Enumeration of permutations

Igor Pak, UCLA

Joint work with Scott Garrabrant

Yandex, Moscow, Russia

September 21, 2015

What is Enumerative Combinatorics?

Selected combinatorial sequences (from `OEIS`):

`A000001`: 1, 1, 1, 2, 1, 2, 1, 5, 2, 2, 1, 5, 1, 2, 1, 14, ... $\leftarrow$ finite groups

`A000040`: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, ... $\leftarrow$ primes

`A000041`: 1, 1, 2, 3, 5, 7, 11, 15, 22, 30, 42, 56, 77, 101, ... $\leftarrow p(n)$

`A000045`: 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 232, ... $\leftarrow Fib(n)$

`A000085`: 1, 1, 2, 4, 10, 26, 76, 232, 764, 2620, 9496, ... $\leftarrow$ involutions in S_n

`A000108`: 1, 2, 5, 14, 42, 132, 429, 1430, 4862, 16796, ... $\leftarrow Cat(n)$

`A000088`: 1, 1, 4, 38, 728, 26704, 1866256, 251548592, ... $\leftarrow$ connected labeled graphs

Main question: Is there a formula?

What is a formula?

(A) *The most satisfactory form of* $f(n)$ *is a* ***completely explicit closed formula*** *involving only well-known functions, and free from summation symbols. Only in rare cases will such a formula exist. As formulas for* $f(n)$ *become more complicated, our willingness to accept them as* "determinations" *of* $f(n)$ *decreases.*

Richard Stanley, Enumerative Combinatorics, (1986)

(B) Formula $=$ ***Algorithm*** working in time $Poly(n)$.

Herb Wilf, What is an answer? (1982)

(C) ***Asymptotic formula***

(A) $\Rightarrow$ (B) , (C) *??*

Asymptotic formulas:

$$Fib(n) \sim \frac{1}{\sqrt{5}}\,\phi^n, \quad \text{where} \;\; \phi = (1+\sqrt{5})/2 \qquad \text{[de Moivre, c. 1705]}$$

$$Cat(n) \sim \frac{4^n}{\sqrt{\pi}\,n^{3/2}} \qquad \text{[Euler + Stirling, 1751]}$$

$$p_n \sim n\log n \qquad \text{[Hadamard, Vallée-Poussin, 1896]}$$

$$\#\{\text{integer partitions of } n\} \sim \frac{1}{4\sqrt{3}\,n}\,e^{\pi\sqrt{2n/3}} \qquad \text{[Hardy, Ramanujan, 1918]}$$

$$\#\{\text{involutions in } S_n\} \sim \frac{1}{\sqrt{2}\,e^{1/4}}\left(\frac{n}{e}\right)^{n/2} e^{\sqrt{n}} \qquad \text{[Chowla, 1950]}$$

$$\#\{\text{groups of order} \le n\} \sim n^{\frac{2}{27}(\log_2 n)^2} \qquad \text{[Pyber, 1993]}$$

$$\#\{\text{graphs on } n \text{ vertices}\} \sim 2^{\binom{n}{2}} \qquad [\Leftrightarrow \text{random graph is connected w.h.p.}]$$

Fibonacci numbers:

$F(n) =$ number of 0-1 sequences of length $n-1$ with no (11).
$F(3) = \mathbf{3}$, $\{00, 01, 10\}$. $F(4) = \mathbf{5}$, $\{000, 001, 010, 100, 101\}$.

$$(1) \qquad F(n+1) \;=\; F(n) + F(n-1)$$

$$(2) \qquad F(n) \;=\; \sum_{i=0}^{\lfloor n/2 \rfloor} \binom{n-i}{i}$$

$$(3) \qquad F(n) \;=\; \frac{1}{\sqrt{5}}\Big(\phi^n + (-1/\phi)^n\Big)$$

Observe: "Closed formula" (3) is not useful for the exact computation, but (1) is the best.

Moral: What's the best "closed formula" is complicated!

Derangement numbers:

$D(n) =$ number of $\sigma \in S_n$ s.t. $\sigma(i) \neq i$ for all $1 \leq i \leq n$

$D(2) = \mathbf{1}$, $\{21\}$. $D(2) = \mathbf{2}$, $\{231, 312\}$. $D(3) = \mathbf{9}$, $D(4) = \mathbf{44}$, ...

$$(1) \qquad D(n) \, = \, \left[n!/e \right]$$

$$(2) \qquad D(n) \, = \, \sum_{k=0}^{n} (-1)^k \frac{n!}{k!}$$

$$(3) \qquad D(n) \, = \, n D(n-1) + (-1)^n$$

Observation: Formula (1) is neither combinatorial nor useful for the exact computation. Summation formula (2) explains ($\diamond$), but the recursive formula (3) is most useful for computation.

Ménage numbers:

$M(n)$ = number of ways to seat n couples at a dining table so that men and women alternate and spouses do not seat together.

$M(2) = \mathbf{0}$. $M(3) = \mathbf{12}$, e.g. [2a3b1c] if couples are 1a, 2b, 3c

Formulas: $M(n) = 2n!a(n)$, where $a(n) \sim n!/e^3$

$$(1) \qquad a(n) = \sum_{k=0}^{n} (-1)^k \frac{2n}{2n-k} \binom{2n-k}{k} (n-k)!$$

$$(2) \qquad a(n) = nA_{n-1} + 2A_{n-2} - (n-4)A_{n-3} - A_{n-4}$$

Here (2) by Lucas (1891) and (1) by Touchard (1934).

Of course, (2) is better even if (1) is more explicit!

Generating Functions

Let $\{a_n\}$ be a combinatorial sequence. Define

$$\mathcal{A}(t) = \sum_n a_n t^n$$

Question: Does $\mathcal{A}(t)$ have a *closed formula*?

1) Let $a_n = F(n)$. Then:

$$\mathcal{A}(t) = \frac{1}{1 - t - t^2}$$

2) $a_n = \mathrm{Cat}(n) = \frac{1}{n+1}\binom{2n}{n}$. Then:

$$\mathcal{A}(t) = \frac{1 - \sqrt{1 - 4t}}{2t}$$

More examples

3) a_n= number of involutions $\sigma \in S_n$ i.e. $\sigma^2 = 1$.

$$a_n = a_{n-1} + (n-1)a_{n-2}$$

$$\sum_n \frac{a_n}{n!} t^n = e^{t+t^2/2}$$

4) $p(n)$= number of integer partitions of n, e.g. $p(4) = 5$
$4 = 4+1 = 2+2 = 2+1+1 = 1+1+1+1$.

$$\sum_n p(n) t^n = \prod_{k=1}^{\infty} \frac{1}{1-t^k}$$

Classes of combinatorial sequences

(1) ***rational*** if g.f. $\mathcal{A}(t) = P(t)/Q(t), \quad P, Q \in \mathbb{Z}[t]$

Equivalent: $c_0 a_n + c_1 a_{n-1} + \ldots + c_k a_{n-k} = 0$ for some $c_i \in \mathbb{Z}$.

Examples: 2^n, Fibonacci numbers, Lah numbers, etc.

(2) ***algebraic*** if g.f. $c_0 \mathcal{A}^k + c_1 \mathcal{A}^{k-1} + \ldots + c_k = 0, \quad c_i(t) \in \mathbb{Z}[t]$

Examples: Catalan numbers, Motzkin numbers, etc.

(3) ***Binomial sums.*** For $\alpha_i, \beta_i : \mathbb{Z}^d \to \mathbb{Z}$ linear functions:

$$a_n = \sum_{v \in \mathbb{Z}^d} c^{\alpha_0(v,n)} \binom{\alpha_1(v,n)}{\beta_1(v,n)} \cdots \binom{\alpha_r(v,n)}{\beta_r(v,n)}$$

Examples: derangement numbers, ménage numbers, etc.

P-recursive sequences

(4) ***D-finite*** g.f. $c_0\mathcal{A} + c_1\mathcal{A}' + \ldots + c_k\mathcal{A}^{(k)} = 0, \quad c_i(t) \in \mathbb{Z}[t]$

Equivalent: $r_0(n)a_n + r_1(n)a_{n-1} + \ldots + r_k(n)a_{n-k}, \quad r_i(n) \in \mathbb{Z}[n]$

Sequences $\{a_n\}$ are called ***polynomially (P-) recursive***.

Observation: P-recursive sequences are computable in poly time.

Examples: $n!$, Fibonacci numbers, Catalan numbers, number of involutions, ménage numbers, etc.

Theorem: **(1)**, **(2)**, **(3)** $\subset$ **(4)**

Non-examples: primes, number of partitions, number of connected graphs

Asymptotics of P-recursive sequences

Claim [Birkhoff, etc.] Let $\{a_n\}$ be P=recursive. Then:

$$a_n \sim C\,(n!)^s\,\lambda^n\,e^{Q(n^{1/m})}\,n^\alpha(\log n)^\beta$$

where $Q(z)$ is a polynomial of deg $< m$, $\lambda \in \overline{\mathbb{Q}}$, $\alpha, s \in \mathbb{Q}$, $\beta, m \in \mathbb{N}$

Theorem [many people]
If $\{a_n\}$ be P-recursive, $a_n \in \mathbb{N}$ and $a_n < C^n$. Then:

$$a_n \sim C\,\lambda^n\,n^\alpha(\log n)^\beta$$

where $\lambda \in \overline{\mathbb{Q}}$, $\alpha \in \mathbb{Q}$, $\beta \in \mathbb{N}$.

Note: this includes all of **(3)**.

Algebraic Differential Equations

(5) ***ADE*** g.f. $Q(t, \mathcal{A}, \mathcal{A}', \ldots, \mathcal{A}^{(k)}) = 0$, $Q \in \mathbb{Z}[t, x_0, x_1, \ldots, x_k]$

Observation: ADE sequences are computable in poly time.

Example: $a_n = \#\{\sigma(1) < \sigma(2) > \sigma(3) < \ldots \in S_n\}$. E.g. $a_3 = 2$, $\{132, 231\}$. These are called *alternating permutations.* Then the e.g.f.

$$2\mathcal{A}' = \mathcal{A}^2 + 1, \qquad \mathcal{A}(t) = \tan(t) + \sec(t)$$

Note: Jacobi proved in 1848 that the *Dirichlet theta function* $\theta(t) := \sum_n t^{n^2}$ satisfies an explicit form ADE.

Curiously, for $\sum_n t^{n^3}$ this is open, but conjectured false.

Permutation classes

Permutation $\sigma \in S_n$ *contains* $\omega \in S_k$ if M_ω is a submatrix of M_σ. Otherwise, σ *avoids* ω. Such ω are called *patterns.*

For example, (5674123) contains (321) but avoids (4321).

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

For a set of patterns $\mathcal{F} \subset S_k$, denote $\mathcal{C}_n(\mathcal{F})$ the set of $\sigma \in S_n$ avoiding each $\omega \in \mathcal{F}$. Let $C_n(\mathcal{F}) = |\mathcal{C}_n(\mathcal{F})|$.

Notable examples:

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

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

(3) $C_n(2413, 3142) =$Schröder(n) [Shapiro, Stephens, 1991]

(4) $C_n(1234) = C_n(2143)$ is P=recursive [Gessel, 1990]

(5) $C_n(1342)$ is algebraic [Bona, 1997]

(6) $C_n(3412, 4231)$ is algebraic [Bousquet-Mélou, Butler, 2007]
counts the number of smooth Schubert varieties X_σ, $\sigma \in S_n$,
by [Lakshmibai, Sandhya, 1990].

Main result

Noonan–Zeilberger Conjecture:

For every $\mathcal{F} \subset S_k$, the sequence $\{C_n(\mathcal{F})\}$ is P-recursive.

(Equivalently, the g.f. for $\{C_n(\mathcal{F})\}$ is D-finite).

Theorem 1. [Garrabrant, P., 2015+]

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

$|\mathcal{F}| < 31000$, s.t. $\{C_n(\mathcal{F})\}$ is **not** P-recursive.

A bit of history

- First stated as an open problem by Gessel (1990)
- Upgraded to a conjecture and extended to count copies contained of each pattern, by Noonan and Zeilberger (1996)
- Atkinson reduced the extended version to the original (1999)
- In 2005, Zeilberger changes his mind, conjectures that $\{C_n(1324)\}$ is not P-recursive [this is still open]
- 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".

As bad as it gets!

Main Lemma [here $\mathbb{X}$ is LARGE, to be clarified below]

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 $\mathcal{F}, \mathcal{F}' \subset S_k$, s.t.

$\xi(n) = C_{an+b}(\mathcal{F}) - C_{an+b}(\mathcal{F}') \bmod 2$ for all n.

Note: Here mod 2 can me changed to any mod p but cannot be completely removed. For example, $C_n(\mathcal{F}) = 0$ implies $C_{n+1}(\mathcal{F}) = 0$, which does not hold for functions $\xi \in \mathbb{X}$.

Theorem 2. [Garrabrant, P., 2015+]

The problem whether $C_n(\mathcal{F}) - C_n(\mathcal{F}') = 0 \bmod 2$ for all $n \geq 1$, is undecidable.

Not convinced yet?

Corollary 1. For all k large enough, there exists $\mathcal{F}, \mathcal{F}' \subset S_k$ such that the smallest n for which $C_n(\mathcal{F}) \neq C_n(\mathcal{F}')$ mod 2 satisfies

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

Corollary 2. There exist two finite sets of patterns $\mathcal{F}$ and $\mathcal{F}'$, such that the problem of whether $C_n(\mathcal{F}) = C_n(\mathcal{F}')$ mod 2 for all $n \in \mathbb{N}$, is independent of ZFC.

Computational Complexity Classes

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

e.g. $\oplus$Hamiltonian cycles in $G \in \oplus\mathsf{P}$

$\mathsf{P} \neq \oplus\mathsf{P}$ is similar to $\mathsf{P} \neq \mathsf{NP}$

In fact, $\mathsf{P} = \oplus\mathsf{P}$ implies $\mathsf{PH} = \mathsf{NP} = \mathsf{BPP}$ [by Toda's theorem]

EXP = exponential time

$\oplus\mathsf{EXP}$ = exponential time version of $\oplus\mathsf{P}$

e.g. $\oplus$Hamiltonian 3-connected graphs on n vertices $\in \oplus\mathsf{EXP}$

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

believed to be correct for more technical CC reasons,

Complexity Implications

Theorem 3. [Garrabrant, P., 2015+]
If $\mathsf{EXP} \neq \oplus\mathsf{EXP}$, then there exists a finite set of patterns $\mathcal{F}$, such that the sequence $\{C_n(\mathcal{F})\}$ cannot be computed in time polynomial in n.

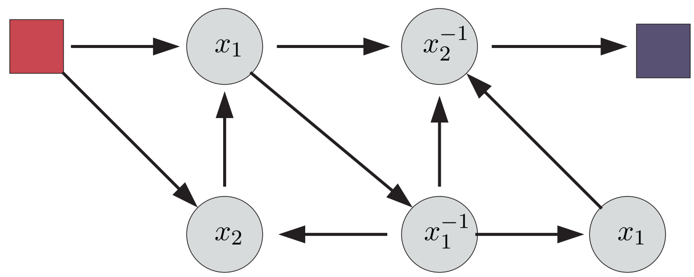
Remark 1: All sequences with D-finite g.f. can be computed in time polynomial in n.

Remark 2: This also answers to 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 $f(n)$?

Two-stack Automata

In the Main Lemma, $\mathbb{X} = \{\xi_\Gamma\}$, where $\xi_\Gamma(n)$ = number of balanced paths of some two-stack automaton Γ.



Γ

Here $\xi(1) = \xi(2) = \xi(3) = 0$, $\xi(4) = 1$, $\xi(5) = 0$, $\xi(6) = 1$.

Note: Two-stack automata are as powerful as Turing machines.

How not to be P-recursive

Lemma 1. Let $\{a_n\}$ be a P-recursive sequence, and let $\overline{\alpha} = (\alpha_1, \alpha_2, \ldots) \in \{0,1\}^\infty$, $\alpha_i = a_i \bmod 2$. Then there is a finite binary word $w \in \{0,1\}^*$ 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

$$0,\ 1,\ 0,0,\ 0,1,\ 1,0,\ 1,1,\ 0,0,0,\ 0,0,1,\ 0,1,0,\ \ldots$$

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

Main Lemma: 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 $P, Q, B, B', E, T_1, \dots, T_v, Z_1, \dots, Z_m$.

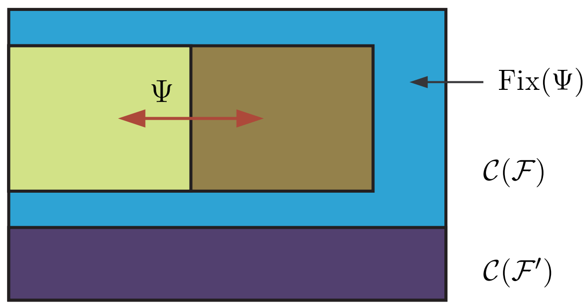
(2) Thinking of T_i's as vertices of Γ and Z_j as variables x_p, y_q, select block matrices $\mathcal{F}$ to simulate Γ. Let $\mathcal{F}' = \mathcal{F} \cup \{B, B'\}$.

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

Sample of forbidden matrices in $\mathcal{F}$:

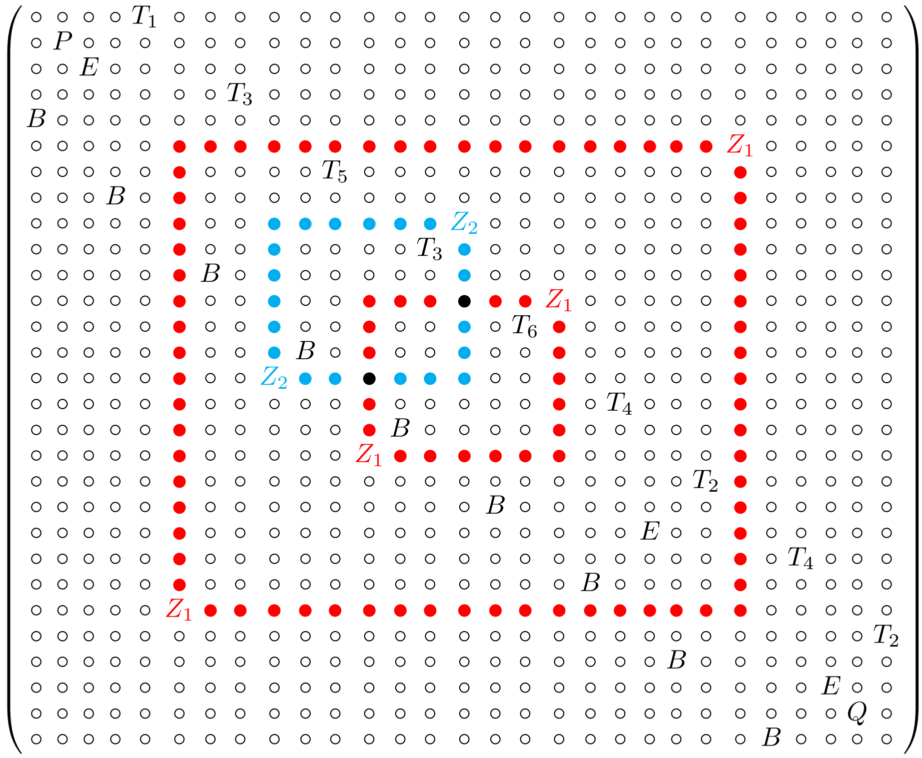
$$
\begin{pmatrix}
\circ & \circ & T_i & \circ & \circ & \circ & \circ & \circ \\
\circ & \circ & \circ & \circ & \circ & T_j & \circ & \circ \\
L & \circ & \circ & \circ & \circ & \circ & \circ & \circ \\
\circ & \circ & \circ & \circ & \circ & \circ & \circ & Z_p \\
\circ & \circ & \circ & \circ & \circ & \circ & T_k & \circ \\
\circ & B' & \circ & \circ & \circ & \circ & \circ & \circ \\
\circ & \circ & \circ & \circ & R & \circ & \circ & \circ \\
\circ & \circ & \circ & Z_p & \circ & \circ & \circ & \circ
\end{pmatrix}
\qquad
\begin{pmatrix}
\circ & \circ & T_i & \circ & \circ & \circ \\
\circ & \circ & \circ & \circ & \circ & T_2 \\
L & \circ & \circ & \circ & \circ & \circ \\
\circ & \circ & \circ & E & \circ & \circ \\
\circ & \circ & \circ & \circ & Q & \circ \\
\circ & B' & \circ & \circ & \circ & \circ
\end{pmatrix}
\qquad
\begin{pmatrix}
\circ & \circ & T_j \\
Z_p & \circ & \circ \\
\circ & Z_q & \circ
\end{pmatrix}
$$

Final count:



Example

$M =$



.

Notes on the proof

(i) We use exactly 6854 partial patterns.

(ii) 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 2 paragraphs, but it took over a year of hard work to state. Natural extensions remain open.

Conjecture 0. [Garrabrant, P.] Let $\overline{\alpha}$ be as in Lemma 1. Then $\overline{\alpha}$ has $O(n)$ subwords of length n.

The non-ADE extension

Theorem 1′. [Garrabrant, P., in preparation]

There is a set $\mathcal{F} \subset S_{80}$, s.t. the g.f. for $\{C_n(\mathcal{F})\}$ is **not** ADE.

Lemma 1′. Let $\{a_n\}$ be an integer sequence, and let $\{n_i\}$ be the sequences of indices with **odd** a_n. Suppose

1) for all $b, c \in \mathbb{N}$, there exists k such that $n_k = b \mod 2^c$,
2) $n_k / n_{k+1} \to 0$ as $k \to \infty$.

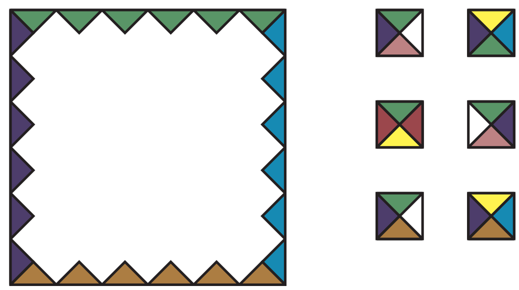
Then the g.f. for $\{a_n\}$ is **not** ADE.

Corollary. Let $\{a_n\}$ be an integer sequence, s.t. a_n is odd if only if $n = k! + k$, for some k. Then the g.f. for $\{a_n\}$ is **not** ADE.

Note: cf. EC2, Exc. 6.63c.

First prequel: Wang tilings

Long and classical story going back to 1960s (Wang, Berger, Robinson, etc.) Key result: tileability of the plane with fixed set of Wang tiles is undecidable. Delicate part: ensuring that the “seed tile” must be present in a tiling. This is what we do by introducing $\mathcal{F}'$.



Second prequel: Kontsevich's problem

Let G be a group and $\mathbb{Z}[G]$ denote its group ring. Fix $u \in \mathbb{Z}[G]$.
Let $a_n = [1]u^n$, where $[g]\,u$ denote the value of u on $g \in G$.
In 2014, Maxim Kontsevich asked whether $\{a_n\}$ is always P-recursive when $G \subseteq \mathrm{GL}(k, \mathbb{Z})$.

Theorem 4. [Garrabrant, P., 2015+]
There exists an element $u \in \mathbb{Z}[\mathrm{SL}(4, \mathbb{Z})]$, such that the sequence $\{\,[1]u^n\}$ is not P-recursive.

Note: Proof uses the same Lemma 1(!)
When $G = \mathbb{Z}^k$ or $G = F_k$, the sequence $\{a_n\}$ is known to be P-recursive for all $u \in \mathbb{Z}[G]$ (Haiman, 1993).

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. For forbidden sets with a single permutation $|\mathcal{F}| = |\mathcal{F}'| = 1$, the Wilf-equivalence problem is decidable.

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

Conjecture 4. There exists a finite set of patterns $\mathcal{F}$, s.t.
computing $\{C_n(\mathcal{F})\}$ is $\#\mathsf{EXP}$-complete, and
computing $\{C_n(\mathcal{F}) \bmod 2\}$ is $\oplus\mathsf{EXP}$-complete.

Grand Finale:

A story how Doron Zeilberger lost faith and then lost \$100.

Thank you!