68	3
31	4060*	584	4.46	−1
61	34220*	1708	3.04	−3
89	109736*	5902	4.79	1
107	192920*	4984	2.76	3
127	325500*	12656	4.94	−1
521	500000	5233	5.45	1
607	500000	4374	5.31	−1
1279	468200	1948	5.32	−1
2203	350300	393	2.47	3
2281	350000	829	5.40	1
3217	280000	492	5.65	1
4253	269400	160	2.53	−3
4423	289000	347	5.31	−1

Note: * means exhaust trials, others are by random sampling.

can be divided neither by X nor by $X+1$ is easily proved to be 2^{p-2}. On the other hand, if p is prime, the number of irreducible polynomials of degree p is known to be $(2^p-2)/p$ [2, p. 84]. Thus, a pentanomial of degree p is irreducible with probability $4(1-2^{1-p})/p \approx 4/p$.

Table C indicates the observed hit ratio for $5 \le p \le 4423$. The above argument implies that the average of the values $p \times$ (hit ratio) should be 4; the observed simple average is 4.35 for $13 \le p \le 4423$. This table suggests that for $p \ge 13$, one has $p \times$ (hit ratio) < 4 if and only if $p = \pm 3 \bmod 8$. It seems that this phenomenon is strongly related to Swan's Corollary referred to above, which clarifies the relation between the discriminant and the parity of the number of irreducible factors. The authors, however, could not generalize the trinomial version of this corollary to a pentanomial one, and pose it as a problem:

Problem. Explain why $p = \pm 3 \bmod 8$ implies a low hit ratio.

ACKNOWLEDGMENT

The authors would like to thank Toshihiro Kinoshita, Cray Research Japan, for his help in program code optimization on the Cray X-MP.

BIBLIOGRAPHY

1. E. R. Berlekamp, *Algebraic coding theory*, McGraw-Hill, New York, 1968.
2. R. Lidl and H. Niederreiter, *Introduction to finite fields and their applications*, Cambridge Univ. Press, Cambridge, 1986.

3. E. R. Rodemich and H. Rumsey, Jr., *Primitive trinomials of high degree*, Math. Comp. **22** (1968), 863–865.
4. W. Stahnke, *Primitive binary polynomials*, Math. Comp. **27** (1973), 977–980.
5. E. J. Watson, *Primitive polynomials* (mod 2), Math. Comp. **16** (1962), 368–369.
6. N. Zierler and J. Brillhart, *On primitive trinomials* (mod 2), Inform. and Control **13** (1968), 541–554; II, **14** (1969), 566–569.
7. N. Zierler, *Primitive trinomials whose degree is a Mersenne exponent*, Inform. and Control **15** (1969), 67–69.

NATIONAL RESEARCH LABORATORY OF METROLOGY, UMEZONO, 1–1–4, TSUKUBA, IBARAKI, 305 JAPAN

RESEARCH INSTITUTE FOR MATHEMATICAL SCIENCES, KYOTO UNIVERSITY, KITASHIRAKAWA OIWAKE-CHO, SAKYO-KU, KYOTO, 606 JAPAN