The beneficial use of homomorphic images in computer algebra

Christoph Koutschan

Tulane University
New Orleans, LA

June 18, 2010

Homomorphic images

Problem involves computations in some domain D
(typically a ring or field)

$$\begin{array}{ccc} \text{Problem in } D & \longrightarrow & \text{Solution in } D \\ \text{hom} \downarrow & & (\uparrow \text{ lift}) \\ \text{Problem in } \tilde{D} & \longrightarrow & \text{Solution in } \tilde{D} \end{array}$$

Homomorphism is typically not injective.

Applications

In general:

- prediction
- proof of non-existence
- compute results by lifting

In particular:

- solving linear systems
- computing determinants
- rational solutions of difference equations
- symbolic summation / integration
- guessing recurrences
- and many more

Homomorphism $\mathbb{Q} \longrightarrow \mathbb{Z}_p$

Integers are reduced modulo p.
Lifting can be done via chinese remaindering.

Example:

$$x \equiv 0 \mod 7 \qquad x \equiv 9 \mod 11$$

$$x = 7m, m \in \mathbb{Z}$$

$$7m \equiv 9 \mod 11$$

$$8 \cdot 7m \equiv 8 \cdot 9 \mod 11$$

$$m \equiv 6 \mod 11$$

$$x \equiv 42 \mod 77$$

Homomorphism $\mathbb{Q} \to \mathbb{Z}_p$

What is $\frac{5}{8}$ modulo 89?
Extended Euclidean Algorithm with 89 and 8:

$$\begin{aligned} 89 &= 1 \cdot 89 + 0 \cdot 8 \\ 8 &= 0 \cdot 89 + 1 \cdot 8 \\ 1 &= 1 \cdot 89 + -11 \cdot 8 \end{aligned}$$

Hence $\frac{1}{8} \equiv -11 \mod 89$ and therefore

$$\frac{5}{8} \equiv -55 \equiv 34 \mod 89.$$

Rational Reconstruction

Extended Euclidean Algorithm with 89 and 34:

r	s	t
89	1	0
34	0	1
21	1	-2
13	-1	3
8	2	-5
5	-3	8
3	5	-13
2	-8	21
1	13	-34
0	-34	89

Invariant: $r = s \cdot 89 + t \cdot 34$.

Hence $r/t \equiv 34 \mod 89$ for every row.

Which row to choose?

Here is another example (mod 2147483629):

r	s	t
57012824	1	-5
19004393	-7	36
19004038	15	-77
355	-22	113
178	1177719	-6049193
177	-1177741	6049306
1	2355460	-12098499
0	-418094161	2147483629

Insertion Homomorphism

For example: $\mathbb{Q}(x) \to \mathbb{Q}$, $x \mapsto n, n \in \mathbb{N}$, corresponds to modular computation modulo the linear polynomial $x - n$.
Lifting can be done via polynomial interpolation and rational function reconstruction.

Both homomorphisms can be combined.
For lifting: the order matters!

HolonomicFunctions

Prove the following identity:

$$\int_0^\infty x^{\mu-1}\sin(ax)\exp\left(-\beta x^2-\gamma x\right)\,dx =$$
$$-\frac{i}{2(2\beta)^{\mu/2}}\left(\Gamma(\mu)\exp\left(\frac{\gamma^2-a^2}{8\beta}\right)\left(\exp\left(-\frac{ia\gamma}{4\beta}\right)D_{-\mu}\left(\frac{\gamma-ia}{\sqrt{2\beta}}\right)\right.\right.$$
$$\left.\left.-\exp\left(\frac{ia\gamma}{4\beta}\right)D_{-\mu}\left(\frac{\gamma+ia}{\sqrt{2\beta}}\right)\right)\right)$$

where $D_\mu(x)$ is the parabolic cylinder function.

Abramov's algorithm

"Rational solutions of linear difference and q-difference equations with polynomial coefficients"

$$a_n(x)y(x+n) + a_{n-1}(x)y(x+n-1) + \cdots + a_0(x)y(x) = b(x)$$

Set $A(x) = a_n(x-n)$, $B(x) = a_0(x)$.

input: nonzero polynomials $A(x), B(x)$
output: a polynomial $u(x)$

$u(x) := 1;$
$R(m) := Res_x(A(x), B(x+m));$
if $R(m)$ has some nonnegative integer root **then**
  $N :=$ the largest nonnegative integer root of $R(m);$
  for $i = 0, 1, ..., N$ **do**
    $d(x) := gcd(A(x), B(x+i));$
    $A(x) := A(x)/d(x);$
    $B(x) := B(x)/d(x-i);$
    $u(x) := u(x)d(x)d(x-1)\ldots d(x-i)$
  od
fi.


The Pekeris project

CK and Doron Zeilberger: "The 1958 Pekeris-Accad-WEIZAC Ground-Breaking Collaboration that computed Ground States of Two-Electron Atoms (and its 2010 Redux)"

Recall the (time-independent) Schrödinger equation for the wave function $\psi = \psi(x_1, y_1, z_1, x_2, y_2, z_2)$ of a two-electron atom

$$\left(\frac{\partial^2}{\partial x_1^2}+\frac{\partial^2}{\partial y_1^2}+\frac{\partial^2}{\partial z_1^2}+\frac{\partial^2}{\partial x_2^2}+\frac{\partial^2}{\partial y_2^2}+\frac{\partial^2}{\partial z_2^2}+2\left(E+\frac{Z}{r_1}+\frac{Z}{r_2}-\frac{1}{r_{12}}\right)\right)\psi = 0$$

where Z denotes the nuclear charge, E the energy of the system, and r_1, r_2 are the distances of the electrons from the nucleus, and r_{12} is their mutual distance.

Guessing

Example: Guess a recurrence for $f_{n,k} = \binom{n}{k}$.

Ansatz with undetermined coefficients $x_{i,j}$:

$$(x_{0,1} + x_{0,2}k + x_{0,3}n)\, f_{n,k} + (x_{1,1} + x_{1,2}k + x_{1,3}n)\, f_{n+1,k}$$

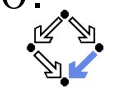
Plug in concrete values:

$$\begin{aligned}
n = 1,\ k = 1: &\quad x_{0,1} + x_{0,2} + x_{0,3} + 2\,(x_{1,1} + x_{1,2} + x_{1,3}) = 0 \\
n = 2,\ k = 1: &\quad 2\,(x_{0,1} + x_{0,2} + 2x_{0,3}) + 3\,(x_{1,1} + x_{1,2} + 2x_{1,3}) = 0 \\
n = 3,\ k = 1: &\quad 3\,(x_{0,1} + x_{0,2} + 3x_{0,3}) + 4\,(x_{1,1} + x_{1,2} + 3x_{1,3}) = 0 \\
n = 1,\ k = 2: &\quad x_{1,1} + 2x_{1,2} + x_{1,3} = 0 \\
n = 2,\ k = 2: &\quad x_{0,1} + 2x_{0,2} + 2x_{0,3} + 3\,(x_{1,1} + 2x_{1,2} + 2x_{1,3}) = 0 \\
n = 3,\ k = 2: &\quad 3\,(x_{0,1} + 2x_{0,2} + 3x_{0,3}) + 6\,(x_{1,1} + 2x_{1,2} + 3x_{1,3}) = 0
\end{aligned}$$

Solve this linear system:

$$x_{0,1} = -C, x_{0,2} = 0, x_{0,3} = -C, x_{1,1} = C, x_{1,2} = -C, x_{1,3} = C$$

Found the recurrence $(-C - nC)f_{n,k} + (C - kC + Cn)f_{n+1,k} = 0$.



Proof of Gessel's conjecture

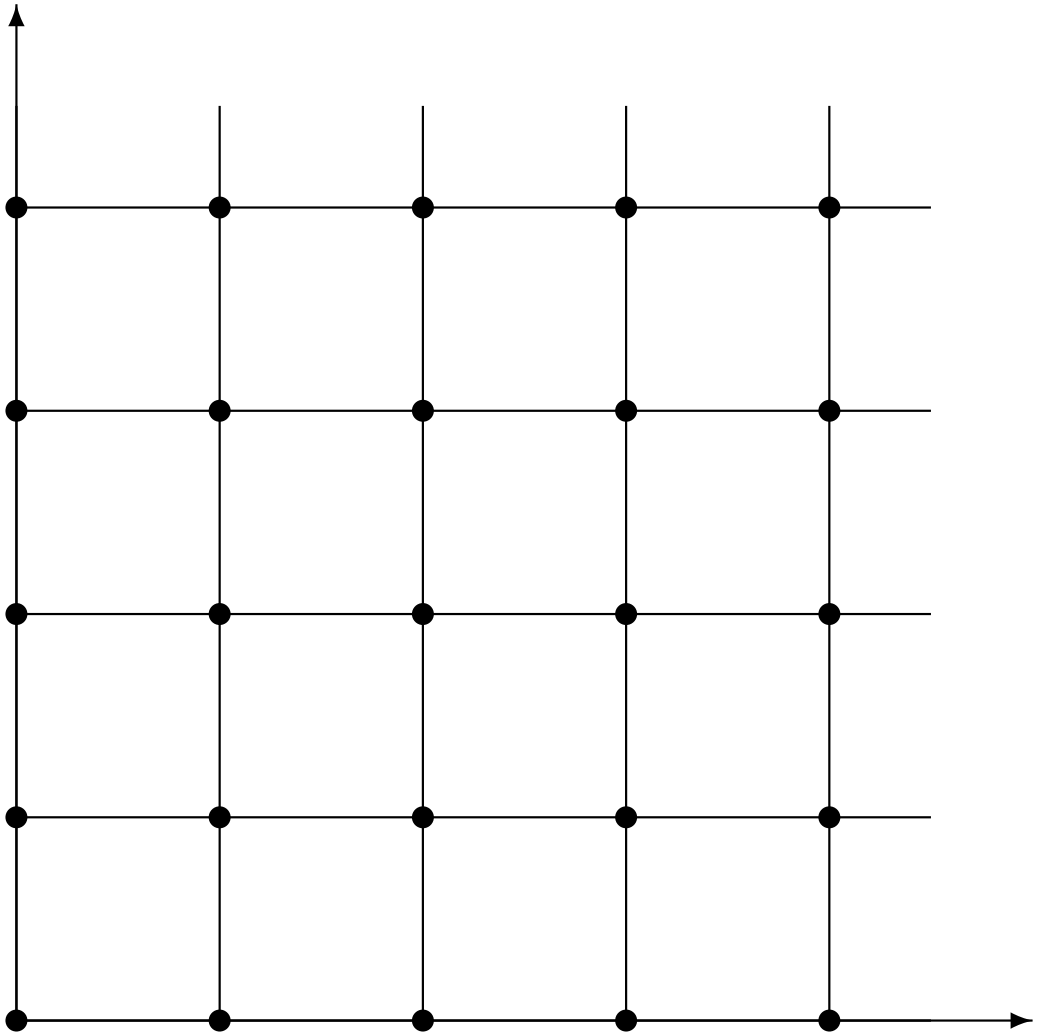
(joint work with M. Kauers and D. Zeilberger)

Let $f(n;0,0)$ count the number of closed Gessel walks (walks in $\mathbb{N}^2$ starting at $(0,0)$ using only the steps E,W,NE,SW.

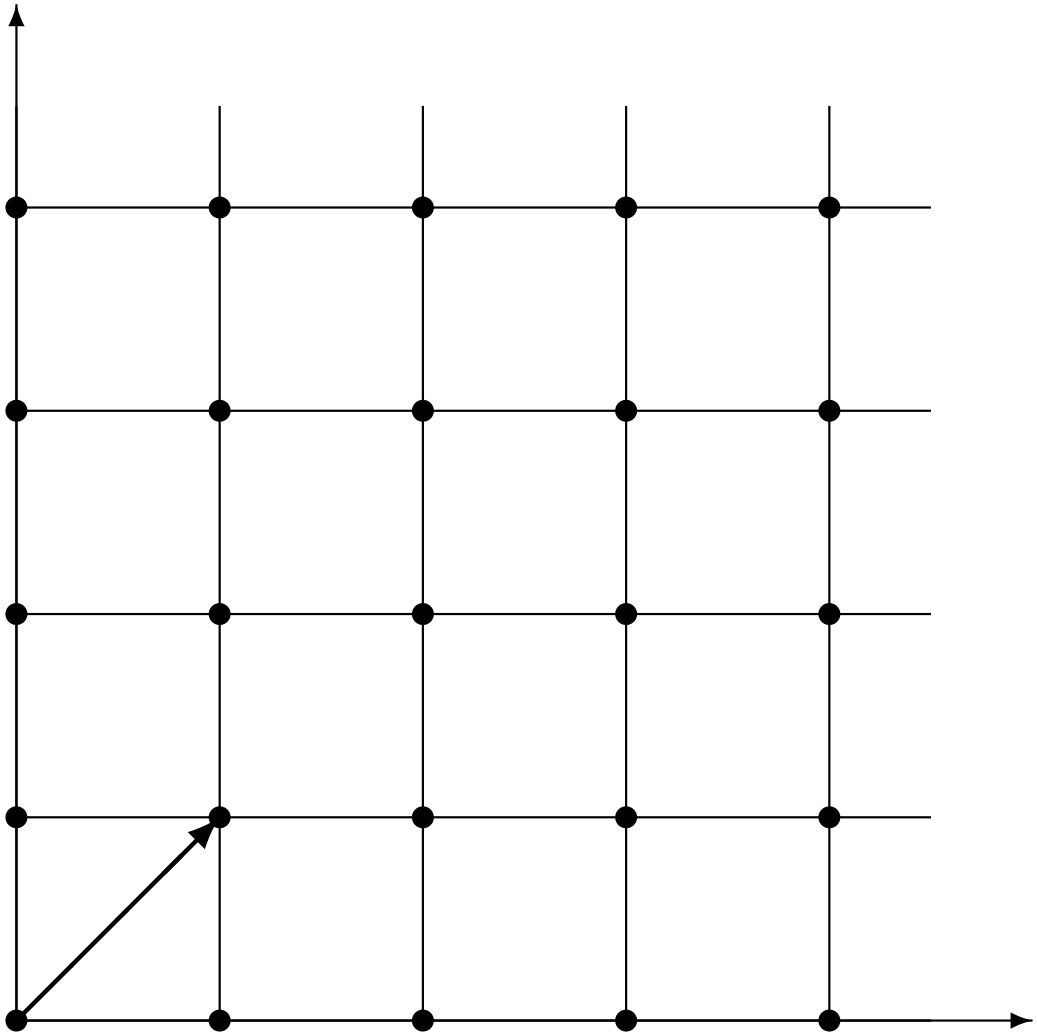
Ira Gessel in 2001 conjectured that

$$f(n;0,0) = \begin{cases} 16^k \frac{(5/6)_k (1/2)_k}{(2)_k (5/3)_k} & \text{if } n = 2k \\ 0 & \text{if } n \text{ is odd} \end{cases}$$

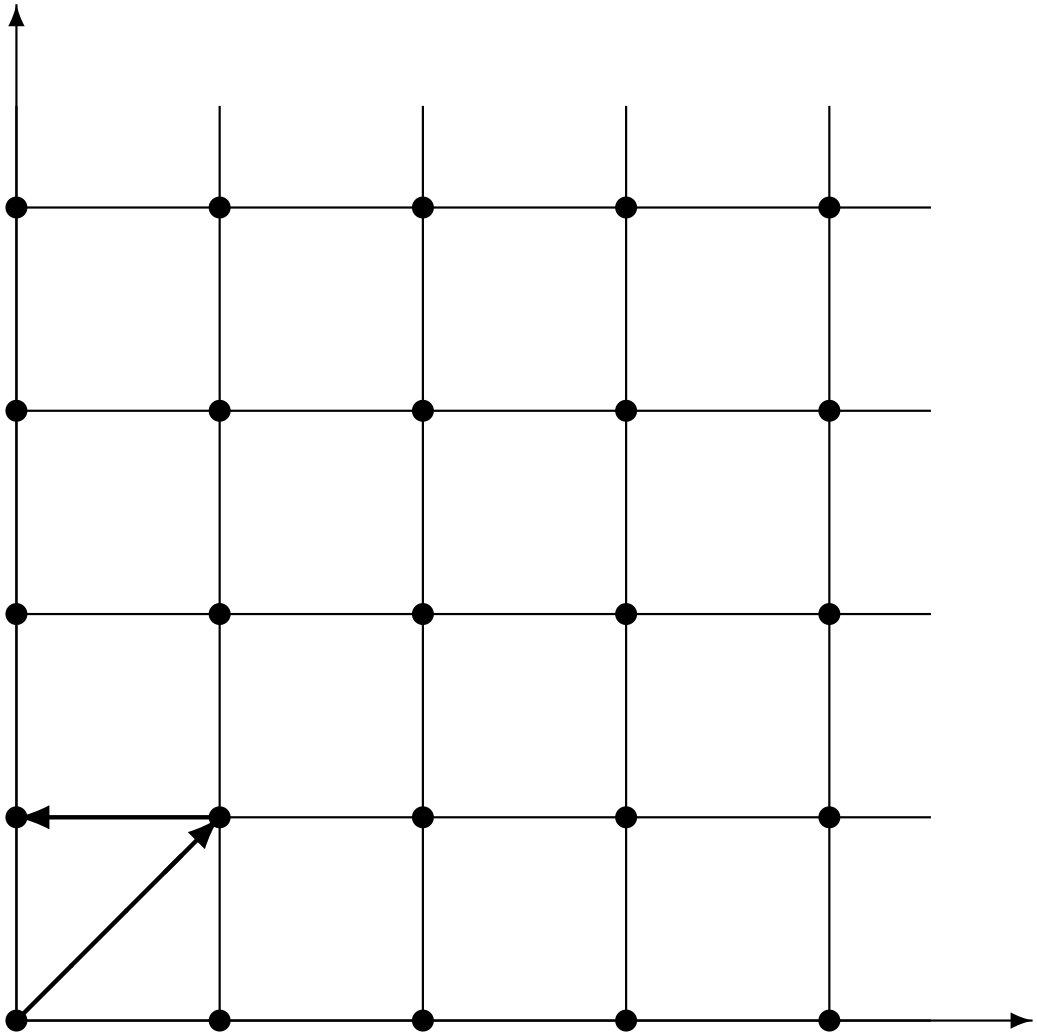
Gessel walks — Example



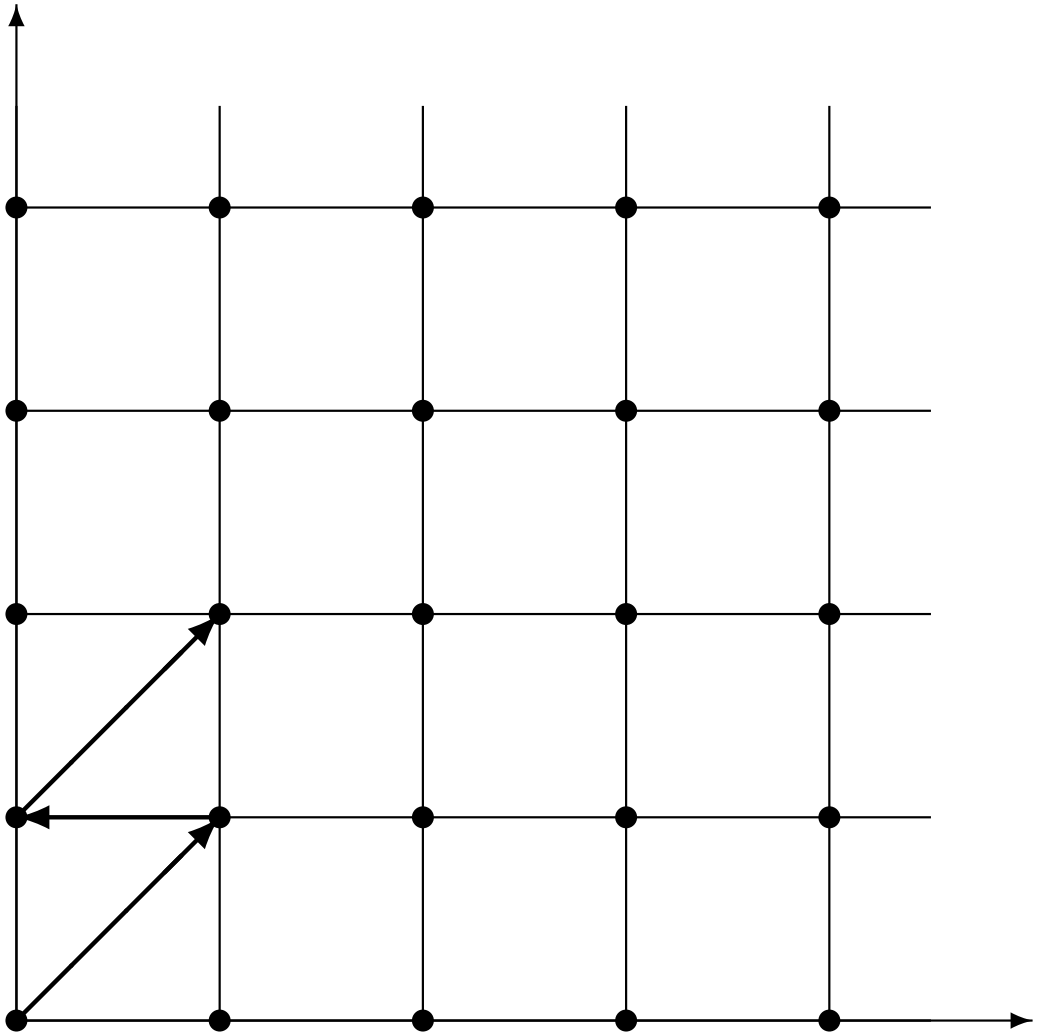
Gessel walks — Example



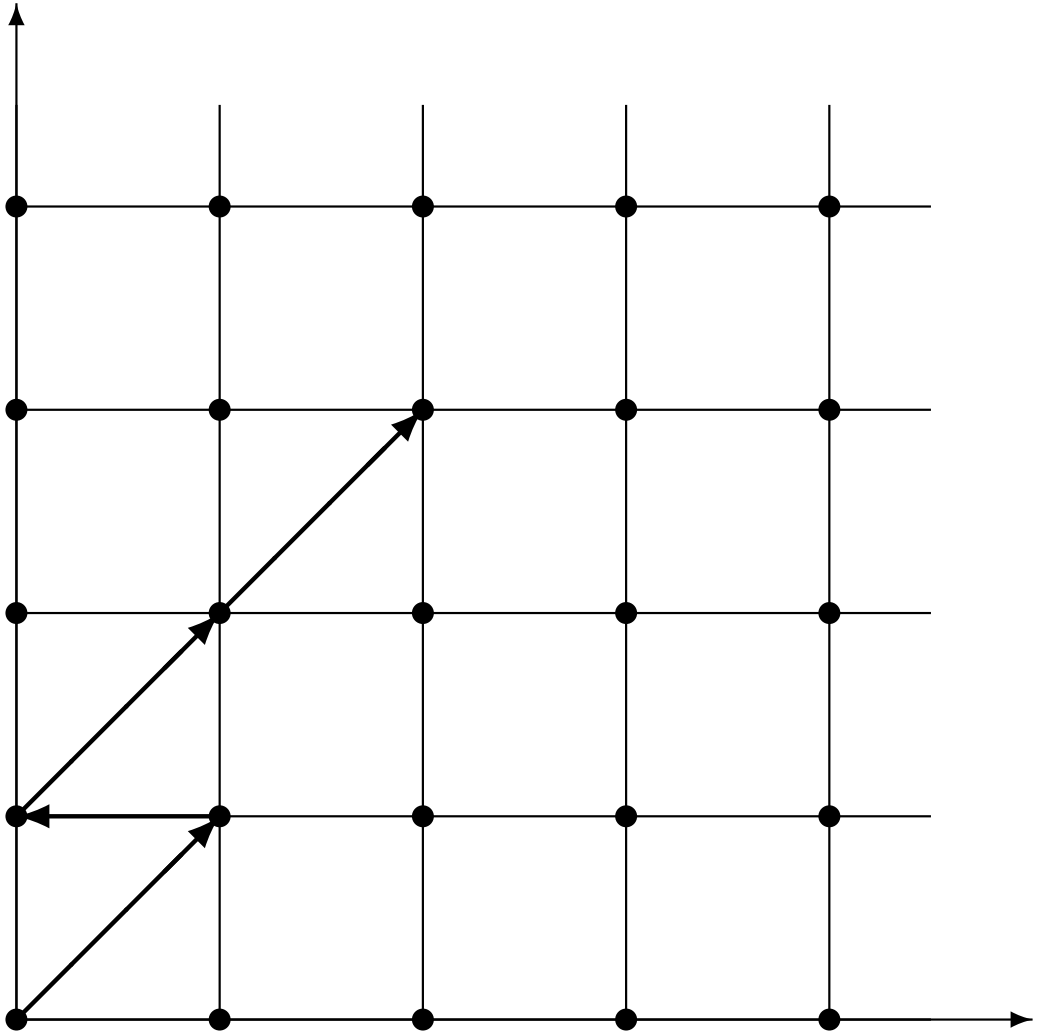
Gessel walks — Example



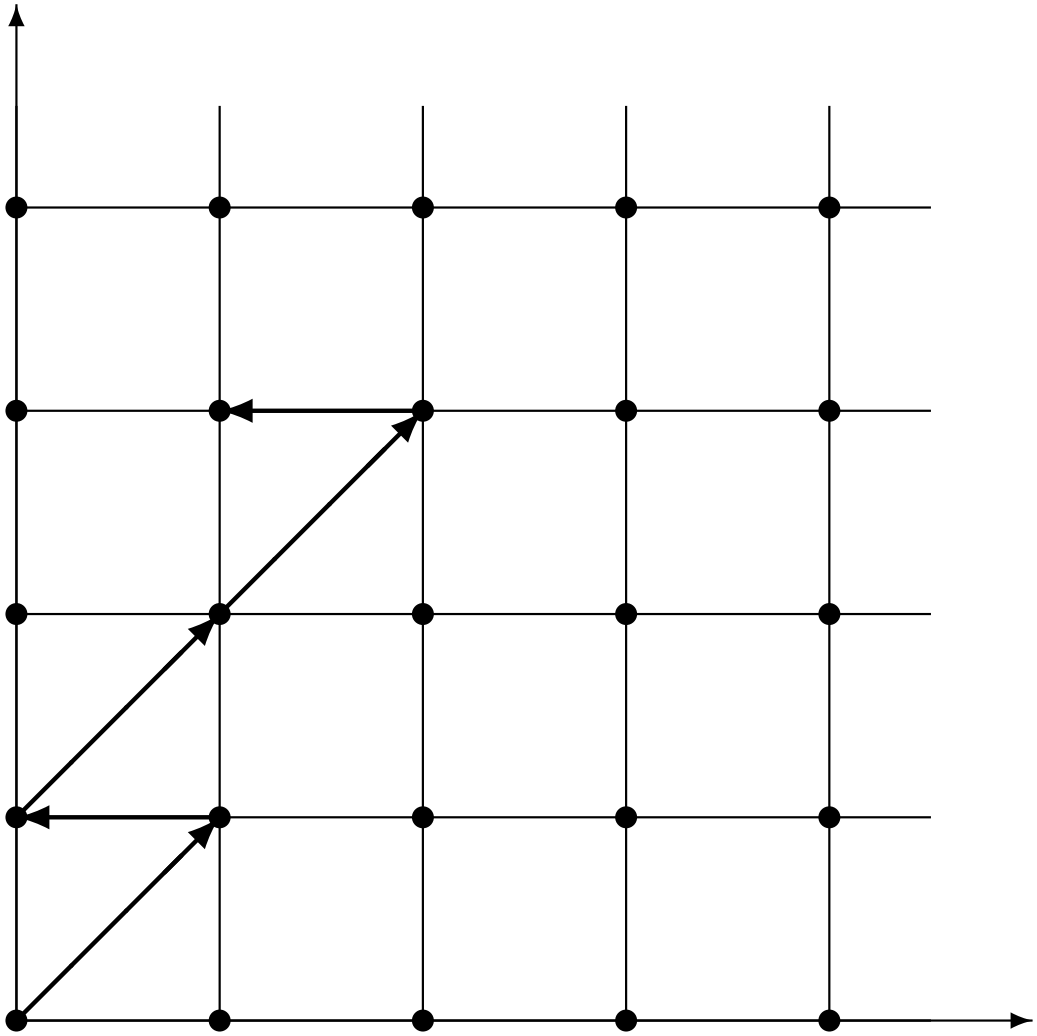
Gessel walks — Example



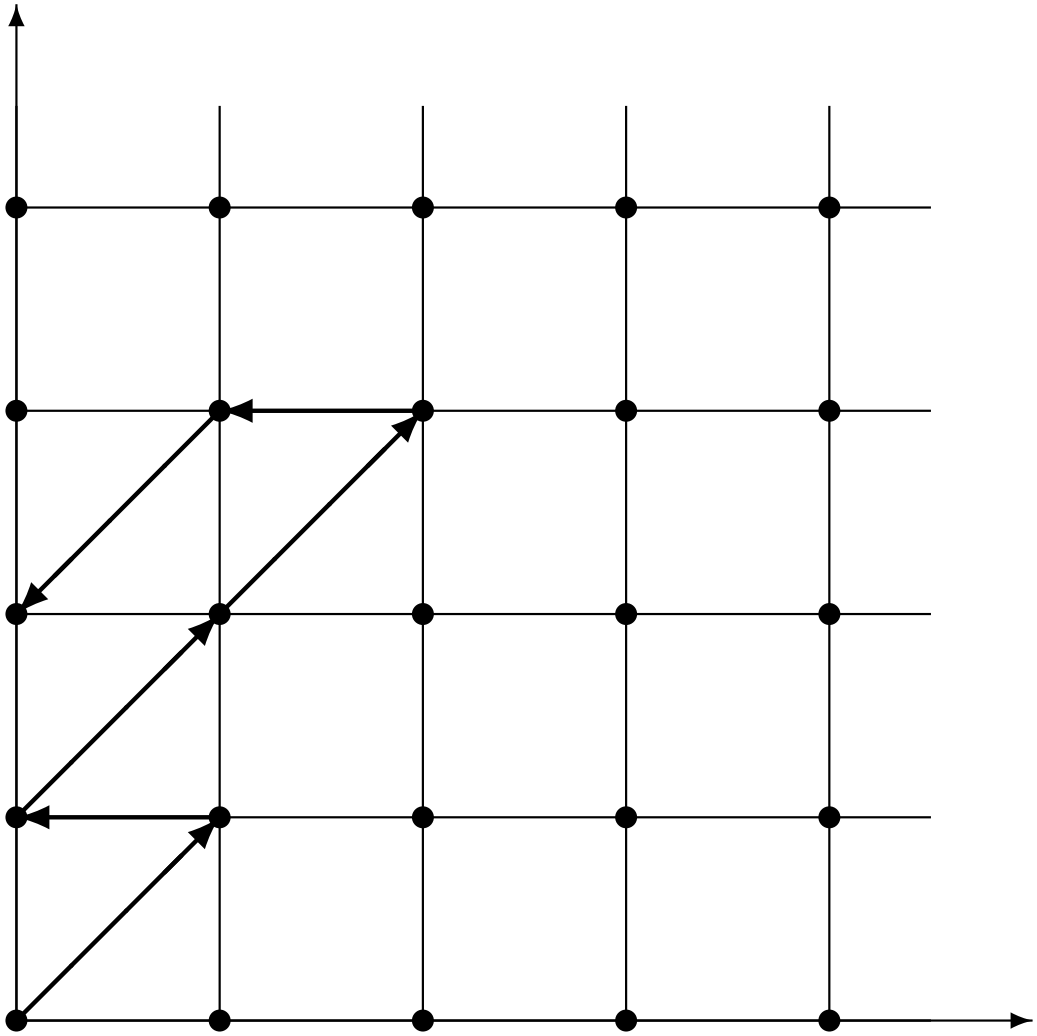
Gessel walks — Example



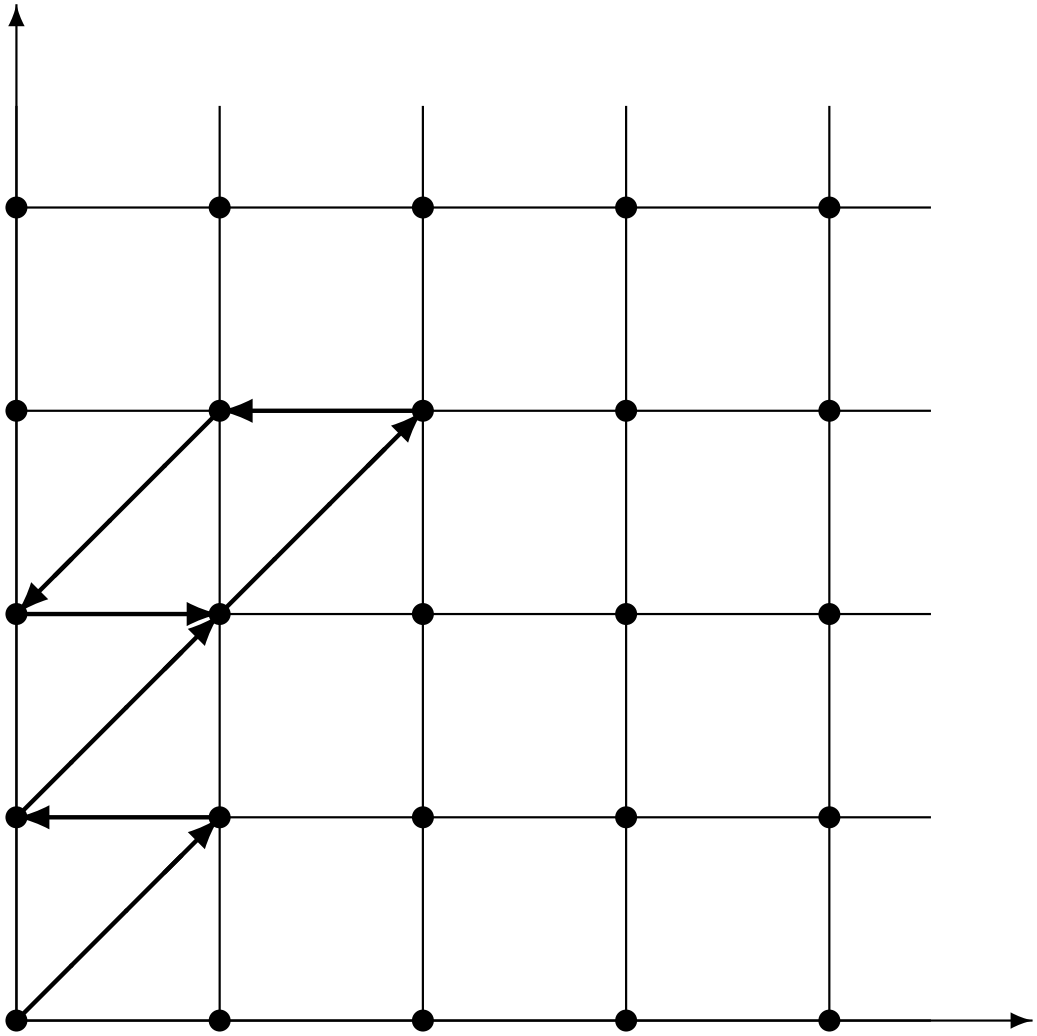
Gessel walks — Example



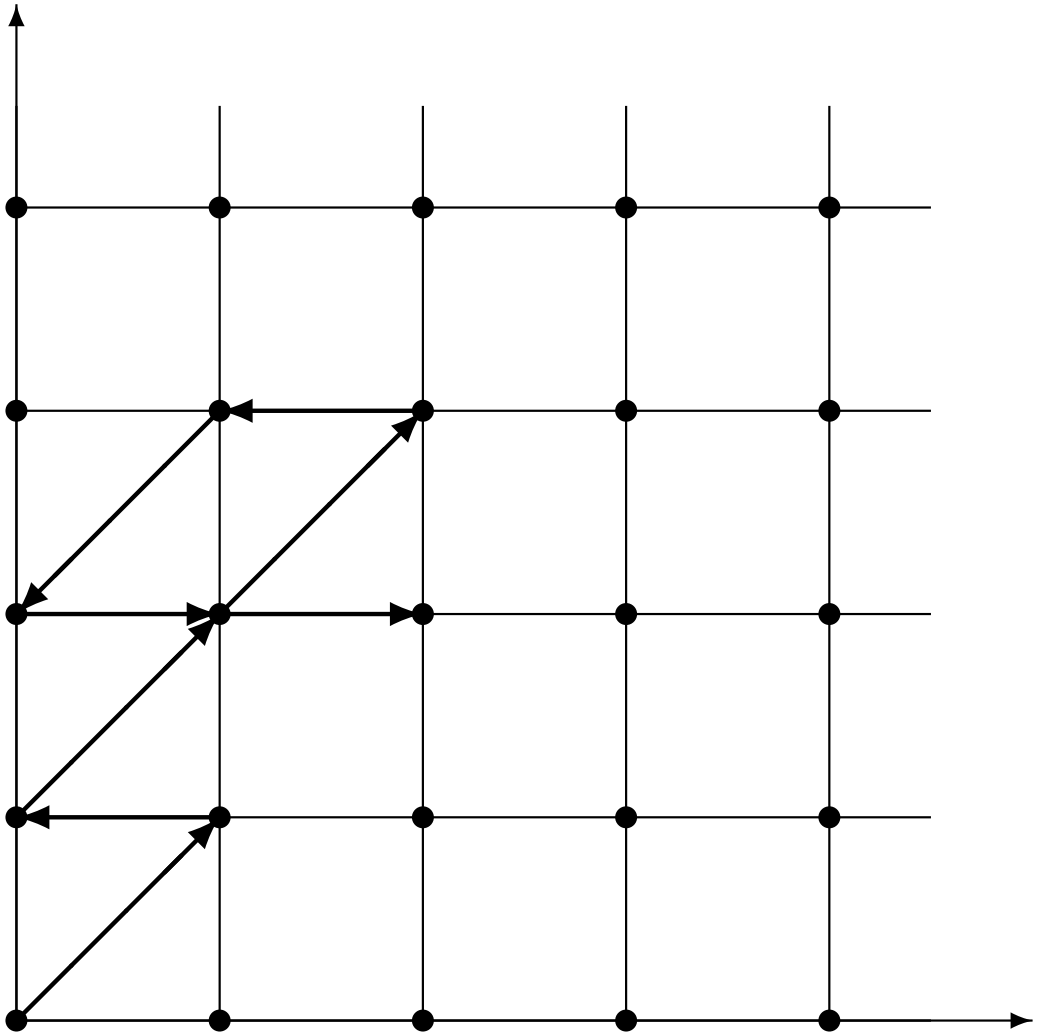
Gessel walks — Example



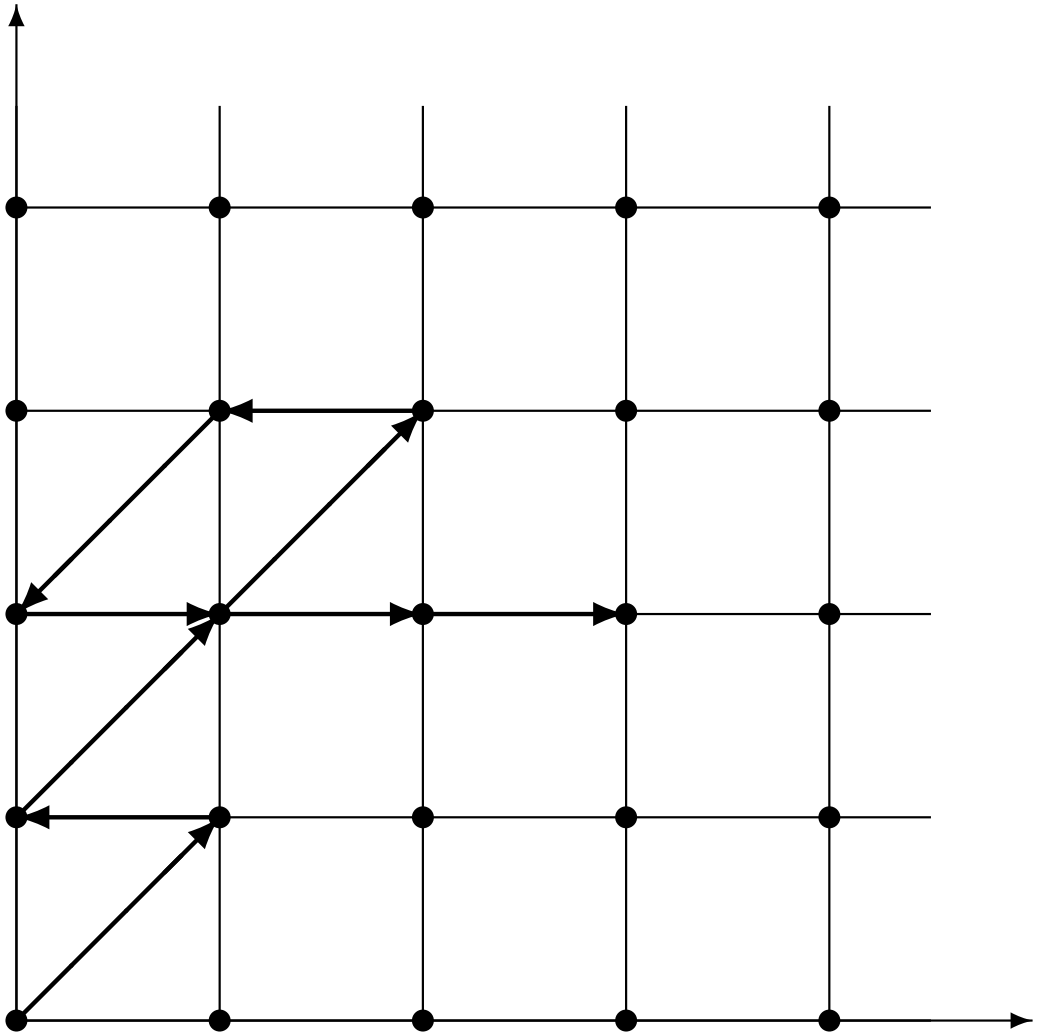
Gessel walks — Example



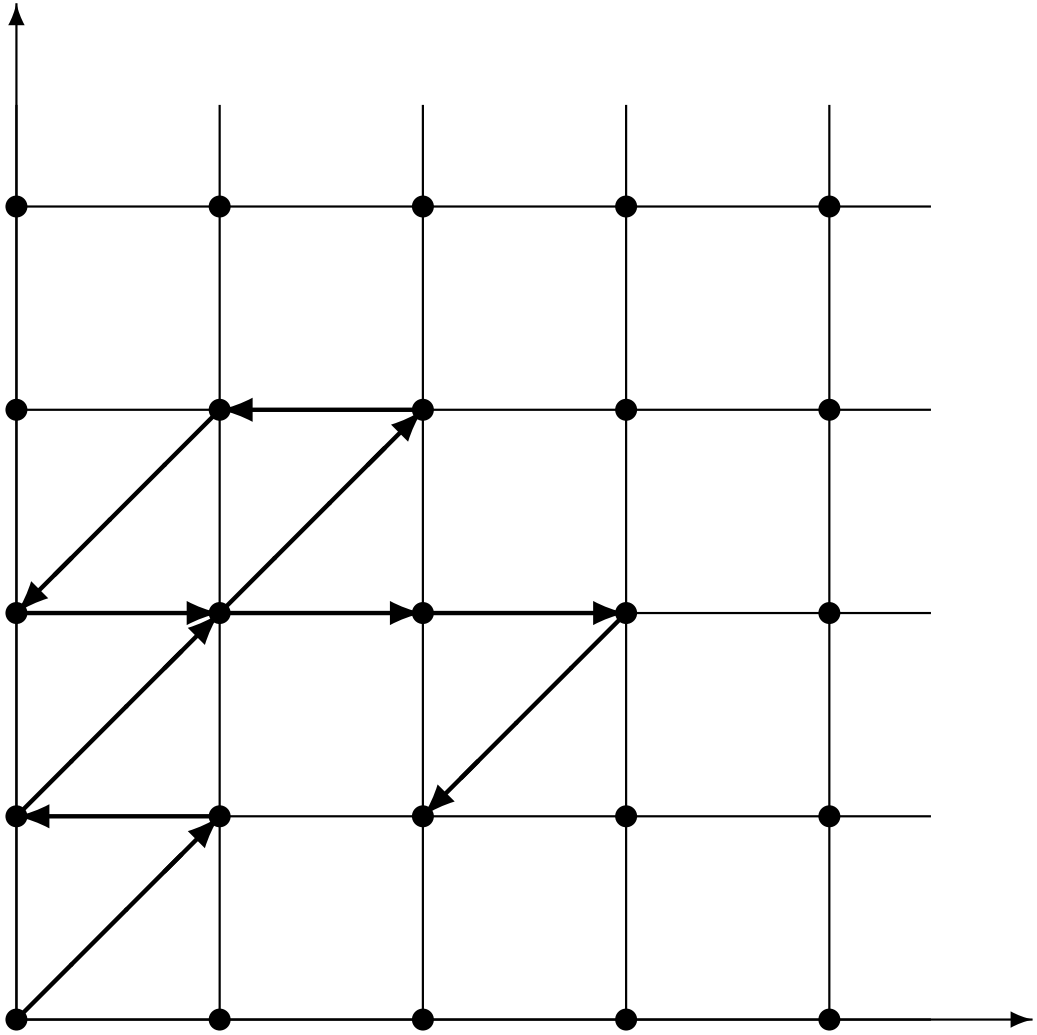
Gessel walks — Example



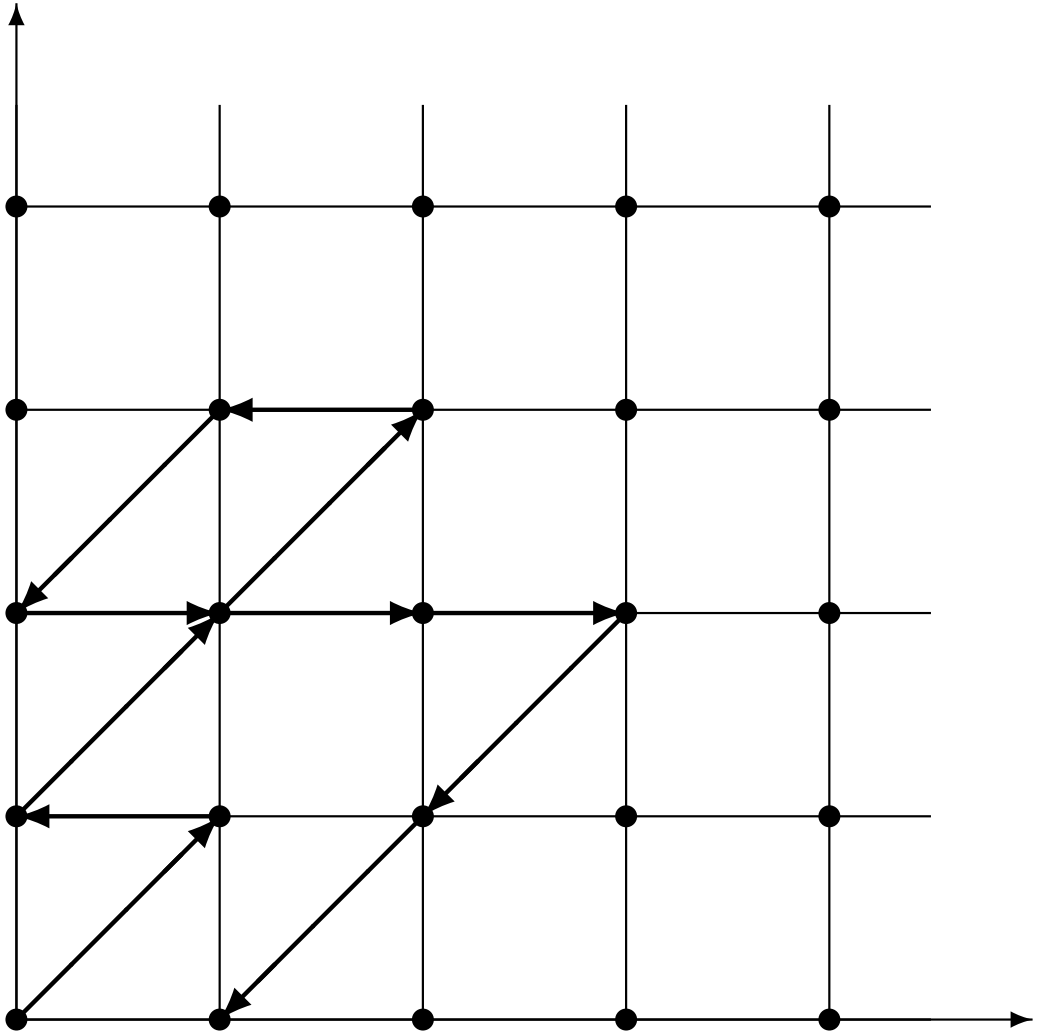
Gessel walks — Example



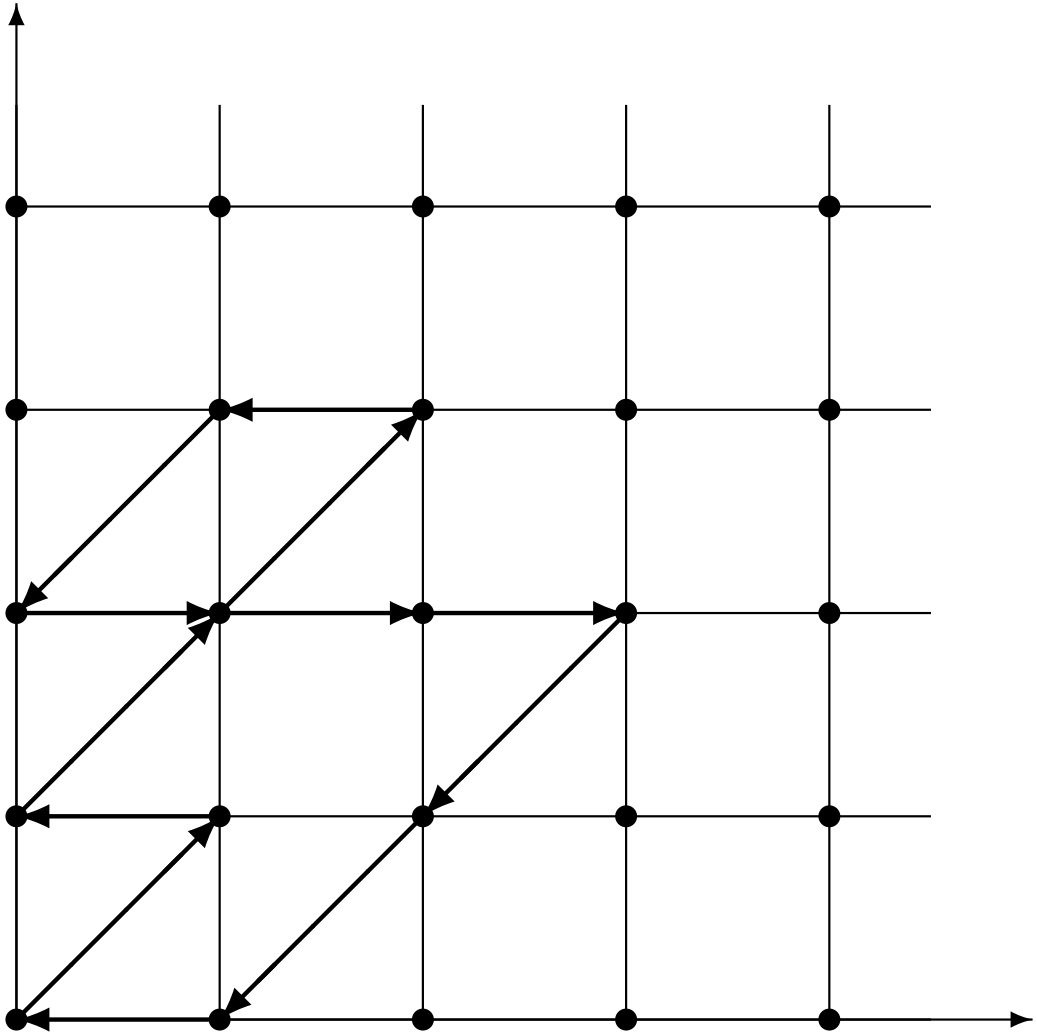
Gessel walks — Example



Gessel walks — Example



Gessel walks — Example



Zeilberger's quasi-holonomic ansatz

Let $f(n;i,j)$ count the Gessel walks with n steps ending at the point (i,j).
Compute a left ideal I of operators that annihilate $f(n;i,j)$.

Idea: Find an operator $R \in I$ of the form

$$\begin{aligned} R(n,i,j,S_n,S_i,S_j) = P(n,S_n) &+ iQ_1(n,i,j,S_n,S_i,S_j) \\ &+ jQ_2(n,i,j,S_n,S_i,S_j) \end{aligned}$$

- $R(n,i,j,S_n,S_i,S_j)$ annihilates $f(n;i,j)$
- set $i=j=0$
- $P(n,S_n)$ annihilates $f(n;0,0)$

Problem: $R(n,i,j,S_n,S_i,S_j)$ is too big to be computed.

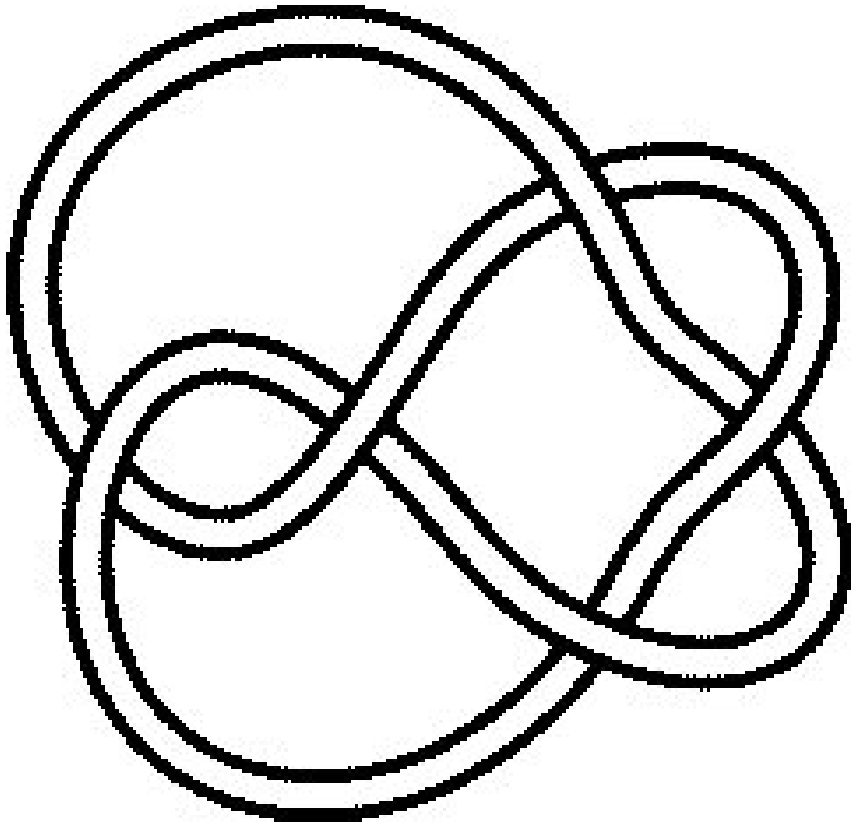
Result

The operator $P(n, S_n)$ annihilating $f(n; 0, 0)$ has

- order 32
- polynomial coefficients of degree 172
- and integer coefficients up to 385 digits.

Knot Theory

Compute the colored Jones polynomial of a given knot, e.g. Knot(5,2):



Computation of the colored Jones polynomial

$$\sum_{k_1=0}^{n}\sum_{k_2=0}^{n}\sum_{k_3=0}^{n}\sum_{k_4=0}^{n}\sum_{k_5=0}^{n}\sum_{k_6=0}^{n}$$

$$q^{-(k_1+k_2+k_3-2k_4+k_5+k_6+3)n-k_5^2-(k_2+k_3-k_4)k_5+k_2+(k_2-k_3)(k_3-k_4)}$$

$$q^{k_1(2k_2-k_3-k_4+k_5+1)+2(k_3-k_4+k_5)+k_6}\begin{bmatrix} k_1+k_3 \\ k_4 \end{bmatrix}_q \begin{bmatrix} k_2+k_5 \\ k_5 \end{bmatrix}_q$$

$$\begin{bmatrix} k_2+k_3-k_4+k_5 \\ k_3 \end{bmatrix}_q \begin{bmatrix} k_1+k_3-k_4+k_5+k_6 \\ k_1 \end{bmatrix}_q$$

$$\begin{bmatrix} k_2+k_3-k_4+k_5+k_6 \\ k_6 \end{bmatrix}_{1/q} (q^{-n};q)_{k_1} \left(q^{k_1-n};q\right)_{k_3}$$

$$\left(q^{-n+k_1+k_3-k_4};q\right)_{k_5} \left(q^{n-k_1-k_3+k_4-k_5};\frac{1}{q}\right)_{k_6}$$

$$\left(q^{-n+k_2-k_4+k_5};q\right)_{k_4} \left(q^{-n+k_3-k_4+k_5+k_6};q\right)_{k_2}$$

Example

For $n = 3$, the colored Jones polynomial is:

$$-\frac{1}{q^{33}}+\frac{1}{q^{32}}+\frac{1}{q^{31}}-\frac{2}{q^{29}}+\frac{2}{q^{27}}+\frac{1}{q^{26}}-\frac{3}{q^{25}}-\frac{1}{q^{24}}+\frac{3}{q^{23}}+\frac{2}{q^{22}}-\frac{3}{q^{21}}-\frac{3}{q^{20}}+\frac{4}{q^{19}}+\frac{2}{q^{18}}-\frac{4}{q^{17}}-\frac{4}{q^{16}}+\frac{5}{q^{15}}+\frac{2}{q^{14}}-\frac{3}{q^{13}}-\frac{3}{q^{12}}+\frac{4}{q^{11}}+\frac{2}{q^{10}}-\frac{2}{q^{9}}-\frac{2}{q^{8}}+\frac{2}{q^{7}}+\frac{1}{q^{6}}-\frac{1}{q^{4}}+\frac{1}{q^{3}}$$

Example

For $n = 3$, the colored Jones polynomial is:

$$-\frac{1}{q^{33}} + \frac{1}{q^{32}} + \frac{1}{q^{31}} - \frac{2}{q^{29}} + \frac{2}{q^{27}} + \frac{1}{q^{26}} - \frac{3}{q^{25}} - \frac{1}{q^{24}} + \frac{3}{q^{23}} + \frac{2}{q^{22}} - \frac{3}{q^{21}} - \frac{3}{q^{20}} + \frac{4}{q^{19}} + \frac{2}{q^{18}} - \frac{4}{q^{17}} - \frac{4}{q^{16}} + \frac{5}{q^{15}} + \frac{2}{q^{14}} - \frac{3}{q^{13}} - \frac{3}{q^{12}} + \frac{4}{q^{11}} + \frac{2}{q^{10}} - \frac{2}{q^{9}} - \frac{2}{q^{8}} + \frac{2}{q^{7}} + \frac{1}{q^{6}} - \frac{1}{q^{4}} + \frac{1}{q^{3}}$$

Observation: coefficients are extremely small.

Modular computations

Plug in an integer for q that is at least twice as big as the largest coefficient in the polynomial.
For example, $q = 16$:

$$\frac{1246513646743677488456574103004774671}{5444517870735015415413993718908291383296}$$

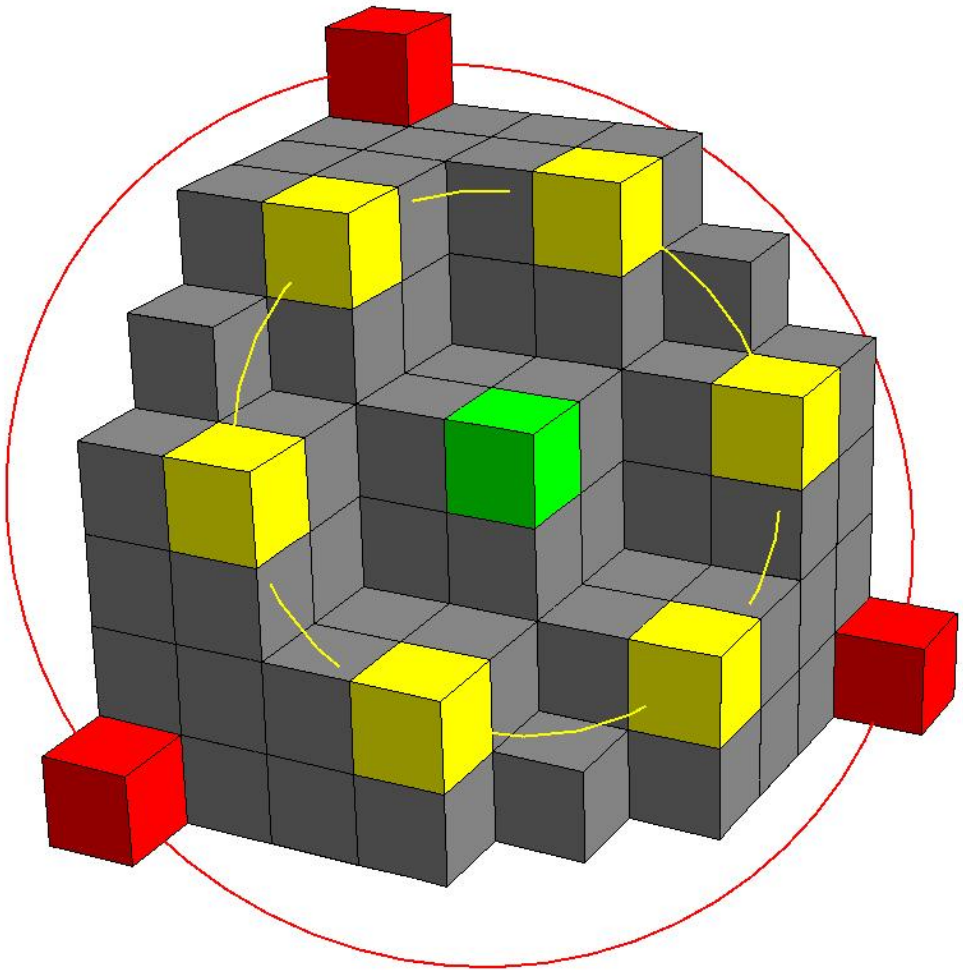
$$5444517870735015415413993718908291383296 = 2^{132} = 16^{33}$$

Write the numerator in base 16 representation:
$15\cdot16^{29}+0\cdot16^{28}+1\cdot16^{27}+1\cdot16^{26}+13\cdot16^{25}+14\cdot16^{24}+2\cdot16^{23}+3\cdot16^{22}+12\cdot16^{21}+13\cdot16^{20}+2\cdot16^{19}+4\cdot16^{18}+11\cdot16^{17}+12\cdot16^{16}+2\cdot16^{15}+3\cdot16^{14}+12\cdot16^{13}+13\cdot16^{12}+2\cdot16^{11}+2\cdot16^{10}+14\cdot16^{9}+13\cdot16^{8}+1\cdot16^{7}+1\cdot16^{6}+15\cdot16^{5}+14\cdot16^{4}+0\cdot16^{3}+1\cdot16^{2}+0\cdot16^{1}+15\cdot16^{0}$

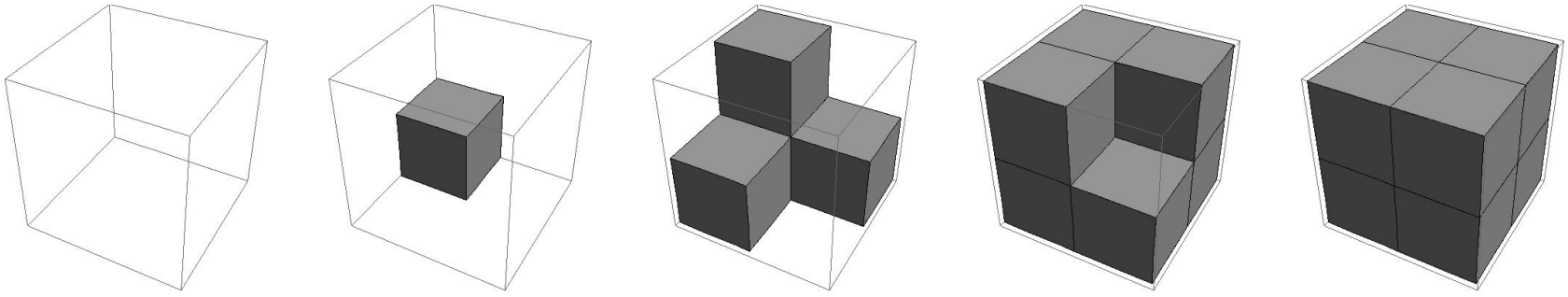
Simple rewriting, e.g.: $15 \cdot 16^{29} = 1 \cdot 16^{30} - 1 \cdot 16^{29}$ and so on.

Proof of the q-TSPP conjecture

(joint work with M. Kauers and D. Zeilberger)



Let $T(n)$ denote set of TSPPs with largest part at most n.



q^0 q^1 q^2 q^3 q^4

Andrews-Robbins q-TSPP conjecture:

$$\sum_{\pi \in T(n)} q^{|\pi/S_3|} = \prod_{1 \le i \le j \le k \le n} \frac{1-q^{i+j+k-1}}{1-q^{i+j+k-2}}$$

For $q = 1$:

$$|T(n)| = \prod_{1 \le i \le j \le k \le n} \frac{i+j+k-1}{i+j+k-2} \qquad \text{(Stembridge)}$$

Some identities

How to prove $$(1+q^n) - c_{n,n-1} + \sum_{j=1}^{n} c'_{n,j} = \frac{b_n}{b_{n-1}}$$

with $$c'_{n,j} = q^{n+j-1}\left(\begin{bmatrix} n+j-2 \\ n-1 \end{bmatrix}_q + q \begin{bmatrix} n+j-1 \\ n \end{bmatrix}_q \right) c_{n,j}\,?$$

Some identities

How to prove $$(1+q^n) - c_{n,n-1} + \sum_{j=1}^{n} c'_{n,j} = \frac{b_n}{b_{n-1}}$$

with $$c'_{n,j} = q^{n+j-1}\left(\begin{bmatrix} n+j-2 \\ n-1 \end{bmatrix}_q + q\begin{bmatrix} n+j-1 \\ n \end{bmatrix}_q\right) c_{n,j}\,?$$

- Compute an annihilating ideal for $c'_{n,j}$ via closure properties.
- Find a relation in this ideal of the form

$$p_7 c'_{n+7,j} + \cdots + p_1 c'_{n+1,j} + p_0 c'_{n,j} = t_{n,j+1} - t_{n,j}$$

  where the $p_7, \ldots, p_0$ are rational functions in $\mathbb{Q}(q, q^n)$ and $t_{n,j}$ is a $\mathbb{Q}(q, q^j, q^n)$-linear combination of certain shifts of $c'_{n,j}$.
- Creative telescoping yields a recurrence for the sum.

Creative telescoping

We consider $\sum_{j=1}^{n} c'_{n,j}$ and have

$$p_7 c'_{n+7,j} + \cdots + p_1 c'_{n+1,j} + p_0 c'_{n,j} = t_{n,j+1} - t_{n,j}$$

where the $p_7, \ldots, p_0$ are rational functions in $\mathbb{Q}(q, q^n)$ and $t_{n,j}$ is a $\mathbb{Q}(q, q^j, q^n)$-linear combination of certain shifts of $c'_{n,j}$.

We show that $c'_{n,j} = 0$ for $j \leq 0$ and for $j > n$.
Now just sum over both sides:

$$\sum_{j=-\infty}^{\infty} \left(p_7 c'_{n+7,j} + \cdots + p_1 c'_{n+1,j} + p_0 c'_{n,j}\right) = \sum_{j=-\infty}^{\infty} \left(t_{n,j+1} - t_{n,j}\right)$$

$$\sum_{j=0}^{n+7} p_7 c'_{n+7,j} + \cdots + \sum_{j=0}^{n+1} p_1 c'_{n+1,j} + \sum_{j=0}^{n} p_0 c'_{n,j} = 0$$

$$p_7 \sum_{j=0}^{n+7} c'_{n+7,j} + \cdots + p_1 \sum_{j=0}^{n+1} c'_{n+1,j} + p_0 \sum_{j=0}^{n} c'_{n,j} = 0$$

Reduction

Algorithm: Normal form computation
Input: an operator p and a Gröbner basis $G = \{g_1, \ldots, g_m\}$ **Output:** normal form of p modulo the left ideal $\langle G \rangle$
while exists $1 \leq i \leq m$ such that $\mathrm{lm}(g_i) \mid \mathrm{lm}(p)$ $g := (\mathrm{lm}(p) / \mathrm{lm}(g_i)) \cdot g_i$ $p := p - (\mathrm{lc}(p) / \mathrm{lc}(g)) \cdot g$ end while return p

lm and lc refer to the leading monomial and the leading coefficient of an operator respectively.

Modular reduction

Algorithm: Modular normal form computation
Input: an operator p and a Gröbner basis $G = \{g_1, \ldots, g_m\}$ **Output:** modular normal form of p modulo the left ideal $\langle G \rangle$
while exists $1 \leq i \leq m$ such that $\mathrm{lm}(g_i) \mid \mathrm{lm}(p)$ $g := h((\mathrm{lm}(p)/\mathrm{lm}(g_i)) \cdot g_i)$ $p := p - (\mathrm{lc}(p)/\mathrm{lc}(g)) \cdot g$ end while return p

- h is an insertion homomorphism
- $h : \mathbb{K}(j, n) \to \mathbb{K}(j)$, $h(f(j, n)) \mapsto f(j, n_0)$, for some $n_0 \in \mathbb{N}$
- most of the computations are done modulo the polynomial $n - n_0$
- coefficient growth is moderate (univariate vs. bivariate)