An algorithm for evaluation of remote terms in a linear recurrence sequence

By J. C. P. Miller* and D. J. Spencer Brown†

A method is described for computing terms U_n given by a linear recurrence relation from initial conditions near $n = 0$, whereby values for large n may be obtained without computing all intermediate values. The total number of operations is of order log n.

1. Linear recurrence relations arise frequently both in number theory and in general numerical computations. As examples requiring the evaluation of terms U_n for high values of n, we can quote

(i) Bernoulli's method for evaluating the largest root of a polynomial equation,
(ii) the interest in factorizing members of the Fibonacci sequence and related sequences.

2. One of the difficulties in using recurrence relations to obtain the necessary U_n is the apparent need to compute all intermediate values up to the U_n required.

This has been overcome for 3-term relations

$$aU_{n+1} + bU_n + cU_{n-1} = 0.$$

For example, the Fibonacci sequence $\{U_n\}$ satisfies

$$U_{n+1} = U_n + U_{n-1}$$

and the two most familiar, and independent, such sequences are $\{U_n\}$, $\{V_n\}$ in which

n	0	1	2	3	4	5	6	7	8
U_n	0	1	1	2	3	5	8	13	21
V_n	2	1	3	4	7	11	18	29	47.

Then we have $U_{2n} = U_nV_n$, $V_{2n} = V_n^2 - 2(-1)^n$

and also $\qquad V_n = U_{n-1} + U_{n+1}.$

Thus from $\qquad U_n, U_{n-1}$

we find

$$U_{n+1} = U_n + U_{n-1}, \quad U_{n+2} = U_{n+1} + U_n$$
$$V_n = U_{n-1} + U_{n+1}, \quad V_{n+1} = U_n + U_{n+2}$$
$$U_{2n} = U_nV_n, \quad U_{2n+2} = U_{n+1}V_{n+1}$$
$$U_{2n+1} = U_{2n+2} - U_{2n}$$

and we can start again, from U_{2n} and U_{2n+1}, or from U_{2n+1} and U_{2n+2}, or from U_{2n-1} and U_{2n}, whichever is convenient.

3. We now give an algorithm that may be used for similar steps for a recurrence relation of any order. This is most conveniently expressed in matrix terms.

3.1. Write the relation in the form

$$y_n + a_1y_{n-1} \ldots + a_ny_0 = 0 \qquad (1)$$

in which the a_r are constants, $a_n \neq 0$.

We now choose n independent sequences

$$\{U_r\} = \{U_{r,0}, U_{r,1}, U_{r,2} \ldots\} \quad r = 1(1)n.$$

That is, we choose the sequences such that

$$\sum_{r=1}^{n} \lambda_r U_{r,s} = 0 \quad s = 0(1)n-1$$

implies that the constants λ_r are all zero. We may then write

$$y_s = \sum_{r=1}^{n} \alpha_r U_{r,s}$$

for appropriate constants α_r.

We choose, in fact, all the $\{U_r\}$ from the *same* special sequence, starting at successive terms,

$$\{U_r\} = \{U_r, U_{r+1}, U_{r+2}, \ldots\}$$

where $\quad U_n = 1, \quad U_r = 0, \quad 1 \leqslant r \leqslant n-1.$

The matrix of values

$$\boldsymbol{U}_1 \equiv \begin{pmatrix} U_1 & U_2 & \ldots & U_n \\ U_2 & U_3 & \ldots & U_{n+1} \\ \vdots & & & \\ U_n & \ldots & \ldots & U_{2n-1} \end{pmatrix}$$

is thus of form

$$\begin{pmatrix} O & & & 1 \\ & & 1 & \\ & \cdot^{\cdot^{\cdot}} & & \\ 1 & & & B \end{pmatrix}$$

and is non-singular, with determinant $(-1)^{n(n-1)/2}$.

We write also

$$\boldsymbol{U}_r \equiv \begin{pmatrix} U_r & U_{r+1} \cdots & U_{r+n-1} \\ \vdots & & \vdots \\ U_{r+n-1} & \cdots & U_{r+2n-2} \end{pmatrix}$$

3.2 We now develop $\boldsymbol{A}_r$ where

$$\boldsymbol{U}_{r+s} = \boldsymbol{A}_r\boldsymbol{U}_s.$$

The matrix $\boldsymbol{A}_r$ is independent of s, and depends only on the coefficients in (1). It is evident that

$$\boldsymbol{A}_r\boldsymbol{A}_s = \boldsymbol{A}_{r+s}$$

* *University Mathematical Laboratory, Corn Exchange Street, Cambridge.*
† *c/o 28b Porchester Terrace, London, W.2.*

whence $\boldsymbol{A}_r = \boldsymbol{A}^r$, so that $\boldsymbol{A}_r$ could be found by matrix squaring and multiplication. However, the special form of $\boldsymbol{U}_r$ and particularly of $\boldsymbol{U}_1$ allows the simplified and efficient method of back substitution.

Suppose $\boldsymbol{U}_r$ is known, involving knowledge of $2n - 1$ consecutive terms of $\{U_r\}$; of these, $n - 1$ may be obtained simply from the recurrence relation after the first n (or any consecutive set of n) are known.

Then $$\boldsymbol{U}_r = \boldsymbol{A}_{r-1}\boldsymbol{U}_1$$

Whence $$\boldsymbol{A}_{r-1} = \boldsymbol{U}_r\boldsymbol{U}_1^{-1}$$

This is easily obtained, since $\boldsymbol{U}_1$ is triangular. In fact, as Professor E. S. Selmer has pointed out, it is evident from (1) that

$$\boldsymbol{C}\boldsymbol{U}_1 = \boldsymbol{I}$$

$$\boldsymbol{C} = \begin{pmatrix} a_{n-1} & a_{n-2} & . & . & a_2 & a_1 & 1 \\ a_{n-2} & a_{n-3} & . & . & a_1 & 1 & 0 \\ . & . & . & . & . & . & . \\ a_1 & 1 & . & . & 0 & 0 & 0 \\ 1 & 0 & . & . & 0 & 0 & 0 \end{pmatrix}$$

and consists of coefficients in the recurrence relation (1), and zeros.

Then $$U_{2r-1} = \boldsymbol{A}_{r-1}\boldsymbol{U}_r$$

is even more readily computed, since we need only the first row of $\boldsymbol{U}_{2r-1}$ which contains U_{2r-1} to U_{2r+n-2}, n consecutive values. A complete set of U_{2r+s} is then filled in by use of the recurrence relation, with the possibility of checking some of them by use of $\boldsymbol{A}_{r-1}\boldsymbol{U}_r$.

3.3. Finally we have $\boldsymbol{Y}_r = \boldsymbol{B}\boldsymbol{U}_{r+1}$ where $\boldsymbol{B}$ is given by $\boldsymbol{B} = \boldsymbol{Y}_0\boldsymbol{U}_1^{-1} = \boldsymbol{Y}_0\boldsymbol{C}$.

4. We illustrate by obtaining y_{43} where

$$y_{r+3} = y_{r+1} + y_r, \quad \text{with} \quad y_0 = 3, \quad y_1 = 0, \quad y_2 = 2$$

so that $y_r = s_r = \alpha_1^r + \alpha_2^r + \alpha_3^r$, where $\alpha_1, \alpha_2, \alpha_3$ are the roots of $x^3 - x - 1 = 0$.

We have

$$\boldsymbol{U}_1 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix} \quad \boldsymbol{C} = \boldsymbol{U}_1^{-1} = \begin{pmatrix} -1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

Now 43 is 1 0 1 0 1 1 in binary, and we develop suffix 43 by doubling for a zero digit, and doubling followed by an increase of a unit for a non-zero digit thus

	1	0	1	0	1	1
0	1	2	5	10	21	43

We start by finding A_{10}. We get readily, by direct recurrence, that

$$U_{11} = 4, \quad U_{12} = 5, \quad U_{13} = 7, \quad U_{14} = 9, \quad U_{15} = 12$$

and find

$$\boldsymbol{A}_{10} = \boldsymbol{U}_{11}\boldsymbol{U}_1^{-1}$$

$$= \begin{pmatrix} 4 & 5 & 7 \\ 5 & 7 & 9 \\ 7 & 9 & 12 \end{pmatrix}\begin{pmatrix} -1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 3 & 5 & 4 \\ 4 & 7 & 5 \\ 5 & 9 & 7 \end{pmatrix}$$

Now $$\boldsymbol{U}_{21} = \boldsymbol{A}_{10}\boldsymbol{U}_{11}$$

so that $U_{21} = 65, \quad U_{22} = 86, \quad U_{23} = 114$

and $U_{24} = 151, \quad U_{25} = 200, \quad U_{26} = 265.$

The next and final cycle now gives

$$\boldsymbol{A}_{21} = \boldsymbol{U}_{22}\boldsymbol{U}_1^{-1}$$

$$= \begin{pmatrix} 86 & 114 & 151 \\ 114 & 151 & 200 \\ 151 & 200 & 265 \end{pmatrix}\begin{pmatrix} -1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 65 & 114 & 86 \\ 86 & 151 & 114 \\ 114 & 200 & 151 \end{pmatrix}$$

and $$\boldsymbol{U}_{43} = \boldsymbol{A}_{21}\boldsymbol{U}_{22}$$

gives $U_{43} = 31572, \quad U_{44} = 41824, \quad U_{45} = 55405$

also $$U_{46} = 73396$$

Next

$$\boldsymbol{B} = \boldsymbol{Y}_0\boldsymbol{U}_1^{-1} = \begin{pmatrix} 3 & 0 & 2 \\ 0 & 2 & 3 \\ 2 & 3 & 2 \end{pmatrix}\begin{pmatrix} -1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 & 3 \\ 3 & 2 & 0 \\ 0 & 3 & 2 \end{pmatrix}$$

so $$\boldsymbol{Y}_{43} = \boldsymbol{B}\boldsymbol{U}_{44}$$

and $$y_{43} = -U_{44} + 3U_{45} = 178364.$$

As a test, since 43 is prime, we verify that 43 divides y_{43}. In fact

$$y_{43} = 43.4148$$
$$= 43.2^2 . 17.61.$$

5. We have remarked in § 3.2 that we need compute only n consecutive U_r occurring in $\boldsymbol{U}_{2r-1}$. This means, in fact, that we have to know either

(i) only a single row or column of $\boldsymbol{A}_r$, any one will do and we can choose the simplest or most convenient; we then need the whole of $\boldsymbol{U}_r$, i.e. $2n - 1$ consecutive values of U_r, or

(ii) only a set of n consecutive U_r, say U_{r+a} to $U_{r+n-1+a}$, together with the whole of $\boldsymbol{A}_r$.

Special circumstances of the particular recurrence relation involved may decide which choice is most convenient (it is hoped to develop this in a subsequent paper). In general, however, it would seem best to adopt the first alternative and compute a single row of $\boldsymbol{A}_r$, and obtain $2n - 1$ consecutive values of U_r, n being supposed known as the result of the step just completed, and the other $n - 1$ obtained by direct use, forwards or backwards, of the original recurrence relation. It does not matter which row or column of $\boldsymbol{A}_r$ is obtained. We have, however, kept the full matrices in the numerical example in order to help understanding.

6. Another way of obtaining these results that is not dependent on matrix ideas and which also casts light on the processes involved is as follows.

The original relation (1) may be written

$$\left.\begin{aligned} y_n &= -a_1 y_{n-1} \ldots -a_n y_0 \\ &= \sum_{r=1}^{n} a_{n,r}\, y_{n-r} \end{aligned}\right\} \tag{6.1}$$

Then

$$y_{n+1} = \sum_{r=1}^{n} a_{n,r} y_{n-r+1}$$

and we may use (6.1) to replace y_n on the right giving

$$y_{n+1} = \sum_{r=1}^{n} a_{n+1,r} y_{n-r}. \tag{6.2}$$

We may now make a double step and use (6.1) and (6.2) to replace y_n and y_{n+1}in

$$y_{n+3} \doteq \sum_{r=1}^{n} a_{n+1,r} y_{n-r+2}$$

to yield

$$y_{n+3} = \sum_{r=1}^{n} a_{n+3,r} y_{n-r}.$$

We shall suppose, however, that we have developed

$$y_{n+s} = \sum_{r=1}^{n} a_{n+s,r} y_{n-r} \quad s = 0(1)n \tag{6.3}$$

and also have, for a particular value of m

$$y_{m+s} = \sum_{r=1}^{n} a_{m+s,r} y_{n-r} \quad s = 0(1)n-1. \tag{6.4}$$

We then apply (6.4) to the relation, itself derived from (6.4) with $s = 0$, and the suffix of each y increased by m,

$$y_{2m} = \sum_{r=1}^{n} a_{m,r} y_{n+m-r}$$

to replace

y_{m+s} (on the right), with $s = n - r = n - 1(-1)0$

by sums involving y_{n-r}, $r = 1(1)n$. This yields

$$y_{2m} = \sum_{r=1}^{n} a_{2m,r} y_{n-r} \tag{6.5}$$

whence

$$y_{2m+s} = \sum_{r=1}^{n} a_{2m,r} y_{n-r+s} \quad s = 1(1)n-1 \text{ or } n$$

which can be reduced by (6.3) to yield

$$y_{2m+s} = \sum_{r=1}^{n} a_{2m+s,r} y_{n-r}$$

for $s = 0(1)n - 1$ or $s = 1(1)n$, whichever is appropriate. This is a repetition of (6.4) with m replaced by $2m$ or $2m + 1$.

In fact (6.4) is equivalent to

$$\mathbf{y}_m = \mathbf{A}_m \mathbf{y}_0.$$

We have seen, however, that $\mathbf{A}_m$ is most easily developed from the special sequence $\{U_0\}$ by

$$\mathbf{U}_{m+1} = \mathbf{A}_m \mathbf{U}_1 \quad \text{or} \quad \mathbf{A}_m = \mathbf{U}_{m+1}\mathbf{C}.$$

We also see that, given

$$y_{n+s} = \sum_{r=1}^{n} a_{n+s,r} y_{n-r}$$

we may obtain

$$\begin{aligned} y_{n+s+1} &= \sum_{r=1}^{n} a_{n+s+1,r} y_{n-r} \\ &= \sum_{r=1}^{n-1} a_{n+s,r+1} y_{n-r} + a_{n+s,1} \sum_{r=1}^{n} a_{n,r} y_{n-r} \end{aligned}$$

yielding

$$a_{n+s+1,r} = a_{n+s,1} a_{n,r} + a_{n+s,r+1}$$

with $a_{n,n+1} = 0$. This is a recurrence relation for $a_{n+s,r}$.

We note that each row $a_{n+s,r}$, $r = 1(1)n$ occurs in n successive matrices $\mathbf{A}_{s+r}$, $r = 0(1)n - 1$.

It is hoped to give in subsequent papers two distinct applications of this algorithm.