RECENT RESULTS ON LINEAR RECURRENCE SEQUENCES

Jan-Hendrik Evertse (Leiden)

General Mathematics Colloquium, Delft

May 19, 2005

INTRODUCTION

A linear recurrence sequence $U = \{u_n\}_{n=0}^{\infty}$ (in $\mathbb{C}$) is a sequence given by a *linear recurrence*

$$(1) \quad u_n = c_1 u_{n-1} + c_2 u_{n-2} + \cdots + c_k u_{n-k} \quad (n \geqslant k)$$

with coefficients $c_i \in \mathbb{C}$ and *initial values* $u_0, \ldots, u_{k-1} \in \mathbb{C}$.

The smallest k such that U satisfies a recurrence of type (1) is called the *order* of U.

If k is the order of U, then the coefficients $c_1, \ldots, c_k$ are uniquely determined.
In that case the *companion polynomial* of U is given by

$$F_U(X) := X^k - c_1 X^{k-1} - c_2 X^{k-2} - \cdots - c_k \, .$$

FACT. *Let* $U = \{u_n\}_{n=0}^{\infty}$ *be a linear recurrence sequence. Assume that its companion polynomial can be factored as*

$$(2) \qquad F_U(X) = (X - \alpha_1)^{e_1} \cdots (X - \alpha_r)^{e_r}$$

with distinct $\alpha_1, \ldots, \alpha_r$ *and* $e_i > 0$.

Then u_n *can be expressed as a polynomial-exponential sum,*

$$(3) \qquad u_n = \sum_{i=1}^{r} f_i(n)\alpha_i^n \quad \text{for } n \geqslant 0$$

where f_i *is a polynomial of degree* $e_i - 1$ *(*$i = 1, \ldots, r$*).*

Conversely, if $\{u_n\}_{n=0}^{\infty}$ *is given by (3) then it is a linear recurrence sequence with companion polynomial given by (2).*

Proof. Let $U = \{u_n\}_{n=0}^{\infty}$ be a linear recurrence sequence of order k with companion polynomial

$$\begin{aligned} F_U(X) &= X^k - c_1 X^{k-1} - \cdots - c_k \\ &= (X-\alpha_1)^{e_1} \cdots (X-\alpha_r)^{e_r}. \end{aligned}$$

Then for some polynomial A of degree $< k$ and for certain constants c_{ij},

$$\begin{aligned} \sum_{n=0}^{\infty} u_n X^n &= \frac{A(X)}{1 - c_1 X - c_2 X^2 - \cdots - c_k X^k} \\ &= \sum_{i=1}^{r} \sum_{j=1}^{e_i} \frac{c_{ij}}{(1-\alpha_i X)^j} \\ &= \sum_{i=1}^{r} \sum_{j=1}^{e_i} c_{ij} \sum_{n=0}^{\infty} \binom{n+j-1}{j-1} \alpha_i^n X^n . \end{aligned}$$

ZERO MULTIPLICITY

The *zero multiplicity* of a linear recurrence sequence $U = \{u_n\}_{n=0}^{\infty}$ is given by
$N(U) := \#\{n \in \mathbb{Z}_{\geqslant 0} : u_n = 0\}$.

Assume that U has companion polynomial

$$F_U(X) = (X - \alpha_1)^{e_1} \cdots (X - \alpha_r)^{e_r}$$

with α_i distinct, $e_i > 0$.
U is called *non-degenerate* if none of the quotients α_i/α_j $(1 \leqslant i < j \leqslant r)$ is a root of unity.

THEOREM (Skolem-Mahler-Lech, 1934-35-53)
Let U be a non-degenerate linear recurrence sequence. Then $N(U)$ is finite.

Example. Let $U = \{u_n\}_{n=0}^{\infty}$ be given by

$$u_n = 3^n + (-3)^n + n(2^n - (2e^{2\pi i/3})^n) \quad (n \geqslant 0).$$

Then U has companion polynomial
$F_U(X) = (X-3)(X+3)(X-2)^2(X-2e^{2\pi i/3})^2$
and $u_n = 0$ for $n = 3, 9, 15, \ldots$.

Problem. Suppose that U is non-degenerate. Find a good upper bound for $N(U)$.

Example. Let $U = \{u_n\}_{n=0}^{\infty}$ be a linear recurrence sequence of order k with terms in $\mathbb{R}$. Suppose that its companion polynomial is

$$F_U(X) = (X - \alpha_1)^{e_1} \cdots (X - \alpha_r)^{e_r}$$

with $0 < \alpha_1 < \cdots < \alpha_r$. Then U is non-degenerate and

$$u_n = \sum_{i=1}^{r} f_i(n)\alpha_i^n \quad (n \geqslant 0)$$

where the f_i are polynomials with real coefficients.

FACT (Follows from Rolle's Theorem)
The function $u(x) := \sum_{i=1}^{r} f_i(x)\alpha_i^x$ has at most $\sum_{i=1}^{r} \deg f_i \leqslant k-1$ zeros in $\mathbb{R}$.

Hence $N(U) \leqslant k-1$.

Old conjecture: $N(U) \leqslant C(k)$ for *every* non-degenerate linear recurrence sequence U of order k with terms in $\mathbb{C}$.

Linear recurrence sequences of order 3

THEOREM (Beukers, 1991)
Let $U = \{u_n\}_{n=0}^{\infty}$ *be a non-degenerate linear recurrence sequence of order* 3 *with terms in* $\mathbb{Q}$. *Then*

$$N(U) \leqslant 6.$$

Example (Berstel, 1974)
$u_{n+3} = 2u_{n+2} - 4u_{n+1} + 4u_n$ $(n \geqslant 3)$,
$u_0 = u_1 = 0$, $u_2 = 1$.
Then $u_0 = u_1 = u_4 = u_6 = u_{13} = u_{52} = 0$.

THEOREM (Beukers, Schlickewei, 1996)
Let $U = \{u_n\}_{n=0}^{\infty}$ *be a non-degenerate linear recurrence sequence of order* 3 *with terms in* $\mathbb{C}$. *Then*

$$N(U) \leqslant 61.$$

Linear recurrence sequences of arbitrary order

Earlier results in the 1990's:
Schlickewei, van der Poorten and Schlickewei, Schlickewei and Schmidt:
upper bounds for $N(U)$ valid for linear recurrence sequences with algebraic terms and depending on the order k of U and other parameters.

THEOREM (Schmidt, 2000).
Let $U = \{u_n\}_{n=0}^{\infty}$ be a non-degenerate linear recurrence sequence of order k with terms in $\mathbb{C}$. Then

$$N(U) \leqslant \exp\exp\exp(20k).$$

Steps in the proof.

1) Reduce to the case that all terms of U are algebraic numbers, using a specialization argument from algebraic geometry.

2) Apply techniques from Diophantine approximation, the Quantitative p-adic Subspace Theorem.

3) Write $u_n = \sum_{i=1}^{r} f_i(n)\alpha_i^n$, where the f_i are polynomials. The proof is by induction on $\sum_{i=1}^{r} \deg f_i$.

4) Special case (Schlickewei, Schmidt, Ev.) Suppose that $u_n = \sum_{i=1}^{k} c_i\alpha_i^n$ where the c_i are non-zero constants. Then

$$N(U) \leqslant e^{(6k)^{3k}}.$$

THE QUOTIENT OF TWO LINEAR RECURRENCE SEQUENCES

If $\{u_n\}_{n=0}^{\infty}$, $\{v_n\}_{n=0}^{\infty}$ are linear recurrence sequences, then so are $\{\lambda u_n + \mu v_n\}_{n=0}^{\infty}$ $(\lambda, \mu \in \mathbb{C})$ and $\{u_n \cdot v_n\}_{n=0}^{\infty}$. What about $\{u_n/v_n\}_{n=0}^{\infty}$?

If this is a linear recurrence sequence then $u_n/v_n = \sum_{i=1}^{r} h_i(n)\gamma_i^n$ for certain polynomials h_i and certain γ_i.

Hence all terms u_n/v_n lie in a finitely generated subring of $\mathbb{C}$, namely the ring generated by the γ_i and the coefficients of the h_i.

THEOREM (Pourchet, 1979, van der Poorten, 1988)
Let $U = \{u_n\}_{n=0}^{\infty}$, $V = \{v_n\}_{n=0}^{\infty}$ be two linear recurrence sequences with terms in $\mathbb{C}$. Suppose that there is a finitely generated subring R of $\mathbb{C}$ such that $u_n/v_n \in R$ for all but finitely many n.
Then there is $n_0 \geqslant 0$ such that $\{u_n/v_n\}_{n=n_0}^{\infty}$ is a linear recurrence sequence.

Can we weaken the condition
"$u_n/v_n \in R$ for all but finitely many n" to
"$u_n/v_n \in R$ for infinitely many n"?

THEOREM (Corvaja, Zannier, 2002)
Let $U = \{u_n\}_{n=0}^{\infty}$, $V = \{v_n\}_{n=0}^{\infty}$ be two linear recurrence sequences with terms in $\mathbb{C}$. Assume that there is a finitely generated subring R of $\mathbb{C}$ such that $u_n/v_n \in R$ for infinitely many n.

Then there are a polynomial $g(X)$ and positive integers a, b such that

$$\left\{g(an+b)\frac{u_{an+b}}{v_{an+b}}\right\}_{n=0}^{\infty}, \quad \left\{\frac{v_{an+b}}{g(an+b)}\right\}$$

are linear recurrence sequences.

Proof.
1) Reduce to the case that U, V have algebraic terms by a specialization argument.
2) Apply the p-adic Subspace Theorem.

Example.

Let

$$u_n = 4^{n-1} - (-1)^{n-1},$$
$$v_n = n \cdot 2^{n-1} + n \cdot (-1)^{n-1} \quad (n \geqslant 0).$$

For every prime number $n \geqslant 3$ we have

$$\frac{u_n}{v_n} = \frac{4^{n-1} - 1}{n(2^{n-1} + 1)} = \frac{2^{n-1} - 1}{n} \in \mathbb{Z}$$

(using Fermat's little theorem).

Hence $u_n/v_n \in \mathbb{Z}$ for infinitely many n.

Verify that

$$(2n+1) \cdot \frac{u_{2n+1}}{v_{2n+1}} = 2^{2n} - 1, \quad \frac{v_{2n+1}}{2n+1} = 2^{2n} + 1$$

are linear recurrence sequences, but that $\{u_n/v_n\}_{n=0}^{\infty}$ and $\{nu_n/v_n\}_{n=0}^{\infty}$ are not linear recurrence sequences.

D-TH ROOTS OF LINEAR RECURRENCE SEQUENCES

Let d be a positive integer, let $\{u_n\}_{n=0}^{\infty}$ be a linear recurrence sequence and suppose that there is a linear recurrence sequence $\{v_n\}_{n=0}^{\infty}$ such that $u_n = v_n^d$ for all n. Write

$$v_n = \sum_{i=1}^{r} h_i(n)\gamma_i^n$$

where $\gamma_i \in \mathbb{C}$ and h_i is a polynomial.
Let R be the ring generated by the γ_i and the coefficients of the h_i.
Then for every n there is $y \in R$ with $y^d = u_n$.

THEOREM (Zannier, 2000)
Let d be a positive integer, let $\{u_n\}_{n=0}^{\infty}$ be a linear recurrence sequence with terms in $\mathbb{C}$ and suppose that there is a finitely generated subring of $\mathbb{C}$ such that for every $n \geqslant 0$ there is $y \in R$ with $y^d = u_n$.
Then there is a linear recurrence sequence $\{v_n\}_{n=0}^{\infty}$ such that $v_n^d = u_n$ for every $n \geqslant 0$.

Proof. Specialization, algebraic number theory, arithmetic geometry.

What if there is $y \in R$ with $y^d = u_n$ for infinitely many n?

THEOREM (Corvaja, Zannier, 1998)
Let d be a positive integer. Let $\{u_n\}_{n=0}^{\infty}$ be a linear recurrence sequence with terms in $\mathbb{Q}$, satisfying the following condition:

$$u_n = \sum_{i=1}^{r} c_i \alpha_i^n \quad \textit{for } n \geqslant 0,$$

where the c_i are non-zero constants, and where

$$|\alpha_1| > \max(|\alpha_2|, \ldots, |\alpha_r|).$$

Assume that for infinitely many n there is $y \in \mathbb{Q}$ such that $y^d = u_n$.
Then there are a linear recurrence sequence $\{v_n\}_{n=0}^{\infty}$ with terms in $\mathbb{Q}$, as well as positive integers a, b, such that

$$v_n^d = u_{an+b} \quad \textit{for every } n \geqslant 0.$$

Proof. p-adic Subspace Theorem.

THE SUBSPACE THEOREM

For $\mathbf{x} = (x_1, \ldots, x_m) \in \mathbb{Z}^m$ put

$$\|\mathbf{x}\| := \max(|x_1|, \ldots, |x_m|)$$

SUBSPACE THEOREM (Schmidt, 1972)
Let $L_i(X) = \alpha_{i1}X_1 + \cdots + \alpha_{im}X_m$ $(i = 1, \ldots, m)$ be m linearly independent linear forms in m variables with algebraic coefficients in $\mathbb{C}$ and let $\delta > 0$.

Then the set of solutions $\mathbf{x} \in \mathbb{Z}^m$ of

$$|L_1(\mathbf{x}) \cdots L_m(\mathbf{x})| \leqslant \|\mathbf{x}\|^{-\delta}$$

is contained in the union of finitely many proper linear subspaces of $\mathbb{Q}^m$.

Example ($m = 3$). Consider

(4)

$$|(x_1 - \sqrt{2}x_2)(x_1 + \sqrt{2}x_2)(x_3 - \sqrt{2}x_2)| \leqslant \|\mathbf{x}\|^{-1}.$$

1) (4) has infinitely many solutions $\mathbf{x} = (x_1, x_2, x_3) \in \mathbb{Z}^3$ in the subspace $x_1 = x_3$, which are given by $x_1 = x_3$, $|x_1^2 - 2x_2^2| = 1$, $x_1 x_2 \geqslant 0$.

2) (4) has infinitely many solutions $\mathbf{x} \in \mathbb{Z}^3$ in the subspace $x_1 = -x_3$, which are given by $x_1 = -x_3$, $|x_1^2 - 2x_2^2| = 1$, $x_1 x_2 \leqslant 0$.

3) (4) has only finitely many solutions $\mathbf{x} \in \mathbb{Z}^3$ with $x_1 \neq \pm x_3$, given by $(\pm 1, 0, 0)$, $(0, 0, \pm 1)$.

Remark. The Pell equation $|x_1^2 - 2x_2^2| = 1$ has infinitely many solutions in integers x_1, x_2.

p-adic absolute values

Given a prime number p we define the p-adic absolute value $|\cdot|_p$ on $\mathbb{Q}$ by

$|0|_p = 0$;

$|a|_p = p^{-r}$ if $a = p^r b/c$ where b, c are integers not divisible by p.

Example: $|\frac{9}{200}|_2 = 2^3$ since $\frac{9}{200} = 2^{-3}\frac{9}{25}$.
Likewise $|\frac{9}{200}|_3 = 3^{-2}$.

Properties:
$|ab|_p = |a|_p |b|_p$; $|a+b|_p \leqslant \max(|a|_p, |b|_p)$;
$a \in \mathbb{Z}$, a divisible by $p^r \Rightarrow |a|_p \leqslant p^{-r}$.

Product formula:
a composed of primes $p_1, \ldots, p_t$
$\Rightarrow |a| \cdot |a|_{p_1} \cdots |a|_{p_t} = 1$.

P-ADIC SUBSPACE THEOREM

(Schlickewei, 1977)

Let $p_1, \ldots, p_t$ be distinct prime numbers.

Let $L_1(X), \ldots, L_m(X)$ be m linearly independent linear forms in m variables with coefficients in $\mathbb{Q}$.

For each $p \in \{p_1, \ldots, p_t\}$, let $L_{1p}(X), \ldots, L_{mp}(X)$ be m linearly independent linear forms in m variables with coefficients in $\mathbb{Q}$.

Let $\delta > 0$.

Then the set of solutions $\mathbf{x} \in \mathbb{Z}^m$ of

$$|L_1(\mathbf{x}) \cdots L_m(\mathbf{x})| \cdot \prod_{i=1}^{t} |L_{1,p_i}(\mathbf{x}) \cdots L_{m,p_i}(\mathbf{x})|_{p_i} \leqslant \|\mathbf{x}\|^{-\delta}$$

is contained in the union of finitely many proper linear subspaces of $\mathbb{Q}^m$.

Remark 1. There is a more general result in which the coefficients of the linear forms L_i, L_{ip} are algebraic, and the solutions $\mathbf{x}$ have their coordinates in a given algebraic number field (Schmidt, Schlickewei).

Remark 2. All proofs given up to now for the (p-adic) Subspace Theorem are *ineffective*, i.e., these proofs do not allow to determine effectively the subspaces containing all solutions.

Remark 3. There is however a *Quantitative p-adic Subspace Theorem*, giving an explicit upper bound for the *number* of subspaces containing all solutions (Schmidt 1989, Schlickewei 1991,..., Schlickewei& Ev., 2002).

This is a crucial tool in the proof of Schmidt's theorem on the zero multiplicity of linear recurrence sequences.

AN APPLICATION

We prove:

THEOREM *Let p, q be two prime numbers with $p > q$. Then there are only finitely many positive integers n such that*

$$\frac{p^n - 1}{q^n - 1} \in \mathbb{Z}\,.$$

(This is a special case of the Theorem of Corvaja and Zannier on quotients of linear recurrence sequences).

Let h be a positive integer. Then

$$(q^{hn}-1)\frac{p^n-1}{q^n-1}=(p^n-1)\Big(\sum_{i=0}^{h-1} q^{in}\Big).$$

Hence

$$q^{hn}\frac{p^n-1}{q^n-1}+\sum_{i=0}^{h-1} q^{in}-\sum_{i=0}^{h-1} p^n q^{in}=\frac{p^n-1}{q^n-1},$$

or

$$x_1+x_2+\cdots+x_{2h+1}=\frac{p^n-1}{q^n-1}$$

where

$x_1=q^{hn}\frac{p^n-1}{q^n-1}$,

$x_i=q^{(i-2)n}$ $(i=2,\ldots,h+1)$,

$x_i=-p^n q^{(i-h-2)n}$ $(i=h+2,\ldots,2h+1)$.

Put

$$\begin{aligned}\mathbf{x}_n &:= (x_1, x_2, \ldots, x_{2h+1}) \\ &= (q^{hn}\tfrac{p^n-1}{q^n-1}, 1, \ldots, q^{(h-1)n}, \\ &\qquad\qquad -p^n, \ldots, -p^n q^{(h-1)n}).\end{aligned}$$

LEMMA *Let $q^{h+1} > p$. Then there is $\delta > 0$ such that for all sufficiently large n with $\frac{p^n-1}{q^n-1} \in \mathbb{Z}$ we have*

$$\begin{aligned}&|(x_1 + \cdots + x_{2h+1})x_2 \cdots x_{2h+1}| \cdot \\ &\qquad \cdot |x_1 \cdots x_{2h+1}|_p \cdot |x_1 \cdots x_{2h+1}|_q \leqslant \|\mathbf{x}_n\|^{-\delta}.\end{aligned}$$

Hence $\{\mathbf{x}_n : \frac{p^n-1}{q^n-1} \in \mathbb{Z}\}$ is contained in a finite union of proper linear subspaces of $\mathbb{Q}^{2h+1}$.

Proof. Suppose $z_n := \frac{p^n-1}{q^n-1} \in \mathbb{Z}$. Recall

$$\begin{aligned}\mathbf{x}_n &= (x_1, x_2, \ldots, x_{2h+1}) \\ &= (q^{hn}\tfrac{p^n-1}{q^n-1}, 1, \ldots, q^{(h-1)n}, \\ &\qquad\qquad -p^n, \ldots, -p^n q^{(h-1)n}).\end{aligned}$$

Hence

$\|\mathbf{x}_n\| = q^{hn}\frac{p^n-1}{q^n-1} \approx (pq^{h-1})^n$.

Further,

$|x_1 + \cdots + x_{2h+1}| = \frac{p^n-1}{q^n-1}$;

$|x_1|_p = |q^{hn} z_n|_p = 1$;

$|x_1|_q = |q^{hn} z_n|_q \leqslant q^{-hn}$;

$|x_i| \cdot |x_i|_p \cdot |x_i|_q = 1$ for $i = 2, \ldots, 2h+1$

and so the product of these terms is at most

$$q^{-hn}\frac{p^n - 1}{q^n - 1} \approx (q^{h+1}/p)^{-n} \approx \|\mathbf{x}_n\|^{-\delta}$$

where $\delta = \frac{\log q^{h+1}/p}{pq^{h-1}}$. QED.

The set $\{\mathbf{x}_n : \frac{p^n-1}{q^n-1} \in \mathbb{Z}\}$ is contained in the union of finitely many proper linear subspaces of $\mathbb{Q}^{2h+1}$.

It suffices to show that if T is any proper linear subspace of $\mathbb{Q}^{2h+1}$, then there are only finitely many n such that $\mathbf{x}_n \in T$.

W.l.o.g. T is given by an equation

$$a_1 x_1 + \cdots + a_{2h+1} x_{2h+1} = 0 \quad \text{with } a_i \in \mathbb{Q}.$$

Substitute

$$\mathbf{x}_n = (q^{hn} \tfrac{p^n - 1}{q^n - 1}, 1, \ldots, q^{(h-1)n}, \\ -p^n, \ldots, -p^n q^{(h-1)n})$$

and multiply with $q^n - 1$.

Then we obtain an equation

$$\sum_{i=1}^{r} c_i \alpha_i^n = 0$$

where each α_i is an integer composed of p and q and each c_i is a constant.

The left-hand side is a non-degenerate linear recurrence sequence.
So by the Skolem-Mahler-Lech Theorem (or Rolle's Theorem), there are only finitely many possibilities for n. **QED**

Two integers a, b are called *multiplicatively independent* if there are no positive integers m, n such that $a^m = b^n$.

By extending the above argument, the following result can be proved:

THEOREM (Bugeaud, Corvaja, Zannier, 2003) *Let a, b be two multiplicatively independent integers. Then*

$$\lim_{n\to\infty} \frac{\log \gcd(a^n - 1, b^n - 1)}{n} = 0.$$