On polynomial recursive sequences

Michaël Cadilhac¹, <u>Filip Mazowiecki</u>², Charles Paperman³, Michał Pilipczuk⁴ and Géraud Sénizergues⁵

¹DePaul University, USA

²Max Planck Institute for Software Systems, Germany

³Université de Lille, France

⁴University of Warsaw, Poland

⁵Université de Bordeaux, France

Outline

1. Introduction (mostly linear recursive sequences)

2. Polynomial recursive sequences

3. Proof that n^n is not polynomially recursive

4. Applications in weighted automata

• Fibonacci sequence F_n

• Fibonacci sequence *F_n*

• Catalan numbers C_n

• Fibonacci sequence *F_n*

• Catalan numbers C_n

 C_n = number of expressions with n pairs of correctly matched parentheses

• Fibonacci sequence *F_n*

• Catalan numbers C_n

 C_n = number of expressions with n pairs of correctly matched parentheses

$$u_{n+k}=a_ku_{n+k-1}+a_{k-1}u_{n+k-1}+\ldots+a_1u_n$$
 fixing $a_1,\ldots,a_k\in\mathbb{Q}$ and $u_0,\ldots,u_{k-1}\in\mathbb{Q}$

$$u_{n+k} = a_k u_{n+k-1} + a_{k-1} u_{n+k-1} + \ldots + a_1 u_n$$

fixing $a_1, \ldots, a_k \in \mathbb{Q}$ and $u_0, \ldots, u_{k-1} \in \mathbb{Q}$

• Example: **Fibonacci sequence** F_n

$$k = 2$$
, $a_1 = a_2 = 1$, $F_0 = 0$, $F_1 = 1$

$$u_{n+k}=a_ku_{n+k-1}+a_{k-1}u_{n+k-1}+\ldots+a_1u_n$$
 fixing $a_1,\ldots,a_k\in\mathbb{Q}$ and $u_0,\ldots,u_{k-1}\in\mathbb{Q}$

• Example: **Fibonacci sequence** F_n

$$k = 2$$
, $a_1 = a_2 = 1$, $F_0 = 0$, $F_1 = 1$

• Non-example: Catalan numbers C_n

$$u_{n+k}=a_ku_{n+k-1}+a_{k-1}u_{n+k-1}+\ldots+a_1u_n$$
 fixing $a_1,\ldots,a_k\in\mathbb{Q}$ and $u_0,\ldots,u_{k-1}\in\mathbb{Q}$

• Example: **Fibonacci sequence** F_n

$$k = 2$$
, $a_1 = a_2 = 1$, $F_0 = 0$, $F_1 = 1$

• Non-example: Catalan numbers C_n

Definition

$$u_n$$
 is linear recursive if there is $L(x_1, x_2, \dots, x_k) = a_1x_1 + \dots a_kx_k$
s.t. $u_{n+k} = L(u_n, \dots, u_{n+k-1})$ for all n

$$u_{n+k}=a_ku_{n+k-1}+a_{k-1}u_{n+k-1}+\ldots+a_1u_n$$
 fixing $a_1,\ldots,a_k\in\mathbb{Q}$ and $u_0,\ldots,u_{k-1}\in\mathbb{Q}$

• Example: **Fibonacci sequence** F_n

$$k = 2$$
, $a_1 = a_2 = 1$, $F_0 = 0$, $F_1 = 1$

• Non-example: Catalan numbers C_n

Definition

$$u_n$$
 is linear recursive if there is $L(x_1, x_2, \dots, x_k) = a_1x_1 + \dots a_kx_k$
s.t. $u_{n+k} = L(u_n, \dots, u_{n+k-1})$ for all n

Fibonacci:
$$L(x_1, x_2) = x_1 + x_2$$

$$u_{n+k}=a_ku_{n+k-1}+a_{k-1}u_{n+k-1}+\ldots+a_1u_n$$
 fixing $a_1,\ldots,a_k\in\mathbb{Q}$ and $u_0,\ldots,u_{k-1}\in\mathbb{Q}$

• Example: **Fibonacci sequence** F_n

$$k = 2$$
, $a_1 = a_2 = 1$, $F_0 = 0$, $F_1 = 1$

• Non-example: Catalan numbers C_n

Definition

$$u_n$$
 is linear recursive if there is $L(x_1, x_2, \dots, x_k) = a_1x_1 + \dots a_kx_k$
s.t. $u_{n+k} = L(u_n, \dots, u_{n+k-1})$ for all n

Fibonacci:
$$L(x_1, x_2) = x_1 + x_2$$

We will see that Catalan numbers C_n are not linear recursive

Can we restrict to recursion depth 1?

Can we restrict to recursion depth 1?

No: $u_{n+1} = c \cdot u_n$ are geometric sequences

Can we restrict to recursion depth 1?

No: $u_{n+1} = c \cdot u_n$ are geometric sequences

Idea: system of linear sequences

Can we restrict to recursion depth 1?

No: $u_{n+1} = c \cdot u_n$ are geometric sequences

Idea: system of linear sequences

Example: Fibonacci F_n with an extra sequence G_n ($= F_{n+1}$)

$$egin{cases} F_0=0 \ G_0=1 \end{cases} egin{cases} F_{n+1}=G_n \ G_{n+1}=F_n+G_n \end{cases}$$

Can we restrict to recursion depth 1?

No: $u_{n+1} = c \cdot u_n$ are geometric sequences

Idea: system of linear sequences

Example: Fibonacci
$$F_n$$
 with an extra sequence G_n ($= F_{n+1}$)

$$egin{cases} F_0 = 0 \ G_0 = 1 \end{cases} egin{cases} F_{n+1} = G_n \ G_{n+1} = F_n + G_n \end{cases}$$

$$u_{n} = u_{n}^{1}.$$

$$\begin{cases} u_{0}^{1} = c_{1} \\ u_{0}^{2} = c_{2} \end{cases} \qquad \begin{cases} u_{n+1}^{1} = L_{1}(u_{n}^{1}, u_{n}^{2}, \dots, u_{n}^{k}) \\ u_{n+1}^{2} = L_{2}(u_{n}^{1}, u_{n}^{2}, \dots, u_{n}^{k}) \\ \vdots \\ u_{0}^{k} = c_{k} \end{cases}$$

$$\vdots$$

$$u_{n+1}^{k} = L_{k}(u_{n}^{1}, u_{n}^{2}, \dots, u_{n}^{k})$$

Can we restrict to recursion depth 1?

No: $u_{n+1} = c \cdot u_n$ are geometric sequences

Idea: system of linear sequences

Example: Fibonacci
$$F_n$$
 with an extra sequence G_n ($= F_{n+1}$)

$$egin{cases} F_0 = 0 \ G_0 = 1 \end{cases} egin{cases} F_{n+1} = G_n \ G_{n+1} = F_n + G_n \end{cases}$$

$$u_{n} = u_{n}^{1}.$$

$$\begin{cases} u_{0}^{1} = c_{1} \\ u_{0}^{2} = c_{2} \end{cases}$$

$$\vdots$$

$$u_{n}^{k} = c_{k}$$

$$\begin{cases} u_{n+1}^{1} = L_{1}(u_{n}^{1}, u_{n}^{2}, \dots, u_{n}^{k}) \\ u_{n+1}^{2} = L_{2}(u_{n}^{1}, u_{n}^{2}, \dots, u_{n}^{k}) \\ \vdots \\ u_{n+1}^{k} = L_{k}(u_{n}^{1}, u_{n}^{2}, \dots, u_{n}^{k}) \end{cases}$$

$$\vec{u}_{n} = (u_{n}^{1}, \dots, u_{n}^{k})$$

$$I = (c_{1}, \dots, c_{k})$$

$$M[i, \bullet] = L_{i}$$

Equivalence of the definitions

Theorem (Folklore)

 a_n is linear recursive iff a_n is definable as a linear system

Equivalence of the definitions

Theorem (Folklore)

 a_n is linear recursive iff a_n is definable as a linear system

Proof (\Rightarrow)

For depth k use k-1 auxiliary shifts.

$$a_{n+4} = 3a_{n+3} - 2a_{n+2} + 4a_{n+1} - a_n$$

$$a_{n+4}=3a_{n+3}-2a_{n+2}+4a_{n+1}-a_n \qquad \leadsto egin{array}{c} a_{n+1}=b_n \ b_{n+1}=c_n \ c_{n+1}=d_n \ d_{n+1}=3a_n-2b_n+4c_n-d_n \end{array}$$

Equivalence of the definitions

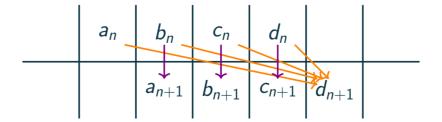
Theorem (Folklore)

 a_n is linear recursive iff a_n is definable as a linear system

Proof (\Rightarrow)

For depth k use k-1 auxiliary shifts.

or depth
$$k$$
 use $k-1$ auxiliary shifts.
$$a_{n+4}=3a_{n+3}-2a_{n+2}+4a_{n+1}-a_n \qquad \rightsquigarrow \qquad \begin{cases} a_{n+1}=b_n\\b_{n+1}=c_n\\c_{n+1}=d_n\\d_{n+1}=3a_n-2b_n+4c_n-d_n \end{cases}$$



Theorem (Folklore)

 a_n is linear recursive iff a_n is definable as a linear system

Proof (←) constructive

Theorem (Folklore)

 a_n is linear recursive iff a_n is definable as a linear system

Proof (*⇐*) constructive

Example

Consider
$$a_n = n^2$$
, recall $(n + 1)^2 = n^2 + 2n + 1$

Theorem (Folklore)

 a_n is linear recursive iff a_n is definable as a linear system

Proof (←) constructive

Example

Consider
$$a_n = n^2$$
, recall $(n + 1)^2 = n^2 + 2n + 1$

$$\begin{cases} a_0 = 0 \\ b_0 = 0 \\ c_0 = 1 \end{cases} \begin{cases} a_{n+1} = a_n + 2b_n + c_n \\ b_{n+1} = b_n + c_n \\ c_{n+1} = c_n \end{cases}$$

Theorem (Folklore)

 a_n is linear recursive iff a_n is definable as a linear system

Proof (←) constructive

Example

Consider
$$a_n = n^2$$
, recall $(n + 1)^2 = n^2 + 2n + 1$

$$\begin{cases} a_0 = 0 \\ b_0 = 0 \\ c_0 = 1 \end{cases} \begin{cases} a_{n+1} = a_n + 2b_n + c_n \\ b_{n+1} = b_n + c_n \\ c_{n+1} = c_n \end{cases}$$

$$M = \begin{pmatrix} 1 & 2 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \qquad det(M - \lambda I) = -\lambda^3 + 3\lambda^2 - 3\lambda + 1$$

Theorem (Folklore)

 a_n is linear recursive iff a_n is definable as a linear system

Proof (←) constructive

Example

Consider
$$a_n = n^2$$
, recall $(n + 1)^2 = n^2 + 2n + 1$

$$\begin{cases} a_0 = 0 \\ b_0 = 0 \\ c_0 = 1 \end{cases} \begin{cases} a_{n+1} = a_n + 2b_n + c_n \\ b_{n+1} = b_n + c_n \\ c_{n+1} = c_n \end{cases}$$

$$M = \begin{pmatrix} 1 & 2 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \qquad det(M - \lambda I) = -\lambda^3 + 3\lambda^2 - 3\lambda + 1$$

Then $a_{n+3} = 3a_{n+2} - 3a_{n+1} + a_n$ (by the Cayley–Hamilton theorem)

Theorem (Folklore)

 a_n is linear recursive iff a_n is definable as a linear system

Theorem (Folklore)

 a_n is linear recursive iff a_n is definable as a linear system

Theorem (Folklore)

 a_n is linear recursive iff a_n is definable as a linear system

$$\begin{aligned}
u_{n} &= u_{n}^{1} \\
u_{0}^{1} &= c_{1} \\
u_{0}^{2} &= c_{2} \\
\vdots \\
u_{0}^{k} &= c_{k}
\end{aligned}
\begin{cases}
u_{n+1}^{1} &= L_{1}(u_{n}^{1}, u_{n}^{2}, \dots, u_{n}^{k}) \\
u_{n+1}^{2} &= L_{2}(u_{n}^{1}, u_{n}^{2}, \dots, u_{n}^{k}) \\
\vdots \\
u_{n+1}^{k} &= L_{k}(u_{n}^{1}, u_{n}^{2}, \dots, u_{n}^{k})
\end{aligned}$$

$$\Rightarrow M \in \mathbb{Q}^{k \times k} \quad \vec{u}_{n}^{T} = M^{n} \cdot \vec{u}_{0}^{T} \\
\vdots \\
u_{n+1}^{k} &= L_{k}(u_{n}^{1}, u_{n}^{2}, \dots, u_{n}^{k})$$

$$\vec{u}_{n} &= (u_{n}^{1}, \dots, u_{n}^{k})$$

Let
$$R : \mathbb{Q}^k \to \mathbb{Q}^{k+1}$$
, $R(\vec{x}) = (e^{\mathsf{T}} M^0 \vec{x}, e^{\mathsf{T}} M^1 \vec{x}, \dots, e^{\mathsf{T}} M^k \vec{x})$
 $e^{\mathsf{T}} = (1, 0, 0, \dots, 0) \in \mathbb{Q}^k$, $R(\vec{u_n}) = (u_n^1, u_{n+1}^1, \dots, u_{n+k}^1)$

Theorem (Folklore)

 a_n is linear recursive iff a_n is definable as a linear system

$$\begin{aligned}
u_{n} &= u_{n}^{1} \\
u_{0}^{1} &= c_{1} \\
u_{0}^{2} &= c_{2} \\
\vdots \\
u_{0}^{k} &= c_{k}
\end{aligned}
\begin{cases}
u_{n+1}^{1} &= L_{1}(u_{n}^{1}, u_{n}^{2}, \dots, u_{n}^{k}) \\
u_{n+1}^{2} &= L_{2}(u_{n}^{1}, u_{n}^{2}, \dots, u_{n}^{k}) \\
\vdots \\
u_{n+1}^{k} &= L_{k}(u_{n}^{1}, u_{n}^{2}, \dots, u_{n}^{k})
\end{aligned}$$

$$\Rightarrow M \in \mathbb{Q}^{k \times k} \quad \vec{u}_{n}^{T} = M^{n} \cdot \vec{u}_{0}^{T} \\
\vdots \\
u_{n+1}^{k} &= L_{k}(u_{n}^{1}, u_{n}^{2}, \dots, u_{n}^{k})$$

$$\vec{u}_{n} &= (u_{n}^{1}, \dots, u_{n}^{k})$$

Let
$$R: \mathbb{Q}^k \to \mathbb{Q}^{k+1}$$
, $R(\vec{x}) = (e^{\mathsf{T}} M^0 \vec{x}, e^{\mathsf{T}} M^1 \vec{x}, \dots, e^{\mathsf{T}} M^k \vec{x})$
 $e^{\mathsf{T}} = (1, 0, 0, \dots, 0) \in \mathbb{Q}^k$, $R(\vec{u_n}) = (u_n^1, u_{n+1}^1, \dots, u_{n+k}^1)$
 \implies nonzero linear $K: \mathbb{Q}^{k+1} \to \mathbb{Q}$ s.t. $\operatorname{im}(R) \subseteq \ker(K)$

Theorem (Folklore)

 a_n is linear recursive iff a_n is definable as a linear system

Let
$$R: \mathbb{Q}^k \to \mathbb{Q}^{k+1}$$
, $R(\vec{x}) = (e^{\mathsf{T}} M^0 \vec{x}, e^{\mathsf{T}} M^1 \vec{x}, \dots, e^{\mathsf{T}} M^k \vec{x})$
 $e^{\mathsf{T}} = (1, 0, 0, \dots, 0) \in \mathbb{Q}^k$, $R(\vec{u_n}) = (u_n^1, u_{n+1}^1, \dots, u_{n+k}^1)$
 \implies nonzero linear $K: \mathbb{Q}^{k+1} \to \mathbb{Q}$ s.t. $\operatorname{im}(R) \subseteq \ker(K)$ i.e. $K(R(\vec{x})) = 0$

Theorem (Folklore)

 a_n is linear recursive iff a_n is definable as a linear system

$$\begin{aligned}
u_{n} &= u_{n}^{1} \\
u_{0}^{1} &= c_{1} \\
u_{0}^{2} &= c_{2} \\
\vdots \\
u_{0}^{k} &= c_{k}
\end{aligned}
\begin{cases}
u_{n+1}^{1} &= L_{1}(u_{n}^{1}, u_{n}^{2}, \dots, u_{n}^{k}) \\
u_{n}^{2}, \dots, u_{n}^{k}, \dots, u_$$

Let
$$R: \mathbb{Q}^k \to \mathbb{Q}^{k+1}$$
, $R(\vec{x}) = (e^T M^0 \vec{x}, e^T M^1 \vec{x}, \dots, e^T M^k \vec{x})$
 $e^T = (1, 0, 0, \dots, 0) \in \mathbb{Q}^k$, $R(\vec{u_n}) = (u_n^1, u_{n+1}^1, \dots, u_{n+k}^1)$
 \Longrightarrow nonzero linear $K: \mathbb{Q}^{k+1} \to \mathbb{Q}$ s.t. $\operatorname{im}(R) \subseteq \ker(K)$ i.e. $K(R(\vec{x})) = 0$

$$K(x_0,\ldots,x_k)=a_0x_0+\ldots a_kx_k$$

Theorem (Folklore)

 a_n is linear recursive iff a_n is definable as a linear system

Proof (*⇐*) **less** constructive

$$u_n = u_n^1$$

$$\begin{cases} u_0^1 = c_1 \\ u_0^2 = c_2 \\ \vdots \\ u_0^k = c_k \end{cases} \begin{cases} u_{n+1}^1 = L_1(u_n^1, u_n^2, \dots, u_n^k) \\ u_{n+1}^2 = L_2(u_n^1, u_n^2, \dots, u_n^k) \\ \vdots \\ u_{n+1}^k = L_k(u_n^1, u_n^2, \dots, u_n^k) \end{cases}$$

Let $R: \mathbb{Q}^k \to \mathbb{Q}^{k+1}$, $R(\vec{x}) = (e^{\mathsf{T}} M^0 \vec{x}, e^{\mathsf{T}} M^1 \vec{x}, \ldots, e^{\mathsf{T}} M^k \vec{x})$

$$e^{\mathsf{T}} = (1, 0, 0, \dots, 0) \in \mathbb{Q}^k$$
, $R(\vec{u_n}) = (u_n^1, u_{n+1}^1, \dots, u_{n+k}^1)$

$$K(x_0, \dots, x_k) = a_0 x_0 + \dots + a_k x_k$$
 $u_{n+k} = -\frac{a_{k-1}}{a_k} u_{n+k-1} - \dots - \frac{a_0}{a_k} u_n$

$$= (1,0,0,\ldots,0) \in \mathbb{Q} , \quad \mathsf{K}(u_n) = (u_n,u_{n+1},\ldots,u_{n+k})$$

$$\implies \text{ nonzero linear } K : \mathbb{Q}^{k+1} \to \mathbb{Q} \text{ s.t. } \operatorname{im}(R) \subseteq \ker(K) \qquad \text{i.e. } K(R(\vec{x})) = 0$$

$$K(x_0,\ldots,x_k) = a_0x_0 + \ldots a_kx_k \qquad u_{n+k} = -\frac{a_{k-1}}{2}u_{n+k-1} - \ldots - \frac{a_0}{2}u_n$$

 $\leadsto M \in \mathbb{Q}^{k \times k} \quad \vec{u}_n^{\mathsf{T}} = M^n \cdot \vec{u_0}$

 $\vec{u_n} = (u_n^1, \dots, u_n^k)$

Outline

1. Introduction (mostly linear recursive sequences)

2. Polynomial recursive sequences

3. Proof that n^n is not polynomially recursive

4. Applications in weighted automata

Polynomial recursive sequences

Example: $a_n = n!$

Polynomial recursive sequences

Example:
$$a_n=n!$$
 $b_n=n+1$
$$\begin{cases} a_0=1\\ b_0=1 \end{cases} \qquad \begin{cases} a_n=a_{n-1}\cdot b_{n-1}\\ b_n=b_{n-1}+1 \end{cases}$$

Polynomial recursive sequences

Example:
$$a_n=n!$$
 $b_n=n+1$
$$\begin{cases} a_0=1\\ b_0=1 \end{cases} \qquad \begin{cases} a_n=a_{n-1}\cdot b_{n-1}\\ b_n=b_{n-1}+1 \end{cases}$$

Remark: $n! \approx 2^{n \log(n)}$ is not linear recursive.

 u_n linear recursive $\implies |u_n| \leq C^n$ for some $C \in \mathbb{Q}$

Polynomial recursive sequences

Example:
$$a_n=n!$$
 $b_n=n+1$
$$\begin{cases} a_0=1 \\ b_0=1 \end{cases} \qquad \begin{cases} a_n=a_{n-1}\cdot b_{n-1} \\ b_n=b_{n-1}+1 \end{cases}$$

Remark: $n! \approx 2^{n \log(n)}$ is not linear recursive.

 u_n linear recursive $\implies |u_n| \leq C^n$ for some $C \in \mathbb{Q}$

Definition

A sequence a_n is **polynomial recursive** if there are u_n^1, \ldots, u_n^k , $a_n = u_n^1$ and polynomials $P_1, \ldots, P_k \in \mathbb{Q}[x_1, \ldots, x_k]$

$$\begin{cases} u_0^1 = c_1 \\ u_0^2 = c_2 \end{cases} \qquad \begin{cases} u_{n+1}^1 = P_1(u_n^1, u_n^2, \dots, u_n^k) \\ u_{n+1}^2 = P_2(u_n^1, u_n^2, \dots, u_n^k) \\ \vdots \\ u_0^k = c_k \end{cases}$$

$$\vdots$$

$$u_{n+1}^k = P_k(u_n^1, u_n^2, \dots, u_n^k)$$

Polynomial recursive sequences

Example:
$$a_n=n!$$
 $b_n=n+1$
$$\begin{cases} a_0=1\\ b_0=1 \end{cases} \qquad \begin{cases} a_n=a_{n-1}\cdot b_{n-1}\\ b_n=b_{n-1}+1 \end{cases}$$

Remark: $n! \approx 2^{n \log(n)}$ is not linear recursive.

 u_n linear recursive $\implies |u_n| < C^n$ for some $C \in \mathbb{Q}$

generalise linear recursive sequences

Definition

A sequence a_n is **polynomial recursive** if there are u_n^1, \ldots, u_n^k , $a_n = u_n^1$ and polynomials $P_1, \ldots, P_k \in \mathbb{Q}[x_1, \ldots, x_k]$

$$\begin{cases} u_0^1 = c_1 \\ u_0^2 = c_2 \\ \vdots \\ u_0^k = c_k \end{cases} \begin{cases} u_{n+1}^1 = P_1(u_n^1, u_n^2, \dots, u_n^k) \\ u_{n+1}^2 = P_2(u_n^1, u_n^2, \dots, u_n^k) \\ \vdots \\ u_{n+1}^k = P_k(u_n^1, u_n^2, \dots, u_n^k) \end{cases}$$

Example 1: $a_n = n!$

Example 1: $a_n = n!$

Example 2: $b_0 = 2$, $b_n = (b_{n-1})^2$

Example 1: $a_n = n!$

Example 2:
$$b_0 = 2$$
, $b_n = (b_{n-1})^2 \longrightarrow b_n = 2^{2^n}$

Example 1: $a_n = n!$

Example 2:
$$b_0 = 2$$
, $b_n = (b_{n-1})^2 \longrightarrow b_n = 2^{2^n}$

Fact: u_n polynomial recursive $\implies |u_n| \leq C^{D^n}$ for some $C, D \in \mathbb{Q}$

Example 1: $a_n = n!$

Example 2:
$$b_0 = 2$$
, $b_n = (b_{n-1})^2 \longrightarrow b_n = 2^{2^n}$

Fact: u_n polynomial recursive $\implies |u_n| \leq C^{D^n}$ for some $C, D \in \mathbb{Q}$

Example 3 (homework)
$$c_n = F_{F_n}$$
 (F_n – Fibonacci)

Example 1: $a_n = n!$

Example 2:
$$b_0 = 2$$
, $b_n = (b_{n-1})^2 \longrightarrow b_n = 2^{2^n}$

Fact: u_n polynomial recursive $\Longrightarrow |u_n| \leq C^{D^n}$ for some $C, D \in \mathbb{Q}$

Example 3 (homework)
$$c_n = F_{F_n}$$
 (F_n – Fibonacci)

Nonexample: Catalan numbers C_n are not polynomial recursive.

Example 1: $a_n = n!$

Example 2:
$$b_0 = 2$$
, $b_n = (b_{n-1})^2 \longrightarrow b_n = 2^{2^n}$

Fact: u_n polynomial recursive $\Longrightarrow |u_n| \leq C^{D^n}$ for some $C, D \in \mathbb{Q}$

Example 3 (homework)
$$c_n = F_{F_n}$$
 (F_n – Fibonacci)

Nonexample: Catalan numbers C_n are not polynomial recursive.

Note:
$$C_n = \frac{1}{n+1} {2n \choose n} \approx 4^n$$
 so no asymptotic argument

Example 1: $a_n = n!$

Example 2:
$$b_0 = 2$$
, $b_n = (b_{n-1})^2 \longrightarrow b_n = 2^{2^n}$

Fact: u_n polynomial recursive $\Longrightarrow |u_n| \leq C^{D^n}$ for some $C, D \in \mathbb{Q}$

Example 3 (homework)
$$c_n = F_{F_n}$$
 (F_n – Fibonacci)

Nonexample: Catalan numbers C_n are not polynomial recursive.

Note:
$$C_n = \frac{1}{n+1} {2n \choose n} \approx 4^n$$
 so no asymptotic argument

Proof. (over \mathbb{Z})

1. u_n polynomial recursive $\implies u_n \mod p$ ultimately periodic

Example 1: $a_n = n!$

Example 2:
$$b_0 = 2$$
, $b_n = (b_{n-1})^2 \longrightarrow b_n = 2^{2^n}$

Fact: u_n polynomial recursive $\Longrightarrow |u_n| \leq C^{D^n}$ for some $C, D \in \mathbb{Q}$

Example 3 (homework)
$$c_n = F_{F_n}$$
 (F_n – Fibonacci)

Nonexample: Catalan numbers C_n are not polynomial recursive.

Note:
$$C_n = \frac{1}{n+1} {2n \choose n} \approx 4^n$$
 so no asymptotic argument

Proof. (over \mathbb{Z})

1. u_n polynomial recursive $\implies u_n \mod p$ ultimately periodic There are p^k possible $(u_n^1 \mod p), (u_n^2 \mod p), \dots, (u_n^k \mod p)$

Example 1: $a_n = n!$

Example 2:
$$b_0 = 2$$
, $b_n = (b_{n-1})^2 \longrightarrow b_n = 2^{2^n}$

Fact: u_n polynomial recursive $\Longrightarrow |u_n| \leq C^{D^n}$ for some $C, D \in \mathbb{Q}$

Example 3 (homework)
$$c_n = F_{F_n}$$
 (F_n – Fibonacci)

Nonexample: Catalan numbers C_n are not polynomial recursive.

Note:
$$C_n = \frac{1}{n+1} {2n \choose n} \approx 4^n$$
 so no asymptotic argument

Proof. (over \mathbb{Z})

- **1.** u_n polynomial recursive $\implies u_n \mod p$ ultimately periodic There are p^k possible $(u_n^1 \mod p), (u_n^2 \mod p), \dots, (u_n^k \mod p)$
- **2.** Fact. C_n is odd iff $n = 2^m 1$ for some m



Example 1: $a_n = n!$

Example 2:
$$b_0 = 2$$
, $b_n = (b_{n-1})^2 \longrightarrow b_n = 2^{2^n}$

Fact: u_n polynomial recursive $\Longrightarrow |u_n| \leq C^{D^n}$ for some $C, D \in \mathbb{Q}$

Example 3 (homework)
$$c_n = F_{F_n}$$
 (F_n – Fibonacci)

Nonexample: Catalan numbers C_n are not polynomial recursive.

Note: $C_n = \frac{1}{n+1} {2n \choose n} \approx 4^n$ so no asymptotic argument

Proof. (over \mathbb{Z}) more technical over \mathbb{Q}

- **1.** u_n polynomial recursive $\implies u_n \mod p$ ultimately periodic There are p^k possible $(u_n^1 \mod p), (u_n^2 \mod p), \ldots, (u_n^k \mod p)$
- **2.** Fact. C_n is odd iff $n = 2^m 1$ for some m

Definition

Consider a class of sequences defined by

$$u_{n+k} = P(u_n, \ldots, u_{n+k-1})$$

for some $P \in \mathbb{Q}[x_1, \dots, x_k]$.

Definition

Consider a class of sequences defined by

$$u_{n+k} = P(u_n, \ldots, u_{n+k-1})$$

for some $P \in \mathbb{Q}[x_1, \dots, x_k]$.

Proposition

This is a strict subclass of polynomial recursive sequences.

For example n! cannot be defined like that.

Definition

Consider a class of sequences defined by

$$u_{n+k} = P(u_n, \ldots, u_{n+k-1})$$

for some $P \in \mathbb{Q}[x_1, \dots, x_k]$.

Proposition

This is a strict subclass of polynomial recursive sequences.

For example n! cannot be defined like that.

But notice

$$\frac{(n+2)!}{(n+1)!} = \frac{(n+1)!}{n!} + 1$$

Definition

Consider a class of sequences defined by

$$u_{n+k} = P(u_n, \ldots, u_{n+k-1})$$

for some $P \in \mathbb{Q}[x_1, \ldots, x_k]$.

Proposition

This is a strict subclass of polynomial recursive sequences.

For example n! cannot be defined like that.

But notice

$$\frac{(n+2)!}{(n+1)!} = \frac{(n+1)!}{n!} + 1$$

$$u_n = n!$$

$$P(x_1, x_2, x_3) = x_3x_1 - x_2^2 - x_2x_1$$

$$P(u_n, u_{n+1}, u_{n+2}) = 0$$

9 / 19

Definition

Consider a class of sequences defined by

$$u_{n+k} = P(u_n, \ldots, u_{n+k-1})$$

for some $P \in \mathbb{Q}[x_1, \dots, x_k]$.

Proposition

This is a strict subclass of polynomial recursive sequences.

For example *n*! cannot be defined like that.

But notice

$$\frac{(n+2)!}{(n+1)!} = \frac{(n+1)!}{n!} + 1$$

$$u_n = n!$$

$$P(x_1, x_2, x_3) = x_3x_1 - x_2^2 - x_2x_1$$

$$P(u_n, u_{n+1}, u_{n+2}) = 0$$

 u_{n+k} nonlinear

Definition

A sequence u_n admits a cancelling polynomial if

$$P(u_n, \ldots, u_{n+k}) = 0$$
 for all n

for some nonzero $P \in \mathbb{Q}[x_1, \dots, x_k]$.

Definition

A sequence u_n admits a cancelling polynomial if

$$P(u_n,\ldots,u_{n+k})=0$$
 for all n

for some nonzero $P \in \mathbb{Q}[x_1, \dots, x_k]$.

Lemma

If u_n is polynomial recursive then it admits a cancelling polynomial.

(proof on the next slide)

Definition

A sequence u_n admits a cancelling polynomial if

$$P(u_n,\ldots,u_{n+k})=0$$
 for all n

for some nonzero $P \in \mathbb{Q}[x_1, \ldots, x_k]$.

Lemma

If u_n is polynomial recursive then it admits a cancelling polynomial. (proof on the next slide)

Remark

The converse is not true.

$$P(x_1) = x_1^2 - 1$$

is cancelling for any u_n over $\{-1,1\}$

Lemma

If u_n is polynomial recursive then it admits a cancelling polynomial.

Lemma

If u_n is polynomial recursive then it admits a cancelling polynomial.

$$\begin{cases} u_{n+1}^1 = P_1(u_n^1, u_n^2, \dots, u_n^k) \\ u_{n+1}^2 = P_2(u_n^1, u_n^2, \dots, u_n^k) \\ \vdots \\ u_{n+1}^k = P_k(u_n^1, u_n^2, \dots, u_n^k) \end{cases}$$

where
$$P_i \in \mathbb{Q}[x_1, \dots, x_k]$$

Lemma

If u_n is polynomial recursive then it admits a cancelling polynomial.

$$\begin{cases} u_{n+1}^{1} = P_{1}(u_{n}^{1}, u_{n}^{2}, \dots, u_{n}^{k}) \\ u_{n+1}^{2} = P_{2}(u_{n}^{1}, u_{n}^{2}, \dots, u_{n}^{k}) \\ \vdots \\ u_{n+1}^{k} = P_{k}(u_{n}^{1}, u_{n}^{2}, \dots, u_{n}^{k}) \end{cases}$$
 where $P_{i} \in \mathbb{Q}[x_{1}, \dots, x_{k}]$

1. Define
$$P_i^{(0)}(x_1, \dots, x_k) = x_i$$

and $P_i^{(t)}(x_1, \dots, x_k) = P_i(P_1^{(t-1)}(x_1, \dots, x_k), \dots, P_k^{(t-1)}(x_1, \dots, x_k))$

Lemma

If u_n is polynomial recursive then it admits a cancelling polynomial.

$$\begin{cases} u_{n+1}^{1} = P_{1}(u_{n}^{1}, u_{n}^{2}, \dots, u_{n}^{k}) \\ u_{n+1}^{2} = P_{2}(u_{n}^{1}, u_{n}^{2}, \dots, u_{n}^{k}) \\ \vdots \\ u_{n+1}^{k} = P_{k}(u_{n}^{1}, u_{n}^{2}, \dots, u_{n}^{k}) \end{cases}$$
 where $P_{i} \in \mathbb{Q}[x_{1}, \dots, x_{k}]$

1. Define
$$P_i^{(0)}(x_1, \dots, x_k) = x_i$$

and $P_i^{(t)}(x_1, \dots, x_k) = P_i(P_1^{(t-1)}(x_1, \dots, x_k), \dots, P_k^{(t-1)}(x_1, \dots, x_k))$
$$P_i^{(t)}(u_n^1, \dots, u_n^k) = u_{n+t}^i$$

Lemma

If u_n is polynomial recursive then it admits a cancelling polynomial.

$$\begin{cases} u_{n+1}^1 = P_1(u_n^1, u_n^2, \dots, u_n^k) \\ u_{n+1}^2 = P_2(u_n^1, u_n^2, \dots, u_n^k) \\ \vdots \\ u_{n+1}^k = P_k(u_n^1, u_n^2, \dots, u_n^k) \end{cases}$$
 where $P_i \in \mathbb{Q}[x_1, \dots, x_k]$

- 1. Define $P_i^{(0)}(x_1,\ldots,x_k)=x_i$ and $P_i^{(t)}(x_1, \dots, x_k) = P_i(P_1^{(t-1)}(x_1, \dots, x_k), \dots, P_k^{(t-1)}(x_1, \dots, x_k))$ $P_i^{(t)}(u_n^1, \dots, u_n^k) = u_{n+t}^i$ 2. Fact. $P_1^{(0)}, \dots, P_1^{(k)}$ are algebraically dependent over \mathbb{Q} in $\mathbb{Q}(x_1, \dots, x_k)$

Lemma

If u_n is polynomial recursive then it admits a cancelling polynomial.

Proof. (Similar to the less constructive proof)

$$\begin{cases} u_{n+1}^1 = P_1(u_n^1, u_n^2, \dots, u_n^k) \\ u_{n+1}^2 = P_2(u_n^1, u_n^2, \dots, u_n^k) \\ \vdots \\ u_{n+1}^k = P_k(u_n^1, u_n^2, \dots, u_n^k) \end{cases}$$
 where $P_i \in \mathbb{Q}[x_1, \dots, x_k]$

- 1. Define $P_i^{(0)}(x_1,\ldots,x_k)=x_i$ and $P_i^{(t)}(x_1, \dots, x_k) = P_i(P_1^{(t-1)}(x_1, \dots, x_k), \dots, P_k^{(t-1)}(x_1, \dots, x_k))$ $P_i^{(t)}(u_n^1, \dots, u_n^k) = u_{n+t}^i$ 2. Fact. $P_1^{(0)}, \dots, P_1^{(k)}$ are algebraically dependent over \mathbb{Q} in $\mathbb{Q}(x_1, \dots, x_k)$

so there is $Q \in \mathbb{Q}[y_0, ..., y_k]$ s.t. $Q(P_1^{(0)}, ..., P_1^{(k)}) = 0$

Outline

1. Introduction (mostly linear recursive sequences)

2. Polynomial recursive sequences

3. Proof that n^n is not polynomially recursive

4. Applications in weighted automata

Theorem

 $u_n = n^n$ is not polynomial recursive

Theorem

 $u_n = n^n$ is not polynomial recursive

1. Asymptotic argument?

Recall that n! is polynomial recursive

Theorem

 $u_n = n^n$ is not polynomial recursive

1. Asymptotic argument?

No!

Recall that n! is polynomial recursive

So is $3^n n!$

 $n! \le n^n \le 3^n n!$ (Stirling)

Theorem

 $u_n = n^n$ is not polynomial recursive

1. Asymptotic argument?

No!

Recall that n! is polynomial recursive

So is $3^n n!$

 $n! \le n^n \le 3^n n!$ (Stirling)

2. Ultimate periodicity mod p?

Recall that polynomial recursive sequences are ultimately periodic mod periodic mod

Theorem

 $u_n = n^n$ is not polynomial recursive

1. Asymptotic argument?

No!

Recall that *n*! is polynomial recursive

So is $3^n n!$

 $n! \le n^n \le 3^n n!$ (Stirling)

2. Ultimate periodicity mod p?

No!

Recall that polynomial recursive sequences are ultimately periodic mod p

 $u_{n+p(p-1)} \equiv u_n \mod p$ (little Fermat)

Proof using cancelling polynomials

Theorem

 $u_n = n^n$ is not polynomial recursive

Proof using cancelling polynomials

Theorem

 $u_n = n^n$ is not polynomial recursive

Proof. (By contradiction, for the next 3 slides)

• If u_n is polynomial recursive there is a cancelling polynomial $Z \in \mathbb{Q}[x_0,\ldots,x_k]$

$$Z(n^n,(n+1)^{n+1},\ldots,(n+k)^{n+k})=0$$

Theorem

 $u_n = n^n$ is not polynomial recursive

Proof. (By contradiction, for the next 3 slides)

ullet If u_n is polynomial recursive there is a cancelling polynomial $Z\in\mathbb{Q}[x_0,\ldots,x_k]$

$$Z(n^n, (n+1)^{n+1}, \ldots, (n+k)^{n+k}) = 0$$

we can assume $Z \in \mathbb{Z}[x_0,\ldots,x_k]$

Theorem

 $u_n = n^n$ is not polynomial recursive

Proof. (By contradiction, for the next 3 slides)

ullet If u_n is polynomial recursive there is a cancelling polynomial $Z\in\mathbb{Q}[x_0,\ldots,x_k]$

$$Z(n^n, (n+1)^{n+1}, \ldots, (n+k)^{n+k}) = 0$$

we can assume $Z \in \mathbb{Z}[x_0, \ldots, x_k]$

Theorem

 $u_n = n^n$ is not polynomial recursive

Proof. (By contradiction, for the next 3 slides)

ullet If u_n is polynomial recursive there is a cancelling polynomial $Z\in\mathbb{Q}[x_0,\ldots,x_k]$

$$Z(n^n, (n+1)^{n+1}, \ldots, (n+k)^{n+k}) = 0$$

we can assume $Z \in \mathbb{Z}[x_0, \ldots, x_k]$

$$4x_0x_1^2x_2^3 = 4 \cdot n^n \cdot (n+1)^{2(n+1)} \cdot (n+2)^{3(n+2)}$$

Theorem

 $u_n = n^n$ is not polynomial recursive

Proof. (By contradiction, for the next 3 slides)

ullet If u_n is polynomial recursive there is a cancelling polynomial $Z\in\mathbb{Q}[x_0,\ldots,x_k]$

$$Z(n^n, (n+1)^{n+1}, \dots, (n+k)^{n+k}) = 0$$

we can assume $Z \in \mathbb{Z}[x_0, \ldots, x_k]$

$$4x_0x_1^2x_2^3 = 4 \cdot n^n \cdot (n+1)^{2(n+1)} \cdot (n+2)^{3(n+2)}$$

= $4(n+1)^2(n+2)^6 \cdot (n(n+1)^2(n+2)^3)^n$

Theorem

 $u_n = n^n$ is not polynomial recursive

Proof. (By contradiction, for the next 3 slides)

ullet If u_n is polynomial recursive there is a cancelling polynomial $Z\in\mathbb{Q}[x_0,\ldots,x_k]$

$$Z(n^n, (n+1)^{n+1}, \ldots, (n+k)^{n+k}) = 0$$

we can assume $Z \in \mathbb{Z}[x_0,\ldots,x_k]$

$$4x_0x_1^2x_2^3 = 4 \cdot n^n \cdot (n+1)^{2(n+1)} \cdot (n+2)^{3(n+2)}$$

$$= 4(n+1)^2(n+2)^6 \cdot (n(n+1)^2(n+2)^3)^n = P(n) \cdot Q(n)^n;$$

$$P(x) = 4(x+1)^2(x+2)^6,$$

$$Q(x) = x(x+1)^2(x+2)^3.$$

Theorem

 $u_n = n^n$ is not polynomial recursive

Proof. (By contradiction, for the next 3 slides)

ullet If u_n is polynomial recursive there is a cancelling polynomial $Z\in\mathbb{Q}[x_0,\ldots,x_k]$

$$Z(n^n, (n+1)^{n+1}, \ldots, (n+k)^{n+k}) = 0$$

we can assume $Z \in \mathbb{Z}[x_0, \ldots, x_k]$

• Consider a **monomial** in Z e.g. $4x_0x_1^2x_2^2$:

$$4x_0x_1^2x_2^3 = 4 \cdot n^n \cdot (n+1)^{2(n+1)} \cdot (n+2)^{3(n+2)}$$

$$= 4(n+1)^2(n+2)^6 \cdot (n(n+1)^2(n+2)^3)^n = P(n) \cdot Q(n)^n;$$

$$P(x) = 4(x+1)^2(x+2)^6,$$

$$Q(x) = x(x+1)^2(x+2)^3.$$

Conclusion: Rewrite $Z(n^n, \ldots, (n+k)^{n+k}) = \sum_{i=1}^{\ell} P_i(n) \cdot Q_i(n)^n$,

where $P_i, Q_i \in \mathbb{Z}[x]$ are nonzero, and Q_i are pairwise different.

It remains to show (by contradiction)

Lemma

There are no
$$P_1,\ldots,P_\ell,Q_1,\ldots,Q_\ell\in\mathbb{Z}[x]$$
, where Q_i pairwise different and $\sum_{i=1}^\ell P_i(n)\cdot Q_i(n)^n=0$ for all $n\in\mathbb{N}$.

It remains to show (by contradiction)

Lemma

There are no $P_1,\ldots,P_\ell,Q_1,\ldots,Q_\ell\in\mathbb{Z}[x]$, where Q_i pairwise different and $\sum_{i=1}^\ell P_i(n)\cdot Q_i(n)^n=0$ for all $n\in\mathbb{N}$.

Fact (key idea)

$$\sum_{i=1}^{\ell} P_i(a) \cdot Q_i(a)^b \equiv 0 \mod p$$
 for all $a, b \in \mathbb{Z}$ $(b > 0)$, p prime.

It remains to show (by contradiction)

Lemma

There are no $P_1,\ldots,P_\ell,Q_1,\ldots,Q_\ell\in\mathbb{Z}[x]$, where Q_i pairwise different and $\sum_{i=1}^\ell P_i(n)\cdot Q_i(n)^n=0$ for all $n\in\mathbb{N}$.

Fact (key idea)

$$\sum_{i=1}^{\ell} P_i(a) \cdot Q_i(a)^b \equiv 0 \mod p$$
 for all $a, b \in \mathbb{Z}$ $(b > 0)$, p prime.

Proof. Take $n \in \mathbb{N}$ such that $n \equiv_p a$ and $n \equiv_{p-1} b$

It remains to show (by contradiction)

Lemma

There are no $P_1, \ldots, P_\ell, Q_1, \ldots, Q_\ell \in \mathbb{Z}[x]$, where Q_i pairwise different and $\sum_{i=1}^{\ell} P_i(n) \cdot Q_i(n)^n = 0$ for all $n \in \mathbb{N}$.

Fact (key idea)

 $\sum_{i=1}^{\ell} P_i(a) \cdot Q_i(a)^b \equiv 0 \mod p$ for all $a, b \in \mathbb{Z}$ (b > 0), p prime.

Proof. Take $n \in \mathbb{N}$ such that $n \equiv_p a$ and $n \equiv_{p-1} b$ (p and p-1 are coprime)

It remains to show (by contradiction)

Lemma

There are no $P_1, \ldots, P_\ell, Q_1, \ldots, Q_\ell \in \mathbb{Z}[x]$, where Q_i pairwise different and $\sum_{i=1}^{\ell} P_i(n) \cdot Q_i(n)^n = 0$ for all $n \in \mathbb{N}$.

Fact (key idea)

$$\sum_{i=1}^{\ell} P_i(a) \cdot Q_i(a)^b \equiv 0 \mod p$$
 for all $a, b \in \mathbb{Z}$ $(b > 0)$, p prime.

Proof. Take
$$n \in \mathbb{N}$$
 such that $n \equiv_p a$ and $n \equiv_{p-1} b$ (p and $p-1$ are coprime)

(
$$p$$
 and $p-1$ are coprime)

$$n \equiv a \mod p \qquad \Rightarrow \qquad P_i(n) \equiv P_i(a) \mod p$$

It remains to show (by contradiction)

Lemma

There are no $P_1, \ldots, P_\ell, Q_1, \ldots, Q_\ell \in \mathbb{Z}[x]$, where Q_i pairwise different and $\sum_{i=1}^{\ell} P_i(n) \cdot Q_i(n)^n = 0$ for all $n \in \mathbb{N}$.

Fact (key idea)

$$\sum_{i=1}^{\ell} P_i(a) \cdot Q_i(a)^b \equiv 0 \mod p$$
 for all $a, b \in \mathbb{Z}$ $(b > 0)$, p prime.

Proof. Take $n \in \mathbb{N}$ such that $n \equiv_p a$ and $n \equiv_{p-1} b$ (p and p-1 are coprime)

$$(p \text{ and } p-1 \text{ are coprime})$$

- (little Fermat)

$$n \equiv a \mod p \qquad \Rightarrow \qquad P_i(n) \equiv P_i(a) \mod p$$

$$n \equiv b \mod p - 1, \ b > 0 \qquad \Rightarrow \qquad Q_i(n)^n \equiv Q_i(a)^n \equiv Q_i(a)^b \mod p$$

$$n \equiv b \mod p - 1, \ b > 0$$

It remains to show (by contradiction)

Lemma

There are no $P_1, \ldots, P_\ell, Q_1, \ldots, Q_\ell \in \mathbb{Z}[x]$, where Q_i pairwise different and $\sum_{i=1}^{\ell} P_i(n) \cdot Q_i(n)^n = 0$ for all $n \in \mathbb{N}$.

Fact (key idea)

$$\sum_{i=1}^{\ell} P_i(a) \cdot Q_i(a)^b \equiv 0 \mod p$$
 for all $a, b \in \mathbb{Z}$ $(b > 0)$, p prime.

Proof. Take
$$n \in \mathbb{N}$$
 such that $n \equiv_p a$ and $n \equiv_{p-1} b$ (p and $p-1$ are coprime)

$$(p \text{ and } p-1 \text{ are coprime})$$

$$n \equiv a \mod p \qquad \Rightarrow \qquad P_i(n) \equiv P_i(a) \mod p$$

$$n \equiv b \mod p - 1, \ b > 0 \qquad \Rightarrow \qquad Q_i(n)^n \equiv Q_i(a)^n \equiv Q_i(a)^b \mod p$$

$$\sum_{i=1}^{\ell} P_i(a) \cdot Q_i(a)^b \equiv_p \sum_{i=1}^{\ell} P_i(n) \cdot Q_i(n)^n = 0$$



 $\sum_{i=1}^{\ell} P_i(a) \cdot Q_i(a)^b \equiv 0 \mod p$ for all $a, b \in \mathbb{Z}$ (b > 0) and all prime p.

 P_i , Q_i are nonzero and Q_i are pairwise different

 $\sum_{i=1}^{\ell} P_i(a) \cdot Q_i(a)^b \equiv 0 \mod p \quad \text{for all } a, b \in \mathbb{Z} \ (b > 0) \text{ and all prime } p.$ $P_i, \ Q_i \text{ are nonzero and } Q_i \text{ are pairwise different}$

Write down for any a, p and all $b = 1, 2, 3, \ldots, \ell$:

 $\sum_{i=1}^{\ell} P_i(a) \cdot Q_i(a)^b \equiv 0 \mod p \quad \text{ for all } a,b \in \mathbb{Z} \ (b>0) \text{ and all prime } p.$

 P_i , Q_i are nonzero and Q_i are pairwise different

Write down for any a, p and all $b = 1, 2, 3, \dots, \ell$:

$$P_1(a) \cdot Q_1(a)^1 + \ldots + P_{\ell}(a) \cdot Q_{\ell}(a)^1 \equiv 0 \mod p$$
 $P_1(a) \cdot Q_1(a)^2 + \ldots + P_{\ell}(a) \cdot Q_{\ell}(a)^2 \equiv 0 \mod p$
 $P_1(a) \cdot Q_1(a)^3 + \ldots + P_{\ell}(a) \cdot Q_{\ell}(a)^3 \equiv 0 \mod p$
 \vdots

$$P_1(a)\cdot Q_1(a)^\ell+\ldots+P_\ell(a)\cdot Q_\ell(a)^\ell\equiv 0 \mod p$$

 $\sum_{i=1}^{\ell} P_i(a) \cdot Q_i(a)^b \equiv 0 \mod p \quad \text{for all } a, b \in \mathbb{Z} \ (b > 0) \text{ and all prime } p.$ $P_i, \ Q_i \text{ are nonzero and } Q_i \text{ are pairwise different}$

Write down for any a, p and all $b = 1, 2, 3, \dots, \ell$:

$$egin{bmatrix} Q_1(a)^1 & Q_2(a)^1 & \cdots & Q_\ell(a)^1 \ Q_1(a)^2 & Q_2(a)^2 & \cdots & Q_\ell(a)^2 \ dots & dots & \ddots & dots \ Q_1(a)^\ell & Q_2(a)^\ell & \cdots & Q_\ell(a)^\ell \end{bmatrix} egin{bmatrix} P_1(a) \ P_2(a) \ dots \ P_\ell(a) \end{bmatrix} \equiv_{
ho} egin{bmatrix} 0 \ 0 \ dots \ P_\ell(a) \end{bmatrix}$$

Write down for any a, p and all $b = 1, 2, 3, \ldots, \ell$:

 $\sum_{i=1}^{\ell} P_i(a) \cdot Q_i(a)^b \equiv 0 \mod p \quad \text{for all } a, b \in \mathbb{Z} \ (b > 0) \text{ and all prime } p.$ $P_i, \ Q_i \text{ are nonzero and } Q_i \text{ are pairwise different}$

Write down for any a, p and all $b = 1, 2, 3, \dots, \ell$:

geometric sequence
$$\begin{bmatrix} Q_1(a)^1 & Q_2(a)^1 & \cdots & Q_\ell(a)^1 \\ Q_1(a)^2 & Q_2(a)^2 & \cdots & Q_\ell(a)^2 \\ \vdots & \vdots & \ddots & \vdots \\ Q_1(a)^\ell & Q_2(a)^\ell & \cdots & Q_\ell(a)^\ell \end{bmatrix} \begin{bmatrix} P_1(a) \\ P_2(a) \\ \vdots \\ P_\ell(a) \end{bmatrix} \equiv_p \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

M(a) is called a square Vandermonde matrix

Write down for any a, p and all $b = 1, 2, 3, \ldots, \ell$:

geometric sequence
$$\underbrace{ \begin{bmatrix} Q_1(a)^1 & Q_2(a)^1 & \cdots & Q_\ell(a)^1 \\ Q_1(a)^2 & Q_2(a)^2 & \cdots & Q_\ell(a)^2 \\ \vdots & \vdots & \ddots & \vdots \\ Q_1(a)^\ell & Q_2(a)^\ell & \cdots & Q_\ell(a)^\ell \end{bmatrix} }_{\pmb{M}(a)} \begin{bmatrix} P_1(a) \\ P_2(a) \\ \vdots \\ P_\ell(a) \end{bmatrix} \equiv_p \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

M(a) is called a square Vandermonde matrix

Fact:
$$\det M(a) = \prod_i Q_i(a) \cdot \prod_{i < j} (Q_i(a) - Q_j(a))$$

Write down for any a, p and all $b = 1, 2, 3, \dots, \ell$:

geometric sequence
$$\underbrace{ \begin{bmatrix} Q_1(a)^1 & Q_2(a)^1 & \cdots & Q_\ell(a)^1 \\ Q_1(a)^2 & Q_2(a)^2 & \cdots & Q_\ell(a)^2 \\ \vdots & \vdots & \ddots & \vdots \\ Q_1(a)^\ell & Q_2(a)^\ell & \cdots & Q_\ell(a)^\ell \end{bmatrix} }_{\pmb{M}(a)} \begin{bmatrix} P_1(a) \\ P_2(a) \\ \vdots \\ P_\ell(a) \end{bmatrix} \equiv_{p} \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

M(a) is called a square Vandermonde matrix

Fact: det
$$M(a) = \prod_i Q_i(a) \cdot \prod_{i < j} (Q_i(a) - Q_j(a))$$

det $M(a)$ is a nonzero polynomial (in a) iff $Q_i(a)$ are pairwise different

Write down for any a, p and all $b = 1, 2, 3, \ldots, \ell$:

geometric sequence
$$\underbrace{ \begin{bmatrix} Q_1(a)^1 & Q_2(a)^1 & \cdots & Q_\ell(a)^1 \\ Q_1(a)^2 & Q_2(a)^2 & \cdots & Q_\ell(a)^2 \\ \vdots & \vdots & \ddots & \vdots \\ Q_1(a)^\ell & Q_2(a)^\ell & \cdots & Q_\ell(a)^\ell \end{bmatrix} }_{\pmb{M}(a)} \begin{bmatrix} P_1(a) \\ P_2(a) \\ \vdots \\ P_\ell(a) \end{bmatrix} \equiv_p \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

M(a) is called a square Vandermonde matrix

Fact: det
$$M(a) = \prod_i Q_i(a) \cdot \prod_{i < j} (Q_i(a) - Q_j(a))$$

det $M(a)$ is a nonzero polynomial (in a) iff $Q_i(a)$ are pairwise different

M(a) is invertible for most $a \in \mathbb{Z}_p$ if p is big.

Write down for any a, p and all $b = 1, 2, 3, \dots, \ell$:

geometric sequence
$$\begin{bmatrix} Q_1(a)^1 & Q_2(a)^1 & \cdots & Q_\ell(a)^1 \\ Q_1(a)^2 & Q_2(a)^2 & \cdots & Q_\ell(a)^2 \\ \vdots & \vdots & \ddots & \vdots \\ Q_1(a)^\ell & Q_2(a)^\ell & \cdots & Q_\ell(a)^\ell \end{bmatrix} \begin{bmatrix} P_1(a) \\ P_2(a) \\ \vdots \\ P_\ell(a) \end{bmatrix} \equiv_{p} \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

M(a) is called a square Vandermonde matrix

Fact: det
$$M(a) = \prod_i Q_i(a) \cdot \prod_{i < j} (Q_i(a) - Q_j(a))$$

 $\det M(a)$ is a nonzero polynomial (in a) iff $Q_i(a)$ are pairwise different

M(a) is invertible for most $a \in \mathbb{Z}_p$ if p is big.

So
$$P_i(a) \equiv_p 0$$
 for most $a \in \mathbb{Z}_p$.

Write down for any a, p and all $b = 1, 2, 3, \dots, \ell$:

geometric sequence
$$\begin{bmatrix} Q_1(a)^1 & Q_2(a)^1 & \cdots & Q_\ell(a)^1 \\ Q_1(a)^2 & Q_2(a)^2 & \cdots & Q_\ell(a)^2 \\ \vdots & \vdots & \ddots & \vdots \\ Q_1(a)^\ell & Q_2(a)^\ell & \cdots & Q_\ell(a)^\ell \end{bmatrix} \begin{bmatrix} P_1(a) \\ P_2(a) \\ \vdots \\ P_\ell(a) \end{bmatrix} \equiv_{p} \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

M(a) is called a square Vandermonde matrix

Fact: det
$$M(a) = \prod_i Q_i(a) \cdot \prod_{i < j} (Q_i(a) - Q_j(a))$$

 $\det M(a)$ is a nonzero polynomial (in a) iff $Q_i(a)$ are pairwise different

M(a) is invertible for most $a \in \mathbb{Z}_p$ if p is big.

So
$$P_i(a) \equiv_p 0$$
 for most $a \in \mathbb{Z}_p$.

but P_i have at most deg P_i zeros in \mathbb{Z}_p

Outline

1. Introduction (mostly linear recursive sequences)

2. Polynomial recursive sequences

3. Proof that n^n is not polynomially recursive

4. Applications in weighted automata

Definition

A weighted automaton \mathcal{A} over \mathbb{Q} is $(d, \Sigma, \{M_a\}_{a \in \Sigma}, I, F)$, where:

- $d \in \mathbb{N}$ is the dimension;
- Σ is a finite alphabet;
- every M_a is a $d \times d$ matrix over \mathbb{Q} ;
- I and F are the initial and the final vector in \mathbb{Q}^d .

Definition

A weighted automaton \mathcal{A} over \mathbb{Q} is $(d, \Sigma, \{M_a\}_{a \in \Sigma}, I, F)$, where:

- $d \in \mathbb{N}$ is the dimension;
- Σ is a finite alphabet;
- every M_a is a $d \times d$ matrix over \mathbb{Q} ;
- I and F are the initial and the final vector in \mathbb{Q}^d .

$$\llbracket \mathcal{A}
rbracket : \Sigma^*
ightarrow \mathbb{Q}$$

$$\llbracket \mathcal{A} \rrbracket (a_1 a_2 \dots a_n) = I^{\mathsf{T}} \cdot M_{a_1} M_{a_2} \dots M_{a_n} \cdot F$$

Definition

A weighted automaton \mathcal{A} over \mathbb{Q} is $(d, \Sigma, \{M_a\}_{a \in \Sigma}, I, F)$, where:

- $d \in \mathbb{N}$ is the dimension;
- Σ is a finite alphabet;
- every M_a is a $d \times d$ matrix over \mathbb{Q} ;
- I and F are the initial and the final vector in \mathbb{Q}^d .

$$\llbracket \mathcal{A}
rbracket : \Sigma^*
ightarrow \mathbb{Q}$$

$$\llbracket \mathcal{A} \rrbracket (a_1 a_2 \dots a_n) = I^{\mathsf{T}} \cdot M_{a_1} M_{a_2} \dots M_{a_n} \cdot F$$

ullet If $|\Sigma|=1$ then $\Sigma^*=\{\epsilon,a,a^2,\ldots\}\equiv \mathbb{N}$

Then $\llbracket \mathcal{A} \rrbracket : \mathbb{N} \to \mathbb{Q}$ are sequences

Definition

A weighted automaton \mathcal{A} over \mathbb{Q} is $(d, \Sigma, \{M_a\}_{a \in \Sigma}, I, F)$, where:

- $d \in \mathbb{N}$ is the dimension;
- Σ is a finite alphabet;
- every M_a is a $d \times d$ matrix over \mathbb{Q} ;
- I and F are the initial and the final vector in \mathbb{Q}^d .

$$\llbracket \mathcal{A} \rrbracket : \Sigma^* \to \mathbb{Q}$$

$$\llbracket \mathcal{A} \rrbracket (a_1 a_2 \dots a_n) = I^{\mathsf{T}} \cdot M_{a_1} M_{a_2} \dots M_{a_n} \cdot F$$

- If $|\Sigma|=1$ then $\Sigma^*=\{\epsilon,a,a^2,\ldots\}\equiv \mathbb{N}$ Then $[\![\mathcal{A}]\!]:\mathbb{N}\to\mathbb{Q}$ are sequences
- If $|\Sigma| = 1$ there is only one $M_a = M$

$$\llbracket \mathcal{A} \rrbracket (n) = I^{\mathsf{T}} \cdot M^n \cdot F$$
 (linear recursive sequences)

Cost-register automata

Definition

Cost-register automata over $\mathbb Q$ are polynomial recursive sequences

like weighted automata over $\mathbb Q$ are linear recursive sequences

Cost-register automata

Definition

Cost-register automata over $\mathbb Q$ are polynomial recursive sequences like weighted automata over $\mathbb Q$ are linear recursive sequences

Fun fact: this model was defined (at least) 3 times

- polynomial recurrent relations [Sénizergues, 2007]
- cost-register automata [Alur, D'Antoni, Deshmukh, Raghothaman, Yuan 2013]
- polynomial automata [Benedikt, Duff, Sharad, Worrell, 2017]

Cost-register automata

Definition

Cost-register automata over $\mathbb Q$ are polynomial recursive sequences like weighted automata over $\mathbb Q$ are linear recursive sequences

Fun fact: this model was defined (at least) 3 times

- polynomial recurrent relations [Sénizergues, 2007] <
- cost-register automata [Alur, D'Antoni, Deshmukh, Raghothaman, Yuan 2013]



But all three papers are interesting for different reasons

Nonlinear extensions of weighted automata Cost-register automata Weighted MSO Weighted CFG [Many people] [Droste and Gastin, 2005] [Baker, 1979]

Nonlinear extensions of weighted automata Cost-register automata Weighted MSO Weighted CFG [Many people] [Droste and Gastin, 2005] [Baker, 1979]

ullet Assume $\Sigma=\{a\}$, so $|\Sigma|=1$ and all models recognise sequences

Nonlinear extensions of weighted automata

Cost-register automata Weighted MSO Weighted CFG

[Many people] [Droste and Gastin, 2005] [Baker, 1979]

• Assume $\Sigma = \{a\}$, so $|\Sigma| = 1$ and all models recognise sequences

Definition (Weighted Context-free grammars)

A context-free grammar assigns the number of derivation trees for a^n .

Cost-register automata Weighted MSO Weighted CFG

[Many people] [Droste and Gastin, 2005] [Baker, 1979]

• Assume $\Sigma = \{a\}$, so $|\Sigma| = 1$ and all models recognise sequences

Definition (Weighted Context-free grammars)

A context-free grammar assigns the number of derivation trees for a^n .

• For example: grammar $G: X \to a, X \to aXX$

G(1)=1 and $G_n=\sum_{i=1}^{n-2}G_iG_{n-i-1} \leadsto \mathsf{Catalan}$ numbers (shifted)

Cost-register automata Weighted MSO Weighted CFG

[Many people] [Droste and Gastin, 2005] [Baker, 1979]

• Assume $\Sigma = \{a\}$, so $|\Sigma| = 1$ and all models recognise sequences

Definition (Weighted Context-free grammars)

A context-free grammar assigns the number of derivation trees for a^n .

• For example: grammar $G: X \to a, X \to aXX$

$$G(1)=1$$
 and $G_n=\sum_{i=1}^{n-2}G_iG_{n-i-1}\leadsto \mathsf{Catalan}$ numbers (shifted)

Definition (Weighted MSO)

$$\sum$$
 instead of \exists and \prod instead of \forall .

• Assume $\Sigma = \{a\}$, so $|\Sigma| = 1$ and all models recognise sequences

Definition (Weighted Context-free grammars)

A context-free grammar assigns the number of derivation trees for a^n .

• For example: grammar $G: X \to a, X \to aXX$

$$G(1)=1$$
 and $G_n=\sum_{i=1}^{n-2}G_iG_{n-i-1}\leadsto \mathsf{Catalan}$ numbers (shifted)

Definition (Weighted MSO)

$$\sum$$
 instead of \exists and \prod instead of $\forall.$

• For example:
$$\sum_{x} 1(n) = n$$
, $\prod_{x} 2(n) = 2^n$, $\prod_{x} \sum_{y} 1(n) = n^n$

• Assume $\Sigma = \{a\}$, so $|\Sigma| = 1$ and all models recognise sequences

Definition (Weighted Context-free grammars)

A context-free grammar assigns the number of derivation trees for a^n .

ullet For example: grammar $G\colon X o a,\,X o aXX$

$$G(1)=1$$
 and $G_n=\sum_{i=1}^{n-2}G_iG_{n-i-1}\leadsto \mathsf{Catalan}$ numbers (shifted)

Definition (Weighted MSO)

 \sum instead of \exists and \prod instead of \forall .

• For example: $\sum_{x} 1(n) = n$, $\prod_{x} 2(n) = 2^{n}$, $\prod_{x} \sum_{y} 1(n) = n^{n}$

Corollary

Cost-register automata do not contain Weighted CFG and Weighted MSO

• We investigated Polynomial recursive sequences

• We investigated Polynomial recursive sequences

• Properties: asymptotic bounds, periodicity and cancelling polynomials

- We investigated Polynomial recursive sequences
- Properties: asymptotic bounds, periodicity and cancelling polynomials
- We proved that Catalan numbers C_n and n^n are not polynomial recursive.

- We investigated Polynomial recursive sequences
- Properties: asymptotic bounds, periodicity and cancelling polynomials
- We proved that Catalan numbers C_n and n^n are not polynomial recursive.
- Are cost-register automata included in weighted MSO?

 F_{F_n} are polynomial recursive (F_n Fibonacci)

Conjecture: F_{F_n} are not in Weighted MSO