On the Periods of Generalized Fibonacci Recurrences[1]

Richard P. Brent
Computer Sciences Laboratory
Australian National University
Canberra, ACT 0200
rpb@cslab.anu.edu.au

TR-CS-92-03
March 1992, revised March 1993

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 pseudo-random number generation, i.e. for 3-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

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

are of interest because they are often used to generate pseudo-random numbers [1, 5, 6, 11, 13, 17]. 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 3-term recurrences of the special form (1). Thus, we consider a general linear recurrence

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

defined by a polynomial

$$Q(t) = q_0 + q_1 t + \ldots + q_r t^r \tag{3}$$

of degree $r > 0$. We assume throughout that q_0 and q_r are odd. q_0 odd implies that 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 [19].

[1] *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, pseudo-random numbers.

To appear in *Mathematics of Computation*, 1994 (accepted 13 March 1993).

 rpb133tr typeset using LaTeX

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

$$A = B \qquad \bmod (m, Q).$$

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

$$t^n = \sum_{j=0}^{r-1} a_{n,j} t^j \qquad \bmod (2^w, Q(t)) \tag{4}$$

then

$$x_n = \sum_{j=0}^{r-1} a_{n,j} x_j \qquad \bmod 2^w. \tag{5}$$

Also, the generating function

$$G(t) = \sum_{n \geq 0} x_n t^n \tag{6}$$

is given by

$$G(t) = \frac{P(t)}{\tilde{Q}(t)} \qquad \bmod 2^w, \tag{7}$$

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

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

is the *reverse* of Q. In the literature, $\tilde{Q}(t)$ is sometimes called the *characteristic polynomial* [4] or the *associated polynomial* [19] of the sequence. The use of generating functions is convenient and has been adopted by many earlier authors (e.g. Schur [15]). Ward [19] does not explicitly use generating functions, but his polynomial U is the same as our $\tilde{Q}$, and many of his results could be obtained via generating functions.

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

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

In the literature, ρ_w is sometimes called the *principal period* [19] of the linear recurrence, sometimes simply the *period* [4]. For brevity we define $\lambda = \rho_1$.

An irreducible polynomial in $Z_2[t]$ is a factor of $t^{2^r} - t$ (see e.g. [18]), so $\lambda | 2^r - 1$. We say that $Q(t)$ is *primitive* (mod 2) if $\lambda = 2^r - 1$. Note that primitivity is a stronger condition than irreducibility[2], i.e. $Q(t)$ primitive implies that $Q(t)$ is irreducible, but the converse is not generally true unless $2^r - 1$ is prime[3]. Tables of irreducible and primitive trinomials are available [4, 10, 14, 16, 20, 22, 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 $\tilde{Q}(t)$ is irreducible (or primitive) of degree r iff 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

$$x_{n+p} = x_n \tag{8}$$

[2]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 $Q(t)$ mod 2 is irreducible (resp. primitive) in $Z_2[t]$.

[3]For example, the polynomial $1 + t + t^2 + t^4 + t^6$ is irreducible, but not primitive, since it has $\lambda = 21 < 2^6 - 1$.

for all sufficiently large n. In fact, because of the reversibility of the sequence, (8) should hold for all $n \geq 0$. The period is sometimes called the *characteristic number* of the sequence [19]. In general the period depends on the initial values $x_0, \ldots, x_{r-1}$, but under our assumptions the period depends only on $Q(t)$, in fact $p_w = \rho_w$ (see Lemma 2).

It is known [7, 12, 19] that

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

with equality holding for all $w > 0$ iff it holds for $w = 3$. The main aim of this paper is to give a simple necessary and sufficient condition for

$$p_w = 2^{w-1}\lambda. \tag{9}$$

The result is stated in Theorem 2 in terms of a simple condition which we call "Condition S" (see Section 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 pseudo-random number generation[4], 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

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

The basic results on linear recurrences modulo m were obtained many years ago – see for example Ward [19]. However, our main results (Theorems 2 and 3) and the statement of "Condition S" (Section 2) appear to be new.

2 A Condition for Maximal Period

The following Lemma is a special case of Hensel's Lemma [7, 8, 21] and may be proved using an application of Newton's method for reciprocals [9].

Lemma 1 *Suppose that* $P(t) \bmod 2$ *is invertible in* $Z_2[t]/Q(t)$. *Then, for all* $w \geq 1$, $P(t) \bmod 2^w$ *is invertible in* $Z_{2^w}[t]/Q(t)$.

We now give a sufficient condition for the periods p_w and ρ_w to be the same.

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

Proof

For brevity we write $p = p_w$ and $\rho = \rho_w$. From (6),

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

where $R(t)$ has degree less than p. Thus, from (7),

$$R(t)\tilde{Q}(t) = (1 - t^p)P(t) \qquad \bmod 2^w. \tag{10}$$

Now $P(t) \bmod 2$ has degree less than r, but is not identically zero. Since $\tilde{Q}(t) \bmod 2$ is irreducible of degree r, application of the extended Euclidean algorithm [7] to $P(t) \bmod 2$ and $\tilde{Q}(t) \bmod 2$

[4] A word of caution is appropriate. Even when the period p_w satisfies (9), it is not desirable to use a full cycle of p_w numbers in applications requiring independent pseudo-random 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.

constructs the inverse of $P(t) \bmod 2$ in $Z_2[t]/\tilde{Q}(t)$. Thus, Lemma 1 shows that $P(t) \bmod 2^w$ is invertible in $Z_{2^w}[t]/\tilde{Q}(t)$. It follows from (10) that

$$t^p = 1 \qquad \bmod (2^w, \tilde{Q}(t)),$$

and $\rho | p$. However, from (4) and (5), $p | \rho$. 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

$$\rho_w = \begin{cases} 3, & \text{if } w = 1; \\ 6, & \text{if } w > 1. \end{cases} \tag{11}$$

It is easy to verify that (11) gives the period p_w of the corresponding recurrence

$$x_n = x_{n-1} - x_{n-2} \qquad \bmod 2^w$$

provided x_0 and x_1 are not both even.

The assumption of irreducibility in Lemma 2 is significant. For example[5], 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 $\tilde{Q}(t) = 1 - t^2$.

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[6]. This is much faster than the method suggested by Knuth [7] or Marsaglia and Tsay [12], which involves forming high powers of $r \times r$ matrices (mod 8).

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

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

Lemma 3 gives an equivalent condition[7] which is more convenient for computational purposes. The proof is straightforward, so is omitted.

Lemma 3 *A polynomial $Q(t)$ of degree r satisfies Condition S iff*

$$\sum_{\substack{j+k=2m \\ 0 \le j < k \le r}} q_j q_k = \epsilon_m \qquad \bmod 2 \tag{12}$$

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

$$\epsilon_m = \frac{q_m(q_m - q_r)}{2}. \tag{13}$$

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 some results regarding arithmetic in the rings $Z_{2^w}[t]/Q(t)$.

[5] We thank a referee for suggesting this example.
[6] $O(r \log r)$ operations if the FFT is used to compute the convolutions in (12).
[7] For another equivalent condition, see (17) and (25).

Lemma 4 *Let $X(t)$ and $Y(t)$ be polynomials over Z. Then, for $w \ge 1$,*

$$X = Y \bmod (2^w, Q) \Rightarrow X^2 = Y^2 \bmod (2^{w+1}, Q). \tag{14}$$

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

$$X^2 = Y^2 \bmod (2, Q) \Leftrightarrow X^2 = Y^2 \bmod (4, Q) \tag{15}$$

and

$$X^2 = Y^2 \bmod (8, Q) \Leftrightarrow X = \pm Y \bmod (4, Q). \tag{16}$$

Proof

If $X = Y \bmod (2^w, Q)$ then $X = Y + 2^w R \bmod Q$ for some polynomial $R(t)$ in $Z[t]$. Thus $X^2 = Y^2 + 2^{w+1}R(Y + 2^{w-1}R) \bmod Q$, and (14) follows.

Now suppose that $Q(t)$ is irreducible. If $X^2 = Y^2 \bmod (2, Q)$ then $(X - Y)^2 = 0 \bmod (2, Q)$. Since Q is irreducible, it follows that $X = Y \bmod (2, Q)$. Thus, from (14), $X^2 = Y^2 \bmod (4, Q)$, and (15) follows.

Finally, if Q is irreducible and $X^2 = Y^2 \bmod (8, Q)$ then, as in the proof of (15), we obtain $X = Y \bmod (2, Q)$, so $X = Y + 2R \bmod Q$, where $R(t)$ is some polynomial in $Z[t]$. 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 (14). This establishes (16). □

The following Theorem is the key to the proof of Theorem 2. There is no obvious generalization to odd moduli.

Theorem 1 *Let $Q(t) \bmod 2$ be irreducible in $Z_2[t]$. Then*

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

iff $Q(t)$ satisfies Condition S, and

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

iff $Q(-t)$ satisfies Condition S.

Proof

Let

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

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

$$Q(t) = V(t^2) + tW(t^2). \tag{17}$$

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

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

Because $X(t^2) = X(t)^2 \bmod 2$ for any polynomial $X(t)$ in $Z[t]$, (18) may be written as

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

λ, being a divisor of $2^r - 1$, is odd, so $t^{\lambda+1}$ is a square. Thus, from (15),

$$V(t)^2 = t^{\lambda+1} W(t)^2 \qquad \bmod\ (4, Q(t)). \tag{20}$$

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

$$V(-t)^2 = t^{\lambda+1} W(-t)^2 \qquad \bmod\ (4, Q(t)). \tag{21}$$

To prove the first half of the Theorem, suppose that

$$t^\lambda = -1 \qquad \bmod\ (4, Q(t)). \tag{22}$$

Thus, from (20),

$$V(t)^2 + tW(t)^2 = 0 \qquad \bmod\ (4, Q(t)). \tag{23}$$

It follows that

$$V(t)^2 + tW(t)^2 - q_r Q(t) = 0 \qquad \bmod\ (4, Q). \tag{24}$$

However, the left hand side of (24) is a polynomial of degree less than r. Hence

$$V(t)^2 + tW(t)^2 - q_r Q(t) = 0 \qquad \bmod\ 4. \tag{25}$$

Replace t by t^2 in the identity (25). From (17), 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, (23) holds. Thus, from (20),

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

Now $W(t)$ has degree less than r, and $W(t) \neq 0 \bmod 2$ because otherwise, from (17), $Q(t) = V(t)^2 \bmod 2$ would contradict the irreducibility of $Q(t)$. Thus, $W(t) \bmod 2$ is invertible in $Z_2[t]/Q(t)$. From Lemma 1, $W(t) \bmod 4$ is invertible in $Z_4[t]/Q(t)$, and we obtain

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

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

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

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

$$t^\lambda = 1 \qquad \bmod\ (4, Q(t)). \tag{26}$$

From (21),

$$V(-t)^2 = tW(-t)^2 \qquad \bmod\ (4, Q(t)). \tag{27}$$

Thus, instead of (25) we obtain

$$V(-t)^2 - tW(-t)^2 - (-1)^r q_r Q(t) = 0 \qquad \bmod\ 4. \tag{28}$$

Replace t by $-t^2$ in the identity (28). 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 $Q(t)$, (26) holds. □

We are now ready to state Theorem 2, which relates the period of the sequence (x_n) to Condition S. It is interesting to note that, in view of Theorem 1, Theorem 2 is implicit in the discussion on page 628 of Ward [19]. 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 $x_0, \ldots, x_{r-1}$ odd. Then the sequence (x_n) has period*

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

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

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

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

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

for all $w \ge 1$ iff 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,

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

Using (14), it follows by induction on w that

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

for all $w \ge 2$. 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

$$t^{2\lambda} \ne 1 \qquad \bmod\ (8, Q(t))$$

and, from (16),

$$t^\lambda \ne \pm 1 \qquad \bmod\ (4, Q(t)). \tag{29}$$

From Theorem 1, neither $Q(t)$ nor $Q(-t)$ can satisfy Condition S, or we would obtain a contradiction to (29).

Conversely, if neither $Q(t)$ or $Q(-t)$ satisfies Condition S, then we show by induction on w that

$$t^{2^{w-1}\lambda} = 1 + 2^w R_w \qquad \bmod\ Q(t), \tag{30}$$

where

$$R_w \ne 0 \qquad \bmod\ (2, Q(t)), \tag{31}$$

for all $w \ge 1$. Certainly

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

but, from Theorem 1,

$$t^\lambda \ne 1 \qquad \bmod\ (4, Q(t)),$$

so (30) and (31) hold for $w = 1$. Defining

$$R_w = R_{w-1}(1 + 2^{w-2}R_{w-1}) \tag{32}$$

for $w \ge 2$, we see that (30) holds for all $w \ge 1$. It remains to prove (31) for $w > 1$. For $w = 2$, (31) follows from Theorem 1 and (16), because $t^\lambda \ne \pm 1 \bmod (4, Q(t))$ implies $t^{2\lambda} \ne 1 \bmod (8, Q(t))$. For $w > 2$, (31) follows by induction from (32), since 2^{w-2} is even. It follows that

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

for all $w \ge 1$. □

3 Primitive Trinomials

In this section we consider a case of interest because of its applications to pseudo-random 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 Section 2 shows.

Theorem 3 *Let $Q(t)$ be a primitive trinomial of degree $r > 2$. Then the sequence (x_n) defined by (2) (with at least one of $x_0, \ldots, x_{r-1}$ 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, $q_0 = q_s = q_r = 1 \bmod 2$. If s is even, say $s = 2m$, then

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

so $\epsilon_m \neq 0$, and (13) 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

$$Q(t) = t^{2s} + t^s + 1 \qquad \bmod 2.$$

In this case $t^{3s} = 1 \bmod (2, Q(t))$. Now $r = 2s > 2$, so $3s < 2^r - 1$, and $Q(t)$ can not 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 $x_0, \ldots, x_{r-1}$ 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 [10]. Such primitive trinomials provide the basis for fast random number generators with extremely long periods and good statistical properties [3].

4 Exceptional Polynomials

We say that a polynomial $Q(t)$ of degree $r > 1$ is *exceptional* if conditions 1–3 hold and is a *candidate* if conditions 2–3 hold –

1. $Q(t)$ mod 2 is primitive.

2. $Q(t)$ has coefficients $q_j \in \{0, -1, +1\}$, and $q_0 = q_r = 1$.

3. $Q(t)$ satisfies Condition S.

By Theorem 2, if $Q(t)$ is exceptional then $Q(t)$ and $Q(-t)$ define simple linear recurrences (mod 2^w) which have less than the maximal period for $w > 2$.

Only the coefficients of $Q(t)$ mod 4 are relevant to Condition S. If condition 2 is relaxed to allow coefficients equal to 2 then, by Lemma 3, there is one such $Q(t)$ corresponding to each primitive polynomial in $Z_2[t]$. With condition 2 as stated the number of these $Q(t)$ is considerably reduced.

It is interesting to consider strengthening condition 2 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 $(-1)^j q_j \geq 0$ for $0 \leq j < r$. The only example for $2 < r \leq 44$ 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

$$x_{n+21} = x_n + x_{n+1} + x_{n+2} + x_{n+5} + x_{n+6} + x_{n+8} + x_{n+9} + x_{n+10} + x_{n+12} + x_{n+13} + x_{n+16} + x_{n+18}$$

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

In Table 1 we list the exceptional polynomials $Q(t)$ of degree $r \leq 14$. If $Q(t)$ is exceptional then so is $\tilde{Q}(t)$. Thus, we only list one of these in Table 1.

The number $\nu(r)$ of exceptional $Q(t)$ (counting only one of $Q(t), \tilde{Q}(t)$) 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 [4]

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

of primitive polynomials of degree r in $Z_2[t]$ (where φ is Euler's totient-function) or the total number of polynomials of degree r with coefficients in $\{0, -1, +1\}$. Heuristic arguments suggest 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 arguments are as follows –

> There are 2^{r-1} polynomials $\bar{Q}(t)$ of degree r with coefficients in $\{0, 1\}$, satisfying $\bar{q}_0 = \bar{q}_r = 1$. Randomly select such a $\bar{Q}(t)$, and compute $\epsilon_0, \epsilon_1, \ldots, \epsilon_r$ from
>
> $$\sum_{\substack{j+k=2m \\ 0 \leq j < k \leq r}} \bar{q}_j \bar{q}_k = \epsilon_m \qquad \bmod 2$$
>
> Extend $\bar{Q}(t)$ to a polynomial $Q(t)$ with coefficients $q_m \in \{-1, 0, 1, 2\}$ such that
>
> $\bar{q}_m = q_m$ mod 2 and (13) is satisfied for $0 \leq m \leq r$. The (unique) mapping is given by
>
> $q_m = \bar{q}_m + 2\epsilon_m$ mod 4. It is easy to see that $q_0 = q_r = 1$. If we *assume* that each q_m for $1 \leq m < r$ 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 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 $\kappa(r)$.

The probability that a randomly chosen $\bar{Q}(t)$ with $\bar{q}_0 = \bar{q}_r = 1$ 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.

In Table 2 we give

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

the numerical evidence suggests that $\bar{\nu}(r)$ converges to a positive constant $\bar{\nu}(\infty)$ as $r \to \infty$. However, $\bar{\nu}(\infty)$ 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

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

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 [7]. 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 (12). Now (13) 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 (13) shows that $q_m = 2 \bmod 4$, contradicting condition 2. The straightforward enumeration has complexity $\Omega(2^r)$, but this can be reduced by two devices –

1. If (13) shows that $q_m = 2 \bmod 4$ for some $m < r/2$, we may use the fact that ϵ_m in (12) 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

$$O\left(r^2 2^r \left(\frac{3}{4}\right)^{r/2}\right) = O(r^2 3^{r/2}).$$

2. Fix s, $0 \le s < r$. Since ϵ_{r-m} in (12) 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 2 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

$$O\left(r^2 2^r \left(\frac{3}{4}\right)^{s/2}\right) = O(r^2 2^{r-s} 3^{s/2})$$

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

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

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 $O(s3^{s/2})$ bits if the table is stored as a list to take advantage of sparsity.

Acknowledgements

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. The ANU Supercomputer Facility provided time on a Fujitsu VP 2200/10 for the discovery of the primitive trinomials mentioned at the end of Section 3.

References

[1] S. L. Anderson, "Random number generators on vector supercomputers and other advanced architectures", *SIAM Review* 32 (1990), 221-251.

[2] R. P. Brent, *On the Periods of Generalized Fibonacci Recurrences*, Technical Report TR-CS-92-03, Computer Sciences Laboratory, ANU, March 1992.

[3] R. P. Brent, "Uniform random number generators for supercomputers", *Proc. Fifth Australian Supercomputer Conference*, Melbourne, Dec. 1992, 95-104.

[4] S. W. Golomb, *Shift Register Sequences*, Holden-Day, San Francisco, 1967. MR 39#3906.

[5] B. F. Green, J. E. K. Smith and L. Klem, "Empirical tests of an additive random number generator", *J. ACM* 6 (1959), 527-537.

[6] F. James, "A review of pseudorandom number generators", *Computer Physics Communications*, 60 (1990), 329-344.

[7] D. E. Knuth, *The Art of Computer Programming, Volume 2: Seminumerical Algorithms* (second edition), Addison-Wesley, Menlo Park, 1981.

[8] E. V. Krishnamurthy, *Error-Free Polynomial Matrix Computations*, Springer-Verlag, New York, 1985, Ch. 4.

[9] H. T. Kung, "On computing reciprocals of power series", *Numer. Math.* 22 (1974), 341-348.

[10] Y. Kurita and M. Matsumoto, "Primitive t-nomials ($t = 3, 5$) over $GF(2)$ whose degree is a Mersenne exponent ≤ 44497", *Mathematics of Computation* 56 (1991), 817-821.

[11] 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.

[12] G. Marsaglia and L. H. Tsay, "Matrices and the structure of random number sequences", *Linear Algebra and Applications*, 67 (1985), 147-156.

[13] J. F. Reiser, *Analysis of Additive Random Number Generators*, Ph. D. thesis, Department of Computer Science, Stanford University, 1977. Also Technical Report STAN-CS-77-601.

[14] E. R. Rodemich and H. Rumsey, Jr., "Primitive trinomials of high degree", *Mathematics of Computation* 22 (1968), 863-865.

[15] I. Schur, "Ganzzahlige Potenzreihen und linear rekurrente Zahlenfolgen", *Issai Schur Gesammelte Abhandlungen, Band 3*, Springer-Verlag, Berlin, 1973, 400-421.

[16] W. Stahnke, "Primitive binary polynomials", *Mathematics of Computation* 27 (1973), 977-980.

[17] R. C. Tausworthe, "Random numbers generated by linear recurrence modulo two", *Mathematics of Computation*, 19 (1965), 201-209.

[18] B. L. van der Waerden, *Modern Algebra*, Vol. 1 (English translation), Frederick Ungar, New York, 1949, Ch. 7.

[19] M. Ward, "The arithmetical theory of linear recurring series", *Trans. Amer. Math. Soc.* 35 (1933), 600-628.

[20] E. J. Watson, "Primitive polynomials (mod 2)", *Mathematics of Computation* 16 (1962), 368-369. MR 26#5764.

[21] H. Zassenhaus, "On Hensel factorization", *Journal of Number Theory* 1 (1969), 291-311.

[22] N. Zierler and J. Brillhart, "On primitive trinomials (mod 2)", *Information and Control*, 13 (1968), 541-554. MR 38#5750.

[23] N. Zierler and J. Brillhart, "On primitive trinomials (mod 2), II", *Information and Control*, 14 (1969), 566-569. MR 39#5521.

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

[25] N. Zierler, "On $x^n + x + 1$ over $GF(2)$", *Information and Control*, 16 (1970), 502-505.

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

Table 1: Exceptional Polynomials of degree $r \leq 14$

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

Table 2: Number of Exceptional Polynomials