The qTSPP Theorem

Manuel Kauers
RISC-Linz

joint work with
Christoph Koutschan and Doron Zeilberger

David Hilbert in 1900

Hilbert's dream: *Only formal proofs are acceptable proofs!*

> *In order to prove a conjecture, apply logical reduction rules until you reach a statement which is true by definition.*

Hilbert's dream: *Only formal proofs are acceptable proofs!*

> *In order to prove a conjecture, apply logical reduction rules until you reach a statement which is true by definition.*

Zeilberger's dream: *Only computer proofs are acceptable proofs!*

> *In order to prove a conjecture, enter it into a suitable computer program and see whether it returns true.*

Hilbert's dream: *Only formal proofs are acceptable proofs!*

In order to prove a conjecture, apply logical reduction rules until you reach a statement which is true by definition.

Zeilberger's dream: *Only computer proofs are acceptable proofs!*

In order to prove a conjecture, enter it into a suitable computer program and see whether it returns true.

Realistic scenario: *Mixed Human-Computer proofs!*

In order to prove a conjecture, apply logical reduction rules until you reach a statement which you can enter into a suitable computer program to see whether it returns true.

Trivial Example

Theorem: There does not exist a point $(x, y, z) \in \mathbb{C}^3$ such that

$$xy - 1 = 0, \qquad xyz - x + y - z = 0,$$
$$z^2 y + 1 = 0, \qquad x^2 - y^2 + z = 0.$$

Trivial Example

Theorem: There does not exist a point $(x, y, z) \in \mathbb{C}^3$ such that

$$xy - 1 = 0, \qquad xyz - x + y - z = 0,$$
$$z^2 y + 1 = 0, \qquad x^2 - y^2 + z = 0.$$

Modern proof:

Trivial Example

Theorem: There does not exist a point $(x, y, z) \in \mathbb{C}^3$ such that

$$\begin{aligned} xy - 1 &= 0, & xyz - x + y - z &= 0, \\ z^2y + 1 &= 0, & x^2 - y^2 + z &= 0. \end{aligned}$$

Modern proof:

- *Human part:* If $(x, y, z) \in \mathbb{C}^3$ is a common root of some polynomials p_1, p_2, p_3, p_4, then it is also a root of

  $$q_1p_1 + q_2p_2 + q_3p_3 + q_4p_4$$

  for any other polynomials q_1, q_2, q_3, q_4.

Trivial Example

Theorem: There does not exist a point $(x, y, z) \in \mathbb{C}^3$ such that

$$\begin{aligned} xy - 1 &= 0, & xyz - x + y - z &= 0, \\ z^2 y + 1 &= 0, & x^2 - y^2 + z &= 0. \end{aligned}$$

Modern proof:

- *Human part:* If $(x, y, z) \in \mathbb{C}^3$ is a common root of some polynomials p_1, p_2, p_3, p_4, then it is also a root of

$$q_1 p_1 + q_2 p_2 + q_3 p_3 + q_4 p_4$$

  for any other polynomials q_1, q_2, q_3, q_4.
  Therefore, if 1 belongs to the ideal $\langle p_1, p_2, p_3, p_4 \rangle$, then there is no common root.

Trivial Example

Theorem: There does not exist a point $(x, y, z) \in \mathbb{C}^3$ such that

$$\begin{aligned} xy - 1 &= 0, & xyz - x + y - z &= 0, \\ z^2y + 1 &= 0, & x^2 - y^2 + z &= 0. \end{aligned}$$

Modern proof:

- *Computer part:* Use a computer to show that

$$1 \in \langle xy - 1,\ xyz - x + y - z,\ yz^2 + 1,\ x^2 - y^2 + z \rangle$$

(e.g., by a Gröbner basis computation). ∎

Trivial Example

Theorem: There does not exist a point $(x, y, z) \in \mathbb{C}^3$ such that

$$\begin{aligned} xy - 1 &= 0, \qquad & xyz - x + y - z &= 0, \\ z^2 y + 1 &= 0, \qquad & x^2 - y^2 + z &= 0. \end{aligned}$$

Can we trust this calculation?

Trivial Example

Theorem: There does not exist a point $(x, y, z) \in \mathbb{C}^3$ such that

$$\begin{aligned} xy - 1 &= 0, & xyz - x + y - z &= 0, \\ z^2 y + 1 &= 0, & x^2 - y^2 + z &= 0. \end{aligned}$$

Can we trust this calculation?

Can we trust it in theory / in practice?

Trivial Example

Theorem: There does not exist a point $(x, y, z) \in \mathbb{C}^3$ such that

$$\begin{aligned} xy - 1 &= 0, \qquad & xyz - x + y - z &= 0, \\ z^2 y + 1 &= 0, \qquad & x^2 - y^2 + z &= 0. \end{aligned}$$

Can we trust this calculation?

Can we trust it in theory / in practice?

Can we check it?

Trivial Example

Theorem: There does not exist a point $(x, y, z) \in \mathbb{C}^3$ such that

$$xy - 1 = 0, \qquad xyz - x + y - z = 0,$$
$$z^2 y + 1 = 0, \qquad x^2 - y^2 + z = 0.$$

Can we trust this calculation?

Can we trust it in theory / in practice?

Can we check it?

Can we get a *certificate?*

Trivial Example

Theorem: There does not exist a point $(x, y, z) \in \mathbb{C}^3$ such that

$$\begin{aligned} xy - 1 &= 0, & xyz - x + y - z &= 0, \\ z^2y + 1 &= 0, & x^2 - y^2 + z &= 0. \end{aligned}$$

A *certificate* is a piece of data which allows to confirm a computational result by doing a “simple” calculation.

Trivial Example

Theorem: There does not exist a point $(x, y, z) \in \mathbb{C}^3$ such that

$$\begin{aligned} xy - 1 &= 0, & xyz - x + y - z &= 0, \\ z^2y + 1 &= 0, & x^2 - y^2 + z &= 0. \end{aligned}$$

A *certificate* is a piece of data which allows to confirm a computational result by doing a "simple" calculation.

In this example, a certificate could be

$$\begin{aligned} q_1 &:= -x - y, & q_2 &:= -y^2z - xyz, \\ q_3 &:= x^2y + xy^2 - x - y + 1, & q_4 &:= -yz. \end{aligned}$$

because for these q_i we have $1 = q_1p_1 + q_2p_2 + q_3p_3 + q_4p_4$.

Trivial Example

Theorem: There does not exist a point $(x, y, z) \in \mathbb{C}^3$ such that

$$\begin{aligned} xy - 1 &= 0, \qquad & xyz - x + y - z &= 0, \\ z^2 y + 1 &= 0, \qquad & x^2 - y^2 + z &= 0. \end{aligned}$$

A *certificate* is a piece of data which allows to confirm a computational result by doing a "simple" calculation.

In this example, a certificate could be

$$\begin{aligned} q_1 &:= -x - y, & q_2 &:= -y^2 z - xyz, \\ q_3 &:= x^2 y + xy^2 - x - y + 1, \qquad & q_4 &:= -yz. \end{aligned}$$

because for these q_i we have $1 = q_1 p_1 + q_2 p_2 + q_3 p_3 + q_4 p_4$.

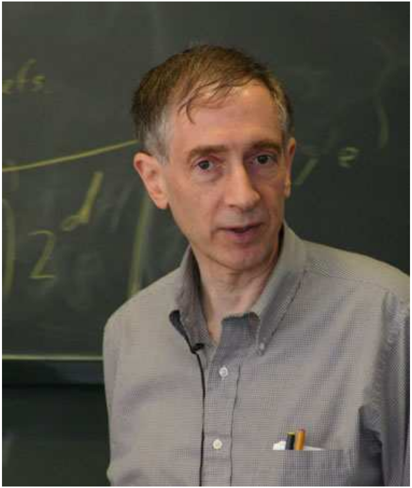
This can be "easily checked".

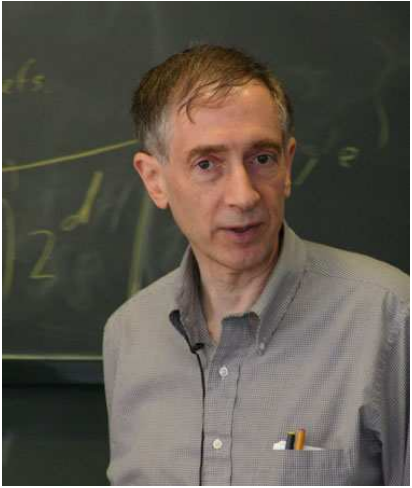
Plan for this talk

Plan for this talk

A non-trivial example for a such a modern proof

proving a longstanding open conjecture in partition theory.





Richard Stanley in 2004

Partitions

A *partition* π of size n is a tuple $(\pi_i)_{i=1}^n \in \mathbb{N}^n$ with $n \geq \pi_1 \geq \pi_2 \geq \cdots \geq \pi_n$.

Partitions

A *partition* π of size n is a tuple $(\pi_i)_{i=1}^n \in \mathbb{N}^n$ with $n \geq \pi_1 \geq \pi_2 \geq \cdots \geq \pi_n$.

Example: $\boxed{5 \mid 3 \mid 3 \mid 2 \mid 1 \mid 0}$ is a partition of size 6

Partitions

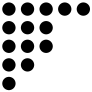
A *partition* π of size n is a tuple $(\pi_i)_{i=1}^n \in \mathbb{N}^n$ with $n \geq \pi_1 \geq \pi_2 \geq \cdots \geq \pi_n$.

Example:

5	3	3	2	1	0

is a partition of size 6

Picture:



Plane Partitions

A *plane partition* π of size n is a matrix $((\pi_{i,j}))_{i,j=1}^{n} \in \mathbb{N}^{n\times n}$ with $n \geq \pi_{i,1} \geq \pi_{i,2} \geq \cdots \geq \pi_{i,n}$ and $n \geq \pi_{1,i} \geq \pi_{2,i} \geq \cdots \geq \pi_{n,i}$ for all i.

Plane Partitions

A *plane partition* π of size n is a matrix $((\pi_{i,j}))_{i,j=1}^{n} \in \mathbb{N}^{n\times n}$ with $n \geq \pi_{i,1} \geq \pi_{i,2} \geq \cdots \geq \pi_{i,n}$ and $n \geq \pi_{1,i} \geq \pi_{2,i} \geq \cdots \geq \pi_{n,i}$ for all i.

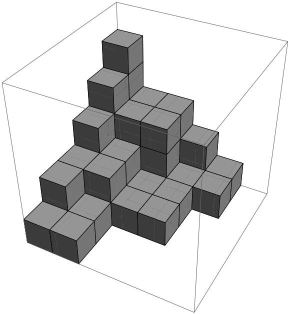
5	3	3	2	1	0
4	3	3	1	1	0
3	2	1	1	0	0
2	2	1	1	0	0
2	1	0	0	0	0
1	1	0	0	0	0

is a plane partition of size 6

Plane Partitions

A *plane partition* π of size n is a matrix $((\pi_{i,j}))_{i,j=1}^{n} \in \mathbb{N}^{n\times n}$ with $n \geq \pi_{i,1} \geq \pi_{i,2} \geq \cdots \geq \pi_{i,n}$ and $n \geq \pi_{1,i} \geq \pi_{2,i} \geq \cdots \geq \pi_{n,i}$ for all i.

5	3	3	2	1	0
4	3	3	1	1	0
3	2	1	1	0	0
2	2	1	1	0	0
2	1	0	0	0	0
1	1	0	0	0	0

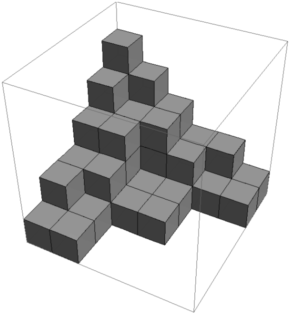


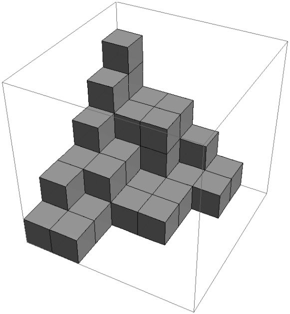
Symmetric Plane Partitions

A *symmetric plane partition* π is a plane partition $((\pi_{i,j}))_{i,j=1}^{n} \in \mathbb{N}^{n \times n}$ with $\pi_{i,j} = \pi_{j,i}$ for all i, j.

Symmetric Plane Partitions

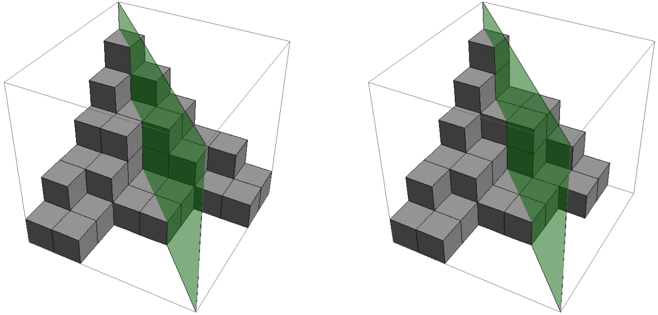
A *symmetric plane partition* π is a plane partition $((\pi_{i,j}))_{i,j=1}^{n} \in \mathbb{N}^{n\times n}$ with $\pi_{i,j} = \pi_{j,i}$ for all i, j.





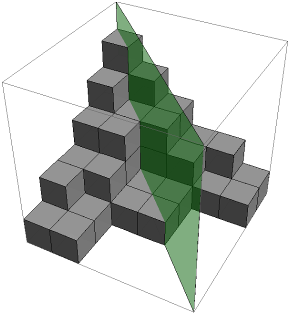
Symmetric Plane Partitions

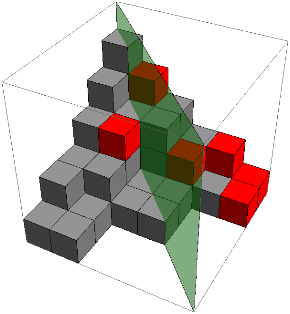
A *symmetric plane partition* π is a plane partition $((\pi_{i,j}))_{i,j=1}^{n} \in \mathbb{N}^{n \times n}$ with $\pi_{i,j} = \pi_{j,i}$ for all i, j.



Symmetric Plane Partitions

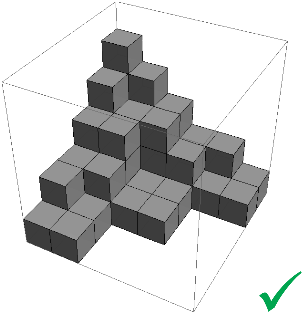
A *symmetric plane partition* π is a plane partition $((\pi_{i,j}))_{i,j=1}^{n} \in \mathbb{N}^{n \times n}$ with $\pi_{i,j} = \pi_{j,i}$ for all i, j.

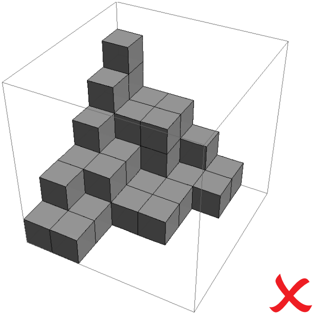




Symmetric Plane Partitions

A *symmetric plane partition* π is a plane partition $((\pi_{i,j}))_{i,j=1}^{n} \in \mathbb{N}^{n\times n}$ with $\pi_{i,j} = \pi_{j,i}$ for all i, j.



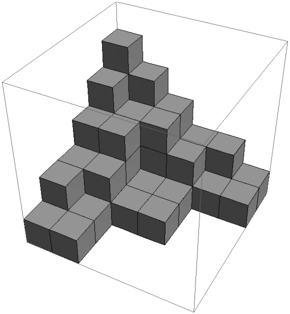


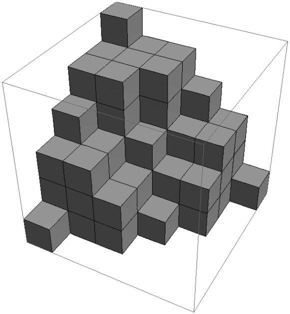
Totally Symmetric Plane Partitions

A *totally symmetric plane partition* π is a symmetric plane partition whose diagram is symmetric about all three diagonal planes.

Totally Symmetric Plane Partitions

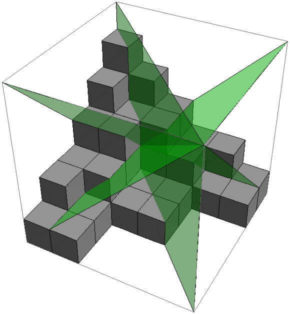
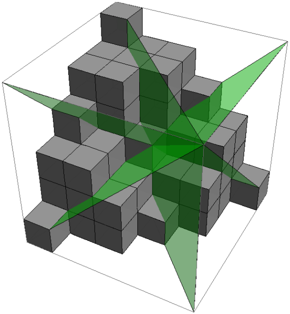
A *totally symmetric plane partition* π is a symmetric plane partition whose diagram is symmetric about all three diagonal planes.





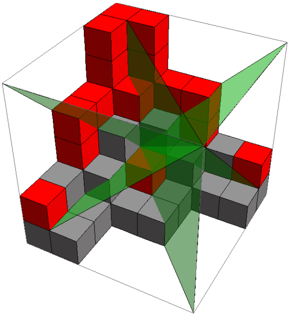
Totally Symmetric Plane Partitions

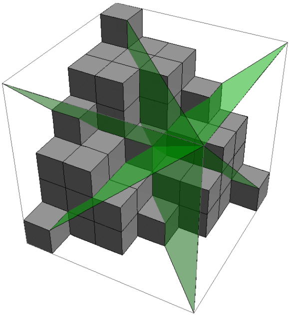
A *totally symmetric plane partition* π is a symmetric plane partition whose diagram is symmetric about all three diagonal planes.

Totally Symmetric Plane Partitions

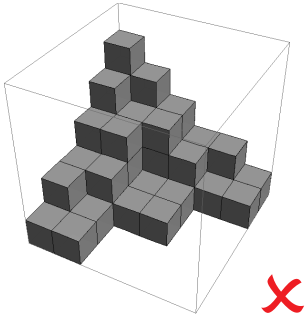
A *totally symmetric plane partition* π is a symmetric plane partition whose diagram is symmetric about all three diagonal planes.

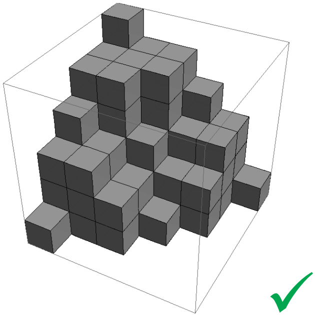




Totally Symmetric Plane Partitions

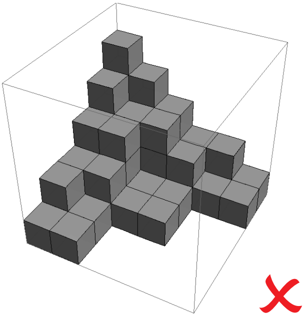
A *totally symmetric plane partition* π is a symmetric plane partition whose diagram is symmetric about all three diagonal planes.

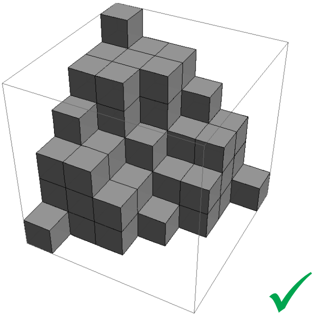




Totally Symmetric Plane Partitions

A *totally symmetric plane partition* π is a symmetric plane partition whose diagram is symmetric about all three diagonal planes.





Totally Symmetric Plane Partitions

Theorem: There are

$$\prod_{1\le i\le j\le k\le n} \frac{i+j+k-1}{i+j+k-2}$$

totally symmetric plane partitions of size n.

Totally Symmetric Plane Partitions

Theorem: There are

$$\prod_{1\leq i\leq j\leq k\leq n} \frac{i+j+k-1}{i+j+k-2}$$

totally symmetric plane partitions of size n.

Proofs:

Totally Symmetric Plane Partitions

Theorem: There are

$$\prod_{1\leq i\leq j\leq k\leq n} \frac{i+j+k-1}{i+j+k-2}$$

totally symmetric plane partitions of size n.

Proofs:

- *Stembridge, 1995:* 100% thinking, 0% computing.

Totally Symmetric Plane Partitions

Theorem: There are

$$\prod_{1 \le i \le j \le k \le n} \frac{i+j+k-1}{i+j+k-2}$$

totally symmetric plane partitions of size n.

Proofs:

- *Stembridge, 1995:* 100% thinking, 0% computing.
- *Andrews, Paule, Schneider, 2005:* 50% thinking, 50% computing.

Totally Symmetric Plane Partitions

Theorem: There are

$$\prod_{1\leq i\leq j\leq k\leq n} \frac{i+j+k-1}{i+j+k-2}$$

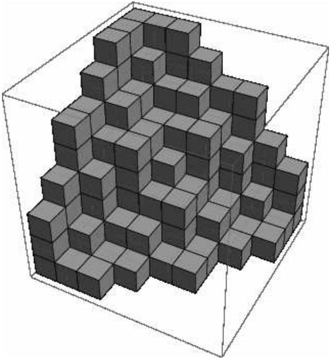
totally symmetric plane partitions of size n.

Proofs:

- *Stembridge, 1995:* 100% thinking, 0% computing.
- *Andrews, Paule, Schneider, 2005:*
  50% thinking, 50% computing.
- *Koutschan, 2010:* $<$1% thinking, $>$99% computing.

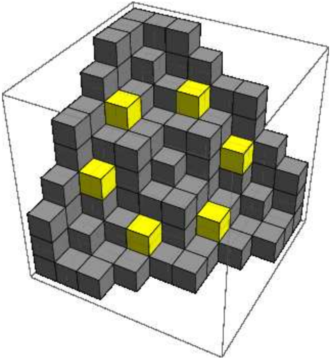
Totally Symmetric Plane Partitions

A totally symmetric plane partition can be decomposed into *orbits:*



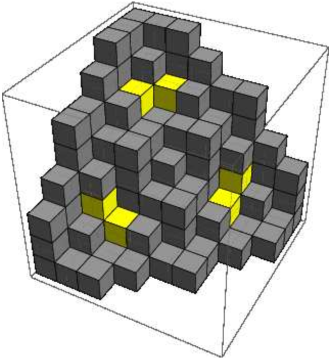
Totally Symmetric Plane Partitions

A totally symmetric plane partition can be decomposed into *orbits:*



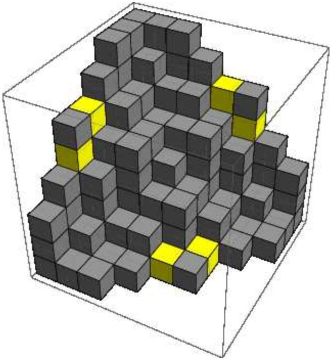
Totally Symmetric Plane Partitions

A totally symmetric plane partition can be decomposed into *orbits:*



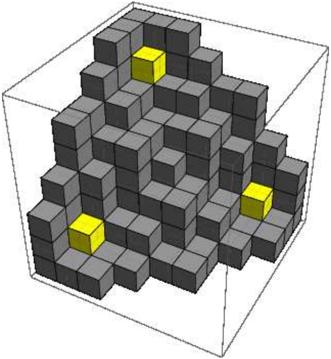
Totally Symmetric Plane Partitions

A totally symmetric plane partition can be decomposed into *orbits:*



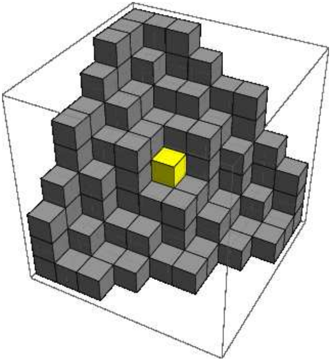
Totally Symmetric Plane Partitions

A totally symmetric plane partition can be decomposed into *orbits:*



Totally Symmetric Plane Partitions

A totally symmetric plane partition can be decomposed into *orbits:*



Totally Symmetric Plane Partitions

Let $R_{n,m}$ be the number of totally symmetric plane partitions of size n with m orbits.

Totally Symmetric Plane Partitions

Let $R_{n,m}$ be the number of totally symmetric plane partitions of size n with m orbits.

Then $\sum_{m=0}^{\infty} R_{n,m} q^m$ is a polynomial in q.

Totally Symmetric Plane Partitions

Let $R_{n,m}$ be the number of totally symmetric plane partitions of size n with m orbits.

Then $\sum_{m=0}^{\infty} R_{n,m} q^m$ is a polynomial in q.

Example: for $n = 7$, this polynomial is

$$q^{84} + q^{83} + \cdots + 542q^{51} + 573q^{50} + \cdots + 2q^3 + q^2 + q + 1.$$

Totally Symmetric Plane Partitions

Let $R_{n,m}$ be the number of totally symmetric plane partitions of size n with m orbits.

Then $\sum_{m=0}^{\infty} R_{n,m} q^m$ is a polynomial in q.

Example: for $n = 7$, this polynomial is

$$q^{84} + q^{83} + \cdots + 542q^{51} + 573q^{50} + \cdots + 2q^3 + q^2 + q + 1.$$

The qTSPP-Theorem (K.K.Z. 2010): For all $n \geq 1$,

$$\sum_{m=0}^{\infty} R_{n,m} q^m = \prod_{1 \leq i \leq j \leq k \leq n} \frac{1 - q^{i+j+k-1}}{1 - q^{i+j+k-2}}.$$

The qTSPP Theorem

$$\sum_{m=0}^{\infty} R_{n,m} q^m = \prod_{1 \le i \le j \le k \le n} \frac{1 - q^{i+j+k-1}}{1 - q^{i+j+k-2}}.$$

Proof Structure

The qTSPP Theorem

$$\sum_{m=0}^{\infty} R_{n,m} q^m = \prod_{1 \le i \le j \le k \le n} \frac{1 - q^{i+j+k-1}}{1 - q^{i+j+k-2}}.$$

Proof Structure

- Reduce the identity to a more comfortable identity (by hand)

The qTSPP Theorem

$$\sum_{m=0}^{\infty} R_{n,m} q^m = \prod_{1 \le i \le j \le k \le n} \frac{1 - q^{i+j+k-1}}{1 - q^{i+j+k-2}}.$$

Proof Structure

- Reduce the identity to a more comfortable identity (by hand)
- Construct a certificate for this identity (empirically; by computer)

The qTSPP Theorem

$$\sum_{m=0}^{\infty} R_{n,m} q^m = \prod_{1 \le i \le j \le k \le n} \frac{1 - q^{i+j+k-1}}{1 - q^{i+j+k-2}}.$$

Proof Structure

- Reduce the identity to a more comfortable identity (by hand)
- Construct a certificate for this identity (empirically; by computer)
- Prove that the certificate really is a certificate (by computer)

The qTSPP Theorem

$$\sum_{m=0}^{\infty} R_{n,m} q^m = \prod_{1 \le i \le j \le k \le n} \frac{1 - q^{i+j+k-1}}{1 - q^{i+j+k-2}}.$$

Proof Structure

- Reduce the identity to a more comfortable identity (by hand)
- Construct a certificate for this identity (empirically; by computer)
- Prove that the certificate really is a certificate (by computer)
- Construct a certificate for the certificate (rigorously; by computer)

Okada's Lemma

If

$$\det((a_{i,j}))_{i,j=1}^{n} = \prod_{1\le i\le j\le k\le n} \left(\frac{1-q^{i+j+k-1}}{1-q^{i+j+k-2}}\right)^2 \quad (n \ge 1)$$

where

$$a_{i,j} = \frac{q^{i+j}+q^i-q-1}{q^{1-i-j}(q^i-1)} \prod_{k=1}^{i-1} \frac{1-q^{k+j-2}}{1-q^k} + (1+q^i)\delta_{i,j} - \delta_{i,j+1}$$

then

$$\sum_{m=0}^{\infty} R_{n,m} q^m = \prod_{1\le i\le j\le k\le n} \frac{1-q^{i+j+k-1}}{1-q^{i+j+k-2}}. \quad (n \ge 1).$$

$$
\begin{array}{ccccccccc}
a_{1,1} & a_{1,2} & a_{1,3} & a_{1,4} & a_{1,5} & a_{1,6} & a_{1,7} & a_{1,8} & \cdots \\
a_{2,1} & a_{2,2} & a_{2,3} & a_{2,4} & a_{2,5} & a_{2,6} & a_{2,7} & a_{2,8} & \cdots \\
a_{3,1} & a_{3,2} & a_{3,3} & a_{3,4} & a_{3,5} & a_{3,6} & a_{3,7} & a_{3,8} & \cdots \\
a_{4,1} & a_{4,2} & a_{4,3} & a_{4,4} & a_{4,5} & a_{4,6} & a_{4,7} & a_{4,8} & \cdots \\
a_{5,1} & a_{5,2} & a_{5,3} & a_{5,4} & a_{5,5} & a_{5,6} & a_{5,7} & a_{5,8} & \cdots \\
a_{6,1} & a_{6,2} & a_{6,3} & a_{6,4} & a_{6,5} & a_{6,6} & a_{6,7} & a_{6,8} & \cdots \\
a_{7,1} & a_{7,2} & a_{7,3} & a_{7,4} & a_{7,5} & a_{7,6} & a_{7,7} & a_{7,8} & \cdots \\
a_{8,1} & a_{8,2} & a_{8,3} & a_{8,4} & a_{8,5} & a_{8,6} & a_{8,7} & a_{8,8} & \cdots \\
a_{9,1} & a_{9,2} & a_{9,3} & a_{9,4} & a_{9,5} & a_{9,6} & a_{9,7} & a_{9,8} & \cdots \\
a_{10,1} & a_{10,2} & a_{10,3} & a_{10,4} & a_{10,5} & a_{10,6} & a_{10,7} & a_{10,8} & \cdots \\
a_{11,1} & a_{11,2} & a_{11,3} & a_{11,4} & a_{11,5} & a_{11,6} & a_{11,7} & a_{11,8} & \cdots \\
a_{12,1} & a_{12,2} & a_{12,3} & a_{12,4} & a_{12,5} & a_{12,6} & a_{12,7} & a_{12,8} & \cdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots
\end{array}
$$

$$
\begin{array}{ccccccccc}
\big| a_{1,1} \big| & a_{1,2} & a_{1,3} & a_{1,4} & a_{1,5} & a_{1,6} & a_{1,7} & a_{1,8} & \cdots \\
a_{2,1} & a_{2,2} & a_{2,3} & a_{2,4} & a_{2,5} & a_{2,6} & a_{2,7} & a_{2,8} & \cdots \\
a_{3,1} & a_{3,2} & a_{3,3} & a_{3,4} & a_{3,5} & a_{3,6} & a_{3,7} & a_{3,8} & \cdots \\
a_{4,1} & a_{4,2} & a_{4,3} & a_{4,4} & a_{4,5} & a_{4,6} & a_{4,7} & a_{4,8} & \cdots \\
a_{5,1} & a_{5,2} & a_{5,3} & a_{5,4} & a_{5,5} & a_{5,6} & a_{5,7} & a_{5,8} & \cdots \\
a_{6,1} & a_{6,2} & a_{6,3} & a_{6,4} & a_{6,5} & a_{6,6} & a_{6,7} & a_{6,8} & \cdots \\
a_{7,1} & a_{7,2} & a_{7,3} & a_{7,4} & a_{7,5} & a_{7,6} & a_{7,7} & a_{7,8} & \cdots \\
a_{8,1} & a_{8,2} & a_{8,3} & a_{8,4} & a_{8,5} & a_{8,6} & a_{8,7} & a_{8,8} & \cdots \\
a_{9,1} & a_{9,2} & a_{9,3} & a_{9,4} & a_{9,5} & a_{9,6} & a_{9,7} & a_{9,8} & \cdots \\
a_{10,1} & a_{10,2} & a_{10,3} & a_{10,4} & a_{10,5} & a_{10,6} & a_{10,7} & a_{10,8} & \cdots \\
a_{11,1} & a_{11,2} & a_{11,3} & a_{11,4} & a_{11,5} & a_{11,6} & a_{11,7} & a_{11,8} & \cdots \\
a_{12,1} & a_{12,2} & a_{12,3} & a_{12,4} & a_{12,5} & a_{12,6} & a_{12,7} & a_{12,8} & \cdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots
\end{array}
$$

$$
\begin{matrix}
a_{1,1} & a_{1,2} & a_{1,3} & a_{1,4} & a_{1,5} & a_{1,6} & a_{1,7} & a_{1,8} & \cdots \\
a_{2,1} & a_{2,2} & a_{2,3} & a_{2,4} & a_{2,5} & a_{2,6} & a_{2,7} & a_{2,8} & \cdots \\
a_{3,1} & a_{3,2} & a_{3,3} & a_{3,4} & a_{3,5} & a_{3,6} & a_{3,7} & a_{3,8} & \cdots \\
a_{4,1} & a_{4,2} & a_{4,3} & a_{4,4} & a_{4,5} & a_{4,6} & a_{4,7} & a_{4,8} & \cdots \\
a_{5,1} & a_{5,2} & a_{5,3} & a_{5,4} & a_{5,5} & a_{5,6} & a_{5,7} & a_{5,8} & \cdots \\
a_{6,1} & a_{6,2} & a_{6,3} & a_{6,4} & a_{6,5} & a_{6,6} & a_{6,7} & a_{6,8} & \cdots \\
a_{7,1} & a_{7,2} & a_{7,3} & a_{7,4} & a_{7,5} & a_{7,6} & a_{7,7} & a_{7,8} & \cdots \\
a_{8,1} & a_{8,2} & a_{8,3} & a_{8,4} & a_{8,5} & a_{8,6} & a_{8,7} & a_{8,8} & \cdots \\
a_{9,1} & a_{9,2} & a_{9,3} & a_{9,4} & a_{9,5} & a_{9,6} & a_{9,7} & a_{9,8} & \cdots \\
a_{10,1} & a_{10,2} & a_{10,3} & a_{10,4} & a_{10,5} & a_{10,6} & a_{10,7} & a_{10,8} & \cdots \\
a_{11,1} & a_{11,2} & a_{11,3} & a_{11,4} & a_{11,5} & a_{11,6} & a_{11,7} & a_{11,8} & \cdots \\
a_{12,1} & a_{12,2} & a_{12,3} & a_{12,4} & a_{12,5} & a_{12,6} & a_{12,7} & a_{12,8} & \cdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots
\end{matrix}
$$

$$
\begin{array}{ccccccccc}
a_{1,1} & a_{1,2} & a_{1,3} & a_{1,4} & a_{1,5} & a_{1,6} & a_{1,7} & a_{1,8} & \cdots \\
a_{2,1} & a_{2,2} & a_{2,3} & a_{2,4} & a_{2,5} & a_{2,6} & a_{2,7} & a_{2,8} & \cdots \\
a_{3,1} & a_{3,2} & a_{3,3} & a_{3,4} & a_{3,5} & a_{3,6} & a_{3,7} & a_{3,8} & \cdots \\
a_{4,1} & a_{4,2} & a_{4,3} & a_{4,4} & a_{4,5} & a_{4,6} & a_{4,7} & a_{4,8} & \cdots \\
a_{5,1} & a_{5,2} & a_{5,3} & a_{5,4} & a_{5,5} & a_{5,6} & a_{5,7} & a_{5,8} & \cdots \\
a_{6,1} & a_{6,2} & a_{6,3} & a_{6,4} & a_{6,5} & a_{6,6} & a_{6,7} & a_{6,8} & \cdots \\
a_{7,1} & a_{7,2} & a_{7,3} & a_{7,4} & a_{7,5} & a_{7,6} & a_{7,7} & a_{7,8} & \cdots \\
a_{8,1} & a_{8,2} & a_{8,3} & a_{8,4} & a_{8,5} & a_{8,6} & a_{8,7} & a_{8,8} & \cdots \\
a_{9,1} & a_{9,2} & a_{9,3} & a_{9,4} & a_{9,5} & a_{9,6} & a_{9,7} & a_{9,8} & \cdots \\
a_{10,1} & a_{10,2} & a_{10,3} & a_{10,4} & a_{10,5} & a_{10,6} & a_{10,7} & a_{10,8} & \cdots \\
a_{11,1} & a_{11,2} & a_{11,3} & a_{11,4} & a_{11,5} & a_{11,6} & a_{11,7} & a_{11,8} & \cdots \\
a_{12,1} & a_{12,2} & a_{12,3} & a_{12,4} & a_{12,5} & a_{12,6} & a_{12,7} & a_{12,8} & \cdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots
\end{array}
$$

$$
\begin{matrix}
a_{1,1} & a_{1,2} & a_{1,3} & a_{1,4} & a_{1,5} & a_{1,6} & a_{1,7} & a_{1,8} & \cdots \\
a_{2,1} & a_{2,2} & a_{2,3} & a_{2,4} & a_{2,5} & a_{2,6} & a_{2,7} & a_{2,8} & \cdots \\
a_{3,1} & a_{3,2} & a_{3,3} & a_{3,4} & a_{3,5} & a_{3,6} & a_{3,7} & a_{3,8} & \cdots \\
a_{4,1} & a_{4,2} & a_{4,3} & a_{4,4} & a_{4,5} & a_{4,6} & a_{4,7} & a_{4,8} & \cdots \\
a_{5,1} & a_{5,2} & a_{5,3} & a_{5,4} & a_{5,5} & a_{5,6} & a_{5,7} & a_{5,8} & \cdots \\
a_{6,1} & a_{6,2} & a_{6,3} & a_{6,4} & a_{6,5} & a_{6,6} & a_{6,7} & a_{6,8} & \cdots \\
a_{7,1} & a_{7,2} & a_{7,3} & a_{7,4} & a_{7,5} & a_{7,6} & a_{7,7} & a_{7,8} & \cdots \\
a_{8,1} & a_{8,2} & a_{8,3} & a_{8,4} & a_{8,5} & a_{8,6} & a_{8,7} & a_{8,8} & \cdots \\
a_{9,1} & a_{9,2} & a_{9,3} & a_{9,4} & a_{9,5} & a_{9,6} & a_{9,7} & a_{9,8} & \cdots \\
a_{10,1} & a_{10,2} & a_{10,3} & a_{10,4} & a_{10,5} & a_{10,6} & a_{10,7} & a_{10,8} & \cdots \\
a_{11,1} & a_{11,2} & a_{11,3} & a_{11,4} & a_{11,5} & a_{11,6} & a_{11,7} & a_{11,8} & \cdots \\
a_{12,1} & a_{12,2} & a_{12,3} & a_{12,4} & a_{12,5} & a_{12,6} & a_{12,7} & a_{12,8} & \cdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots
\end{matrix}
$$

$$
\begin{array}{ccccccccc}
a_{1,1} & a_{1,2} & a_{1,3} & a_{1,4} & a_{1,5} & a_{1,6} & a_{1,7} & a_{1,8} & \cdots \\
a_{2,1} & a_{2,2} & a_{2,3} & a_{2,4} & a_{2,5} & a_{2,6} & a_{2,7} & a_{2,8} & \cdots \\
a_{3,1} & a_{3,2} & a_{3,3} & a_{3,4} & a_{3,5} & a_{3,6} & a_{3,7} & a_{3,8} & \cdots \\
a_{4,1} & a_{4,2} & a_{4,3} & a_{4,4} & a_{4,5} & a_{4,6} & a_{4,7} & a_{4,8} & \cdots \\
a_{5,1} & a_{5,2} & a_{5,3} & a_{5,4} & a_{5,5} & a_{5,6} & a_{5,7} & a_{5,8} & \cdots \\
a_{6,1} & a_{6,2} & a_{6,3} & a_{6,4} & a_{6,5} & a_{6,6} & a_{6,7} & a_{6,8} & \cdots \\
a_{7,1} & a_{7,2} & a_{7,3} & a_{7,4} & a_{7,5} & a_{7,6} & a_{7,7} & a_{7,8} & \cdots \\
a_{8,1} & a_{8,2} & a_{8,3} & a_{8,4} & a_{8,5} & a_{8,6} & a_{8,7} & a_{8,8} & \cdots \\
a_{9,1} & a_{9,2} & a_{9,3} & a_{9,4} & a_{9,5} & a_{9,6} & a_{9,7} & a_{9,8} & \cdots \\
a_{10,1} & a_{10,2} & a_{10,3} & a_{10,4} & a_{10,5} & a_{10,6} & a_{10,7} & a_{10,8} & \cdots \\
a_{11,1} & a_{11,2} & a_{11,3} & a_{11,4} & a_{11,5} & a_{11,6} & a_{11,7} & a_{11,8} & \cdots \\
a_{12,1} & a_{12,2} & a_{12,3} & a_{12,4} & a_{12,5} & a_{12,6} & a_{12,7} & a_{12,8} & \cdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots
\end{array}
$$

$$
\begin{array}{ccccccccc}
a_{1,1} & a_{1,2} & a_{1,3} & a_{1,4} & a_{1,5} & a_{1,6} & a_{1,7} & a_{1,8} & \cdots \\
a_{2,1} & a_{2,2} & a_{2,3} & a_{2,4} & a_{2,5} & a_{2,6} & a_{2,7} & a_{2,8} & \cdots \\
a_{3,1} & a_{3,2} & a_{3,3} & a_{3,4} & a_{3,5} & a_{3,6} & a_{3,7} & a_{3,8} & \cdots \\
a_{4,1} & a_{4,2} & a_{4,3} & a_{4,4} & a_{4,5} & a_{4,6} & a_{4,7} & a_{4,8} & \cdots \\
a_{5,1} & a_{5,2} & a_{5,3} & a_{5,4} & a_{5,5} & a_{5,6} & a_{5,7} & a_{5,8} & \cdots \\
a_{6,1} & a_{6,2} & a_{6,3} & a_{6,4} & a_{6,5} & a_{6,6} & a_{6,7} & a_{6,8} & \cdots \\
a_{7,1} & a_{7,2} & a_{7,3} & a_{7,4} & a_{7,5} & a_{7,6} & a_{7,7} & a_{7,8} & \cdots \\
a_{8,1} & a_{8,2} & a_{8,3} & a_{8,4} & a_{8,5} & a_{8,6} & a_{8,7} & a_{8,8} & \cdots \\
a_{9,1} & a_{9,2} & a_{9,3} & a_{9,4} & a_{9,5} & a_{9,6} & a_{9,7} & a_{9,8} & \cdots \\
a_{10,1} & a_{10,2} & a_{10,3} & a_{10,4} & a_{10,5} & a_{10,6} & a_{10,7} & a_{10,8} & \cdots \\
a_{11,1} & a_{11,2} & a_{11,3} & a_{11,4} & a_{11,5} & a_{11,6} & a_{11,7} & a_{11,8} & \cdots \\
a_{12,1} & a_{12,2} & a_{12,3} & a_{12,4} & a_{12,5} & a_{12,6} & a_{12,7} & a_{12,8} & \cdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots
\end{array}
$$

$$
\begin{array}{ccccccccc}
a_{1,1} & a_{1,2} & a_{1,3} & a_{1,4} & a_{1,5} & a_{1,6} & a_{1,7} & a_{1,8} & \cdots \\
a_{2,1} & a_{2,2} & a_{2,3} & a_{2,4} & a_{2,5} & a_{2,6} & a_{2,7} & a_{2,8} & \cdots \\
a_{3,1} & a_{3,2} & a_{3,3} & a_{3,4} & a_{3,5} & a_{3,6} & a_{3,7} & a_{3,8} & \cdots \\
a_{4,1} & a_{4,2} & a_{4,3} & a_{4,4} & a_{4,5} & a_{4,6} & a_{4,7} & a_{4,8} & \cdots \\
a_{5,1} & a_{5,2} & a_{5,3} & a_{5,4} & a_{5,5} & a_{5,6} & a_{5,7} & a_{5,8} & \cdots \\
a_{6,1} & a_{6,2} & a_{6,3} & a_{6,4} & a_{6,5} & a_{6,6} & a_{6,7} & a_{6,8} & \cdots \\
a_{7,1} & a_{7,2} & a_{7,3} & a_{7,4} & a_{7,5} & a_{7,6} & a_{7,7} & a_{7,8} & \cdots \\
a_{8,1} & a_{8,2} & a_{8,3} & a_{8,4} & a_{8,5} & a_{8,6} & a_{8,7} & a_{8,8} & \cdots \\
a_{9,1} & a_{9,2} & a_{9,3} & a_{9,4} & a_{9,5} & a_{9,6} & a_{9,7} & a_{9,8} & \cdots \\
a_{10,1} & a_{10,2} & a_{10,3} & a_{10,4} & a_{10,5} & a_{10,6} & a_{10,7} & a_{10,8} & \cdots \\
a_{11,1} & a_{11,2} & a_{11,3} & a_{11,4} & a_{11,5} & a_{11,6} & a_{11,7} & a_{11,8} & \cdots \\
a_{12,1} & a_{12,2} & a_{12,3} & a_{12,4} & a_{12,5} & a_{12,6} & a_{12,7} & a_{12,8} & \cdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots
\end{array}
$$

$$
\begin{array}{|cccccccc|c}
a_{1,1} & a_{1,2} & a_{1,3} & a_{1,4} & a_{1,5} & a_{1,6} & a_{1,7} & a_{1,8} & \cdots \\
a_{2,1} & a_{2,2} & a_{2,3} & a_{2,4} & a_{2,5} & a_{2,6} & a_{2,7} & a_{2,8} & \cdots \\
a_{3,1} & a_{3,2} & a_{3,3} & a_{3,4} & a_{3,5} & a_{3,6} & a_{3,7} & a_{3,8} & \cdots \\
a_{4,1} & a_{4,2} & a_{4,3} & a_{4,4} & a_{4,5} & a_{4,6} & a_{4,7} & a_{4,8} & \cdots \\
a_{5,1} & a_{5,2} & a_{5,3} & a_{5,4} & a_{5,5} & a_{5,6} & a_{5,7} & a_{5,8} & \cdots \\
a_{6,1} & a_{6,2} & a_{6,3} & a_{6,4} & a_{6,5} & a_{6,6} & a_{6,7} & a_{6,8} & \cdots \\
a_{7,1} & a_{7,2} & a_{7,3} & a_{7,4} & a_{7,5} & a_{7,6} & a_{7,7} & a_{7,8} & \cdots \\
a_{8,1} & a_{8,2} & a_{8,3} & a_{8,4} & a_{8,5} & a_{8,6} & a_{8,7} & a_{8,8} & \cdots \\
\multicolumn{1}{c}{a_{9,1}} & a_{9,2} & a_{9,3} & a_{9,4} & a_{9,5} & a_{9,6} & a_{9,7} & \multicolumn{1}{c}{a_{9,8}} & \cdots \\
\multicolumn{1}{c}{a_{10,1}} & a_{10,2} & a_{10,3} & a_{10,4} & a_{10,5} & a_{10,6} & a_{10,7} & \multicolumn{1}{c}{a_{10,8}} & \cdots \\
\multicolumn{1}{c}{a_{11,1}} & a_{11,2} & a_{11,3} & a_{11,4} & a_{11,5} & a_{11,6} & a_{11,7} & \multicolumn{1}{c}{a_{11,8}} & \cdots \\
\multicolumn{1}{c}{a_{12,1}} & a_{12,2} & a_{12,3} & a_{12,4} & a_{12,5} & a_{12,6} & a_{12,7} & \multicolumn{1}{c}{a_{12,8}} & \cdots \\
\multicolumn{1}{c}{\vdots} & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \multicolumn{1}{c}{\vdots} & \ddots
\end{array}
$$

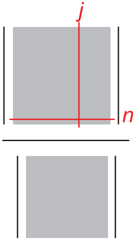
How to certify a determinant identity

How to certify a determinant identity

Assume that $\det((a_{i,j}))_{i,j=1}^{n} \stackrel{?}{=} b_n \ (\neq 0)$ is indeed true.

How to certify a determinant identity

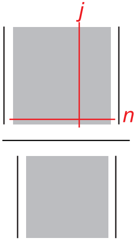
Assume that $\det((a_{i,j}))_{i,j=1}^{n} \stackrel{?}{=} b_n \; (\neq 0)$ is indeed true.

Define $c_{n,j} := (-1)^{n+j}$ 

for $j = 1, \ldots, n$.

How to certify a determinant identity

Assume that $\det((a_{i,j}))_{i,j=1}^{n} \stackrel{?}{=} b_n \ (\neq 0)$ is indeed true.

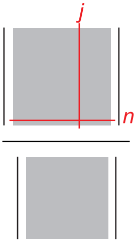
Define $c_{n,j} := (-1)^{n+j}$ 

for $j = 1, \ldots, n$.

Then:

How to certify a determinant identity

Assume that $\det((a_{i,j}))_{i,j=1}^{n} \stackrel{?}{=} b_n \ (\neq 0)$ is indeed true.

Define $c_{n,j} := (-1)^{n+j}$ 

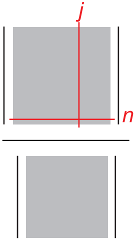
for $j = 1, \ldots, n$.

Then:

$$c_{n,n} = 1$$

How to certify a determinant identity

Assume that $\det((a_{i,j}))_{i,j=1}^{n} \stackrel{?}{=} b_n$ $(\neq 0)$ is indeed true.

Define $c_{n,j} := (-1)^{n+j}$ 

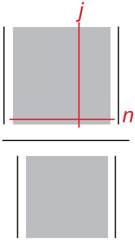
for $j = 1, \ldots, n$.

Then:

$$= b_{n-1} \sum_{j=1}^{n} a_{n,j} c_{n,j} = b_n.$$

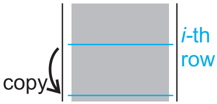
How to certify a determinant identity

Assume that $\det((a_{i,j}))_{i,j=1}^{n} \stackrel{?}{=} b_n \ (\neq 0)$ is indeed true.

Define $c_{n,j} := (-1)^{n+j}$ 

for $j = 1, \ldots, n$.

Then:



$= b_{n-1} \sum_{j=1}^{n} a_{i,j} c_{n,j} = 0.$

How to certify a determinant identity

The $c_{n,j}$ satisfy the linear system

$$\begin{pmatrix} a_{1,1} & \cdots & a_{1,n-1} & a_{1,n} \\ \vdots & \ddots & \vdots & \vdots \\ a_{n-1,1} & \cdots & a_{n-1,n-1} & a_{n-1,n} \\ 0 & \cdots & 0 & 1 \end{pmatrix} \begin{pmatrix} c_{n,1} \\ \vdots \\ c_{n,n-1} \\ c_{n,n} \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}.$$

How to certify a determinant identity

The $c_{n,j}$ satisfy the linear system

$$\begin{pmatrix} a_{1,1} & \cdots & a_{1,n-1} & a_{1,n} \\ \vdots & \ddots & \vdots & \vdots \\ a_{n-1,1} & \cdots & a_{n-1,n-1} & a_{n-1,n} \\ 0 & \cdots & 0 & 1 \end{pmatrix} \begin{pmatrix} c_{n,1} \\ \vdots \\ c_{n,n-1} \\ c_{n,n} \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}.$$

This system has a *unique solution.*

How to certify a determinant identity

The $c_{n,j}$ satisfy the linear system

$$\begin{pmatrix} a_{1,1} & \cdots & a_{1,n-1} & a_{1,n} \\ \vdots & \ddots & \vdots & \vdots \\ a_{n-1,1} & \cdots & a_{n-1,n-1} & a_{n-1,n} \\ 0 & \cdots & 0 & 1 \end{pmatrix} \begin{pmatrix} c_{n,1} \\ \vdots \\ c_{n,n-1} \\ c_{n,n} \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}.$$

This system has a *unique solution.*

The reasoning can therefore be put *upside down:*

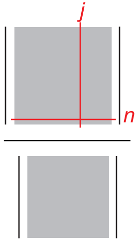
How to certify a determinant identity

If $c_{n,j}$ is such that *(1)* $c_{n,n} = 1$ and *(2)* $\sum_{j=1}^{n} a_{i,j} c_{n,j} = 0 \; (i < n)$,

How to certify a determinant identity

If $c_{n,j}$ is such that *(1)* $c_{n,n} = 1$ and *(2)* $\sum_{j=1}^{n} a_{i,j} c_{n,j} = 0$ $(i < n)$, then

$$c_{n,j} = (-1)^{n+j}$$

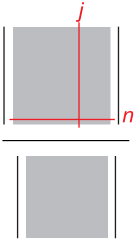


$$(j = 1, \ldots, n).$$

How to certify a determinant identity

If $c_{n,j}$ is such that *(1)* $c_{n,n} = 1$ and *(2)* $\sum_{j=1}^{n} a_{i,j} c_{n,j} = 0$ $(i < n)$, then

$$c_{n,j} = (-1)^{n+j}$$



$$(j = 1, \ldots, n).$$

If in addition

$$\text{(3)} \quad \sum_{j=1}^{n} a_{n,j} c_{n,j} = \frac{b_n}{b_{n-1}},$$

then $\det((a_{i,j}))_{i,j=1}^{n} = b_n$.

How to certify a determinant identity

A function $c_{n,j}$ satisfying *(1)*, *(2)*, *(3)* certifies the determinant identity $\det((a_{i,j}))_{i,j=1}^{n} = b_n$.

How to certify a determinant identity

$$\boxed{\text{A function } c_{n,j} \text{ satisfying } \textit{(1)}, \textit{(2)}, \textit{(3)} \text{ certifies the determinant identity } \det((a_{i,j}))_{i,j=1}^{n} = b_n.}$$

Note:

How to certify a determinant identity

> A function $c_{n,j}$ satisfying *(1)*, *(2)*, *(3)* certifies the determinant identity $\det((a_{i,j}))_{i,j=1}^{n} = b_n$.

Note:

- $a_{i,j}$ and b_n can be described by recurrence equations.

How to certify a determinant identity

$\boxed{\text{A function } c_{n,j} \text{ satisfying } \textit{(1)}, \textit{(2)}, \textit{(3)} \text{ certifies the determinant identity } \det((a_{i,j}))_{i,j=1}^{n} = b_n.}$

Note:

- $a_{i,j}$ and b_n can be described by recurrence equations.
- If there is also a recursive description of $c_{n,j}$, then proving *(1)*, *(2)*, *(3)* is “routine”.

How to certify a determinant identity

> A function $c_{n,j}$ satisfying *(1)*, *(2)*, *(3)* certifies the determinant identity $\det((a_{i,j}))_{i,j=1}^{n} = b_n$.

Note:

- $a_{i,j}$ and b_n can be described by recurrence equations.
- If there is also a recursive description of $c_{n,j}$, then proving *(1)*, *(2)*, *(3)* is "routine".
- How to discover a recursive description for $c_{n,j}$?

How to certify a determinant identity

> A function $c_{n,j}$ satisfying *(1)*, *(2)*, *(3)* certifies the determinant identity $\det((a_{i,j}))_{i,j=1}^{n} = b_n$.

Note:

- $a_{i,j}$ and b_n can be described by recurrence equations.
- If there is also a recursive description of $c_{n,j}$, then proving *(1)*, *(2)*, *(3)* is "routine".
- How to discover a recursive description for $c_{n,j}$?
- Compute $c_{n,j}$ explicity for $1 \leq j \leq n \leq 500$, say, and construct recurrence equations fitting this data.

How to certify a determinant identity

A function $c_{n,j}$ satisfying *(1)*, *(2)*, *(3)* certifies the determinant identity $\det((a_{i,j}))_{i,j=1}^{n} = b_n$.

Note:

- $a_{i,j}$ and b_n can be described by recurrence equations.
- If there is also a recursive description of $c_{n,j}$, then proving *(1)*, *(2)*, *(3)* is "routine".
- How to discover a recursive description for $c_{n,j}$?
- Compute $c_{n,j}$ explicity for $1 \leq j \leq n \leq 500$, say, and construct recurrence equations fitting this data.
- Then offer these recurrence equations as a definition for $c_{n,j}$.

End of story?

End of story?

- The defining equations for $c_{n,j}$ are *30 Megabytes* big.

End of story?

- The defining equations for $c_{n,j}$ are *30 Megabytes* big.
- Checking *(1)*, *(2)*, *(3)* is no problem in theory.

End of story?

- The defining equations for $c_{n,j}$ are *30 Megabytes* big.
- Checking *(1)*, *(2)*, *(3)* is no problem in theory.
- But it is quite a computational challenge.

End of story?

- The defining equations for $c_{n,j}$ are *30 Megabytes* big.
- Checking *(1)*, *(2)*, *(3)* is no problem in theory.
- But it is quite a computational challenge.
- A referee might not be willing (or able) to do this.

End of story?

- The defining equations for $c_{n,j}$ are *30 Megabytes* big.
- Checking *(1)*, *(2)*, *(3)* is no problem in theory.
- But it is quite a computational challenge.
- A referee might not be willing (or able) to do this.
- *Idea:* Provide certificates that $c_{n,j}$ satisfies *(1)*, *(2)*, *(3)*.

End of story?

- The defining equations for $c_{n,j}$ are *30 Megabytes* big.
- Checking *(1)*, *(2)*, *(3)* is no problem in theory.
- But it is quite a computational challenge.
- A referee might not be willing (or able) to do this.
- *Idea:* Provide certificates that $c_{n,j}$ satisfies *(1)*, *(2)*, *(3)*.
- Computing such certificates is even more painful.

End of story?

- The defining equations for $c_{n,j}$ are *30 Megabytes* big.
- Checking *(1)*, *(2)*, *(3)* is no problem in theory.
- But it is quite a computational challenge.
- A referee might not be willing (or able) to do this.
- *Idea:* Provide certificates that $c_{n,j}$ satisfies *(1)*, *(2)*, *(3)*.
- Computing such certificates is even more painful.
- But checking them is reasonably cheap.

End of story?

- The defining equations for $c_{n,j}$ are *30 Megabytes* big.
- Checking *(1)*, *(2)*, *(3)* is no problem in theory.
- But it is quite a computational challenge.
- A referee might not be willing (or able) to do this.
- *Idea:* Provide certificates that $c_{n,j}$ satisfies *(1)*, *(2)*, *(3)*.
- Computing such certificates is even more painful.
- But checking them is reasonably cheap.
- We managed to provide such certificates.

End of story?

- The defining equations for $c_{n,j}$ are *30 Megabytes* big.
- Checking *(1)*, *(2)*, *(3)* is no problem in theory.
- But it is quite a computational challenge.
- A referee might not be willing (or able) to do this.
- *Idea:* Provide certificates that $c_{n,j}$ satisfies *(1)*, *(2)*, *(3)*.
- Computing such certificates is even more painful.
- But checking them is reasonably cheap.
- We managed to provide such certificates.
- The biggest of them is *7 Gigabytes* big.

The Computational Challenge

Expected runtime with a naive algorithm:

The Computational Challenge

Expected runtime with a naive algorithm: 4.5 Mio years

The Computational Challenge

Expected runtime with a naive algorithm: 4.5 Mio years

- Use homomorphic images
  $\mathbb{Q}(q, q^n, q^j) \to \mathbb{Q} \to \mathbb{Z}_p \to \mathbb{Q} \to \mathbb{Q}(q, q^n, q^j)$.

The Computational Challenge

Expected runtime with a naive algorithm: 4.5 Mio years

- Use homomorphic images
  $\mathbb{Q}(q, q^n, q^j) \to \mathbb{Q} \to \mathbb{Z}_p \to \mathbb{Q} \to \mathbb{Q}(q, q^n, q^j)$.
- Use an optimized ansatz for the shape of the certificate.

The Computational Challenge

Expected runtime with a naive algorithm: 4.5 Mio years

- Use homomorphic images
  $\mathbb{Q}(q, q^n, q^j) \to \mathbb{Q} \to \mathbb{Z}_p \to \mathbb{Q} \to \mathbb{Q}(q, q^n, q^j)$.
- Use an optimized ansatz for the shape of the certificate.
- Use plausible guesses for the denominators in the certificate and only compute the numerators.

The Computational Challenge

Expected runtime with a naive algorithm: 4.5 Mio years

- Use homomorphic images
  $\mathbb{Q}(q, q^n, q^j) \to \mathbb{Q} \to \mathbb{Z}_p \to \mathbb{Q} \to \mathbb{Q}(q, q^n, q^j)$.
- Use an optimized ansatz for the shape of the certificate.
- Use plausible guesses for the denominators in the certificate and only compute the numerators.
- Use a fine tuned implementation with lots of technical refinements.

The Computational Challenge

Expected runtime with a naive algorithm: 4.5 Mio years

- Use homomorphic images
  $\mathbb{Q}(q, q^n, q^j) \to \mathbb{Q} \to \mathbb{Z}_p \to \mathbb{Q} \to \mathbb{Q}(q, q^n, q^j)$.
- Use an optimized ansatz for the shape of the certificate.
- Use plausible guesses for the denominators in the certificate and only compute the numerators.
- Use a fine tuned implementation with lots of technical refinements.
- Use parallel hardware with big memory and fast CPUs.

The Computational Challenge

Expected runtime with a naive algorithm: 4.5 Mio years

- Use homomorphic images
  $\mathbb{Q}(q, q^n, q^j) \to \mathbb{Q} \to \mathbb{Z}_p \to \mathbb{Q} \to \mathbb{Q}(q, q^n, q^j)$.
- Use an optimized ansatz for the shape of the certificate.
- Use plausible guesses for the denominators in the certificate and only compute the numerators.
- Use a fine tuned implementation with lots of technical refinements.
- Use parallel hardware with big memory and fast CPUs.

Expected runtime with a clever algorithm:

The Computational Challenge

Expected runtime with a naive algorithm: 4.5 Mio years

- Use homomorphic images
  $\mathbb{Q}(q, q^n, q^j) \to \mathbb{Q} \to \mathbb{Z}_p \to \mathbb{Q} \to \mathbb{Q}(q, q^n, q^j)$.
- Use an optimized ansatz for the shape of the certificate.
- Use plausible guesses for the denominators in the certificate and only compute the numerators.
- Use a fine tuned implementation with lots of technical refinements.
- Use parallel hardware with big memory and fast CPUs.

Expected runtime with a clever algorithm: 20 days