Computability and Enumeration

Igor Pak, UCLA

(joint work with Scott Garrabrant)

Mathematics of Jiří Matoušek Conference

Prague, Czech Republic, July 26, 2016

Integer sequences

Let $\{a_n\}$ be a *combinatorial sequence*, e.g.

$$a_n = \# \text{ of triangulations of a convex } n\text{-gon}$$
$$a_n = \# \text{ of domino tilings of } [n \times n]$$
$$a_n = \# \text{ of connected labeled graphs on } n$$
vertices
$$a_n = \# \text{ of triangulations of a } n \times n \text{ grid}$$

Question 1: Does $\mathcal{A}(t) = \sum_n a_n t^n$ have a *formula*?

Question 2: Can a_n be *computed efficiently*?

Conjecture [Wilf, 1982]: Number of unlabeled graphs on n vertices

is *hard* to compute.

Classes of combinatorial sequences

(1) ***rational*** g.f. $\mathcal{A}(t) = P(t)/Q(t)$, $P, Q \in \mathbb{Z}[t]$
e.g. $a_n = \mathrm{Fib}(n)$, then $\mathcal{A}(t) = 1/(1-t-t^2)$.

(2) ***algebraic*** g.f. $c_0\mathcal{A}^k + c_1\mathcal{A}^{k-1} + \ldots + c_k = 0$, $c_i \in \mathbb{Z}[t]$
e.g. $a_n = \mathrm{Cat}(n)$, then $\mathcal{A}(t) = (1-\sqrt{1-4t})/2t$.

(3) ***D-finite*** g.f. $c_0\mathcal{A} + c_1\mathcal{A}' + \ldots + c_k\mathcal{A}^{(k)} = 0$, $c_i \in \mathbb{Z}[t]$
e.g. $a_n = \#$ involutions in S_n, then $a_n = a_{n-1} + (n-1)a_{n-2}$.
The sequences $\{a_n\}$ are called ***P-recursive***

(4) ***ADE*** g.f. $Q\big(t, \mathcal{A}, \mathcal{A}', \ldots, \mathcal{A}^{(k)}\big) = 0, Q \in \mathbb{Z}[t, x_0, x_1, \ldots, x_k]$
e.g. $a_n = \#\{\sigma(1) < \sigma(2) > \sigma(3) < \ldots \in S_n\}$, then $\mathcal{A}' = \mathcal{A}^2 + 1$.
also $p(n) = \#$ integer partitions of n (Jacobi, Ramanujan).

Inclusions: (1) $\subset$ (2) $\subset$ (3) $\subset$ (4).

General philosophy:

Definition: Sequence $\{a_n\}$ can be *computed efficiently* if there is an algorithm which computes a_n in time Poly(n).

Proposition: ADE sequences $\{a_n\}$ can be computed efficiently.

- Most combinatorial sequences have *nice* g.f. (D-finite, ADE, etc.)
- Proving that $\mathcal{A}(t) = \sum_n a_n t^n$ is *not* D-finite or ADE is difficult.
- Thus, proving non-D-finite and non-ADE are important first steps.

Theorem: (Jacobi, 1848) $\sum_n t^{n^2}$ is ADE.

Theorem: (Lipshitz, Rubel, 1986) $\sum_n t^{2^n}$ is *not* ADE.

Conjecture: $\sum_n t^{n^3}$ is *not* ADE.

Permutation classes

Permutation $\sigma \in S_n$ contains $\pi \in S_k$ if M_π is a submatrix of M_σ.

Otherwise, σ *avoids* π. Such π are called *patterns*.

For example, (4564123) contains (321) but avoids (4321).

$$\begin{pmatrix} \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 \\ \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot \\ 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot \end{pmatrix} \qquad \begin{pmatrix} \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \end{pmatrix}$$

Fix a set of patterns $\mathcal{F} \subset S_k$. Denote by $C_n(\mathcal{F})$ the number of $\sigma \in S_n$
which avoids all $\pi \in \mathcal{F}$.

Question 1: Is $\mathcal{A}(t) = \sum_n C_n(\mathcal{F}) t^n$ always D-finite or ADE?

Question 2: Can $C_n(\mathcal{F})$ always be computed in Poly(n) time?

Notable results and examples:

(0) $C_n(12\cdots k, \ell\cdots 21) = 0$, $\forall n > (k-1)(\ell-1)$ [Erdős, Szekeres, 1935]

(1) $C_n(123) = C_n(213) = \mathrm{Cat}(n)$ [MacMahon, 1915], [Knuth, 1973]

(2) $C_n(123, 132, 213) = \mathrm{Fib}(n+1)$ [Simion, Shmidt, 1985]

(3) $C_n(2413, 3142) = \text{Shröder}(n)$ [Shapiro, Stephens, 1991]

(4) $C_n(1234) = C_n(2143)$ has D-finite g.f. [Gessel, 1990]

(5) $C_n(1342) = C_n(2416385)$ has algebraic g.f. [Bona, 1997]

(6) $C_n(\mathcal{F}) < K(\mathcal{F})^n$ [Marcus, Tardos, 2004], improving [Alon, Friedgut, 2000]

(7) $K(\pi) = e^{k^{\Omega(1)}}$ w.h.p., for $\pi \in S_k$ random [Fox, 2013]

(8) σ contains π is NP-complete [Bose, Buss, Lubiw, 1998]

(9) can be decided in $O(n \log n)$ for π fixed [Guillemot, Marx, 2014]

Main results

Noonan–Zeilberger Conjecture (1996):

The g.f. for $\{C_n(\mathcal{F})\}$ is D-finite, for all fixed $\mathcal{F} \subset S_k$.

Theorem 1 [Garrabrant, Pak, 2015]

The NZ Conjecture is false. To be precise, there is a set $\mathcal{F} \subset S_{80}$,

$|\mathcal{F}| < 31000$, *such that* $\sum_n C_n(\mathcal{F}) t^n$ *is* not *D-finite.*

Theorem 2 [Garrabrant, Pak, 2016+]

There is a set $\mathcal{F} \subset S_{80}$, *such that* $\sum_n C_n(\mathcal{F}) t^n$ *is* not *ADE.*

Historical notes: NZ Conjecture was first stated by Gessel in 1990. In 2005,

Zeilberger changes his mind, conjectures that $\{C_n(1324)\}$ is a counterexample.

In 2014, Zeilberger changes his mind half-way back, writes:

"if I had to bet on it now I would give only a 50% chance."

Computability implications

Theorem 3 [Garrabrant, Pak, 2015]

The problem whether $C_n(\mathcal{F}) = C_n(\mathcal{F}') \mod 2 \ \forall n$, *is undecidable.*

Corollary 1. For all k large enough, there exists $\mathcal{F}, \mathcal{F}' \subset S_k$, s.t.

the first time $C_n(\mathcal{F}) \neq C_n(\mathcal{F}') \mod 2$ is for

$$n > 2^{2^{2^{2^{2^k}}}}.$$

Corollary 2. There exist two finite sets of patterns $\mathcal{F}$ and $\mathcal{F}'$ in S_k,

s.t. the problem of whether $C_n(\mathcal{F}) = C_n(\mathcal{F}') \mod 2$, for all $n \in \mathbb{N}$,

is independent of ZFC.

Complexity result and Wilf's question

Theorem 4 [Garrabrant, Pak, 2015]

If $\mathsf{EXP} \neq \oplus\mathsf{EXP}$*, then there exists a finite set of patterns* $\mathcal{F}$*, such that*

the sequence $\{C_n(F)\}$ *cannot be computed in time polynomial in* n*.*

Reminder: EXP = exponential time,

$\oplus\mathsf{P}$ = parity version of the class of counting problem $\#\mathsf{P}$,

$\oplus\mathsf{EXP}$ = parity version of the class of counting problem $\#\mathsf{EXP}$.

$\mathsf{EXP} \neq \oplus\mathsf{EXP}$ assumption is similar to $\mathsf{P} \neq \oplus\mathsf{P}$.

Remark: This answers Wilf's question (1982)

"Can one describe a reasonable and natural family of combinatorial

enumeration problems for which there is provably no polynomial-in-n

time formula or algorithm to compute $f(n)$*?"*

Simulating Turing Machines

Let $\mathbb{X}$ denote the set of sequences $\{\xi_\Gamma(n)\}$, where

Γ is a two-stack automaton with source S and sink T, and

$\xi_\Gamma(n)$ is the number of balanced $S-T$ paths of length n.

(Here *balanced* means that both stacks are empty at the end).

Main Lemma

Let $\xi : \mathbb{N} \to \mathbb{N}$ *be a function in* $\mathbb{X}$. *Then there exist* $k, a, b \in \mathbb{N}$

and sets of patterns $\mathcal{F}, \mathcal{F}' \in S_k$, *such that*
$\xi(n) = C_{an+b}(\mathcal{F}) - C_{an+b}(\mathcal{F}') \mod 2$, *for all* $n \geq 1$.

Main Lemma can be used to derive both Theorem 3 and Theorem 4.

Note: Here mod 2 can be changed to any mod p, but cannot be completely removed.

Proof of Theorem 1.

Lemma 1. Let $\{a_n\}$ be a P-recursive sequence (i.e. with D-finite g.f.)

Let $\overline{\alpha} = (\alpha_1, \alpha_2, \ldots)$, $\overline{\alpha} \in \{0,1\}^\infty$ defined by $\alpha_n = a_n \mod 2$.

Then there is a finite binary word w which is NOT a subword of $\overline{\alpha}$.

Lemma 2. There is a two-stack automaton Γ s.t. the number of balanced paths $\xi_\Gamma(n)$ is given by the sequence

0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, ...

Lemma 1, Lemma 2 and the Main Lemma imply Theorem 1.

Proof of Theorem 2.

Lemma 1′. Let $\{a_n\}$ be a sequence, and let $\{n_i\}$ be the sequence of indices with odd a_n. Suppose
1) for all $b, c \in \mathbb{N}$, there exists i such that $n_i = b \bmod 2c$,
2) $n_i/n_{i+1} \to 0$ as $i \to \infty$.
Then the g.f. for $\{a_n\}$ is not ADE.

Observe: $\{a_n = n! + n\}$ satisfies conditions of Lemma 1′.

Lemma 2′. There is a two-stack automaton Γ s.t. the number of balanced paths $\xi_\Gamma(n) = n! + n$.

Lemma 1′, Lemma 2′ and the Main Lemma imply Theorem 2.

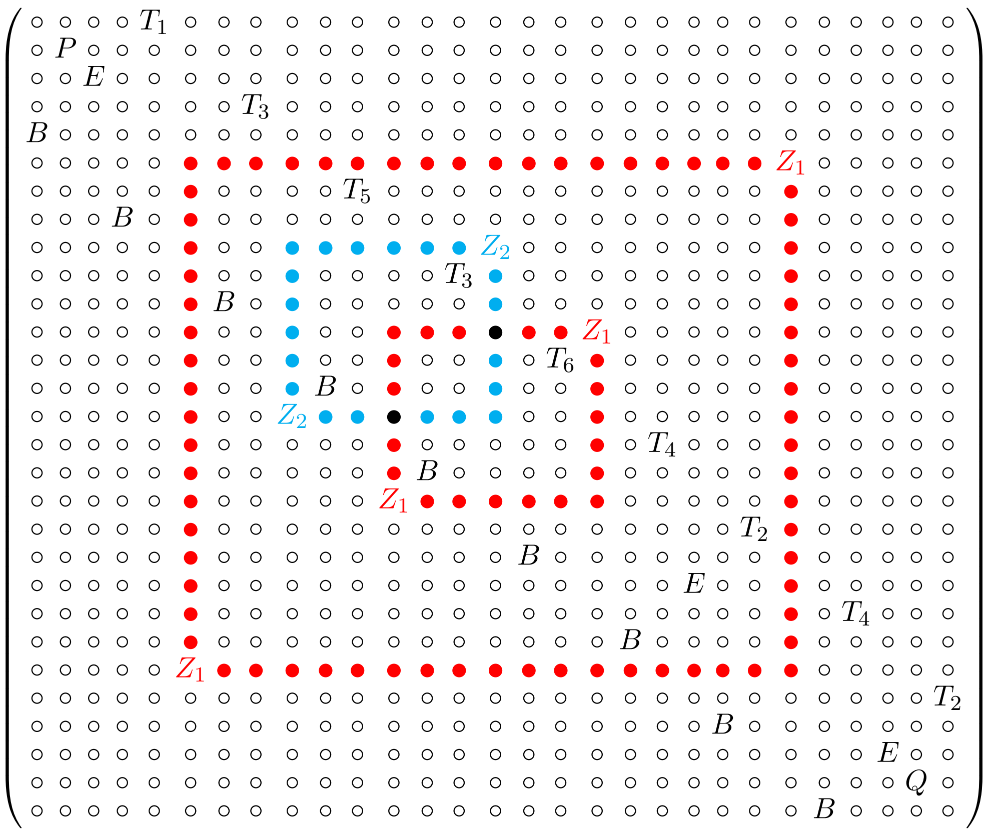
Main Lemma: proof outline

(0) Allow general partial patterns (rectangular $0-1$ matrices with no two 1's in the same row or column).

(1) Fix a sufficiently large "alphabet" of "incomparable" matrices
Specifically, we take all simple 10-permutations which contain (5674123).
Arbitrarily name them $P, Q, B, B', E, T_1, ..., T_v, Z_1, ..., Z_m$.

(2) Thinking of T_i's as vertices of Γ and Z_j as variables x_p, y_q, select block matrices $\mathcal{F}$ to simulate Γ. Let $\mathcal{F}' = \mathcal{F} \cup \{B, B'\}$.

(3) Define involution Ψ on $C_n(\mathcal{F}) \smallsetminus C_n(\mathcal{F}')$ by $B \leftrightarrow B'$. Check that fixed points of Ψ are in bijection with balanced paths in Γ.

$M =$  .

Notes on the proofs:

(i) We use exactly 6854 partial patterns.

(i) Automaton Γ in Lemma 2 uses 31 vertices, which is why
the alphabet has size 10×10 only.

(iii) The largest matrix in $\mathcal{F}$ has 8×8 blocks,
which is why Theorem 1 has permutations in S_{80}.

(iv) Proof of Lemma 1 has only 2 paragraphs, but it took over
a year
to find a statement. Lemma $1'$ took another year.

(v) Condition n_i / n_{i+1} in Lemma $1'$ cannot be weakened,
e.g. $\mathrm{Cat}(n)$ is odd if and only if $n = 2^m - 1$.

Open problems:

Conjecture 1. The *Wilf-equivalence problem* of whether $C_n(\mathcal{F}_1) = C_n(\mathcal{F}_2)$ for all $n \in \mathbb{N}$, is undecidable.

Conjecture 2. The *Wilf-equivalence problem* for single permutations: $C_n(\sigma) = C_n(\omega)$ for all $n \in \mathbb{N}$, is decidable.

Conjecture 3. Sequence $\{C_n(1324)\}$ is not P-recursive.

Conjecture 4. There exists a fixed set of patterns $\mathcal{F}$, s.t. computing $\{C_n(\mathcal{F})\}$is #EXP-complete.

Grand finale:

Story how Doron Zeilberger lost $100.

Thank you!