Abstract

Linear recurrence sequences,

Michel Waldschmidt

Sorbonne University, Paris Institut de Mathématiques de Jussieu http://www.imj-prg.fr/~michel.waldschmidt/

Applications of linear recurrence sequences

Combinatorics

Elimination

Symmetric functions

Hypergeometric series

Language

Communication, shift registers

Finite difference equations

Logic

Approximation

Pseudo-random sequences

Linear recurrence sequences are ubiquitous. They occur in biology, economics, computer science (analysis of algorithms), digital signal processing and number theory. We give a survey of this subject, together with connections with linear combinations of powers, with powers of matrices and with linear differential equations. We first work over a field of any characteristic. Next we consider linear recurrence sequences over finite fields.

◆□ ▶ < □ ▶ < ■ ▶ < ■ ▶ < ■ ▶ < ■ ▶ < ■ ▶ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ∧ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ < ■ ♪ <

Applications of linear recurrence sequences

- Biology (Integrodifference equations, spatial ecology).
- Computer science (analysis of algorithms).
- Digital signal processing (infinite impulse response (IIR) digital filters).
- Economics (time series analysis).

https://en.wikipedia.org/wiki/Recurrence_relation

Linear recurrence sequences : definitions

A linear recurrence sequence is a sequence of numbers $\mathbf{u} = (u_0, u_1, u_2, \dots)$ for which there exist a positive integer d together with numbers a_1, \ldots, a_d with $a_d \neq 0$ such that, for $n \geq 0$,

(*) $u_{n+d} = a_1 u_{n+d-1} + \dots + a_d u_n.$

Here, a *number* means an element of a field \mathbb{K} .

Given $\underline{a} = (a_1, \ldots, a_d) \in \mathbb{K}^d$, the set E_a of linear recurrence sequences $\mathbf{u} = (u_n)_{n \ge 0}$ satisfying (\star) is a K-vector subspace of dimension d of the space $\mathbb{K}^{\mathbb{N}}$ of all sequences.

A basis of this space is obtained by taking for the initial dvalues $(u_0, u_1, \ldots, u_{d-1})$ the elements of the canonical basis of \mathbb{K}^{d} . ・ ロ ト ・ 母 ト ・ ヨ ト ・ ヨ ・ つへで

5/46

Linear recurrence sequences : examples

• Constant sequence : $u_n = u_0$. Linear recurrence sequence of order 1 : $u_{n+1} = u_n$. Characteristic polynomial : f(X) = X - 1. Generating series :

$$\sum_{n\geq 0} u_0 X^n = \frac{u_0}{1-X} \cdot$$

• Geometric progression : $u_n = u_0 \gamma^n$. Linear recurrence sequence of order 1 : $u_n = \gamma u_{n-1}$. Characteristic polynomial $f(X) = X - \gamma$. Generating series :

$$\sum_{n\geq 0} u_0 \gamma^n X^n = \frac{u_0}{1 - \gamma X}$$

・ロト・日本・モン・モン・モー わへで 7 / 46

Generating series, characteristic polynomial

The generating series is the formal series

$$\sum_{n\geq 0} u_n X^n.$$

Let $\gamma \in K^{\times}$; the sequence $(\gamma^n)_{n\geq 0}$ satisfies the linear recurrence

(*) $u_{n+d} = a_1 u_{n+d-1} + \dots + a_d u_n.$

if and only if $\gamma^d = a_1 \gamma^{d-1} + \cdots + a_d$. The characteristic (or companion) polynomial of the linear recurrence is

 $f(X) = X^d - a_1 X^{d-1} - \dots - a_d$

Recall that 0 is not a root of this polynomial $(a_d \neq 0)$.

Linear recurrence sequences : examples

• $u_n = n$. This is a linear recurrence sequence of order 2 :

$$n+2 = 2(n+1) - n.$$

Characteristic polynomial

$$f(X) = X^2 - 2X + 1 = (X - 1)^2.$$

Generating series

$$\sum_{n \ge 0} nX^n = \frac{1}{1 - 2X + X^2}$$

Power of matrices :

$$\begin{pmatrix} 0 & 1 \\ -1 & 2 \end{pmatrix}^n = \begin{pmatrix} -n+1 & n \\ -n & n+1 \end{pmatrix}.$$

オロトオ間トオミトオミト ヨーのへの 8 / 46

Linear recurrence sequences : examples

• $u_n = p(n)$, where p is a polynomial of degree d. This is a linear recurrence sequence of order d + 1.

Proof. The sequences

 $(p(n))_{n\geq 0}, \quad (p(n+1))_{n\geq 0}, \quad \cdots, \quad (p(n+k))_{n\geq 0}$

are K-linearly independent in $\mathbb{K}^{\mathbb{N}}$ for k = d - 1 and linearly dependent for k = d.

A basis of the space of polynomials of degree d is given by the d+1 polynomials

```
p(X), p(X+1), \ldots, p(X+d).
```

Question : which is the characteristic polynomial?

Order of a linear recurrence sequence

If $\mathbf{u} = (u_n)_{n \ge 0}$ satisfies the linear recurrence, the characteristic polynomial of which is f, then, for any monic polynomial $g \in \mathbb{K}[X]$ with $g(0) \neq 0$, this sequence \mathbf{u} also satisfies the linear recurrence, the characteristic polynomial of which is fg. Example : for $g(X) = X - \gamma$ with $\gamma \neq 0$, from

$$(\star) \qquad \qquad u_{n+d} - a_1 u_{n+d-1} - \dots - a_d u_n = 0$$

we deduce

$$u_{n+d+1} - a_1 u_{n+d} - \dots - a_d u_{n+1} - \gamma (u_{n+d} - a_1 u_{n+d-1} - \dots - a_d u_n) = 0.$$

The order of a linear recurrence sequence is the smallest d such that (\star) holds for all $n \ge 0$.

Linear sequences which are ultimately recurrent

The sequence

 $(1, 0, 0, \dots)$

is not a linear recurrence sequence.

The condition

 $u_{n+1} = u_n$

is satisfied only for $n \geq 1$.

The relation

 $u_{n+2} = u_{n+1} + 0u_n$

with d = 2, $a_d = 0$ does not fulfil the requirement $a_d \neq 0$.

・ロト ・ 一部 ト ・ 目 ト ・ 目 ・ つ へ (* 10 / 46

Generating series of a linear recurrence sequence Let $\mathbf{u} = (u_n)_{n>0}$ be a linear recurrence sequence

(*)
$$u_{n+d} = a_1 u_{n+d-1} + \cdots + a_d u_n$$
 for $n \ge 0$

with characteristic polynomial

 $f(X) = X^d - a_1 X^{d-1} - \dots - a_d.$

Denote by f^- the reciprocal polynomial of f:

$$f^{-}(X) = X^{d} f(X^{-1}) = 1 - a_1 X - \dots - a_d X^{d}.$$

Then

$$\sum_{n=0}^{\infty} u_n X^n = \frac{r(X)}{f^-(X)},$$

where r is a polynomial of degree less than d determined by the initial values of **u**.

Generating series of a linear recurrence sequence

Assume

$$u_{n+d} = a_1 u_{n+d-1} + \dots + a_d u_n \quad \text{for} \quad n \ge 0.$$

Then

$$\sum_{n=0}^{\infty} u_n X^n = \frac{r(X)}{f^-(X)}.$$

Proof. Comparing the coefficients of X^n for $n \ge d$ shows that

$$f^{-}(X)\sum_{n=0}^{\infty}u_{n}X^{n}$$

is a polynomial of degree less than d.

<ロト < 合 > < 言 > く 言 > こ > う Q (~ 13/46

15/46

Linear differential equations

Given a sequence $(u_n)_{n\geq 0}$ of numbers, its exponential generating power series is

$$\psi(z) = \sum_{n \ge 0} u_n \frac{z^n}{n!} \cdot$$

For $k \geq 0$, the k-the derivative $\psi^{(k)}$ of ψ satisfies

$$\psi^{(k)}(z) = \sum_{n \ge 0} u_{n+k} \frac{z^n}{n!} \cdot$$

Hence the sequence satisfies the linear recurrence relation

(*) $u_{n+d} = a_1 u_{n+d-1} + \dots + a_d u_n$ for $n \ge 0$

if and only if ψ is a solution of the homogeneous linear differential equation

$$y^{(d)} = a_1 y^{(d-1)} + \dots + a_{d-1} y' + a_d y.$$

Taylor coefficients of rational functions

Conversely, the sequence of coefficients in the Taylor expansion of any rational fraction a(X)/b(X) with deg $a < \deg b$ and $b(0) \neq 0$ satisfies the recurrence relation with characteristic polynomial $f \in K[X]$ given by $f(X) = b^{-}(X)$.

Therefore a sequence $\mathbf{u} = (u_n)_{n \ge 0}$ satisfies the recurrence relation (*) with characteristic polynomial $f \in K[X]$ if and only if

$$\sum_{n=0}^{\infty} u_n X^n = \frac{r(X)}{f^-(X)},$$

where r is a polynomial of degree less than d determined by the initial values of **u**.

<□▶ < □▶ < □▶ < ■▶ < ■▶ < ■▶ < ■ > ○へへ 14/46

Matrix notation for a linear recurrence sequence

The linear recurrence sequence

(*)
$$u_{n+d} = a_1 u_{n+d-1} + \dots + a_d u_n$$
 for $n \ge 0$

can be written

$$\begin{pmatrix} u_{n+1} \\ u_{n+2} \\ \vdots \\ u_{n+d} \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ a_d & a_{d-1} & a_{d-2} & \cdots & a_1 \end{pmatrix} \begin{pmatrix} u_n \\ u_{n+1} \\ \vdots \\ u_{n+d-1} \end{pmatrix}.$$

Matrix notation for a linear recurrence sequence

$$U_{n+1} = AU_n$$

with

 $U_{n} = \begin{pmatrix} u_{n} \\ u_{n+1} \\ \vdots \\ u_{n+d-1} \end{pmatrix}, \quad A = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ a_{d} & a_{d-1} & a_{d-2} & \cdots & a_{1} \end{pmatrix}.$

The determinant of $I_d X - A$ (the characteristic polynomial of A) is nothing but

 $f(X) = X^d - a_1 X^{d-1} - \dots - a_d,$

the characteristic polynomial of the linear recurrence sequence. By induction

Conversely :

Given a linear recurrence sequence $\mathbf{u} \in \mathbb{K}^{\mathbb{N}}$, there exist an integer $d \geq 1$ and a matrix $A \in \mathrm{GL}_d(\mathbb{K})$ such that, for each $n \geq 0$,

 $u_n = a_{11}^{(n)}.$

The characteristic polynomial of A is the characteristic polynomial of the linear recurrence sequence.

EVEREST G., VAN DER POORTEN A., SHPARLINSKI I., WARD T. – *Recurrence sequences,* Mathematical Surveys and Monographs (AMS, 2003), volume 104.

<ロ> < 団> < 団> < 目> < 目> < 目> < 目> のへの 19/46

Powers of matrices

Let $A = (a_{ij})_{1 \le i,j \le d} \in \operatorname{GL}_{d \times d}(\mathbb{K})$ be a $d \times d$ matrix with coefficients in \mathbb{K} and nonzero determinant. For $n \ge 0$, define

$$A^n = \left(a_{ij}^{(n)}\right)_{1 \le i,j \le d}$$

Then each of the d^2 sequences $(a_{ij}^{(n)})_{n\geq 0}$, $(1\leq i,j\leq d)$ is a linear recurrence sequence. The roots of the characteristic polynomial of these linear recurrences are the eigenvalues of A.

In particular the sequence $(\operatorname{Tr}(A^n))_{n\geq 0}$ satisfies the linear recurrence, the characteristic polynomial of which is the characteristic polynomial of the matrix A.

<ロト < 部ト < 言ト < 言ト 言 のへ(~ 18/46

Linear recurrence sequences : simple roots

A basis of $E_{\underline{a}}$ over \mathbb{K} is obtained by attributing to the initial values u_0, \ldots, u_{d-1} the values given by the canonical basis of \mathbb{K}^d .

Given γ in \mathbb{K}^{\times} , a necessary and sufficient condition for a sequence $(\gamma^n)_{n\geq 0}$ to satisfy (*) is that γ is a root of the characteristic polynomial

 $f(X) = X^d - a_1 X^{d-1} - \dots - a_d.$

If this polynomial has d distinct roots $\gamma_1, \ldots, \gamma_d$ in \mathbb{K} ,

 $f(X) = (X - \gamma_1) \cdots (X - \gamma_d), \quad \gamma_i \neq \gamma_j,$

then a basis of $E_{\underline{a}}$ over \mathbb{K} is given by the d sequences $(\gamma_i^{\ n})_{n\geq 0}, \ i=1,\ldots,d.$

Linear recurrence sequences : double roots

The characteristic polynomial of the linear recurrence $u_n = 2\gamma u_{n-1} - \gamma^2 u_{n-2}$ is $X^2 - 2\gamma X + \gamma^2 = (X - \gamma)^2$ with a double root γ .

The sequence $(n\gamma^n)_{n\geq 0}$ satisfies

 $n\gamma^n = 2\gamma(n-1)n\gamma^{n-1} - \gamma^2(n-2)\gamma^{n-2}.$

A basis of $E_{\underline{a}}$ for $a_1 = 2\gamma$, $a_2 = -\gamma^2$ is given by the two sequences $(\gamma^n)_{n\geq 0}$, $(n\gamma^n)_{n\geq 0}$.

Given $\gamma \in \mathbb{K}^{\times}$, a necessary and sufficient condition for the sequence $n\gamma^n$ to satisfy the linear recurrence relation (*) is that γ is a root of multiplicity ≥ 2 of f(X).

Polynomial combinations of powers

The sum and the product of any two linear recurrence sequences are linear recurrence sequences.

The set $\bigcup_{\underline{a}} E_{\underline{a}}$ of all linear recurrence sequences with coefficients in \mathbb{K} is a sub- \mathbb{K} -algebra of $\mathbb{K}^{\mathbb{N}}$.

Given polynomials p_1, \ldots, p_ℓ in $\mathbb{K}[X]$ and elements $\gamma_1, \ldots, \gamma_\ell$ in \mathbb{K}^{\times} , the sequence

 $\left(p_1(n)\gamma_1^n + \dots + p_\ell(n)\gamma_\ell^n\right)_{n>0}$

is a linear recurrence sequence.

Conversely, any linear recurrence sequence is of this form.

In general, when the characteristic polynomial splits as

Linear recurrence sequences : multiple roots

$$X^{d} - a_1 X^{d-1} - \dots - a_d = \prod_{i=1}^{\ell} (X - \gamma_i)^{t_i},$$

a basis of $E_{\underline{a}}$ is given by the d sequences

$$(n^k \gamma_i^n)_{n \ge 0}, \qquad 0 \le k \le t_i - 1, \quad 1 \le i \le \ell.$$

▲□▶ ▲圖▶ ▲ 볼▶ ▲ 볼▶ 볼 ∽) Q (~ 22 / 46

Consequence

• When p is a polynomial of degree < d, the characteristic polynomial of the sequence $u_n = p(n)$ divides $(X - 1)^d$.

Proof. Set

$$A = \begin{pmatrix} 1 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 1 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 1 \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{pmatrix} = I_d + N$$

where I_d is the $d \times d$ identity matrix and N is nilpotent : $N^d = 0$.

Consequence

The characteristic polynomial of A is $(X-1)^d$. Hence for $1 \leq i, j \leq d$, the sequence u_n of the coefficient $a_{ij}^{(n)}$ of A^n satisfies the linear recurrence relation

$$(\star) \qquad \qquad u_{n+d} = a_1 u_{n+d-1} + \dots + a_d u_n,$$

that is

$$u_{n+d} = du_{n+d-1} - \binom{d}{2} u_{n+d-2} + \dots + (-1)^{d-2} du_{n+1} + (-1)^{d-1} u_n$$

The characteristic polynomial of this recurrence relation is $(X-1)^d$.

Sum of polynomial combinations of powers

If \mathbf{u}_1 and \mathbf{u}_2 are two linear recurrence sequences of characteristic polynomials f_1 and f_2 respectively, then $\mathbf{u}_1 + \mathbf{u}_2$ satisfies the linear recurrence, the characteristic polynomial of which is

 $\frac{f_1f_2}{\gcd(f_1,f_2)}$

Characteristic polynomial of the recurrence sequence p(n).

Since, for $1 \leq i, j \leq d$ and $n \geq 0$, we have

 $a_{ij}^{(n)} = \binom{n}{j-i}$

(where we agree that $\binom{n}{k} = 0$ for k < 0 and for k > n, while $\binom{d}{0} = \binom{d}{d} = 1$), we deduce that each of the d polynomials

1,
$$\frac{X(X+1)\cdots(X+k-1)}{k!}$$
 $k = 1, 2, \dots, d-1$

namely

$$1, X, \frac{X(X+1)}{2}, \dots, \frac{X(X+1)\cdots(X+d-2)}{(d-1)!},$$

satisfies the recurrence (*). These d polynomials constitute a basis of the space of polynomials of degree $\leq d_{\odot}$, and d_{\odot} .

Product of polynomial combinations of powers

If the characteristic polynomials of the two linear recurrence sequences \mathbf{u}_1 and \mathbf{u}_2 are respectively

$$f_1(T) = \prod_{j=1}^{\ell} (T - \gamma_j)^{t_j} \quad \text{and} \quad f_2(T) = \prod_{k=1}^{\ell'} (T - \gamma_k')^{t_k'},$$

then $\mathbf{u}_1\mathbf{u}_2$ satisfies the linear recurrence, the characteristic polynomial of which is

$$\prod_{j=1}^{\ell} \prod_{k=1}^{\ell'} (T - \gamma_j \gamma'_k)^{t_j + t'_k - 1}.$$

Linear recurrence sequences and Brahmagupta–Pell–Fermat Equation

Let d be a positive integer, not a square. The solutions $(x,y)\in\mathbb{Z}\times\mathbb{Z}$ of the Brahmagupta–Pell–Fermat Equation

 $x^2 - dy^2 = \pm 1$

form a sequence $(x_n, y_n)_{n \in \mathbb{Z}}$ defined by

$$x_n + \sqrt{dy_n} = (x_1 + \sqrt{dy_1})^n.$$

From

 $2x_n = (x_1 + \sqrt{dy_1})^n + (x_1 - \sqrt{dy_1})^n$

we deduce that $(x_n)_{n\geq 0}$ is a linear recurrence sequence. Same for y_n , and also for $n\leq 0$.

・ロト ・ (ア・・ヨト ・ヨト) ま の へ ()
29 / 46

Discrete version of linear differential equations

A sequence $\mathbf{u} \in \mathbb{K}^{\mathbb{N}}$ can be viewed as a linear map $\mathbb{N} \longrightarrow \mathbb{K}$. Define the discrete derivative \mathcal{D} by

 $\mathcal{D}\mathbf{u}: \mathbb{N} \longrightarrow \mathbb{K} \\ n \longmapsto u_{n+1} - u_n.$

A sequence $\mathbf{u} \in \mathbb{K}^{\mathbb{N}}$ is a linear recurrence sequence if and only if there exists $Q \in \mathbb{K}[T]$ with $Q(1) \neq 1$ such that

$$Q(\mathcal{D})\mathbf{u} = 0.$$

Linear recurrence sequences are a discrete version of linear differential equations with constant coefficients.

The condition $Q(1) \neq 0$ reflects $a_d \neq 0$ – otherwise one gets *ultimately* recurrent sequences.

Doubly infinite linear recurrence sequences

A sequence $(u_n)_{n\in\mathbb{Z}}$ indexed by \mathbb{Z} is a linear recurrence sequence if it satisfies

 $(\star) \qquad \qquad u_{n+d} = a_1 u_{n+d-1} + \dots + a_d u_n.$

for all $n \in \mathbb{Z}$.

Recall $a_d \neq 0$.

Such a sequence is determined by d consecutive values.

<ロト < 回 ト < 目 ト < 三 ト < 三 ト 三 の へ () 30 / 46

Conclusion

The same mathematical object occurs in a different guise :

• Linear recurrence sequences

 $u_{n+d} = a_1 u_{n+d-1} + \dots + a_d u_n.$

• Linear combinations with polynomial coefficients of powers

 $p_1(n)\gamma_1^n + \cdots + p_\ell(n)\gamma_\ell^n.$

- Taylor coefficients of rational functions.
- Coefficients of power series which are solutions of homogeneous linear differential equations.

Reference

EVEREST, GRAHAM; VAN DER POORTEN, ALF; SHPARLINSKI, IGOR; WARD, TOM – *Recurrence sequences*, Mathematical Surveys and Monographs (AMS, 2003), volume 104. 1290 references.





Graham Everest



Alf van der Poorten

```
Igor Shparlinski
```



Linear recurrence sequences over finite fields

Reference: Chapter 8 : Linear recurring sequences of

LIDL, RUDOLF; NIEDERREITER, HARALD.

Finite fields. Paperback reprint of the hardback 2nd edition 1996. (English)

Encyclopedia of Mathematics and Its Applications 20. Cambridge University Press (ISBN 978-0-521-06567-2/pbk). xiv, 755 p. (2008).



```
・ロト < 
同 ト < 
言 ト < 
言 ト ミ ・ 
う へ (や
34 / 46
</p>
```

```
34 / 40
```

Linear recurring sequences

Given a, a_0, \ldots, a_{k-1} in a finite field \mathbb{F}_q , consider a *k*-th order linear recurrence relation : for $n = 0, 1, 2, \ldots$,

 $u_{n+k} = a_{k-1}u_{n+k-1} + a_{k-2}u_{n+k-2} + \dots + a_1u_{n+1} + a_0u_n + a$

Homogeneous : a = 0.

Initial values : $u_0, u_1, \ldots, u_{k-1}$.

State vector : $\mathbf{u}_n = (u_n, u_{n+1}, \dots, u_{n+k-1}).$

Initial state vector : $\mathbf{u}_0 = (u_0, u_1, ..., u_{k-1}).$

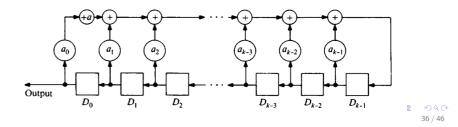
< □ > < ⑦ > < ≧ > < ≧ > < ≧ > ≥ の Q (~ 35 / 46

Feedback shift register

Electronic switching circuit : adder, constant multiplier, constant adder, delay element (*flip-flop*)



$u_{n+k} = a_{k-1}u_{n+k-1} + a_{k-2}u_{n+k-2} + \dots + a_1u_{n+1} + a_0u_n +$



The least period of a linear recurrence sequence

Since \mathbb{F}_q is finite, any linear recurrence sequence $(u_n)_{n\geq 0}$ in \mathbb{F}_q is *ultimately periodic*: there exists r > 0 and $n_0 \geq 0$ such that $u_n = u_{n+r}$ for $n \geq n_0$. The least n_0 for which this relation holds is the *preperiod*.

Any period is a multiple of the least period.

A linear recurrence sequence $(u_n)_{n\geq 0}$ is periodic if there exists a period r > 0 such that $u_n = u_{n+r}$ for $n \geq 0$. In this case this relation holds for the least period; the preperiod is 0. If $a_0 \neq 0$, then the sequence is periodic.

The least period r of a (homogeneous) linear recurrence sequence in \mathbb{F}_q of order k satisfies $r \leq q^k - 1$.

The least period

Assume $a_0 \neq 0$

The least period of the linear recurrence sequence divides the order of the matrix A in the general linear group $\operatorname{GL}_k(\mathbb{F}_q)$.

The *impulse response sequence* is the linear recurrence sequence with the initial state $(0, 0, \ldots, 0, 1)$.

The least period of a linear recurrence sequence divides the least period of the corresponding impulse response sequence.

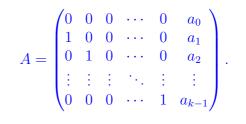
The companion matrix

The linear recurrence sequence

$$u_{n+k} = a_{k-1}u_{n+k-1} + \dots + a_0u_n$$
 for $n \ge 0$

can be written

where



 $\mathbf{u}_n = \mathbf{u}_0 A^n$

▲□▶ ▲圖▶ ▲ 圖▶ ▲ 圖▶ ■ 今 Q (~ 38 / 46

Further examples of linear recurrence sequences

- Fibonacci
- Lucas
- Perrin
- Padovan
- Narayana

References

Linear recurrence sequences : an introduction.

http://www.imj-prg.fr/-michel.waldschmidt/articles/pdf/LinearRecurrenceSequencesIntroduction.pdf Linear recurrence sequences, exponential polynomials and Diophantine approximation.

http://www.imj-prg.fr/~michel.waldschmidt/articles/pdf/LinRecSeqDiophAppxVI.pdf

Leonardo Pisano (Fibonacci)

Fibonacci sequence $(F_n)_{n \ge 0}$, 0, 1, 1, 2, 3, 5, 8, 13, 21,

 $34, 55, 89, 144, 233, \dots$ is defined by

$$F_0 = 0, \ F_1 = 1,$$

Leonardo Pisano (Fibonacci) (1170–1250)

$$F_{n+2} = F_{n+1} + F_n \quad \text{for} \quad n \ge 0.$$

http://oeis.org/A000045

Perrin sequence

http://oeis.org/A001608

The Perrin sequence (also called *skiponacci sequence*) is the linear recurrence sequence $(P_n)_{n\geq 0}$ defined by

$$P_{n+3} = P_{n+1} + P_n \quad \text{for} \quad n \ge 0,$$

with the initial conditions

$$P_0 = 3, P_1 = 0, P_2 = 2$$

It starts with

$$3, 0, 2, 3, 2, 5, 5, 7, 10, 12, 17, 22, 29, 39, 51, 68, \ldots$$

François Olivier Raoul Perrin (1841-1910) :

https://en.wikipedia.org/wiki/Perrin_number

Lucas sequence

http://oeis.org/000032

The Lucas sequence $(L_n)_{n\geq 0}$ satisfies the same recurrence relation as the Fibonacci sequence, namely

$$L_{n+2} = L_{n+1} + L_n \quad \text{for} \quad n \ge 0,$$

only the initial values are different :

 $L_0 = 2, \ L_1 = 1.$

The sequence of Lucas numbers starts with

 $2, 1, 3, 4, 7, 11, 18, 29, 47, 76, 123, 199, 322, \ldots$

A closed form involving the Golden ratio Φ is

 $L_n = \Phi^n + (-\Phi)^{-n},$

from which it follows that for $n \ge 2$, L_n is the nearest integer to Φ^n .

Narayana sequence

https://oeis.org/A000930

Narayana sequence is defined by the recurrence relation

$$C_{n+3} = C_{n+2} + C_n$$

with the initial values $C_0 = 2$, $C_1 = 3$, $C_2 = 4$. It starts with

 $2, 3, 4, 6, 9, 13, 19, 28, 41, 60, 88, 129, 189, 277, \ldots$

Real root of
$$x^3 - x^2 - 1$$

$$\frac{\sqrt[3]{\frac{29+3\sqrt{93}}{2}}+\sqrt[3]{\frac{29-3\sqrt{93}}{2}}+1}{3} = 1.465571231876768\dots$$

▲□▶ ▲圖▶ ▲ 圖▶ ▲ 圖▶ ▲ 圖 → 의 Q (%) 44 / 46

43 / 46

Padovan sequence

https://oeis.org/A000931

The Padovan sequence $(p_n)_{n\geq 0}$ satisfies the same recurrence

 $p_{n+3} = p_{n+1} + p_n$

as the Perrin sequence but has different initial values :

$$p_0 = 1, \quad p_1 = p_2 = 0.$$

It starts with

$$1, 0, 0, 1, 0, 1, 1, 1, 2, 2, 3, 4, 5, 7, 9, 12, 16, \ldots$$

Richard Padovan

http://mathworld.wolfram.com/LinearRecurrenceEquation.html

◆□ ▶ ◆ □ ▶ ◆ ■ ▶ ◆ ■ ▶ ◆ ■ ◆ ○ へ ○ 45 / 46

Linear recurrence sequences,

Michel Waldschmidt

Sorbonne University, Paris Institut de Mathématiques de Jussieu http://www.imj-prg.fr/~michel.waldschmidt/

・< 回 ・ < 言 ・ < 言 ・ 言 ・ う Q (~
 46 / 46