Research Report

KSTS/RR-98/009
August 18, 1998

# New Primitive $t$-nomials ($t = 3, 5$) over $GF(2)$ Whose Degree Is a Mersenne Exponent

by

T. Kumada, L. Hannes, Y. Kurita and M. Matsumoto

Toshihiro Kumada and Makoto Matsumoto
Department of Mathematics
Keio University

Leeb Hannes
Department of Mathematics
University of Salzburg

Yoshiharu Kurita
Hungarian Productivity Center

Department of Mathematics
Faculty of Science and Technology
Keio University


3-14-1 Hiyoshi, Kohoku-ku, Yokohama, 223-8522 Japan

KSTS/RR-98/009
August 18, 1998

# New primitive $t$-nomials $(t = 3, 5)$ over $GF(2)$ whose degree is a Mersenne exponent

Toshihiro Kumada
Keio University, Department of Mathematics
Yokohama, Kanagawa, Japan
kumada@math.keio.ac.jp

Leeb Hannes*
University of Salzburg, Department of Mathematics
Salzburg, Austria
leeb@random.mat.sbg.ac.at

Yoshiharu Kurita
Hungarian Productivity Center
Budapest, Hungary
ykurit@ibm.net

Makoto Matsumoto
Keio University, Department of Mathematics
Yokohama, Kanagawa, Japan
matumoto@math.keio.ac.jp

*Research supported by the Austrian Science Foundation (FWF), project no. P11143-MAT

KSTS/RR-98/009
August 18, 1998

**Abstract**

All of the primitive trinomials over $GF(2)$ with degree 859433 which is 33th Mersenne exponent are presented. Also examples of primitive pentanomials over $GF(2)$ with degree 86243 which is 28th Mersenne exponent are presented. The sieve used is briefly described.

# 1 Introduction

Primitive $t$-nomials ($t$-term polynomials) over $GF(2)$ are useful in the applications like random number generation, coding theory, and cryptography. Heringa et. al.[2] exhaustly listed all primitive trinomials of Mersenne exponent degree up to the 31th Mersenne exponent 216091. This note is an extension of these works.

Let $M_n$ denote the $n$th Mersenne exponent (for example, $M_{28} = 86243$ and $2^{M_{28}} - 1$ is known to be a prime). As of April 20, 1998, 37 Mersenne exponents are found. 3021377 is the greatest in them. The primality test of all exponents less than 2000000 is done at least once (it proves that $M_{35} = 1398269$). The known Mersenne exponents greater than 2000000 are 2976221 and 3021377. In this paper, we define $M_{36\#} = 2976221$ and $M_{37\#} = 3021377$. The sharp mark behind 36 and 37 show that the search for Mersenne exponent $p$ in the interval $2000000 < p < 3021376$ has not been exhaustive. See [3, 4] for the information about the current search status of Mersenne exponents.

Table 1 lists all primitive trinomials $X^p + X^q + 1$ over $GF(2)$ with degree $p = M_n (33 \leq n \leq 36\#)$, $q \leq \lfloor p/2 \rfloor$. Table 2 lists examples of primitive pentanomials $X^p + X^{q_1} + X^{q_2} + X^{q_3} + 1$ over $GF(2)$ with degree $p = M_{28}$. In Tables 1 and 2, only the exponents of the terms are listed.

# 2 Test for Primitivity

## 2.1 Primitivity of trinomials

Let $f(X) = X^p + X^q + 1$ be a trinomial of degree $p = M_n$. Our aim is to find such $q$ that $X^p + X^q + 1$ is primitive. By considering the reciprocal polynomial, we may assume that $1 \leq q \leq \lfloor p/2 \rfloor$ holds. 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 test, but they reject about 90% of the candidates. The third sieve is a necessary and sufficient test. The third sieve can determine whether $f(X)$ is irreducible or not with $O(p^2)$ computation.

Let $k_n$ denote $2^n - 1$. Sieves I and II are based on the well-known theorem[6, p.48]: let $\phi(X)$ be an irreducible polynomial over $GF(2)$ of degree $m$. Then $\phi(X)|(X^{1+k_n} - X)$ if and only if $m|n$. Thus by computing $\gcd(f(X), X^{k_n} - 1)$ we know whether $f(X)$ has a factor of degree $m|n$.

Sieve I: mod $k$ test. One can determine easily whether $\gcd(f(X), X^k - 1)$ equals 1 or not for small $k$ as follows. If it equals 1, then $f(X)$ goes forward to the next sieve.

Let $K$ be a finite set of positive odd numbers. Let $k$ be an element of $K$. Then $\gcd(f(X), X^k - 1) = \gcd(X^p + X^q + 1, X^k - 1) = \gcd(X^{(p \pmod k)} + X^{(q \pmod k)} + 1, X^k - 1)$ holds. Thus we can obtain the set

$$R = \{(k, q) \mid k \in K,\ q \in \mathbf{Z}/k\mathbf{Z}\ \ s.t.\ \ X^p + X^q + 1\ is\ reducible\}.$$

Hence for $1 \leq q \leq \lfloor p/2 \rfloor$, if there exists $k \in K$ such that $(k, q \pmod k) \in R$, the number should be rejected. We put $K = \{k \mid k\ is\ odd,\ 3 \leq k \leq k_{12} + 2\} \cup \{k_{13}, k_{14}, k_{15}\}$ This test rejects about 89% of the candidates.

Sieve II: direct gcd test. Let $f(X)$ be a trinomial which passed Sieve I. By computing $\gcd(f(X), X^{k_n} - 1)$ $(n = 16, 17, 18)$ we can eliminate some candidates. Sieves I and II reject about 91% of the candidates.

Sieve III is a necessary and sufficient irreducibility test based on the Theorem 1(see below). The following description is quoted from [7].

Let $\mathcal{S}^\infty$ denote the $GF(2)$ -vector space of all infinite sequences of 0,1. That is,

$$\mathcal{S}^\infty := \{\chi = (\cdots, x_5, x_4, x_3, x_2, x_1, x_0) \mid x_i \in GF(2)\}.$$

Let $D$ (*delay* operator) and $H$ (*decimation* operator) be linear operators from $\mathcal{S}^\infty$ to $\mathcal{S}^\infty$ defined by

$$D(\cdots, x_4, x_3, x_2, x_1, x_0) = (\cdots, x_5, x_4, x_3, x_2, x_1),$$
$$H(\cdots, x_4, x_3, x_2, x_1, x_0) = (\cdots, x_{10}, x_8, x_6, x_4, x_2, x_0).$$

Let $\varphi(X)$ be the characteristic polynomial of a linear recurrence, and $\chi$ be an element of $\mathcal{S}^\infty$. Then, $\chi$ satisfies the recurrence if and only if $\varphi(D)\chi = 0$. Note that $\varphi(D)$ is a linear operator and 0 denotes the zero sequence.

It is easy to check that

$$DH = HD^2.$$

Since the coefficients are in $GF(2)$, we have $\varphi(X^2) = \varphi(X)^2$, and thus if $\varphi(D)\chi = 0$ then

$$\varphi(D)H\chi = H\varphi(D^2)\chi = H\varphi(D)^2\chi = 0,$$

i.e., $H\chi$ also satisfies the same recurrence. The following theorem holds[7].

**Theorem 1** *Let $\varphi(X)$ be a polynomial over $GF(2)$ whose degree $p$ is a Mersenne exponent. Take $\chi \in \mathcal{S}^\infty$ such that $\varphi(D)\chi = 0$ and $H\chi \neq \chi$. Then $\varphi(t)$ is primitive if and only if $H^p\chi = \chi$.*

In the above theorem, put $\varphi(X) := X^p + X^q + 1$. Let $T = (\cdots, t_4, t_3, t_2, t_1, t_0)$ be an element of $\mathcal{S}^\infty$ such that $\varphi(D)T = 0$, i.e.,

$$t_{p+i} = t_{q+i} + t_i,$$

holds for all non-negative integer $i$.
Sieve III: final test.
(1) Determine an initial vector $T_0 = (t_{p-1}, \ldots, t_i, \ldots, t_0)$ such that $H(T_0)$ dose not equal $T_0$. It is easy to satisfy this assumption. For example $t_{2i} = 1$ for a certain $i(2i \leq p-1)$, and $t_j = 0$(for all $j \neq 2i$, $0 \leq j \leq p-1$) is sufficient.
(2) Compute successively the sequences $S_i, T_i$ as follows. $S_i := Extend(T_i)$, $T_{i+1} := H(S_i)$. $Extend(T_i)$ means to compute the sequence based on the recurrence formula. Remark that the first $2p-1$ values of $S_i$ are sufficient to know the first $p$ values of $H(S_i)$.
(3) If $T_p$ equals $T_0$. $f(x)$ is primitive, and otherwise not primitive.

## 2.2 Primitivity of pentanomials

Basically, the necessary test for primitivity of pentanomials is similar to that of trinomials.

The necessary and sufficient irreducibility test is different from that of trinomials. Let $f(X) = X^p + X^{q_1} + X^{q_2} + X^{q_3} + 1$ be a pentanomial of degree $p$. We compute $X^N$ mod $f(X)$, where $N = 2^p - 1$. The pentanomial 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 $X_i = X_{i-1}^2$ mod $f(X)$ over $GF(2)$ and $X_0 = X$. See [5] for more information.

# 3 Results

Concerning the trinomials, we tried searching primitive trinomials whose degree is $M_{33}, M_{34}, M_{35}$ and $M_{36\#}$. We did not search primitive trinomials of degree $M_{32}$ and $M_{37\#}$.

For $p = M_{34}, M_{35}$ and $M_{36\#}$, nonexistence of primitive trinomials is proved as follows: Swans's Corollary[1, p.170] guarantees that the $X^p+X^q+1$ is reducible over $GF(2)$ if $p = \pm 3 \bmod 8$ and if $q \neq 2$. Next by Sieve III, we show that $X^p + X^2 + 1$ is reducible, where $p = M_{34}, M_{35}$ and $M_{36\#}$.

In case of $p = M_{33}$, 40656 candidates passed Sieves I and II. For the computer search, we used an SGI POWER Challenge 10000 GR parallel computer with 20 processors and 2.5 GB RAM. After minor architecture-specific optimizations, we were able to test approximately one candidate parameter per an hour. Hence, checking all 40656 candidates consumed a total accumulated time of 4.6 years; using 19 of the available processors, the search was completed in about 3 months.

**Table 1**
*primitive trinomials*

| $n$ | $M_n \bmod 8$ | $p = M_n$ | $q$ |
|---|---|---|---|
| 32 | -1 | 756839 | the search is not done |
| 33 | 1 | 859433 | 288477 |
| 34 | 3 | 1257787 | none |
| 35 | -3 | 1398269 | none |
| 36# | -3 | 2976221 | none |
| 37# | 1 | 3021377 | the search is not done |

The non-exhaustive search for primitive pentanomials was done in the AIST computer center (RIPS), Tsukuba. We succeeded in finding two primitive pentanomials whose degree is $M_{28}$.

**Table 2**
*primitive pentanomials*

| $n$ | $p = M_n$ | $q_1$ | $q_2$ | $q_3$ |
|---|---|---|---|---|
| 28 | 86243 | 62833 | 50942 | 11754 |
| | | 64043 | 41667 | 19434 |

*Acknowledgments*

We would like to thank Prof. Zinterhof for putting the computing facilities of the University of Salzburg's RIST++ institute at our disposal.

# References

[1] E. R. Berlekampe, *Algebraic coding theory*, McGraw-Hill, New York, 1968.

[2] J. R. Heringa, H. W. J. Blöte and A. Compagner, *New primitive trinomials of Mersenne-exponent degrees for random-number generation*, Int. J. Mod. Phys. C Vol. 3, No. 3, (1992), 561-564.

[3] http://www.mersenne.org/status.htm

[4] http://www.utm.edu:80/research/primes/mresenne.shtml

[5] Y. Kurita and M. Matsumoto, *Primitive t-nomials* $(t = 3, 5)$ *over GF(2) whose degree is a Mersenne exponent* $\leq 44497$, Math. Comp. Vol. 56, No. 194, April (1991), 817-821

[6] R. Lidl and H. Niederreiter, *Introduction on finite fields and their applications*, Cambridge Univ. Press, Cambridge, 1986.

[7] M. Matsumoto and T. Nishimura, *Mersenne Twister: A 623-dimensionally equidistributed uniform pseudorandom number generator*, ACM Trans. on Modeling and Computer Simulation Vol. 8, No. 1, January (1998), to appear.