Nonlinear extensions of linear recurrence sequences

Filip Mazowiecki

Uniwersytet Warszawski

Based on works with:

Michaël Cadilhac, Lorenzo Clemente, Maria Donten-Bury, Charles Paperman, Michał Pilipczuk, Cristian Riveros, Géraud Sénizergues, Aleksander Wiśniewski

SAMSA 2026

Linear recurrence sequences (LRS)

$a : \mathbb{N} \to \mathbb{Q}$

For example $a_n = n^2$

$$a_0 = 0, \quad a_{n+1} = a_n + 2b_n + c_n$$

$$b_0 = 0, \quad b_{n+1} = b_n + c_n$$

$$c_0 = 1, \quad c_{n+1} = c_n$$

Linear recurrence sequences (LRS)

$a : \mathbb{N} \to \mathbb{Q}$

For example $a_n = n^2$

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

$$a_n = \begin{pmatrix} 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}^n \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$$

In general $u_n = I^\top M^n F$

Linear recurrence sequences (LRS)

$a : \mathbb{N} \to \mathbb{Q}$

For example $a_n = n^2$

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

$$a_n = \begin{pmatrix} 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 2 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}^n \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$$

In general $u_n = I^\top M^n F$

Can be also defined by $a_{n+3} = 3a_{n+2} - 3a_{n+1} + a_n$

In general $u_{n+k} = \sum_{i=0}^{k-1} \alpha_i u_{n+i}$

Many nice properties of LRS

- Unique, computable minimal degree

  ($d = 3$ for $a_n = n^2$)

Many nice properties of LRS

- Unique, computable minimal degree

  ($d = 3$ for $a_n = n^2$)

- Closure properties, given LRS a_n, b_n:

  $$c_n = a_n + b_n, \quad c_n = a_n \cdot b_n, \quad c_n = a_n * b_n = \sum_{i<n} a_i \cdot b_{n-i-1}$$

Many nice properties of LRS

- Unique, computable minimal degree

  $(d = 3 \text{ for } a_n = n^2)$

- Closure properties, given LRS a_n, b_n:

  $c_n = a_n + b_n, \quad c_n = a_n \cdot b_n, \quad c_n = a_n * b_n = \sum_{i<n} a_i \cdot b_{n-i-1}$

- Closed form

  $a_n = \sum_i p_i(n) \cdot \lambda_i^n$

  (for n big enough)

Many nice properties of LRS

- Unique, computable minimal degree

  ($d = 3$ for $a_n = n^2$)

- Closure properties, given LRS a_n, b_n:

  $$c_n = a_n + b_n, \quad c_n = a_n \cdot b_n, \quad c_n = a_n * b_n = \sum_{i<n} a_i \cdot b_{n-i-1}$$

- Closed form

  $a_n = \sum_i p_i(n) \cdot \lambda_i^n$

  (for n big enough)

  e.g. $F_n = \frac{1}{\sqrt{5}}\varphi^n + \frac{1}{\sqrt{5}}\psi^n$

Weighted automata over the rational field

- $\mathcal{A}$ is defined by $\Sigma = \{a, b, c\}, \quad M_a, M_b, M_c \in \mathbb{Q}^{d\times d}, \quad I, F \in \mathbb{Q}^d$

Weighted automata over the rational field

- $\mathcal{A}$ is defined by $\Sigma = \{a, b, c\}, \quad M_a, M_b, M_c \in \mathbb{Q}^{d \times d}, \quad I, F \in \mathbb{Q}^d$

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

  $\mathcal{A}(w) = I^\top M_w F$, where $M_w = M_{w_1} \dots M_{w_n}$ for $w = w_1 \dots w_n$.

Weighted automata over the rational field

- $\mathcal{A}$ is defined by $\Sigma = \{a, b, c\}, \quad M_a, M_b, M_c \in \mathbb{Q}^{d\times d}, \quad I, F \in \mathbb{Q}^d$

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

  $\mathcal{A}(w) = I^\top M_w F$, where $M_w = M_{w_1} \dots M_{w_n}$ for $w = w_1 \dots w_n$.

- LRS are weighted automata for $|\Sigma| = 1$.

  $a^* \equiv \mathbb{N}, \quad$ hence $\mathcal{A} : \mathbb{N} \to \mathbb{Q}$

Weighted automata over the rational field

- $\mathcal{A}$ is defined by $\Sigma = \{a, b, c\}$, $\quad M_a, M_b, M_c \in \mathbb{Q}^{d \times d}$, $\quad I, F \in \mathbb{Q}^d$

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

  $\mathcal{A}(w) = I^\top M_w F$, where $M_w = M_{w_1} \dots M_{w_n}$ for $w = w_1 \dots w_n$.

- LRS are weighted automata for $|\Sigma| = 1$.

  $a^* \equiv \mathbb{N}$, $\quad$ hence $\mathcal{A} : \mathbb{N} \to \mathbb{Q}$

  Minimal degree and closure properties of LRS follow easily

Weighted automata over the rational field

- $\mathcal{A}$ is defined by $\Sigma = \{a, b, c\}, \quad M_a, M_b, M_c \in \mathbb{Q}^{d\times d}, \quad I, F \in \mathbb{Q}^d$

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

  $\mathcal{A}(w) = I^\top M_w F$, where $M_w = M_{w_1} \dots M_{w_n}$ for $w = w_1 \dots w_n$.

- LRS are weighted automata for $|\Sigma| = 1$.

  $a^* \equiv \mathbb{N}, \quad$ hence $\mathcal{A} : \mathbb{N} \to \mathbb{Q}$

  Minimal degree and closure properties of LRS follow easily

- We consider extensions of LRS from this point of view.

Weighted automata over the rational field

- $\mathcal{A}$ is defined by $\Sigma = \{a, b, c\}, \quad M_a, M_b, M_c \in \mathbb{Q}^{d\times d}, \quad I, F \in \mathbb{Q}^d$

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

  $\mathcal{A}(w) = I^\top M_w F$, where $M_w = M_{w_1} \dots M_{w_n}$ for $w = w_1 \dots w_n$.

- LRS are weighted automata for $|\Sigma| = 1$.

  $a^* \equiv \mathbb{N}, \quad$ hence $\mathcal{A} : \mathbb{N} \to \mathbb{Q}$

  Minimal degree and closure properties of LRS follow easily

- We consider extensions of LRS from this point of view.

  We work over $\mathbb{Q}$

Polynomial sequences (polyrec)

Change matrices M_a to polynomial maps

Polynomial sequences (polyrec)

Change matrices M_a to polynomial maps

Polynomial automata, cost-register automata, polynomial recurrent relations

[Benedikt et al., 2017], [Alur et al., 2013], [Sénizergues, 2007]

Polynomial sequences (polyrec)

Change matrices M_a to polynomial maps

Polynomial automata, cost-register automata, polynomial recurrent relations

[Benedikt et al., 2017], [Alur et al., 2013], [Sénizergues, 2007]

Example $a_n = 2^{2^n}$

$a_0 = 2, \quad a_{n+1} = a_n^2, \quad f_1(x) = x^2$

Polynomial sequences (polyrec)

Change matrices M_a to polynomial maps

Polynomial automata, cost-register automata, polynomial recurrent relations

[Benedikt et al., 2017], [Alur et al., 2013], [Sénizergues, 2007]

Example $a_n = 2^{2^n}$

$a_0 = 2, \quad a_{n+1} = a_n^2, \quad f_1(x) = x^2$

Example $a_n = n!$

$a_0 = 1, \quad a_{n+1} = a_n \cdot b_n, \quad f_1(x, y) = xy$

$b_0 = 1, \quad b_{n+1} = b_n + 1, \quad f_2(x, y) = y + 1$

Polynomial sequences (polyrec)

Change matrices M_a to polynomial maps

Polynomial automata, cost-register automata, polynomial recurrent relations

[Benedikt et al., 2017], [Alur et al., 2013], [Sénizergues, 2007]

Example $a_n = 2^{2^n}$

$$a_0 = 2, \quad a_{n+1} = a_n^2, \quad f_1(x) = x^2$$

Example $a_n = n!$

$$a_0 = 1, \quad a_{n+1} = a_n \cdot b_n, \quad f_1(x, y) = xy$$

$$b_0 = 1, \quad b_{n+1} = b_n + 1, \quad f_2(x, y) = y + 1$$

Example $a_n = 2^{2^n} + n!$, or $a_n = 2^{2^n} \cdot n!$

Polyrec formally

$$\begin{aligned} a^1_{n+1} &= P_1(a^1_n, \dots, a^k_n) \\ a^2_{n+1} &= P_2(a^1_n, \dots, a^k_n) \\ &\vdots \\ a^k_{n+1} &= P_k(a^1_n, \dots, a^k_n) \end{aligned}$$

For some fixed polynomials $P_1, \dots, P_k \in Q[x_1 \dots, x_k]$

Polyrec formally

$$\begin{aligned} a^1_{n+1} &= P_1(a^1_n, \ldots, a^k_n) \\ a^2_{n+1} &= P_2(a^1_n, \ldots, a^k_n) \\ &\vdots \\ a^k_{n+1} &= P_k(a^1_n, \ldots, a^k_n) \end{aligned}$$

For some fixed polynomials $P_1, \ldots, P_k \in Q[x_1 \ldots, x_k]$

$a_n = a^1_n$ is the defined sequence

Polyrec formally

$$\begin{aligned}
a^1_{n+1} &= P_1(a^1_n, \dots, a^k_n) \\
a^2_{n+1} &= P_2(a^1_n, \dots, a^k_n) \\
&\vdots \\
a^k_{n+1} &= P_k(a^1_n, \dots, a^k_n)
\end{aligned}$$

For some fixed polynomials $P_1, \dots, P_k \in Q[x_1 \dots, x_k]$

$a_n = a^1_n$ is the defined sequence

If P_i are rational functions this is a larger class called ratrec

Algebraic sequences

In the automata definition generalise to context-free grammars (CFGs)

Weighted/probabilistic CFGs [Chomsky and Schützenberger, 1959]

Algebraic sequences

In the automata definition generalise to context-free grammars (CFGs)

Weighted/probabilistic CFGs [Chomsky and Schützenberger, 1959]

Generating function satisfy a polynomial equation $P(x, A(x)) = 0$

$A(x) = \sum_{i=0}^{\infty} a_i \cdot x^i$, where a_n is the sequence

Algebraic sequences

In the automata definition generalise to context-free grammars (CFGs)

Weighted/probabilistic CFGs [Chomsky and Schützenberger, 1959]

Generating function satisfy a polynomial equation $P(x, A(x)) = 0$

$A(x) = \sum_{i=0}^{\infty} a_i \cdot x^i$, where a_n is the sequence

Example C_n Catalan numbers

$1 - C(x) + xC(x)^2 = 0$

Algebraic sequences

In the automata definition generalise to context-free grammars (CFGs)

Weighted/probabilistic CFGs [Chomsky and Schützenberger, 1959]

Generating function satisfy a polynomial equation $P(x, A(x)) = 0$

$A(x) = \sum_{i=0}^{\infty} a_i \cdot x^i$, where a_n is the sequence

Example C_n Catalan numbers

$1 - C(x) + xC(x)^2 = 0$

Example $a_n = \binom{2n}{n}$

$(1 - 4x)A(x)^2 - 1 = 0$

Algebraic sequences

In the automata definition generalise to context-free grammars (CFGs)

Weighted/probabilistic CFGs [Chomsky and Schützenberger, 1959]

Generating function satisfy a polynomial equation $P(x, A(x)) = 0$

$A(x) = \sum_{i=0}^{\infty} a_i \cdot x^i, \quad$ where a_n is the sequence

Example C_n Catalan numbers

$1 - C(x) + xC(x)^2 = 0$

Example $a_n = \binom{2n}{n}$

$(1 - 4x)A(x)^2 - 1 = 0$

Example $a_n = C_n + a_n$

Algebraic sequences a bit more formally

Take a CFG and add a weight to each rule

Derivation tree: product of weights, sum over all derivation trees

Algebraic sequences a bit more formally

Take a CFG and add a weight to each rule

Derivation tree: product of weights, sum over all derivation trees

For unary alphabet the grammar defines a system of polynomial equations

Algebraic sequences a bit more formally

Take a CFG and add a weight to each rule

Derivation tree: product of weights, sum over all derivation trees

For unary alphabet the grammar defines a system of polynomial equations

(that can be eliminated, leaving one equation)

Algebraic sequences a bit more formally

Take a CFG and add a weight to each rule

Derivation tree: product of weights, sum over all derivation trees

For unary alphabet the grammar defines a system of polynomial equations

(that can be eliminated, leaving one equation)

Algebraic sequences are contained in holonomic sequences

allow polynomials (in n) in the recursion (special case of ratrec)

Algebraic sequences a bit more formally

Take a CFG and add a weight to each rule

Derivation tree: product of weights, sum over all derivation trees

For unary alphabet the grammar defines a system of polynomial equations

(that can be eliminated, leaving one equation)

Algebraic sequences are contained in holonomic sequences

allow polynomials (in n) in the recursion (special case of ratrec)

Example C_n Catalan numbers

$C_0 = 1, \quad (n+2)C_{n+1} = (4n+2)C_n$

Algebraic sequences a bit more formally

Take a CFG and add a weight to each rule

Derivation tree: product of weights, sum over all derivation trees

For unary alphabet the grammar defines a system of polynomial equations

(that can be eliminated, leaving one equation)

Algebraic sequences are contained in holonomic sequences

allow polynomials (in n) in the recursion (special case of ratrec)

Example C_n Catalan numbers

$C_0 = 1, \quad (n+2)C_{n+1} = (4n+2)C_n$

Example $a_n = n!$

$a_0 = 1, \quad a_{n+1} = a_n \cdot n$

MSO sequences

Present in the logic framework, replace quantifiers with aggregators

Weighted MSO [Droste and Gastin, 2005]

MSO sequences

Present in the logic framework, replace quantifiers with aggregators

Weighted MSO [Droste and Gastin, 2005]

MSO formula evaluate to 0 or 1,   constants

$\exists$, $\forall$ become $\sum$ and $\prod$

MSO sequences

Present in the logic framework, replace quantifiers with aggregators

Weighted MSO [Droste and Gastin, 2005]

MSO formula evaluate to 0 or 1, constants

$\exists$, $\forall$ become $\sum$ and $\prod$

Example $a_n = n^n$ and $b_n = n!$

$a_n = \prod_x \sum_y 1, \quad b_n = \prod_x \sum_y [x \leq y]$

MSO sequences

Present in the logic framework, replace quantifiers with aggregators

Weighted MSO [Droste and Gastin, 2005]

MSO formula evaluate to 0 or 1,   constants

$\exists$, $\forall$ become $\sum$ and $\prod$

Example $a_n = n^n$ and $b_n = n!$

$a_n = \prod_x \sum_y 1, \quad b_n = \prod_x \sum_y [x \leq y]$

Example $a_n = 2^n$ and $b_n = 2^{2^n}$

$a_n = \sum_X 1, \quad b_n = \prod_X 2$

MSO sequences

Present in the logic framework, replace quantifiers with aggregators

Weighted MSO [Droste and Gastin, 2005]

MSO formula evaluate to 0 or 1, constants

$\exists$, $\forall$ become $\sum$ and $\prod$

Example $a_n = n^n$ and $b_n = n!$

$a_n = \prod_x \sum_y 1, \quad b_n = \prod_x \sum_y [x \leq y]$

Example $a_n = 2^n$ and $b_n = 2^{2^n}$

$a_n = \sum_X 1, \quad b_n = \prod_X 2$

Example $a_n = 2^{2^n} + n!$, or $a_n = 2^{2^n} \cdot n!$

MSO sequences formally

Atomic formulas: $q \in \mathbb{Q}$, where $[\![q]\!] = q$, MSO formulas, where $[\![\varphi]\!] \in \{0, 1\}$

MSO sequences formally

Atomic formulas: $q \in \mathbb{Q}$, where $[\![q]\!] = q$, MSO formulas, where $[\![\varphi]\!] \in \{0, 1\}$

binary operators: $+$ and $\cdot$ (instead of $\vee$ and $\wedge$)

MSO sequences formally

Atomic formulas: $q \in \mathbb{Q}$, where $[\![q]\!] = q$, MSO formulas, where $[\![\varphi]\!] \in \{0, 1\}$

binary operators: $+$ and $\cdot$ (instead of $\vee$ and $\wedge$)

$\sum_x, \sum_X, \prod_x, \prod_X$ quantifiers (instead of $\exists_x, \exists_X, \forall_x, \forall_X$)

MSO sequences formally

Atomic formulas: $q \in \mathbb{Q}$, where $[\![q]\!] = q$, MSO formulas, where $[\![\varphi]\!] \in \{0, 1\}$

binary operators: $+$ and $\cdot$ (instead of $\vee$ and $\wedge$)

$\sum_x$, $\sum_X$, $\prod_x$, $\prod_X$ quantifiers (instead of $\exists_x$, $\exists_X$, $\forall_x$, $\forall_X$)

$(\sum_X)^* \prod_x \varphi$ are weighted automata

MSO sequences formally

Atomic formulas: $q \in \mathbb{Q}$, where $[\![q]\!] = q$, MSO formulas, where $[\![\varphi]\!] \in \{0, 1\}$

binary operators: $+$ and $\cdot$ (instead of $\vee$ and $\wedge$)

$\sum_x$, $\sum_X$, $\prod_x$, $\prod_X$ quantifiers (instead of $\exists_x$, $\exists_X$, $\forall_x$, $\forall_X$)

$(\sum_X)^* \prod_x \varphi$ are weighted automata

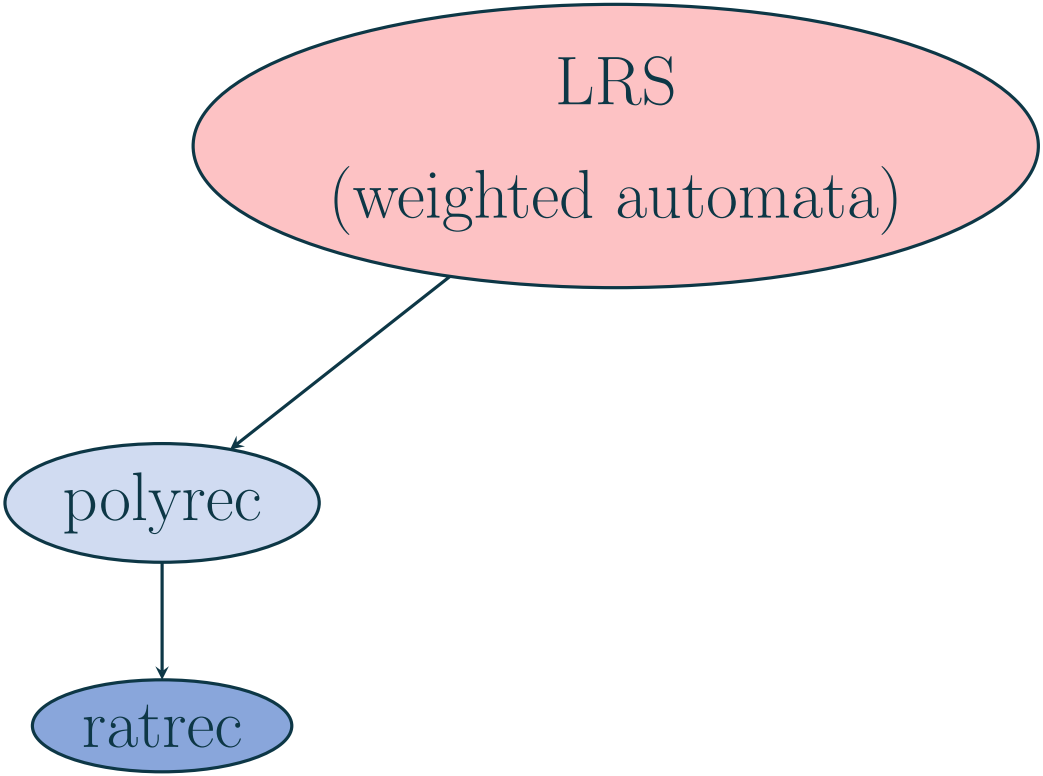
$(\sum_x)^* \prod_x \varphi$ are polynomially ambiguous weighted automata

Nonlinear extensions summary

LRS

(weighted automata)

Nonlinear extensions summary



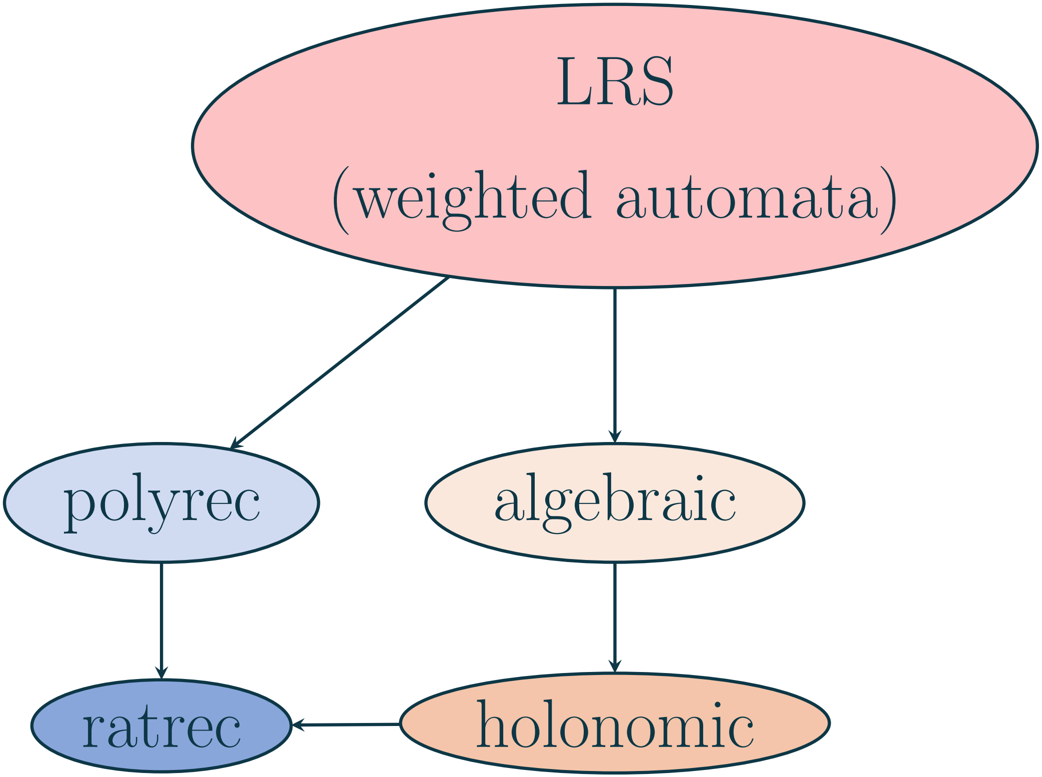
LRS

(weighted automata)

polyrec

ratrec

Nonlinear extensions summary



LRS

(weighted automata)

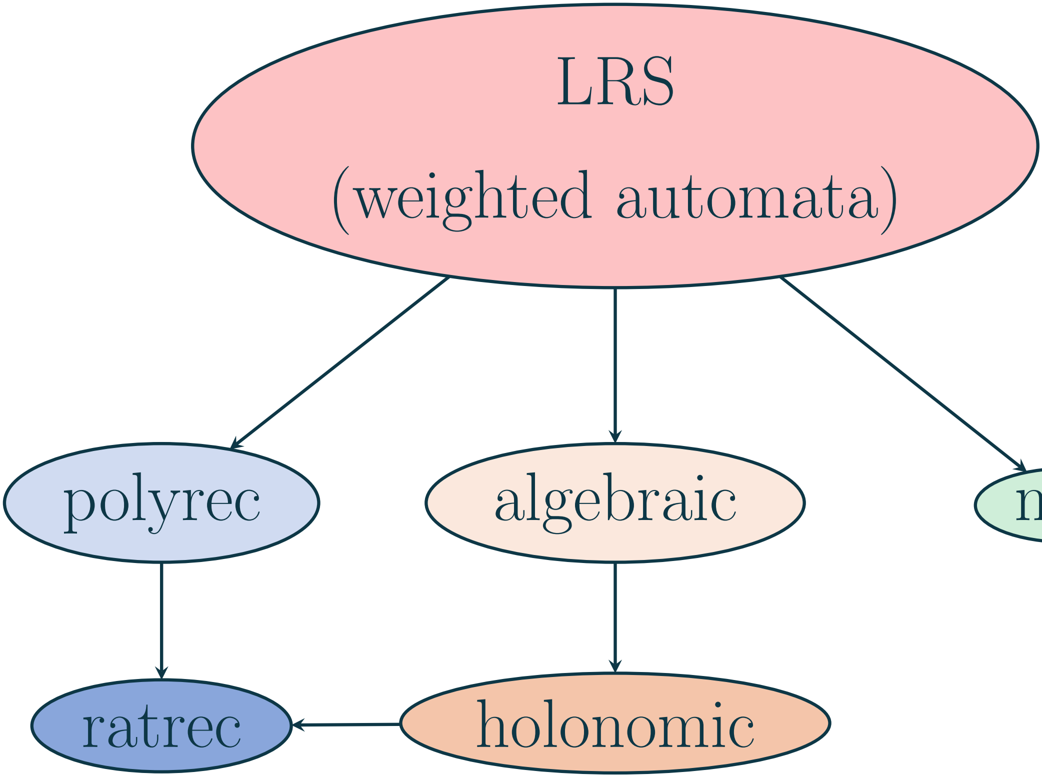
polyrec

algebraic

ratrec

holonomic

Nonlinear extensions summary



LRS

(weighted automata)

polyrec

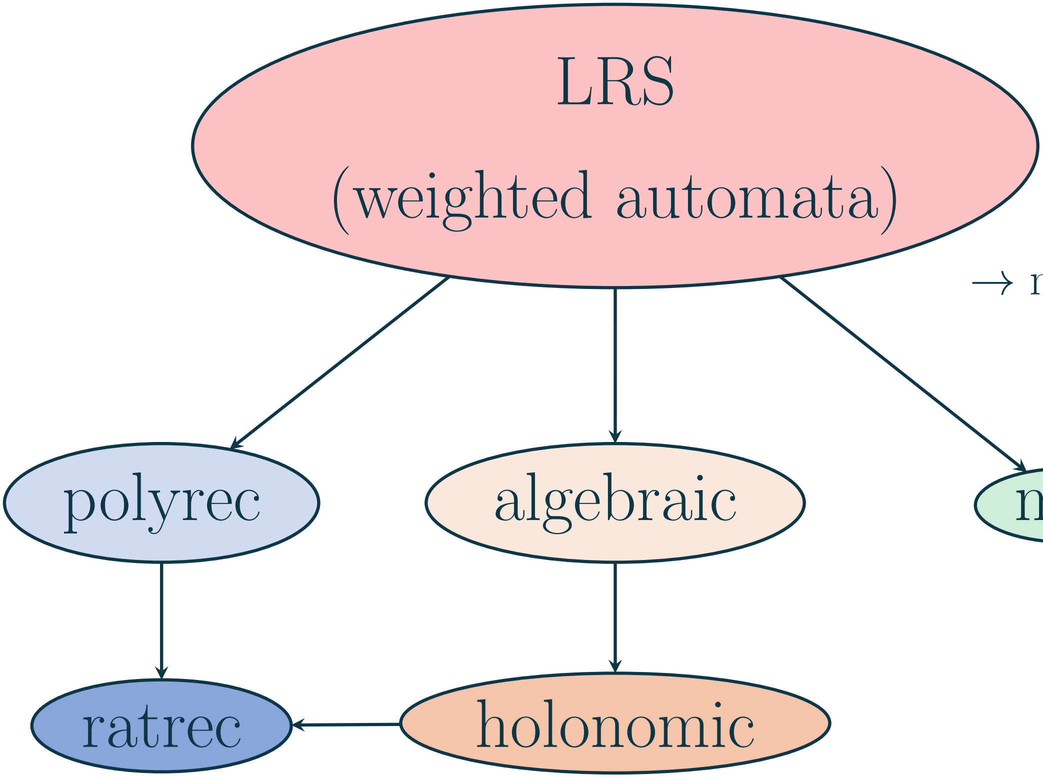
algebraic

mso

ratrec

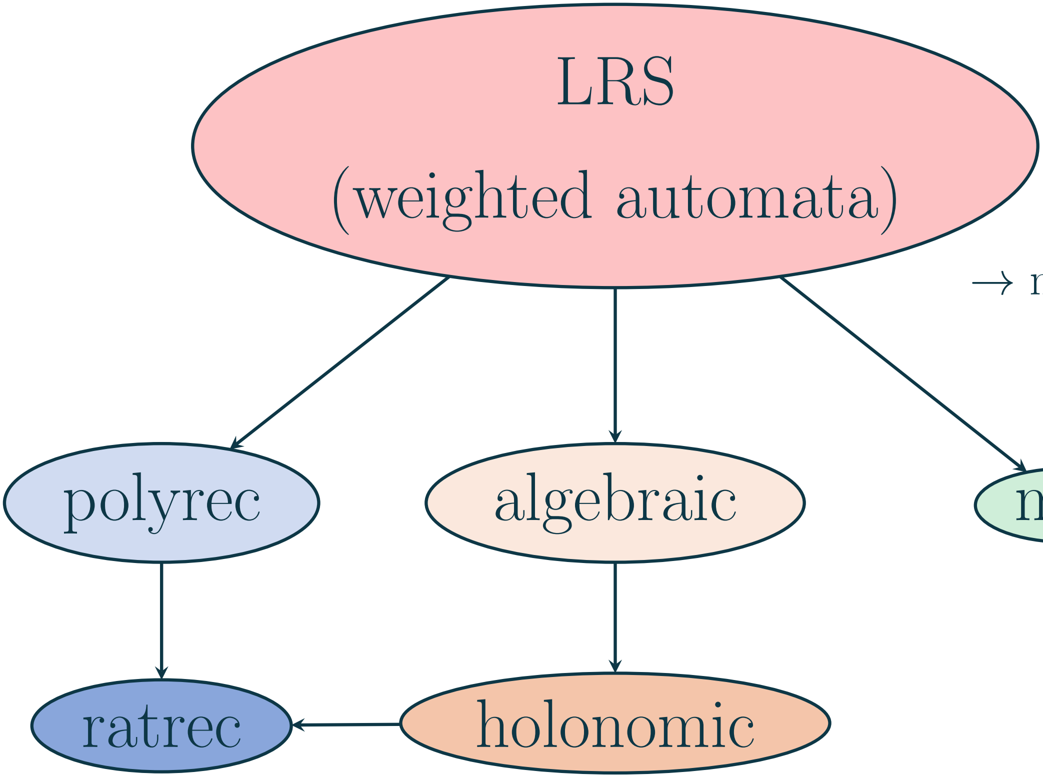
holonomic

Nonlinear extensions summary



→ means inclusion

Nonlinear extensions summary



→ means inclusion

Goal: show that there are no other inclusions.

Asymptotics of sequences

Bound on $|a_n| \leq f(n)$?

Asymptotics of sequences

Bound on $|a_n| \leq f(n)$?

- For LRS and algebraic $f(n) = c^n$

Asymptotics of sequences

Bound on $|a_n| \leq f(n)$?

- For LRS and algebraic $f(n) = c^n$

- For holonomic $f(n) = c^{n \log n}$

Asymptotics of sequences

Bound on $|a_n| \leq f(n)$?

- For LRS and algebraic $f(n) = c^n$
- For holonomic $f(n) = c^{n \log n}$
- For polyec, ratrec and mso $f(n) = c^{d^n}$

Asymptotics of sequences

Bound on $|a_n| \leq f(n)$?

- For LRS and algebraic $f(n) = c^n$
- For holonomic $f(n) = c^{n \log n}$
- For polyec, ratrec and mso $f(n) = c^{d^n}$

Corollary: holonomic cannot contain polyrec or mso

Asymptotics of sequences

Bound on $|a_n| \leq f(n)$?

- For LRS and algebraic $f(n) = c^n$

- For holonomic $f(n) = c^{n \log n}$

- For polyec, ratrec and mso $f(n) = c^{d^n}$

Corollary: holonomic cannot contain polyrec or mso

Also algebraic are strictly contained in holonomic

Sequences modulo primes

Assume $a_n \in \mathbb{N}$, define $b_n = a_n \mod p$.

Sequences modulo primes

Assume $a_n \in \mathbb{N}$, define $b_n = a_n \mod p$.

For Fibonacci $\mod 2$ we get: $0, 1, 1, 0, 1, 1, 0, \ldots$

Sequences modulo primes

Assume $a_n \in \mathbb{N}$, define $b_n = a_n \mod p$.

For Fibonacci $\mod 2$ we get: $0, 1, 1, 0, 1, 1, 0, \ldots$

For $n!$ we get: $b_0 = 1,\ b_1 = 1,\ b_2 =?, \ldots, b_p = 0,\ b_{p+1} = 0, \ldots$

Sequences modulo primes

Assume $a_n \in \mathbb{N}$, define $b_n = a_n \mod p$.

For Fibonacci mod 2 we get: $0, 1, 1, 0, 1, 1, 0, \ldots$

For $n!$ we get: $b_0 = 1,\ b_1 = 1,\ b_2 = ?, \ldots, b_p = 0,\ b_{p+1} = 0, \ldots$

In general for polyrec we eventually get a cycle

$$a^1_{n+1} = P_1(a^1_n, \ldots, a^k_n) \mod p$$
$$a^2_{n+1} = P_2(a^1_n, \ldots, a^k_n) \mod p$$
$$\vdots$$
$$a^k_{n+1} = P_k(a^1_n, \ldots, a^k_n) \mod p$$

Sequences modulo primes

Assume $a_n \in \mathbb{N}$, define $b_n = a_n \mod p$.

For Fibonacci mod 2 we get: $0, 1, 1, 0, 1, 1, 0, \ldots$

For $n!$ we get: $b_0 = 1,\ b_1 = 1,\ b_2 = ?, \ldots, b_p = 0,\ b_{p+1} = 0, \ldots$

In general for polyrec we eventually get a cycle

$$
\begin{aligned}
&a^1_{n+1} = P_1(a^1_n, \ldots, a^k_n) \mod p\\
&a^2_{n+1} = P_2(a^1_n, \ldots, a^k_n) \mod p\\
&\vdots\\
&a^k_{n+1} = P_k(a^1_n, \ldots, a^k_n) \mod p
\end{aligned}
$$

This makes sense for p big enough ($a^i_n \in \mathbb{Q}$)

Sequences modulo primes

Corollary: for p big enough polyrec mod p are ultimately periodic

Sequences modulo primes

Corollary: for p big enough polyrec mod p are ultimately periodic

Theorem (Droste and Gastin 2005, Wiśniewski 2025)

MSO sequences mod p are ultimately periodic.

Sequences modulo primes

Corollary: for p big enough polyrec mod p are ultimately periodic

Theorem (Droste and Gastin 2005, Wiśniewski 2025)

MSO sequences mod p are ultimately periodic.

Catalan numbers C_n are odd iff $n = 2^m - 1$

Sequences modulo primes

Corollary: for p big enough polyrec mod p are ultimately periodic

Theorem (Droste and Gastin 2005, Wiśniewski 2025)

MSO sequences mod p are ultimately periodic.

Catalan numbers C_n are odd iff $n = 2^m - 1$

More generally they are not ultimately periodic modulo any prime

Sequences modulo primes

Corollary: for p big enough polyrec mod p are ultimately periodic

Theorem (Droste and Gastin 2005, Wiśniewski 2025)

MSO sequences mod p are ultimately periodic.

Catalan numbers C_n are odd iff $n = 2^m - 1$

More generally they are not ultimately periodic modulo any prime

Corollary: polyrec and MSO sequences do not contain algebraic

(in particular polyrec is strictly smaller than ratrec)

Sequences modulo primes

Corollary: for p big enough polyrec mod p are ultimately periodic

Theorem (Droste and Gastin 2005, Wiśniewski 2025)

MSO sequences mod p are ultimately periodic.

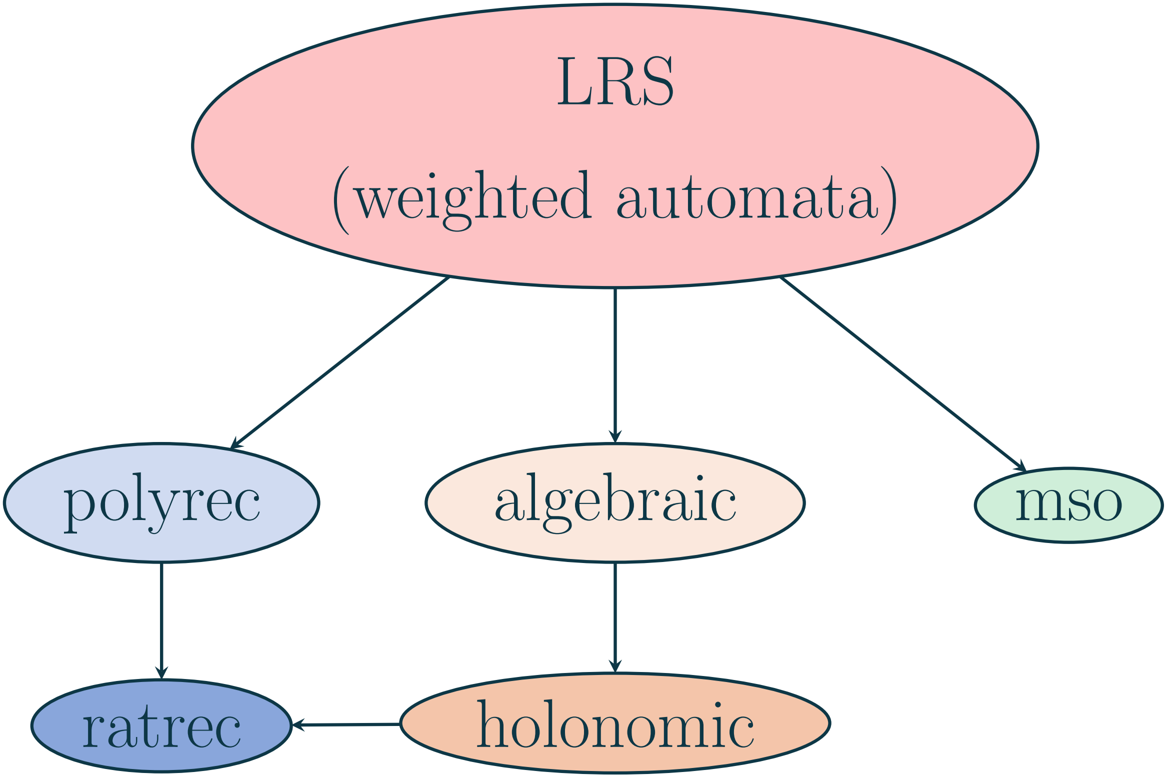
Catalan numbers C_n are odd iff $n = 2^m - 1$

More generally they are not ultimately periodic modulo any prime

Corollary: polyrec and MSO sequences do not contain algebraic
(in particular polyrec is strictly smaller than ratrec)

It remains to compare polyrec/ratrec with MSO sequences

Nonlinear extensions summary



LRS

(weighted automata)

polyrec

algebraic

mso

ratrec

holonomic

An MSO sequence which is not polyrec

$\prod_x \sum_y 1$, i.e. $a_n = n^n$

An MSO sequence which is not polyrec

$\prod_x \sum_y 1$, i.e. $a_n = n^n$

How to show it's not polyrec?

An MSO sequence which is not polyrec

$\prod_x \sum_y 1$, i.e. $a_n = n^n$

How to show it's not polyrec?

- Asymptotic argument?

  $n! \leq n^n \leq 3^n \cdot n!$

An MSO sequence which is not polyrec

$\prod_x \sum_y 1, \quad$ i.e. $a_n = n^n$

How to show it's not polyrec?

- Asymptotic argument?

  $n! \leq n^n \leq 3^n \cdot n!$

- Ultimate periodicity?

  $a_{n+p(p-1)} = (n + p(p-1))^{n+p(p-1)}$

An MSO sequence which is not polyrec

$\prod_x \sum_y 1$, i.e. $a_n = n^n$

How to show it's not polyrec?

- Asymptotic argument?

  $n! \leq n^n \leq 3^n \cdot n!$

- Ultimate periodicity?

  $a_{n+p(p-1)} = (n + p(p-1))^{n+p(p-1)}$

  $\equiv n^n \cdot n^{p(p-1)} \equiv n^n \mod p$

Cancelling polynomials

Definition

A sequence a_n admits a cancelling polynomial if there exists $k \in \mathbb{N}$ and nonzero $Z \in \mathbb{Q}[x_0, \ldots, x_k]$ such that $Z(a_n, a_{n+1}, \ldots, a_{n+k}) = 0$ for all n.

Cancelling polynomials

Definition

A sequence a_n admits a cancelling polynomial if there exists $k \in \mathbb{N}$ and nonzero $Z \in \mathbb{Q}[x_0, \ldots, x_k]$ such that $Z(a_n, a_{n+1}, \ldots, a_{n+k}) = 0$ for all n.

For $a_n = 2^{2^n}$ consider $k = 1$ and $Z(x_0, x_1) = (x_0)^2 - x_1$
works since $a_{n+1} = (a_n)^2$

Cancelling polynomials

Definition

A sequence a_n admits a cancelling polynomial if there exists $k \in \mathbb{N}$ and nonzero $Z \in \mathbb{Q}[x_0, \ldots, x_k]$ such that $Z(a_n, a_{n+1}, \ldots, a_{n+k}) = 0$ for all n.

For $a_n = 2^{2^n}$ consider $k = 1$ and $Z(x_0, x_1) = (x_0)^2 - x_1$
works since $a_{n+1} = (a_n)^2$

For $a_n = n!$ observe that
$\frac{(n+2)!}{(n+1)!} = \frac{(n+1)!}{(n)!} + 1$

Cancelling polynomials

Definition

A sequence a_n admits a cancelling polynomial if there exists $k \in \mathbb{N}$ and nonzero $Z \in \mathbb{Q}[x_0, \ldots, x_k]$ such that $Z(a_n, a_{n+1}, \ldots, a_{n+k}) = 0$ for all n.

For $a_n = 2^{2^n}$ consider $k = 1$ and $Z(x_0, x_1) = (x_0)^2 - x_1$

works since $a_{n+1} = (a_n)^2$

For $a_n = n!$ observe that

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

Take $k = 2$ and $Z(x_0, x_1, x_2) = x_2 \cdot x_0 - (x_1)^2 - x_1 \cdot x_0$

Cancelling polynomials

Theorem

Polyrec and ratrec sequences admit cancelling polynomials

Cancelling polynomials

Theorem

Polyrec and ratrec sequences admit cancelling polynomials

Theorem

n^n does not admit a cancelling polynomial

Cancelling polynomials

Theorem

Polyrec and ratrec sequences admit cancelling polynomials

Theorem

n^n does not admit a cancelling polynomial

(See part 2 of the talk)

Cancelling polynomials

Theorem

Polyrec and ratrec sequences admit cancelling polynomials

Theorem

n^n does not admit a cancelling polynomial

(See part 2 of the talk)

This is not unique, consider $k = 0$ and $(x_0)^2 - 1$

Cancelling polynomial of any (not polyrec even) sequence over $\{-1, 1\}$

Cancelling polynomials

Theorem

Polyrec and ratrec sequences admit cancelling polynomials

Theorem

n^n does not admit a cancelling polynomial

(See part 2 of the talk)

This is not unique, consider $k = 0$ and $(x_0)^2 - 1$

Cancelling polynomial of any (not polyrec even) sequence over $\{-1, 1\}$

Corollary: polyrec and ratrec do not contain MSO sequences

A polyrec sequence which is not an MSO sequence

Well, we don't know.

A polyrec sequence which is not an MSO sequence

Well, we don't know.

Conjecture

$a_n = F_{F_n}$ is not an MSO sequence, where F_n is Fibonacci

A polyrec sequence which is not an MSO sequence

Well, we don't know.

Conjecture

$a_n = F_{F_n}$ is not an MSO sequence, where F_n is Fibonacci

(nested Fibonacci, double exponential growth)

A polyrec sequence which is not an MSO sequence

Well, we don't know.

Conjecture

$a_n = F_{F_n}$ is not an MSO sequence, where F_n is Fibonacci

(nested Fibonacci, double exponential growth)

Nothing convincing to support the conjecture

A polyrec sequence which is not an MSO sequence

Well, we don’t know.

Conjecture

$a_n = F_{F_n}$ is not an MSO sequence, where F_n is Fibonacci

(nested Fibonacci, double exponential growth)

Nothing convincing to support the conjecture

Maybe that double exponential comes from $\prod_X$

Composing LRS over $\mathbb{N}$

Theorem (Sénizergues)

If a_n, b_n are LRS $\mathbb{N} \to \mathbb{N}$ then $c_n = a_{b_n}$ is polyrec

Composing LRS over $\mathbb{N}$

Theorem (Sénizergues)

If a_n, b_n are LRS $\mathbb{N} \to \mathbb{N}$ then $c_n = a_{b_n}$ is polyrec

In particular F_{F_n} is polyrec

Composing LRS over $\mathbb{N}$

Theorem (Sénizergues)

If a_n, b_n are LRS $\mathbb{N} \to \mathbb{N}$ then $c_n = a_{b_n}$ is polyrec

In particular F_{F_n} is polyrec

Recall that $F_{n+2} = F_{n+1} + F_n$ and $F_n = \begin{pmatrix} 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^n \begin{pmatrix} 1 \\ 0 \end{pmatrix}$

Composing LRS over $\mathbb{N}$

Theorem (Sénizergues)

If a_n, b_n are LRS $\mathbb{N} \to \mathbb{N}$ then $c_n = a_{b_n}$ is polyrec

In particular F_{F_n} is polyrec

Recall that $F_{n+2} = F_{n+1} + F_n$ and $F_n = \begin{pmatrix} 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^n \begin{pmatrix} 1 \\ 0 \end{pmatrix}$

$$F_{F_n} = \begin{pmatrix} 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^{F_n} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^{F_{n-1}} \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^{F_{n-2}} \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

Composing LRS over $\mathbb{N}$

Theorem (Sénizergues)

If a_n, b_n are LRS $\mathbb{N} \to \mathbb{N}$ then $c_n = a_{b_n}$ is polyrec

In particular F_{F_n} is polyrec

Recall that $F_{n+2} = F_{n+1} + F_n$ and $F_n = \begin{pmatrix} 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^n \begin{pmatrix} 1 \\ 0 \end{pmatrix}$

$$F_{F_n} = \begin{pmatrix} 0 & 1 \end{pmatrix} \underbrace{\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^{F_n}} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \end{pmatrix} \underbrace{\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^{F_{n-1}} \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^{F_{n-2}}} \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

To express this we use 8 sequences

a_n, b_n, c_n, d_n (Fibonacci), x_n, y_n, z_n, w_n (previous Fibonacci)

Composing LRS over $\mathbb{N}$

$$\begin{pmatrix} a_{n+1} & b_{n+1} \\ c_{n+1} & d_{n+1} \end{pmatrix} = \begin{pmatrix} a_n & b_n \\ c_n & d_n \end{pmatrix} \begin{pmatrix} x_n & y_n \\ z_n & w_n \end{pmatrix}$$

Composing LRS over $\mathbb{N}$

$$\begin{pmatrix} a_{n+1} & b_{n+1} \\ c_{n+1} & d_{n+1} \end{pmatrix} = \begin{pmatrix} a_n & b_n \\ c_n & d_n \end{pmatrix} \begin{pmatrix} x_n & y_n \\ z_n & w_n \end{pmatrix}$$

For example $a_{n+1} = a_n \cdot x_n + b_n \cdot z_n$

Composing LRS over $\mathbb{N}$

$$\begin{pmatrix} a_{n+1} & b_{n+1} \\ c_{n+1} & d_{n+1} \end{pmatrix} = \begin{pmatrix} a_n & b_n \\ c_n & d_n \end{pmatrix} \begin{pmatrix} x_n & y_n \\ z_n & w_n \end{pmatrix}$$

For example $a_{n+1} = a_n \cdot x_n + b_n \cdot z_n$

$$\begin{pmatrix} x_{n+1} & y_{n+1} \\ z_{n+1} & w_{n+1} \end{pmatrix} = \begin{pmatrix} a_n & b_n \\ c_n & d_n \end{pmatrix}$$

Composing LRS over $\mathbb{N}$

$$\begin{pmatrix} a_{n+1} & b_{n+1} \\ c_{n+1} & d_{n+1} \end{pmatrix} = \begin{pmatrix} a_n & b_n \\ c_n & d_n \end{pmatrix} \begin{pmatrix} x_n & y_n \\ z_n & w_n \end{pmatrix}$$

For example $a_{n+1} = a_n \cdot x_n + b_n \cdot z_n$

$$\begin{pmatrix} x_{n+1} & y_{n+1} \\ z_{n+1} & w_{n+1} \end{pmatrix} = \begin{pmatrix} a_n & b_n \\ c_n & d_n \end{pmatrix}$$

It so happens that $F_{F_n} = c_n$

Composing LRS over $\mathbb{N}$

$$\begin{pmatrix} a_{n+1} & b_{n+1} \\ c_{n+1} & d_{n+1} \end{pmatrix} = \begin{pmatrix} a_n & b_n \\ c_n & d_n \end{pmatrix} \begin{pmatrix} x_n & y_n \\ z_n & w_n \end{pmatrix}$$

For example $a_{n+1} = a_n \cdot x_n + b_n \cdot z_n$

$$\begin{pmatrix} x_{n+1} & y_{n+1} \\ z_{n+1} & w_{n+1} \end{pmatrix} = \begin{pmatrix} a_n & b_n \\ c_n & d_n \end{pmatrix}$$

It so happens that $F_{F_n} = c_n$

Note that we can compose only once (asymptotics)

Two definitions of sequences

For LRS

1. $a_{n+k} = \sum_{i=0}^{k-1} \alpha_i a_{n+i}$ (one sequence)

Two definitions of sequences

For LRS

1. $a_{n+k} = \sum_{i=0}^{k-1} \alpha_i a_{n+i}$ (one sequence)

2. $a_n = I^\top M^n F$ (system of sequences)

Two definitions of sequences

For LRS

1. $a_{n+k} = \sum_{i=0}^{k-1} \alpha_i a_{n+i}$ (one sequence)

2. $a_n = I^\top M^n F$ (system of sequences)

Of course a system can remember previous k values

Two definitions of sequences

For LRS

1. $a_{n+k} = \sum_{i=0}^{k-1} \alpha_i a_{n+i}$ (one sequence)

2. $a_n = I^\top M^n F$ (system of sequences)

Of course a system can remember previous k values

Conversely see part 2

One sequence definition for polyrec?

$a_{n+k} = P(a_n, a_{n+1}, \ldots, a_{n+k-1})$ for some $P \in \mathbb{Q}[x_0, \ldots, x_{k-1}]$

One sequence definition for polyrec?

$a_{n+k} = P(a_n, a_{n+1}, \ldots, a_{n+k-1})$ for some $P \in \mathbb{Q}[x_0, \ldots, x_{k-1}]$

Cancelling polynomial is almost this

but doesn't have to be linear in a_{n+k}

One sequence definition for polyrec?

$a_{n+k} = P(a_n, a_{n+1}, \ldots, a_{n+k-1})$ for some $P \in \mathbb{Q}[x_0, \ldots, x_{k-1}]$

Cancelling polynomial is almost this

but doesn't have to be linear in a_{n+k}

For $n!$ it was $a_{n+2} \cdot a_n - (a_{n+1})^2 - a_{n+1} \cdot a_n = 0$.

One sequence definition for polyrec?

$a_{n+k} = P(a_n, a_{n+1}, \ldots, a_{n+k-1})$ for some $P \in \mathbb{Q}[x_0, \ldots, x_{k-1}]$

Cancelling polynomial is almost this

but doesn't have to be linear in a_{n+k}

For $n!$ it was $a_{n+2} \cdot a_n - (a_{n+1})^2 - a_{n+1} \cdot a_n = 0$.

Proposition

One sequence polyrec definition is not possible for $a_n = n!$.

One sequence definition for polyrec?

$a_{n+k} = P(a_n, a_{n+1}, \ldots, a_{n+k-1})$ for some $P \in \mathbb{Q}[x_0, \ldots, x_{k-1}]$

Cancelling polynomial is almost this

but doesn't have to be linear in a_{n+k}

For $n!$ it was $a_{n+2} \cdot a_n - (a_{n+1})^2 - a_{n+1} \cdot a_n = 0$.

Proposition

One sequence polyrec definition is not possible for $a_n = n!$.

Asymptotic reasons (next slide)

$n!$ not definable by one polynomial

Suppose $a_{n+k} = P(a_n, a_{n+1}, \ldots, a_{n+k-1})$

$n!$ not definable by one polynomial

Suppose $a_{n+k} = P(a_n, a_{n+1}, \dots, a_{n+k-1})$

$P = Q + A$, where A is the sum of all monomials of degree at most 1

$n!$ not definable by one polynomial

Suppose $a_{n+k} = P(a_n, a_{n+1}, \ldots, a_{n+k-1})$

$P = Q + A$, where A is the sum of all monomials of degree at most 1

Observation: $|A(a_n, a_{n+1}, \ldots, a_{n+k-1})| < c \cdot (n+k-1)! < (n+k)!$

$n!$ not definable by one polynomial

Suppose $a_{n+k} = P(a_n, a_{n+1}, \dots, a_{n+k-1})$

$P = Q + A$, where A is the sum of all monomials of degree at most 1

Observation: $|A(a_n, a_{n+1}, \dots, a_{n+k-1})| < c \cdot (n+k-1)! < (n+k)!$

This is almost true $(n!)^2 \mid Q(a_n, a_{n+1}, \dots, a_{n+k-1})$

$n!$ not definable by one polynomial

Suppose $a_{n+k} = P(a_n, a_{n+1}, \ldots, a_{n+k-1})$

$P = Q + A$, where A is the sum of all monomials of degree at most 1

Observation: $|A(a_n, a_{n+1}, \ldots, a_{n+k-1})| < c \cdot (n+k-1)! < (n+k)!$

This is almost true $(n!)^2 \mid Q(a_n, a_{n+1}, \ldots, a_{n+k-1})$

But $(n!)^2$ is too big to divide $(n+k)! - A(a_n, a_{n+1}, \ldots, a_{n+k-1})$

$n!$ not definable by one polynomial

Suppose $a_{n+k} = P(a_n, a_{n+1}, \ldots, a_{n+k-1})$

$P = Q + A$, where A is the sum of all monomials of degree at most 1

Observation: $|A(a_n, a_{n+1}, \ldots, a_{n+k-1})| < c \cdot (n+k-1)! < (n+k)!$

This is almost true $(n!)^2 \mid Q(a_n, a_{n+1}, \ldots, a_{n+k-1})$

But $(n!)^2$ is too big to divide $(n+k)! - A(a_n, a_{n+1}, \ldots, a_{n+k-1})$

Thus $Q = 0$ (contradiction)

What about ratrec definable by one polynomial?

$a_{n+k} = R(a_n, a_{n+1}, \ldots, a_{n+k-1})$ for some $R \in \mathbb{Q}(x_0, \ldots, x_{k-1})$

What about ratrec definable by one polynomial?

$a_{n+k} = R(a_n, a_{n+1}, \ldots, a_{n+k-1})$ for some $R \in \mathbb{Q}(x_0, \ldots, x_{k-1})$

For $n!$ we have $a_{n+2} = \frac{(a_{n+1})^2}{a_n} + a_{n+1}$

What about ratrec definable by one polynomial?

$a_{n+k} = R(a_n, a_{n+1}, \ldots, a_{n+k-1})$ for some $R \in \mathbb{Q}(x_0, \ldots, x_{k-1})$

For $n!$ we have $a_{n+2} = \frac{(a_{n+1})^2}{a_n} + a_{n+1}$

For Catalan numbers we have $C_{n+2} = \frac{2C_{n+1}(C_{n+1}+8C_n)}{10C_n - C_{n+1}}$

What about ratrec definable by one polynomial?

$a_{n+k} = R(a_n, a_{n+1}, \ldots, a_{n+k-1})$ for some $R \in \mathbb{Q}(x_0, \ldots, x_{k-1})$

For $n!$ we have $a_{n+2} = \frac{(a_{n+1})^2}{a_n} + a_{n+1}$

For Catalan numbers we have $C_{n+2} = \frac{2C_{n+1}(C_{n+1}+8C_n)}{10C_n - C_{n+1}}$

Conjecture

ratrec can be defined with one sequence

What about ratrec definable by one polynomial?

$a_{n+k} = R(a_n, a_{n+1}, \ldots, a_{n+k-1})$ for some $R \in \mathbb{Q}(x_0, \ldots, x_{k-1})$

For $n!$ we have $a_{n+2} = \frac{(a_{n+1})^2}{a_n} + a_{n+1}$

For Catalan numbers we have $C_{n+2} = \frac{2C_{n+1}(C_{n+1}+8C_n)}{10C_n - C_{n+1}}$

Conjecture

ratrec can be defined with one sequence

Theorem (Tabuguia and Worrell 2024)

This is true for holonomic sequences

Problematic sequence

Given a ratrec defined with d sequences

One would conjecture that the recursion depth is $k = f(d)$

$a_{n+k} = R(a_n, a_{n+1}, \ldots, a_{n+k-1})$

Problematic sequence

Given a ratrec defined with d sequences

One would conjecture that the recursion depth is $k = f(d)$

$a_{n+k} = R(a_n, a_{n+1}, \ldots, a_{n+k-1})$

Let $P_m(x) = x(x-1)\ldots(x-m)$ for $m \in \mathbb{N}$

$u_n = P_m(n)$

Problematic sequence

Given a ratrec defined with d sequences

One would conjecture that the recursion depth is $k = f(d)$

$a_{n+k} = R(a_n, a_{n+1}, \ldots, a_{n+k-1})$

Let $P_m(x) = x(x-1)\ldots(x-m)$ for $m \in \mathbb{N}$

$u_n = P_m(n)$

Can be defined as a system of $d = 2$ sequences (using $b_n = n$)

Problematic sequence

Given a ratrec defined with d sequences

One would conjecture that the recursion depth is $k = f(d)$

$a_{n+k} = R(a_n, a_{n+1}, \dots, a_{n+k-1})$

Let $P_m(x) = x(x-1)\dots(x-m)$ for $m \in \mathbb{N}$

$u_n = P_m(n)$

Can be defined as a system of $d = 2$ sequences (using $b_n = n$)

In general if $a_0, a_1, \dots, a_{k-1}, a_k = 0$ then $a_n = 0 \quad$ (for all n)

Problematic sequence

Given a ratrec defined with d sequences

One would conjecture that the recursion depth is $k = f(d)$

$a_{n+k} = R(a_n, a_{n+1}, \ldots, a_{n+k-1})$

Let $P_m(x) = x(x-1)\ldots(x-m)$ for $m \in \mathbb{N}$

$u_n = P_m(n)$

Can be defined as a system of $d = 2$ sequences (using $b_n = n$)

In general if $a_0, a_1, \ldots, a_{k-1}, a_k = 0$ then $a_n = 0 \quad$ (for all n)

But the first nonzero element of u_n depends on m (independent of $d = 2$)

Possible application

Checking if ratrec is well-defined is Skolem hard

Possible application

Checking if ratrec is well-defined is Skolem hard

But the conjecture could be applied to polyrec

Possible application

Checking if ratrec is well-defined is Skolem hard

But the conjecture could be applied to polyrec

If $k = f(?)$ is “small” this gives an efficient algorithm for zeroness

Possible application

Checking if ratrec is well-defined is Skolem hard

But the conjecture could be applied to polyrec

If $k = f(?)$ is "small" this gives an efficient algorithm for zeroness

Currently we know PSPACE-hardness and Ackermann upper bound.

Conclusion

- polyrec is interesting

Conclusion

- polyrec is interesting
- ratrec is interesting

Conclusion

- polyrec is interesting
- ratrec is interesting
- Are MSO sequences interesting?

Cancelling polynomial for polyrec and ratrec

Recall LRS $a_n = I^{\top} M^n F$ (system of sequences)

Goal: $a_{n+k} = \sum_{i=0}^{k-1} \alpha_i a_{n+i}$

Cancelling polynomial for polyrec and ratrec

Recall LRS $a_n = I^\top M^n F$ (system of sequences)

Goal: $a_{n+k} = \sum_{i=0}^{k-1} \alpha_i a_{n+i}$

Consider $R : \mathbb{Q}^k \to \mathbb{Q}^{k+1}$

$R(\vec{x}) = (I^\top M^0 \vec{x}, I^\top M^0 \vec{x}, \ldots, I^\top M^k \vec{x})$

Cancelling polynomial for polyrec and ratrec

Recall LRS $a_n = I^\top M^n F$ (system of sequences)

Goal: $a_{n+k} = \sum_{i=0}^{k-1} \alpha_i a_{n+i}$

Consider $R : \mathbb{Q}^k \to \mathbb{Q}^{k+1}$

$R(\vec{x}) = (I^\top M^0 \vec{x}, I^\top M^0 \vec{x}, \ldots, I^\top M^k \vec{x})$

Let $\vec{u}_n = M^n F$

$R(\vec{u}_n) = (a_n, a_{n+1}, \ldots, a_{n+k})$

Cancelling polynomial for polyrec and ratrec

Recall LRS $a_n = I^\top M^n F$ (system of sequences)

Goal: $a_{n+k} = \sum_{i=0}^{k-1} \alpha_i a_{n+i}$

Consider $R : \mathbb{Q}^k \to \mathbb{Q}^{k+1}$

$R(\vec{x}) = (I^\top M^0 \vec{x}, I^\top M^0 \vec{x}, \ldots, I^\top M^k \vec{x})$

Let $\vec{u}_n = M^n F$

$R(\vec{u}_n) = (a_n, a_{n+1}, \ldots, a_{n+k})$

So there is nonzero $K : \mathbb{Q}^{n+1} \to \mathbb{Q}$ s.t. $\mathrm{Im}(R) = \ker(K)$
which defines the recursion

Cancelling polynomial for polyrec and ratrec

$$\begin{aligned} a^1_{n+1} &= P_1(a^1_n, \ldots, a^k_n) \\ a^2_{n+1} &= P_2(a^1_n, \ldots, a^k_n) \\ &\vdots \\ a^k_{n+1} &= P_k(a^1_n, \ldots, a^k_n) \end{aligned}$$

Goal nonzero $Z \in \mathbb{Q}[x_0, \ldots, x_k]$ such that $Z(a_n, a_{n+1} \ldots, a_{n+k}) = 0$ for all n

$a_n = a^1_n$

Cancelling polynomial for polyrec and ratrec

$$a^1_{n+1} = P_1(a^1_n, \ldots, a^k_n)$$
$$a^2_{n+1} = P_2(a^1_n, \ldots, a^k_n)$$
$$\vdots$$
$$a^k_{n+1} = P_k(a^1_n, \ldots, a^k_n)$$

Goal nonzero $Z \in \mathbb{Q}[x_0, \ldots, x_k]$ such that $Z(a_n, a_{n+1} \ldots, a_{n+k}) = 0$ for all n

$a_n = a^1_n$

Theorem

In $\mathbb{Q}(x_1, \ldots, x_k)$ every $k+1$ elements are algebraically dependent.

Cancelling polynomial for polyrec and ratrec

$$
\begin{aligned}
a^1_{n+1} &= P_1(a^1_n, \ldots, a^k_n)\\
a^2_{n+1} &= P_2(a^1_n, \ldots, a^k_n)\\
&\vdots\\
a^k_{n+1} &= P_k(a^1_n, \ldots, a^k_n)
\end{aligned}
$$

Goal nonzero $Z \in \mathbb{Q}[x_0, \ldots, x_k]$ such that $Z(a_n, a_{n+1} \ldots, a_{n+k}) = 0$ for all n

$a_n = a^1_n$

Theorem

In $\mathbb{Q}(x_1, \ldots, x_k)$ every $k + 1$ elements are algebraically dependent.

Define $P^t_i \in \mathbb{Q}[x_1, \ldots, x_k]$

$P^0_i(x_1, \ldots, x_k) = x_i, \quad$ and $P^t_i(\vec{x}) = P_i(P^{t-1}_1(\vec{x}), \ldots P^{t-1}_k(\vec{x}))$.

Cancelling polynomial for polyrec and ratrec

Observation: $P_i^t(a_n^1, \ldots, a_n^k) = a_{n+t}^i$

Cancelling polynomial for polyrec and ratrec

Observation: $P_i^t(a_n^1, \ldots, a_n^k) = a_{n+t}^i$

Consider the polynomials $P_1^0, P_1^1, \ldots P_1^k \in \mathbb{Q}[x_1, \ldots, x_k]$

Cancelling polynomial for polyrec and ratrec

Observation: $P_i^t(a_n^1, \ldots, a_n^k) = a_{n+t}^i$

Consider the polynomials $P_1^0, P_1^1, \ldots P_1^k \in \mathbb{Q}[x_1, \ldots, x_k]$

They are algebraically dependent

Cancelling polynomial for polyrec and ratrec

Observation: $P_i^t(a_n^1, \dots, a_n^k) = a_{n+t}^i$

Consider the polynomials $P_1^0, P_1^1, \dots P_1^k \in \mathbb{Q}[x_1, \dots, x_k]$

They are algebraically dependent

So there is $R \in \mathbb{Q}[x_1, \dots, x_k]$, which is the cancelling polynomial for a_n

Cancelling polynomial for polyrec and ratrec

Observation: $P_i^t(a_n^1, \ldots, a_n^k) = a_{n+t}^i$

Consider the polynomials $P_1^0, P_1^1, \ldots P_1^k \in \mathbb{Q}[x_1, \ldots, x_k]$

They are algebraically dependent

So there is $R \in \mathbb{Q}[x_1, \ldots, x_k]$, which is the cancelling polynomial for a_n

Note: we can assume $R \in \mathbb{Z}[x_1, \ldots, x_k]$

No cancelling polynomial for n^n

Lemma

Suppose $0 \neq Z \in \mathbb{Z}[x_0, \ldots, x_k]$. There exists $P_1, \ldots, P_m, Q_1, \ldots, Q_m \in \mathbb{Z}[x]$ s.t. $Z(n^n, (n+1)^{n+1}, \ldots, (n+k)^{n+k}) = \sum_{i=1}^{m} P_i(n)^n \cdot Q_i(n)$ for all n.

No cancelling polynomial for n^n

Lemma

Suppose $0 \neq Z \in \mathbb{Z}[x_0, \ldots, x_k]$. There exists $P_1, \ldots, P_m, Q_1, \ldots, Q_m \in \mathbb{Z}[x]$ s.t. $Z(n^n, (n+1)^{n+1}, \ldots, (n+k)^{n+k}) = \sum_{i=1}^{m} P_i(n)^n \cdot Q_i(n)$ for all n.

Important: all polynomials are nonzero, and P_i are pairwise different.

No cancelling polynomial for n^n

Lemma

Suppose $0 \neq Z \in \mathbb{Z}[x_0, \dots, x_k]$. There exists $P_1, \dots, P_m, Q_1, \dots, Q_m \in \mathbb{Z}[x]$ s.t. $Z(n^n, (n+1)^{n+1}, \dots, (n+k)^{n+k}) = \sum_{i=1}^{m} P_i(n)^n \cdot Q_i(n)$ for all n.

Important: all polynomials are nonzero, and P_i are pairwise different.

Proof: take a monomial $M(x_0, \dots, x_k) = c \cdot \prod_{j=0}^{k} x_j^{d_j}$

No cancelling polynomial for n^n

Lemma

Suppose $0 \neq Z \in \mathbb{Z}[x_0, \dots, x_k]$. There exists $P_1, \dots, P_m, Q_1, \dots, Q_m \in \mathbb{Z}[x]$ s.t. $Z(n^n, (n+1)^{n+1}, \dots, (n+k)^{n+k}) = \sum_{i=1}^{m} P_i(n)^n \cdot Q_i(n)$ for all n.

Important: all polynomials are nonzero, and P_i are pairwise different.

Proof: take a monomial $M(x_0, \dots, x_k) = c \cdot \prod_{j=0}^{k} x_j^{d_j}$

$$M(n^n, \dots, (n+k)^{n+k}) = c \cdot \prod_{j=0}^{k} (n+j)^{d_j(n+j)}$$

No cancelling polynomial for n^n

Lemma

Suppose $0 \neq Z \in \mathbb{Z}[x_0, \ldots, x_k]$. There exists $P_1, \ldots, P_m, Q_1, \ldots, Q_m \in \mathbb{Z}[x]$ s.t. $Z(n^n, (n+1)^{n+1}, \ldots, (n+k)^{n+k}) = \sum_{i=1}^{m} P_i(n)^n \cdot Q_i(n)$ for all n.

Important: all polynomials are nonzero, and P_i are pairwise different.

Proof: take a monomial $M(x_0, \ldots, x_k) = c \cdot \prod_{j=0}^{k} x_j^{d_j}$

$$M(n^n, \ldots, (n+k)^{n+k}) = c \cdot \prod_{j=0}^{k} (n+j)^{d_j(n+j)}$$

Take $P_i = \prod_{j=0}^{k} (x+j)^{d_j}$

No cancelling polynomial for n^n

Suppose $\sum_{i=1}^{m} P_i(n)^n \cdot Q_i(n) = 0$ for all n

No cancelling polynomial for n^n

Suppose $\sum_{i=1}^{m} P_i(n)^n \cdot Q_i(n) = 0$ for all n

- Idea: $P_i(n)^n$ make them independent

No cancelling polynomial for n^n

Suppose $\sum_{i=1}^{m} P_i(n)^n \cdot Q_i(n) = 0$ for all n

- Idea: $P_i(n)^n$ make them independent

Lemma

For every prime p, and $a, b \in \mathbb{Z}$ s.t. $b > 0$
$$\sum_{i=1}^{m} P_i(a)^b \cdot Q_i(a) \equiv 0 \mod p$$

No cancelling polynomial for n^n

Suppose $\sum_{i=1}^{m} P_i(n)^n \cdot Q_i(n) = 0$ for all n

- Idea: $P_i(n)^n$ make them independent

Lemma

For every prime p, and $a, b \in \mathbb{Z}$ s.t. $b > 0$

$$\sum_{i=1}^{m} P_i(a)^b \cdot Q_i(a) \equiv 0 \mod p$$

Take $n > b$ s.t. $n \equiv a \mod p$ and $n \equiv b \mod p - 1$.

No cancelling polynomial for n^n

Suppose $\sum_{i=1}^{m} P_i(n)^n \cdot Q_i(n) = 0$ for all n

- Idea: $P_i(n)^n$ make them independent

Lemma

For every prime p, and $a, b \in \mathbb{Z}$ s.t. $b > 0$

$$\sum_{i=1}^{m} P_i(a)^b \cdot Q_i(a) \equiv 0 \mod p$$

Take $n > b$ s.t. $n \equiv a \mod p$ and $n \equiv b \mod p-1$.

Observe $Q_i(n) \equiv Q_i(a) \mod p$, and $P_i(n)^n \equiv P_i(a)^b \mod p$

No cancelling polynomial for n^n

$\vec{u}_a = (Q_1(a), \ldots, Q_m(a))$

$$D_a = \begin{pmatrix} P_1(a) & P_1(a)^2 & \ldots & P_1(a)^m \\ P_2(a) & P_2(a)^2 & \ldots & P_2(a)^m \\ & & \vdots & \\ P_m(a) & P_m(a)^2 & \ldots & P_m(a)^m \end{pmatrix}$$

No cancelling polynomial for n^n

$\vec{u}_a = (Q_1(a), \ldots, Q_m(a))$

$$D_a = \begin{pmatrix} P_1(a) & P_1(a)^2 & \ldots & P_1(a)^m \\ P_2(a) & P_2(a)^2 & \ldots & P_2(a)^m \\ & \vdots & & \\ P_m(a) & P_m(a)^2 & \ldots & P_m(a)^m \end{pmatrix}$$

Then $\vec{u}_a \cdot D_a \equiv \vec{0} \mod p$, (for all primes p)

No cancelling polynomial for n^n

$$\vec{u}_a = (Q_1(a), \ldots, Q_m(a))$$

$$D_a = \begin{pmatrix} P_1(a) & P_1(a)^2 & \ldots & P_1(a)^m \\ P_2(a) & P_2(a)^2 & \ldots & P_2(a)^m \\ & \vdots & & \\ P_m(a) & P_m(a)^2 & \ldots & P_m(a)^m \end{pmatrix}$$

Then $\vec{u}_a \cdot D_a \equiv \vec{0} \mod p, \quad$ (for all primes p)

Lemma

There is $\hat{D}_a$ such that $D_a \hat{D}_a = \det(D_a) I$

No cancelling polynomial for n^n

$\vec{u}_a = (Q_1(a), \ldots, Q_m(a))$

$$D_a = \begin{pmatrix} P_1(a) & P_1(a)^2 & \ldots & P_1(a)^m \\ P_2(a) & P_2(a)^2 & \ldots & P_2(a)^m \\ & \vdots & & \\ P_m(a) & P_m(a)^2 & \ldots & P_m(a)^m \end{pmatrix}$$

Then $\vec{u}_a \cdot D_a \equiv \vec{0} \mod p, \quad$ (for all primes p)

Lemma

There is $\hat{D}_a$ such that $D_a \hat{D}_a = \det(D_a) I$

So $\vec{u}_a \cdot \det(D_a) \equiv 0 \mod p$

(Almost) Vandermonde matrix

Theorem

$$\det(D_a) = \prod_{i=1}^{m} P_i(a) \cdot \prod_{1 \leq i < j \leq m} (P_i(a) - P_j(a))$$

(Almost) Vandermonde matrix

Theorem

$$\det(D_a) = \prod_{i=1}^{m} P_i(a) \cdot \prod_{1 \le i < j \le m} (P_i(a) - P_j(a))$$

If P_i are pairwise different then

$$S(x) = \prod_{i=1}^{m} P_i(x) \cdot \prod_{1 \le i < j \le m} (P_i(x) - P_j(x)) \text{ is nonzero}$$

(Almost) Vandermonde matrix

Theorem

$$\det(D_a) = \prod_{i=1}^{m} P_i(a) \cdot \prod_{1 \le i < j \le m} (P_i(a) - P_j(a))$$

If P_i are pairwise different then

$$S(x) = \prod_{i=1}^{m} P_i(x) \cdot \prod_{1 \le i < j \le m} (P_i(x) - P_j(x)) \text{ is nonzero}$$

But $S(a) \cdot Q_i(a) \equiv 0 \mod p$ for all $a \in \mathbb{N}$ and $1 \le i \le m$

(Almost) Vandermonde matrix

Theorem

$$\det(D_a) = \prod_{i=1}^{m} P_i(a) \cdot \prod_{1 \leq i < j \leq m} (P_i(a) - P_j(a))$$

If P_i are pairwise different then

$$S(x) = \prod_{i=1}^{m} P_i(x) \cdot \prod_{1 \leq i < j \leq m} (P_i(x) - P_j(x)) \text{ is nonzero}$$

But $S(a) \cdot Q_i(a) \equiv 0 \mod p \quad$ for all $a \in \mathbb{N}$ and $1 \leq i \leq m$

Take big p

and recall that nonzero polynomials have bounded number of zeros