MATHEMATICS OF COMPUTATION
VOLUME 63, NUMBER 207
JULY 1994, PAGES 389-401

# ON THE PERIODS OF GENERALIZED FIBONACCI RECURRENCES

RICHARD P. BRENT

ABSTRACT. We give a simple condition for a linear recurrence (mod $2^w$) of degree $r$ to have the maximal possible period $2^{w-1}(2^r - 1)$. It follows that the period is maximal in the cases of interest for pseudorandom number generation, i.e., for three-term linear recurrences defined by trinomials which are primitive (mod 2) and of degree $r > 2$. We consider the enumeration of certain exceptional polynomials which do not give maximal period, and list all such polynomials of degree less than 15.

## 1. INTRODUCTION

The Fibonacci numbers satisfy a linear recurrence

$$F_n = F_{n-1} + F_{n-2}.$$

*Generalized Fibonacci* recurrences of the form

$$x_n = \pm x_{n-s} \pm x_{n-r} \mod 2^w \tag{1}$$

are of interest because they are often used to generate pseudorandom numbers [1, 6, 7, 12, 14, 18]. We assume throughout that $x_0, \ldots, x_{r-1}$ are given and not all even, and $w > 0$ is a fixed exponent. Usually, $w$ is close to the wordlength of the (binary) computer used.

Apart from computational convenience, there is no reason to restrict attention to three-term recurrences of the special form (1). Thus, we consider a general linear recurrence

$$q_0 x_n + q_1 x_{n+1} + \cdots + q_r x_{n+r} = 0 \mod 2^w \tag{2}$$

defined by a polynomial $Q(t) = q_0 + q_1 t + \cdots + q_r t^r$ with integer coefficients and degree $r > 0$. We assume throughout that $q_0$ and $q_r$ are odd. Because $q_0$ is odd, the sequence $(x_n)$ is reversible, i.e., $x_n$ is uniquely defined (mod $2^w$) by $x_{n+1}, \ldots, x_{n+r}$. Thus, $(x_n)$ is purely periodic [20].

Received by the editor May 4, 1992 and, in revised form, December 23, 1992.

1991 *Mathematics Subject Classification*. Primary 11Y55, 12E05, 05A15; Secondary 11-04, 11T06, 11T55, 12-04, 12E10, 65C10, 68R05.

*Key words and phrases*. Fibonacci sequence, generalized Fibonacci sequence, irreducible trinomial, linear recurrence, maximal period, periodic integer sequence, primitive trinomial, pseudorandom numbers.

©1994 American Mathematical Society
0025-5718/94 \$1.00 + \$.25 per page

In the following we often work in a ring $\mathbf{Z}_m[t]/Q(t)$ of polynomials (mod $Q$) whose coefficients are regarded as elements of $\mathbf{Z}_m$, the ring of integers mod $m$. For relations $A = B$ in $\mathbf{Z}_m[t]/Q(t)$ we use the notation

$$A = B \mod (m, Q).$$

It may be shown by induction on $n$ that, if $a_{n,0}, \ldots, a_{n,r-1}$ are defined by

$$t^n = \sum_{j=0}^{r-1} a_{n,j} t^j \mod (2^w, Q(t)), \tag{3}$$

then

$$x_n = \sum_{j=0}^{r-1} a_{n,j} x_j \mod 2^w. \tag{4}$$

Also, the generating function

$$G(t) = \sum_{n=0}^{\infty} x_n t^n \tag{5}$$

is given by

$$G(t) = \frac{P(t)}{\widetilde{Q}(t)} \mod 2^w, \tag{6}$$

where

$$P(t) = \sum_{k=0}^{r-1} \left( \sum_{j=0}^{k} q_{r+j-k} x_j \right) t^k$$

is a polynomial of degree less than $r$, and

$$\widetilde{Q}(t) = t^r Q(1/t) = q_0 t^r + q_1 t^{r-1} + \cdots + q_r$$

is the *reverse* of $Q$. In the literature, $\widetilde{Q}(t)$ is sometimes called the *characteristic polynomial* [5] or the *associated polynomial* [20] of the sequence. The use of generating functions is convenient and has been adopted by many earlier authors (e.g., Schur [16]). Ward [20] does not explicitly use generating functions, but his polynomial $U$ is the same as our $\widetilde{Q}$, and many of his results could be obtained via generating functions.

Let $\rho_w$ be the period of $t$ under multiplication mod $(2^w, Q(t))$, i.e., $\rho_w$ is the least positive integer $\rho$ such that

$$t^\rho = 1 \mod (2^w, Q(t)).$$

In the literature, $\rho_w$ is sometimes called the *principal period* [20] of the linear recurrence, sometimes simply the *period* [5]. For brevity we define $\lambda = \rho_1$.

If $Q(t)$ is irreducible in $\mathbf{Z}_2[t]$, then $Q(t)$ is a factor of $t^{2^r} - t$ (see, e.g., [19]), so $\lambda \mid 2^r - 1$. We say that $Q(t)$ is *primitive* (mod 2) if $\lambda = 2^r - 1$. Note that primitivity is a stronger condition than irreducibility, i.e., $Q(t)$ primitive implies that $Q(t)$ is irreducible[1], but the converse is not generally true unless $2^r - 1$ is prime. For example, the polynomial $1 + t + t^2 + t^4 + t^6$ is irreducible, but not primitive, since it has $\lambda = 21 < 2^6 - 1$. Tables of irreducible and primitive trinomials are available [5, 11, 15, 17, 21, 23, 24, 25].

In the following we usually assume that $Q(t)$ is irreducible. Our assumption that $q_0$ and $q_r$ are odd excludes the trivial case $Q(t) = t$, and implies that $\widetilde{Q}(t)$ is irreducible (or primitive) of degree $r$ if and only if the same is true of $Q(t)$.

We are interested in the period $p_w$ of the sequence $(x_n)$, i.e., the minimal positive $p$ such that

$$x_{n+p} = x_n \tag{7}$$

for all sufficiently large $n$. In fact, because of the reversibility of the sequence, (7) should hold for all $n$. The period is sometimes called the *characteristic number* of the sequence [20]. In general, the period depends on the initial values $x_0, \dots, x_{r-1}$, but under our assumptions the period depends only on $Q(t)$, in fact $p_w = \rho_w$ (see Lemma 2).

It is known [8, 13, 20] that $p_w \le 2^{w-1}\lambda$, with equality holding for all $w > 0$ if and only if it holds for $w = 3$. The main aim of this paper is to give a simple necessary and sufficient condition for

$$p_w = 2^{w-1}\lambda. \tag{8}$$

The result is stated in Theorem 2 in terms of a simple condition which we call "Condition S" (see §2). In Theorem 3 we deduce that the period is maximal if $Q(t)$ is a primitive trinomial of degree greater than 2. Thus, in cases of practical interest for pseudorandom number generation, it is only necessary to verify that $Q(t)$ is primitive. This is particularly easy if $2^r - 1$ is a Mersenne prime, because then a necessary and sufficient condition is

$$t^{2^r} = t \mod (2, Q(t)).$$

A word of caution is appropriate. Even when the period $p_w$ satisfies (8), it is not desirable to use a full cycle of $p_w$ numbers in applications requiring independent pseudorandom numbers. This is because only the most significant bit has the full period. If the bits are numbered from 1 (least significant) to $w$ (most significant), then bit $k$ has period $p_k$.

The basic results on linear recurrences modulo $m$ were obtained many years ago—see, for example, Ward [20]. However, our main results (Theorems 2 and 3) and the statement of "Condition S" (§2) appear to be new.

## 2. A Condition for maximal period

The following lemma is a special case of Hensel's Lemma [8, 9, 22] and may be proved using an application of Newton's method for reciprocals [10].

**Lemma 1.** *Suppose that $P(t) \bmod 2$ is invertible in $\mathbf{Z}_2[t]/Q(t)$. Then, for all $w \ge 1$, $P(t) \bmod 2^w$ is invertible in $\mathbf{Z}_{2^w}[t]/Q(t)$.*

---

[1]For brevity we usually omit the "mod 2" when saying that a polynomial is irreducible or primitive. Thus "$Q(t)$ is irreducible (resp. primitive)" means that $Q(t) \bmod 2$ is irreducible (resp. primitive) in $\mathbf{Z}_2[t]$.

We now give a sufficient condition for the periods $p_w$ and $\rho_w$ to be the same.

**Lemma 2.** *If $Q(t)$ is irreducible of degree $r$, and at least one of $x_0, \dots, x_{r-1}$ is odd, then $p_w = \rho_w$.*

*Proof.* For brevity we write $p = p_w$ and $\rho = \rho_w$. From (5),

$$G(t) = \frac{R(t)}{1 - t^p} \mod 2^w,$$

where $R(t)$ has degree less than $p$. Thus, from (6),

$$R(t)\widetilde{Q}(t) = (1 - t^p)P(t) \mod 2^w. \tag{9}$$

$P(t) \bmod 2$ has degree less than $r$, but is not identically zero. Since $\widetilde{Q}(t) \bmod 2$ is irreducible of degree $r$, application of the extended Euclidean algorithm [8] to $P(t) \bmod 2$ and $\widetilde{Q}(t) \bmod 2$ constructs the inverse of $P(t) \bmod 2$ in $\mathbf{Z}_2[t]/\widetilde{Q}(t)$. Thus, Lemma 1 shows that $P(t) \bmod 2^w$ is invertible in $\mathbf{Z}_{2^w}[t]/\widetilde{Q}(t)$. It follows from (9) that

$$t^p = 1 \mod (2^w, \widetilde{Q}(t)),$$

and $\rho \mid p$. However, from (3) and (4), $p \mid \rho$. Thus, $p = \rho$. □

As an example, consider $Q(t) = 1 - t + t^2$. We have $t^3 = 1 \bmod (2, Q(t))$, $t^3 = -1 \bmod Q(t)$, and $t^6 = 1 \bmod Q(t)$, so

$$\rho_w = \begin{cases} 3 & \text{if } w = 1, \\ 6 & \text{if } w > 1. \end{cases} \tag{10}$$

It is easy to verify that (10) gives the period $p_w$ of the corresponding recurrence

$$x_n = x_{n-1} - x_{n-2} \mod 2^w,$$

provided $x_0$ and $x_1$ are not both even.

The assumption of irreducibility in Lemma 2 is significant. For example, consider $Q(t) = t^2 - 1$ and $w = 1$, with initial values $x_0 = x_1 = 1$. The recurrence is $x_n = x_{n-2} \bmod 2$, so $p_1 = 1$, but $\rho_1 = 2$. Here, $P(t) = 1 + t$ is a divisor of $\widetilde{Q}(t) = 1 - t^2$.

We now define a condition which must be satisfied by $Q(\pm t)$ if the period $p_w$ of the sequence $(x_n)$ is less than $2^{w-1}\lambda$ (see Theorem 2 for details). For given $Q(t)$ the condition can be checked in $O(r^2)$ operations, or in $O(r \log r)$ operations if the FFT is used to compute the convolutions in (11). Even the $O(r^2)$ algorithm is much faster than the method suggested by Marsaglia and Tsay [13], which involves forming high powers of $r \times r$ matrices (mod 8), or the method of Knuth [8, ex. 3.2.2.11], which involves forming high powers in $\mathbf{Z}_8[t]/Q(t)$.

*Condition* S. Let $Q(t) = \sum_{j=0}^{r} q_j t^j$ be a polynomial of degree $r$. We say that $Q(t)$ satisfies Condition S if and only if

$$Q(t)^2 + Q(-t)^2 = 2q_r Q(t^2) \mod 8.$$

Lemma 3 gives an equivalent condition, which is more convenient for computational purposes. For another equivalent condition, see the remark following (22) in the proof of Theorem 1. The proof of Lemma 3 is straightforward, so is omitted.

**Lemma 3.** *A polynomial $Q(t)$ of degree $r$ satisfies Condition* S *if and only if*

$$\sum_{\substack{j+k=2m \\ 0\le j<k\le r}} q_j q_k = \epsilon_m \mod 2 \tag{11}$$

*for $0 \le m \le r$, where*

$$\epsilon_m = \frac{q_m(q_m - q_r)}{2}. \tag{12}$$

As an exercise, the reader may verify that the polynomial $Q(t) = 1 - t + t^2$ satisfies both the definition of Condition S and the equivalent conditions of Lemma 3. For other examples, see Table 1.

For convenience we collect in Lemma 4 some results regarding arithmetic in the rings $\mathbf{Z}_{2^w}[t]/Q(t)$.

**Lemma 4.** *Let $X(t)$ and $Y(t)$ be polynomials over* $\mathbf{Z}$, *and $Q(t)$ be as in* §1. *Then, for $w \ge 1$,*

$$X = Y \mod (2^w, Q) \Rightarrow X^2 = Y^2 \mod (2^{w+1}, Q). \tag{13}$$

*Also, if $Q(t)$ is irreducible, then*

$$X^2 = Y^2 \mod (2, Q) \Leftrightarrow X^2 = Y^2 \mod (4, Q) \tag{14}$$

*and*

$$X^2 = Y^2 \mod (8, Q) \Leftrightarrow X = \pm Y \mod (4, Q). \tag{15}$$

*Proof.* If $X = Y \bmod (2^w, Q)$, then $X = Y + 2^w R \bmod Q$ for some polynomial $R(t)$ in $\mathbf{Z}[t]$. Thus, $X^2 = Y^2 + 2^{w+1}R(Y + 2^{w-1}R) \bmod Q$, and (13) follows.

If $Q(t)$ is irreducible and $X^2 = Y^2 \bmod (2, Q)$, then $(X - Y)^2 = 0 \bmod (2, Q)$. Since $Q$ is irreducible, it follows that $X = Y \bmod (2, Q)$. Thus, from (13), $X^2 = Y^2 \bmod (4, Q)$, and (14) follows.

Finally, if $Q$ is irreducible and $X^2 = Y^2 \bmod (8, Q)$ then, as in the proof of (14), we obtain $X = Y \bmod (2, Q)$, so $X = Y + 2R \bmod Q$, where $R(t)$ is some polynomial in $\mathbf{Z}[t]$. Thus, $4R(Y + R) = 0 \bmod (8, Q)$, i.e., $R(Y + R) = 0 \bmod (2, Q)$. Since $Q$ is irreducible, either $R = 0 \bmod (2, Q)$ or $Y + R = 0 \bmod (2, Q)$. In the former case, $X = Y \bmod (4, Q)$, and in the latter case, $X = -Y \bmod (4, Q)$. Thus, $X = \pm Y \bmod (4, Q)$. The implication in the other direction follows from (13). This establishes (15). □

The following result is the key to the proof of Theorem 2. There is no obvious generalization to odd moduli. Recall that $\lambda = \rho_1$.

**Theorem 1.** *Let* $Q(t) \bmod 2$ *be irreducible in* $\mathbf{Z}_2[t]$. *Then*

$$t^\lambda = -1 \mod (4, Q(t))$$

*if and only if* $Q(t)$ *satisfies Condition* S, *and*

$$t^\lambda = 1 \mod (4, Q(t))$$

*if and only if* $Q(-t)$ *satisfies Condition* S.

*Proof.* Let

$$V(t) = \sum_{j=0}^{\lfloor r/2 \rfloor} q_{2j} t^j, \qquad W(t) = \sum_{j=0}^{\lfloor (r-1)/2 \rfloor} q_{2j+1} t^j,$$

so $Q(t)$ splits into even and odd parts:

$$Q(t) = V(t^2) + tW(t^2). \tag{16}$$

By the definition of $\lambda$, we have $t = t^{\lambda+1} \bmod (2, Q(t))$, so

$$V(t^2) = t^{\lambda+1} W(t^2) \mod (2, Q(t)). \tag{17}$$

Because $X(t^2) = X(t)^2 \bmod 2$ for any polynomial $X(t)$ in $\mathbf{Z}[t]$, equation (17) may be written as

$$V(t)^2 = t^{\lambda+1} W(t)^2 \mod (2, Q(t)).$$

Since $\lambda$ is a divisor of $2^r - 1$, it is odd, so $t^{\lambda+1}$ is a square. Thus, from (14),

$$V(t)^2 = t^{\lambda+1} W(t)^2 \mod (4, Q(t)). \tag{18}$$

Also, since $V(t) = V(-t) \bmod 2$ and $W(t) = W(-t) \bmod 2$, we have

$$V(-t)^2 = t^{\lambda+1} W(-t)^2 \mod (4, Q(t)). \tag{19}$$

To prove the first half of the theorem, suppose that

$$t^\lambda = -1 \mod (4, Q(t)).$$

Thus, from (18),

$$V(t)^2 + tW(t)^2 = 0 \mod (4, Q(t)). \tag{20}$$

It follows that

$$V(t)^2 + tW(t)^2 - q_r Q(t) = 0 \mod (4, Q). \tag{21}$$

However, the left side of (21) is a polynomial of degree less than $r$. Hence,

$$V(t)^2 + tW(t)^2 - q_r Q(t) = 0 \mod 4. \tag{22}$$

Replace $t$ by $t^2$ in the identity (22). From (16), the result is easily seen to be equivalent to $Q(t)$ satisfying Condition S.

To prove the converse, suppose that $Q(t)$ satisfies Condition S. Reversing our argument, we see that (20) holds. Thus, from (18),

$$(t^{\lambda+1}+t)W(t)^2 = 0 \mod (4, Q(t)).$$

Now $W(t)$ has degree less than $r$, and $W(t) \neq 0 \bmod 2$, because otherwise, using (16), $Q(t) = V(t)^2 \bmod 2$ would contradict the irreducibility of $Q(t)$. It follows that $W(t) \bmod 2$ is invertible in $\mathbf{Z}_2[t]/Q(t)$. From Lemma 1, $W(t) \bmod 4$ is invertible in $\mathbf{Z}_4[t]/Q(t)$, and we obtain

$$t^{\lambda+1}+t = 0 \mod (4, Q(t)).$$

Since $Q(t) \neq t \bmod 2$, we can divide by $t$ to obtain

$$t^{\lambda} = -1 \mod (4, Q(t)).$$

This completes the proof of the first half of the theorem.

The proof of the second half is similar, with appropriate changes of sign. Suppose that

$$t^{\lambda} = 1 \mod (4, Q(t)). \tag{23}$$

From (19),

$$V(-t)^2 = tW(-t)^2 \mod (4, Q(t)).$$

Thus, instead of (22) we obtain

$$V(-t)^2 - tW(-t)^2 - (-1)^r q_r Q(t) = 0 \mod 4. \tag{24}$$

Replace $t$ by $-t^2$ in the identity (24). The result is equivalent to $Q(-t)$ satisfying Condition S. The converse also applies: if $Q(-t)$ satisfies Condition S then, by reversing our argument and using irreducibility of $Q(t)$, we find that (23) holds. □

We are now ready to state Theorem 2, which relates the period of the sequence $(x_n)$ to Condition S. In view of Theorem 1, Theorem 2 is implicit in Ward [20, p. 628]. More precisely, Ward's case $T > 1$ corresponds to $Q(-t)$ satisfying Condition S, while Ward's case ($T = 1$, $K(x) = 1 \bmod 2$) corresponds to $Q(t)$ satisfying Condition S. However, Ward's exposition is complicated by consideration of odd prime power moduli (see for example his Theorem 13.1), so we give an independent proof.

**Theorem 2.** *Let $Q(t)$ be irreducible and define a linear recurrence by* (2), *with at least one of $x_0, \dots, x_{r-1}$ odd. Then the sequence $(x_n)$ has period*

$$p_w \leq 2^{w-2}\lambda$$

*for all $w \geq 2$ if $Q(-t)$ satisfies Condition* S,

$$p_w \leq 2^{w-2}\lambda$$

*for all $w \geq 3$ if $Q(t)$ satisfies Condition* S, *and*

$$p_w = 2^{w-1}\lambda$$

*for all $w \geq 1$ if and only if neither $Q(t)$ nor $Q(-t)$ satisfies Condition* S.

*Proof.* From Lemma 2, $p_w = \rho_w$ is the order of $t \bmod (2^w, Q(t))$. If $Q(-t)$ satisfies Condition S, then, from Theorem 1,

$$t^\lambda = 1 \mod (4, Q(t)).$$

By (13), it follows by induction on $w$ that

$$t^{2^{w-2}\lambda} = 1 \mod (2^w, Q(t))$$

for all $w \geq 2$. This proves the first part of the theorem. The second part is similar, so it only remains to prove the third part.

Suppose that $\rho_w = 2^{w-1}\lambda$ for all $w > 0$. In particular, for $w = 3$ we have period $\rho_3 = 4\lambda$. Thus,

$$t^{2\lambda} \neq 1 \mod (8, Q(t))$$

and, from (15),

$$t^\lambda \neq \pm 1 \mod (4, Q(t)). \tag{25}$$

From Theorem 1, neither $Q(t)$ nor $Q(-t)$ can satisfy Condition S, or we would obtain a contradiction to (25).

Conversely, if neither $Q(t)$ nor $Q(-t)$ satisfies Condition S, then we show by induction on $w$ that

$$t^{2^{w-1}\lambda} = 1 + 2^w R_w \mod Q(t), \tag{26}$$

where

$$R_w \neq 0 \mod (2, Q(t)), \tag{27}$$

for all $w \geq 1$. Certainly,

$$t^\lambda = 1 \mod (2, Q(t)),$$

but, from Theorem 1,

$$t^\lambda \neq 1 \mod (4, Q(t)),$$

so (26) and (27) hold for $w = 1$. Defining

$$R_w = R_{w-1}(1 + 2^{w-2}R_{w-1}) \tag{28}$$

for $w \geq 2$, we see that (26) holds for all $w \geq 1$. It remains to prove (27) for $w > 1$.

For $w = 2$, inequality (27) follows from Theorem 1 and (15), as $t^\lambda \neq \pm 1 \bmod (4, Q(t))$ implies $t^{2\lambda} \neq 1 \bmod (8, Q(t))$. For $w > 2$, the inequality (27) follows by induction from (28), since $2^{w-2}$ is even. It follows that $\rho_w = 2^{w-1}\lambda$ for all $w \geq 1$. □

## 3. Primitive trinomials

In this section we consider a case of interest because of its applications to pseudorandom number generation:

$$Q(t) = q_0 + q_s t^s + q_r t^r$$

is a trinomial $(r > s > 0)$. Theorem 3 shows that the period is always maximal in cases of practical interest. The condition $r > 2$ is necessary, as the example $Q(t) = 1 - t + t^2$ of §2 shows.

**Theorem 3.** *Let $Q(t) = q_0 + q_s t^s + q_r t^r$ be a primitive trinomial of degree $r > 2$. Then the sequence $(x_n)$ defined by (2), with at least one of $x_0, \dots, x_{r-1}$ odd, has period $p_w = 2^{w-1}(2^r - 1)$.*

*Proof.* From Theorem 2 it is sufficient to show that $Q(t)$ does not satisfy Condition S. (Since $Q(-t)$ is also a trinomial, the same argument shows that $Q(-t)$ does not satisfy Condition S.)

Suppose, by way of contradiction, that $Q(t)$ satisfies Condition S. We use the formulation of Condition S given in Lemma 3. Since $Q(t)$ is irreducible, we have $q_0 = q_s = q_r = 1 \bmod 2$. If $s$ is even, say $s = 2m$, then

$$\sum_{\substack{j+k=2m \\ 0\le j<k\le r}} q_j q_k = q_0 q_s = 1 \mod 2,$$

so $\epsilon_m \neq 0$, and (12) implies that $q_m \neq 0$. Since $0 < m < s < r$, this contradicts the assumption that $Q(t)$ is a trinomial. Hence, $s$ must be odd.

If $r$ is odd then $r + s$ is even, and a similar argument shows that $q_{(r+s)/2} \neq 0$, contradicting the assumption that $Q(t)$ is a trinomial. Hence, $r$ must be even.

Taking $m = r/2$, we see that $\epsilon_m \neq 0$, so $q_m \neq 0$. This is only possible if $m = s$, so $Q(t) = t^{2s} + t^s + 1 \mod 2$. In this case, $t^{3s} = 1 \bmod (2, Q(t))$. Now $r = 2s > 2$, so $3s < 2^r - 1$, and $Q(t)$ cannot be primitive. This contradiction completes the proof. □

A minor modification of the proof of Theorem 3 gives:

**Theorem 4.** *Let $Q(t) = q_0 + q_s t^s + q_r t^r$ be an irreducible trinomial of degree $r \neq 2s$. Then the sequence $(x_n)$ defined by (2), with at least one of $x_0, \dots, x_{r-1}$ odd, has period $p_w = 2^{w-1}\lambda$.*

As mentioned above, it is easy to find primitive trinomials of very high degree $r$ if $2^r - 1$ is a Mersenne prime. Zierler [24] gives examples with $r \le 9689$, and we found two examples with higher degree: $t^{19937} + t^{9842} + 1$ and $t^{23209} + t^{9739} + 1$. These and other examples with $r \le 44497$ were found independently by Kurita and Matsumoto [11]. Such primitive trinomials provide the basis for fast random number generators with extremely long periods and good statistical properties [3]. In general, random number generators with larger $r$ have better statistical properties than those with smaller $r$, and generators with small $r$ should be avoided [3, 4].

## 4. Exceptional polynomials

We say that a polynomial $Q(t)$ of degree $r > 1$ is *exceptional* if conditions E1–E3 hold, and is a *candidate* if conditions E2–E3 hold:

E1. $Q(t) \bmod 2$ is primitive.
E2. $Q(t)$ has coefficients $q_j \in \{0, -1, +1\}$, and $q_0 = q_r = 1$.
E3. $Q(t)$ satisfies Condition S.

If $Q(t)$ is exceptional then, by Theorem 2, $Q(t)$ and $Q(-t)$ define linear recurrences (mod $2^w$) which have less than the maximal period for all $w > 2$. In Table 1 we list the exceptional polynomials $Q(t)$ of degree $r \le 14$. If $Q(t)$ is exceptional, then so is $\widetilde{Q}(t)$. Thus, we only list one of these in Table 1.

TABLE 1. Exceptional polynomials of degree $r \le 14$

| $r$ | $Q(t)$ |
|---|---|
| 2 | $1 - t + t^2$ |
| 5 | $1 - t - t^2 + t^4 + t^5$ |
| 9 | $1 - t + t^2 + t^3 - t^4 - t^6 + t^9$<br>$1 - t + t^2 - t^3 - t^4 + t^8 + t^9$<br>$1 - t + t^2 - t^3 - t^4 - t^5 + t^6 + t^8 + t^9$ |
| 10 | $1 - t + t^2 + t^3 + t^4 + t^6 - t^7 + t^9 + t^{10}$ |
| 11 | $1 - t + t^2 - t^3 - t^4 + t^5 + t^6 - t^8 + t^{11}$ |
| 12 | $1 - t + t^2 - t^3 - t^4 - t^8 + t^9 + t^{11} + t^{12}$ |
| 13 | $1 - t + t^2 - t^3 + t^4 - t^5 - t^6 + t^{12} + t^{13}$<br>$1 - t + t^2 - t^3 + t^4 - t^5 - t^6 - t^7 + t^8 + t^{12} + t^{13}$<br>$1 - t - t^2 - t^4 - t^6 + t^7 - t^8 + t^9 + t^{10} + t^{12} + t^{13}$<br>$1 - t + t^2 + t^3 + t^4 + t^5 + t^7 + t^9 - t^{11} - t^{12} + t^{13}$<br>$1 - t + t^2 + t^3 + t^4 + t^5 - t^8 - t^9 - t^{11} - t^{12} + t^{13}$ |
| 14 | $1 - t + t^2 + t^3 - t^4 - t^6 - t^7 + t^8 + t^9 - t^{11} + t^{14}$<br>$1 + t + t^3 - t^4 - t^5 + t^6 + t^7 + t^8 + t^9 - t^{11} + t^{14}$<br>$1 - t - t^2 + t^3 - t^5 + t^6 + t^7 - t^8 - t^9 + t^{13} + t^{14}$<br>$1 - t - t^2 - t^3 - t^5 + t^7 + t^9 + t^{10} - t^{11} + t^{13} + t^{14}$<br>$1 - t - t^2 + t^4 - t^6 + t^8 + t^9 + t^{10} + t^{11} + t^{13} + t^{14}$ |

Only the coefficients of $Q(t) \bmod 4$ are relevant to Condition S. If condition E2 is relaxed to allow coefficients equal to 2, then, by Lemma 3, there is one such $Q(t)$ corresponding to each primitive polynomial in $\mathbf{Z}_2[t]$. With condition E2 as stated, the number of these $Q(t)$ is considerably reduced.

It is interesting to consider strengthening condition E2 by asking for certain patterns in the signs of the coefficients. For example, we might ask for polynomials $Q(t)$ with all coefficients $q_j \in \{0, 1\}$, or for all coefficients of $\pm Q(-t)$ to be in $\{0, 1\}$. There are candidates satisfying these conditions, but we have not found any which are also exceptional, apart from the trivial $Q(t) = 1 - t + t^2$. It is possible for an exceptional polynomial to have $(-1)^j q_j \ge 0$ for $0 \le j < r$. The only example for $2 < r \le 44$ is

$$Q(t) = 1 - t + t^2 - t^5 + t^6 + t^8 - t^9 + t^{10} + t^{12} - t^{13} + t^{16} + t^{18} + t^{21}.$$

Observe that $Q(-t)$ defines a linear recurrence with nonnegative coefficients

$$\begin{aligned} x_{n+21} = & x_n + x_{n+1} + x_{n+2} + x_{n+5} + x_{n+6} + x_{n+8} \\ & + x_{n+9} + x_{n+10} + x_{n+12} + x_{n+13} + x_{n+16} + x_{n+18}, \end{aligned}$$

which has period $p_2 = p_1 = 2^{21} - 1$ when considered mod 2 *or* mod 4.

The number $\nu(r)$ of exceptional $Q(t)$ (counting only one of $Q(t)$, $\widetilde{Q}(t)$) is given in Table 2. The term "exceptional" is justified as $\nu(r)$ appears to be a much more slowly growing function of $r$ than the number [5]

$$\lambda_2(r) = \varphi(2^r - 1)/r$$

TABLE 2. Number of exceptional polynomials

| $r$ | $\nu(r)$ | $\overline{\nu}(r)$ | $r$ | $\nu(r)$ | $\overline{\nu}(r)$ | $r$ | $\nu(r)$ | $\overline{\nu}(r)$ | $r$ | $\nu(r)$ | $\overline{\nu}(r)$ |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 0 | 0 | 11 | 1 | 0.13 | 21 | 79 | 0.3923 | 31 | 4380 | 0.4721 |
| 2 | 1 | 1.78 | 12 | 1 | 0.22 | 22 | 94 | 0.4390 | 32 | 3125 | 0.4636 |
| 3 | 0 | 0 | 13 | 5 | 0.33 | 23 | 231 | 0.4837 | 33 | 7232 | 0.4549 |
| 4 | 0 | 0 | 14 | 5 | 0.37 | 24 | 129 | 0.4650 | 34 | 8862 | 0.4656 |
| 5 | 1 | 0.70 | 15 | 15 | 0.62 | 25 | 428 | 0.4388 | 35 | 18870 | 0.4792 |
| 6 | 0 | 0 | 16 | 12 | 0.58 | 26 | 448 | 0.4615 | 36 | 10516 | 0.4560 |
| 7 | 0 | 0 | 17 | 26 | 0.45 | 27 | 883 | 0.4964 | 37 | 40082 | 0.4547 |
| 8 | 0 | 0 | 18 | 18 | 0.41 | 28 | 635 | 0.4218 | 38 | 39858 | 0.4623 |
| 9 | 3 | 0.83 | 19 | 62 | 0.53 | 29 | 1933 | 0.4410 | 39 | 75370 | 0.4712 |
| 10 | 1 | 0.30 | 20 | 34 | 0.45 | 30 | 1470 | 0.4619 | 40 | 54758 | 0.4598 |

of primitive polynomials of degree $r$ in $\mathbf{Z}_2[t]$ (where $\varphi$ is Euler's totient function) or the total number of polynomials of degree $r$ with coefficients in $\{0, -1, +1\}$. A heuristic argument suggests that the number $\kappa(r)$ of candidates should grow like $(3/2)^r$ and that $\nu(r)$ should grow like $(3/4)^r\lambda_2(r)$. The argument is as follows:

There are $2^{r-1}$ polynomials $\overline{Q}(t)$ of degree $r$ with coefficients in $\{0, 1\}$, satisfying $\overline{q}_0 = \overline{q}_r = 1$. Randomly select such a $\overline{Q}(t)$, and compute $\epsilon_0, \epsilon_1, \dots, \epsilon_r$ from

$$\sum_{\substack{j+k=2m\\ 0\le j<k\le r}} \overline{q}_j\overline{q}_k = \epsilon_m \mod 2.$$

Extend $\overline{Q}(t)$ to a polynomial $Q(t)$ with coefficients $q_m \in \{-1, 0, 1, 2\}$ such that $\overline{q}_m = q_m \bmod 2$ and (12) is satisfied for $0 \le m \le r$. The (unique) mapping is given by $q_m = \overline{q}_m + 2\epsilon_m \mod 4$. It is easy to see that $q_0 = q_r = 1$. If we *assume* that, for $1 \le m < r$, each $q_m$ has independent probability $1/4$ of assuming the "forbidden" value 2, then the probability that $Q(t)$ is a candidate is $(3/4)^{r-1}$. Thus,

$$\kappa(r) \simeq (3/2)^{r-1}.$$

The probability that a randomly chosen $\overline{Q}(t)$ with $\overline{q}_0 = \overline{q}_r = 1$ is primitive is just $\lambda_2(r)/2^{r-1}$. If there is the same probability that a randomly chosen candidate is primitive, then the number of primitive candidates should be $(3/4)^{r-1}\lambda_2(r)$, and $\nu(r)$ should be half this number.

The argument is not strictly correct. For example, it gives a positive probability that $q_1 = 0$, $q_2 = 1$, but this never occurs for $r > 2$. However, the argument does appear to predict the correct order of magnitude of $\kappa(r)$ and $\nu(r)$. In Table 2 we give

$$\overline{\nu}(r) = \frac{\nu(r)}{(3/4)^r\lambda_2(r)} \quad ;$$

the numerical evidence suggests that $\overline{\nu}(r)$ converges to a positive constant $\overline{\nu}(\infty)$ as $r \to \infty$. However, $\overline{\nu}(\infty)$ is less than the value $2/3$ predicted by the heuristic argument. Our best estimate (obtained from a separate computation which gives faster convergence) is

$$\overline{\nu}(\infty) = 0.45882 \pm 0.00002.$$

The computation of Table 2 took 166 hours on a VaxStation 3100. We outline the method used. It is easy to check if a candidate polynomial is exceptional [8]. A straightforward method of enumerating all candidate polynomials of degree $r$ is to associate a polynomial $Q(t)$ such that $q_0 = q_r = 1$ with an $(r-1)$-bit binary number $N = b_1 \cdots b_{r-1}$, where $b_j = q_j \bmod 2$. For each such $N$, compute $\epsilon_0, \ldots, \epsilon_r$ from (11). Now (12) defines $q_0, \ldots, q_r \bmod 4$. If there is an index $m$ such that $\epsilon_m = 1 \bmod 2$ but $q_m = 0 \bmod 2$, then (12) shows that $q_m = 2 \bmod 4$, contradicting condition E2. The straightforward enumeration has complexity $\Omega(2^r)$, but this can be reduced by two devices:

A. If (12) shows that $q_m = 2 \bmod 4$ for some $m < r/2$, we may use the fact that $\epsilon_m$ in (11) depends only on $q_0, \ldots, q_{2m}$ to skip over a block of $2^{r-2m-1}$ numbers $N$. By an argument similar to the heuristic argument for the order of magnitude of $\nu(r)$, with support from empirical evidence for $r \le 40$, we conjecture that this device reduces the complexity of the enumeration to

$$O(r^2 2^r (3/4)^{r/2}) = O(r^2 3^{r/2}).$$

B. Fix $s$, $0 \le s < r$. Since $\epsilon_{r-m}$ in (11) depends only on $q_{r-2m}, \ldots, q_r$, we can tabulate those low-order bits $b_{r-s} \cdots b_{r-1}$ which do not necessarily lead to condition E2 being violated for some $q_{r-m}$, $2m \le s$. In the enumeration we need only consider $N$ with low-order bits in the table. We conjecture that this reduces the complexity of the enumeration to

$$O(r^2 2^r (3/4)^{s/2}) = O(r^2 2^{r-s} 3^{s/2}),$$

provided care is taken to generate the table efficiently.

The two devices can be combined, but they are not independent. The complexity of the combination is conjectured to be

$$O(r^2 2^r (3/4)^{(6r+5s)/12}) = O(r^2 3^{r/2} (3/4)^{5s/12}),$$

where the exponent $5s/12$ (instead of $s/2$) reflects the lack of independence. In the computation of Table 2 we used $s \le 22$ because of memory constraints. The table size is $O(s 3^{s/2})$ bits, if the table is stored as a list to take advantage of sparsity.

*Note added in proof.* Examples of primitive trinomials with $r \le 132049$ were recently found by Heringa, Blöte and Compagner, Internat. J. Modern Phys. C **3** (1992), 561–564.


## Acknowledgments

We thank a referee for pointing out an error in the formulation of Lemma 2 given in [2], and for providing references to the classical literature. Richard Walker's assistance with $\mathcal{A}\mathcal{M}\mathcal{S}$-LaTeX was invaluable. The ANU Supercomputer Facility provided time on a Fujitsu VP 2200/10 for the discovery of the primitive trinomials mentioned at the end of §3.

## Bibliography

1. S. L. Anderson, *Random number generators on vector supercomputers and other advanced architectures,* SIAM Rev. **32** (1990), 221–251.
2. R. P. Brent, *On the periods of generalized Fibonacci recurrences,* Technical Report TR-CS-92-03, Computer Sciences Laboratory, Australian National University, Canberra, March 1992.
3. ———, *Uniform random number generators for supercomputers,* Proc. Fifth Australian Supercomputer Conference, Melbourne, Dec. 1992, pp. 95–104.
4. A. M. Ferrenberg, D. P. Landau, and Y. J. Wong, *Monte Carlo simulations: Hidden errors from "good" random number generators,* Phys. Rev. Lett. **69** (1992), 3382–3384.
5. S. W. Golomb, *Shift register sequences,* Holden-Day, San Francisco, 1967.
6. B. F. Green, J. E. K. Smith, and L. Klem, *Empirical tests of an additive random number generator,* J. Assoc. Comput. Mach. **6** (1959), 527–537.
7. F. James, *A review of pseudorandom number generators,* Comput. Phys. Comm. **60** (1990), 329–344.
8. D. E. Knuth, *The art of computer programming, Volume* 2: *Seminumerical algorithms* (2nd ed.), Addison-Wesley, Menlo Park, CA, 1981.
9. E. V. Krishnamurthy, *Error-free polynomial matrix computations,* Chapter 4, Springer-Verlag, New York, 1985.
10. H. T. Kung, *On computing reciprocals of power series,* Numer. Math. **22** (1974), 341–348.
11. Y. Kurita and M. Matsumoto, *Primitive t-nomials* $(t = 3, 5)$ *over* GF(2) *whose degree is a Mersenne exponent* $\leq 44497$, Math. Comp. **56** (1991), 817–821.
12. G. Marsaglia, *A current view of random number generators,* Computer Science and Statistics: The Interface (edited by L. Billard), Elsevier Science Publishers B. V. (North-Holland), 1985, 3–10.
13. G. Marsaglia and L. H. Tsay, *Matrices and the structure of random number sequences,* Linear Algebra Appl. **67** (1985), 147–156.
14. J. F. Reiser, *Analysis of additive random number generators,* Ph. D. thesis, Department of Computer Science, Stanford University, Stanford, CA, 1977. Also Technical Report STAN-CS-77-601.
15. E. R. Rodemich and H. Rumsey, Jr., *Primitive trinomials of high degree,* Math. Comp. **22** (1968), 863–865.
16. I. Schur, *Ganzzahlige Potenzreihen und linear rekurrente Zahlenfolgen,* Issai Schur Gesammelte Abhandlungen, Band 3, Springer-Verlag, Berlin, 1973, pp. 400–421.
17. W. Stahnke, *Primitive binary polynomials,* Math. Comp. **27** (1973), 977–980.
18. R. C. Tausworthe, *Random numbers generated by linear recurrence modulo two,* Math. Comp. **19** (1965), 201–209.
19. B. L. van der Waerden, *Algebra,* Vol. 1, Chapter 7 (English transl. by Fred Blum, 5th ed.), Ungar, New York, 1953.
20. M. Ward, *The arithmetical theory of linear recurring series,* Trans. Amer. Math. Soc. **35** (1933), 600–628.
21. E. J. Watson, *Primitive polynomials* (mod 2), Math. Comp. **16** (1962), 368–369.
22. H. Zassenhaus, *On Hensel factorization,* J. Number Theory **1** (1969), 291–311.
23. N. Zierler and J. Brillhart, *On primitive trinomials* (mod 2), Inform. and Control **13** (1968), 541–554. Also part II, *ibid.* **14** (1969), 566–569.
24. N. Zierler, *Primitive trinomials whose degree is a Mersenne exponent,* Inform. and Control **15** (1969), 67–69.
25. ———, *On* $x^n + x + 1$ *over* GF(2), Inform. and Control **16** (1970), 502–505.

Computer Sciences Laboratory, Australian National University, Canberra, ACT 0200, Australia

*E-mail address*: `rpb@cslab.anu.edu.au`