Umění počítat a mocninné řady

Martin Klazar
Katedra aplikované matematiky, MFF UK

Přehled

1. Proč mocninné řady
2. Mocninné řady v kombinatorické enumeraci
3. Mocninné řady v teorii čísel
4. Mocninné řady v teorii pravděpodobnosti
5. Mocninné řady v informatice

–Proč mocninné řady 1–

Mocninná řada s *koeficienty* a_n je výraz

$$F(x) = \sum_{n=0}^{\infty} a_n x^n = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots,$$

kde a_n jsou čísla (celá, reálná, komplexní) a x je proměnná. $F(x)$ je *generující funkce* posloupnosti $(a_0, a_1, a_2, \ldots)$; a_n je často počet čehosi.

A generating function is a clothesline on which we hang up a sequence of numbers for display.

(H. S. Wilf, *generatingfunctionology*, Academic Press, 1994)

• zapouzdření nekonečného objektu $(a_0, a_1, \ldots)$ do vyšší entity $F(x)$, např.

$(1, 1, 2, 3, 5, 8, 13, \ldots)$ jako $F(x) = 1/(1 - x - x^2)$

• dvě tváře m. řad, diskrétní a analytická, např.

$(1, 1, 1, \ldots)$ a funkce $\mathbf{C}\backslash\{1\} \ni z \mapsto 1/(1 - z)$

• překlad struktury objektů počítaných a_n do řeči algebraických vlastností $F(x)$ a naopak

–Proč mocninné řady 2–

Mocninné řady a generující funkce v matematice a informatice

• **matematická analýza** (funkce komplexní proměnné, řešení diferenciálních rovnic, aplikace)
• **teorie pravděpodobnosti** (diskrétní rozdělení, náhodné procházky, tzv. charakteristické funkce)
• **teorie čísel** (obyčejné gf v aditivní TČ, Dirichletovy řady v multiplikativní TČ, modulární formy, zeta funkce)
• **algebraická geometrie** (lokální parametrizace křivek)
• **diskrétní matematika**
• **kombinatorická enumerace** (počítání různých struktur)
• **teoretická informatika** (analýza algoritmů, teorie formálních jazyků)
• **algebra a logika** (mocninné řady jsou zajímavé objekty i samy o sobě)

–Proč mocninné řady 3–

Hlavní typy generujících funkcí (gf) posloupností $(a_0, a_1, a_2, \ldots)$:

- *obyčejné gf*

$$F(x) = \sum_{n=0}^{\infty} a_n x^n = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots$$

- *exponenciální gf (Taylorovy řady)*

$$F(x) = \sum_{n=0}^{\infty} \frac{a_n x^n}{n!} = a_0 + a_1 x + \frac{a_2 x^2}{2} + \frac{a_3 x^3}{6} + \cdots$$

- *Dirichletovy řady*

$$F(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s} = a_1 + \frac{a_2}{2^s} + \frac{a_3}{3^s} + \frac{a_4}{4^s} + \cdots$$

Obecně: $\lambda_1 < \lambda_2 < \ldots$ buďte reálná čísla, pak

$$F(s) = \sum_{n=0}^{\infty} a_n \mathrm{e}^{-\lambda_n s}$$

dává ogf pro $\lambda_n = n$ ($x = \mathrm{e}^{-s}$) a Dirichletovu řadu pro $\lambda_n = \log n$. Další zobecnění: více proměnných, koeficienty a_n z okruhu R, ...

–Proč mocninné řady 4–

Násobení ogf. Nechť a_n (resp. b_n) je počet A-struktur (resp. B-struktur) váhy $v(A) = n$ (resp. $v(B) = n$), např. počet nějakých grafů na množině $[n] = \{1, 2, \ldots, n\}$. Součin odpovídajících ogf

$$\sum_{n\geq 0} a_n x^n \sum_{n\geq 0} b_n x^n = \sum_{n\geq 0} \Big(\sum_{k=0}^{n} a_k b_{n-k} \Big) x^n$$

má tento smysl: koeficient u x^n je počet dvojic (α, β), kde α je A-struktura, β je B-struktura a $v(A) + v(B) = n$.

Násobení egf. Nechť a_n (resp. b_n) je počet A-struktur (resp. B-struktur) na množině $[n]$. Součin odpovídajících egf

$$\sum_{n\geq 0} \frac{a_n x^n}{n!} \sum_{n\geq 0} \frac{b_n x^n}{n!} = \sum_{n\geq 0} \Big(\sum_{k=0}^{n} \binom{n}{k} a_k b_{n-k} \Big) \frac{x^n}{n!}$$

má tento smysl: koeficient u x^n je počet dvojic $((X, \alpha), (Y, \beta))$, kde (X, Y) je rozklad množiny $[n]$, α je A-struktura na X a β je B-struktura na Y.

–Proč mocninné řady 5–

Příklad na násobení ogf (na egf později). Nechť a_n (resp. b_n) je počet slov délky n nad $\{a,b,c\}$ (resp. nad $\{1,2,3\}$). Pak $a_n = b_n = 3^n$ a

$$\begin{aligned}\sum_{n\geq 0} a_n x^n \sum_{n\geq 0} b_n x^n &= \Big(\sum_{n\geq 0} 3^n x^n\Big)^2 \\ &= \sum_{n\geq 1} (n+1)3^n x^n\end{aligned}$$

a $(n+1)3^n = \#$ slov nad abecedou $\{a,b,c,1,2,3\}$ typu "nejprve písmena, pak číslice".

Násobení Dř. V součinu Dirichletových řad

$$\sum_{n\geq 1} \frac{a_n}{n^s} \sum_{n\geq 1} \frac{b_n}{n^s} = \sum_{n\geq 1} \Big(\sum_{d|n} a_d b_{n/d}\Big) \frac{1}{n^s}$$

dostáváme Dirichletovu konvoluci (a_n) a (b_n). Např.

$$\zeta(s)^2 = \left(\sum_{n\geq 1} \frac{1}{n^s}\right)^2 = \sum_{n\geq 1} \frac{\tau(n)}{n^s},$$

kde $\tau(n)$ je počet dělitelů čísla n.

–Proč mocninné řady 6–

Algebraický pohled. Operace $+$ a $\times$ na množině $\mathbf{C}[[x]]$ formálních součtů $\sum_{n\geq 0} a_n x^n$, $a_n \in \mathbf{C}$:

$$\sum_{n\geq 0} a_n x^n + \sum_{n\geq 0} b_n x^n \;=\; \sum_{n\geq 0} (a_n + b_n) x^n$$

$$\sum_{n\geq 0} a_n x^n \times \sum_{n\geq 0} b_n x^n \;=\; \sum_{n\geq 0} \Big(\sum_{k=0}^{n} a_k b_{n-k} \Big) x^n.$$

$(\mathbf{C}[[x]], +, \times)$ je obor integrity (komut. okruh s 1, $FG = 0 \Rightarrow F = 0$ nebo $G = 0$).

Jednotky: $1/\sum_{n\geq 0} a_n x^n$ existuje $\iff$ $a_0 \neq 0$.

Těleso zlomků: množina $\mathbf{C}((x))$ form. součtů $\sum_{n\geq k} a_n x^n$, kde $k \in \mathbf{Z}$ (Laurentovy řady).

Formální konvergence. Nechť $[x^n]F$ je koeficient u x^n v F. Posloupnost m. řad $(F_1, F_2, \ldots)$ (formálně) konverguje, pokud pro každé $n \geq 0$ je posloupnost koeficientů

$$([x^n]F_1, [x^n]F_2, [x^n]F_3, \ldots)$$

od jistého členu dále konstantní. Pak $F_n \to F$.

–Proč mocninné řady 7–

Nechť

$$\operatorname{ord}(F) = \min\{n \geq 0 \mid [x^n]F \neq 0\}, \quad \operatorname{ord}(0) = \infty.$$

Nekonečné součty a součiny m. řad

$$\sum_{n=1}^{\infty} F_n \quad \text{a} \quad \prod_{n=1}^{\infty} (1 + G_n)$$

jsou formální limity částečných součtů a částečných součinů. Existují, právě když $\operatorname{ord}(F_n) \to \infty$ a $\operatorname{ord}(G_n) \to \infty$. Např.

$$\prod_{n=1}^{\infty} (1 + x^n) = 1 + x + x^2 + 2x^3 + 2x^4 + 3x^5 + \cdots$$

Skládání. Nechť $F(x) = \sum_{n\geq 0} a_n x^n$ a G splňuje $G(0) = [x^0]G = 0$, pak $F(G(x))$ definujeme jako formální součet

$$F(G(x)) = \sum_{n\geq 0} a_n G(x)^n$$

(OK, protože $\operatorname{ord}(a_n G^n) \geq n$). Naopak, pokud $G(0) \neq 0$ a F není polynom, nemá substituce $F(G(x))$ smysl. Skládání m. řad je asociativní.

–Proč mocninné řady 8–

$G(x)$ je **kompoziční inverz** m. řady $F(x)$, značíme $G = F^{\langle -1\rangle}$, pokud $F(G) = x$. Nutně $\mathrm{ord}(F) = \mathrm{ord}(G) = 1$.

Tvrzení. F má kompoziční inverz, právě když $\mathrm{ord}(F) = 1$. Dále platí $F^{\langle -1\rangle}(F) = F(F^{\langle -1\rangle}) = x$.

Lagrangeova inverzní formule. Pro $F \in \mathbf{C}[[x]]$ s $\mathrm{ord}(F) = 1$,

$$[x^n]F^{\langle -1\rangle} = \frac{1}{n}[x^{n-1}]\Big(\frac{x}{F(x)}\Big)^n.$$

Ekvivalentně: pokud $G(0) \neq 0$ a F je řešením rovnice $F = xG(F)$, pak

$$[x^n]F = \frac{1}{n}[x^{n-1}](G(x))^n.$$

Příklad. Rovnici $xF^5 - F + x = 0$ v $\mathbf{C}[[x]]$ vyřešíme snadno: $F = x(1 + F^5)$, a tak, pro $n = 5m + 1$,

$$[x^n]F = \frac{1}{n}[x^{n-1}](1 + x^5)^n = \frac{1}{n}\binom{n}{m}$$

a jinak $[x^n]F = 0$. (V $\mathbf{C}[[x]]$ je jediné řešení.)

–Proč mocninné řady 9–

Analytický pohled. Pro m. řadu

$$F(z) = \sum_{n \geq 0} a_n z^n \in \mathbf{C}[[z]]$$

máme právě jedno číslo R — *poloměr kovergence* $F(z)$ — že $0 \leq R \leq \infty$ a $F(z)$ absolutně konverguje pro $|z| < R$ a diverguje pro $|z| > R$. Kolik je R?

• Hadamard (1892, dizertace):

$$R = \frac{1}{\limsup_{n \to \infty} |a_n|^{1/n}}.$$

$\rightsquigarrow$ Koeficienty a_n pro $n \to \infty$ rostou zhruba jako $(1/R)^n$.

• $R = \min |s|$, $s \in \mathbf{C}$ je singularita *funkce* $F(z)$.
$\rightsquigarrow$ R je modul singularity nejbližší k 0.

• Pringsheim ($\leq$1932): Pokud $a_n \geq 0$ pro všechny $n \in \mathbf{N}_0$, pak R je singularitou $F(z) = \sum_{n \geq 0} a_n z^n$.
$\rightsquigarrow$ Singularitu nejbližší k 0 pak stačí hledat na kladné části reálné osy.

–Proč mocninné řady 10–

Příklady. 1. $a_n = \#$ zobrazení z $\{1, 2, \ldots, n\}$ *na* $\{1, 2, \ldots, m\}$, $m \leq n$ ($\#$ surjekcí). Ukážeme, že

$$F(z) = \sum_{n=0}^{\infty} \frac{a_n z^n}{n!} = \frac{1}{2 - \mathrm{e}^z}.$$

Ale $2 - \mathrm{e}^z = 0 \iff z = \log 2 + 2k\pi i, k \in \mathbf{Z}$, tedy $R = \log 2$ a $a_n \sim (1/\log 2)^n n!$.

2. $a_n = \#$ dobrých uzávorkování s n páry závorek, např. $a_3 = 5$: ()()(), ()(()), (())(), (()()) a ((())). Spočte se celkem snadno, že

$$F(z) = \sum_{n \geq 0} a_n z^n = 1 + z + 2z^2 + \cdots = \frac{1}{2z}(1 - \sqrt{1 - 4z}).$$

Ale $1 - 4z = 0 \iff z = 1/4$, tedy $R = 1/4$ a $a_n \sim 4^n$. (Přesněji: $a_n = \frac{1}{n+1}\binom{2n}{n}$.)

3. O dva slajdy dříve, v příkladu na LIF, jsme měli $F(z) = \sum_{n \geq 0} a_n z^n$ splňující

$$zF^5 - F + z = 0.$$

Jak určíme R bez vzorce pro a_n?

–Proč mocninné řady 11–

Věta o implicitní funkci a Pringsheim: dvojice $(z, F) = (R, F(R))$ musí být řešením soustavy

$$zF^5 - F + z = 0 \;\; \& \;\; \partial_F(zF^5 - F + z) = 5zF^4 - 1 = 0.$$

Jediné řešení se $z > 0$ je $(\frac{4^{4/5}}{5}, \frac{1}{4^{1/5}})$. Takže $R = \frac{4^{4/5}}{5}$ a $a_n \sim (1/R)^n = \left(\frac{5}{4^{4/5}}\right)^n = (1.64938\ldots)^n$, což souhlasí s $a_n = \frac{1}{n}\binom{n}{(n-1)/5}$.

Obecněji. Nechť $f(z) = \sum_{n\geq 0} f_n z^n$ má v $R > 0$ singularitu a je analytická v oblasti $\Delta = \Delta(r, \phi) = \{z : \; |z| < r, \; |\arg(z - R)| > \phi\}$, $r > R$ a $0 < \phi < \pi/2$ ("camembertová" oblast). Nechť $\sigma(z), \tau(z)$ jsou lin. kombinace funkcí ze škály ($\alpha, \beta \in \mathbf{C}$)

$$\frac{1}{(1 - z/R)^\alpha}\Big(\frac{1}{z/R}\log\frac{1}{1 - z/R}\Big)^\beta.$$

Věta. (Flajolet & Odlyzko, 1990). V této situaci platí přenos asymptotik ($z \to R, z \in \Delta$ a $n \to \infty$)

$$f(z) = \sigma(z) + O(\tau(z)) \Rightarrow f_n = \sigma_n + O(\tau_n).$$

–Proč mocninné řady 12–

Obecněji o implicitní funkci.

Věta. (Odlyzko, 1995). Nechť m. řady $E(z,w) = \sum_{i,j\geq 0} e_{ij} z^i w^j$ s $e_{00} = 0$, $e_{01} < 1$ a $e_{ij} \geq 0$ a $F(z) = \sum_{i\geq 1} f_i z^i$ s $f_i \geq 0$ splňují:

(a) $F(z)$ je analytická v $z = 0$.
(b) $F(z) = E(z, F(z))$.
(c) $f_i, f_j, f_k > 0$ a $(j-i, k-i) = 1$ pro nějaká tři čísla $0 < i < j < k$.
(d) Existují čísla $R, S, \delta > 0$ taková, že $E(z,w)$ je analytická v $|z| < R+\delta$ a $|w| < S+\delta$, $\underline{E(R,S) = S}$, $E_z(R,S) \neq 0$, $\underline{E_w(R,S) = 1}$ a $E_{ww}(R,S) \neq 0$.

Potom R je poloměr konvergence $F(z)$, $F(R) = S$ a pro $n \to \infty$ platí

$$f_n = (1 + o(1)) \sqrt{\frac{R \cdot E_z(R,S)}{2\pi \cdot E_{ww}(R,S)}} \cdot n^{-3/2} \cdot \Big(\frac{1}{R}\Big)^n.$$

–Proč mocninné řady 13–

Experiment v r. 2003, resp. 2006, s vyhledáváním v internetové databázi vědeckých časopisů SCIENCE DIRECT (přes 1700 časopisů). Dotaz na **“power series”** v názvech, abstraktech a klíčových slovech vrátil 1324, resp. 1984, článků. Dotaz na **“generating function”** vrátil 1250, resp. 1890, článků. Některé časopisy:

Advances in Mathematics
Chemical Physics Letters
Composite Structures
Chaos, Solitons & Fractals
Discrete Mathematics
Fluid Phase Equilibria
Fuzzy Sets and Systems
Historia Mathematica
Information Processing Letters
Insurance: Mathematics and Economics
International J. of Pressure Vessels and Piping

International Review of Financial Analysis
J. of Aerosol Science
J. of Crystal Growth
J. of Discrete Algorithms
J. of Number Theory
J. of Petroleum Science
J. of Statistical Planning and Inference
Microelectronics and Reliability
Neurocomputing
Nuclear Physics B
Ocean Engineering
Optics Communications
Performance Evaluation
Powder Technology
Reliability Engineering & System Safety
Signal Processing
Solar Energy Materials and Solar Cells
Stochastic Processes and their Applications
Tectonophysics
Theoretical Computer Science
Theoretical Population Biology
Thin Solid Films
Vacuum
Vistas in Astronomy

–Kombinatorická enumerace 1–

Exponenciální generující funkce (egf) posloupnosti $a_0, a_1, \ldots$ je mocninná řada

$$A(x) = \sum_{n=0}^{\infty} \frac{a_n x^n}{n!} = a_0 + \frac{a_1 x}{1!} + \frac{a_2 x^2}{2!} + \frac{a_3 x^3}{3!} + \cdots$$

Součinová formule: Posloupnosti $(a_0, a_1, \ldots)$ a $(b_0, b_1, \ldots)$ mějte egf $A(x)$ a $B(x)$ a posloupnost $(c_0, c_1, \ldots)$ buď dána vztahem

$$c_n = \sum_{k=0}^{m} \binom{n}{k} a_k b_{n-k}$$

($c_n = \#$ C-struktur na $[n]$ tvaru $((X, \alpha), (Y, \beta))$, kde (X, Y) je rozklad $[n]$, α je A-struktura na X a β je B-struktura na Y). Pak

$$C(x) = \sum_{n=0}^{\infty} \frac{c_n x^n}{n!} = A(x)B(x).$$

Příklad. Nechť $a_n = b_n = 1$, pak $c_n = \#$ (podmnožin množiny $[n]$) $= 2^n$. Vskutku,

$$C(x) = A(x)B(x) = \mathrm{e}^x \mathrm{e}^x = \mathrm{e}^{2x} = \sum_{n=0}^{\infty} \frac{2^n x^n}{n!}.$$

–Kombinatorická enumerace 2–

Kompoziční formule. Nechť $A(x)$ a $B(x)$ jsou egf počtů nějakých A-struktur a B-struktur na množinách $[n]$, $n \in \mathbf{N}$. Odvozená C-struktura je daná rozkladem $\{Y_1, \ldots, Y_k\}$ množiny $[n]$ na neprázdné množiny, volbou A-struktury na $[k]$ a volbami B-struktur na množinách $Y_1, \ldots, Y_k$. Pak počty C-struktur mají egf danou kompozicí

$$C(x) = \sum_{n=0}^{\infty} \frac{c_n x^n}{n!} = A(B(x)).$$

Exponenciální formule je speciální případ s $a_n = 1$ a tedy $A(x) = \mathrm{e}^x$: Je-li $c_n = \#$ struktur na $[n]$ typu $(Y_1, \beta_1, Y_2, \beta_2, \ldots, Y_k, \beta_k)$, kde $\{Y_1, \ldots, Y_k\}$ je rozklad $[n]$ a β_i je B-struktura na Y_i, pak

$$C(x) = \sum_{n=0}^{\infty} \frac{c_n x^n}{n!} = \mathrm{e}^{B(x)}.$$

Poznámka. V obou formulích je nutné, aby $b_0 = 0$, tj. $B(x) = b_1 x + b_2 x^2/2! + \cdots$, jinak dosazení $B(x)$ nedává obecně smysl.

–Kombinatorická enumerace 3–

Uvedeme několik příkladů na tyto formule.

Bellova čísla. Nechť $c_n = \#$ neusp. rozkladů $\{Y_1, \ldots, Y_k\}$ množiny $[n]$ na neprázdné množiny. Počty c_n se dostanou exp. konstrukcí s $b_n = 1$ pro $n \geq 1$ a $b_0 = 0$, takže $B(x) = \exp(x) - 1$. Exp. formule dává

$$C(x) = \sum_{n=0}^{\infty} \frac{c_n x^n}{n!} = \mathrm{e}^{B(x)} = \mathrm{e}^{\mathrm{e}^x - 1}.$$

Uspořádaná Bellova čísla (# surjekcí). Nyní čísla c_n počítají uspořádané rozklady $(Y_1, \ldots, Y_k)$ množiny $[n]$. Dostanou se komp. konstrukcí s $a_n = n!$, $b_n = 1$ pro $n \geq 1$ a $b_0 = 0$. Takže $A(x) = \sum_{n \geq 0} n! x^n/n! = 1/(1-x)$, $B(x) = \exp(x) - 1$ a

$$C(x) = \sum_{n=0}^{\infty} \frac{c_n x^n}{n!} = A(B(x)) = \frac{1}{1 - (\mathrm{e}^x - 1)} = \frac{1}{2 - \mathrm{e}^x}.$$

Odtud se hned dostane asymptotika ($c > 0$ je konstanta)

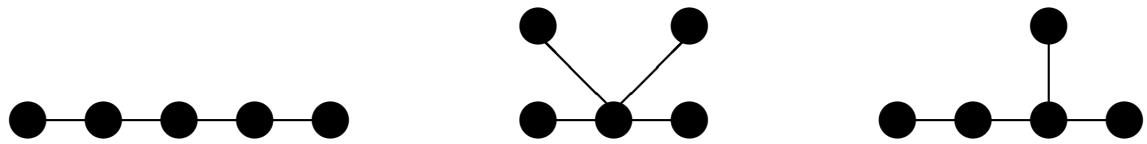
$$c_n = (c + o(1))(1/\log 2)^n n! = (c + o(1))(1.44269\ldots)^n n!.$$

–Kombinatorická enumerace 4–

Odvodíme **Cayleyho vzorec** (Cayley, 1857)

$$t_n = n^{n-2}$$

pro počet stromů (souvislých grafů bez kružnic) na množině vrcholů $\{1, 2, \ldots, n\}$.
Např. $t_5 = 5^3 = 125$, protože pro 5 vrcholů máme jen tři možné neizomorfní typy stromů (cestu, hvězdu a vidličku):



a ty se na množině $\{1, 2, 3, 4, 5\}$ realizují $3\binom{5}{3}2 + 5 + 3\binom{5}{3}2 = 5 + 60 + 60 = 125$ způsoby.
Nebudeme pracovat s egf čísel t_n, ale s egf

$$K(x) = \sum_{n=1}^{\infty} \frac{k_n x^n}{n!}$$

počtů k_n kořenových stromů (stromů s vyznačeným vrcholem). Zřejmě $k_n = n t_n$.

–Kombinatorická enumerace 5–

Kořenový strom T se po vypuštění kořene rozpadne na množinu několika kořenových stromů, které mají dohromady o 1 méně vrcholů a z nichž se T dá jednoduše zrekonstruovat. Takže:

$$\begin{aligned}&\#\{\text{kořenové stromy } T \text{ na } [n]\}\\&= \#\{(A,(B_1,T_1),(B_2,T_2),\ldots,(B_k,T_k))\},\end{aligned}$$

kde $\{A,B_1,\ldots,B_k\}$ je rozklad $[n]$ na neprázdné množiny, $|A|=1$ (kořen T) a T_i je kořenový strom na B_i. Podle součinové a exponenciální formule dostáváme rovnici

$$K(x) = \frac{1x^1}{1!}\exp(K(x)) = x\exp(K(x)).$$

Vyřešíme ji Lagrangeovou inverzní formulí:

$$\begin{aligned}k_n &= n![x^n]K(x) = \frac{n!}{n}[x^{n-1}]\exp(x)^n\\&= \frac{n!}{n}[x^{n-1}]\exp(nx) = \frac{n!\cdot n^{n-1}}{n\cdot(n-1)!}\\&= n^{n-1}\end{aligned}$$

a tedy $t_n = k_n/n = n^{n-1}/n = n^{n-2}$.

–Kombinatorická enumerace 6–

Střídavé permutace. $\sigma = \sigma_1\sigma_2\ldots\sigma_n$ je *střídavá* permutace čísel $1, 2, \ldots, n$, pokud

$$\sigma_1 < \sigma_2 > \sigma_3 < \sigma_4 > \sigma_5 < \cdots.$$

$p_n = \#$ stř. permutací =?? Klademe $p_0 = 1$. Zkusíme pomocí egf $P(x)$ rovné

$$\begin{aligned}\sum_{n\geq 0} \frac{p_n x^n}{n!} &= \sum_{2m+1\geq 1} \frac{p_{2m+1}x^{2m+1}}{(2m+1)!} + \sum_{2m\geq 0} \frac{p_{2m}x^{2m}}{(2m)!} \\ &= L(x) + S(x).\end{aligned}$$

Pokud $\sigma \in L$ a $|\sigma| > 1$, pak $\sigma = (\kappa, n, \lambda)$, kde $\kappa, \lambda \in L$. Pokud $\sigma \in S$ a $|\sigma| > 0$, pak $\sigma = (\kappa, n, \lambda)$, kde $\kappa \in L$ a $\lambda \in S$. A naopak ...
Takže $P(x) = L(x) + S(x)$ a

$$(L(x) - x)' = L(x)^2 \quad \text{a} \quad (S(x) - 1)' = L(x)S(x).$$

Vyřešením diferenciálních rovnic dostaneme

$$\sum_{n\geq 0} \frac{p_n x^n}{n!} = L(x) + S(x) = \tan x + \frac{1}{\cos x}.$$

Nenulový koeficient u x^n v Taylorově rozvoji funkcí $\sec x = 1/\cos x$ a $\tan x$ je tedy roven $p_n/n!$.

–Kombinatorická enumerace 7–

Ogf — racionální funkce. Důležitou třídou ogf jsou racionální m. řady, charakterizované touto větou:

Věta. Následující tři vlastnosti mocninné řady $F(x) = \sum_{n\geq 0} a_n x^n \in \mathbf{C}[[x]]$ jsou ekvivalentní.

1. $F(x) = p(x)/q(x)$, kde p, q jsou polynomy.
2. Pro $n > n_0$ platí

$$a_n + c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_r a_{n-r} = 0,$$

kde $c_i \in \mathbf{C}$ jsou konstanty.
3. Pro $n > n_0$ platí, že

$$a_n = p_1(n)\alpha_1^n + p_2(n)\alpha_2^n + \cdots + p_k(n)\alpha_k^n,$$

kde p_i jsou polynomy a $\alpha_i \in \mathbf{C}$ jsou různá čísla (kořeny polynomu $q(x)$).

Důsledek. Operace Hadamardova součinu

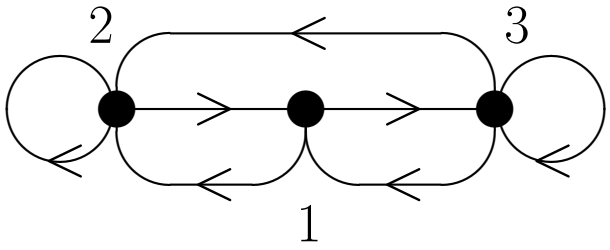
$$\sum_{n\geq 0} a_n x^n * \sum_{n\geq 0} b_n x^n = \sum_{n\geq 0} a_n b_n x^n$$

zachovává třídu racionálních m. řad.

–Kombinatorická enumerace 8–

Metoda přechodové matice (transfer matrix method). Úlohy "lokálního" charakteru či s "konečnou" historií vedou na racionální ogf.

G buď orientovaný graf, násobné šipky a smyčky jsou povoleny. *Procházka* (v G) délky n z vrcholu u do vrcholu v je posloupnost n na sebe navazujících šipek $e_1 e_2 \dots e_n$, začínající v u a končící ve v. G může vypadat třeba takto:



Nechť má každá hrana e z G váhu $w(e) \in R$ (R je komut. okruh s 1). Pro procházku $P = e_1 e_2 \dots e_n$ definujeme $w(P) = w(e_1) w(e_2) \dots w(e_n)$. Grafu G, kde $V(G) = \{v_1, \dots, v_p\}$, a délce procházky $n \in \mathbf{N}_0$ přiřadíme $p \times p$ matici $A(n) = (A_{ij}(n))$,

$$A_{ij}(n) = \sum_{P \text{ z } v_i \text{ do } v_j,\ |P|=n} w(P).$$

–Kombinatorická enumerace 9–

Klademe $A_{ij}(0) = \delta_{ij}$. Pro $n = 1$ máme matici sousednosti $A = A(1)$, $A_{ij} = \sum$ vah šipek jdoucích z v_i do v_j.
Pozorování: $A_{ij}(n) = (A^n)_{ij}$ a tedy $A(n) = A^n$.

Definujeme ogf a matici

$$\begin{aligned} F_{ij}(G,x) &= \sum_{n\geq 0} A_{ij}(n)x^n \in R[[x]] \\ F(G,x) &= (F_{ij}(G,x)) \in R[[x]]^{p\times p}. \end{aligned}$$

Díky $R[[x]]^{p\times p} \cong R^{p\times p}[[x]]$ a pozorování máme

$$F(G,x) = \sum_{n\geq 0} A(n)x^n = \sum_{n\geq 0} A^n x^n = (I - xA)^{-1},$$

z čehož plyne
Věta (MPM). $F_{ij}(G,x)$ je $((I-xA)^{-1})_{ij}$, a tak

$$F_{ij}(G,x) = \frac{(-1)^{i+j}\det(I - xA : j,i)}{\det(I-xA)}.$$

$F_{ij}(G,x)$ je tedy racionální m. řada z $R[[x]]$ a posloupnost $A_{ij}(0)$, $A_{ij}(1)$, $A_{ij}(2),\ldots$ splňuje lineární rekurenci s konstantními koeficienty.

–Kombinatorická enumerace 10–

Příklad. Nechť a_n je počet slov $u = u_1 u_2 \dots u_n$ délky n nad abecedou $\{1,2,3\}$ takových, že ani 11 ani 23 se neobjevuje jako $u_i u_{i+1}$. Kolik je a_n?

Definujeme orientovaný graf G na $\{1,2,3\}$ tak, že $i \to j$, pokud v u může následovat j po i. G je na předpředešlém slajdu. Nyní $R = \mathbf{Z}$ a

$$A = A(1) = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}.$$

Označíme $Q(x) = \det(I - xA) = 1 - 2x - x^2 + x^3$ a $Q_{ij} = \det(I - xA : j, i)$. Podle MPM máme

$$\begin{aligned} \sum_{n \geq 0} a_{n+1} x^n &= \frac{\sum_{i,j=1}^{3} Q_{ij}(x)}{Q(x)} \\ &\vdots \\ &= \frac{3 + x - x^2}{1 - 2x - x^2 + x^3}. \end{aligned}$$

Odtud $a_n = 2a_{n-1} + a_{n-2} - a_{n-3}$ pro $n \geq 4$ ($a_1 = 3$, $a_2 = 7$, $a_3 = 16$).

–Teorie čísel 1–

ogf v aditivní TČ. V r. 1770 Lagrange dokázal, že každé číslo $n \in \mathbf{N}_0$ je součtem 4 čtverců, např. $5 = 2^2 + 1^2 + 0^2 + 0^2$, $300 = 16^2 + 6^2 + 2^2 + 2^2$. (Čísla tvaru $8n + 7$ nejsou součtem 3 čtverců.)
Důkaz (Jacobi, 1829). Nechť

$$r_4(n) = \#(x_1, x_2, x_3, x_4) \in \mathbf{Z}^4 : n = x_1^2 + x_2^2 + x_3^2 + x_4^2.$$

Chceme ukázat, že vždy $r_4(n) > 0$. Máme

$$\sum_{n \geq 0} r_4(n) x^n = \Big(\sum_{n=-\infty}^{\infty} x^{n^2} \Big)^4.$$

Po sérii transformací se čtvrtá mocnina vpravo nakonec přetransmutuje v

$$1 + 8 \sum_{n \geq 1} \frac{n x^n}{1 - x^n} - 8 \sum_{n \geq 1} \frac{4n x^{4n}}{1 - x^{4n}}.$$

Ovšem

$$\begin{aligned} \sum_{n \geq 1} \frac{n x^n}{1 - x^n} &= \sum_{n \geq 1} (n x^n + n x^{2n} + n x^{3n} + \cdots) \\ &= \sum_{n \geq 1} \Big(\sum_{d | n} d \Big) x^n. \end{aligned}$$

Tedy $r_4(0) = 1$ a pro $n \geq 1$,

$$r_4(n) = 8 \sum_{d|n,\, 4 \not| d} d.$$

Pro $n \in \mathbf{N}$ skutečně $r_4(n) = 8(1 + \cdots) \geq 8 > 0$. □

Např. $r_4(20) = 8(1+2+5+10) = 144$, což souhlasí s $20 = 4^2 + 2^2 + 0^2 + 0^2 = 3^2 + 3^2 + 1^2 + 1^2$.

Další identity? Třeba $r_8(n) = 16 \sum_{d|n} (-1)^{n+d} d^3$ (Jacobi, 1829) nebo (Milne, 2002)

$$\begin{aligned} r_{24}(n) &= (-1)^n \frac{16}{9}\Big(17\sigma_3^\dagger(n) + 8\sigma_5^\dagger(n) + 2\sigma_7^\dagger(n)\Big) \\ &\quad + (-1)^n \frac{512}{9} \sum_{m=1}^{n-1} \Big(\sigma_3^\dagger(m)\sigma_7^\dagger(n-m) \\ &\qquad - \sigma_5^\dagger(m)\sigma_5^\dagger(n-m)\Big), \end{aligned}$$

kde

$$\sigma_k^\dagger(n) = \sum_{d|n} (-1)^d d^k.$$

–Teorie čísel 3–

Rozklad $\mathbf{N}$ na AP. Množinu $\mathbf{N} = \{1, 2, 3, 4, \ldots\}$ můžeme rozložit jako

$$\begin{aligned} \mathbf{N} &= \{1, 3, 5, \ldots\} \cup \{2, 4, 6, \ldots\} \\ &= \{1, 3, 5, \ldots\} \cup \{2, 6, 10, \ldots\} \cup \{4, 8, 12, \ldots\} \end{aligned}$$

atd.

Lze $\mathbf{N}$ psát jako disjunktní sjednocení aritmetických posloupností $A_1, \ldots, A_l$ ($l > 1$) se vzájemně různými diferencemi $d_1 > d_2 > \ldots > d_l$?

Ne:

$$\sum_{k \geq 1} z^k = \sum_{k \in A_1} z^k + \sum_{k \in A_2} z^k + \cdots + \sum_{k \in A_l} z^k$$

$$\frac{z}{1-z} = \frac{z^{a_1}}{1-z^{d_1}} + \frac{z^{a_2}}{1-z^{d_2}} + \cdots + \frac{z^{a_l}}{1-z^{d_l}}$$

a vezmi $z \to \exp(2\pi i/d_1)$.
Bez disjunktnosti ano: každé $n \in \mathbf{N}$ splňuje alespoň jednu ze šesti kongruencí: $\equiv 0\ (2)$, $\equiv 0\ (3)$, $\equiv 1\ (4)$, $\equiv 3\ (8)$, $\equiv 7\ (12)$ a $\equiv 23\ (24)$ (Erdős, 1950).

–Teorie čísel 4–

Dirichletovy řady v multiplikativní TČ. Dirichletova řada posloupnosti $(a_1, a_2, \ldots)$ je

$$F(s) = \sum_{n\geq 1} \frac{a_n}{n^s} \quad \text{(obvykle } s \in \mathbf{C}\text{)}.$$

Pro $(1, 1, \ldots)$ dostáváme dzeta funkci

$$\zeta(s) = \prod_{n=1}^{\infty} \left(1 - 1/p^s\right)^{-1} = \sum_{n=1}^{\infty} \frac{1}{n^s} \quad (\mathrm{Re}(s) > 1).$$

Odtud

$$1/\zeta(s) = \prod_{n=1}^{\infty} \left(1 - 1/p^s\right) = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s},$$

kde $\mu(n)$, Möbiova funkce, se rovná $(-1)^r$ pro $n = p_1 p_2 \ldots p_r$ a jinak $\mu(n) = 0$.

Möbiova inverze. Nechť posloupnosti a_n a b_n pro $\forall n \in \mathbf{N}$ splňují $b_n = \sum_{d|n} a_d$. Tedy

$$\sum_{n\geq 1} \frac{b_n}{n^s} = \zeta(s) \sum_{n\geq 1} \frac{a_n}{n^s} \iff \zeta(s)^{-1} \sum_{n\geq 1} \frac{b_n}{n^s} = \sum_{n\geq 1} \frac{a_n}{n^s},$$

a ekvivalentně $a_n = \sum_{d|n} \mu(d) b_{n/d}$.

–Teorie čísel 5–

Důkaz nekonečnosti počtu prvočísel. Prvočísla: $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, \ldots$ Podle *Základní věty aritmetiky* má každé číslo $n \in \mathbf{N}$ jednoznačný rozklad $n = p_1^{a_1} p_2^{a_2} \ldots p_r^{a_r}$, kde $2 \leq p_1 < p_2 < \ldots$ jsou prvočísla a $a_i \in \mathbf{N}$.

Euclides (-3. st.): Existuje nekonečně mnoho prvočísel.

Důkaz (Euler, 18.st.) Sporem. Nejprve ale **Lemma.** Nechť dvě řady kladných reálných čísel $A = a_0 + a_1 + a_2 + \cdots$ a $B = b_0 + b_1 + b_2 + \cdots$ konvergují. Potom konverguje i jejich součin

$$a_0 b_0 + (a_0 b_1 + a_1 b_0) + (a_0 b_2 + a_1 b_1 + a_2 b_0) + \cdots$$

Totéž pro více řad.
Důkaz. Pro $c_n = \sum_{i=0}^{n} a_i b_{n-i}$ máme

$$\begin{aligned} & c_0 + c_1 + \cdots + c_n \\ & < (a_0 + a_1 + \cdots + a_n)(b_0 + b_1 + \cdots + b_n) \\ & < AB. \end{aligned}$$

□

–Teorie čísel 6–

Pokračujeme v Eulerově (?) důkazu nekonečnosti počtu prvočísel. Pro každé prvočíslo p geometrická řada

$$\frac{1}{1-1/p^s} = 1 + \frac{1}{p^s} + \frac{1}{(p^2)^s} + \frac{1}{(p^3)^s} + \cdots$$

konverguje pro $s > 0$. Pokud je prvočísel konečně mnoho, $p_1, p_2, \ldots, p_k$, součin těchto řad se podle ZVA rovná

$$\begin{aligned}
\prod_{i=1}^{k} \frac{1}{1-1/p_i^s} &= \prod_{i=1}^{k} \left(1 + \frac{1}{p_i^s} + \frac{1}{(p_i^2)^s} + \cdots\right) \\
&= \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \frac{1}{5^s} + \frac{1}{6^s} + \cdots \\
&= \sum_{n=1}^{\infty} \frac{1}{n^s} = \zeta(s)
\end{aligned}$$

a podle Lemmatu konverguje taky pro $s > 0$. Ale výsledná řada pro $0 < s \leq 1$ diverguje — spor. □

–Teorie čísel 7–

Uspořádané faktorizace. Nechť $m(n)$ je počet způsobů, jak přirozené číslo n vyjádřit jako součin několika činitelů větších než 1, přičemž záleží na poradí. Např. $m(1) = 0$, $m(2) = 1$, $m(12) = 8$ (12, 2×6, 6×2, 3×4, 4×3, $2 \times 2 \times 3$, $2 \times 3 \times 2$, $3 \times 2 \times 2$). Hodnoty $m(n)$ pro $n = 1, 2, \ldots, 60$:

$$1, 1, 1, 2, 1, 3, 1, 4, 2, 3, 1, 8, 1, 3, 3, 8, 1, 8, 1, 8, 3, 3, 1,$$
$$20, 2, 3, 4, 8, 1, 13, 1, 16, 3, 3, 3, 26, 1, 3, 3, 20, 1, 13, 1,$$
$$8, 8, 3, 1, \underline{48}, 2, 8, 3, 8, 1, 20, 3, 20, 3, 3, 1, 44, \ldots$$

Jak (ne)smí být velká hodnota $m(n)$? Pomůže nám Dirichletova řada. Pomocí

$$\zeta(s) - 1 = \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \frac{1}{5^s} + \frac{1}{6^s} + \cdots$$

máme

$$F(s) = \sum_{n=1}^{\infty} \frac{m(n)}{n^s} = \sum_{k=0}^{\infty} (\zeta(s) - 1)^k = \frac{1}{2 - \zeta(s)}.$$

$F(s)$ konverguje pro $s > \rho$, kde $\rho = 1.72864\ldots$ je řešení rovnice $\zeta(\rho) = 2$. Takže $m(n) > cn^{\rho+\varepsilon}$, $c > 0$ je konstanta, nemůže nastat pro nekonečně mnoho n. Tudíž $m(n) = o(n^{\rho+\varepsilon})$ pro $n \to \infty$.

Vlastně platí $m(n) \leq n^\rho$ pro každé $n \in \mathbf{N}$. Důkaz indukcí (Coppersmith & Lewenstein, 2005): $m(1) = 1 \leq 1^\rho$ a pro $n > 1$

$$\begin{aligned} m(n) &= \sum_{d|n,\, d>1} m(n/d) \leq \sum_{d|n,\, d>1} n^\rho/d^\rho \\ &< n^\rho \sum_{d>1} 1/d^\rho = n^\rho(\zeta(\rho) - 1) \\ &= n^\rho. \end{aligned}$$

Přesnější odhady $m(n)$**.** (Klazar & Luca, 200?) Pro každé $\varepsilon > 0$ pro všechna $n > n_0(\varepsilon)$ platí

$$m(n) < \frac{n^\rho}{\exp\left((\log n)^{1/\rho}/(\log\log n)^{1+\varepsilon}\right)}$$

a existuje nekonečně mnoho n takových, že

$$m(n) > \frac{n^\rho}{\exp\left(3(\log n)^{1/\rho}/(\log\log n)^{1/\rho}\right)}.$$

Dolní odhad dokazujeme pomocí Dirichletových řad. ($\rho = 1.72864\ldots$ a $1/\rho = 0.57848\ldots$)

–Teorie pravděpodobnosti 1–

gfp. X buď diskrétní náhodná veličina s hodnotami v $\mathbf{N}_0$. Její gfp, gf pravděpodobností, je

$$p(u) = p_X(u) = \sum_{n \geq 0} \mathbf{P}(X = n) \cdot u^n.$$

Zřejmě $p(1) = 1$.

Příklad. $X = X_n = \#$ nul v max. počátečním úseku nul ve slově $u \in \{0,1\}^n$ a $Y = Y_n =$ celkový $\#$ nul v u; každé slovo u má pravděpodobnost $1/2^n$. Patrně ($\langle V \rangle$ je char. funkce výroku V)

$$\begin{aligned} \mathbf{P}(X = k) &= \frac{\langle 0 \leq k < n \rangle}{2^{k+1}} + \frac{\langle k = n \rangle}{2^n} \\ \mathbf{P}(Y = k) &= \frac{1}{2^n}\binom{n}{k}. \end{aligned}$$

Takže

$$\begin{aligned} p_X(u) &= \sum_{i=0}^{n-1} \frac{u^i}{2^{i+1}} + \frac{u^n}{2^n} = \frac{(u/2)^n - 1}{u - 2} + \frac{u^n}{2^n} \\ p_Y(u) &= \sum_{i=0}^{n} \frac{1}{2^n}\binom{n}{k} u^n = \left(\frac{1+u}{2}\right)^n. \end{aligned}$$

–Teorie pravděpodobnosti 2–

Stř. hodnota a rozptyl z gfp. Patrně

$$\begin{aligned}\mathbf{E}(X) &= \sum_{n\geq 0} n\mathbf{P}(X=n) = p'_X(1)\\ \mathbf{V}(X) &= \mathbf{E}(X^2) - \mathbf{E}(X)^2\\ &= p''_X(1) + p'_X(1) - p'_X(1)^2.\end{aligned}$$

Limitní zákony. V příkladu s binárními slovy pro pevné k a $n \to \infty$ máme $\mathbf{P}(X_n = k) \to 1/2^{k+1}$ (diskrétní limitní zákon, geometrické rozdělení) a $\mathbf{P}(Y_n = k) \to 0$, ale — pro $\mu_n = n/2$, $\sigma_n = \sqrt{n}/2$ a pevné y —

$$\mathbf{P}(Y_n \leq \mu_n + y\sigma_n) \to \Phi(y) := \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{y} \mathrm{e}^{-t^2/2}\, dt$$

(spojitý limitní zákon, normální rozdělení).

"Centrální limitní zákony": gfp $p_n(u)$ pro $n \to \infty$ splňují jisté podmínky $\Rightarrow$ náhodné veličiny X_n mají pro $n \to \infty$ spojitý limitní zákon s normálním rozdělením.

–Teorie pravděpodobnosti 3–

Bender & Richmond, 1983; Hwang, 1994:

Věta. Nechť gfp $p_n(u)$ náh. veličin X_n v pevném okolí $u = 1$ pro $n \to \infty$ stejnoměrně splňují

$$p_n(u) = A(u)B(u)^{\beta_n}(1 + O(1/\kappa_n)),$$

kde posloupnosti $\beta_n, \kappa_n \to \infty$, $A(u)$ a $B(u)$ jsou analytické v $u = 1$, $A(1) = B(1) = 1$ a $B''(1) + B'(1) - B'(1)^2 \neq 0$. Pak

$$\mathbf{P}\Big(\frac{X_n - \mu_n}{\sigma_n} \leq y\Big) = \Phi(y) + O\Big(1/\kappa_n + 1/\sqrt{\beta_n}\Big),$$

kde

$$\begin{aligned} \mu_n &= A'(1) + \beta_n B'(1) + O(1/\kappa_n) \\ \sigma_n^2 &= A''(1) + A'(1) - A'(1)^2 \\ &\quad + \beta_n(B''(1) + B'(1) - B'(1)^2) + O(1/\kappa_n). \end{aligned}$$

Aplikace. Nechť $X_n = m$ v náhodné surjekci $[n] \to [m]$, $m \leq n$. Platí, že $X_n \to \Phi$ s $\mu_n \sim C_1 n$ a $\sigma_n \sim \sqrt{C_2 n}$, kde $C_1 = 1/2\log 2$ a $C_2 = (1 - \log 2)/(4\log 2)^2$.

–Informatika 1–

Frobeniův problém. $a_1, a_2, \ldots, a_d \in \mathbf{N}$ buďte vesměs nesoudělná čísla a

$$S = \{x_1 a_1 + x_2 a_2 + \cdots + x_d a_d : \ x_i \in \mathbf{N}_0\} \subset \mathbf{N}_0$$

buďte nezáporné lineární kombinace čísel a_i, tj. aditivní pologrupa generovaná $a_1, \ldots, a_d$. Dá se lehce dokázat, že S obsahuje všechna $n > n_0$.

Např. pro $a_1 = 4$ a $a_2 = 7$ máme $1 = 2 \cdot 4 - 1 \cdot 7$, takže $42 = 6 \cdot 7$, $43 = 42 + 1 = 2 \cdot 4 + 5 \cdot 7$, $44 = 43 + 1 = 4 \cdot 4 + 4 \cdot 7$, …, $48 = 12 \cdot 4 + 0 \cdot 7$, $49 = 7 \cdot 7$, $50 = 2 \cdot 4 + 6 \cdot 7$ atd. Ve skutečnosti ale $S \supset [18, +\infty)$ a $17 \notin S$, takže 17 je největší $N \notin S = S(4, 7)$.

- Frobenius: jaké je největší $N \notin S(a_1, \ldots, a_d)$?
- Teorie složitosti: pro neomezené d je to NP těžká úloha.
- Erdős a Graham, 1972: pro každé d může být N velké až $\gg t^2$, kde $t = \max(a_1, a_2, \ldots, a_d)$.

–Informatika 2–

• Kannan, 1992: existuje algoritmus, který pro pevné d nalezne N v počtu kroků polynomiálním ve velikosti vstupu $a_1, a_2, \ldots, a_d$ $(= d + \sum_{i=1}^{d} \log_2 a_i)$.

Existuje polynomiální algoritmus, který by pro pevné d a vstup $a_1, a_2, \ldots, a_d$ (+ případné další parametry jako $a, b \in \mathbf{N}$) nalezl počet $n \in \mathbf{N} \backslash S$? Počet $n \in [a, b] \backslash S$? Počet $n \equiv a \pmod b, n \notin S$?

• Takový algoritmus, založený na racionálních m. řadách ve více proměnných, našli v r. 2003 Barvinok a Woods.

Nástin jejich algoritmu. Pro $A \subset \mathbf{N}_0$, nechť $f(A; z) = \sum_{n \in A} z^n$. Je-li $p(z)/q(z)$ rac. funkce,

$$f(A; z) = p(z)/q(z)$$

chápeme jako rovnost pro $|z| < 1$ (a $z \neq$ póly).

–Informatika 3–

Pro daná (nesoudělná) $a_1, a_2, \ldots, a_d \in \mathbf{N}$ a $S = S(a_1, \ldots, a_d)$ máme triviálně

$$f(S; z) = \sum_{n \in S} z^n = p(z) + \frac{z^{N+1}}{1 - z},$$

kde $N = \max(\mathbf{N} \backslash S)$ a $p(z)$ je polynom stupně $< N$ (a s koeficienty 0 a 1). Tato reprezentace $f(S; z)$ je však obecně exponenciálně velká ve velikosti vstupu.

Věta (Barvinok a Woods, 2003). Nechť d je pevné. Pak existuje $s = s(d) \in \mathbf{N}$ a polynomiální algoritmus, který pro vstup $a_1, a_2, \ldots, a_d$ nalezne $f(S; z)$, $S = S(a_1, \ldots, a_2)$, ve tvaru

$$f(S; z) = \sum_{i \in I} \frac{\alpha_i z^{p_i}}{(1 - z^{b_{i1}})(1 - z^{b_{i2}}) \ldots (1 - z^{b_{is}})},$$

kde I je množina indexů, $\alpha_i \in \mathbf{Q}$, $p_i, b_{ij} \in \mathbf{Z}$ a $b_{ij} \neq 0$. (A rovnost chápeme jako výše.)

–Informatika 4–

Protože je tato reprezentace vygenerována polyn. algoritmem, $|I| = O(|\text{vstup}|^c)$; podobně jsou čísla α_i, p_i a b_{ij} jen polynomiálně velká. Hledaný počet čísel v $\mathbf{N}\backslash S$ se pak rovná

$$|\mathbf{N}\backslash S| = \lim_{z\to 1}\left(\frac{z}{1-z} - f(S;z)\right),$$

kde se z vhodně blíží k 1. Podobně se efektivně spočtou i $\#[a,b]\backslash S$ a $\#n \equiv a \pmod b, n \notin S$.

Věta je důsledkem dvou obecnějších výsledků.
• Barvinok, 1994: Pro pevné d ex. polyn. algoritmus, který pro vstupní racionální polyedr $P \subset \mathbf{R}^d$ nalezne pro gf $\sum_{a\in P\cap\mathbf{Z}^d} x_1^{a_1}\dots x_d^{a_d}$ efektivní reprezentaci racionální funkcí.
• Barvinok & Woods, 2003: Totéž pro gf množin tvaru $T(P\cap\mathbf{Z}^d)$, kde T je lineární transformace $T:\ \mathbf{R}^d\to\mathbf{R}^k$, $T(\mathbf{Z}^d)\subset\mathbf{Z}^k$, a polyedr P je *omezený*.

Ve Frobeniově pr. vezmeme $P = \{x \in \mathbf{R}^d_{\geq 0} : \|x\|_1 \leq N\}$ a $T : \mathbf{R}^d \to \mathbf{R}$, $T(x) = x_1a_1 + \dots + x_da_d$.

Děkuji!