MATHEMATICS OF COMPUTATION, VOLUME 29, NUMBER 129
JANUARY 1975, PAGES 173–180

# Continued Fractions and Linear Recurrences

By W. H. Mills

**Abstract.** Let $t_0, t_1, t_2, \cdots$ be a sequence of elements of a field $F$. We give a continued fraction algorithm for $t_0x + t_1x^2 + t_2x^3 + \cdots$. If our sequence satisfies a linear recurrence, then the continued fraction algorithm is finite and produces this recurrence.

More generally the algorithm produces a nontrivial solution of the system

$$\sum_{j=0}^{s} t_{i+j}\lambda_j, \qquad 0 \leqslant i \leqslant s-1,$$

for every positive integer $s$.

1. Let $t_0, t_1, t_2, \cdots$ be a sequence of elements of a field $F$. Set

$$T = \sum_{j=0}^{\infty} t_j x^j.$$

Let $d$ be a nonnegative integer. We say that $T^*$ is an approximation of $T$ of degree $d$ if there exist polynomials $V$ and $W$ such that $T^* = V/W$, $\deg V < d$, $\deg W \leqslant d$, $x \nmid W$, and $x^{2d} | WT - V$.

We shall give a continued fraction expansion for $xT$. This yields polynomials $V_i$, $W_i$, and integers $d_i$, $0 = d_1 < d_2 < d_3 < \cdots$, such that $(V_i, W_i) = 1$ and $V_i/W_i$ is an approximation of $T$ of degree $d_i$. Suppose $T^*$ is any approximation of $T$ of some degree $d$. Then $T^* = V_i/W_i$ for that value of $i$ such that $d_i \leqslant d < d_{i+1}$.

If the sequence of the $t_j$ satisfies a linear recurrence of degree $d$, but not one of smaller degree, then there is an $m$ such that $d_m = d$ and the linear recurrence is given by the polynomial $W_m$. In this case, $W_mT = V_m$, the continued fraction expansion, terminates at $i = m$, and we can determine $W_m$ from the first $2d$ of the $t_j$, i.e., from those $t_j$ such that $0 \leqslant j < 2d$.

Our algorithm is closely related to Zierler's version of Berlekamp's algorithm [1].

2. We consider continued fraction expansions of the form

$$\alpha = N_1 + \cfrac{1}{N_2 + \cfrac{1}{N_3 + \cdots}},$$

where $N_1, N_2, N_3, \cdots$ are elements from some field $E$. We can write

Received January 28, 1974.
*AMS (MOS) subject classifications* (1970). Primary 12C10, 10F20.

$$\alpha = N_1 + R_1, \quad 1/R_1 = N_2 + R_2, \quad 1/R_2 = N_3 + R_3, \cdots .$$

If $R_m = 0$ for some $m$, then the continued fraction terminates with $N_m$. Otherwise it is an infinite continued fraction.

In the classical case, $\alpha$ is a real number, the $N_i$ are integers, and $0 \leqslant R_i < 1$ for all $i$. We are interested in a different case.

We set

(1) $$P_0 = 1, \quad Q_0 = 0; \quad P_1 = N_1, \quad Q_1 = 1,$$

(2) $$P_i = N_i P_{i-1} + P_{i-2}, \quad i \geqslant 2,$$

and

(3) $$Q_i = N_i Q_{i-1} + Q_{i-2}, \quad i \geqslant 2.$$

It is well known, and easy to show, that

$$P_1/Q_1 = N_1, \quad P_2/Q_2 = N_1 + 1/N_2,$$
$$P_3/Q_3 = N_1 + 1/(N_2 + 1/N_3), \cdots .$$

The sequence $P_1/Q_1, P_2/Q_2, P_3/Q_3, \cdots$ converges to $\alpha$ in many cases, including the classical case.

We put

$$\Delta_i = \alpha Q_i - P_i, \quad i \geqslant 0.$$

Then we have

(4) $$\Delta_0 = -1, \quad \Delta_1 = \alpha - N_1$$

and

(5) $$\Delta_i = N_i \Delta_{i-1} + \Delta_{i-2}, \quad i \geqslant 2.$$

Clearly $R_1 = \alpha - N_1 = -\Delta_1/\Delta_0$. Since $R_{i+1} = -N_{i+1} + 1/R_i$ it follows from (5), by induction on $i$, that

(6) $$R_i = -\Delta_i/\Delta_{i-1}, \quad i \geqslant 1.$$

3. We now take $E$ to be the field of all series of the form $\Sigma_{j=k}^{\infty} a_j x^j$, where the $a_j$ are elements of the field $F$ and $k$ is a rational integer which may be negative. For convenience let $y = 1/x$. We set $\alpha = xT$ and $N_1 = 0$. Then $R_1 = \alpha = xT$. We now define the $N_i$ and $R_i$ inductively using

(7) $$1/R_{i-1} = N_i + R_i, \quad i \geqslant 2,$$

where we take $N_i$ to be a polynomial in $y$ and $x | R_i$. Thus if

$$1/R_{i-1} = \sum_{j=k}^{\infty} a_j x^j, \quad a_k \neq 0,$$

it turns out that $k < 0$ and we have

$$N_i = \sum_{j=k}^{0} a_j x^j = \sum_{u=0}^{-k} a_{-u} y^u \quad \text{and} \quad R_i = \sum_{j=1}^{\infty} a_j x^j.$$

This determines the $N_i$ and $R_i$ uniquely. If $R_m = 0$ for some $m$, then the process terminates at this point. The $P_i$, $Q_i$, and $\Delta_i$ are now determined by (1), (2), (3), (4), and (5).

We shall write $x^r \| A$ if $x^r$ divides $A$, but $x^{r+1}$ does not divide $A$. This means that $A$ is of the form $A = \Sigma_{j=r}^{\infty} a_j x^j$ with $a_r \neq 0$. Let $x^{r_i} \| R_i$, $i \geqslant 1$. If $R_m = 0$, we set $r_m = \infty$. Then $r_i \geqslant 1$ for $i \geqslant 1$. For $i \geqslant 2, N_i$ is a polynomial in $y$ of degree $r_{i-1}$. Set

$$d_i = \sum_{j=1}^{i-1} r_j. \tag{8}$$

Then we have $0 = d_1 < d_2 < d_3 < \cdots$. It follows from (1) and (3), by induction on $i$, that $Q_i$ is a polynomial in $y$ of degree $d_i$. Similarly, for $i \geqslant 2$, $P_i$ is a polynomial in $y$ of degree $d_i - r_1$. Set

$$V_i = x^{d_i - 1} P_i, \qquad W_i = x^{d_i} Q_i.$$

Then $V_i$ and $W_i$ are polynomials in $x$, deg $V_i < d_i$, and deg $W_i \leqslant d_i$. Moreover, $W_i$ has a nonzero constant term so that $x \nmid W_i$. Now

$$TW_i - V_i = x^{d_i - 1}(\alpha Q_i - P_i) = x^{d_i - 1} \Delta_i.$$

Since $\Delta_0 = -1$, (6) gives us

$$\Delta_i = (-1)^{i+1} \prod_{j=1}^{i} R_j.$$

Since $x^{r_j} \| R_j$, we have

$$x^{d_{i+1}} \| \Delta_i \tag{9}$$

by (8). Hence

$$x^{d_i + d_{i+1} - 1} \| TW_i - V_i. \tag{10}$$

Therefore, $x^{2d_i} | TW_i - V_i$ so that $V_i/W_i$ is an approximation of $T$ of degree $d_i$.

LEMMA 1. *Let $T^*$ be an approximation of $T$ of degree $d$. Let $i$ be the integer such that $d_i \leqslant d < d_{i+1}$. Then $T^* = V_i/W_i$.*

*Proof.* We have $T^* = V/W$, where $\deg W \leqslant d$, $\deg V < d$, and $x^{2d} | WT - V$. Now $d + d_i \leqslant 2d$ so that $x^{d+d_i} | WT - V$. Moreover, $d + d_i \leqslant d_i + d_{i+1} - 1$ so that $x^{d+d_i} | W_i T - V_i$ by (10). Since

$$V_i W - V W_i = W_i(WT - V) - W(W_i T - V_i),$$

we have

$$x^{d+d_i} | V_i W - V W_i.$$

Now the degree of $V_i W - VW_i$ is less than $d + d_i$. Therefore $V_i W - VW_i = 0$, so that

$$T^* = V/W = V_i/W_i.$$

LEMMA 2. *If* $V_i/W_i = V_j/W_j$, *then* $i = j$.

*Proof.* Suppose $V_i/W_i = V_j/W_j$. Then we have $V_i = VD$, $W_i = WD$, $V_j = VE$, $W_j = WE$ for suitable polynomials $V, W, D, E$ with $(V, W) = 1$. Since $x \nmid W_i$, we have $x \nmid D$ so that (10) yields

$$x^{d_i+d_{i+1}-1} \| TW - V.$$

Similarly

$$x^{d_j+d_{j+1}-1} \| TW - V.$$

Hence

$$d_i + d_{i+1} - 1 = d_j + d_{j+1} - 1.$$

Therefore, $i = j$.

LEMMA 3. $(V_i, W_i) = 1$.

*Proof.* Suppose $(V_i, W_i) = D$ where $\deg D > 0$. Then $V_i = VD$, $W_i = WD$ for suitable polynomials $V, W$ such that $x \nmid W$, $\deg W < d_i$, and $\deg V < d_i - 1$. Moreover $x \nmid D$ so that $x^{2d_i} | TW - V$. Hence $V/W$ is an approximation of $T$ of degree less than $d_i$. By Lemma 1 we have $V/W = V_j/W_j$ for some $j < i$. This contradicts Lemma 2.

LEMMA 4. *For any particular value of* $i$ *we have either* $\deg V_i = d_i - 1$ *or* $\deg W_i = d_i$.

*Proof.* Since $\deg W_1 = 0 = d_1$, we may suppose $i > 1$. If the result is false, then $V_i/W_i$ is an approximation of $T$ of degree less than $d_i$. By Lemma 1 this implies that $V_i/W_i = V_j/W_j$ for some $j < i$, which contradicts Lemma 2.

4. Let $\{t_j\} = \{t_0, t_1, \cdots, t_{n-1}\}$ be a finite sequence of elements of $F$, and set

$$T = \sum_{j=0}^{n-1} t_j x^j.$$

Let $W$ be a polynomial of degree $s$ with a nonzero constant term. Thus $W = \Sigma_{j=0}^{s} w_j x^j$, where the $w_j$ are elements of $F$, $w_0 \neq 0$, $w_s \neq 0$. The linear recurrence given by $W$ is

$$\sum_{i=0}^{s} w_i t_{k-i} = 0. \tag{11}$$

If (11) holds for a particular value $k_0$ of $k$, we say that the linear recurrence $W$ holds for $k_0$. If (11) holds for all values of $k$ for which the left side is defined, i.e., for $s \leqslant k \leqslant n-1$, then we say that the sequence $\{t_j\}$ satisfies the linear recurrence $W$.

Whenever we speak of a linear recurrence $W$ we shall mean a polynomial $W$ with a nonzero constant term. The degree of the linear recurrence is defined to be the degree of this polynomial.

In order to determine $W$, up to a multiplicative constant, we must have (11) satisfied by at least $s$ values of $k$. Hence we must have $2s \leqslant n$. Our problem is to determine whether or not the sequence $\{t_j\}$ satisfies a linear recurrence of degree $\leqslant n/2$, and if so to determine the linear recurrence of lowest degree that $\{t_j\}$ satisfies.

Let $h = [n/2]$. Thus $h$ is an integer and either $n = 2h$ or $n = 2h+1$. Let $xT$ be expanded in a continued fraction as indicated in Section 2 and Section 3. This gives us polynomials $V_i$ and $W_i$ and integers $d_i$. Let $m$ be the integer such that $d_m \leqslant h < d_{m+1}$. This is equivalent to

$$2d_m \leqslant n < 2d_{m+1}. \tag{12}$$

Now suppose that the sequence $\{t_j\}$ satisfies a linear recurrence $W$ of degree $s$, where $s \leqslant n/2$. Thus $s \leqslant h$. We suppose $W$ chosen so that $s$ is minimal. Set $V = \Sigma_{j=0}^{s-1} v_j x^j$, where

$$v_j = \sum_{i=0}^{j} w_i t_{j-i}.$$

Then $x^n | TW - V$ by (11) so that $V/W$ is an approximation of $T$ of degree $h$. More precisely it is an approximation of $T$ of degree $d$ for any $d$ such that $s \leqslant d \leqslant h$. By Lemma 1 and the choice (12) of $m$ we have $V/W = V_m/W_m$. Since $W$ is of minimal degree, we have $(V, W) = 1$. Moreover $(V_m, W_m) = 1$ by Lemma 3, so that $W = \lambda W_m$ for some nonzero element $\lambda$ of $F$.

More generally, suppose only that the linear recurrence $W$ holds for those $k$ such that $h \leqslant k \leqslant n-1$, that $\deg W \leqslant h$, and that $W$ is a linear recurrence of minimal degree with these properties. As above there is a polynomial $V$ such that $V/W$ is an approximation of $T$ of degree $h$, $(V, W) = 1$, and $W = \lambda W_m$ for some nonzero $\lambda$ in $F$.

It is easy to see that there need not be such a linear recurrence. For example, we may take $\{t_j\} = \{0, 0, \cdots, 0, 1\}$. However, we have shown that if there is one, then it must be $W_m$, up to a multiplicative constant.

Now

$$x^{d_m + d_{m+1} - 1} \| TW_m - V_m$$

by (10). Hence if $n \geqslant d_m + d_{m+1}$, then $\{t_j\}$ does not satisfy the linear recurrence $W_m$, in fact $W_m$ fails to hold for $d_m + d_{m+1} - 1$. Thus we have the following result:

THEOREM 1. *If* $d_m + d_{m+1} \leqslant n < 2d_{m+1}$, *then the sequence* $\{t_j\}$ *does* *not satisfy any linear recurrence of degree* $\leqslant n/2$. *In fact, there is no linear recurrence of degree* $\leqslant n/2$ *that holds for all* $k$ *such that* $h \leqslant k \leqslant n-1$.

Now suppose that $n < d_m + d_{m+1}$. Then the linear recurrence $W_m$ holds for all $k$ in the range $d_m \leqslant k \leqslant n-1$. We have $\deg W_m \leqslant d_m$. If $\deg W_m = d_m$, then $\{t_j\}$ satisfies the linear recurrence $W_m$. However, if $\deg W_m < d_m$, then $\deg V_m = d_m - 1$ by Lemma 4, and, therefore, the linear recurrence $W_m$ fails to hold at $d_m - 1$. Thus we have the following result:

THEOREM 2. *Suppose* $2d_m \leqslant n < d_m + d_{m+1}$. *If* $\deg W_m = d_m$, *then* $W_m$ *is a linear recurrence of minimal degree satisfied by* $\{t_j\}$. *If* $\deg W_m < d_m$, *then there is no linear recurrence of degree* $\leqslant n/2$ *which is satisfied by* $\{t_j\}$. *However,* $W_m$ *is a linear recurrence of minimal degree that holds for all* $k$ *such that* $h \leqslant k \leqslant n-1$. *It holds for all* $k$ *in the range* $d_m \leqslant k \leqslant n-1$, *and fails to hold for* $d_m - 1$.

**5.** In this section, we shall describe an efficient method of computing the polynomial $W_m$. As before, let $\{t_j\} = \{t_0, t_1, \cdots, t_{n-1}\}$ be the finite sequence we are interested in. We start with $N_1 = 0$, $\Delta_0 = -1$, and

$$\Delta_1 = xT - N_1 \doteq \sum_{j=0}^{n-1} t_j x^{j+1}.$$

For $i \geqslant 2$, (6) and (7) give us

$$N_i + R_i = 1/R_{i-1} = -\Delta_{i-2}/\Delta_{i-1},$$

where $x|R_i$ and $N_i$ is a polynomial in $y$, $y = 1/x$. Thus $N_i$ can be obtained from $\Delta_{i-2}$ and $\Delta_{i-1}$ by an ordinary division process. Then $\Delta_i$ is given by (5): $\Delta_i = N_i\Delta_{i-1} + \Delta_{i-2}$. In this way, the $N_i$ and the $\Delta_i$ can be successively obtained. We must continue this out to $i = m$ where $2d_m \leqslant n < 2d_{m+1}$. Since $x^{d_i}\|\Delta_{i-1}$ by (9), we know at once when we have reached $i = m$. If $d_m + d_{m+1} \leqslant n$, then there is no solution. If $d_m + d_{m+1} > n$, then we calculate $Q_m$ from the $N_i$ and the relations $Q_0 = 0$, $Q_1 = 1$, $Q_i = N_iQ_{i-1} + Q_{i-2}$.

If $Q_m$ has a nonzero constant term, then $\deg W_m = d_m$ and $W_m = x^{d_m}Q_m$ is the required linear recurrence. If $Q_m$ has no constant term, then $\deg W_m < d_m$ and $\{t_j\}$ does not satisfy a linear recurrence of degree $\leqslant n/2$. However, in this case, $W_m = x^{d_m}Q_m$ is a linear recurrence that holds for all $k$ such that $d_m \leqslant k \leqslant n-1$.

We note that $x^{d_i}\|\Delta_{i-1}$, $x^{d_{i-1}}\|\Delta_{i-2}$, and $d_i = r_{i-1} + d_{i-1}$. Hence in performing the division $\Delta_{i-2}/\Delta_{i-1}$ we need only use the first $r_{i-1} + 1$ terms of $\Delta_{i-2}$ and the same number of terms of $\Delta_{i-1}$. This is sufficient to determine $N_i$ completely.

Finally we note that it is only necessary to calculate $\Delta_i$ out to the term in $x^{n-d_i}$. This corresponds to the fact that $\Delta = xT$ is known only out to the term in $x^n$. To see this, consider the division of $\Delta_{i-2}$ by $\Delta_{i-1}$. We need $r_{i-1} + 1$ terms of each. More terms of $\Delta_{i-2}$ are assumed known than of $\Delta_{i-1}$. The number of terms of $\Delta_{i-1}$ that we have is $n - d_{i-1} - d_i + 1 = n - 2d_i + r_{i-1} + 1$. Since we may suppose $i \leqslant m$, this is at least $r_{i-1} + 1$ terms. Thus $N_i$ may be computed exactly. Clearly if we know $\Delta_{i-2}$ out to the term in $x^{n-d_{i-2}}$ and $\Delta_{i-1}$ out to the term in $x^{n-d_{i-1}}$, then once $N_i$ is known as a polynomial in $y$ of degree $r_{i-1}$, we may calculate $\Delta_i$ out to the term in $x^{n-d_i}$.

Tables 1 and 2 give examples of the calculation for small $n$ and $F = GF(2)$. The unnecessary terms of $\Delta_i$, i.e., those beyond $x^{n-d_i}$, are given in parenthesis. In the first example $n = 12$, $m = 3$, $d_3 = 3$, $d_4 = 7$, $d_m + d_{m+1} \leqslant n$, so there is no solution and the $Q_i$ are not calculated. In the second example, the sequence satisfies the linear recurrence $x^4 + x + 1$.

TABLE 1

$F = GF(2)$, $n = 12$, $\{t_j\} = \{100101110111\}$

| $i$ | $N_i$ | $\Delta_i$ |
|---|---|---|
| 0 | – | $1$ |
| 1 | 0 | $x + x^4 + x^6 + x^7 + x^8 + x^{10} + x^{11} + x^{12}$ |
| 2 | $y$ | $x^3 + x^5 + x^6 + x^7 + x^9 + x^{10} + x^{11}$ |
| 3 | $y^2 + 1$ | $x^7(+x^{12})$ |

There is no linear recurrence of degree $\leqslant 6$.

TABLE 2

$F = GF(2)$, $n = 8$, $\{t_j\} = \{11101011\}$

| $i$ | $N_i$ | $\Delta_i$ | $Q_i$ |
|---|---|---|---|
| 0 | – | $1$ | $0$ |
| 1 | 0 | $x + x^2 + x^3 + x^5 + x^7 + x^8$ | $1$ |
| 2 | $y + 1$ | $x^3 + x^4 + x^5 + x^6(+x^8)$ | $y + 1$ |
| 3 | $y^2$ | $x^4 + x^5(+x^6 + x^7 + x^8)$ | $y^3 + y^2 + 1$ |
| 4 | $y$ | $(x^7 + x^8)$ | $y^4 + y^3 + 1$ |

The linear recurrence is $x^4(y^4 + y^3 + 1) = x^4 + x + 1$.

**6.** We now consider the system

$$\sum_{j=0}^{s} t_{i+j}\lambda_j, \qquad 0 \leqslant i \leqslant s-1, \tag{13}$$

of $s$ linear equations in $s + 1$ unknowns. This system must have at least one nontrivial solution in $F$. If we set

$$\Lambda = \sum_{j=0}^{s} \lambda_j x^{s-j},$$

then we can write $\Lambda = x^r W$, where $W$ is a polynomial with nonzero constant term, and $\deg W \leqslant s - r$. If (13) holds, then there is a polynomial $V$ such that $\deg V < s - r$ and $X^{2s-r} | TW - V$. Thus $V/W$ is an approximation of $T$ of degree $s - r$. Hence $V/W = V_m/W_m$ for some $m$ with $d_m \leqslant s - r$ and $d_m + d_{m+1} - 1 \geqslant 2s - r$, so that $d_m \leqslant s < d_{m+1}$. Thus we see that our algorithm can be used to solve the system (13) for any positive integer $s$.

Institute for Defense Analyses
Communications Research Division
Princeton, New Jersey 08540

1. NEAL ZIERLER, "Linear recurring sequences and error-correcting codes," *Error Correcting Codes*, edited by H. B. Mann, Wiley, New York, 1968, pp. 47–59. MR **40** #2438.