NOTE ON THE ARITHMETIC OF BILINEAR TRANSFORMATIONS

DONALD M. ADELMAN

1. Introduction. Since the time of Lucas many papers have appeared investigating the properties of sequences of rational integers satisfying linear recurrence relations. Very little,[1] however, has been done in the nonlinear cases, although the generalization to variable coefficients seems to have awakened more interest than the generalization to relations of higher degree but with fixed coefficients. The present paper deals with one of the simplest problems of the latter type.

Let a sequence be defined by the value x_1 and by the relation:

$$x_{n+1} = (ax_n + b)/(cx_n + d); \tag{1}$$

$ad-bc\neq 0$; a, b, c, d, rational integers. Under what conditions are all the x_i integral? That such integral sequences exist may be shown by two examples. First, if $x_{n+1}=x_n/(x_n-1)$, $x_1=2$ generates the sequence 2, 2, 2, $\cdots$; second, if $x_{n+1}=(178x_n-1492)/(7x_n+2)$, $x_1=4$ generates the sequence 4, -26, 34, 19, 14, 10, 4, $\cdots$. If we write $y_n=cx_n+d$, $e=a+d$, $m=bc-ad$, (1) becomes:

$$y_{n+1} = e + m/y_n \tag{2}$$

where $\{y_i\}$ is integral if $\{x_i\}$ is.

THEOREM 1. *Every sequence of integers satisfying* (1) *or* (2) *is periodic.*

PROOF. In (2) every y_n must be one of the finitely many divisors of m. The periodicity of $\{y_i\}$ entails that of $\{x_i\}$. Moreover, the period begins with the first term of the sequence, since each value of x_n permits only one value for x_{n-1}.

2. Classification by fixed points. The possible sequences satisfying (2) are related to the roots, r_1 and r_2, of $r^2-er-m=0$.

THEOREM 2. *If the roots are real and of unequal magnitude there are no sequences satisfying* (2) *or just two such sequences, each of period one. In the latter case* r_1 *and* r_2 *are integral and generate the two sequences.*

Received by the editors May 7, 1949.

[1] An exception is Morgan Ward's recent memoir on "elliptic" divisibility sequences in vol. 70 of the American Journal of Mathematics.

PROOF. Suppose $|r_1| < |r_2|$ and write (2) as:

$$\frac{y_{n+1} - r_2}{y_{n+1} - r_1} = \frac{r_1}{r_2}\,\frac{y_n - r_2}{y_n - r_1} = \left(\frac{r_1}{r_2}\right)^n \frac{y_1 - r_2}{y_1 - r_1}. \tag{3}$$

$y_1 = r_1$ only if r_1 is integral and the sequence is $r_1, r_1, r_1, \cdots$. Otherwise $\lim_{n\to\infty}(r_1/r_2)^n = 0$, and $\lim_{n\to\infty}(y_{n+1} - r_2)/(y_{n+1} - r_1) = 0$, which is only possible if $y_{n+1} = r_2$.

If the roots are real and equal except for sign, $e = 0$ so that we may take y_1 as any divisor of m and the sequence becomes:

$$y_1,\ m/y_1,\ y_1,\ m/y_1, \cdots.$$

If $r_1 = r_2 = r$, (3) is of no use and instead we define a sequence, $p_0, p_1, p_2, \cdots$ by $p_0 = 1$, $p_1 = y_1$, $p_{n+2} = ep_{n+1} + mp_n$. Then:

LEMMA 1. $y_n = p_n/p_{n-1}$.

PROOF. Set $p_n/p_{n-1} = q_n$. Then $q_1 = y_1$, and the recurrence relation becomes:

$$q_{n+2}q_{n+1}p_n = eq_{n+1}p_n + mp_n. \tag{4}$$

Now, from the theory of second order recurrence sequences we know that the general solution for p_n is $p_n = (An + B)r^n$, where A and B are not both zero since $p_0 = 1$. Evidently $p_n = 0$ for at most one value $n = t$. For all values of n except t, (4) then reduces to

$$q_{n+2} = e + \frac{m}{q_{n+1}},$$

which is the same relation satisfied by the y_i without exception. The q-sequence and the y-sequence therefore agree in their first $t+1$ terms. Also, in both, the $t+2$nd term is equal to e, in the y-sequence because y_{t+1} is infinite, in the q-sequence by setting $p_t = 0$ in the second order recurrence relation and using the definition of q_{t+2}. Therefore the two sequences agree in all their terms and the lemma is proved.

Thus it is required that $((An + B)/(A(n-1) + B))r = y_n$ should be integral for all values of n. But, if $A = 0$, $y_n = r$, and otherwise $\lim_{n\to\infty} y_n = r$, so that again the only possible sequence occurs when r is integral. This gives:

THEOREM 3. *If $r_1 = r_2 = r$, there is just one sequence satisfying* (2) *or none according as r is or is not an integer. In the former case the sequence is $r, r, r, \cdots$.*

Inasmuch as we have already seen an example of a sequence of

period six, we may expect the case of complex roots to be more difficult. For real roots, of course, it is hardly necessary to use (2) since (1) and the value of e give all the required information.

3. **Complex roots.** Again we consider the linear recurrence relation:

$$p_{n+1} = ep_n + mp_{n-1}, \tag{5}$$

but this time define a sequence $\{p_i\}$ by the initial values $p_0=0$, $p_1=1$. This is called the principal sequence, and its first seven terms are 0, 1, e, e^2+m, e^3+2em, $e^4+3e^2m+m^2$, $e^5+4e^3m+3em^2$. Using this sequence, we obtain the following result:

THEOREM 4. *If* $\{y_i\}$ *satisfies* (2) *and* $\{p_i\}$ *is the principal solution of* (5), *then*

$$y_n = \frac{p_n y_1 + mp_{n-1}}{p_{n-1}y_1 + mp_{n-2}}.$$

The proof is by induction.

THEOREM 5. *The sequence* $\{y_i\}$ *satisfying* (2) *has a period* w *if and only if* $p_w=0$.

PROOF. Suppose $p_w=0$. Then by (5), $p_{w+1}=mp_{w-1}$ and from Theorem 4, $y_{w+1}=y_1$. On the other hand, suppose $y_{w+1}=y_1$. Then:

$$p_w y_1^2 + mp_{w-1}y_1 = p_{w+1}y_1 + mp_w,$$
$$p_w y_1^2 - (p_{w+1} - mp_{w-1})y_1 - mp_w = 0 = p_w y_1^2 - ep_w y_1 - mp_w,$$
$$p_w(y_1^2 - ey_1 - m) = 0,$$

and since the factor in parentheses cannot be zero, $p_w=0$.

Of course the period of $\{y_i\}$ is the smallest value of $w>0$ for which $p_w=0$.

LEMMA 2.[2] *If* $\{p_i\}$ *is the principal solution of* (5), *for* $n>0$ p_n *is a homogeneous polynomial of degree* $[(n-1)/2]$ *in the variables* e^2 *and* m *if* n *is odd, and* e *times such a polynomial if* n *is even. In both cases all the coefficients are integers and the coefficient of the highest power of* e *is unity.*

---

[2] The proof beginning here is not the one that most readily suggests itself. If p_n is expressed explicitly in terms of the scalar roots, namely, as $p_n=(r_1^n-r_2^n)/(r_1-r_2)$, the problem of finding its zeros reduces to that of determining the exponent of an element in a quadratic field. But the proof given above relies on simpler and somewhat more relevant ideas.

The proof is by induction.

It follows from Theorem 5 that if (2) is satisfied by some integral sequence $\{y_i\}$ with period w, the values of e and m from (2) make the homogeneous polynomial of Lemma 2 zero. Consequently e^2/m is the root of a polynomial with integral coefficients and leading coefficient unity. Therefore, since the root is rational it must be integral and we have:

LEMMA 3. *$p_w=0$ only if $e^2+km=0$ for some integer, k.*

Not all values of k correspond to a w however, as is seen from:

THEOREM 6. *If r_1 and r_2 are complex, and if $\{y_i\}$ satisfies (2) with period w, then $e^2+km=0$ for one of four values of k, $k=0,1,2$, or 3, corresponding respectively to $w=2$, 3, 4, or 6.*

PROOF. Since the roots are complex, $e^2+4m<0$ and $m<0$. Therefore $e^2+km>0$ for $k<0$, and $e^2+km<0$ for $k\geqq 4$. Only four values of k remain, and we obtain the corresponding periods from the factorization of the first seven terms of the sequence $\{p_i\}$.

4. **The complete period.** We now know that any sequence $\{y_i\}$ of integers satisfying (2) must be periodic, and conditions on e and m in (2)—or on a, b, c, and d in (1)—for periodicity. But these conditions do not guarantee that for an arbitrary value of y_1, or even for any value of y_1, the sequences $\{x_i\}$ and $\{y_i\}$ should be entirely integral. We establish certain preliminary theorems.

THOREM 7. *If w is the period of a sequence $\{y_i\}$ of integers satisfying (2), then $(y_1y_2\cdot\cdot\cdot y_w)^2=(-m)^w$.*

PROOF. $r_i=e+m/r_i$ for $i=1$ and 2. Subtracting both these equations from (2) and multiplying the results, we obtain:

$$(y_{n+1}-r_1)(y_{n+1}-r_2)=\frac{m^2}{r_1r_2y_n^2}(y_n-r_1)(y_n-r_2)$$

or, if $Q(y)=y^2-ey-m$,

$$Q(y_{n+1})=\frac{-m}{y_n^2}Q(y_n).$$

Multiplying these equations over a complete period we obtain the result, since $Q(y)\neq 0$ for y real.

COROLLARY 1. *If an integer s divides each term of $\{y_i\}$, then $s^2\mid m$ and $s\mid e$.*

PROOF. From Theorem 7, $s^{2w} \mid (-m)^w$ or $s^2 \mid m$. Then, from Theorem 6, $s \mid e$.

COROLLARY 2. *If* $\{x_i\}$ *is a sequence of integers satisfying* (1) *and if* $s=(c, d)$, *then* $s \mid a$ *and* $s \mid b$. *Accordingly we may assume* $(c, d)=1$.

PROOF. Every term of the sequence $\{y_i\}$ derived from $\{x_i\}$ is divisble by s. By Corollary 1, $s \mid e=a+d$, and therefore $s \mid a$. Writing (1) as

$$x_{n+1}(cx_n + d) = ax_n + b,$$

we have $s \mid b$.

DEFINITION. *Let* $R(g, h)$ *be the greatest divisor of* g *prime to* h.

Then, for example, $R(6, 9)=2$; $R(9, 6)=1$.

THEOREM 8. *An integral sequence* $\{x_i\}$ *satisfying* (1) *corresponds to an integral sequence* $\{y_i\}$ *satisfying* (2) *if and only if* c *is a divisor of* $R(y_1-y_2, y_1)$.

PROOF. If we begin with the sequence $\{x_i\}$, then $y_1=cx_1+d$, $y_2=cx_2+d$, and $c \mid (y_1-y_2)$. By Corollary 2 we may assume that c is prime to d, consequently to each y_i, and in particular to y_1.

Start, however, from a sequence $\{y_i\}$ and let c be any divisor of $R(y_1-y_2, y_1)$. Choose an arbitrary integer x_1 and define d by $y_1=cx_1+d$. Then, since $(c, y_1)=1$, $(c, d)=1$. Next, define a by means of $e=a+d$. Now, since $c \mid (y_1-y_2)$, $y_1 \equiv y_2 \equiv d \pmod{c}$, and writing (2) as

$$y_{n+1}y_n = ey_n + m, \tag{6}$$

we have $d^2 \equiv ed+m \pmod{c}$ by taking $n=1$, or, $d(d-e) \equiv m \equiv -ad \pmod{c}$, using the definition of a. So, $(m+ad)/c$ is an integer, say b. We thus have found integers, a, b, c, and d, such that, in (2), $e=a+d$ and $m=bc-ad$. It remains to show that all the x_i are integral. Obviously, this will be true if and only if $y_i \equiv d \pmod{c}$ for each i. We already know this for $i=1$, and from (6), if $y_n \equiv d \pmod{c}$,

$$y_{n+1}d \equiv (a + d)d - ad \pmod{c} \equiv d^2$$

or, since $(c, d)=1$, $y_{n+1} \equiv d \pmod{c}$.

COROLLARY. *For any given sequence* $\{y_i\}$ *of integers satisfying* (2), $R(y_n-y_{n+1}, y_n)$ *is a constant.*

PROOF. Since $\{y_i\}$ is periodic, it does not matter which term we consider the first in defining a value of c as in Theorem 8. In particular, the largest possible value of c cannot change.

5. **Parametric solution.** Theorem 8 completely elucidates the connection between sequences satisfying (2) and sequences satisfying (1). We shall now give a parametric solution to the problem of finding all possible sequences satisfying (2). Evidently this is hardly necessary when r_1 and r_2 are real or when $e=0$, so that by Theorem 6, $k=-e^2/m$ must assume one of the three values 1, 2, or 3. Introducing an integral parameter t, we must have, according to the value of k, $e=t$ and $m=-t^2$, or $e=2t$ and $m=-2t^2$, or $e=3t$ and $m=-3t^2$. This gives the first part of the following theorem.

THEOREM 9. *If* $e^2+4m<0$ *and* $e\neq 0$, *the transformation* (2) *must take one of three forms*:

$$y_{n+1} = k(t - t^2/y_n), \qquad k = 1, 2, \text{ or } 3,$$

where t *is an integer. In addition, there must exist relatively prime integers,* u *and* v, *such that* t *is divisible by* $uv(u-v)$ *if* $k=1$, *by either* $uv(u-v)(u-2v)$ *or* $uv(u-v)(u-2v)/4$ *according as* u *is odd or even if* $k=2$, *or by either* $uv(u-v)(2u-3v)(u-2v)(u-3v)$ *or* $uv(u-v)(2u-3v)(u-2v)(u-3v)/27$ *according as* u *is not or is divisible by 3. In all cases* $y_1=ut/v$.

PROOF. The proof is much the same for any value of k and will be given for $k=2$. If a sequence $\{y_i\}$ of integers satisfies $y_{n+1}=2t-2t^2/y_n$, we may certainly find relatively prime integers, u and v, such that $y_1=ut/v$. Then y_2, y_3, and y_4 may be calculated as:

$$2t\frac{u-v}{u}, \qquad t\frac{u-2v}{u-v}, \quad \text{and} \quad 2t\frac{-v}{u-2v}.$$

It is easily seen that if the fraction u/v is in its lowest terms so are $(u-v)/u$, $(u-2v)/(u-v)$, and $v/(u-2v)$. Consequently, $v \mid t$, $u \mid 2t$, $(u-v) \mid t$, and $(u-2v) \mid 2t$. If u is odd, u, v, $u-v$, and $u-2v$ have no factor in common since $(u, v)=1$. If u is even, $(u, u-2v)=2$. The theorem follows.

EXAMPLE. Take $u=4$, $v=3$. Then t must be divisible by $4\cdot 3\cdot 1\cdot(-2)/4=-6$. A possible value for t is $t=12$ which gives $y_1=16$, the transformation being: $y_{n+1}=24-288/y_n$, and the sequence: 16, 6, -24, 36, 16, $\cdots$, $R(y_1-y_2, y_1)=R(10, 16)=5$. Thus, to construct a sequence satisfying (1) we may take $c=5$, and perhaps—the choice is arbitrary—$x_1=3$; then $d=1$, $a=e-d=23$, $b=(m+ad)/c=-53$. The transformation is therefore $x_{n+1}=(23x_n-53)/(5x_n+1)$, and the sequence: 3, 1, -5, 7, 3, $\cdots$.

UNIVERSITY OF CONNECTICUT