TEN NEW PRIMITIVE BINARY TRINOMIALS

RICHARD P. BRENT AND PAUL ZIMMERMANN

Abstract. We exhibit ten new primitive trinomials over GF(2) of record degrees 24 036 583, 25 964 951, 30 402 457, and 32 582 657. This completes the search for the currently known Mersenne prime exponents.

Primitive trinomials of degree up to 6 972 593 were previously known [4]. We have completed a search for all known Mersenne prime exponents [7]. Ten new primitive trinomials were found. Our results are summarized in the following theorem:

Theorem 1. *For the integers r listed in Table 1, the primitive trinomials x^r+x^s+1 of degree r over* GF(2) *are exactly those given in Table 1, and the corresponding reciprocal trinomials $x^r + x^{r-s} + 1$.*

Proof. From the GIMPS Project [7], the integers r listed in Table 1 are exponents of Mersenne primes $2^r - 1$. Thus, irreducible trinomials of degree r are necessarily primitive. Irreducibility of the trinomials listed in Table 1 follows from the authors' computations, using the new algorithm described in [5, 6] (verified using the algorithm of [3] and independently verified by Allan Steel using Magma). Finally, the fact that no irreducible trinomials were missed during the search, for those degrees r, follows from the certificates given on the authors' web pages [1]. $\square$

Remarks. The integers r listed in Table 1 are the known Mersenne exponents of the form $r = \pm 1 \bmod 8$ in the interval $[100\,000, 32\,582\,657]$. For smaller exponents, omitted to save space, see [10] or our web site [1]. According to the GIMPS Project [7], the list is complete for $r \leq 16\,300\,000$. Known Mersenne exponents of the form $r = \pm 3 \bmod 8$ for $r > 5$ can not be the degrees of irreducible trinomials because of Swan's theorem [12]; the possibility $x^r + x^2 + 1$ permitted by Swan's theorem is easily ruled out in all known cases with $r > 5$: see the authors' web site [1].

Our search used a new algorithm [5, 6] relying on fast arithmetic in GF(2)[x], whose details are given in [2]. Another significant improvement over previous work is that certificates were produced; this enables one easily to check that the claimed non-primitive trinomials are indeed reducible. A certificate is simply an encoding of a nontrivial factor of smallest degree. A 2.4Ghz Intel Core 2 takes only 15 minutes to check the certificates of all 16 291 325 reducible trinomials ($s \leq r/2$) of degree $r = 32\,582\,657$ with our `check-ntl` program based on NTL [11].

Acknowledgements. The authors thank Allan Steel, who independently verified (with Magma) the ten new primitive trinomials, and the authors of the Magma and NTL software tools that were used to check reducibility of the other trinomials. Part

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

Key words and phrases. $GF(2)[x]$, irreducible polynomials, irreducible trinomials, primitive polynomials, primitive trinomials, Mersenne exponents, Mersenne numbers.

of the computations reported in this paper were carried out using the Grid'5000 experimental testbed, an initiative of the French Ministry of Research through the ACI GRID incentive action, INRIA, CNRS and RENATER and other contributing partners (see `https://www.grid5000.fr`). The work of the first author was supported by the Australian Research Council.

r	s	Notes
110 503	25230, 53719	Heringa *et al.* [8]
132 049	7000, 33912, 41469, 52549, 54454	Heringa *et al.* [8]
756 839	215747, 267428, 279695	Brent *et al.* [3]
859 433	170340, 288477	Brent *et al.* [3], Kumada *et al.* [9]
3 021 377	361604, 1010202	Brent *et al.* [3]
6 972 593	3037958	Brent *et al.* [4]
24 036 583	8412642, 8785528	Brent and Zimmermann, 2007
25 964 951	880890, 4627670, 4830131, 6383880	Brent and Zimmermann, 2007
30 402 457	2162059	Brent and Zimmermann, 2007
32 582 657	5110722, 5552421, 7545455	Brent and Zimmermann, 2008

Table 1. Known primitive trinomials $x^r + x^s + 1$ of degree a Mersenne exponent $r \geq 100\,000$, for $s \leq r/2$.

References

[1] Richard P. Brent, *Search for primitive trinomials (mod 2)*, `http://wwwmaths.anu.edu.au/~brent/trinom.html`, 2008.

[2] Richard Brent, Pierrick Gaudry, Emmanuel Thomé, and Paul Zimmermann, *Faster multiplication in* GF(2)[x], Proc. of the 8th International Symposium on Algorithmic Number Theory (ANTS VIII), *Lecture Notes in Computer Science* **5011**, Springer-Verlag, 2008, 153–166.

[3] Richard P. Brent, Samuli Larvala, and Paul 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. MR1972745 (2004b:11161)

[4] ———, *A primitive trinomial of degree* 6972593, Math. Comp. **74** (2005), 1001–1002. MR2114660 (2005h:11054)

[5] Richard P. Brent and Paul Zimmermann, *A multi-level blocking distinct degree factorization algorithm* (extended abstract), Proceedings of the 8th International Conference on Finite Fields and Applications (Fq8) (Melbourne, Australia), 2007.

[6] ———, *A multi-level blocking distinct degree factorization algorithm*, Contemporary Mathematics, special issue, to appear. Also available as arXiv:0710.4410.

[7] The Great Internet Mersenne Prime Search, `mersenne.org`.

[8] J. R. Heringa, H. W. J. Blöte, and A. Compagner, *New primitive trinomials of Mersenne-exponent degrees for random-number generation*, International Journal of Modern Physics C **3** (1992), 561–564. MR1169571 (94a:11118)

[9] 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; MR1665959 (2000i:11183); corrigenda: *ibid* **71** (2002), 1337–1338; MR1898761 (2003c:11153)

[10] 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. MR1068813 (91h:11138)

[11] Victor Shoup, *NTL: A library for doing number theory*, `http://www.shoup.net/ntl/`, 2007.

[12] R. G. Swan, *Factorization of polynomials over finite fields*, Pacific J. Math. **12** (1962), 1099–1106. MR0144891 (26 #2432)

Australian National University, Canberra, Australia
E-mail address: `trinomials@rpbrent.com`

INRIA Nancy - Grand Est, Villers-lès-Nancy, France
E-mail address: `Paul.Zimmermann@loria.fr`