EQUIDISTRIBUTION OF LINEAR RECURRING SEQUENCES IN FINITE FIELDS

BY

HARALD NIEDERREITER AND JAU-SHYONG SHIUE

(Communicated by Prof. J. H. van Lint at the meeting of February 26, 1977)

1. INTRODUCTION

According to a general principle established by the first author [12], any linear recurring sequence in a finite field which has a sufficiently long period is almost equidistributed, in the sense that each element of the field occurs about equally often in the full period of the sequence. This raises the question of characterizing those linear recurring sequences for which we have exact equidistribution. We settle this problem for linear recurrences of low order. Although the pattern of a general method emerges clearly from the ensuing investigation, a detailed discussion becomes increasingly complex for higher-order linear recurring sequences. Therefore we restrict the attention to linear recurrences of order at most 4. We note that distribution properties of linear recurring sequences are of interest for applications to coding theory (compare with [13]).

Related work concerning the distribution of second-order linear recurring sequences in residue class rings $\mathbb{Z}/m\mathbb{Z}$ has been carried out recently. The first results were obtained for special classes of sequences, such as Fibonacci numbers and Lucas numbers, considered modulo prime powers ([6], [7], [11]). Further work dealt with somewhat more general second-order linear recurring sequences of integers ([5], [8], [15], [16]). Finally, several authors obtained a complete characterization of the second-order linear recurring sequences with the equidistribution property in $\mathbb{Z}/m\mathbb{Z}$ ([1], [2], [10], [17]). For prime moduli, we recapture this characterization in a very easy manner (see Theorem 2).

2. DEFINITIONS AND GENERAL FACTS

Let F_q be a finite field with q elements and of characteristic p. A sequence (x_n), $n=0, 1, \ldots$, of elements of F_q is said to be *equidistributed* (or *uniformly distributed*, abbreviated *u.d.*) in F_q if

$$\lim_{N\to\infty} \frac{A(c, N)}{N} = \frac{1}{q} \text{ for all } c \in F_q,$$

where $A(c, N) = A(c, N, (x_n))$ denotes the number of n, $0 \leqslant n \leqslant N-1$, for

which $x_n = c$ (compare with [4, p. 331, Exercise 3.5]). For a periodic sequence (x_n), this definition is obviously equivalent to the requirement that each element of F_q occurs equally often in the full period of (x_n).

LEMMA 1. Two sequences (x_n) and (y_n) in F_q have the same distribution of elements among the first N terms if and only if $\sum_{n=0}^{N-1} \chi(x_n) = \sum_{n=0}^{N-1} \chi(y_n)$ for all nontrivial additive characters χ of F_q.

PROOF. The condition is obviously necessary. To show the converse, we note that for any $c \in F_q$,

$$A(c, N, (x_n)) = \sum_{n=0}^{N-1} \frac{1}{q} \sum_{\chi} \chi(x_n - c) = \frac{1}{q} \sum_{\chi} \overline{\chi(c)} \sum_{n=0}^{N-1} \chi(x_n),$$

where χ runs through all additive characters of F_q. An analogous formula holds for $A(c, N, (y_n))$. From the given identity, which is also valid for the trivial additive character, it follows that $A(c, N, (x_n)) = A(c, N, (y_n))$ for all $c \in F_q$.

COROLLARY 1. A sequence (x_n) in F_q with period τ is u.d. in F_q if and only if $\sum_{n=0}^{\tau-1} \chi(x_n) = 0$ for all nontrivial additive characters χ of F_q.

LEMMA 2. Let (x_n) and (y_n) be two sequences in F_q. Then $A(c, N, (x_n)) \equiv A(c, N, (y_n)) \pmod{p}$ for all $c \in F_q$ if and only if $\sum_{n=0}^{N-1} x_n^j = \sum_{n=0}^{N-1} y_n^j$ for $1 \leqslant j \leqslant q-1$.

PROOF. The condition is easily seen to be necessary. Conversely, we note that $A(c, N, (x_n))$, viewed as an element of F_q, is given by

$$A(c, N, (x_n)) = \sum_{n=0}^{N-1} (1 - (x_n - c)^{q-1}) = N - N(-c)^{q-1} - \\ - \sum_{j=1}^{q-1} \binom{q-1}{j} (-c)^{q-1-j} \sum_{n=0}^{N-1} x_n^j.$$

An analogous formula holds for $A(c, N, (y_n))$. It follows then from the given hypothesis that $A(c, N, (x_n)) = A(c, N, (y_n))$ as elements of F_q, and so $A(c, N, (x_n)) \equiv A(c, N, (y_n)) \pmod{p}$ as integers.

COROLLARY 2. Let (x_n) be a sequence in F_q with period dq, where d is an integer with $1 \leqslant d \leqslant p-1$. Then (x_n) is u.d. in F_q if and only if

$$\sum_{n=0}^{dq-1} x_n^j = \begin{cases} 0 \text{ for } 1 \leqslant j \leqslant q-2, \\ -d \text{ for } j = q-1. \end{cases} \tag{1}$$

PROOF. Since

$$\sum_{c \in F_q} c^j = \begin{cases} 0 \text{ for } 1 \leqslant j \leqslant q-2, \\ -1 \text{ for } j = q-1, \end{cases} \tag{2}$$

by [9, p. 191, Lemma 8.24], it follows from Lemma 2 that (1) is equivalent to $A(c, dq, (x_n)) \equiv d \pmod{p}$ for all $c \in F_q$. Therefore, (1) is necessary for the equidistribution of (x_n) in F_q. Conversely, because of $1 \leqslant d \leqslant p-1$, the above congruence implies $A(c, dq, (x_n)) \geqslant d$ for all $c \in F_q$, and so $A(c, dq, (x_n)) = d$ for all $c \in F_q$.

A sequence (u_n), $n = 0, 1, \ldots$, of elements of F_q is called a *kth order linear recurring sequence* if it satisfies a linear recurrence relation of the form

$$u_{n+k} = a_{k-1}u_{n+k-1} + \ldots + a_1 u_{n+1} + a_0 u_n \text{ for } n = 0, 1, \ldots, \tag{3}$$

where the coefficients $a_0, a_1, \ldots, a_{k-1}$ are fixed elements of F_q and $k \geqslant 1$. We can assume, without loss of generality, that (3) is the linear recurrence relation of lowest order satisfied by the sequence (u_n). In this case, the polynomial $m(x) = x^k - a_{k-1}x^{k-1} - \ldots - a_1 x - a_0 \in F_q[x]$ associated with (3) is called the *minimal polynomial* of (u_n).

For the purpose of investigating the equidistribution of (u_n), *we can, and will, also assume that* $m(0) \neq 0$. For if $m(0) = 0$, then either $m(x) = x^k$ or $m(x) = x^h g(x)$, where $h \geqslant 1$ and $g(x) \in F_q[x]$ is monic of positive degree with $g(0) \neq 0$. In the first case, we have $u_n = 0$ for all $n \geqslant k$, and so (u_n) cannot be u.d. in F_q. In the second case, the sequence (u_{n+h}), $n = 0, 1, \ldots$, has the minimal polynomial $g(x)$, and (u_n) is u.d. in F_q if and only if (u_{n+h}) is u.d. in F_q. Therefore, it suffices to consider linear recurrence relations for which the coefficient a_0 in (3) is nonzero. In this case, however, the sequence (u_n) is periodic (in the general case, the sequence may have a preperiod).

In the following lemma, we collect some standard facts about linear recurring sequences in finite fields. We refer to [14] and [18] for a detailed treatment of these matters.

LEMMA 3. Let $m(x) = (x-\alpha_1)^{r_1} \ldots (x-\alpha_s)^{r_s}$ be the canonical factorization of $m(x)$ in a suitable finite extension E of F_q, so that $\alpha_1, \ldots, \alpha_s$ are distinct nonzero elements of E. Then any linear recurring sequence (u_n) in F_q with minimal polynomial $m(x)$ is periodic with period ep^t, where e is the smallest positive integer with $\alpha_j^e = 1$ for $1 \leqslant j \leqslant s$ and p^t is the smallest integral power of p with $p^t \geqslant \max(r_1, \ldots, r_s)$. Furthermore, if $\max(r_1, \ldots, r_s) \leqslant p$, then the terms of (u_n) are given explicitly by

$$u_n = \sum_{j=1}^{s} Q_j(n)\alpha_j^n \text{ for } n = 0, 1, \ldots, \tag{4}$$

where $Q_j(x) \in E[x]$ has degree at most $r_j - 1$.

From the above lemma one easily deduces some important necessary conditions for the equidistribution of (u_n). We note that since F_q is of characteristic p, we can write $q=p^f$ with an integer $f\geqslant 1$.

LEMMA 4. If $q=p^f$ and the linear recurring sequence (u_n) is u.d. in F_q, then necessarily $f\leqslant t$, where t is as in Lemma 3.

PROOF. If E is the field from Lemma 3, then $\alpha_j^{p^h-1}=1$ for $1\leqslant j\leqslant s$, where p^h is the number of elements of E. Therefore, the integer e in Lemma 3 divides p^h-1. Now if (u_n) is u.d. in F_q, then q must divide the length of the period of (u_n), which is ep^t by Lemma 3. But q and e are relatively prime by the previous remark, so that q divides p^t and hence $f\leqslant t$.

COROLLARY 3. If the linear recurring sequence (u_n) is u.d. in F_q, then its minimal polynomial $m(x)$ must necessarily have a multiple root.

PROOF. By Lemma 4 we must have $t\geqslant 1$, and so the definition of t in Lemma 3 shows that $\max(r_1, \ldots, r_s)\geqslant 2$.

Because of Corollary 3, *we shall only consider minimal polynomials $m(x)$ with at least one multiple root.* If $m(x)$ has a special type of factorization, then a result for linear recurring sequences of any order can be established.

THEOREM 1. Let (u_n) be a linear recurring sequence in F_q with minimal polynomial $m(x)=(x-a)^2m_1(x)$, where $a\in F_q$, $m_1(x)\in F_q[x]$ has only simple roots, and $m_1(a)\neq 0$. Then (u_n) is u.d. in F_q if and only if q is prime.

PROOF. In the notation of Lemma 3, we have $\max(r_1, \ldots, r_s)=2$, and so $t=1$. Therefore, $q=p$ is a necessary condition for the equidistribution of (u_n) because of Lemma 4. Conversely, suppose $q=p$ and let $m_1(x)=$ $=(x-\alpha_2)\ldots(x-\alpha_s)$, where $\alpha_2, \ldots, \alpha_s$ are distinct elements of a suitable finite extension of F_p. By (4) we have

$$u_n=(c_0+c_1n)a^n+c_2\alpha_2^n+\ldots+c_s\alpha_s^n \text{ for all } n\geqslant 0.$$

Here $c_1\neq 0$, for otherwise (u_n) would satisfy a linear recurrence relation of lower order. If e is as in Lemma 3, then for any $j\geqslant 0$ and $n\geqslant 0$ we get

$$u_{n+je}=(c_0+c_1n+c_1je)a^n+c_2\alpha_2^n+\ldots+c_s\alpha_s^n=u_n+jc_1ea^n. \tag{5}$$

Since e is not divisible by p (see the proof of Lemma 4), it follows in particular that $c_1\in F_p$. Furthermore, the period of (u_n) is ep by Lemma 3. For each fixed n, $0\leqslant n\leqslant e-1$, the finite sequence (u_{n+je}), $j=0, 1, \ldots, p-1$, runs exactly once through F_p because of $c_1ea^n\neq 0$ and (5). Therefore, among the first ep terms of (u_n) each element of F_p appears e times, and so (u_n) is u.d. in F_p.

3. SECOND AND THIRD-ORDER RECURRENCES

Obviously, a first-order linear recurring sequence in F_q can never be u.d. in F_q. Therefore, we can proceed to consider second-order linear recurring sequences.

THEOREM 2. A linear recurring sequence (u_n) in F_q with minimal polynomial $m(x)$ of degree 2 is u.d. in F_q if and only if q is prime and $m(x)$ has a multiple root.

PROOF. This is an immediate consequence of Corollary 3 and Theorem 1

For third-order linear recurring sequences, one has to distinguish two cases depending on the form of the canonical factorization of $m(x)$. The corresponding criteria for equidistribution are enunciated in Theorems 3A and 3B.

THEOREM 3A. Let (u_n) be a linear recurring sequence in F_q with minimal polynomial $m(x)=(x-a)^2(x-b)$, where $a, b \in F_q$ and $a \neq b$. Then (u_n) is u.d. in F_q if and only if q is prime.

PROOF. This is a special case of Theorem 1.

THEOREM 3B. Let (u_n) be a linear recurring sequence in F_q with minimal polynomial $m(x)=(x-a)^3$, $a \in F_q$. If $p \geqslant 3$, then (u_n) is u.d. in F_q if and only if $q=p$, a is not a square in F_p, and $(u_2-4au_1+a^2u_0)^2 = 4a^2u_0u_2$. If $p=2$, then (u_n) is u.d. in F_q if and only if either (i) $q=2$; or (ii) $q=4$, $a=1$, and u_0, u_1, u_2 are distinct; or (iii) $q=4$, $a \notin F_2$, and exactly one of $a^2u_0(u_2+a^2u_0)^{-1}$ and $au_1(u_2+a^2u_0)^{-1}$ is in F_2.

PROOF. In the notation of Lemma 3, we have $\max(r_1, \ldots, r_s)=3$. Therefore, if $p \geqslant 3$, then $t=1$, and so $q=p$ is a necessary condition for the equidistribution of (u_n) in F_q because of Lemma 4. Furthermore, (u_n) has period ep and by (4),

$$u_n=(c_0+c_1n+c_2n^2)a^n \text{ for all } n \geqslant 0, \tag{6}$$

where $c_0, c_1, c_2 \in F_p$. We have $c_2 \neq 0$, for otherwise (u_n) would satisfy a linear recurrence relation of lower order. For $n \geqslant 0$ and $i \geqslant 0$, we get

$$u_{n+ip}=(c_0+c_1n+c_2n^2)a^{n+ip}=(c_0+c_1n+c_2n^2)a^na^i=a^iu_n.$$

Thus, if (u_n) is u.d. in F_p, then exactly one term among $u_0, u_1, \ldots, u_{p-1}$ must be 0. It follows from (6) that the polynomial $g(x)=c_0+c_1x+c_2x^2 \in \in F_p[x]$ has one root in F_p of multiplicity 2, and so the discriminant $c_1^2-4c_0c_2$ of $g(x)$ is 0. Now (6) leads to $u_0=c_0$, $u_1=c_0a+c_1a+c_2a$, $u_2=c_0a^2+ +2c_1a^2+4c_2a^2$. Solving this system, we find $c_1=(2a^2)^{-1}(-u_2+4au_1-3a^2u_0)$, $c_2=(2a^2)^{-1}(u_2-2au_1+a^2u_0)$. By substituting into the equation $c_1^2=4c_0c_2$ and simplifying, we obtain $(u_2-4au_1+a^2u_0)^2=4a^2u_0u_2$, which is therefore

a necessary condition for (u_n) to be u.d. in F_p. We thus have $g(x)=c_2(x-c)^2$ for a suitable $c\in F_p$, and so $u_n=c_2(n-c)^2a^n$ for all $n\geqslant 0$. If a were a square in F_p, then (u_n) would run only through squares or only through nonsquares and 0, depending on whether c_2 is a square or a nonsquare. Thus, (u_n) can only be u.d. in F_p if a is a nonsquare in F_p. Now suppose that all those necessary conditions are satisfied. Since a is a nonsquare in F_p, the multiplicative order e of a is even. Furthermore, $u_{n+je}=$ $=c_2(n-c+je)^2a^n$ for $n\geqslant 0$ and $j\geqslant 0$. Transforming summation variables, we get for every nontrivial additive character χ of F_p,

$$\sum_{n=0}^{ep-1}\chi(u_n)=\sum_{n=0}^{e-1}\sum_{j=0}^{p-1}\chi(u_{n+je})=\sum_{n=0}^{e-1}\sum_{j=0}^{p-1}\chi(c_2a^n(n-c+je)^2)$$

$$=\sum_{n=0}^{e-1}\sum_{j=0}^{p-1}\chi(c_2a^nj^2)=\sum_{n=0}^{(e/2)-1}\left(\sum_{j=0}^{p-1}\chi(c_2a^{2n}j^2)+\sum_{j=0}^{p-1}\chi(c_2a^{2n+1}j^2)\right)$$

$$=\sum_{n=0}^{(e/2)-1}\left(\sum_{j=0}^{p-1}\chi(c_2j^2)+\sum_{j=0}^{p-1}\chi(c_2aj^2)\right)=2\sum_{n=0}^{(e/2)-1}\sum_{j=0}^{p-1}\chi(j)=0,$$

and so (u_n) is u.d. in F_p by Corollary 1.

Now let $p=2$. Since $\max(r_1,\ldots,r_s)=3$, we have $t=2$ in this case, and so Lemma 4 shows that (u_n) is u.d. in F_q only if $q=2$ or 4. If $q=2$, one shows by inspection that all 4 linear recurring sequences in F_2 with minimal polynomial $m(x)=(x-1)^3$ are u.d. in F_2. For $q=4$, we first consider the case where $m(x)=(x-1)^3$. A linear recurring sequence (u_n) in F_4 with this minimal polynomial has period 4, and so it will be u.d. in F_4 if and only if u_0, u_1, u_2, u_3 run through all elements of F_4. Then u_0, u_1, u_2 are necessarily distinct, but this is also sufficient since $u_3=u_2+u_1+u_0$ always gives the remaining element of F_4. Finally, let $m(x)=(x-a)^3$ with $a\notin F_2$. Then $a^2+a+1=0$ and (u_n) has period 12. If $d=u_2+a^2u_0$, then $d\neq 0$, for otherwise (u_n) would satisfy the second-order linear recurrence relation $u_{n+2}=a^2u_n$ for $n\geqslant 0$. By calculating the terms $u_0, u_1, \ldots, u_{11}$ in the full period of (u_n), one finds the following elements: u_0, a^2u_0+d, u_1, a^2u_1+ad, as well as those elements obtained by multiplying these 4 elements by a and a^2. Therefore, one sees easily that (u_n) is u.d. in F_4 if and only if exactly one of the 4 elements listed is 0. This condition can be transformed readily into the condition given in the theorem.

4. FOURTH-ORDER RECURRENCES

The methods in the previous section can be adapted to work for fourth-order linear recurring sequences as well. However, the procedure becomes very technical and cumbersome, so that we will only outline the results here.

For fourth-order linear recurring sequences, one has to distinguish four cases depending on the form of the canonical factorization of $m(x)$. The simplest case is already contained in Theorem 1.

THEOREM 4A. Let (u_n) be a linear recurring sequence in F_q with minimal polynomial $m(x)=(x-a)^2(x-\beta)(x-\gamma)$, where $a \in F_q$, $\beta, \gamma \in F_{q^2}$, and a, β, γ are distinct. Then (u_n) is u.d. in F_q if and only if q is prime.

THEOREM 4B. Let (u_n) be a linear recurring sequence in F_q with minimal polynomial $m(x)=(x-\alpha)^2(x-\beta)^2$, where $\alpha, \beta \in F_{q^2}$ and $\alpha \neq \beta$. Then (u_n) is u.d. in F_q if and only if q is prime and the element

$$[\alpha^2\beta u_0-(\alpha^2+2\alpha\beta)u_1+(2\alpha+\beta)u_2-u_3][-\alpha\beta^2u_0+(2\alpha\beta+\beta^2)u_1- \\ -(\alpha+2\beta)u_2+u_3]^{-1} \in F_{q^2}$$

is not a power of $\alpha\beta^{-1}$.

In the third case, one has to discuss $p=2$ separately (compare with Theorem 3B). For $p \geqslant 3$, one obtains the following criterion.

THEOREM 4C. Let (u_n) be a linear recurring sequence in F_q with minimal polynomial $m(x)=(x-a)^3(x-b)$, where $a, b \in F_q$ and $a \neq b$. If $p \geqslant 3$, then (u_n) is u.d. in F_q if and only if $q=p$, a is not a square in F_p, and

$$\sum_{\substack{i=0 \\ i \equiv h_j \pmod{e_1}}}^{j} \binom{j}{i} c^i = 0 \tag{7}$$

for all j with $1 \leqslant j \leqslant p-1$ and $j \equiv e_3/2 \pmod{e_3/e_1}$, where e_1 is the multiplicative order of ba^{-1} in F_p, $e_3=\text{l.c.m.}(e_1, e_2)$ with e_2 being the multiplicative order of b in F_p, h_j is an integer with $(ba^{-1})^{h_j}=-b^j$, and $c=vw^{-1}$ with

$$v=8a^2[(3a^2b-3ab^2+b^3)u_0-3a^2u_1+3au_2-u_3][a^2bu_0-(a^2+2ab)u_1+ \\ +(2a+b)u_2-u_3]-[(-5a^3b+3a^2b^2)u_0+(5a^3+5a^2b-4ab^2)u_1+ \\ +(-8a^2+ab+b^2)u_2+(3a-b)u_3]^2$$

and

$$w=8a^2[a^2bu_0-(a^2+2ab)u_1+(2a+b)u_2-u_3](-a^3u_0+3a^2u_1-3au_2+u_3).$$

In the proof, one shows first that $q=p$ and a being a nonsquare in F_p are necessary conditions. Then one proves that (u_n) is u.d. in F_p if and only if an auxiliary sequence (w_n) of the form $w_n=\varrho a^n+\sigma b^n$, $n=0, 1, \ldots$, with $\varrho, \sigma \in F_p$ has the property that the two subsequences (w_{2n}) and (w_{2n+1}) have the same distribution of elements. On the basis of Lemma 2, this can be reduced to the condition (7) in the theorem.

The last case requires a separate discussion for $p=2$ and $p=3$. The criterion for $p \geqslant 5$ employs the following notion. We note that for $g(x) \in F_p[x]$ there exists a unique polynomial $\tilde{g}(x) \in F_p[x]$ of degree at most $p-1$ with $g(x) \equiv \tilde{g}(x) \pmod{(x^p-x)}$; then the *reduced degree of* $g(x)$ is defined to be the degree of $\tilde{g}(x)$.

THEOREM 4D. Let (u_n) be a linear recurring sequence in F_q with minimal polynomial $m(x)=(x-a)^4$, where $a \in F_q$. Suppose $p \geqslant 5$, and let $f(x)=x^3+d_2x^2+d_1x+d_0$ with

$$d_0 = -6a^3u_0(a^3u_0-3a^2u_1+3au_2-u_3)^{-1},$$
$$d_1 = (11a^3u_0-18a^2u_1+9au_2-2u_3)(a^3u_0-3a^2u_1+3au_2-u_3)^{-1},$$
$$d_2 = (-6a^3u_0+15a^2u_1-12au_2+3u_3)(a^3u_0-3a^2u_1+3au_2-u_3)^{-1}.$$

Then (u_n) is u.d. in F_q if and only if $q=p$, the polynomial $f(x)$ has exactly one root in F_p, and the reduced degree of $(f(x))^{ej}$ is at most $p-2$ for each j with $1 \leqslant j < (p-1)/e$, where e is the multiplicative order of a.

The proof is based on Corollary 2. An interesting connection with classical problems arises for $a=1$ and $q=p$. In this case, we have $u_n=h(n)$ for $n=0, 1, \ldots$, where $h(x)$ is a cubic polynomial over F_p which differs from $f(x)$ by a nonzero constant factor. Therefore, (u_n) is u.d. in F_p if and only if $f(x)$ is a permutation polynomial over F_p (compare with [9, Ch. 4, Sec. 8]). The cubic permutation polynomials over F_p have been characterized by Dickson [3].

Department of Mathematics
University of Illinois
Urbana, IL 61801, USA

Department of Mathematical Sciences
National Chengchi University
Taipei, Taiwan, Republic of China

REFERENCES

1. Bumby, R. T. – A distribution property for linear recurrence of the second order, Proc. Amer. Math. Soc. **50**, 101–106 (1975).
2. Bundschuh, P. and J.-S. Shiue – Solution of a problem on the uniform distribution of integers, Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. (8) **55**, 172–177 (1973).
3. Dickson, L. E. – Analytic functions suitable to represent substitutions, Amer. J. Math. **18**, 210–218 (1896).
4. Kuipers, L. and H. Niederreiter – Uniform Distribution of Sequences, Wiley-Interscience, New York (1974).
5. Kuipers, L. and J.-S. Shiue – On the distribution modulo m of sequences of generalized Fibonacci numbers, Tamkang J. Math. **2**, 181–186 (1971).
6. Kuipers, L. and J.-S. Shiue – A distribution property of the sequence of Fibonacci numbers, Fibonacci Quart. **10**, 375–376, 392 (1972).
7. Kuipers, L. and J.-S. Shiue – A distribution property of the sequence of Lucas numbers, Elemente der Math. **27**, 10–11 (1972).
8. Kuipers, L. and J.-S. Shiue – A distribution property of a linear recurrence of the second order, Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. (8) **52**, 6–10 (1972).
9. Lausch, H. and W. Nöbauer – Algebra of Polynomials, North-Holland, Amsterdam (1973).
10. Nathanson, M. B. – Linear recurrences and uniform distribution, Proc. Amer. Math. Soc. **48**, 289–291 (1975).
11. Niederreiter, H. – Distribution of Fibonacci numbers mod 5^k, Fibonacci Quart. **10**, 373–374 (1972).
12. Niederreiter, H. – On the cycle structure of linear recurring sequences, Math. Scand. **38**, 53–77 (1976).

13. Niederreiter, H. – Weights of cyclic codes, Information and Control 34, 130–140 (1977).
14. Selmer, E. S. – Linear Recurrence Relations over Finite Fields, mimeographed notes, Univ. of Bergen (1966).
15. Shiue, J.-S. – A remark on a paper by Bundschuh, Tamkang J. Math. 4, 129–130 (1973).
16. Shiue, J.-S. and M.-H. Hu – Some remarks on the uniform distribution of a linear recurrence of the second order, Tamkang J. Math. 4, 101–103 (1973).
17. Webb, W. A. and C. T. Long – Distribution modulo p^h of the general linear second order recurrence, Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. (8) 58, 92–100 (1975).
18. Zierler, N. – Linear recurring sequences, J. Soc. Industr. Appl. Math. 7, 31–48 (1959).