PROJECTIVE MAPS OF LINEAR RECURRING SEQUENCES WITH MAXIMAL *p-adic* PERIODS

Huang Minqiang
Institute of Systems Science, Academia Sinica, PRC

Dai Zongduo
Graduate School of USTC, Academia Sinica, PRC

(Submitted June 1990)

1. Introduction

Let $\alpha = \sum_{i \geq 0} p_i \alpha^i$ be the *p-adic* expansion of an n^{th}-order linear recurring sequence α of rational (or *p-adic*) integers. In this paper the projective map $\phi_d \colon \alpha \to \alpha_{d-1}$ is shown to be injective modulo p^d for linear sequences having maximal modulo p^d periods.

Let R be the ring of rational (or *p-adic*) integers, p a prime number. For a polynomial $f(x) = \sum_{i=0}^{n} c_i x^i \in R[x]$ and a sequence α over R, define the operation

$$f(x)\alpha = \sum_{i=0}^{n} c_i \mathrm{L}^i \alpha$$

where L is the left-shift operator of sequences. α is said to be an n^{th}-order linear recurring sequence modulo p^d [or over $R_d = R/(p^d)$] generated by $f(x)$ if $f(x)$ is monic and $f(x)\alpha \equiv 0 \pmod{p^d}$. It is well known ([3], [4], [6], [7]) that the residue sequence $\alpha \bmod p^d$ is ultimately periodic with the period

$$\text{(1)} \qquad \operatorname{per}(\alpha)_{p^d} \leq p^{d-1}(p^n - 1).$$

Definition: An n^{th}-order linear sequence α attaining the upper bound in (1) is said to be primitive over R_d. Furthermore, α is primitive over R if it is primitive over R_d for all $d \geq 2$.

The arithmetical properties of this special class of sequences have been studied in [1], [2], [3], and [6]. Write α in its *p-adic* form

$$\alpha = \alpha_0 + p\alpha_1 + p^2\alpha_2 + \cdots,$$

where the α_i's are p-ary sequences, and consider the d^{th} projective map

$$\phi_d \colon \alpha \to \alpha_{d-1}.$$

The purpose of this paper is to prove that ϕ_d is a modulo p^d injection on the set of $f(x)$-generated R_d-primitive sequences. More precisely, our main result is

Theorem 1: Suppose α and α' are n^{th}-order primitive sequences generated by $f(x)$ over R_d. Then $\alpha_{d-1} = \alpha'_{d-1}$ if and only if $\alpha \equiv \alpha' \pmod{p^d}$.

The proof is given in Sections 3 and 4.

2. Primitive Sequences and Polynomials over R_d

For a monic polynomial $f(x) \in R[x]$, define its modulo p^d period as follows

$$\operatorname{per}(f(x))_{p^d} = \min\{t > 0 \mid x^t \equiv 1 \bmod (f(x), p^d)\}.$$

Let $T = \operatorname{per}(f(x))_p$. By definition, there is an $h(x) \in R[x]$ so that

$$\text{(2)} \qquad x^T \equiv 1 + ph_1(x) \pmod{f(x)}.$$

For $i \geq 1$, let

$$(3) \qquad h_{i+1}(x) = \sum_{i \leq r \leq p} \binom{p}{r} p^{ri-i-1} h_i(x)^r.$$

It follows immediately that

$$(4) \qquad x^{p^{i-1}T} \equiv 1 + p^i h_i(x) \pmod{f(x)}, \quad 1 \leq i \leq d,$$

which implies

$$(5) \qquad \mathrm{per}(f(x))_{p^i} \mid p^{i-1}T \leq p^{i-1}(p^n - 1), \quad 1 \leq i \leq d.$$

Similar to the case of sequences, $f(x)$ is said to be primitive over R_d if

$$\mathrm{per}(f(x))_{p^d} = p^{d-1}(p^n - 1).$$

By (4) and (5), this is clearly equivalent to the fact that $f(x)$ is primitive over $GF(p)$ (i.e., $T = p^n - 1$) where $GF(p)$ denotes the finite field of order p, a prime, and

$$(6) \qquad h_i(x) \not\equiv 0 \bmod (f(x), p), \quad 1 \leq i < d.$$

By the inductive definition of $h_i(x)$, when $i \geq 2$ we have

$$(7) \qquad h_i(x) \equiv \begin{cases} h_1(x) \bmod (p, f(x)), & \text{if } p \geq 3, \\ h_2(x) \equiv h_1(x) + h_1(x)^2 \bmod (2, f(x)), & \text{if } p = 2. \end{cases}$$

Therefore, (6) is equivalent to

$$(8) \qquad h_1(x) \not\equiv \begin{cases} 0, \quad \bmod (p, f(x)), & \text{if } p \geq 3, \text{ or } p = 2 \text{ and } d = 2, \\ 0, 1 \quad \bmod (2, f(x)), & \text{if } p = 2 \text{ and } d \geq 3. \end{cases}$$

An explicit criterion for $f(x)$ to be primitive over R_d is given in [2]. Ward had shown in [6] that an $f(x)$-generated linear sequence α is primitive over R_d if and only if $\alpha \not\equiv 0 \pmod{p}$ and $f(x)$ is primitive over R_d. Now assume this is the case and write

$$\alpha = \sum_{i \geq 0} \alpha_i p^i.$$

For $1 \leq i < d$, notice that $\mathrm{per}(\alpha)_{p^i} \mid \mathrm{per}(f(x))_{p^i} = p^{i-1}T$, we have

$$(9) \qquad (x^{p^{i-1}T} - 1)\alpha = (x^{p^{i-1}T} - 1)\sum_{k \geq i} \alpha_k p^k \equiv p^i (x^{p^{i-1}T} - 1)\alpha_i \pmod{p^{i+1}}.$$

On the other hand, applying (4) to α gives

$$(10) \qquad (x^{p^{i-1}T} - 1)\alpha \equiv p^i h_i(x)\alpha \pmod{p^{i+1}}.$$

From (9) and (10), we obtain the relation over $GF(p)$

$$(11) \qquad (x^{p^{i-1}T} - 1)\alpha_i = h_i(x)\alpha_0 = \begin{cases} h_1(x)\alpha_0, & \text{if } p \geq 3, \text{ or } p = 2 \text{ and } i = 1, \\ h_2(x)\alpha_0, & \text{if } p = 2 \text{ and } i \geq 2. \end{cases}$$

In what follows, discussions of p-ary sequences are over $GF(p)$.

For any $g(x) \in GF(p)[x]$, denote by $G(g(x))$ the set of sequences over $GF(p)$ generated by $g(x)$. Let $m_0 = \alpha_0$,

$$(12) \qquad m_i = (x^{p^{i-1}T} - 1)\alpha_i = h_i(x)m_0, \quad 1 \leq i < d.$$

Clearly, m_i, $i = 0, 1, \ldots$, are primitive sequences in $G(f_0(x))$. They are the key factors in our approach to proving the main theorem. The following Lemma, which will play a technical role in Sections 3 and 4, can be derived from (11) and the theory of primitive sequence products ([4, Ch. 8], [5]).

Lemma 1: (i) The product of two primitive sequences over $GF(p)$ is not zero.
(ii) Let $\lambda = \sum_{i \geq 0} p^i \lambda_i$ be any $f(x)$-generated sequence over R_d. If there is a p-ary primitive sequence $m \in G(f_0(x))$ such that

$$m\lambda_{d-1} \equiv m\lambda_{d-2} \mod G(x^T - 1),$$

then $\lambda \equiv 0 \pmod{p^{d-1}}$.

3. Proof of Theorem 1 for $p \geq 3$

Let $\rho = \sum_{i \geq 0} \rho_i p^i$ be the *p-adic* form of $\alpha' - \alpha$. We want to show that

$\alpha'_{d-1} = \alpha_{d-1}$ implies $\rho \equiv 0 \pmod{p^{d-1}}$.

Assume on the contrary that $\rho = p^e \beta$, with $0 \leq e < d - 1$ and

$$\beta = \sum_{i \geq 0} \beta_i p^i \not\equiv 0 \pmod{p}.$$

Obviously, β is generated by $f(x)$ over R_{d-e}. By (11),

$$m = (x^{p^{d-e-2}} - 1)\beta_{d-e-1}$$

is a primitive sequence generated by $f(x)$ over $GF(p)$. On the other hand, let

$$\alpha = (\alpha(t))_{t \geq 0}, \quad \alpha' = (\alpha'(t))_{t \geq 0}, \quad \beta_{d-e-1} = (\beta(t))_{t \geq 0}$$

and define the "borrow" sequence $\delta_{d-1} = (\delta(t))_{t \geq 0}$ by

$$\delta(t) = \begin{cases} 0, & \text{if } \alpha'(t) \bmod p^{d-1} \geq \alpha(t) \bmod p^{d-1}, \\ 1, & \text{otherwise.} \end{cases}$$

Then

$$\beta(t) = (\alpha'_{d-1}(t) - \alpha_{d-1}(t) - \delta(t)) \bmod p = (-\delta(t)) \bmod p = 0 \text{ or } p - 1$$

for all t. Therefore, the $GF(p)$-primitive sequence

$$m = (x^{p^{d-e-2}} - 1)\beta_{d-e-1}$$

consists of at most three elements: 0, 1, and $p - 1$. When $p \geq 5$, this is impossible because a primitive sequence contains all p elements in $GF(x)$. Now, assume $p = 3$, and write $m = (m(t))_{t \geq 0}$. From the equation

$$\beta(t + p^{d-e-2}T) - \beta(t) = m(t)$$

and the fact that $\beta(t) = 0$ or 2 for all t, we have $\beta(t) = 2$ when $m(t) = 1$, and $\beta(t) = 0$ when $m(t) = 2$. Hence,

$$m(t)\ (t) = m(t)(m(t) + 1) \text{ for all } t \geq 0,$$

or equivalently,

$$m\beta_{d-e-1} = m(m + 1). \tag{13}$$

Applying the operator $x^{p^{d-e-2}} - 1$ to both sides of (13) gives rise to $m^2 = 0$, which contradicts (i) of Lemma 1.

So Theorem 1 has been proved for $p \geq 3$.

4. Proof of Theorem 1 for $p = 2$

When $p = 2$, our main theorem is obviously equivalent.

Theorem 2: Let α and α' be as in Theorem 1. Then for $d \geq 2$,

$$\alpha_{d-1} + \alpha'_{d-1} \in G(f_0(x)) \text{ if and only if } \alpha \equiv \alpha' \pmod{2^{d-1}}.$$

The "if" part is clear. To prove the other direction, we need some preparations. Suppose $\rho = \alpha' - \alpha$ and $\omega = \alpha + \alpha'$, with 2-*adic* expansions

$$\rho = \sum_{i \geq 0} 2^i \rho_i \quad \text{and} \quad \omega = \sum_{i \geq 0} 2^i \omega_i.$$

Let $\theta_i = \alpha_i + \alpha_i'$, then over $GF(2)$ we have

(14) $\quad \omega_i = \theta_i + \gamma_i,$

(15) $\quad \rho_i = \theta_i + \delta_i$

where γ_i is the "carry" from $\alpha \bmod 2^i$ and $\alpha' \bmod 2^i$, and δ_i is the "borrow" defined by $\alpha \bmod 2^i$ and $\alpha' \bmod 2^i$. Denote by $\overline{\theta}_i$ the binary complement of θ_i, it is easily seen that

(16) $\quad \delta_i = \theta_{i-1}\alpha_{i-1} + \overline{\theta}_{i-1}\delta_{i-1},$

(17) $\quad \gamma_i = \overline{\theta}_{i-1}\alpha_{i-1} + \theta_{i-1}\gamma_{i-1}.$

Lemma 2: Suppose α and α' are $f(x)$-generated primitive sequences over R_d. If $\theta_{d-1} - G(x^T + 1)$, then

$$\theta_{d-2}m_{d-2} = \varepsilon m_{d-2}$$

where $\varepsilon = 0$ or 1. Furthermore, we have $\rho \equiv 0 \pmod{2^{d-1}}$ or $\omega \equiv 0 \pmod{2^{d-1}}$, respectively, according to $\varepsilon = 0$ or 1.

Proof: The fact that $(x^T + 1)\theta_{d-1} = 0$ implies $m_i = m_i'$ and $\theta_i \in G(x^{2^{i-1}T} + 1)$ for all $i \leq d - 1$.

If $d = 2$, we have $m_0 = m_0'$, and the conclusion holds.

Now assume $d \geq 3$. Notice that $\rho \equiv 0 \pmod 2$, and

$$\rho' = \rho/2 = \sum_{i \geq 0} 2^i \rho_{i+1}$$

is generated by $f(x)$ over R_{d-1}. From (11) it follows that

$$(x^{2^{d-3}T} + 1)\rho_{d-1} = h_{d-2}(x)\rho_1 \in G(f_0(x)).$$

On the other hand, by the observation that $\mathrm{per}(\delta_{-2}) \mid 2^{d-3}T$ and

(18) $\quad \rho_{d-1} = \theta_{d-1} + \theta_{d-2}\alpha_{d-2} + \overline{\theta}_{d-2}\delta_{d-2},$

we have

(19) $\quad (x^{2^{d-3}T} + 1)\rho_{d-1} = \theta_{d-2}(x^{2^{d-3}T} + 1)\alpha_{d-2} = \theta_{d-2}m_{d-2}.$

Therefore, $\theta_{d-2}m_{d-2} = \varepsilon m_{d-2}$ with $\varepsilon = 0$ or 1.

If $\varepsilon = 0$, i.e., $\theta_{d-2}m_{d-2} = 0$, then $\overline{\theta}_{d-2}m_{d-2} = m_{d-2}$. From (18) and (15), we can derive

$$m_{d-2}\rho_{d-1} = m_{d-2}\theta_{d-1} + m_{d-2}\delta_{d-2} \equiv m_{d-2}\rho_{d-1} \bmod G(x^T + 1)$$

which leads to $\rho \equiv 0 \pmod{2^{d-1}}$ by Lemma 1.

The case of $\varepsilon = 1$ can be shown in a similar way. The proof is thus completed.

Corollary: If $(x^T + 1)\theta_2 = 0$, then $\alpha \equiv \alpha' \pmod 4$.

Proof: Assume, on the contrary, that $\varepsilon = 1$ and $\theta_1 m_1 = m_1$. Since $m_0 = m_0'$ and $\theta_1 \in G(f_0(x))$, we have $\theta_1 = m_1$.

On the other hand, the fact that $\omega \equiv 0 \pmod 4$ and $\omega_1 = \theta_1 + m_0$ implies $\theta_1 = m_0$. Therefore

$$m_1 = \theta_1 = m_0$$

which is impossible by (12) and (8).

Now we are in a position to give an inductive proof of the remaining part of Theorem 2:

$$\theta_{d-1} \in G(f_0(x)) \text{ implies } \alpha \equiv \alpha' \pmod{2^{d-1}}.$$

The conclusions for $d = 2$ and 3 are proved above.

Suppose $d \geq 4$ and the theorem holds for $d - 1$. If it fails for d, we would have $\theta_{d-2}m_{d-2} = m_{d-2}$ and $\omega \equiv 0 \pmod{2^{d-1}}$. Consequently,

$$\omega_{d-2} = \theta_{d-2} + \gamma_{d-2} = 0,$$

$$\omega_{d-1} = \theta_{d-1} + \overline{\theta}_{d-2}\alpha_{d-2} + \theta_{d-2} \in G(f_0(x)),$$

$$m_{d-2}\omega_{d-1} = m_{d-2}\theta_{d-1} + m_{d-2} = m_{d-2}(\theta_{d-1} + m_{d-2}). \tag{20}$$

Since m_{d-2}, ω_{d-1}, and $\theta_{d-1} \in G(f_0(x))$, by Lemma 1(i), equation (20) leads to

$$\theta_{d-1} + m_{d-2} = \omega_{d-1} = \theta_{d-1} + \overline{\theta}_{d-2}\alpha_{d-2} + \theta_{d-2},$$

and hence $m_{d-2} = \theta_{d-2}\alpha_{d-2} + \theta_{d-2}$. Multiplying both sides by θ_{d-2} gives

$$m_{d-2} = \theta_{d-2}m_{d-2} = \theta_{d-2}.$$

Now we have reduced the case to $d - 1$. By the inductive assumption, we have $\rho \equiv 0 \pmod{2^{d-2}}$, and hence

$$\alpha = (\omega - \rho)/2 \equiv 0 \pmod{2^{d-3}}$$

which contradicts the fact that α is primitive over R_d and $d \geq 4$.

The theorem is thus proved.

References

1. Zongduo Dai & Minqiang Huang. "A Criterion for Primitiveness of Polynomials over $\mathbb{Z}$ mod 2^d." *Chinese Science Bulletin* (Chinese ed.) *35* (1990):1129-31 (English ed. will appear in 1990).
2. Minqiang Huang. "Maximal Period Polynomials over $\mathbb{Z}$ mod p^d." Preprint.
3. M. Hall. "An Isomorphism between Linear Recurring Sequences and Algebraic Rings." *Trans. Amer. Math. Soc. 44* (1938):196-218.
4. R. Lidl & H. Niederreiter. *Finite Fields*. Encyclopedia of Mathematics and Its Applications, Vol. 20. New York: Addison-Wesley, 1983 (now distributed by Cambridge University Press).
5. W. H. Mills & N. Zierler. "Products of Linear Recurring Sequences." *J. Algebra 27* (1973):147-57.
6. M. Ward. "The Arithmetical Theory of Linear Recurring Series." *Trans. Amer. Math. Soc. 35* (1933):600-28.
7. A. Vince. "Period of a Linear Recurrence." *Acta Arith. 39* (1981):303-11.

*****