The (inescapable) p-adics

Alex J. Best

5/5/2018

BU Math Retreat 2018

Linear recurrence sequences

Definition (Linear recurrence sequence)
A **linear recurrence sequence**, is a sequences whose nth term is the linear combination of the previous k terms (for all $n \geq k$)

Definition (Linear recurrence sequence)

A **linear recurrence sequence**, is a sequences whose nth term is the linear combination of the previous k terms (for all $n \geq k$)

Example (Fibonacci)

$a_0 = 0, a_1 = 1$ and $a_n = a_{n-1} + a_{n-2}$ for $n \geq k = 2$:

$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610, 987, 1597, 2584, 4181,$

Definition (Linear recurrence sequence)

A **linear recurrence sequence**, is a sequences whose *n*th term is the linear combination of the previous k terms (for all $n \geq k$)

Example (Fibonacci)

$a_0 = 0, a_1 = 1$ and $a_n = a_{n-1} + a_{n-2}$ for $n \geq k = 2$:

$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610, 987, 1597, 2584, 4181,$

a_n grows exponentially.

Definition (Linear recurrence sequence)

A **linear recurrence sequence**, is a sequences whose nth term is the linear combination of the previous k terms (for all $n \geq k$)

Example (A periodic sequence)

$a_0 = 1, a_1 = 0$ with $a_n = -a_{n-1} - a_{n-2}$

$1, 0, -1, 1, 0, -1, 1, 0, -1, 1, 0, -1, 1, 0, -1, 1, 0, -1, 1, 0, -1, 1, 0, -1, 1, 0,$

Linear recurrence sequences

Definition (Linear recurrence sequence)

A **linear recurrence sequence**, is a sequences whose nth term is the linear combination of the previous k terms (for all $n \geq k$)

Example (A periodic sequence)

$a_0 = 1, a_1 = 0$ with $a_n = -a_{n-1} - a_{n-2}$

$1, 0, -1, 1, 0, -1, 1, 0, -1, 1, 0, -1, 1, 0, -1, 1, 0, -1, 1, 0, -1, 1, 0, -1, 1, 0,$

a_n is periodic now.

Definition (Linear recurrence sequence)

A **linear recurrence sequence**, is a sequences whose nth term is the linear combination of the previous k terms (for all $n \geq k$)

Example (Natural numbers interlaced with zeroes)

$a_0 = 1, a_1 = 0, a_2 = 2, a_3 = 0$ with $a_n = 2a_{n-2} - a_{n-4}$

$1, 0, 2, 0, 3, 0, 4, 0, 5, 0, 6, 0, 7, 0, 8, 0, 9, 0, 10, 0, 11, 0, 12, 0, 13, 0, 14, 0, 15, 0$

Definition (Linear recurrence sequence)

A **linear recurrence sequence**, is a sequences whose nth term is the linear combination of the previous k terms (for all $n \geq k$)

Example (Natural numbers interlaced with zeroes)

$a_0 = 1, a_1 = 0, a_2 = 2, a_3 = 0$ with $a_n = 2a_{n-2} - a_{n-4}$

$1, 0, 2, 0, 3, 0, 4, 0, 5, 0, 6, 0, 7, 0, 8, 0, 9, 0, 10, 0, 11, 0, 12, 0, 13, 0, 14, 0, 15, 0$

not periodic but the zeroes *do* have a regular repeating pattern.

The ultimate question

Question

What possible patterns are there for the zeroes of a linear recurrence sequence?

The ultimate question

Question

What possible patterns are there for the zeroes of a linear recurrence sequence?

Observation

A linear recurrence sequence is the Taylor expansion around 0 of a rational function

$$\frac{a_1 + a_2 x + \cdots + a_\ell x^\ell}{b_1 + b_2 x \cdots + b_k x^k}$$

with $b_1 \neq 0$ (so that the expansion makes sense).

Linear recurrence sequences

Example

$$\frac{x}{1-x-x^2}. \leftrightarrow \text{Fibonacci}$$

Example

$$\frac{x}{1-x-x^2}. \leftrightarrow \text{Fibonacci}$$

$$\frac{1}{1+x+x^2}. \leftrightarrow 1, 0, -1, 1, 0, -1, 1, 0, -1, 1, 0, -1, 1, 0, -1, 1, 0, -1, 1, 0, -$$

Example

$$\frac{x}{1-x-x^2}. \leftrightarrow \text{Fibonacci}$$

$$\frac{1}{1+x+x^2}. \leftrightarrow 1, 0, -1, 1, 0, -1, 1, 0, -1, 1, 0, -1, 1, 0, -1, 1, 0, -1, 1, 0, -$$

$$\frac{1}{(1-x^2)^2}. \leftrightarrow 1, 0, 2, 0, 3, 0, 4, 0, 5, 0, 6, 0, 7, 0, 8, 0, 9, 0, 10, 0, 11, 0, 12, 0, 1$$

Example

$$\frac{x}{1-x-x^2}. \leftrightarrow \text{Fibonacci}$$

$$\frac{1}{1+x+x^2}. \leftrightarrow 1, 0, -1, 1, 0, -1, 1, 0, -1, 1, 0, -1, 1, 0, -1, 1, 0, -1, 1, 0, -$$

$$\frac{1}{(1-x^2)^2}. \leftrightarrow 1, 0, 2, 0, 3, 0, 4, 0, 5, 0, 6, 0, 7, 0, 8, 0, 9, 0, 10, 0, 11, 0, 12, 0, 1$$

$$\begin{aligned}\frac{(1+x)^3-x^3}{(1+x)^5-x^5} \leftrightarrow & 1, -2, 3, -5, 10, -20, 35, -50, 50, 0, -175, 625, \\ & -1625, 3625, -7250, 13125, -21250, 29375, -29375, \\ & 0, 106250, -384375, 1006250, -2250000, 4500000, \\ & -8140625, 13171875, -18203125, 18203125, 0, -65859\end{aligned}$$

Consequences

Observation

The set of all linear recurrence sequences is a vector space! Hard to tell how the rule changes.

Consequences

Observation

The set of all linear recurrence sequences is a vector space! Hard to tell how the rule changes.

We can always mess up a finite amount of behaviour. So assume a_n has infinitely many zeroes, what is the structure of the zero set?

Example

$$\frac{1}{(1-x^2)^2} - (1 - x + 2x^2 + 3x^4 + 4x^6) \leftrightarrow 0, 1, 0, 0, 0, 0, 0, 0, 5, 0, 6, 0, 7, 0, 8, 0,$$

Example

$$\frac{1}{(1-x^2)^2} - (1 - x + 2x^2 + 3x^4 + 4x^6) \leftrightarrow 0, 1, 0, 0, 0, 0, 0, 0, 5, 0, 6, 0, 7, 0, 8, 0,$$

Interlacing with 0 and *shifting* correspond to plugging in x^2 and multiplying by x respectively in the rational functions

Example

$$\frac{1}{(1-x^2)^2} - (1 - x + 2x^2 + 3x^4 + 4x^6) \leftrightarrow 0, 1, 0, 0, 0, 0, 0, 0, 5, 0, 6, 0, 7, 0, 8, 0,$$

Interlacing with 0 and *shifting* correspond to plugging in x^2 and multiplying by x respectively in the rational functions

$$\frac{1}{(1-x)^2} \leftrightarrow 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21,$$

Example

$$\frac{1}{(1-x^2)^2}-(1-x+2x^2+3x^4+4x^6) \leftrightarrow 0,1,0,0,0,0,0,0,5,0,6,0,7,0,8,0,$$

Interlacing with 0 and *shifting* correspond to plugging in x^2 and multiplying by x respectively in the rational functions

$$\frac{1}{(1-x)^2} \leftrightarrow 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,$$

$$\frac{1}{(1-x^2)^2} \leftrightarrow 1,0,2,0,3,0,4,0,5,0,6,0,7,0,8,0,9,0,10,0,11,0,12,0,13$$

Linear recurrence sequences

$$\frac{1}{(1-x)^2} \leftrightarrow 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21,$$

$$\frac{1}{(1-x^2)^2} \leftrightarrow 1, 0, 2, 0, 3, 0, 4, 0, 5, 0, 6, 0, 7, 0, 8, 0, 9, 0, 10, 0, 11, 0, 12, 0, 13$$

$$\frac{1}{(1-x^4)^2} \leftrightarrow 1, 0, 0, 0, 2, 0, 0, 0, 3, 0, 0, 0, 4, 0, 0, 0, 5, 0, 0, 0, 6, 0, 0, 0, 7, 0, 0$$

Linear recurrence sequences

$$\frac{1}{(1-x)^2} \leftrightarrow 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21,$$

$$\frac{1}{(1-x^2)^2} \leftrightarrow 1, 0, 2, 0, 3, 0, 4, 0, 5, 0, 6, 0, 7, 0, 8, 0, 9, 0, 10, 0, 11, 0, 12, 0, 13$$

$$\frac{1}{(1-x^4)^2} \leftrightarrow 1, 0, 0, 0, 2, 0, 0, 0, 3, 0, 0, 0, 4, 0, 0, 0, 5, 0, 0, 0, 6, 0, 0, 0, 7, 0, 0$$

$$\frac{x}{(1-x^4)^2} \leftrightarrow 0, 1, 0, 0, 0, 2, 0, 0, 0, 3, 0, 0, 0, 4, 0, 0, 0, 5, 0, 0, 0, 6, 0, 0, 0, 7, 0$$

Linear recurrence sequences

$$\frac{1}{(1-x)^2} \leftrightarrow 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21,$$

$$\frac{1}{(1-x^2)^2} \leftrightarrow 1, 0, 2, 0, 3, 0, 4, 0, 5, 0, 6, 0, 7, 0, 8, 0, 9, 0, 10, 0, 11, 0, 12, 0, 13$$

$$\frac{1}{(1-x^4)^2} \leftrightarrow 1, 0, 0, 0, 2, 0, 0, 0, 3, 0, 0, 0, 4, 0, 0, 0, 5, 0, 0, 0, 6, 0, 0, 0, 7, 0, 0$$

$$\frac{x}{(1-x^4)^2} \leftrightarrow 0, 1, 0, 0, 0, 2, 0, 0, 0, 3, 0, 0, 0, 4, 0, 0, 0, 5, 0, 0, 0, 6, 0, 0, 0, 7, 0$$

$$\frac{1+2x}{(1-x^4)^2} \leftrightarrow 1, 2, 0, 0, 2, 4, 0, 0, 3, 6, 0, 0, 4, 8, 0, 0, 5, 10, 0, 0, 6, 12, 0, 0, 7, 1$$

Linear recurrence sequences

$$\frac{1}{(1-x)^2} \leftrightarrow 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21,$$

$$\frac{1}{(1-x^2)^2} \leftrightarrow 1, 0, 2, 0, 3, 0, 4, 0, 5, 0, 6, 0, 7, 0, 8, 0, 9, 0, 10, 0, 11, 0, 12, 0, 13$$

$$\frac{1}{(1-x^4)^2} \leftrightarrow 1, 0, 0, 0, 2, 0, 0, 0, 3, 0, 0, 0, 4, 0, 0, 0, 5, 0, 0, 0, 6, 0, 0, 0, 7, 0, 0$$

$$\frac{x}{(1-x^4)^2} \leftrightarrow 0, 1, 0, 0, 0, 2, 0, 0, 0, 3, 0, 0, 0, 4, 0, 0, 0, 5, 0, 0, 0, 6, 0, 0, 0, 7, 0$$

$$\frac{1+2x}{(1-x^4)^2} \leftrightarrow 1, 2, 0, 0, 2, 4, 0, 0, 3, 6, 0, 0, 4, 8, 0, 0, 5, 10, 0, 0, 6, 12, 0, 0, 7, 1$$

Still has periodic zero set, all n congruent to $2, 3$ modulo 4.

Approach

Expand into partial fractions

$$\frac{p(x)}{q(x)} = \sum_{i=1}^{m} \sum_{j=1}^{n_j} \frac{r_{ij}}{(1-\alpha_i x)^j}$$

Approach

Expand into partial fractions

$$\frac{p(x)}{q(x)} = \sum_{i=1}^{m} \sum_{j=1}^{n_j} \frac{r_{ij}}{(1 - \alpha_i x)^j}$$

do some math:

$$\sum_{n=0}^{\infty} \left(\sum_{i=1}^{m} \sum_{j=1}^{n_j} r_{ij} \binom{n+j-1}{j-1} \alpha_i^n \right) x^n$$

Approach

Expand into partial fractions

$$\frac{p(x)}{q(x)} = \sum_{i=1}^{m} \sum_{j=1}^{n_j} \frac{r_{ij}}{(1 - \alpha_i x)^j}$$

do some math:

$$\sum_{n=0}^{\infty} \left(\sum_{i=1}^{m} \sum_{j=1}^{n_j} r_{ij} \binom{n+j-1}{j-1} \alpha_i^n \right) x^n$$

Upshot: there are polynomials $A_i(n)$ such that

$$a_n = \sum_{i=1}^{m} A_i(n) \alpha_i^n.$$

Like that formula for Fibonacci with the golden ratio in.

Approach

So a_n is an analytic function of n which has zeroes for infinitely many integer values.

Approach

So a_n is an analytic function of n which has zeroes for infinitely many integer values.

Like

$$\sin(\pi x)!$$

Approach

So a_n is an analytic function of n which has zeroes for infinitely many integer values.

Like

$$\sin(\pi x)!$$

Ridiculous suggestion

What if the integers were bounded? In that case infinitely many zeroes $\implies$ the function is zero!

Theorem (Ostrowski)

The only absolute values on $\mathbf{Q}$ *are*

$$\textit{the usual one} \;\&\; |\cdot|_p$$

defined by $|p|_p = \frac{1}{p}$ *and* $|q|_p = 1$ *for all other primes* $q \neq p$.

Theorem (Ostrowski)

The only absolute values on $\mathbf{Q}$ *are*

$$\text{the usual one } \& \ |\cdot|_p$$

defined by $|p|_p = \frac{1}{p}$ *and* $|q|_p = 1$ *for all other primes* $q \neq p$.

With $|\cdot|_p$ the integers are bounded!

Theorem (Ostrowski)

The only absolute values on $\mathbf{Q}$ *are*

$$\text{the usual one } \& \ |\cdot|_p$$

defined by $|p|_p = \frac{1}{p}$ *and* $|q|_p = 1$ *for all other primes* $q \neq p$*.*

With $|\cdot|_p$ the integers are bounded! Are the functions

$$\sum_{i=1}^{m} A_i(n)\alpha_i^n$$

p-adic analytic functions of n?

Theorem (Ostrowski)

The only absolute values on $\mathbf{Q}$ *are*

$$\text{the usual one } \& \ |\cdot|_p$$

defined by $|p|_p = \frac{1}{p}$ *and* $|q|_p = 1$ *for all other primes* $q \neq p$*.*

With $|\cdot|_p$ the integers are bounded! Are the functions

$$\sum_{i=1}^{m} A_i(n)\alpha_i^n$$

p-adic analytic functions of n?

Problem

The p-adic exponential function has finite radius of convergence.

Theorem (Ostrowski)

The only absolute values on $\mathbf{Q}$ *are*

$$\textit{the usual one } \& \ |\cdot|_p$$

defined by $|p|_p = \frac{1}{p}$ *and* $|q|_p = 1$ *for all other primes* $q \neq p$.

With $|\cdot|_p$ the integers are bounded! Are the functions

$$\sum_{i=1}^{m} A_i(n)\alpha_i^n$$

p-adic analytic functions of n?

Problem

The p-adic exponential function has finite radius of convergence.

The fix

Choose p so that $|\alpha_i|_p = 1$ for all i, then $\alpha_i^{p-1} = 1 + \lambda_i$ with $|\lambda_i|_p \leq \frac{1}{p}$. Now $(\alpha_i^{p-1})^n$ is analytic!

Write n as $r + (p-1)n'$ with $0 \leq r < p-1$

Write n as $r + (p-1)n'$ with $0 \leq r < p-1$, then

$$a_n = \sum_{i=1}^{m} A_i(n)\alpha_i^n = \sum_{i=1}^{m} A_i(r+(p-1)n')\alpha_i^{r+(p-1)n'}$$

$$= \sum_{i=1}^{m} A_i(r+(p-1)n')\alpha_i^r(\alpha_i^{(p-1)})^{n'}$$

for each fixed r this function of n' is analytic.

Write n as $r + (p-1)n'$ with $0 \leq r < p-1$, then

$$a_n = \sum_{i=1}^{m} A_i(n)\alpha_i^n = \sum_{i=1}^{m} A_i(r + (p-1)n')\alpha_i^{r+(p-1)n'}$$

$$= \sum_{i=1}^{m} A_i(r + (p-1)n')\alpha_i^r(\alpha_i^{(p-1)})^{n'}$$

for each fixed r this function of n' is analytic. Infinitely many zeroes for integer n means $\exists r$ with infinitely many zeroes of the form $r + (p-1)n'$. So the function

$$\sum_{i=1}^{m} A_i(r + (p-1)n')\alpha_i^r(\alpha_i^{(p-1)})^{n'}$$

is identically zero, and all these $a_n = 0$ when $n \equiv r \pmod{p-1}$.

Finale

Theorem (Skolem $\rightsquigarrow$ Mahler $\rightsquigarrow$ Lech)

All except finitely many indicies of the zeroes of a linear recurrence lie in a a finite union of arithmetic progressions, i.e. they are all of the form $nM + b$ for some $b \in B \subset \{0, \ldots, M-1\}$, $n \in \mathbf{N}$.

Finale

Theorem (Skolem $\rightsquigarrow$ Mahler $\rightsquigarrow$ Lech)

All except finitely many indicies of the zeroes of a linear recurrence lie in a a finite union of arithmetic progressions, i.e. they are all of the form $nM + b$ for some $b \in B \subset \{0, \dots, M-1\}$, $n \in \mathbf{N}$.