NOTES ON CONTINUED FRACTIONS AND RECURRENCE SEQUENCES

A. J. van der Poorten

Macquarie University

Introduction. The purpose of these notes is to support the papers included in this volume by providing self-contained summaries of related mathematics emphasising those aspects actually used or required. I have selected two topics that are easily described from first principles yet for which it is peculiarly difficult to find congenial introductions that warrant citing.

The theory of continued fractions is less widely known than it should be; yet one can readily retrieve its fundamental results with little more than the ability to multiply 2×2 matrices.

A linear feedback shift register (LFSR) is just a recurrence sequence defined over the field F_2 of 2 elements; or, better, its generating function is a rational function defined over F_2. It seems useful to interpret familiar activities in the creation of stream ciphers in classical terms if only to establish a dictionary translating the jargon of stream ciphers into the language of mathematics.

1. Continued Fractions

1.1 An introduction to continued fractions. A continued fraction is an object of the shape

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ddots}}}$$

which we denote in a space-saving flat notation by

$$[a_0\ ,\ a_1\ ,\ a_2\ ,\ a_3\ ,\ \ldots\ldots]\,.$$

Virtually all principles of the subject are revealed by the following correspondence:

Proposition 1 (Fundamental Correspondence). *Given a sequence* $a_0, a_1, a_2, \ldots\ldots$

$$(1) \qquad \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots\cdots \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{pmatrix} \quad \textit{for } n = 0,\ 1,\ 2,\ \ldots\ldots$$

if and only if

$$\frac{p_n}{q_n} = [a_0\ ,\ a_1\ ,\ \ldots\ldots\ ,\ a_n] \quad \textit{for } n = 0,\ 1,\ 2,\ \ldots\ldots\ .$$

Research partially supported by the Australian Research Council.

PROOF: This correspondence is readily established by a thoughtful inductive argument. Notice firstly that the sequence of *partial quotients* (a_h) defines the sequences (p_h) and (q_h) appearing in the first column of the matrix product. Since the empty product of 2×2 matrices is the identity matrix, we are committed to

$$\begin{pmatrix} p_{-1} & p_{-2} \\ q_{-1} & q_{-2} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} . \tag{2}$$

We may then readily verify by induction on n that the second column of the product indeed has the alleged entries. Thus we have the recursive formulae

$$\begin{aligned} p_{n+1} &= a_{n+1}p_n + p_{n-1} \\ q_{n+1} &= a_{n+1}q_n + q_{n-1} \, . \end{aligned} \tag{3}$$

We verify the principal claim by induction on the *number* $n+1$ of matrices appearing on the left in the product. The claim is easily seen true for $n = 0$ since, indeed $p_0 = a_0$ and $q_0 = 1$. Accordingly, we suppose that

$$\begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_2 & 1 \\ 1 & 0 \end{pmatrix} \cdots\cdots \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} x_n & x_{n-1} \\ y_n & y_{n-1} \end{pmatrix} \quad \text{for } n = 0,\ 1,\ 2,\ \ldots\ldots$$

if and only if

$$\frac{x_n}{y_n} = [a_1\ , a_2\ , \ldots\ldots , a_n] \quad \text{for } n = 0,\ 1,\ 2,\ \ldots\ldots \ ,$$

noting that this is a case of just n matrices.

But

$$\begin{pmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{pmatrix} = \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x_n & x_{n-1} \\ y_n & y_{n-1} \end{pmatrix} = \begin{pmatrix} a_0x_n + y_n & a_0x_{n-1} + y_{n-1} \\ x_n & x_{n-1} \end{pmatrix}$$

entails

$$\frac{p_n}{q_n} = a_0 + \frac{y_n}{x_n} = a_0 + \frac{1}{[a_1\ , \ldots\cdots , a_n]} = [a_0\ , a_1\ , \ldots\ldots , a_n] \, , \tag{4}$$

verifying the claim by induction. ∎

Taking determinants in the correspondence immediately yields the fundamental formula

$$p_nq_{n-1} - p_{n-1}q_n = (-1)^{n+1} \text{ or } \frac{p_n}{q_n} = \frac{p_{n-1}}{q_{n-1}} + (-1)^{n-1}\frac{1}{q_{n-1}q_n} \, . \tag{5}$$

It is then immediate that

$$\frac{p_n}{q_n} = a_0 + \frac{1}{q_0q_1} - \frac{1}{q_1q_2} + \cdots + (-1)^{n-1}\frac{1}{q_{n-1}q_n} \, . \tag{6}$$

Almost invariably, but not always, in the sequel the a_i are positive integers — excepting a_0 which may have any sign.

It follows that we can make sense of nonterminating continued fractions

$$\alpha = [a_0\ ,\ a_1\ ,\ \ldots\ldots]\,,$$

for evidently,

$$\alpha = a_0 + \frac{1}{q_0 q_1} - \frac{1}{q_1 q_2} + \cdots = a_0 + \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{q_{n-1} q_n} \tag{7}$$

and, this being an alternating series of terms with decreasing size, the series converges to some real number α.

In this context the terminating continued fractions

$$\frac{p_n}{q_n} = [a_0\ ,\ a_1\ ,\ \ldots\ldots\ ,\ a_n] \qquad\qquad n = 0,\ 1,\ 2,\ \ldots\ldots$$

are called *convergents* of α and the tails

$$\alpha_{n+1} = [a_{n+1}\ ,\ a_{n+2}\ ,\ \ldots\ldots] \tag{8}$$

are known as its *complete quotients*. Note that we have, formally,

$$\alpha = [a_0\ ,\ a_1\ ,\ \ldots\ldots\ ,\ a_n, \alpha_{n+1}] \qquad\qquad n = 0,\ 1,\ 2,\ \ldots\ldots\ . \tag{9}$$

These remarks immediately yield the approximation properties of the convergents. For we have

$$\alpha - \frac{p_n}{q_n} = (-1)^n \left(\frac{1}{q_n q_{n+1}} - \frac{1}{q_{n+1} q_{n+2}} + \cdots\cdots \right)\,. \tag{10}$$

This shows that the sequence $(q_n \alpha - p_n)$ alternates in sign and that, in absolute value, it converges monotonically to zero. Less precisely, we see that

$$\left| \alpha - \frac{p_n}{q_n} \right| < \frac{1}{q_n q_{n+1}}$$

and, recalling (3) : $q_{n+1} = a_{n+1} q_n + q_{n-1}$ implies yet less accurately that

$$\left| \alpha - \frac{p_n}{q_n} \right| < \frac{1}{a_{n+1} q_n^2}\,.$$

Thus a convergent yields an exceptionally sharp approximation when the *next* partial quotient is exceptionally large. For example, reminded that

$$\pi = [3\ ,\ 7\ ,\ 15\ ,\ 1\ ,\ 292\ ,\ 1\ ,\ \ldots]$$

and noting

$$[3\ ,\ 7] = 22/7 \qquad\qquad [3\ ,\ 7\ ,\ 15\ ,\ 1] = 355/113$$

we have

$$\left|\pi - \frac{22}{7}\right| < \frac{1}{15.7^2} \qquad\qquad \left|\pi - \frac{355}{113}\right| < \frac{1}{292.113^2}$$

making appropriate the popularity of these rational approximations to π.

Because the sequence $(q_n\alpha - p_n)$ alternates in sign it is clear that one need only consider every second convergent if one is interested in just those approximations below (underestimating), respectively above (overestimating) α. It is an interesting exercise to confirm that if, say, $[a_0\ ,\ a_1\ ,\ \ldots\ldots\ ,\ a_n]$ is a convergent overestimating α, and $a_n > 1$, then the *intermediate convergent* $[a_0\ ,\ a_1\ ,\ \ldots\ldots\ ,\ a_n - 1]$ is a quite good underestimate for α.

We now return to the beginning. Noting that

$$\alpha = [a_0\ ,\ a_1\ ,\ \ldots] = a_0 + \frac{1}{[a_1\ ,\ a_2\ ,\ \ldots]}$$

we see that

$$a_0 = \lfloor \alpha \rfloor$$

and

$$\alpha_1 = [a_1\ ,\ a_2\ ,\ \ldots] = (\alpha - a_0)^{-1}\,.$$

The general step in the continued fraction algorithm is

$$a_n = \lfloor \alpha_n \rfloor \text{ and } \alpha_{n+1} = (\alpha_n - a_n)^{-1} \qquad n = 0,\ 1,\ 2,\ \ldots\ldots$$

An infinite partial quotient terminates the expansion. Since

$$[a_0\ ,\ a_1\ ,\ \ldots\cdots\ ,\ a_n]$$

is rational it is evident that if the continued fraction of some α terminates then that α is rational. Conversely, since, as is plain from (5), p_n and q_n are relatively prime, and, since by (3) the sequences $(|p_n|)$ and (q_n) are both monotonic increasing, it follows that if α is rational then its continued fraction does terminate. Indeed, for a rational $\alpha = b/c$, the continued fraction algorithm is just the Euclidean algorithm. Thus

$$\begin{aligned}
b &= a_0 c \ + c_1 && 0 \le c_1 < c \\
c &= a_1 c_1 \ + c_2 && 0 \le c_2 < c_1 \\
c_1 &= a_2 c_2 \ + c_3 && 0 \le c_3 < c_2 \\
&\ \ \vdots \\
c_{n-1} &= a_n c_n
\end{aligned}$$

corresponds to

$$\frac{b}{c} = [a_0\ ,\ a_1\ ,\ \cdots\ ,\ a_n] \text{ and } \gcd(b, c) = d = c_n$$

and explains the term 'partial quotient'. Since $b/c = p_n/q_n$ with $\gcd(p_n, q_n) = 1$ we must have $dp_n = b$ and $dq_n = c$. Moreover, by (5)

$$p_n q_{n-1} - p_{n-1} q_n = (-1)^{n+1} \text{ so } bq_{n-1} - cp_{n-1} = (-1)^{n-1} d\,,$$

and this displays the greatest common divisor as a Z-linear combination of b and c. By $|p_{n-1}| < |p_n|$ and $q_{n-1} < q_n$ it follows that this combination is minimal.

This is an appropriate point at which to remark that it will be an easy matter to generalise the continued fraction algorithm to completions of the quotient field of any Euclidean domain — for R is just the completion with respect to the usual absolute value $|\ |$ of the quotient field Q of the rational integers Z. An evident example replaces Z by the ring of polynomials over some field and R by the field of Laurent series over that field.

The entire matter of continued fractions of real numbers could have been introduced using the following

PROPOSITION 2. *A rational p'/q' with $\gcd(p', q') = 1$ is a convergent of α if and only if*

$$|q'\alpha - p'| < |q\alpha - p| \text{ for all integers } q < q' \text{ and } p\,.$$

PROOF: Suppose, as we may, that $q_{n-1} < q < q_n$. Then, by the unimodularity of the matrix

$$\begin{pmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{pmatrix}$$

there are integers a and b so that

$$\begin{aligned} ap_{n-1} + bp_n &= p \\ aq_{n-1} + bq_n &= q \end{aligned}$$

and, necessarily, $ab < 0$. Multiplying by α and subtracting yields

$$q\alpha - p = a(q_{n-1}\alpha - p_{n-1}) + b(q_n\alpha - p_n)\,.$$

But, by (10), we have $(q_{n-1}\alpha - p_{n-1})(q_n\alpha - p_n) < 0$. Hence

$$|q\alpha - p| = |a||q_{n-1}\alpha - p_{n-1}| + |b||q_n\alpha - p_n|\,,$$

and plainly $|q\alpha - p| > |q_n\alpha - p_n|$ as asserted. ∎

The proposition asserts that the convergents of α are exactly those quantities yielding the *locally best approximations* to α. It is an interesting exercise to develop the entire theory (working backwards in the present program) from the notion of locally best approximation; once again, the formula (5) plays the fundamental role.

Moreover, we have the following useful criterion:

PROPOSITION 3. *If*

$$|q\alpha - p| < \frac{1}{2q}$$

then p/q is a convergent of α.

Note that this condition is sufficient but not nececessary.

PROOF: By proposition 2 it suffices to show that $|q\alpha - p|$ is a locally best approximation. To see that is so take integers r, s with $0 < s < q$ and notice that

$$\begin{aligned} 1 \le |qr - ps| = |s(q\alpha - p) - q(s\alpha - r)| &\le s|q\alpha - p| + q|s\alpha - r| \\ &\le \frac{s}{2q} + q|s\alpha - r|\,. \end{aligned}$$

So certainly $q|s\alpha - r| \ge 1 - s/2q > 1/2$ and it follows that $|q\alpha - p| < |s\alpha - r|$ as claimed. ∎

Notice that it is just this criterion that is applied by Worley [7] at §8 of his remarks.

I conclude by applying the matrix correspondence to develop a formulaire: From

$$\alpha = [a_0\ ,\ a_1\ ,\ \ldots\cdots\ ,\ a_n\ ,\ \alpha_{n+1}] \longleftrightarrow \begin{pmatrix} p_n & p_{n-1} \\ q_n & q_{n_1} \end{pmatrix} \begin{pmatrix} \alpha_{n+1} & 1 \\ 1 & 0 \end{pmatrix}$$

we have

$$\alpha = \frac{\alpha_{n+1}p_n + p_{n-1}}{\alpha_{n+1}q_n + q_{n-1}} \text{ and } \alpha_{n+1} = -\frac{q_{n-1}\alpha - p_{n-1}}{q_n\alpha - p_n}\,.$$

Transposition of

$$\begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots\cdots \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{pmatrix}$$

yields

$$\frac{p_n}{p_{n-1}} = [a_n\ ,\ a_{n-1}\ ,\ \cdots\ ,\ a_0] \text{ and } \frac{q_n}{q_{n-1}} = [a_n\ ,\ a_{n-1}\ ,\ \cdots\ ,\ a_1]\,.$$

Hence

$$-\alpha_{n+1} = \frac{-\alpha q_{n-1} + p_{n-1}}{\alpha q_n + p_n} \longleftrightarrow -\alpha_{n+1} = [a_n\ ,\ a_{n-1}\ ,\ \cdots\ ,\ a_0\ ,\ -\alpha]\,.$$

1.2 Applying the theory of continued fractions. Suppose one suspects that some computed number is actually some nice neat vulgar fraction. For example, one's calculator has produced the number

$$\alpha = 2.117647059\ldots$$

Expanding α as a continued fraction yields

$$\alpha \approx [2\ ,\ 8\ ,\ 2] = 36/17$$

up to the accuracy of the data, essentially verifying the suspicion that $\alpha = 36/17$. Thus the continued fraction algorithm provides an efficient method of converting a decimal to a

vulgar fraction reversing the more usual algorithm that converts a fraction to a decimal. The point is, of course, that instead of having to test all possible rational approximations one only meets very good rational approximations.

This is the spirit of Wiener's cryptanalytic attack on the use of short secret exponents in the RSA cipher mentioned by Lidl [4] in this volume. Recall that $n = uv$ (I use u and v for the unknown primes since I wish to mind my p s and q s for convergents) and one hopes to guess $(u-1)(v-1) = n - (u+v) + 1$. More precisely, one wishes, given the public key e to find a secret key d so that

$$ed \equiv 1 \bmod \operatorname{lcm}(u-1, v-1)\,.$$

Now this is just

$$ed = 1 + k(u-1)(v-1) = 1 + k(n - (u+v) + 1)\,,$$

so certainly

$$\frac{k}{d} - \frac{e}{n} < k(u+v)/nd\,.$$

One expects that $u \simeq v \simeq n^{\frac{1}{2}}$. Then k/d is necessarily a convergent of e/n if $n^{\frac{1}{2}} \gg kd$. The convergents can all be found in polynomial time and, as Lidl points out, each is readily tested for correctness by parity check and detection of squares. Thus the encryption scheme is insecure if $d < n^{\frac{1}{4}}$ and k is not large. However $kn \simeq ed$, so, indeed, choosing $e \gg n^{\frac{3}{2}}$ always protects against the present rather naïve attack.

To save clutter I have not emphasised the fact that k is a rational with denominator $\gcd(u-1, v-1)$ rather than an integer as my notation suggests.

1.3 Continued fraction expansion of Laurent series. Suppose now that the partial quotients $a_i = a_i(X)$ are polynomials each (other than perhaps $a_0(X)$ which may be constant) of degree at least 1. The formalism is unchanged but one needs to understand the sense in which a series

$$\alpha(X) = a_0(X) + \frac{1}{q_0(X)q_1(X)} - \frac{1}{q_1(X)q_2(X)} + \cdots = a_0(X) + \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{q_{n-1}(X)q_n(X)} \tag{11}$$

converges when $(q_n(X))$ is a sequence of polynomials with monotonically increasing degree. The essence is to so 'value' rational functions that the terms of the sum (11) have value decreasing to zero. It turns out the order of vanishing at infinity yields the appropriate value. In effect one views the polynomials $q_i(X)$ as rational functions in X^{-1} and then the sum (11) 'converges' as a formal power series in X^{-1}. The limit α of the continued fraction is a Laurent series, in fact, the sum of a polynomial $a_0(X)$ and a power series in X^{-1}. The continued fraction algorithm proceeds by taking the polynomial part (including the constant term) of the complete quotient and then inverting the remainder to yield the next complete quotient.

1.4 Continued fraction expansion of algebraic numbers. It is not difficult to see that a periodic continued fraction represents a zero of a quadratic polynomial. The converse, Legendre's Theorem, is somewhat deeper but, indeed, every real quadratic irrational has a periodic continued fraction expansion. In an important sense the continued fraction algorithm is tailored to quadratic quantities: that is manifested in the correspondence with products of 2×2 matrices. Williams [6] alludes at §2 to the manner in which the continued fraction algorithm yields an information on the ideal class group of a real quadratic field.

For algebraic numbers of higher degree it is conjectured on deep theoretical grounds that the partial quotients are always unbounded but, in fact, no example displaying that property is known (nor, of course, is any counterexample). There is not all that much experimental data and more might prove instructive. On the other hand, surprisingly perhaps, the analogous situation for Laurent series over a finite field is different [1]. There are nonperiodic continued fractions all of whose partial quotients are polynomials of degree 1 which represent Laurent series algebraic over the rational functions. Thus, see Lidl [L], §4 for the relevant notion, there are sequences (s_n) with perfect linear complexity profile for which $\sum s_n X^{-n}$ is an algebraic function of degree greater than 2.

2. Recurrence Sequences

2.1 Generalised power sums, rational functions and recurrence sequences. A *generalised power sum* $a(h)\,,\ h=0,1,2,\ldots\ldots$ is an expression of the shape

$$a(h)=\sum_{i=1}^{m} A_i(h)\alpha_i^h\ ,\ h=0,1,2,\ldots\ldots \tag{12}$$

with *roots* $\alpha_i\,, 1\le i\le m\,,$ distinct non-zero quantities, and *coefficients* $A_i(h)$ polynomials of respective degrees $n_i-1\,,$ for positive integers $n_i\,,\ 1\le i\le m\,.$ The generalised power sum $a(h)$ is said to have *order*

$$n=\sum_{i=1}^{m} n_i\,.$$

Set

$$s(X)=\prod_{i=1}^{m}(1-\alpha_i X)^{n_i}=1-s_1X-\cdots-s_nX^n\,. \tag{13}$$

Then the sequence (a_h) with $a_h=a(h)\,,\ h=0,1,2,\ldots\ldots$ satisfies the linear homogeneous recurrence relation

$$a_{h+n}=s_1a_{h+n-1}+\cdots+s_na_h\,,\ h=0,1,2,\ldots\,. \tag{14}$$

To see this let $E: f(h)\mapsto f(h+1)$ be the shift operator and $\Delta=E-1$ the difference operator. Then

$$(E-\alpha)\big(A_i(h)\alpha_i^h\big)=(\Delta A_i(h))\alpha_i^{h+1}$$

and since $\Delta A_i(h)$ has lower degree than does A_i, by linearity of E and induction it is plain that

$$\prod_{i=1}^{m}(E-\alpha_i)^{n_i}$$

annihilates the sequence (a_h) as asserted. Thus generalised power sums are interesting in that they coincide with the sequences satisfying the recurrence relations (14). It follows that there is a polynomial $r(x)$, of degree less than n, so that the power series

$$\sum_{h=0}^{\infty} a_h X^h = \frac{r(X)}{s(X)} \tag{15}$$

is a rational function; to see this multiply by $s(X)$ and note the recurrence relation.

Conversely given a rational function as above, with $\deg r < \deg s$, a partial fraction expansion yields

$$\frac{r(X)}{s(X)} = \sum_{i=1}^{m}\sum_{j=1}^{n_i}\frac{r_{ij}}{(1-\alpha_i X)^j} = \sum_{h=0}^{\infty}\left(\sum_{i=1}^{m}\sum_{j=1}^{n_i} r_{ij}\binom{h+j-1}{j-1}\alpha_i^h\right)X^h$$

and the coefficients of X^h, $h = 0, 1, 2, \ldots\ldots$ are indeed the values of a generalised power sum as described.

Accordingly, results on generalised power sums are equivalent to corresponding results for the Taylor coefficients of rational functions.

A sequence (a_h) satisfying a relation (14) is often called a *recurrence sequence* (or *linearly recursive sequence*) of *order* n; the polynomial $X^n s(X^{-1})$ reciprocal to the polynomial (13) is called the *characteristic* or *companion polynomial* of the recurrence sequence. Our "roots" α_i are the distinct zeros of the companion polynomial. The archetypal example of a recurrence sequence is of course the celebrated Fibonacci sequence (f_h) defined by

$$f_{h+2} = f_{h+1} + f_h\,,\ h = 0, 1, 2, \ldots \text{ with } f_0 = 0\,, f_1 = 1\ ;$$

and generated by

$$\frac{X}{1-X-X^2} = \sum_{h=0}^{\infty} f_h X^h\,.$$

The expression (12) for the $a_h = a(h)$ as a generalised power sum provides a well known formula for the terms of a recurrence sequence. One obtains a less well known formula from directly expanding (15). In terms of the given *initial values* $a_0, a_1, \ldots, a_{n-1}$ of (a_h) one has

$$r(X) = \sum_{j=0}^{n-1}\left(a_j - \sum_{i=1}^{j} s_i a_{j-i}\right)X^j\,,$$

and

$$s(X)^{-1} = \sum_{h=0}^{\infty} \sum_{j_1+2j_2\cdots+nj_n=h} \frac{(j_1+j_2\cdots+j_n)!}{j_1!\ldots j_n!} s_1^{j_1}\cdots s_n^{j_n} X^h\,.$$

For the Fibonacci numbers this yields (with the usual conventions for interpreting the combinatorial symbol)

$$f_{h+1} = \sum_j \binom{h-j}{j}\,.$$

2.2 Hadamard operations. If $\sum a_h X^h$ and $\sum b_h X^h$ represent rational functions then so do their sum $\sum(a_h+b_h)X^h$ and their *Hadamard product*

$$\sum a_h b_h X^h\,.$$

This is not obvious as stated but is an immediate consequence of the fact that the sum and, respectively, the product of generalised power sums is again a generalised power sum. Incidentally, it turns out that the Hadamard product of a rational and of an algebraic power series is algebraic but over a field of characteristic zero the Hadamard product of algebraic functions is not necessarily algebraic. The most quoted example is

$$(1-4x_1)^{-1/2} = \sum \binom{2h}{h} x_1^h\,,\ \text{but}\ \sum \binom{2h}{h}^2 x_1^h$$

is not algebraic. The first remark is the useful identity

$$\binom{2h}{h} = (-1)^h \binom{-\frac{1}{2}}{h}$$

and, with a little work and some elementary calculus one sees that the latter series is given by the integral

$$\frac{2}{\pi}\int_0^{\pi/2} \frac{dt}{\sqrt{(1-16x_1\sin^2 t)}}\,.$$

This is a complete elliptic integral well known not to represent an algebraic function.

Remarkably, [3] the Hadamard product of algebraic power series defined over a field of *positive* characteristic is always again algebraic; in particular this is so for the Hadamard product of algebraic power series over a finite field. It turns out the sequences of Taylor coefficients of algebraic functions over finite fields are generated by finite automata, suggesting a rather more subtle source for stream ciphers quite different from those generated by rational functions. An efficient introduction to the mathematical background may be found in [5].

2.3 Recurrence sequences and LFSR s. Recall that (a_h) is a recurrence sequence if and only if its terms are given by a generalised power sum

$$a(h) = a_h = \sum_{i=1}^{m} A_i(h)\alpha_i^h \ , \quad h = 0, 1, 2, \ldots \ldots$$

and that the recurence sequence has characteristic polynomial

$$\prod_{i=1}^{m} (X - \alpha_i)^{n_i} \ .$$

Obviously, for each positive integer d, (a_{dh}) again yields a generalised power sum, and it has characteristic polynomial

$$\prod_{i=1}^{m} (X - \alpha_i^d)^{n_i} \ .$$

A generalised power sum yields a periodic sequence if and only if each root α_i is a root of unity and each coefficient $A_i(h)$ is a periodic function of h. Over a finite field a nonzero element is a root of unity and in characteristic p a polynomial in h is trivially periodic with period p. Thus, over a finite field every recurrence sequence is periodic. Conversely, a periodic sequence with period t is the sequence of Taylor coefficients of a rational function with denominator $1 - X^t$.

Given the characteristic polynomial, the initial values a_0, a_1 $\ldots$, a_{n-1} of the recurrence sequence, the coefficients A_i of the generalised power sum and the numerator of the generating rational function determine one another. Different recurrence sequences with the same characteristic polynomial are the sequences of Taylor coefficients of rational functions with the one denominator but different numerators.

The product of k generalised power sums each with roots α_i, but possibly with different coefficients, is a generalised power sum with roots consisting of all monomials of weight k in the α s. Hence the non-linear combination of recurrence sequences defined at §4.1 of [2] is a recurrence sequence with roots consisting of all monomials of weight at most L in the roots of the original sequence. The Groth sequences mentioned at §4.3 of [2] are sums of different recurrence sequences each with characteristic polynomial having zeros consisting of all pairs $\alpha_i\alpha_j$.

More generally, each of the sequences mentioned in [D], no matter how apparently complex its formation rule, is itself a recurrence sequence which, in principle, can be generated by the one simple LFSR. That follows immediately over the finite field $\mathbf{F}_2$ by periodicity, but in fact, with the exception of the 'multiplexed sequence' mentioned at §7.2, would hold had the generating sequences been defined over any field. The formation rules are a trade-off between ease of generation and the endeavour to satisfy various 'randomness' criteria.

References

[1] L. E. Baum and M. M. Sweet, 'Continued fractions of algebraic poower series in characteristic 2', *Annals of Math.* **103** (1976), 593–610

[2] Ed Dawson, 'Linear feedback shift registers and stream ciphers', this volume

[3] H. Furstenberg, 'Algebraic functions over finite fields', J. Alg **7** (1967), 271–277

[4] R. Lidl,'Mathematical aspects of cryptanalysis', this volume

[5] Leonard Lipshitz and Alfred J. van der Poorten, 'Rational functions, diagonals, automata and arithmetic', in Richard A. Mollin ed., *Number Theory*, (First Conference of the Canadian Number Theory Association, Banff 1988), (de Gruyter, 1989)

[6] H. C. Williams, 'Quadratic fields and cryptography' this volume

[7] R. T. Worley, 'Insecurity of the knapsack one-time pad', this volume

School of Mathematics, Physics, Computing and Electronics

Macquarie University, NSW 2109

Australia

alf@mqcomp.mqcs.mq.oz