TECHNICAL NOTES AND SHORT PAPERS

Primitive Trinomials of High Degree*

By Eugene R. Rodemich and Howard Rumsey, Jr.**

Summary. New primitive polynomials (mod 2) of high degree were found by the methods described here. The polynomials are all trinomials; such trinomials are useful for generating pseudo-random sequences of 0's and 1's of long length [1].

I. **Introduction.** An irreducible polynomial of degree n over $GF(2)$ has the form

$$P(x) = x^n + \sum_{k=1}^{n} a_k x^{n-k},$$

where $a_k = 0$ or 1, $k = 1, \cdots, n$. It is easily shown that the roots of $P(x)$ lie in $GF(2^n)$; accordingly, they satisfy the equation

$$x^{2^n-1} = 1 . \tag{1}$$

$P(x)$ is said to be *primitive* if its roots do not satisfy $x^m = 1$ for any positive m less than $2^n - 1$. Then, for any root of $P(x)$, the numbers $x, x^2, \cdots, x^{2^n-1}$ are all the nonzero elements of $GF(2^n)$ [2].

There is a linear recurrence relation associated with $P(x)$. Let $y_1, y_2, \cdots, y_n$ have values zero and one, and define $y_j = 0$ or 1, for $j \geqq n + 1$, by

$$y_j \equiv \sum_{k=1}^{n} a_k y_{j-k} \pmod 2 .$$

If $P(x)$ is primitive, and n and $2^n - 1$ are relatively prime, consecutive sets of n-tuples $(y_{ln+1}, y_{ln+2}, \cdots, y_{ln+n})$, $l = 0, 1, 2, \cdots$, have many statistical properties which approximate those of a sequence of independent random n-tuples of zeros and ones (see [1]). Thus a primitive polynomial of degree n is useful for generating a pseudo-random sequence of n-tuples of zeros and ones. In this application, trinomials are better than polynomials with more nonzero coefficients, because the complexity of the hardware needed grows with the number of coefficients.

II. **Method.** In general, to determine whether a given trinomial $P(x)$ of high degree n is primitive is no simple task. If n is a Mersenne exponent, that is if $2^n - 1$ is prime, the following lemma can be used.

LEMMA. *If $2^n - 1$ is prime, a trinomial of degree n is primitive if and only if it is a factor of $x^{2^n-1} + 1$.*

Proof. Let x_1 be any root of the trinomial $P(x)$, and let m be the smallest positive number such that $x_1^m = 1$. Then m is a factor of $2^n - 1$. By hypothesis, $2^n - 1$ is prime, hence $m = 2^n - 1$. $P(x)$ must be irreducible, for if x_1 were a root

Received January 23, 1967. Revised January 25, 1968.

* This paper presents the results of one phase of research carried out at the Jet Propulsion Laboratory, California Institute of Technology, under Contract No. NAS 7-100, sponsored by the National Aeronautics and Space Administration.

** Communications Systems Research Section of the California Institute of Technology Jet Propulsion Laboratory, 4800 Oak Grove Drive, Pasadena, California.

of an irreducible factor of $P(x)$ of degree $d < n$, m would divide $2^d - 1$.

This lemma can be applied in the following way. For a general root x of $P(x)$, any power of x can be written as a polynomial of degree less than n, reducing the degree by application of the relation

$$x^N = \sum_{k=1}^{n} a_k x^{N-k}, \qquad N \geqq n .$$

In particular,

$$x^{2^j} = Q_j(x) , \qquad j = 1, 2, \cdots ,$$

where $Q_j(x)$ has degree less than n. $Q_j(x)$ can be determined from $Q_{j-1}(x)$ by squaring and reducing the degree. By the lemma, if $2^n - 1$ is prime, $P(x)$ is irreducible if and only if $Q_n(x) = x$.

Using various Mersenne exponents n, the trinomials

$$P(x) = x^n + x^p + 1 , \qquad 1 \leqq p < n/2$$

were tested for primitivity. Only values of $p < n/2$ were used, because if $P(x)$ is primitive, then

$$x^n P(1/x) = x^n + x^{n-p} + 1$$

is also primitive. To speed up the work, a simpler test than the one described above was used to eliminate about 80% of the possible values of p.

This simpler test checked $P(x)$ for factors in common with the polynomials $x^{2^j-1} + 1$, $j = 2, 3, \cdots, 10$. $P(x)$ has a factor in common with $x^{2^j-1} + 1$ if p belongs to certain residue classes modulo $2^j - 1$ (depending on n). For example, $P(x)$ and $x^3 + 1$ have a common factor if $n + p \equiv 0 \pmod 3$. For each value of n, these prohibited residue classes were computed at the beginning by running through the values of $p \pmod{2^j - 1}$ and applying Euclid's algorithm for finding a common factor. Then for $p = 1, 2, \cdots, (n - 1)/2$, if p did not belong to any of these residue classes, the coefficients of $Q_n(x)$ were computed. The work was done on an SDS 930 computer.

III. **Results.** In the following table, all Mersenne exponents n from 127 to 2281 are listed [3]. The values given for p are all choices of the second exponent which are less than $n/2$, such that $P(x)$ is primitive. L. D. Baumert has pointed out that a result of Swan [5] shows that there are no primitive trinomials of degree 2203.

TABLE 1

Exponents for primitive trinomials

n	p
127	1, 7, 15, 30, 63
521	32, 48, 158, 168
607	105, 147, 273
1279	216, 418
2203	none
2281	715, 915, 1029

The accuracy of the program was tested by computing all primitive trinomials of degree n for all Mersenne exponents $n < 100$. This list of trinomials was compared with an unpublished table (by E. J. Watson) of all irreducible trinomials over $GF(2)$ of degree less than 100.

A list of primitive polynomials of lower degree is given in [4].

Jet Propulsion Laboratory
California Institute of Technology
Pasadena, California 91109

1. R. C. TAUSWORTHE, "Random numbers generated by linear recurrence modulo two," *Math. Comp.*, v. 19, 1965, pp. 201–209. MR **32** #1878.
2. A. A. ALBERT, *Fundamental Concepts of Higher Algebra*, Univ. of Chicago Press, Chicago, Ill., 1958. MR **20** #5190.
3. S. W. GOLOMB, et. al., *Digital Communications With Space Applications*, Prentice-Hall, Englewood Cliffs, N. J., 1964.
4. E. J. WATSON, "Primitive polynomials (mod 2)," *Math. Comp.*, v. 16, 1962, pp. 368-369. MR **26** #5764.
5. R. G. SWAN, "Factorization of polynomials over finite fields, " *Pacific J. Math.*, v. 12, 1962, pp. 1099–1106. MR **26** #2432.