Computer Proofs for Polynomial Identities in Arbitrarily Many Variables

Manuel Kauers

RISC-Linz, Austria

Motivation

- For every $n \in \mathbb{N}$, we have

$$\Bigl(\sum_{k=1}^{n} x_k\Bigr)^3 = \sum_{i=1}^{n} x_i^3 + 3\sum_{i=1}^{n}\sum_{j=1}^{i-1}(x_i^2 x_j + x_i x_j^2) + 6\sum_{i=1}^{n}\sum_{j=1}^{i-1}\sum_{k=1}^{j-1} x_i x_j x_k$$

Motivation

- For every $n \in \mathbb{N}$, we have

$$\Big(\sum_{k=1}^{n} x_k\Big)^3 = \sum_{i=1}^{n} x_i^3 + 3\sum_{i=1}^{n}\sum_{j=1}^{i-1}(x_i^2 x_j + x_i x_j^2) + 6\sum_{i=1}^{n}\sum_{j=1}^{i-1}\sum_{k=1}^{j-1} x_i x_j x_k$$

- For every given $n \in \mathbb{N}$, lhs and rhs are polynomials in n variables.

Motivation

- For every $n \in \mathbb{N}$, we have

$$\Bigl(\sum_{k=1}^{n} x_k\Bigr)^3 = \sum_{i=1}^{n} x_i^3 + 3\sum_{i=1}^{n}\sum_{j=1}^{i-1}(x_i^2 x_j + x_i x_j^2) + 6\sum_{i=1}^{n}\sum_{j=1}^{i-1}\sum_{k=1}^{j-1} x_i x_j x_k$$

- For every given $n \in \mathbb{N}$, lhs and rhs are polynomials in n variables.
- Equality can be checked easily in this case.

Motivation

- For every $n \in \mathbb{N}$, we have

$$\Bigl(\sum_{k=1}^{n} x_k\Bigr)^3 = \sum_{i=1}^{n} x_i^3 + 3\sum_{i=1}^{n}\sum_{j=1}^{i-1}(x_i^2 x_j + x_i x_j^2) + 6\sum_{i=1}^{n}\sum_{j=1}^{i-1}\sum_{k=1}^{j-1} x_i x_j x_k$$

- For every given $n \in \mathbb{N}$, lhs and rhs are polynomials in n variables.
- Equality can be checked easily in this case.
- But how to prove the identity for *general* n?

Motivation

- For every $n \in \mathbb{N}$, we have

$$\Bigl(\sum_{k=1}^{n} x_k\Bigr)^3 = \sum_{i=1}^{n} x_i^3 + 3\sum_{i=1}^{n}\sum_{j=1}^{i-1}(x_i^2 x_j + x_i x_j^2) + 6\sum_{i=1}^{n}\sum_{j=1}^{i-1}\sum_{k=1}^{j-1} x_i x_j x_k$$

- For every given $n \in \mathbb{N}$, lhs and rhs are polynomials in n variables.
- Equality can be checked easily in this case.
- But how to prove the identity for *general* n?
- Can this been done algorithmically?

Overview

Admissible univariate sequences

Zero equivalence test for admissible sequences

Extension to arbitrarily many variables

Admissible univariate sequences

Nested Polynomial Recurrences

- A sequence is admissible if it satisfies a *(nested) polynomial recurrence.*
- Example: Definition of a sequence $(f_1(n))_{n=1}^{\infty}$

$$f_1(1), f_1(2), f_1(3)\text{: initial values of } f_1$$

$f_1(1)$	$f_1(2)$	$f_1(3)$	$f_1(4)$	$f_1(5)$	$f_1(6)$	$f_1(7)$
$f_2(1)$	$f_2(2)$	$f_2(3)$	$f_2(4)$	$f_2(5)$	$f_2(6)$	$f_2(7)$
$f_3(1)$	$f_3(2)$	$f_3(3)$	$f_3(4)$	$f_3(5)$	$f_3(6)$	$f_3(7)$

Nested Polynomial Recurrences

- A sequence is admissible if it satisfies a *(nested) polynomial recurrence.*
- Example: Definition of a sequence $(f_1(n))_{n=1}^{\infty}$

$$f_1(4) = p(f_1(1), f_1(2), f_1(3))$$
$$p = \text{poly or } p = 1/\text{poly} \quad \text{fixed}$$

$f_1(1)$	$f_1(2)$	$f_1(3)$	$f_1(4)$	$f_1(5)$	$f_1(6)$	$f_1(7)$
$f_2(1)$	$f_2(2)$	$f_2(3)$	$f_2(4)$	$f_2(5)$	$f_2(6)$	$f_2(7)$
$f_3(1)$	$f_3(2)$	$f_3(3)$	$f_3(4)$	$f_3(5)$	$f_3(6)$	$f_3(7)$

Nested Polynomial Recurrences

- A sequence is admissible if it satisfies a *(nested) polynomial recurrence.*
- Example: Definition of a sequence $(f_1(n))_{n=1}^{\infty}$

$$f_1(5) = p(f_1(2), f_1(3), f_1(4))$$
$$p = \text{poly or } p = 1/\text{poly} \quad \text{fixed}$$

$f_1(1)$	$f_1(2)$	$f_1(3)$	$f_1(4)$	$f_1(5)$	$f_1(6)$	$f_1(7)$
$f_2(1)$	$f_2(2)$	$f_2(3)$	$f_2(4)$	$f_2(5)$	$f_2(6)$	$f_2(7)$
$f_3(1)$	$f_3(2)$	$f_3(3)$	$f_3(4)$	$f_3(5)$	$f_3(6)$	$f_3(7)$

Nested Polynomial Recurrences

- A sequence is admissible if it satisfies a *(nested) polynomial recurrence.*
- Example: Definition of a sequence $(f_1(n))_{n=1}^{\infty}$

$$f_1(6) = p(f_1(3), f_1(4), f_1(5))$$
$$p = \text{poly or } p = 1/\text{poly} \quad \text{fixed}$$

$f_1(1)$	$f_1(2)$	$f_1(3)$	$f_1(4)$	$f_1(5)$	$f_1(6)$	$f_1(7)$
$f_2(1)$	$f_2(2)$	$f_2(3)$	$f_2(4)$	$f_2(5)$	$f_2(6)$	$f_2(7)$
$f_3(1)$	$f_3(2)$	$f_3(3)$	$f_3(4)$	$f_3(5)$	$f_3(6)$	$f_3(7)$

Nested Polynomial Recurrences

- A sequence is admissible if it satisfies a *(nested) polynomial recurrence.*
- Example: Definition of a sequence $(f_1(n))_{n=1}^{\infty}$

$$f_1(7) = p(f_1(4), f_1(5), f_1(6))$$
$$p = \text{poly or } p = 1/\text{poly} \quad \text{fixed}$$

$f_1(1)$	$f_1(2)$	$f_1(3)$	$f_1(4)$	$f_1(5)$	$f_1(6)$	$f_1(7)$
$f_2(1)$	$f_2(2)$	$f_2(3)$	$f_2(4)$	$f_2(5)$	$f_2(6)$	$f_2(7)$
$f_3(1)$	$f_3(2)$	$f_3(3)$	$f_3(4)$	$f_3(5)$	$f_3(6)$	$f_3(7)$

Nested Polynomial Recurrences

- A sequence is admissible if it satisfies a *(nested) polynomial recurrence.*
- Example: Definition of a sequence $(f_2(n))_{n=1}^{\infty}$

$f_2(1), f_2(2)$: initial values of f_2

$f_1(1)$	$f_1(2)$	$f_1(3)$	$f_1(4)$	$f_1(5)$	$f_1(6)$	$f_1(7)$
$f_2(1)$	$f_2(2)$	$f_2(3)$	$f_2(4)$	$f_2(5)$	$f_2(6)$	$f_2(7)$
$f_3(1)$	$f_3(2)$	$f_3(3)$	$f_3(4)$	$f_3(5)$	$f_3(6)$	$f_3(7)$

Nested Polynomial Recurrences

- A sequence is admissible if it satisfies a *(nested) polynomial recurrence.*
- Example: Definition of a sequence $(f_2(n))_{n=1}^{\infty}$

$$f_2(3) = q(f_2(1), f_2(2), f_1(1), f_1(2), f_1(3))$$
$$q = \text{poly or } q = 1/\text{poly} \quad \text{fixed}$$

$f_1(1)$	$f_1(2)$	$f_1(3)$	$f_1(4)$	$f_1(5)$	$f_1(6)$	$f_1(7)$
$f_2(1)$	$f_2(2)$	$f_2(3)$	$f_2(4)$	$f_2(5)$	$f_2(6)$	$f_2(7)$
$f_3(1)$	$f_3(2)$	$f_3(3)$	$f_3(4)$	$f_3(5)$	$f_3(6)$	$f_3(7)$

Nested Polynomial Recurrences

- A sequence is admissible if it satisfies a *(nested) polynomial recurrence.*
- Example: Definition of a sequence $(f_2(n))_{n=1}^{\infty}$

$$f_2(4) = q(f_2(2), f_2(3), f_1(2), f_1(3), f_1(4))$$
$$q = \text{poly or } q = 1/\text{poly} \quad \text{fixed}$$

$f_1(1)$	$f_1(2)$	$f_1(3)$	$f_1(4)$	$f_1(5)$	$f_1(6)$	$f_1(7)$
$f_2(1)$	$f_2(2)$	$f_2(3)$	$f_2(4)$	$f_2(5)$	$f_2(6)$	$f_2(7)$
$f_3(1)$	$f_3(2)$	$f_3(3)$	$f_3(4)$	$f_3(5)$	$f_3(6)$	$f_3(7)$

Nested Polynomial Recurrences

- A sequence is admissible if it satisfies a *(nested) polynomial recurrence.*
- Example: Definition of a sequence $(f_2(n))_{n=1}^{\infty}$

$$f_2(5) = q(f_2(3), f_2(4), f_1(3), f_1(4), f_1(5))$$
$$q = \text{poly or } q = 1/\text{poly} \quad \text{fixed}$$

$f_1(1)$	$f_1(2)$	$f_1(3)$	$f_1(4)$	$f_1(5)$	$f_1(6)$	$f_1(7)$
$f_2(1)$	$f_2(2)$	$f_2(3)$	$f_2(4)$	$f_2(5)$	$f_2(6)$	$f_2(7)$
$f_3(1)$	$f_3(2)$	$f_3(3)$	$f_3(4)$	$f_3(5)$	$f_3(6)$	$f_3(7)$

Nested Polynomial Recurrences

- A sequence is admissible if it satisfies a *(nested) polynomial recurrence.*
- Example: Definition of a sequence $(f_2(n))_{n=1}^{\infty}$

$$f_2(6) = q(f_2(4), f_2(5), f_1(4), f_1(5), f_1(6))$$
$$q = \text{poly or } q = 1/\text{poly} \quad \text{fixed}$$

$f_1(1)$	$f_1(2)$	$f_1(3)$	$f_1(4)$	$f_1(5)$	$f_1(6)$	$f_1(7)$
$f_2(1)$	$f_2(2)$	$f_2(3)$	$f_2(4)$	$f_2(5)$	$f_2(6)$	$f_2(7)$
$f_3(1)$	$f_3(2)$	$f_3(3)$	$f_3(4)$	$f_3(5)$	$f_3(6)$	$f_3(7)$

Nested Polynomial Recurrences

- A sequence is admissible if it satisfies a *(nested) polynomial recurrence.*
- Example: Definition of a sequence $(f_2(n))_{n=1}^{\infty}$

$$f_2(7) = q(f_2(5), f_2(6), f_1(5), f_1(6), f_1(7))$$
$$q = \text{poly or } q = 1/\text{poly} \quad \text{fixed}$$

$f_1(1)$	$f_1(2)$	$f_1(3)$	$f_1(4)$	$f_1(5)$	$f_1(6)$	$f_1(7)$
$f_2(1)$	$f_2(2)$	$f_2(3)$	$f_2(4)$	$f_2(5)$	$f_2(6)$	$f_2(7)$
$f_3(1)$	$f_3(2)$	$f_3(3)$	$f_3(4)$	$f_3(5)$	$f_3(6)$	$f_3(7)$

Nested Polynomial Recurrences

- A sequence is admissible if it satisfies a *(nested) polynomial recurrence.*
- Example: Definition of a sequence $(f_3(n))_{n=1}^{\infty}$

$f_3(1), f_3(2), f_3(3), f_3(4)$: initial values of f_3

$f_1(1)$	$f_1(2)$	$f_1(3)$	$f_1(4)$	$f_1(5)$	$f_1(6)$	$f_1(7)$
$f_2(1)$	$f_2(2)$	$f_2(3)$	$f_2(4)$	$f_2(5)$	$f_2(6)$	$f_2(7)$
$f_3(1)$	$f_3(2)$	$f_3(3)$	$f_3(4)$	$f_3(5)$	$f_3(6)$	$f_3(7)$

Nested Polynomial Recurrences

- A sequence is admissible if it satisfies a *(nested) polynomial recurrence.*
- Example: Definition of a sequence $(f_3(n))_{n=1}^{\infty}$

$$f_3(5) = r(f_3(1), \dots, f_3(4), f_2(1), \dots, f_2(5), f_1(1), \dots, f_1(5))$$
$$r = \text{poly or } r = 1/\text{poly} \quad \text{fixed}$$

$f_1(1)$	$f_1(2)$	$f_1(3)$	$f_1(4)$	$f_1(5)$	$f_1(6)$	$f_1(7)$
$f_2(1)$	$f_2(2)$	$f_2(3)$	$f_2(4)$	$f_2(5)$	$f_2(6)$	$f_2(7)$
$f_3(1)$	$f_3(2)$	$f_3(3)$	$f_3(4)$	$f_3(5)$	$f_3(6)$	$f_3(7)$

Nested Polynomial Recurrences

- A sequence is admissible if it satisfies a *(nested) polynomial recurrence.*
- Example: Definition of a sequence $(f_3(n))_{n=1}^{\infty}$

$$f_3(6) = r(f_3(2), \ldots, f_3(5), f_2(2), \ldots, f_2(6), f_1(2), \ldots, f_1(6))$$
$$r = \text{poly or } r = 1/\text{poly} \quad \text{fixed}$$

$f_1(1)$	$f_1(2)$	$f_1(3)$	$f_1(4)$	$f_1(5)$	$f_1(6)$	$f_1(7)$
$f_2(1)$	$f_2(2)$	$f_2(3)$	$f_2(4)$	$f_2(5)$	$f_2(6)$	$f_2(7)$
$f_3(1)$	$f_3(2)$	$f_3(3)$	$f_3(4)$	$f_3(5)$	$f_3(6)$	$f_3(7)$

Nested Polynomial Recurrences

- A sequence is admissible if it satisfies a *(nested) polynomial recurrence.*
- Example: Definition of a sequence $(f_3(n))_{n=1}^{\infty}$

$$f_3(7) = r(f_3(3), \dots, f_3(6), f_2(3), \dots, f_2(7), f_1(3), \dots, f_1(7))$$

$r =$ poly or $r = 1/$poly fixed

$f_1(1)$	$f_1(2)$	$f_1(3)$	$f_1(4)$	$f_1(5)$	$f_1(6)$	$f_1(7)$
$f_2(1)$	$f_2(2)$	$f_2(3)$	$f_2(4)$	$f_2(5)$	$f_2(6)$	$f_2(7)$
$f_3(1)$	$f_3(2)$	$f_3(3)$	$f_3(4)$	$f_3(5)$	$f_3(6)$	$f_3(7)$

Some admissible Sequences

Many sequences are admissible. For instance:

Some admissible Sequences

Many sequences are admissible. For instance:

- holonomic sequences (hypergeometric sequences, orthogonal polynomials, etc.)

Some admissible Sequences

Many sequences are admissible. For instance:

- holonomic sequences (hypergeometric sequences, orthogonal polynomials, etc.)
- sequences like 2^{2^n}

Some admissible Sequences

Many sequences are admissible. For instance:

- holonomic sequences (hypergeometric sequences, orthogonal polynomials, etc.)
- sequences like 2^{2^n}
- rational functions of other admissible sequences

Some admissible Sequences

Many sequences are admissible. For instance:

- holonomic sequences (hypergeometric sequences, orthogonal polynomials, etc.)
- sequences like 2^{2^n}
- rational functions of other admissible sequences
- indefinite sums and products of other admissible sequences

Some admissible Sequences

Many sequences are admissible. For instance:

- holonomic sequences (hypergeometric sequences, orthogonal polynomials, etc.)
- sequences like 2^{2^n}
- rational functions of other admissible sequences
- indefinite sums and products of other admissible sequences
- indefinite continued fractions of other admissible sequences

Zero equivalence test for admissible sequences

Algebraic Representation of admissible Sequences

- Model admissible sequences by *difference algebra* concepts

Algebraic Representation of admissible Sequences

- Model admissible sequences by *difference algebra* concepts
- Example:

$$\begin{array}{cccc}
f_1(n) & f_1(n+1) & f_1(n+2) & \cdots \\
f_2(n) & f_2(n+1) & f_2(n+2) & \cdots \\
f_3(n) & f_3(n+1) & f_3(n+2) & \cdots
\end{array}$$

Algebraic Representation of admissible Sequences

- Model admissible sequences by *difference algebra* concepts
- Example:

$$\begin{array}{cccc} f_1(n) & f_1(n+1) & f_1(n+2) & \cdots \\ f_2(n) & f_2(n+1) & f_2(n+2) & \cdots \\ f_3(n) & f_3(n+1) & f_3(n+2) & \cdots \end{array} \quad \rightsquigarrow \quad \begin{array}{cccc} t_{1,0} & t_{1,1} & t_{1,2} & \cdots \\ t_{2,0} & t_{2,1} & t_{2,2} & \cdots \\ t_{3,0} & t_{3,1} & t_{3,2} & \cdots \end{array}$$

Algebraic Representation of admissible Sequences

- Model admissible sequences by *difference algebra* concepts
- Example:

$$\begin{array}{cccc} \hline f_1(n) & f_1(n+1) & f_1(n+2) & \cdots \\ f_2(n) & f_2(n+1) & f_2(n+2) & \cdots \\ f_3(n) & f_3(n+1) & f_3(n+2) & \cdots \\ \hline \end{array} \quad \rightsquigarrow \quad \begin{array}{cccc} \hline t_{1,0} & t_{1,1} & t_{1,2} & \cdots \\ t_{2,0} & t_{2,1} & t_{2,2} & \cdots \\ t_{3,0} & t_{3,1} & t_{3,2} & \cdots \\ \hline \end{array}$$

- Consider the $t_{i,j}$ as indeterminates of a polynomial ring

Algebraic Representation of admissible Sequences

- Model admissible sequences by *difference algebra* concepts
- Example:

$$\begin{array}{cccc} \hline f_1(n) & f_1(n+1) & f_1(n+2) & \cdots \\ f_2(n) & f_2(n+1) & f_2(n+2) & \cdots \\ f_3(n) & f_3(n+1) & f_3(n+2) & \cdots \\ \hline \end{array} \quad \rightsquigarrow \quad \begin{array}{cccc} \hline t_{1,0} & t_{1,1} & t_{1,2} & \cdots \\ t_{2,0} & t_{2,1} & t_{2,2} & \cdots \\ t_{3,0} & t_{3,1} & t_{3,2} & \cdots \\ \hline \end{array}$$

- Consider the $t_{i,j}$ as indeterminates of a polynomial ring
- The recurrence relations give rise to polynomial relations among these indeterminates.

Proving Zero Equivalence of Admissible Sequences

- *Goal:* Show that $f_3(n) = 0$ for all $n \in \mathbb{N}$

Proving Zero Equivalence of Admissible Sequences

- *Goal:* Show that $f_3(n) = 0$ for all $n \in \mathbb{N}$
- *Idea:* Use ideal arithmetic to construct an induction proof

Proving Zero Equivalence of Admissible Sequences

- *Goal:* Show that $f_3(n) = 0$ for all $n \in \mathbb{N}$
- *Idea:* Use ideal arithmetic to construct an induction proof
- *Observation:* Every $t_{i,j}$ (j high enough) is "connected" with other indeterminates via a polynomial relation

$$\underbrace{t_{i,j} - \text{poly}}_{=:d(t_{i,j})} = 0 \quad \text{or} \quad \underbrace{\text{poly} \cdot t_{i,j} - 1}_{=:d(t_{i,j})} = 0$$

The polynomial $d(t_{i,j})$ is called the *defining relation* of $t_{i,j}$.

Proving Zero Equivalence of Admissible Sequences

- *Goal:* Show that $f_3(n) = 0$ for all $n \in \mathbb{N}$

$t_{1,0}$	$t_{1,1}$	$t_{1,2}$	$d(t_{1,3})$	$d(t_{1,4})$	$t_{1,5}$	$t_{1,6}$
$t_{2,0}$	$t_{2,1}$	$d(t_{2,2})$	$d(t_{2,3})$	$d(t_{2,4})$	$t_{2,5}$	$t_{2,6}$
$t_{3,0}$	$t_{3,1}$	$t_{3,2}$	$t_{3,3}$	$d(t_{3,4})$	$t_{3,5}$	$t_{3,6}$

Proving Zero Equivalence of Admissible Sequences

- *Goal:* Show that $f_3(n) = 0$ for all $n \in \mathbb{N}$

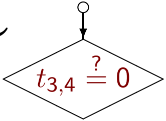
$$\begin{array}{ccccccc}
\hline
t_{1,0} & t_{1,1} & t_{1,2} & d(t_{1,3}) & d(t_{1,4}) & t_{1,5} & t_{1,6} \\
t_{2,0} & t_{2,1} & d(t_{2,2}) & d(t_{2,3}) & d(t_{2,4}) & t_{2,5} & t_{2,6} \\
t_{3,0} & t_{3,1} & t_{3,2} & t_{3,3} & d(t_{3,4}) & t_{3,5} & t_{3,6} \\
\hline
\multicolumn{4}{c}{\underbrace{t_{3,0} \qquad t_{3,1} \qquad t_{3,2} \qquad t_{3,3}}_{\overset{!}{=}0 \text{ by IH}}} & & &
\end{array}$$

Proving Zero Equivalence of Admissible Sequences

- *Goal:* Show that $f_3(n) = 0$ for all $n \in \mathbb{N}$

$t_{1,0}$	$t_{1,1}$	$t_{1,2}$	$d(t_{1,3})$	$d(t_{1,4})$	$t_{1,5}$	$t_{1,6}$
$t_{2,0}$	$t_{2,1}$	$d(t_{2,2})$	$d(t_{2,3})$	$d(t_{2,4})$	$t_{2,5}$	$t_{2,6}$
$t_{3,0}$	$t_{3,1}$	$t_{3,2}$	$t_{3,3}$	$d(t_{3,4})$	$t_{3,5}$	$t_{3,6}$

$$\underbrace{t_{3,0} \qquad t_{3,1} \qquad t_{3,2} \qquad t_{3,3}}_{\overset{!}{=}0 \text{ by IH}}$$



$t_{3,4} \overset{?}{=} 0$

Proving Zero Equivalence of Admissible Sequences

- *Goal:* Show that $f_3(n) = 0$ for all $n \in \mathbb{N}$

$t_{1,0}$	$t_{1,1}$	$t_{1,2}$	$d(t_{1,3})$	$d(t_{1,4})$	$t_{1,5}$	$t_{1,6}$
$t_{2,0}$	$t_{2,1}$	$d(t_{2,2})$	$d(t_{2,3})$	$d(t_{2,4})$	$t_{2,5}$	$t_{2,6}$
$t_{3,0}$	$t_{3,1}$	$t_{3,2}$	$t_{3,3}$	$d(t_{3,4})$	$t_{3,5}$	$t_{3,6}$

$$\underbrace{t_{3,0} \qquad t_{3,1} \qquad t_{3,2} \qquad t_{3,3}}_{\overset{!}{=}0 \text{ by IH}}$$

$$\boxed{t_{3,4} \overset{?}{=} 0}$$

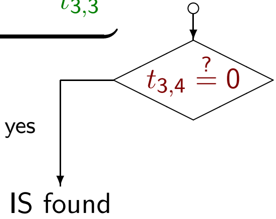
- This can be decided by a radical membership test in $K[t_{1,0}, \ldots, t_{3,4}]$

Proving Zero Equivalence of Admissible Sequences

- *Goal:* Show that $f_3(n) = 0$ for all $n \in \mathbb{N}$

$t_{1,0}$	$t_{1,1}$	$t_{1,2}$	$d(t_{1,3})$	$d(t_{1,4})$	$t_{1,5}$	$t_{1,6}$
$t_{2,0}$	$t_{2,1}$	$d(t_{2,2})$	$d(t_{2,3})$	$d(t_{2,4})$	$t_{2,5}$	$t_{2,6}$
$t_{3,0}$	$t_{3,1}$	$t_{3,2}$	$t_{3,3}$	$d(t_{3,4})$	$t_{3,5}$	$t_{3,6}$

$$\underbrace{t_{3,0} \qquad t_{3,1} \qquad t_{3,2} \qquad t_{3,3}}_{\overset{!}{=} 0 \text{ by IH}}$$

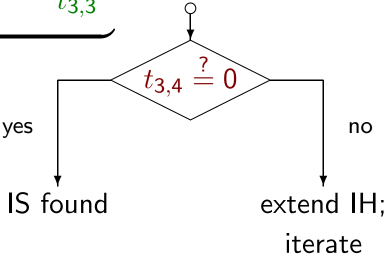


Proving Zero Equivalence of Admissible Sequences

- *Goal:* Show that $f_3(n) = 0$ for all $n \in \mathbb{N}$

$$\begin{array}{ccccccc}
t_{1,0} & t_{1,1} & t_{1,2} & d(t_{1,3}) & d(t_{1,4}) & t_{1,5} & t_{1,6} \\
t_{2,0} & t_{2,1} & d(t_{2,2}) & d(t_{2,3}) & d(t_{2,4}) & t_{2,5} & t_{2,6} \\
t_{3,0} & t_{3,1} & t_{3,2} & t_{3,3} & d(t_{3,4}) & t_{3,5} & t_{3,6} \\
\hline
\end{array}$$

$$\underbrace{t_{3,0} \qquad t_{3,1} \qquad t_{3,2} \qquad t_{3,3}}_{\overset{!}{=} 0 \text{ by IH}}$$



Proving Zero Equivalence of Admissible Sequences

- *Goal:* Show that $f_3(n) = 0$ for all $n \in \mathbb{N}$

$t_{1,0}$	$t_{1,1}$	$t_{1,2}$	$d(t_{1,3})$	$d(t_{1,4})$	$d(t_{1,5})$	$t_{1,6}$
$t_{2,0}$	$t_{2,1}$	$d(t_{2,2})$	$d(t_{2,3})$	$d(t_{2,4})$	$d(t_{2,5})$	$t_{2,6}$
$t_{3,0}$	$t_{3,1}$	$t_{3,2}$	$t_{3,3}$	$d(t_{3,4})$	$d(t_{3,5})$	$t_{3,6}$

$$\underbrace{t_{3,0} \qquad t_{3,1} \qquad t_{3,2} \qquad t_{3,3} \qquad t_{3,4}}_{\overset{!}{=}0 \text{ by IH}}$$

$$t_{3,5} \overset{?}{=} 0$$

Proving Zero Equivalence of Admissible Sequences

- *Goal:* Show that $f_3(n) = 0$ for all $n \in \mathbb{N}$

$$\begin{array}{ccccccc}
\hline
t_{1,0} & t_{1,1} & t_{1,2} & d(t_{1,3}) & d(t_{1,4}) & d(t_{1,5}) & d(t_{1,6})\\
t_{2,0} & t_{2,1} & d(t_{2,2}) & d(t_{2,3}) & d(t_{2,4}) & d(t_{2,5}) & d(t_{2,6})\\
t_{3,0} & t_{3,1} & t_{3,2} & t_{3,3} & d(t_{3,4}) & d(t_{3,5}) & d(t_{3,6})\\
\hline
\end{array}$$

$$\underbrace{t_{3,0} \quad t_{3,1} \quad t_{3,2} \quad t_{3,3} \quad t_{3,4} \quad t_{3,5}}_{\overset{!}{=}0 \text{ by IH}}$$

$$t_{3,6} \overset{?}{=} 0$$

Proving Zero Equivalence of Admissible Sequences

- *Goal:* Show that $f_3(n) = 0$ for all $n \in \mathbb{N}$

$t_{1,0}$	$t_{1,1}$	$t_{1,2}$	$d(t_{1,3})$	$d(t_{1,4})$	$d(t_{1,5})$	$\cdots$
$t_{2,0}$	$t_{2,1}$	$d(t_{2,2})$	$d(t_{2,3})$	$d(t_{2,4})$	$d(t_{2,5})$	$\cdots$
$t_{3,0}$	$t_{3,1}$	$t_{3,2}$	$t_{3,3}$	$d(t_{3,4})$	$d(t_{3,5})$	$\cdots$
$t_{3,0}$	$t_{3,1}$	$t_{3,2}$	$t_{3,3}$	$t_{3,4}$	$t_{3,5}$	$\cdots$

- Finally, check sufficiently many initial values

Proving Zero Equivalence of Admissible Sequences

- *Goal:* Show that $f_3(n) = 0$ for all $n \in \mathbb{N}$

$t_{1,0}$	$t_{1,1}$	$t_{1,2}$	$d(t_{1,3})$	$d(t_{1,4})$	$d(t_{1,5})$	$\cdots$
$t_{2,0}$	$t_{2,1}$	$d(t_{2,2})$	$d(t_{2,3})$	$d(t_{2,4})$	$d(t_{2,5})$	$\cdots$
$t_{3,0}$	$t_{3,1}$	$t_{3,2}$	$t_{3,3}$	$d(t_{3,4})$	$d(t_{3,5})$	$\cdots$
$t_{3,0}$	$t_{3,1}$	$t_{3,2}$	$t_{3,3}$	$t_{3,4}$	$t_{3,5}$	$\cdots$

- Finally, check sufficiently many initial values
- *Correctness:* complete induction on n

Proving Zero Equivalence of Admissible Sequences

- *Goal:* Show that $f_3(n) = 0$ for all $n \in \mathbb{N}$

$$
\begin{array}{ccccccc}
\hline
t_{1,0} & t_{1,1} & t_{1,2} & d(t_{1,3}) & d(t_{1,4}) & d(t_{1,5}) & \cdots \\
t_{2,0} & t_{2,1} & d(t_{2,2}) & d(t_{2,3}) & d(t_{2,4}) & d(t_{2,5}) & \cdots \\
t_{3,0} & t_{3,1} & t_{3,2} & t_{3,3} & d(t_{3,4}) & d(t_{3,5}) & \cdots \\
\hline
t_{3,0} & t_{3,1} & t_{3,2} & t_{3,3} & t_{3,4} & t_{3,5} & \cdots
\end{array}
$$

- Finally, check sufficiently many initial values
- *Correctness:* complete induction on n
- *Termination:* see paper

Extension to arbitrarily many variables

Arbitrarily many Variables

- *Goal:* Handle identities with “arbitrarily many variables”

Arbitrarily many Variables

- *Goal:* Handle identities with "arbitrarily many variables"
- *Requirement:* Find algebraic representation of variable sequences $(x_n)_{n=1}^{\infty}$

Arbitrarily many Variables

- *Goal:* Handle identities with “arbitrarily many variables”
- *Requirement:* Find algebraic representation of variable sequences $(x_n)_{n=1}^{\infty}$
- *Idea:* Represent $f_1(n+i) := x_{n+i}$ by indeterminates $t_{1,i}$ without defining relation

Arbitrarily many Variables

- *Goal:* Handle identities with "arbitrarily many variables"
- *Requirement:* Find algebraic representation of variable sequences $(x_n)_{n=1}^{\infty}$
- *Idea:* Represent $f_1(n+i) := x_{n+i}$ by indeterminates $t_{1,i}$ without defining relation
- *Consequences:*

Arbitrarily many Variables

- *Goal:* Handle identities with “arbitrarily many variables”
- *Requirement:* Find algebraic representation of variable sequences $(x_n)_{n=1}^{\infty}$
- *Idea:* Represent $f_1(n+i) := x_{n+i}$ by indeterminates $t_{1,i}$ without defining relation
- *Consequences:*
  1. Expressions involving x_n can be represented

Arbitrarily many Variables

- *Goal:* Handle identities with "arbitrarily many variables"
- *Requirement:* Find algebraic representation of variable sequences $(x_n)_{n=1}^{\infty}$
- *Idea:* Represent $f_1(n+i) := x_{n+i}$ by indeterminates $t_{1,i}$ without defining relation
- *Consequences:*
  1. Expressions involving x_n can be represented
  2. The same algorithm is still applicable

Arbitrarily many Variables

- *Goal:* Handle identities with "arbitrarily many variables"
- *Requirement:* Find algebraic representation of variable sequences $(x_n)_{n=1}^{\infty}$
- *Idea:* Represent $f_1(n+i) := x_{n+i}$ by indeterminates $t_{1,i}$ without defining relation
- *Consequences:*
  1. Expressions involving x_n can be represented
  2. The same algorithm is still applicable
  3. But it will not terminate in general

Arbitrarily many Variables

- *Goal:* Handle identities with “arbitrarily many variables”
- *Requirement:* Find algebraic representation of variable sequences $(x_n)_{n=1}^{\infty}$
- *Idea:* Represent $f_1(n+i) := x_{n+i}$ by indeterminates $t_{1,i}$ without defining relation
- *Consequences:*
  1. Expressions involving x_n can be represented
  2. The same algorithm is still applicable
  3. But it will not terminate in general
- *Fix:* Put all $t_{i,j}$ without relations into the ground field

Proving Zero Equivalence of Admissible Sequences

- *Goal:* Show that $f_3(n) = 0$ for all $n \in \mathbb{N}$

Proving Zero Equivalence of Admissible Sequences

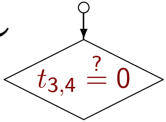
- *Goal:* Show that $f_3(n) = 0$ for all $n \in \mathbb{N}$
- Suppose $f_1(n) = x_n$ is free

Proving Zero Equivalence of Admissible Sequences

- *Goal:* Show that $f_3(n) = 0$ for all $n \in \mathbb{N}$
- Suppose $f_1(n) = x_n$ is free

$t_{1,0}$	$t_{1,1}$	$t_{1,2}$	$t_{1,3}$	$t_{1,4}$	$t_{1,5}$	$\cdots$
$t_{2,0}$	$t_{2,1}$	$d(t_{2,2})$	$d(t_{2,3})$	$d(t_{2,4})$	$t_{2,5}$	$\cdots$
$t_{3,0}$	$t_{3,1}$	$t_{3,2}$	$t_{3,3}$	$d(t_{3,4})$	$t_{3,5}$	$\cdots$

$$\underbrace{t_{3,0} \qquad t_{3,1} \qquad t_{3,2} \qquad t_{3,3}}_{\overset{!}{=} 0 \text{ by IH}}$$



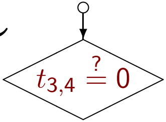
$t_{3,4} \overset{?}{=} 0$

Proving Zero Equivalence of Admissible Sequences

- *Goal:* Show that $f_3(n) = 0$ for all $n \in \mathbb{N}$
- Suppose $f_1(n) = x_n$ is free

$$\begin{array}{ccccccc}
\hline
t_{1,0} & t_{1,1} & t_{1,2} & t_{1,3} & t_{1,4} & t_{1,5} & \cdots \\
t_{2,0} & t_{2,1} & d(t_{2,2}) & d(t_{2,3}) & d(t_{2,4}) & t_{2,5} & \cdots \\
t_{3,0} & t_{3,1} & t_{3,2} & t_{3,3} & d(t_{3,4}) & t_{3,5} & \cdots \\
\hline
\end{array}$$

$$\underbrace{t_{3,0} \qquad t_{3,1} \qquad t_{3,2} \qquad t_{3,3}}_{\overset{!}{=}0 \text{ by IH}}$$

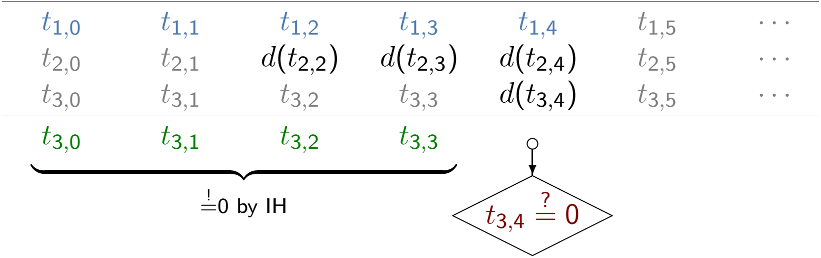


$t_{3,4} \overset{?}{=} 0$

- This can be decided by a radical membership test in $K(t_{1,0}, \ldots, t_{1,4})[t_{2,0}, \ldots, t_{3,4}]$

Proving Zero Equivalence of Admissible Sequences

- *Goal:* Show that $f_3(n) = 0$ for all $n \in \mathbb{N}$
- Suppose $f_1(n) = x_n$ is free



$t_{1,0}$	$t_{1,1}$	$t_{1,2}$	$t_{1,3}$	$t_{1,4}$	$t_{1,5}$	$\cdots$
$t_{2,0}$	$t_{2,1}$	$d(t_{2,2})$	$d(t_{2,3})$	$d(t_{2,4})$	$t_{2,5}$	$\cdots$
$t_{3,0}$	$t_{3,1}$	$t_{3,2}$	$t_{3,3}$	$d(t_{3,4})$	$t_{3,5}$	$\cdots$

$$\underbrace{t_{3,0} \quad t_{3,1} \quad t_{3,2} \quad t_{3,3}}_{\overset{!}{=}0 \text{ by IH}}$$

$$\boxed{t_{3,4} \overset{?}{=} 0}$$

- This can be decided by a radical membership test in $K(t_{1,0}, \ldots, t_{1,4})[t_{2,0}, \ldots, t_{3,4}]$
- Everything else carries over literally

Simple Example

Prove: $$\sum_{k=0}^{n}\sum_{i=0}^{k} x_i = (n+1)\sum_{k=0}^{n} x_k - \sum_{k=0}^{n} k\,x_k.$$

Simple Example

Prove: $\displaystyle\sum_{k=0}^{n}\sum_{i=0}^{k} x_i = (n+1)\sum_{k=0}^{n} x_k - \sum_{k=0}^{n} k\,x_k.$

Step 0 Describe $f(n) :=$ lhs $-$ rhs in terms of recurrences.

Simple Example

Prove: $$\sum_{k=0}^{n}\sum_{i=0}^{k} \underline{x_i} = (n+1)\sum_{k=0}^{n} \underline{x_k} - \sum_{k=0}^{n} k\, \underline{x_k}.$$

Step 0 Describe $f(n) :=$ lhs − rhs in terms of recurrences.

$f_0(n) = x_n$ no defining relation

Simple Example

Prove: $\displaystyle\sum_{k=0}^{n}\sum_{i=0}^{k} x_i = (\underline{n}+1)\sum_{k=0}^{n} x_k - \sum_{k=0}^{n} \underline{k}\, x_k.$

Step 0 Describe $f(n) :=$ lhs $-$ rhs in terms of recurrences.

$f_0(n) = x_n$	no defining relation
$f_1(n) = n$	$f_1(0) = 0, f_1(n+1) = f_1(n) + 1$

Simple Example

Prove: $\sum_{k=0}^{n} \underline{\sum_{i=0}^{k} x_i} = (n+1)\underline{\sum_{k=0}^{n} x_k} - \sum_{k=0}^{n} k\, x_k.$

Step 0 Describe $f(n) :=$ lhs − rhs in terms of recurrences.

$f_0(n) = x_n$	no defining relation
$f_1(n) = n$	$f_1(0) = 0, f_1(n+1) = f_1(n) + 1$
$f_2(n) = \sum_{k=0}^{n} x_k$	$f_2(0) = x_0, f_2(n+1) = f_2(n) + f_0(n+1)$

Simple Example

Prove: $\displaystyle\sum_{k=0}^{n}\sum_{i=0}^{k} x_i = (n+1)\sum_{k=0}^{n} x_k - \sum_{k=0}^{n} k\, x_k.$

Step 0 Describe $f(n) :=$ lhs − rhs in terms of recurrences.

$f_0(n) = x_n$ no defining relation

$f_1(n) = n$ $f_1(0) = 0, f_1(n+1) = f_1(n) + 1$

$f_2(n) = \sum_{k=0}^{n} x_k$ $f_2(0) = x_0, f_2(n+1) = f_2(n) + f_0(n+1)$

$f_3(n) = \sum_{k=0}^{n} k x_k$ $f_3(0) = 0, f_3(n+1) = f_3(n) + f_0(n+1) f_1(n+1)$

$f_4(n) =$ lhs $f_4(0) = x_0, f_4(n+1) = f_4(n) + f_2(n+1)$

$f(n) =$ lhs − rhs $f(0) = 0, f(n) = f_4(n) - (f_1(n)+1) f_2(n) - f_3(n)$

Simple Example

Prove: $\displaystyle \sum_{k=0}^{n}\sum_{i=0}^{k} x_i = (n+1)\sum_{k=0}^{n} x_k - \sum_{k=0}^{n} k\,x_k.$

Step 1 Translate recurrences to defining relations

$$
\begin{array}{rl}
f_0(n) \sim t_{0,0} & \text{none} \\
f_1(n) \sim t_{1,0} & t_{1,1} - t_{1,0} - 1 \\
f_2(n) \sim t_{2,0} & t_{2,1} - t_{2,0} - t_{0,1} \\
f_3(n) \sim t_{3,0} & t_{3,1} - t_{3,0} - t_{0,1}t_{1,1} \\
f_4(n) \sim t_{4,0} & t_{4,1} - t_{4,0} - t_{2,1} \\
f(n) \sim t_{5,0} & t_{5,0} - t_{4,0} + (t_{1,0} + 1)t_{2,0} + t_{3,0}
\end{array}
$$

Let D be the set of defining relations.

Simple Example

Prove: $\displaystyle\sum_{k=0}^{n}\sum_{i=0}^{k} x_i = (n+1)\sum_{k=0}^{n} x_k - \sum_{k=0}^{n} k\,x_k.$

Step 2 Find the induction step

$$t_{5,1} \in \mathrm{Rad}(\langle\{t_{5,0}\} \cup D\rangle)$$

This means $\forall\ n \in \mathbb{N} : f(n) = 0 \ \Rightarrow\ f(n+1) = 0$.
(No iteration necessary in this example.)

Simple Example

Prove: $\displaystyle\sum_{k=0}^{n}\sum_{i=0}^{k} x_i = (n+1)\sum_{k=0}^{n} x_k - \sum_{k=0}^{n} k\, x_k.$

Step 3 Check initial conditions: $f(0) = 0$. $\square$

Further Examples

- *Christoffel-Darboux identity:* For each $(c_n)_{n=1}^{\infty}$, $(\lambda_n)_{n=1}^{\infty}$ the recurrence

$$P_n(x) = (x - c_n)P_{n-1}(x) - \lambda_n P_{n-2}(x)$$

defines a family of orthogonal polynomials. We can prove

$$\sum_{k=0}^{n} \frac{P_k(x)P_k(u)}{\prod_{i=1}^{k+1} \lambda_i} = \frac{P_{n+1}(x)P_n(u) - P_n(x)P_{n+1}(u)}{(x-u)\prod_{i=1}^{n+1} \lambda_i}$$

$$\sum_{k=0}^{n} \frac{P_k(x)^2}{\prod_{i=1}^{k+1} \lambda_i} = \frac{P_n(x)P'_{n+1}(x) - P_{n+1}(x)P'_n(x)}{\prod_{i=1}^{n+1} \lambda_i}$$

for general $(c_n)_{n=1}^{\infty}$ and $(\lambda_n)_{n=1}^{\infty}$.

Further Examples

- *A hypergeometric identity for general $_mF_n$* Defining the multivariate sequences $f(n,m)$ and $g(n,m)$ by

$$f(n,m) = F\left(\begin{matrix} a_1, a_1 + \frac{1}{2}, \dots, a_m, a_m + \frac{1}{2} \\ b_1, b_1 + \frac{1}{2}, \dots, b_n, b_n + \frac{1}{2}, \frac{1}{2} \end{matrix} \,\middle|\, (2^{m-n-1}z)^2\right)$$

$$g(n,m) = \frac{1}{2}\left[F\left(\begin{matrix} 2a_1, \dots, 2a_m \\ 2b_1, \dots, 2b_n \end{matrix} \,\middle|\, z\right) + F\left(\begin{matrix} 2a_1, \dots, 2a_m \\ 2b_1, \dots, 2b_n \end{matrix} \,\middle|\, -z\right)\right],$$

we can prove

$$f(n,m) = g(n,m)$$

for general n and m (see paper).

Conclusion

Conclusion

- A large class of sequences can be represented by difference algebra tools

Conclusion

- A large class of sequences can be represented by difference algebra tools
- Free sequences can be represented as well

Conclusion

- A large class of sequences can be represented by difference algebra tools
- Free sequences can be represented as well
- An algorithm for deciding zero equivalence is known

Conclusion

- A large class of sequences can be represented by difference algebra tools
- Free sequences can be represented as well
- An algorithm for deciding zero equivalence is known
- This allows for proving certain polynomial identities in arbitrarily many variables by the computer

Conclusion

- A large class of sequences can be represented by difference algebra tools
- Free sequences can be represented as well
- An algorithm for deciding zero equivalence is known
- This allows for proving certain polynomial identities in arbitrarily many variables by the computer
- *Latest Development:* Some of these identities can not only be proven but also be *found* by the computer (↑ Schneider's talk)

Conclusion

- A large class of sequences can be represented by difference algebra tools
- Free sequences can be represented as well
- An algorithm for deciding zero equivalence is known
- This allows for proving certain polynomial identities in arbitrarily many variables by the computer
- *Latest Development:* Some of these identities can not only be proven but also be *found* by the computer (↑ Schneider's talk)
- . . . but is there any use of all this?