MATHEMATICS OF COMPUTATION
VOLUME 62, NUMBER 205
JANUARY 1994, PAGES 385-386

A TABLE OF PRIMITIVE BINARY POLYNOMIALS

MIODRAG ŽIVKOVIĆ

ABSTRACT. For those $n < 5000$ for which the factorization of $2^n - 1$ is known, the first primitive trinomial (if such exists) and a randomly generated primitive 5- and 7-nomial of degree n in GF(2) are given.

A primitive polynomial of degree n over GF(2) is useful for generating a pseudorandom sequence of n-tuples of zeros and ones, see [8]. If the polynomial has a small number k of terms, then the sequence is easily computed. But for cryptological applications (correlation attack, see [5]) it is often necessary to have the primitive polynomials with larger values of k than one can find in the existing tables. For example, Zierler and Brillhart [10, 11] have calculated all irreducible trinomials of degree $n \leq 1000$, with the period for some for which the factorization of $2^n - 1$ is known; Stahnke [7] has listed one example of a trinomial or pentanomial of degree $n \leq 168$; Zierler [12] has listed all primitive trinomials whose degree is a Mersenne exponent $\leq 11213 = M_{23}$ (there, M_j denotes the jth Mersenne exponent); Rodemich and Rumsey [6] have listed all primitive trinomials of degree M_j, $12 \leq j \leq 17$; Kurita and Matsumoto [2] have listed all primitive trinomials of degree M_j, $24 \leq j \leq 28$, and one example of primitive pentanomials of degree M_j, $8 \leq j \leq 27$.

Here we give (see Table 1 in the Supplement section) one primitive binary k-nomial (k-term polynomial) of degree n (if such exists and the factorization of $2^n - 1$ is known) for $2 \leq n \leq 5000$, $k \in \{3, 5, 7\}$. For chosen n and k, we have the polynomial $1 + x^n + \sum x^a$, where a takes the values from the entry at the intersection of the row n and the column k.

The 5- and 7-nomials listed in Table 1 were obtained using a random number generator. Randomly chosen k-nomials of degree n are checked for primitivity (see [9], for example) and rejected until a primitive polynomial is found. The trinomials were tested in the natural order.

The primitivity check is carried out using the factorizations of $2^n - 1$ from [1], and also from [3] $(2^{512}+1)$, [4] $(2^{484}+1)$. These factorizations are known for all $n \leq 310$, and for some $n \leq 2460$, where $2^n - 1$ is not a Mersenne prime. An asterisk in front of n in Table 1 means that $2^n - 1$ contains "probably a prime" factor [1], i.e., a factor without the complete primality proof.

Received by the editor April 3, 1992.

1991 *Mathematics Subject Classification*. Primary 11T06, 11T71.

Key words and phrases. Primitive polynomials, finite field.

This research was supported by Science Fund of Serbia, grant number 0401A, through Matematički Institut.

Bibliography

1. J. Brillhart, D. H. Lehmer, J. L. Selfridge, B. Tuckerman, and S. S. Wagstaff, Jr., *Factorization of* $b^n \pm 1$, $b = 2, 3, 5, 6, 7, 10, 11, 12$ *up to high powers*, 2nd ed., Contemp. Math., vol. 22, Amer. Math. Soc., Providence, RI, 1988.
2. 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.
3. A. K. Lenstra et al., a note in *Editor's corner*, IACR Newsletter **7**, no. 2 (June 1990), 1–2.
4. A. K. Lenstra and M. S. Manasse, *Factoring with two large primes*, Advances in Cryptology—EUROCRYPT'90, Lecture Notes in Comput. Sci., vol. 473, Springer-Verlag, Berlin and New York, 1991, pp. 77–82.
5. W. Meier and O. Staffelbach, *Fast correlation attacks on certain stream ciphers*, J. Cryptology **1** (1989), 159–176.
6. E. R. Rodemich and H. Rumsey, Jr., *Primitive trinomials of high degree*, Math. Comp. **22** (1968), 863–865.
7. W. Stahnke, *Primitive binary polynomials*, Math. Comp. **27** (1973), 977–980.
8. R. C. Tausworthe, *Random numbers generated by linear recurrence modulo two*, Math. Comp. **19** (1965), 201–209.
9. E. J. Watson, *Primitive polynomials* (mod 2), Math. Comp. **16** (1962), 368–369.
10. N. Zierler and J. Brillhart, *On primitive trinomials* (mod 2), Inform. and Control **13** (1968), 541–554.
11. ——, *On primitive trinomials* (mod 2). II, Inform. and Control **14** (1969), 566–569.
12. N. Zierler, *Primitive trinomials whose degree is a Mersenne exponent*, Inform. and Control **15** (1969), 67–69.

Institute for Applied Mathematics and Electronics, Beograd, Yugoslavia