A PRIMITIVE TRINOMIAL OF DEGREE 6972593

RICHARD P. BRENT, SAMULI LARVALA, AND PAUL ZIMMERMANN

Abstract. We describe a search for primitive trinomials of degree 6972593 over GF(2). The only primitive trinomials found were $x^{6972593} + x^{3037958} + 1$ and its reciprocal. This completes the search for primitive trinomials whose degree is a Mersenne exponent less than ten million.

1. Introduction

In this note we describe an extension of the computation [3], to which we refer for motivations, definitions, historical comments and additional references. Throughout, all polynomials are assumed to be in $Z_2[x]$. When considering trinomials $T(x) = x^r + x^s + 1$, we assume that $1 \le s \le \lfloor r/2 \rfloor$, so we disregard the reciprocal trinomial $x^r T(1/x) = x^r + x^{r-s} + 1$.

Using standard algorithms, it is possible to find irreducible polynomials of high degree r, but it appears to be impossible to test if these polynomials are primitive unless the complete factorization of $2^r - 1$ is known. For this reason we restrict our attention to Mersenne exponents r, for which $2^r - 1$ is prime.

Primitive trinomials $x^r + x^s + 1$ whose degree is a Mersenne exponent $r \le 3021377$ were considered in [3, 7, 8, 9, 15]. Here we consider the next Mersenne exponent $r = 6972593$. According to the GIMPS project [14], 6972593 is the only Mersenne exponent in the interval $(3021377, 10^7)$.

We remark that, at the time of writing (August 2003), one larger Mersenne exponent is known. This exponent, $r = 13466917$, is not the degree of a primitive trinomial. Because $r = 5 \bmod 8$, Swan's theorem [13] implies that we only need to consider $s = 2$. However, $x^r + x^2 + 1$ is divisible by $x^2 + x + 1$, since $r = 1 \bmod 3$.

For Mersenne exponents $r = \pm 3 \bmod 8$, $5 < r < 10^7$, no primitive trinomial of degree r exists. However, in each case we can find a primitive polynomial of degree r dividing a trinomial $x^{r+\delta} + x^s + 1$, for some $\delta \le 12$. Such trinomials are called *almost primitive* and are discussed in [4, 5].

2. Computational results

Using the algorithm of [3, §4], a search for irreducible trinomials of degree $r = 6972593$ was started in February 2001 and completed in July 2003. Sieving eliminated all but 236244 (6.78%) of the $\lfloor r/2 \rfloor = 3486296$ candidate trinomials and took about 5% of the total time. (For the case $r = 3021377$ considered in [3], the corresponding figures are 109245 (7.23%) of 1510688.) In most cases we sieved

1991 *Mathematics Subject Classification.* Primary 11B83, 11Y16; Secondary 11-04, 11N35, 11R09, 11T06, 11Y55, 12-04.

Key words and phrases. Irreducible polynomials, irreducible trinomials, primitive polynomials, primitive trinomials, Mersenne exponents, Mersenne numbers.

Version of 26 August 2003. Submitted to *Mathematics of Computation.*

 rpb214 typeset using $\mathcal{AMS}$-LaTeX.

up to degree 26 (versus 24 for $r = 3021377$). We found that sieving for factors of degree k removed about 1 in k of the remaining trinomials, e.g. sieving for factors of degree 25 removed 9593 of the 253723 candidates remaining after we had already sieved for factors of degree $2, 3, \ldots, 24$.

For the 236244 candidate trinomials $T(x)$ not eliminated by sieving, we performed a "full irreducibility test": $T(x)$ is irreducible iff $x^{2^r} = x \bmod T(x)$. In some cases we tested the reciprocal of $T(x)$ instead of $T(x)$, see [3, Thm. 2 & §4].

One primitive trinomial,

$$T(x) = x^{6972593} + x^{3037958} + 1,$$

was found on August 31, 2002. Our computations show that this is the only primitive trinomial of degree 6972593, apart from its reciprocal.

If we consider irreducible trinomials of degree r, it is plausible that Mersenne exponents $r = \pm 1 \bmod 8$ behave like other primes $r = \pm 1 \bmod 8$. There are 1613 such primes $r < 30000$, giving a total of 5276 irreducible trinomials. Of these 1613 primes, 189 (11.7%) are associated with exactly one irreducible trinomial. For 63 (3.9%) of the primes r, there is no irreducible trinomial of degree r. The distribution of the number of irreducible trinomials for given prime degree $r = \pm 1 \bmod 8$, $r < 30000$, appears to be approximately Poisson with mean 3.271 ± 0.045.

The existing data for Mersenne exponents $r = \pm 1 \bmod 8$ is consistent with such a Poisson distribution: for the 21 Mersenne exponents $r = \pm 1 \bmod 8$ in $[7, 10^7]$, there are 64 irreducible trinomials (mean 3.05 ± 0.38 per exponent) and two exponents (89 and 6972593) are associated with exactly one irreducible trinomial.

The computation for $r = 6972593$ was performed on an average of about 300 processors and took approximately 230000 Mips-years (17.8 times as long as for $r = 3021377$). The bit-complexity[1] of the computation is $O(r^3)$. In practice the time increases faster than r^3 because of cache effects: $(6972593/3021377)^3 \approx 12.3 < 17.8$. For processors whose speed is limited by memory bandwidth, it is relevant to note that approximately $236244 \times 3.5 \times r^2/64 \approx 6.28 \times 10^{17}$ 64-bit memory references were required for the full irreducibility tests (see [3, §4]).

3. Checking the results

It is important to check the results of such a long computation to detect human, software and/or hardware errors [8, 10, 14]. Ideally, we should repeat the entire computation with an independently-written program, but this is not feasible with our current computing resources. Most software that can be used to compute irreducible/primitive trinomials is impractical for degrees as large as 6972593 because of inefficient use of memory or non-optimized algorithms. NTL [12] is the only general-purpose package that we have found capable of checking the irreducibility of a trinomial of degree 6972593 over Z_2, and NTL takes three times longer than our program `irred` (13 hours versus 4.33 hours on an 833 Mhz Alpha EV68 to verify our primitive trinomial).

Our program `irred`, which is available as open-source software [2], produces a log file where each line is a triple (r, s, k). Such a line indicates that the trinomial $T(x) = x^r + x^s + 1$ has been tested. If k is an integer, then $T(x)$ has an irreducible factor of degree k and no factor of smaller degree. For example, the line

[1] This assumes that a classical GCD is used for sieving – the bit-complexity could be reduced if we used an asymptotically faster GCD and sieved further.

```
6972593 5 10
```

indicates that $x^{6972593} + x^5 + 1$ has an irreducible factor of degree 10. By reducing the exponents mod 1023 (to reduce memory requirements), and then taking a GCD with $x^{1023} - 1$, we can easily verify with NTL or Magma [6] that the irreducible factor is $x^{10} + x^7 + x^6 + x^5 + x^3 + x^2 + 1$.

If k has the form $\mathtt{x}d_7 \cdots d_0$ then the low 32 coefficients of $x^{2^r} \bmod T(x)$ are encoded in the hexadecimal number $d_7 \cdots d_0$. For example, the line

```
6972593 27 x08053348
```

indicates that the trinomial $T(x) = x^{6972593} + x^{27} + 1$ passed the sieving phase, but failed a full irreducibility test, and

$$\left(x^{2^{6972593}} \bmod T(x)\right) \bmod x^{32} = x^{27} + x^{18} + x^{16} + x^{13} + x^{12} + x^9 + x^8 + x^6 + x^3.$$

If k has the form $\mathtt{y}d_7 \cdots d_0$ then the reciprocal polynomial was tested, and the low 32 coefficients of $x^{2^r} \bmod x^r T(1/x)$ are encoded in $d_7 \cdots d_0$. This usually occurs when s is even, see [3, §4].

Finally, a line such as

```
6972593 3037958 irreducible (may be primitive)
```

means that $x^r + x^s + 1$ is irreducible (and hence primitive if r is a Mersenne exponent, but `irred` does not check this).

Since a bug in our sieving routine might result in a primitive trinomial being discarded erroneously, we have taken care to check the sieving phase of our program with NTL. For degree $r = 3021377$, we have checked the log entries for 1396610 (99.7%) of the 1401443 trinomials discarded by sieving (including degrees up to 23). Thirteen of the log entries for trinomials not discarded by sieving have also been checked with NTL. For $r = 6972593$, we have checked the log entries for 3183710 (98.0%) of the 3250052 trinomials discarded by sieving (including degrees up to 20). No discrepancies have been found.

Agreement with the checks performed by NTL gives confidence in the correctness of the different versions of `irred` (32 and 64-bit, C, Intel MMX, PowerPC). We have also cross-checked by duplicating more than 2% of the results with different versions of `irred`. To guard against the possibility of hardware errors, we are running the complete computation for degree $r = 3021377$ again. The computations for smaller Mersenne exponents $r = \pm 1 \bmod 8$ have been double-checked, as already reported in [3, §6].

The log files for $r = 6972593$ and other Mersenne exponents less than 10^7 are available on our web site [2], and any discrepancies found during testing will be reported there.

Acknowledgements. The following institutions and individuals contributed to the computing task (approximate percentages in parentheses): Centre Informatique National de l'Enseignement Supérieur (CINES) (30%); Oxford Supercomputing Centre (OSC) (26%); Oxford Centre for Computational Finance (OCCF) (19%); Oxford University Computing Laboratory (OUCL) (14%); Australian National University Supercomputer Facility (ANUSF) and Australian Partnership for Advanced Computing (APAC), courtesy of Brendan McKay (9%); Juan Luis Varona (1.3%); Barry Mead (0.4%); Nicolas Daminelli (0.2%); and Nate Begeman (0.1%). Nate also ported our program to the Mac G4, using Motorola's AltiVec ISA extension [1] to the PowerPC processor. We thank Philippe Falandry for assistance in compiling

our program on the IBM SP in 64-bit mode, Julian Seward and Andrew Tridgell for their assistance in running the `valgrind` simulator [11], Victor Shoup for his NTL package [12], and George Woltman and the GIMPS project [14] for providing information on Mersenne exponents. The first author gratefully acknowledges the tolerance of OSC/OUCL support staff and the support of the EPSRC under Grant GR/N35366/01.

References

[1] Apple Corporation, G4 with velocity engine, `http://developer.apple.com/hardware/ve/`.

[2] R. P. Brent, Search for primitive trinomials, `http://www.comlab.ox.ac.uk/oucl/work/richard.brent/trinom.html`.

[3] R. P. Brent, S. Larvala and P. Zimmermann, A fast algorithm for testing reducibility of trinomials mod 2 and some new primitive trinomials of degree 3021377, *Math. Comp.* **72** (2003), 1443–1452.

[4] R. P. Brent and P. Zimmermann, Random number generators with period divisible by a Mersenne prime, in *Computational Science and its Applications – ICCSA 2003*, *Lecture Notes in Computer Science* **2667**, Springer-Verlag, Berlin, 2003, 1–10.

[5] R. P. Brent and P. Zimmermann, Algorithms for finding almost irreducible and almost primitive trinomials, in *Proceedings of a Conference in Number Theory in Honour of Professor Hugh Cowie Williams* (Banff, Canada, May 2003), The Fields Institute, Toronto, to appear. Preprint available from `http://www.comlab.ox.ac.uk/oucl/work/richard.brent/pub/pub212.html`.

[6] J. Cannon *et al.*, The Magma computational algebra system, `http://magma.maths.usyd.edu.au/magma/`.

[7] J. R. Heringa, H. W. J. Blöte and A. Compagner, New primitive trinomials of Mersenne-exponent degrees for random-number generation, *International J. of Modern Physics C* **3** (1992), 561–564.

[8] T. Kumada, H. Leeb, Y. Kurita and M. Matsumoto, New primitive t-nomials ($t = 3, 5$) over GF(2) whose degree is a Mersenne exponent, *Math. Comp.* **69** (2000), 811–814. Corrigenda: *ibid* **71** (2002), 1337–1338. MR **2000i:**11183.

[9] Y. Kurita and M. Matsumoto, Primitive t-nomials ($t = 3, 5$) over GF(2) whose degree is a Mersenne exponent ≤ 44497, *Math. Comp.* **56** (1991), 817–821.

[10] T. J. Nicely, Enumeration to 10^{14} of the twin primes and Brun's constant, *Virginia Journal of Science* **46** (1995), 195–204. MR **97e:**11014.

[11] J. Seward, Valgrind, an open-source memory debugger for x86-GNU/Linux, `http://developer.kde.org/~sewardj/`.

[12] V. Shoup, NTL: A library for doing number theory (version 5.3.1), `http://www.shoup.net/ntl/`.

[13] R. G. Swan, Factorization of polynomials over finite fields, *Pacific J. Math.* **12** (1962), 1099–1106. MR **26**#2432.

[14] G. Woltman *et al.*, GIMPS, The Great Internet Mersenne Prime Search, `http://www.mersenne.org/`.

[15] N. Zierler, Primitive trinomials whose degree is a Mersenne exponent, *Information and Control* **15** (1969), 67–69.

Oxford University Computing Laboratory, Wolfson Building, Parks Road, Oxford, OX1 3QD, England

E-mail address: `trinomials@rpbrent.co.uk`

Helsinki University of Technology, Espoo, Finland

E-mail address: `slarvala@cc.hut.fi`

LORIA/INRIA Lorraine, 615 rue du jardin botanique, BP 101, F-54602 Villers-lès-Nancy, France

E-mail address: `Paul.Zimmermann@loria.fr`