FINITE FIELDS AND THEIR APPLICATIONS **3,** 70–83 (1997)
ARTICLE NO. FF960164

Stability of Two-Term Recurrence Sequences with Even Parameter

WALTER CARLIP AND ELIOT JACOBSON

Department of Mathematics, Ohio University, Athens, Ohio 45701
E-mail: carlip@oucsace.cs.ohiou.edu; jacobson@mars.math.ohiou.edu

Communicated by Harald Niederreiter

Received August 4, 1995; revised April 29, 1996

The authors characterize the stability modulo two of two-term recurrence sequences with one defining parameter even and determine their periods modulo sufficiently high powers of two. © 1997 Academic Press

1. INTRODUCTION

Let a and b be fixed integers and let $\{u_i \mid i \geq 0\}$ be the two-term recurrence sequence defined by $u_0 = 0$, $u_1 = 1$, and

$$u_i = au_{i-1} + bu_{i-2}. \tag{1.1}$$

For any positive integer m, consider the corresponding sequence $\{\overline{u}_i\}$, where $\overline{u}_i \in \mathbf{Z}/m\mathbf{Z}$ is obtained by reduction modulo m. If b and m are relatively prime, then $\{\overline{u}_i\}$ is purely periodic and, for each integer d, we denote the number of occurrences of the residue d (mod m) in one (shortest) period by $\nu(m, d)$. The function $\nu(m, d)$ is called the *frequency distribution function* of the recurrence $\{u_i\}$ modulo m. A number of interesting open problems concern these periodic sequences and their distribution functions, among them the determination of the periods as a function of a, b, and m (see, e.g., [4, 10, 11]) and the description of the frequency distribution functions (see, e.g., [5, 7, 9]).

1071-5797/97 $25.00

Corresponding to a fixed recurrence sequence $\{u_i\}$ and modulus m, we define

$$\Omega(m) = \{\nu(m, d) \mid d \in \mathbf{Z}\}$$

and say that the sequence is *stable* modulo a prime p if there is a positive integer N such that

$$\Omega(p^k) = \Omega(p^N) \qquad \text{for all } k \geq N.$$

In [1–3] we examined the stability modulo two of sequences for which the parameter a is odd and showed how stability leads to a precise description of the frequency distribution functions of such sequences. In this paper we apply techniques similar to those used in [1] to characterize the stability of sequences whose parameter a is even.

2. Preliminary Results

For the duration of this section fix a two-term recurrence sequence $\{u_i\}$, as defined in (1.1), with a even and b odd. Define parameters r, s, and t as follows:

$$2^{t+1} \parallel a, \qquad 2^{s+1} \parallel (b-1), \qquad \text{and} \qquad 2^{r+1} \parallel (b+1). \tag{2.1}$$

Note that r, s, and t are not always defined: t is not defined when $a = 0$, and r and s are not defined when $b = 1$ and $b = -1$, respectively. Except where explicitly stated, we will assume that r, s, and t are defined. Our main results on stability depend on the relationships between r, s, and t.

We begin by stating without proof several well-known properties of the two-term recurrence sequence $\{u_i\}$ (see, e.g., [2, 3, 8]).

Fact 1. The following formulas hold for all $m \geq 1$ and $n \geq 0$:

(a) $u_{m+n} = bu_{m-1}u_n + u_m u_{n+1}$,

(b) $u_{2n+1} = b(u_n)^2 + (u_{n+1})^2$, and

(c) $u_{2n} = 2u_n u_{n+1} - a(u_n)^2$.

Fact 2. If $n \geq 0$ and $m \geq 0$, then u_n divides u_{nm}.

Fact 3. The integer u_n is even if and only if n is even.

Lemma 2.1. *If $m > 0$, then $2^{t+m} \parallel u_{2^m}$.*

Proof. Proceed by induction on m.

If $m = 1$, then $u_{2^m} = u_2 = a$ and the lemma follows from the definition of t.

Now suppose that $m \geq 1$ and that $2^{t+m} \parallel u_{2^m}$. By Fact 1, $u_{2^{m+1}} = 2u_{2^m}u_{2^m+1} - a(u_{2^m})^2$. By the induction hypothesis and Fact 3, $2^{t+m+1} \parallel 2u_{2^m}u_{2^m+1}$. On the other hand, the induction hypothesis also implies that $2^{3t+2m+1} \parallel a(u_{2^m})^2$. Since $3t + 2m + 1 > t + m + 1$, it follows that $2^{t+m+1} \parallel u_{2^{m+1}}$, as desired. ■

In the next two lemmas we gather together several useful, related congruences.

LEMMA 2.2. *Suppose that $\{u_i\}$ is the two-term recurrence sequence defined above.*

(a) *If $k > 0$, then $u_{2^k+1} \equiv 1 \pmod{2^k}$.*
(b) *If $k > t$ and $0 < t < s$, then $u_{2^{k-1}+1} \equiv 1 \pmod{2^{k+1}}$.*
(c) *If $k > t + 1$ and $0 < t < r$, then $u_{2^{k-1}+1} \equiv 1 \pmod{2^{k+1}}$.*

Proof. Each part follows from Fact 1 and Lemma 2.1 by induction on k. We prove (c) and leave the similar proofs of (a) and (b) to the reader.

Suppose that $k = t + 2$. Then $u_{2^{k-1}+1} = u_5 = b(u_2)^2 + (u_3)^2$. Since $2^{2(t+1)} \parallel a^2$, it follows that $a^2 \equiv 0 \pmod{2^{k+1}}$. Therefore, since $u_2 = a$ and $u_3 = a^2 + b$, it follows that $u_5 \equiv b^2 \pmod{2^{k+1}}$. However, $b^2 - 1 = (b - 1)(b + 1)$ and $2^{r+1} \parallel (b + 1)$, so $2^{r+2} \parallel b^2 - 1$. Since $r + 2 \geq t + 3 = k + 1$, it follows that $b^2 - 1 \equiv 0 \pmod{2^{k+1}}$. Hence $u_{2^{k-1}+1} \equiv 1 \pmod{2^{k+1}}$, as desired.

Suppose that $k > t + 2$ and assume that $u_{2^{k-t-1}+1} \equiv 1 \pmod{2^k}$. Then, by Lemma 2.1, $2^{k-1} \parallel u_{2^{k-t-1}}$ and, since $k \geq 3$, it follows that $(u_{2^{k-t-1}})^2 \equiv 0 \pmod{2^{k+1}}$. Moreover, the induction hypothesis implies that $(u_{2^{k-t-1}+1})^2 \equiv 1 \pmod{2^{k+1}}$. Now, Fact 1 yields

$$u_{2^{k-t}+1} = b(u_{2^{k-t-1}})^2 + (u_{2^{k-t-1}+1})^2 \equiv 1 \pmod{2^{k+1}}. \quad ■$$

LEMMA 2.3. *Suppose that $\{u_i\}$ is the two-term recurrence sequence defined above.*

(a) *If $k > 1$ and $t = 0$, then $u_{2^k+1} \equiv 1 + 2^k \pmod{2^{k+1}}$.*
(b) *If $k > s$ and $0 < s < 2t$, then $u_{2^{k-s}+1} \equiv 1 + 2^k \pmod{2^{k+1}}$.*
(c) *If $k > 2t + 1$ and $2t < s$, then $u_{2^{k-2t}+1} \equiv 1 + 2^k \pmod{2^{k+1}}$.*
(d) *If $k > r + 1$ and $0 < r < 2t$, then $u_{2^{k-r}+1} \equiv 1 + 2^k \pmod{2^{k+1}}$.*
(e) *If $k > 2t + 1$ and $2t < r$, then $u_{2^{k-2t}+1} \equiv 1 + 2^k \pmod{2^{k+1}}$.*

Proof. As in the previous lemma, the proofs of each part proceed by induction on k and follow from Fact 1 and Lemma 2.1. We illustrate by proving (e) and leave the remaining parts to the reader.

Suppose that $k = 2t + 2$. Then $u_{2^{k-2t}+1} = u_{2^2+1} = u_5$. Note that $u_2 = a$, and therefore $2^k \parallel b(u_2)^2$. Moreover, $u_3 + 1 = (a^2 + b) + 1 = a^2 + (b + 1)$. Since $r > 2t$, either $r = 2t + 1$ or $r > 2t + 1$. In both cases $2^k \mid u_3 + 1$ and $(u_3)^2 - 1 \equiv 0 \pmod{2^{k+1}}$. Thus, by Fact 1, $u_5 - 1 = b(u_2)^2 + (u_3)^2 - 1 \equiv 2^k \pmod{2^{k+1}}$.

Now suppose that $k > 2t + 2$ and assume that $u_{2^{k-2t-1}+1} \equiv 1 + 2^{k-1} \pmod{2^k}$. Then, by Lemma 2.1, $2^{t+k-2t-1} \parallel u_{2^{k-2t-1}}$ and $2(t + k - 2t - 1) = (k + 1) + (k - 2t - 3) \geq k + 1$. Thus, $b(u_{2^{k-2t-1}})^2 \equiv 0 \pmod{2^{k+1}}$. Moreover, since $k \geq 3$, the induction hypothesis implies that $(u_{2^{k-2t-1}+1})^2 \equiv 1 + 2^k \pmod{2^{k+1}}$. Finally, Fact 1 yields

$$u_{2^{k-2}+1} = b(u_{2^{k-2t-1}})^2 + (u_{2^{k-2t-1}+1})^2 \equiv 1 + 2^k \pmod{2^{k+1}}. \quad \blacksquare$$

PROPOSITION 2.4. *Suppose that $\{u_i\}$ is the two-term recurrence sequence defined above.*

(a) *If $k > 1$ and $t = 0$, then $u_{n+2^k} \equiv u_n + 2^k \pmod{2^{k+1}}$.*

(b) *If $k > t$ and n is even, then $u_{n+2^{k-t}} \equiv u_n + 2^k \pmod{2^{k+1}}$.*

(c) *If $k > s$, $0 < s < 2t$, and n is odd, then $u_{n+2^{k-s}} \equiv u_n + 2^k \pmod{2^{k+1}}$.*

(d) *If $k > 2t + 1$, $0 < 2t < s$, and n is odd, then $u_{n+2^{k-2t}} \equiv u_n + 2^k \pmod{2^{k+1}}$.*

(e) *If $k > r + 1$, $0 < r < 2t$, and n is odd, then $u_{n+2^{k-r}} \equiv u_n + 2^k \pmod{2^{k+1}}$.*

(f) *If $k > 2t + 1$, $0 < 2t < r$, and n is odd, then $u_{n+2^{k-2t}} \equiv u_n + 2^k \pmod{2^{k+1}}$.*

Proof. (a) By Fact 1,

$$u_{n+2^k} = bu_{n-1}u_{2^k} + u_n u_{2^k+1}. \tag{2.2}$$

Suppose that n is odd. Then Fact 3 implies that u_{n-1} is even and u_n is odd. Hence, by Lemma 2.1, $bu_{n-1}u_{2^k} \equiv 0 \pmod{2^{k+1}}$. Then Lemma 2.3(a) and (2.2) imply that $u_{n+2^k} \equiv u_n + 2^k \pmod{2^{k+1}}$.

Now suppose that n is even. Then Fact 3 implies that u_n is even and u_{n-1} is odd. Hence, by Lemma 2.1, $bu_{n-1}u_{2^k} \equiv 2^k \pmod{2^{k+1}}$. On the other hand, $u_n(1 + 2^k) \equiv u_n \pmod{2^{k+1}}$. Thus, Lemma 2.3(a) and (2.2) again imply that $u_{n+2^k} \equiv u_n + 2^k \pmod{2^{k+1}}$.

(b) Since n is even, Fact 3 implies that u_{n-1} is odd. By Lemma 2.1, $2^{t+k-t} \parallel u_{2^{k-t}}$, and therefore $u_{2^{k-t}} \equiv 2^k \pmod{2^{k+1}}$. On the other hand, Fact 2 implies that $u_2 \mid u_n$, and hence $2^{t+1} \mid u_n$. Moreover, by Lemma 2.2(a) with $k - t$ in place of k, $u_{2^{k-t}+1} \equiv 1 \pmod{2^{k-t}}$, and hence $u_n u_{2^{k-t}+1} \equiv u_n \pmod{2^{k+1}}$. Consequently, Fact 1 yields

$$u_{n+2^{k-t}} = bu_{n-1}u_{2^{k-t}} + u_n u_{2^{k-t}+1} \equiv u_n + 2^k \pmod{2^{k+1}}.$$

(c) Since n is odd, Fact 3 implies that u_{n-1} is even, and therefore Fact 2 implies that $u_2 \mid u_{n-1}$. It follows that $2^{t+1} \mid u_{n-1}$. By Lemma 2.1, $2^{t+k-s} \parallel u_{2^{k-s}}$, and consequently $2^{2t+k-s+1} \mid bu_{n-1}u_{2^{k-s}}$. Since $2t - s > 0$, it follows that $bu_{n-1}u_{2^{k-s}} \equiv 0 \pmod{2^{k+1}}$. Finally, by Fact 1 and Lemma 2.3(b),

$$u_{n+2^{k-s}} = bu_{n-1}u_{2^{k-s}} + u_n u_{2^{k-s}+1} \equiv u_n + 2^k \pmod{2^{k+1}}.$$

(d), (e), (f) Imitate the proof of (c) using, respectively, Lemmas 2.3(c), 2.3(d), and 2.3(e) in place of Lemma 2.3(b). ∎

3. Periods

If $\{u_i\}$ is a two-term recurrence sequence, as defined in (1.1), and b is relatively prime to m, then the reduced sequence modulo m is purely periodic. The determination of the periods of reduced two-term recurrence sequences is an interesting open problem—even for the Fibonacci sequence itself (see, e.g., [10]).

If a is even and b is odd, the sequence $\{u_i\}$ is purely periodic modulo 2^k for any positive integer k. We will denote the length of a (smallest) period by λ_k. In this section we will completely determine the periods λ_k when k is sufficiently large. The periods depend upon the values of the parameters r, s, and t defined in (2.1).

Theorem 3.1. *Suppose that $\{u_i\}$ is a two-term recurrence sequence as defined in* (1.1), *with a even and b odd.*

(a) *If $k > 1$ and $t = 0$, then $\lambda_k = 2^k$.*
(b) *If $k > s + 1$ and $0 < s \le t$, then $\lambda_k = 2^{k-s}$.*
(c) *If $k > t$ and $0 < t < s$, then $\lambda_k = 2^{k-t}$.*
(d) *If $k > r + 2$ and $0 < r \le t$, then $\lambda_k = 2^{k-r}$.*
(e) *If $k > t + 1$ and $0 < t < r$, then $\lambda_k = 2^{k-t}$.*

Proof. (a) By Lemma 2.1 and Lemma 2.3(a), $u_{2^k} \equiv 0 \pmod{2^k}$ and $u_{2^k+1} \equiv 1 \pmod{2^k}$. Thus λ_k divides 2^k. On the other hand, Lemma 2.1

implies that $u_{2^{k-1}} \equiv 2^{k-1} \pmod{2^k}$, and it follows that λ_k does not divide 2^{k-1}. Thus $\lambda_k = 2^k$.

(b) By Lemma 2.1, $2^{t+k-s} \parallel u_{2^{k-s}}$. Since $s \le t$, it follows that $2^k \mid u_{2^{k-s}}$, and hence $u_{2^{k-s}} \equiv 0 \pmod{2^k}$. Moreover, by Lemma 2.3(b), $u_{2^{k-s}+1} \equiv 1 \pmod{2^k}$. It follows that λ_k divides 2^{k-s}. On the other hand, Lemma 2.3(b) also implies that $u_{2^{k-s}+1} \equiv 1 + 2^{k-1} \pmod{2^k}$. Thus λ_k does not divide 2^{k-s-1}, and hence $\lambda_k = 2^{k-s}$.

(c) By Lemma 2.1, $2^k \parallel u_{2^{k-t}}$. Thus $u_{2^{k-t}} \equiv 0 \pmod{2^k}$. Moreover, by Lemma 2.2(b), $u_{2^{k-t}+1} \equiv 1 \pmod{2^k}$. It follows that λ_k divides 2^{k-t}. On the other hand, Lemma 2.1 also implies that $2^{k-1} \parallel u_{2^{k-t-1}}$, and thus $u_{2^{k-t-1}} \equiv 2^{k-1} \pmod{2^k}$. It follows that λ_k does not divide 2^{k-t-1}, and hence $\lambda_k = 2^{k-t}$.

(d) Imitate the proof of (b) using Lemma 2.3(d) in place of Lemma 2.3(b).

(e) Imitate the proof of (c) using Lemma 2.2(c) in place of Lemma 2.2(b). ■

4. Stability

In this section we state and prove the following two theorems.

THEOREM 4.1. *Suppose that $\{u_i\}$ is a two-term recurrence sequence determined as in* (1.1) *by parameters a and b, with a even and b odd, and that r, s, and t are defined by* (2.1). *Then $\{u_i\}$ is stable modulo* 2 *provided one of the following conditions is true:*

(a) $t = 0$,

(b) $s \neq 2t$ *and* $r \neq 2t$, *or*

(c) $a \neq 0$ *and* $b = \pm 1$.

THEOREM 4.2. *Suppose that $\{u_i\}$ is a two-term recurrence sequence determined as in* (1.1) *by parameters a and b, with a even and b odd, and that r, s, and t are defined by* (2.1).

If d is any integer, then $\nu(2^{k+1}, d) = \nu(2^k, d)$ for all sufficiently large k provided one of the following conditions is true:

(a) $t = 0$,

(b) $s \neq 2t$ *and* $r \neq 2t$, *or*

(c) $a \neq 0$ *and* $b = \pm 1$.

More precisely, in (a) *it is sufficient to require $k > 1$ and in* (b) *and* (c) *it is sufficient to require $k > 2t + 1$.*

Note. Condition (c) in Theorems 4.1 and 4.2 corresponds to t being defined while one of r or s is not defined.

The requirement that $t = 0$ in (a) of Theorems 4.1 and 4.2 is equivalent to $a \equiv 2 \pmod 4$. It is worth observing that the sequences $\{u_i\}$ satisfying this condition are uniformly distributed (see, e.g., Theorem 3.5, p. 38 of [6]). We include a proof of stability in this case for completeness.

The proof of Theorem 4.1 requires only a short argument after Theorem 4.2 has been proven. Theorem 4.2 follows from a series of lemmas corresponding to the relationships between the parameters r, s, and t and the parity of d. We defer the proofs of these theorems to the end of the section.

Before presenting the proofs of Lemmas 4.3 through 4.13, we fix some notation and make some observations common to the proofs of each lemma. In each lemma, $\{u_i\}$ will be a recurrence sequence with defining parameters a and b, with a even and b odd. Parameters r, s, and t will be defined by (2.1), and in each lemma, r, s, and t will be subject to certain constraints. The integer k will be fixed in each lemma and subject to a given inequality. In each lemma, d will be a fixed integer and $\nu = \nu(2^k, d)$. Finally, integers n_i will be chosen to satisfy

$$0 \le n_1 < n_2 < \cdots < n_\nu < \lambda_k \text{ and } u_{n_i} \equiv d \pmod{2^k} \text{ for each } i.$$

Clearly, for each i, either $u_{n_i} \equiv d \pmod{2^{k+1}}$ or $u_{n_i} \equiv d + 2^k \pmod{2^{k+1}}$. Finally, by Fact 3, $n_i \equiv d \pmod 2$ for each i.

LEMMA 4.3. *Suppose that $k > 1$ and $t = 0$. Then $\nu(2^{k+1}, d) = \nu(2^k, d)$.*

Proof. Fix an index i such that $0 < i \le \nu$. Since $t = 0$, Theorem 3.1(a) implies that $\lambda_k = 2^k$. By Proposition 2.4(a), $u_{n_i+\lambda_k} \equiv u_{n_i} + 2^k \pmod{2^{k+1}}$.

It follows that the elements $\{u_{n_i}, u_{n_i+\lambda_k}\}$ are congruent modulo 2^{k+1} to d and $d + 2^k$ in some order. Choose $a_i \in \{n_i, n_i + \lambda_k\}$ such that $u_{a_i} \equiv d \pmod{2^{k+1}}$. Since $a_i \equiv n_i \pmod{2^k}$ and $0 \le a_i \le 2\lambda_k = \lambda_{k+1}$, it follows that the integers $\{a_1, a_2, \ldots, a_\nu\}$ are distinct and

$$\nu(2^{k+1}, d) \ge \nu = \nu(2^k, d).$$

The same argument, with $d + 2^k$ in place of d, yields

$$\nu(2^{k+1}, d + 2^k) \ge \nu(2^k, d + 2^k) = \nu(2^k, d).$$

On the other hand, since $\lambda_{k+1} = 2\lambda_k$ it follows that

$$\nu(2^{k+1}, d) + \nu(2^{k+1}, d + 2^k) = 2\nu(2^k, d). \tag{4.1}$$

Therefore the two preceding inequalities are equalities, and the lemma follows. ■

LEMMA 4.4. *Suppose that* $k > s + 1$, $0 < s \leq t$, *and* d *is odd. Then* $\nu(2^{k+1}, d) = \nu(2^k, d)$.

Proof. Fix an index i such that $0 < i \leq \nu$. By Theorem 3.1(b), $\lambda_k = 2^{k-s}$. By Proposition 2.4(c) (and the observation that n_i is odd), $u_{n_i+\lambda_k} \equiv u_{n_i} + 2^k \pmod{2^{k+1}}$.

It follows that the elements $\{u_{n_i}, u_{n_i+\lambda_k}\}$ are congruent modulo 2^{k+1} to d and $d + 2^k$ in some order. Choose $a_i \in \{n_i, n_i + \lambda_k\}$ such that $u_{a_i} \equiv d \pmod{2^{k+1}}$. Since $a_i \equiv n_i \pmod{2^k}$ and $0 \leq a_i \leq 2\lambda_k = \lambda_{k+1}$, it follows that the integers $\{a_1, a_2, \ldots, a_\nu\}$ are distinct and

$$\nu(2^{k+1}, d) \geq \nu = \nu(2^k, d).$$

The same argument, with $d + 2^k$ in place of d, yields

$$\nu(2^{k+1}, d + 2^k) \geq \nu(2^k, d + 2^k) = \nu(2^k, d).$$

As in Lemma 4.3, the lemma follows from the two preceding inequalities and (4.1). ■

LEMMA 4.5. *Suppose that* $k > s$, $0 < t < s < 2t$, *and* d *is odd. Then* $\nu(2^{k+1}, d) = \nu(2^k, d)$.

Proof. Fix an index i such that $0 < i \leq \nu$. By Theorem 3.1(c), $\lambda_k = 2^{k-t}$. The observation that n_i is odd, followed by repeated application of Proposition 2.4(c), yields, for all positive odd integers δ,

$$u_{n_i+\delta 2^{-(s-t)}\lambda_k} \equiv u_{n_i} + 2^k \qquad \pmod{2^{k+1}}.$$

Since $0 \leq n_i < \lambda_k$ there is a unique integer $\ell_i \in \{0, 1, 2, \ldots, 2^{s-t} - 1\}$ such that

$$\ell_i 2^{-(s-t)}\lambda_k \leq n_i < (\ell_i + 1)2^{-(s-t)}\lambda_k. \tag{4.2}$$

Let $\delta_i = 2^{(s-t+1)} - 2\ell_i - 1$. Clearly, δ_i is odd and $1 \leq \delta_i \leq 2^{(s-t+1)} - 1$. Thus

$$u_{n_i+\delta_i 2^{-(s-t)}\lambda_k} \equiv u_{n_i} + 2^k \qquad \pmod{2^{k+1}}. \tag{4.3}$$

By (4.2),

$$n_i + \left(\frac{\delta_i}{2^{(s-t)}}\right)\lambda_k \geq \left(\frac{\ell_i}{2^{(s-t)}} + \frac{2^{(s-t+1)} - 2\ell_i - 1}{2^{(s-t)}}\right)\lambda_k$$
$$= \left(\frac{2^{(s-t+1)} - \ell_i - 1}{2^{(s-t)}}\right)\lambda_k \geq \left(\frac{2^{(s-t+1)} - 2^{s-t}}{2^{(s-t)}}\right)\lambda_k = \lambda_k. \tag{4.4}$$

Moreover, by (4.2) and Theorem 3.1(c),

$$n_i + \left(\frac{\delta_i}{2^{(s-t)}}\right)\lambda_k < \left(\frac{\ell_i + 1}{2^{(s-t)}} + \frac{2^{(s-t+1)} - 2\ell_i - 1}{2^{(s-t)}}\right)\lambda_k$$
$$= \left(\frac{2^{(s-t+1)} - \ell_i}{2^{(s-t)}}\right)\lambda_k \leq \left(\frac{2^{(s-t+1)}}{2^{(s-t)}}\right)\lambda_k = 2\lambda_k = \lambda_{k+1}. \tag{4.5}$$

Together (4.4) and (4.5) imply that $\lambda_k \leq n_i + \delta_i 2^{-(s-t)}\lambda_k < 2\lambda_k$.

By (4.3), the elements u_{n_i} and $u_{n_i+\delta_i 2^{-(s-t)}}$ (in some order) are congruent modulo 2^{k+1} to d and $d + 2^k$. Choose $a_i \in \{u_{n_i}, u_{n_i+\delta_i 2^{-(s-t)}}\}$ such that $a_i \equiv d \pmod{2^{k+1}}$.

We now claim that $\nu(2^{k+1}, d) \geq \nu(2^k, d)$. It suffices to show that the integers $\{a_1, a_2, \ldots, a_\nu\}$ are distinct. To this end, suppose that i and j satisfy $i < j$ and $a_i = a_j$. Then $n_i < n_j < \lambda_k$. On the other hand, $\lambda_k < n_i + \delta_i 2^{-(s-t)}\lambda_k$ and $\lambda_k < n_j + \delta_j 2^{-(s-t)}\lambda_k$. This can only occur when

$$n_i + \delta_i 2^{-(s-t)}\lambda_k = n_j + \delta_j 2^{-(s-t)}\lambda_k.$$

It follows that

$$n_j - n_j = \left(\frac{\delta_i - \delta_j}{2^{s-t}}\right)\lambda_k = \left(\frac{2(\ell_j - \ell_i)}{2^{s-t}}\right)\lambda_k. \tag{4.6}$$

On the other hand, by (4.2),

$$n_j - n_i < \left(\frac{\ell_j + 1}{2^{s-t}}\right)\lambda_k - \left(\frac{\ell_i}{2^{s-t}}\right)\lambda_k = \left(\frac{\ell_j - \ell_i + 1}{2^{s-t}}\right)\lambda_k. \tag{4.7}$$

Together, (4.6) and (4.7) imply that $\ell_j - \ell_i < 1$. However, since $n_j > n_i$, we know that $\ell_j > \ell_i$, and therefore $\ell_j - \ell_i > 0$. This contradiction proves the claim.

The same argument, with $d + 2^k$ in place of d, yields

$$\nu(2^{k+1}, d + 2^k) \geq \nu(2^k, d + 2^k) = \nu(2^k, d).$$

As in Lemma 4.3, the lemma follows from the two preceding inequalities and (4.1). ■

LEMMA 4.6. *Suppose that either* $k > 2t + 1$, $0 < 2t < s$, *and* d *is odd or* $t > 0$, $k > 2t + 1$, s *is undefined, and* d *is odd. Then* $\nu(2^{k+1}, d) = \nu(2^k, d)$.

Proof. Fix an index i such that $0 < i \leq \nu$. By Theorem 3.1(c), $\lambda_k = 2^{k-t}$. Repeated application of Proposition 2.4(d) (and the observation that n_i is odd) yields, for all positive odd integers δ,

$$u_{n_i+\delta 2^{-t}\lambda_k} \equiv u_{n_i} + 2^k \pmod{2^{k+1}}.$$

The remainder of the proof is similar to the proof of Lemma 4.5. Choose ℓ_i such that $\ell_i \in \{0, 1, 2, \ldots, 2^t - 1\}$ and

$$\ell_i 2^{-t}\lambda_k \leq n_i < (\ell_i + 1)2^{-t}\lambda_k. \tag{4.8}$$

Define δ_i by $\delta_i = 2^{-t+1} - 2\ell_i - 1$. As in the proof of Lemma 4.5, it now follows that

$$u_{n_i+\delta_i 2^{-t}\lambda_k} \equiv u_{n_i} + 2^k \pmod{2^{k+1}}, \tag{4.9}$$

and

$$\lambda_k \leq n_i + \delta_i 2^{-t}\lambda_k < 2\lambda_k.$$

We can now choose $a_i \in \{u_{n_i}, u_{n_i+\delta_i 2^{-t}}\}$ such that $a_i \equiv d \pmod{2^{k+1}}$. As in the proof of Lemma 4.5, it is easy to prove that the integers $\{a_1, a_2, \ldots, a_\nu\}$ are distinct, and therefore

$$\nu(2^{k+1}, d) \geq \nu = \nu(2^k, d).$$

The same argument, with $d + 2^k$ in place of d, yields

$$\nu(2^{k+1}, d + 2^k) \geq \nu(2^k, d + 2^k) = \nu(2^k, d).$$

As in Lemma 4.3, the lemma follows from the two preceding inequalities and (4.1). ■

LEMMA 4.7. *Suppose that* $k > r + 2$, $0 < r \leq t$, *and* d *is odd. Then* $\nu(2^{k+1}, d) = \nu(2^k, d)$.

Proof. Fix an index i such that $0 < i \leq \nu$. By Theorem 3.1(d), $\lambda_k = 2^{k-r}$. By Proposition 2.4(e), (and the observation that n_i is odd) $u_{n_i+\lambda_k} \equiv u_{n_i} + 2^k \pmod{2^{k+1}}$.

It follows that the elements $\{u_{i_i}, u_{i_i+\lambda_k}\}$ are congruent modulo 2^{k+1} to d and $d + 2^k$ in some order. As in the proofs of Lemma 4.3 and Lemma 4.4, we can choose distinct $a_i \in \{n_i, n_i + \lambda_k\}$ such that $u_{a_i} \equiv d \pmod{2^{k+1}}$. Therefore $\nu(2^{k+1}, d) \geq \nu = \nu(2^k, d)$.

The same argument, with $d + 2^k$ in place of d, yields

$$\nu(2^{k+1}, d + 2^k) \geq \nu(2^k, d + 2^k) = \nu(2^k, d).$$

As in Lemma 4.3, the lemma follows from the two preceding inequalities and (4.1). ∎

LEMMA 4.8. *Suppose that $k > r + 1$, $0 < t < r < 2t$, and d is odd. Then $\nu(2^{k+1}, d) = \nu(2^k, d)$.*

Proof. Fix an index i such that $0 < i \leq \nu$. By Theorem 3.1(e), $\lambda_k = 2^{k-t}$. The observation that n_i is odd, followed by repeated application of Proposition 2.4(e), yields, for all positive odd integers δ,

$$u_{i_i+\delta 2^{-(r-t)}\lambda_k} \equiv u_{n_i} + 2^k \pmod{2^{k+1}}.$$

The remainder of the proof parallels the proof of Lemma 4.5. ∎

LEMMA 4.9. *Suppose that either $k > 2t + 1$, $0 < 2t < r$, and d is odd or $t > 0$, $k > 2t + 1$, r is undefined, and d is odd. Then $\nu(2^{k+1}, d) = \nu(2^k, d)$.*

Proof. Fix an index i such that $0 < i \leq \nu$. By Theorem 3.1(e), $\lambda_k = 2^{k-t}$. Repeated application of Proposition 2.4(f) (and the observation that n_i is odd) yields, for all positive odd integers δ,

$$u_{n_i+\delta 2^{-t}\lambda_k} \equiv u_{n_i} + 2^k \pmod{2^{k+1}}.$$

The remainder of the proof parallels the proof of Lemma 4.6. ∎

Having treated odd residues, we now turn to the even. Since the proofs of these lemmas follow the same scheme as the previous lemmas, we are content to sketch the proofs.

LEMMA 4.10. *Suppose that $k > \max(s + 1, t)$, $0 < s \leq t$, and d is even. Then $\nu(2^{k+1}, d) = \nu(2^k, d)$.*

Proof. By Theorem 3.1(b), $\lambda_k = 2^{k-s}$. By Proposition 2.4(b), $u_{n_i+2^{-(t-s)}\lambda_k} \equiv u_{n_i} + 2^k \pmod{2^{k+1}}$. The remainder of the proof parallels the proof of Lemma 4.5.

LEMMA 4.11. *Suppose that either $k > t$, $0 < t < s$, and d is even or $t > 0$, $k >$ t, s is undefined, and d is even. Then $\nu(2^{k+1}, d) = \nu(2^k, d)$.*

Proof. By Theorem 3.1(c), $\lambda_k = 2^{k-t}$. By Proposition 2.4(b), $u_{n_i+\lambda_k} \equiv u_{n_i} + 2^k \pmod{2^{k+1}}$.

As in Lemma 4.3, we can choose distinct $a_i \in \{n_i, n_i + \lambda_k\}$ such that $u_{a_i} \equiv \pmod{2^{k+1}}$. Therefore $\nu(2^{k+1}, d) \geq \nu = \nu(2^k, d)$.

The same argument, with $d + 2^k$ in place of d, yields

$$\nu(2^{k+1}, d + 2^k) \geq \nu(2^k, d + 2^k) = \nu(2^k, d).$$

As in Lemma 4.3, the lemma follows from the two preceding inequalities and (4.1). ■

LEMMA 4.12. *Suppose that* $k > \max(r + 2, t)$, $0 < r \leq t$, *and d is even. Then* $\nu(2^{k+1}, d) = \nu(2^k, d)$.

Proof. By Theorem 3.1(d), $\lambda_k = 2^{k-r}$. By Proposition 2.4(b), $u_{n_i+2^{-(t-r)}\lambda_k} \equiv u_{n_i} + 2^k \pmod{2^{k+1}}$. The remainder of the proof parallels the proof of Lemma 4.5.

LEMMA 4.13. *Suppose that either* $k > t + 1$, $0 < t < r$, *and d is even or* $t > 0$, $k > t + 1$, *r is undefined, and d is even. Then* $\nu(2^{k+1}, d) = \nu(2^k, d)$.

Proof. By Theorem 3.1(e), $\lambda_k = 2^{k-t}$. By Proposition 2.4(b), $u_{n_i+\lambda_k} \equiv u_{n_i} + 2^k \pmod{2^{k+1}}$.

As in Lemma 4.3, we can choose distinct $a_i \in \{n_i, n_i + \lambda_k\}$ such that $u_{a_i} \equiv d \pmod{2^{k+1}}$. Therefore $\nu(2^{k+1}, d) \geq \nu = \nu(2^k, d)$.

The same argument, with $d + 2^k$ in place of d, yields

$$\nu(2^{k+1}, d + 2^k) \geq \nu(2^k, d + 2^k) = \nu(2^k, d).$$

As in Lemma 4.3, the lemma follows from the two preceding inequalities and (4.1). ■

Now, we turn to the proofs of Theorems 4.1 and 4.2.

Proof of Theorem 4.2. First note that if $t = 0$, then the proposition follows from Lemma 4.3.

Next, suppose that r, s, and t are all defined. If $s = 0$ then $r > 0$ and there are two cases: either $0 < r \leq t$ and the proposition follows from Lemmas 4.7 and 4.12 or $0 < t < r$ and the proposition follows from Lemmas 4.8, 4.9, and 4.13. If $s > 0$ then there are two additional cases: either $0 < s \leq t$ and the proposition follows from Lemmas 4.4 and 4.10 or $0 < t < s$ and the proposition follows from Lemmas 4.5, 4.6, and 4.11.

Now, suppose that t is defined and $t > 0$, but that r is not defined. Then the proposition follows from Lemmas 4.9 and 4.13.

Finally, suppose that t is defined and $t > 0$, but that s is not defined. Then the proposition follows from Lemmas 4.6 and 4.11.

Finally, we prove Theorem 4.1.

Proof of Theorem 4.1. Assume the hypotheses of Theorem 4.1. By Theorem 4.2, for all sufficiently large k,

$$\begin{aligned}\Omega(2^{k+1}) &= \{\nu(2^{k+1}, d) \mid 0 \le d < 2^{k+1}\}\\ &= \{\nu(2^{k+1}, d) \mid 0 \le d < 2^{k}\} \cup \{\nu(2^{k+1}, d + 2^k) \mid 0 \le d < 2^k\}\\ &= \{\nu(2^k, d) \mid 0 \le d < 2^k\} \cup \{\nu(2^k, d) \mid 0 \le d < 2^k\}\\ &= \Omega(2^k) \cup \Omega(2^k) = \Omega(2^k).\end{aligned}$$

Thus $\Omega(2^{k+1}) = \Omega(2^k)$, as desired. ■

5. Addendum

As we noted after (2.1), the parameters r, s, and t are not always defined. In particular, t is not defined when $a = 0$, r is not defined when $b = 1$, and s is not defined when $b = -1$. By Theorem 4.1 the sequence $\{u_i\}$ is stable when $a \neq 0$ and either $b = 1$ or $b = -1$. For completeness we consider here the case that $a = 0$. As we will show, for most values of b these sequences are not stable.

Suppose that $a = 0$, so that t is not defined. Clearly the sequence $\{u_i\}$ has the form

$$0, 1, 0, b, 0, b^2, 0, b^3, \ldots. \tag{5.1}$$

If $b = \pm 1$, stability of the resulting sequences is obvious: a single period of the sequence modulo 2^k is either 0, 1 (if $k = 1$ or $b = 1$) or $0, 1, 0, -1$ (if $k > 1$ and $b = -1$). Consequently $\Omega(2^k) =$ of $\{0, 1\}$ for all $k \geq 2$ in the first case and $\Omega(2^k) =$ of $\{0, 1, 2\}$ for all $k \geq 2$ in the second.

If $b \neq \pm 1$ the period λ_k and the frequency distribution function $\nu(2^k, d)$ depend upon the multiplicative order of b modulo 2^k. On the other hand, if $b \neq \pm 1$ then r and s are defined and the multiplicative order of b modulo 2^k can be computed in terms of r and s.

Theorem 5.1. *Suppose that $a = 0$ and $b \neq \pm 1$.*

(a) *If $s > 0$ and $k > s$ then $\lambda_k = 2^{k-s}$.*
(b) *If $r > 0$ and $k > r$ then $\lambda_k = 2^{k-r}$.*

Proof. We prove (a) and (b) simultaneously. Let ℓ be the multiplicative order of b modulo 2^k. Then it is clear from (5.1) that $\lambda_k = 2\ell$.

Now, the group of units modulo 2^k is a 2-group, so, by Lagrange's theorem, the order of b is a power of two. Moreover, an easy inductive argument shows for all $j \geq 0$ that $2^{s+j+1} \parallel b^{2^j} - 1$ under hypothesis (a) and for all $j \geq 1$ that $2^{r+j+1} \parallel b^{2^j} - 1$ under hypothesis (b). Therefore $\ell = 2^{k-s-1}$ and $\ell = 2^{k-r-1}$ are the least powers of b such that $b^\ell \equiv 1 \pmod{2^k}$ under hypotheses (a) and (b), respectively. ■

THEOREM 5.2. *Suppose that $a = 0$ and $b \neq \pm 1$.*

(a) *If $s > 0$ and $k > s$ then $\nu(2^k, 0) = 2^{k-s-1}$, $\nu(2^k, b^j) = 1$ for all j, and $\nu(2^k, d) = 0$ otherwise.*

(b) *If $r > 0$ and $k > r$ then $\nu(2^k, 0) = 2^{k-r-1}$, $\nu(2^k, b^j) = 1$ for all j, and $\nu(2^k, d) = 0$ otherwise.*

Proof. As in Theorem 5.1, let ℓ be the multiplicative order of b modulo 2^k. Then the powers of b below ℓ have distinct nonzero residues modulo 2^k, and it follows that $\nu(2^k, b^d) = 1$ for all d. Moreover, it is clear from (5.1) and Theorem 5.1 that $\nu(2^k, 0) = 2^{k-s-1}$ and $\nu(2^k, 0) = 2^{k-r-1}$ under hypotheses (a) and (b), respectively. Finally, in both cases it follows from (5.1) that $\nu(2^k, d) = 0$ when d is neither 0 nor a power of b. ■

COROLLARY 5.3. *If $a = 0$, then $\{u_i\}$ is stable when $b = \pm 1$ and is not stable for all other odd b.*

REFERENCES

1. W. Carlip and E. Jacobson, A criterion for stability of two-term recurrence sequences modulo 2^k, *Finite Fields Appl.* **2** (1996), 369–406.
2. W. Carlip and E. Jacobson, On the stability of certain Lucas sequences modulo 2^k, *Fibonacci Quart.* **34** (1996), 289–305.
3. W. Carlip and E. Jacobson, Unbounded stability of two-term recurrence sequences modulo 2^k, *Acta Arith.* **74** (1996), 329–346.
4. R. D. Carmichael, On sequences of integers defined by recurrence relations, *Quart. J. Pure Appl. Math.* **48** (1920), 343–372.
5. E. T. Jacobson, Distribution of the Fibonacci numbers mod 2^k, *Fibonacci Quart.* (1992), 211–215.
6. W. Narkiewicz, “Uniform Distribution of Sequences of Integers in Residue Classes,” Lecture Notes In Mathematics, Vol. 1087, Springer-Verlag, New York, 1984.
7. J. Pihko, A note on a theorem of Schinzel, *Fibonacci Quart.* **29** (1991), 333–338.
8. P. Ribenboim, “The Little Book of Big Primes,” Springer-Verlag, New York, 1991.
9. A. Schinzel, Special Lucas sequences, including the Fibonacci sequence, modulo a prime, *in* “A Tribute to Paul Erdõs (Cambridge, England)” (A. Baker, B. Bollobás, and A. Hajnal, Eds.), pp. 349–357, Cambridge Univ. Press, Cambridge, 1990.
10. D. D. Wall, Fibonacci series modulo m, *Amer. Math. Monthly* **67** (1960), 525–532.
11. M. Ward, The arithmetical theory of linear recurring series, *Trans. Amer. Math. Soc.* **95** (1933), 600–628.