ACTA ARITHMETICA
XXXVIII (1980)

Equidistribution of linear recurring sequences in finite fields, II

by

HARALD NIEDERREITER (Kingston, Jamaica) and
JAU-SHYONG SHIUE (Taipei, Taiwan)

1. Introduction. 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

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

where $A(c, N) = A(c, N, (x_n))$ denotes the number of n, $0 \leqslant n \leqslant N-1$, for which $x_n = c$ (see [3] and [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).

We are interested in characterizing those u.d. sequences in F_q satisfying a linear recurrence relation. For linear recurrences of order 2 and 3, this has been carried out in [7]. In the present paper, we give the details for the case of fourth-order linear recurrences. The discussion becomes increasingly complex and technical for higher-order linear recurring sequences, although in principle the methods developed so far should be quite adequate.

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

$$(1) \qquad u_{n+k} = a_{k-1}u_{n+k-1} + \ldots + a_1 u_{n+1} + a_0 u_n \quad \text{for} \quad n = 0, 1, \ldots,$$

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 (1) 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 (1) is called the *minimal polynomial* of (u_n). For the zero sequence, which satisfies any linear recurrence relation, one sets $m(x) = 1$. It was shown in [7] that for the purpose of investigating the equidistribution of linear recurring sequences, it suffices to consider minimal polynomials $m(x)$ satisfying $m(0) \neq 0$ and having at least one multiple root.

2. Auxiliary results. In Lemma 1 below, we collect some standard facts about linear recurring sequences in finite fields (see [8], [9]). For a field F, we denote by F^* the multiplicative group of nonzero elements of F.

LEMMA 1. *Let $m(x) = (x-\alpha_1)^{r_1} \dots (x-\alpha_s)^{r_s}$ be the canonical factorization of $m(x)$ in a suitable finite extension E of F_q, so that $\alpha_1, \dots, \alpha_s$ are distinct 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 least common multiple of the orders of $\alpha_1, \dots, \alpha_s$ in E^* and p^t is the smallest integral power of p with $p^t \geqslant r = \max(r_1, \dots, r_s)$. Furthermore, if $r \leqslant p$, then the terms of (u_n) are given explicitly by*

$$u_n = \sum_{j=1}^{s} Q_j(n)\alpha_j^n \quad for \quad n = 0, 1, \dots, \tag{2}$$

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

Since F_q is of characteristic p, we can write $q = p^f$ with an integer $f \geqslant 1$. The subsequent necessary condition for the equidistribution of (u_n) was established in [7].

LEMMA 2. *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 1.*

We shall also use the following criteria for equidistribution which were shown in [7].

LEMMA 3. *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 4. *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*

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

3. Fourth-order recurrences. We consider now linear recurring sequences with a minimal polynomial $m(x)$ of degree 4. As we have already observed in Section 1, we may assume that $m(0) \neq 0$ and that $m(x)$ has at least one multiple root. We have to distinguish four cases depending on the form of the canonical factorization of $m(x)$. The corresponding criteria for equidistribution are enunciated in Theorems 1, 2, 3, and 4.

THEOREM 1. *Let (u_n) be a linear recurring sequence in F_q with minimal polynomial $m(x) = (x-\alpha)^2(x-\beta)(x-\gamma)$, where $\alpha \in F_q^*$, $\beta, \gamma \in F_{q^2}^*$, and α, β, γ are distinct. Then (u_n) is u.d. in F_q if and only if q is prime.*

Proof. This is a special case of [7], Theorem 1.

THEOREM 2. *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*

$$[\alpha^2\beta u_0 - (\alpha^2 + 2\alpha\beta)u_1 + (2\alpha+\beta)u_2 - u_3] \times \\ \times [-\alpha\beta^2 u_0 + (2\alpha\beta + \beta^2)u_1 - (\alpha + 2\beta)u_2 + u_3]^{-1} \in F_{q^2} \tag{3}$$

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

Proof. In the notation of Lemma 1, we have $r = 2$, and so $t = 1$. By Lemma 2, (u_n) can only be u.d. in F_q if $q = p$. Then (u_n) has period ep, where e is as in Lemma 1, and by (2) we obtain

$$u_n = (c_0 + c_1 n)\alpha^n + (c_2 + c_3 n)\beta^n \quad \text{for all } n \geqslant 0, \tag{4}$$

where $c_0, c_1, c_2, c_3 \in F_{p^2}$. We have $c_1 \neq 0$ and $c_3 \neq 0$, for otherwise (u_n) would satisfy a linear recurrence relation of lower order. For $n \geqslant 0$ and $j \geqslant 0$ we get

$$u_{n+je} = (c_0 + c_1 n + c_1 je)\alpha^n + (c_2 + c_3 n + c_3 je)\beta^n = u_n + je(c_1\alpha^n + c_3\beta^n). \tag{5}$$

It is a consequence of the definition of e that p does not divide e. It follows then from (5) that $c_1\alpha^n + c_3\beta^n \in F_p$ for all $n \geqslant 0$.

Now suppose that $c_1\alpha^n + c_3\beta^n \neq 0$ for all $n \geqslant 0$. Then for each fixed n, $0 \leqslant n \leqslant e-1$, the finite sequence (u_{n+je}), $j = 0, 1, \dots, p-1$, runs exactly once through F_p because of $e(c_1\alpha^n + c_3\beta^n) \neq 0$ and (5). Therefore, among the first ep terms of (u_n) each element of F_p appears e times, and since ep is the period of (u_n), the sequence is u.d. in F_p.

On the other hand, suppose that $c_1\alpha^{n_0} + c_3\beta^{n_0} = 0$ for some $n_0 \geqslant 0$. Then $-c_3c_1^{-1} = (\alpha\beta^{-1})^{n_0}$, and if e' denotes the order of $\alpha\beta^{-1}$ in $F_{p^2}^*$, then e' divides e and there are e/e' values of n, $0 \leqslant n \leqslant e-1$, with $(\alpha\beta^{-1})^n = -c_3c_1^{-1}$. For these values of n, the terms u_{n+je}, $j = 0, 1, \dots, p-1$, are all equal to u_n by (5). Since p does not divide e/e', not all elements of F_p appear equally often among these u_n. For the other values of n with $0 \leqslant n \leqslant e-1$, the finite sequence (u_{n+je}), $j = 0, 1, \dots, p-1$, runs exactly once through F_p. Altogether, among the first ep terms of (u_n) not all elements of F_p appear equally often, and so (u_n) is not u.d. in F_p.

Hence, (u_n) is u.d. in F_p if and only if $-c_3c_1^{-1}$ is not a power of $\alpha\beta^{-1}$. By using (4) for $n = 0, 1, 2, 3$, we obtain a system of linear equations for c_0, c_1, c_2, c_3, which allows us to express these elements in terms of $u_0, u_1,$

u_2, u_3. As a result of this calculation,

$$-c_3c_1^{-1} = \alpha\beta^{-1}[\alpha^2\beta u_0-(\alpha^2+2\alpha\beta)u_1+(2\alpha+\beta)u_2-u_3]\times$$
$$\times[-\alpha\beta^2u_0+(2\alpha\beta+\beta^2)u_1-(\alpha+2\beta)u_2+u_3]^{-1},$$

and so $-c_3c_1^{-1}$ is not a power of $\alpha\beta^{-1}$ if and only if the element in (3) is not a power of $\alpha\beta^{-1}$.

Remark 1. The method in the proof of Theorem 2 can also be applied to a linear recurring sequence (u_n) with a minimal polynomial $m(x)$ of the form $m(x) = (x-\alpha)^2(x-\beta)^2(x-\gamma_1)\dots(x-\gamma_s)$, where $\alpha, \beta, \gamma_1, \dots, \gamma_s$ are distinct nonzero elements of a suitable finite extension E of F_q. Then

$$u_n = (c_0+c_1n)\alpha^n+(c_2+c_3n)\beta^n+d_1\gamma_1^n+\dots+d_s\gamma_s^n \quad \text{for all } n\geq 0,$$

with coefficients in E, and the above argument shows that (u_n) is u.d. in F_q if and only if q is prime and $-c_3c_1^{-1}$ is not a power of $\alpha\beta^{-1}$.

Theorem 3. *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 $p\geq 3$, then (u_n) is u.d. in F_q if and only if $q = p$, a is not a square in F_p, and*

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

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

$$(6)\qquad v = 8a^2[(3a^2b-3ab^2+b^3)u_0-3a^2u_1+3au_2-u_3][a^2bu_0-$$
$$-(a^2+2ab)u_1+(2a+b)u_2-u_3]-$$
$$-[(-5a^3b+3a^2b^2)u_0+(5a^3+5a^2b-4ab^2)u_1+$$
$$+(-8a^2+ab+b^2)u_2+(3a-b)u_3]^2$$

and

$$(7)\qquad w = 8a^2[a^2bu_0-(a^2+2ab)u_1+(2a+b)u_2-u_3]\times$$
$$\times(-a^3u_0+3a^2u_1-3au_2+u_3).$$

If $p = 2$, then (u_n) is u.d. in F_q if and only if $q = 4$ and either

(i) $a = 1$, $b\notin F_2$, and (u_n) is obtained from one of the two sequences $0, 0, 0, 1, 1+b, 1, b, b, b, 1+b, 1, 1+b, \dots$ and $0, 1, 0, b, b, b, 1, 0, 1, 1+b, 1+b, 1+b, \dots$ of period 12 by multiplying by an element of F_4^* and shifting; or

(ii) $a\notin F_2$, $b = 1$, and (u_n) is obtained from one of the two sequences $0, 0, 0, 1, 1+a, 1+a, 1+a, 1, a, a, a, 1, \dots$ and $0, 1, 0, a, 1+a, 1, 1+a, 0, a, 1, a, 1+a, \dots$ of period 12 by multiplying by an element of F_4^* and shifting; or

(iii) $a\notin F_2$, $b = 1+a$, and (u_n) is obtained from one of the two sequences $0, 0, 0, 1, 1, b, a, b, 1, b, a, a, \dots$ and $0, 1, 0, 1, a, b, b, 0, a, a, b, 1, \dots$ of period 12 by multiplying by an element of F_4^* and shifting.

Proof. In the notation of Lemma 1, we have $r = 3$. Thus, if $p\geq 3$, then $t = 1$, and so $q = p$ is a necessary condition for the equidistribution of (u_n) in F_q because of Lemma 2. Furthermore, (u_n) has period ep, where e is as in Lemma 1, and by (2) we obtain

$$(8)\qquad u_n = (c_0+c_1n+c_2n^2)a^n+c_3b^n \quad \text{for all } n\geq 0,$$

where $c_0, c_1, c_2, c_3 \in F_p$. We have $c_2\neq 0$ and $c_3\neq 0$, for otherwise (u_n) would satisfy a linear recurrence relation of lower order. We note that (u_n) is u.d. in F_p if and only if $(v_n) = (4c_2u_n)$ is u.d. in F_p. Now

$$v_n = 4c_2u_n = \big((2c_2n+c_1)^2+4c_0c_2-c_1^2\big)a^n+4c_2c_3b^n \quad \text{for all } n\geq 0.$$

For $n\geq 0$ and $j\geq 0$ we get

$$v_{n+je} = \big((2c_2n+2c_2je+c_1)^2+4c_0c_2-c_1^2\big)a^n+4c_2c_3b^n$$
$$= (2c_2ej+2c_2n+c_1)^2a^n+w_n$$

with

$$w_n = (4c_0c_2-c_1^2)a^n+4c_2c_3b^n.$$

Now let χ be a nontrivial additive character of F_p. Then,

$$(9)\qquad \sum_{n=0}^{ep-1}\chi(v_n) = \sum_{n=0}^{e-1}\sum_{j=0}^{p-1}\chi(v_{n+je}) = \sum_{n=0}^{e-1}\chi(w_n)\sum_{j=0}^{p-1}\chi\big((2c_2ej+2c_2n+c_1)^2a^n\big).$$

If a is a square in F_p, then each inner sum in the last expression is equal to the Gaussian sum $G(\chi) = \sum_{j=0}^{p-1}\chi(j^2)$, and so

$$\sum_{n=0}^{ep-1}\chi(v_n) = G(\chi)\sum_{n=0}^{e-1}\chi(w_n).$$

It is well known that $G(\chi)\neq 0$ ([1], Ch. 2). Also, (w_n) cannot be u.d. in F_p since it has a period $e<p$. Therefore, by Lemma 3, there exists a nontrivial χ with $\sum_{n=0}^{e-1}\chi(w_n)\neq 0$. For this χ we have then $\sum_{n=0}^{ep-1}\chi(v_n)\neq 0$, and so, by Lemma 3, (v_n) is not u.d. in F_p. Therefore, (v_n) can only be u.d. in F_p if a is a nonsquare in F_p. Then the order of a in F_p^* is even, and so e is even. Now consider the last expression in (9). For even n, the inner sum is equal to $G(\chi)$; for odd n, the inner sum is $\sum_{j=0}^{p-1}\chi(aj^2) = -G(\chi)$. Thus,

$$\sum_{n=0}^{ep-1}\chi(v_n) = G(\chi)\Big(\sum_{n=0}^{(e/2)-1}\chi(w_{2n})-\sum_{n=0}^{(e/2)-1}\chi(w_{2n+1})\Big).$$

Since $G(\chi) \neq 0$, it follows from Lemma 3 that (v_n) is u.d. in F_p if and only if

$$(10) \qquad \sum_{n=0}^{(e/2)-1} \chi(w_{2n}) = \sum_{n=0}^{(e/2)-1} \chi(w_{2n+1})$$

for all nontrivial additive characters χ of F_p. Now set

$$x_n = w_{2n} = \zeta a^{2n} + \sigma b^{2n}, \qquad y_n = w_{2n+1} = (a\zeta) a^{2n} + (b\sigma) b^{2n}$$

for $n \geqslant 0$, where $\zeta = 4c_0c_2 - c_1^2$ and $\sigma = 4c_2c_3$. Because of [7], Lemmas 1 and 2, and $0 \leqslant A\big(c, e/2, (x_n)\big), A\big(c, e/2, (y_n)\big) \leqslant e/2 < p$ for all $c \in F_p$, (10) is equivalent to

$$(11) \qquad \sum_{n=0}^{(e/2)-1} x_n^j = \sum_{n=0}^{(e/2)-1} y_n^j \quad \text{for} \quad 1 \leqslant j \leqslant p-1.$$

Now for each j, $1 \leqslant j \leqslant p-1$, we have

$$\sum_{n=0}^{(e/2)-1} x_n^j = \sum_{n=0}^{(e/2)-1} (\zeta a^{2n} + \sigma b^{2n})^j = \sum_{n=0}^{(e/2)-1} \sum_{i=0}^{j} \binom{j}{i} \zeta^i \sigma^{j-i} a^{2in} b^{2(j-i)n}$$

$$= \sum_{i=0}^{j} \binom{j}{i} \zeta^i \sigma^{j-i} \sum_{n=0}^{(e/2)-1} (a^{2i} b^{2j-2i})^n = (e/2) \sum_{i=0}^{j}{}' \binom{j}{i} \zeta^i \sigma^{j-i},$$

where the dash indicates that only those i with $a^{2i}b^{2j-2i} = 1$ are considered. By replacing ζ by $a\zeta$ and σ by $b\sigma$, we get

$$\sum_{n=0}^{(e/2)-1} y_n^j = \frac{e}{2} \sum_{i=0}^{j}{}' \binom{j}{i} a^i b^{j-i} \zeta^i \sigma^{j-i}.$$

Therefore, (11) is equivalent to the requirement that

$$\sum_{i=0}^{j}{}' \binom{j}{i} (1 - a^i b^{j-i}) (\zeta\sigma^{-1})^i = 0 \quad \text{for} \quad 1 \leqslant j \leqslant p-1.$$

From the restriction on i, namely $a^{2i}b^{2j-2i} = 1$, it follows that $a^i b^{j-i} = \pm 1$, and so (11) is equivalent to the condition

$$(12) \qquad \sum_{i=0}^{j}{}^{*} \binom{j}{i} (\zeta\sigma^{-1})^i = 0 \quad \text{for} \quad 1 \leqslant j \leqslant p-1,$$

where the asterisk indicates that only those i with $b^j = -(ba^{-1})^i$ are considered.

We determine now for which j there can exist an i with $b^j = -(ba^{-1})^i$. First let the order e_1 of ba^{-1} in F_p^* be even. Then -1 is a power of ba^{-1}, and so b^j should be in the cyclic subgroup H_1 of F_p^* generated by ba^{-1}.

Let H_2 be the cyclic subgroup of F_p^* generated by b. Then $\mathrm{card}(H_1) = e_1$, $\mathrm{card}(H_2) = e_2$, and since F_p^* is cyclic, $\mathrm{card}(H_1 \cap H_2) = \text{g.c.d.}\,(e_1, e_2)$. Therefore the condition on j becomes $j \equiv 0 \big(\mathrm{mod}\, e_2/\text{g.c.d.}\,(e_1, e_2)\big)$, or $j \equiv 0 \equiv e_3/2 \,(\mathrm{mod}\, e_3/e_1)$ because $e_3 = \text{l.c.m.}\,(e_1, e_2)$. Now let e_1 be odd. Then e_2 is even since the order of a in F_p^* is even. Let H_3 be the subgroup of F_p^* generated by -1 and ba^{-1}. Then $\mathrm{card}(H_3) = 2e_1$, and so $\mathrm{card}(H_2 \cap H_3) = \text{g.c.d.}\,(e_2, 2e_1) = 2\text{g.c.d.}\,(e_1, e_2)$. Thus necessarily we have $j \equiv 0 \big(\mathrm{mod}\, e_2/2\text{g.c.d.}\,(e_1, e_2)\big)$. But we also have $b^j \notin H_1$, for otherwise $-1 \in H_1$, contradicting the oddness of e_1. By the case considered earlier, $b^j \notin H_1$ is equivalent to $j \not\equiv 0 \big(\mathrm{mod}\, e_2/\text{g.c.d.}\,(e_1, e_2)\big)$, and so $j \equiv e_2/2\text{g.c.d.}\,(e_1, e_2) \big(\mathrm{mod}\, e_2/\text{g.c.d.}(e_1, e_2)\big)$, or $j \equiv e_3/2e_1 \equiv e_3/2 \,(\mathrm{mod}\, e_3/e_1)$.

If j is fixed, then the corresponding values of i with $(ba^{-1})^i = -b^j$ run through the arithmetic progression $i \equiv h_j \,(\mathrm{mod}\, e_1)$. The element $\zeta\sigma^{-1}$ appearing in (12) can be calculated in terms of the initial values of the sequence (u_n). By using (8) for $n = 0, 1, 2, 3$, one obtains a system of linear equations for c_0, c_1, c_2, c_3. Upon solving this system and recalling that $\zeta = 4c_0c_2 - c_1^2$ and $\sigma = 4c_2c_3$, one gets $\zeta\sigma^{-1} = vw^{-1} = c$, where v and w are given by (6) and (7), respectively. This completes the discussion of the case $p \geqslant 3$.

Now let $p = 2$. Then $t = 2$, and so q can only be 2 or 4 according to Lemma 2. But $q = 2$ is impossible since a and b are distinct elements of F_q^*, and so $q = 4$. In each of the cases (i), (ii), and (iii), (u_n) has period 12, and there are 144 sequences with minimal polynomial $m(x)$. Using the fact that the equidistribution of (u_n) is invariant under shifts and under termwise multiplication by an element of F_q^*, one shows by inspection that the list of equidistributed sequences in the theorem is complete.

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 $g(x) \equiv \tilde{g}(x) \big(\mathrm{mod}\,(x^p - x)\big)$. We define the *reduced degree* of $g(x)$ to be the degree of $\tilde{g}(x)$.

THEOREM 4. *Let (u_n) be a linear recurring sequence in F_q with minimal polynomial $m(x) = (x-a)^4$, where $a \in F_q^*$. For $p \geqslant 5$, 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 $\big(f(x)\big)^{ej}$ is at most $p-2$ for each j with $1 \leqslant j < (p-1)/e$, where e is the order of a in F_p^*. If $p = 2$, then (u_n) is u.d. in F_q if and only if $q = 4$, $a \notin F_2$, and exactly one of u_0, u_1, u_2, u_3 is 0. If $p = 3$, then (u_n) is u.d. in F_q if and only if we have one of the following cases:

(i) $q = 3$;

(ii) $q = 9$, $a = 1$, *and no two of* $u_0(u_3-u_0)^{-1}$, $u_1(u_3-u_0)^{-1}$, $u_2(u_3-u_0)^{-1}$ *differ by an element of* F_3;

(iii) $q = 9$, $a \neq 1$, *and exactly one of* $a^3u_0(u_3-a^3u_0)^{-1}$, $a^2u_1(u_3-a^3u_0)^{-1}$, $au_2(u_3-a^3u_0)^{-1}$ *is in* F_3.

Proof. In the notation of Lemma 1, we have $r = 4$. Thus, if $p \geq 5$, then $t = 1$, and so Lemma 2 implies that (u_n) can be u.d. in F_q only for $q = p$. Then (u_n) has period ep and by (2) we obtain

$$u_n = (c_0 + c_1 n + c_2 n^2 + c_3 n^3)a^n \quad \text{for all } n \geq 0, \tag{13}$$

where $c_0, c_1, c_2, c_3 \in F_p$. We have $c_3 \neq 0$, for otherwise (u_n) would satisfy a linear recurrence relation of lower order. For $1 \leq j \leq p-1$ we get

$$\sum_{n=0}^{ep-1} u_n^j = \sum_{i=0}^{e-1}\sum_{n=0}^{p-1} u_{i+ne}^j = \sum_{i=0}^{e-1}\sum_{n=0}^{p-1}\big(c_0 + c_1(i+ne) + c_2(i+ne)^2 + c_3(i+ne)^3\big)^j a^{ij}$$

$$= \sum_{i=0}^{e-1}(a^j)^i \sum_{n=0}^{p-1}(c_0 + c_1 n + c_2 n^2 + c_3 n^3)^j.$$

Now

$$\sum_{i=0}^{e-1}(a^j)^i = \begin{cases} e & \text{if } e \text{ divides } j, \\ 0 & \text{otherwise.} \end{cases}$$

On account of Lemma 4, we obtain that (u_n) is u.d. in F_p if and only if

$$\sum_{n=0}^{p-1}(c_3 n^3 + c_2 n^2 + c_1 n + c_0)^{ej} = \begin{cases} 0 & \text{for } 1 \leq j < (p-1)/e, \\ -1 & \text{for } j = (p-1)/e, \end{cases}$$

or equivalently,

$$\sum_{n=0}^{p-1}(n^3 + c_2c_3^{-1}n^2 + c_1c_3^{-1}n + c_0c_3^{-1})^{ej} = \begin{cases} 0 & \text{for } 1 \leq j < (p-1)/e, \\ -1 & \text{for } j = (p-1)/e. \end{cases}$$

By using (13) with $n = 0, 1, 2, 3$, one can express c_0, c_1, c_2, c_3 in terms of u_0, u_1, u_2, u_3, and this calculation leads to $c_h c_3^{-1} = d_h$ for $h = 0, 1, 2$. Therefore, (u_n) is u.d. in F_p if and only if

$$\sum_{n=0}^{p-1}\big(f(n)\big)^{ej} = \begin{cases} 0 & \text{for } 1 \leq j < (p-1)/e, \\ -1 & \text{for } j = (p-1)/e. \end{cases} \tag{14}$$

For $j = (p-1)/e$, condition (14) is equivalent to saying that $f(x)$ has exactly one root in F_p. For $1 \leq j < (p-1)/e$, let $\tilde{g}_j(x) \in F_p[x]$ be the unique polynomial of degree at most $p-1$ with $\big(f(x)\big)^{ej} \equiv \tilde{g}_j(x) \pmod{x^p - x}$. Then $\big(f(n)\big)^{ej} = \tilde{g}_j(n)$ for all $n \geq 0$, and so $\sum_{n=0}^{p-1}\big(f(n)\big)^{ej} = \sum_{n=0}^{p-1}\tilde{g}_j(n)$. The last sum is equal to 0 if and only if the coefficient of x^{p-1} in $\tilde{g}_j(x)$ is 0 (compare with [5], p. 191, Lemma 8.24, and [7], eq. (2)), i.e., if and only if the reduced degree of $\big(f(x)\big)^{ej}$ is at most $p-2$. This completes the discussion of the case $p \geq 5$.

If $p = 2$, then $t = 2$, and so q can only be 2 or 4 according to Lemma 2. If $q = 2$, then $m(x) = (x-1)^4$, and one shows by inspection that none of the 8 sequences with this minimal polynomial is u.d. in F_2. If $q = 4$ and $m(x) = (x-1)^4$, then (u_n) has period 4, and so (u_n) is u.d. in F_4 exactly if u_0, u_1, u_2, u_3 are distinct. But then $u_0 + u_1 + u_2 + u_3 = 0$, and (u_n) satisfies the linear recurrence relation $u_{n+3} = u_{n+2} + u_{n+1} + u_n$ of order 3, a contradiction. If $q = 4$ and $a \notin F_2$, then (u_n) satisfies $u_{n+4} = au_n$ for all $n \geq 0$ and has period 12. Thus it is easily seen that (u_n) is u.d. in F_4 if and only if exactly one of u_0, u_1, u_2, u_3 is 0.

If $p = 3$, then $t = 2$, and so q can only be 3 or 9 according to Lemma 2. If $q = 3$ and $a = 1$, then $u_{n+4} = u_{n+3} + u_{n+1} - u_n$ for all $n \geq 0$ and (u_n) has period 9. Furthermore, $d = u_3 - u_0 \neq 0$, for otherwise (u_n) would satisfy $u_{n+3} = u_n$ for all $n \geq 0$. The terms in the full period are

$$u_0,\ u_1,\ u_2,\ u_0+d,\ u_1+d,\ u_2+d,\ u_0-d,\ u_1-d,\ u_2-d. \tag{15}$$

Since $\{b, b+d, b-d\} = F_3$ for all $b \in F_3$, the sequence (u_n) is always u.d. in F_3. If $q = 3$ and $a = -1$, then $u_{n+4} = -u_{n+3} - u_{n+1} - u_n$ for all $n \geq 0$ and (u_n) has period 18. Furthermore, $d = u_3 + u_0 \neq 0$, for otherwise (u_n) would satisfy $u_{n+3} = -u_n$ for all $n \geq 0$. The terms in the full period are $u_0, u_1, u_2, -u_0+d, -u_1-d, -u_2+d, u_0+d, u_1-d, u_2+d, -u_0, -u_1, -u_2, u_0-d, u_1+d, u_2-d, -u_0-d, -u_1+d, -u_2-d$. By considering every sixth term, it is seen as above that (u_n) is always u.d. in F_3.

Now let $q = 9$ and $a = 1$. Then the terms in the full period are again given by (15), and (u_n) is u.d. in F_9 if and only if the terms in (15) run exactly through all elements of F_9. This is equivalent to the condition that no two of u_0, u_1, u_2 differ by d, $-d$, or 0, and so equivalent to the condition in the theorem. For $a \neq 1$, consider the matrix

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -a^4 & a^3 & 0 & a \end{pmatrix}$$

associated with the minimal polynomial $m(x) = (x-a)^4$ (compare with [6], Section 2). Then

$$A^9 = \begin{pmatrix} a & 0 & 0 & 0 \\ 0 & a & 0 & 0 \\ 0 & 0 & a & 0 \\ 0 & 0 & 0 & a \end{pmatrix},$$

and so

$$u_{n+9} = au_n \quad \text{for all } n \geqslant 0 \tag{16}$$

according to [6], eq. (3). Furthermore, $d = u_3 - a^3 u_0 \neq 0$, for otherwise (u_n) would satisfy $u_{n+3} = a^3 u_n$ for all $n \geqslant 0$. The sequence (u_n) is u.d. in F_9 precisely if $(u_n d^{-1})$ is u.d. in F_9. The first nine terms of $(u_n d^{-1})$ are easily calculated to be

$$u_0 d^{-1}, \quad u_1 d^{-1}, \quad u_2 d^{-1}, \quad a^3 u_0 d^{-1} + 1, \quad a(a^2 u_1 d^{-1} + 1),$$
$$a^2(au_2 d^{-1} + 1), \quad a^3(a^3 u_0 d^{-1} - 1), \quad a^4(a^2 u_1 d^{-1} - 1), \quad a^5(au_2 d^{-1} - 1).$$

Because of (16) we get all terms in the full period by multiplying these nine terms by all powers a^j, $0 \leqslant j \leqslant e-1$. The terms thus generated may be described as follows: take $a^3u_0d^{-1}$, $a^3u_0d^{-1}+1$, $a^3u_0d^{-1}-1$, $a^2u_1d^{-1}$, $a^2u_1d^{-1}+1$, $a^2u_1d^{-1}-1$, au_2d^{-1}, $au_2d^{-1}+1$, $au_2d^{-1}-1$ and multiply them by all powers a^j, $0 \leqslant j \leqslant e-1$. Then it is clear that exactly one of $a^3u_0d^{-1}$, $a^2u_1d^{-1}$, au_2d^{-1} must belong to F_3, for otherwise 0 would occur either not at all or too frequently. Conversely, suppose exactly one of these three elements is in F_3. Since $a \in F_9$ and $a \neq 1$, we have

$$\{a^j\colon 0 \leqslant j \leqslant e-1\} = \{\pm a^j\colon 0 \leqslant j \leqslant (e/2)-1\}.$$

Therefore, the terms in the full period of $(u_n d^{-1})$ can be produced by taking the 18 elements $\pm b$, $\pm b \pm 1$, with $b = a^3u_0d^{-1}$, $a^2u_1d^{-1}$, and au_2d^{-1}, and multiplying them by the powers a^j, $0 \leqslant j \leqslant (e/2)-1$. Now if $b \in F_3$, then $\pm b$, $\pm b \pm 1$ run exactly twice through F_3, and if $b \notin F_3$, then $\pm b$, $\pm b \pm 1$ run exactly once through $F_9 \setminus F_3$. Therefore, by the given hypothesis, the above 18 elements run exactly twice through F_9. After multiplying by all a^j, $0 \leqslant j \leqslant (e/2)-1$, the resulting terms in the full period of $(u_n d^{-1})$ will run exactly e times through F_9, and so $(u_n d^{-1})$ is u.d. in F_9.

Remark 2. If $p \equiv 1 \pmod 3$ and a is a cube in F_p, then (u_n) is not u.d. in F_p. To see this, we note that $a^{(p-1)/3} = 1$, and so e divides $(p-1)/3$. Then we can choose $j = (p-1)/3e$ in Theorem 4 to get $(f(x))^{ej} = (x^3 + d_2x^2 + d_1x + d_0)^{(p-1)/3}$, which has leading term x^{p-1}. Thus, the condition in the theorem is not satisfied.

Remark 3. If $p \geqslant 5$ and $f(x)$ is the cube of a linear polynomial, then (u_n) is u.d. in F_p if and only if either (i) $p \equiv 2 \pmod 3$; or (ii) $p \equiv 1 \pmod 3$ and a is not a cube in F_p. For if $f(x) = (x-b)^3$ with $b \in F_p$ and $p \equiv 2 \pmod 3$, and if (u_n) were not u.d. in F_p, then according to (14) there would exist j, $1 \leqslant j < (p-1)/e$, with $\sum_{n=0}^{p-1}(n-b)^{3ej} = \sum_{n=0}^{p-1} n^{3ej} \neq 0$. But this is only possible if $p-1$ divides $3ej$. Since $p-1 \equiv 1 \pmod 3$, it would follow that $p-1$ divides ej, a contradiction. If $p \equiv 1 \pmod 3$ and (u_n) is not u.d. in F_p, then we have again $\sum_{n=0}^{p-1} n^{3ej} \neq 0$ for some j with $1 \leqslant j < (p-1)/e$. It follows that $p-1$ divides $3ej$, and so $3ej$ can only be $p-1$ or $2(p-1)$. In either case, e divides g.c.d. $(p-1, 2(p-1)/3) = (p-1)/3$, hence $a^{(p-1)/3} = 1$, and so a is a cube in F_p. An application of Remark 2 completes the proof.

Remark 4. If $p \geqslant 5$ and $a = 1$, then (u_n) is u.d. in F_p if and only if $f(x) = x^3 + d_2x^2 + d_1x + d_0$ is a permutation polynomial over F_p (compare with [5], Ch. 4, Sect. 8). According to a result of Dickson [2], the cubic polynomial $f(x)$ is a permutation polynomial over F_p if and only if $p \equiv 2 \pmod 3$ and $f(x)$ is of the form $f(x) = (x-b)^3 + c$ with $b, c \in F_p$.

References

[1] H. Davenport, *Multiplicative number theory*, Chicago 1967.

[2] L. E. Dickson, *Analytic functions suitable to represent substitutions*, Amer. J. Math. 18 (1896), pp. 210–218.

[3] L. Gotusso, *Successioni uniformemente distribuite in corpi finiti*, Atti Sem. Mat. Fis. Univ. Modena 12 (1962/63), pp. 215–232.

[4] L. Kuipers and H. Niederreiter, *Uniform distribution of sequences*, New York 1974.

[5] H. Lausch and W. Nöbauer, *Algebra of polynomials*, Amsterdam 1973.

[6] H. Niederreiter, *On the cycle structure of linear recurring sequences*, Math. Scand. 38 (1976), pp. 53–77.

[7] H. Niederreiter and J.-S. Shiue, *Equidistribution of linear recurring sequences in finite fields*, Indagationes Math. 80 (1977), pp. 397–405.

[8] E. S. Selmer, *Linear recurrence relations over finite fields*, Bergen 1966.

[9] N. Zierler, *Linear recurring sequences*, J. Soc. Industr. Appl. Math. 7 (1959), pp. 31–48.

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF THE WEST INDIES
Kingston 7
Jamaica

DEPARTMENT OF MATHEMATICAL SCIENCES
NATIONAL CHENGCHI UNIVERSITY
Taipei
Taiwan, Republic of China

Received on 7. 3. 1978 (1049)