Přednáška 6, 3. dubna 2014

Dokážeme charakterizaci racionálních generujících funkcí.

Věta (o racionálních fmř a GF). *Následující tři vlastnosti posloupnosti* $(a_n)_{n\geq 0} \subset \mathbb{C}$ *a její GF* $A(x) = \sum_{n\geq 0} a_n x^n$ *jsou ekvivalentní a vzájemně na sebe jednoduše převeditelné.*

1. *Daná posloupnost pro velké* n *splňuje* C*-rekurenci: existují takové konstanty* $\alpha_1, \ldots, \alpha_k \in \mathbb{C}$, *že pro každé* $n > n_0$ *(búno* $n_0 \geq k$*) je*

$$a_n = \sum_{i=1}^{k} \alpha_i a_{n-i} \ .$$

2. $A(x)$ *je racionální:*

$$A(x) = \frac{p(x)}{q(x)}$$

   pro nějaké polynomy $p, q \in \mathbb{C}[x]$, $q(0) \neq 0$.

3. *Prvky posloupnosti lze pro velké* n *vyjádřit mocninnou sumou: existuje* r *nenulových polynomů* $p_i \in \mathbb{C}[x]$ *a* r *různých nenulových čísel* $\gamma_i \in \mathbb{C}$, *že pro každé* $n > n_0$ *je*

$$a_n = \sum_{i=1}^{r} p_i(n) \gamma_i^n \ .$$

Důkaz. Implikace 1 ⇒ 2. Pro každé $n > n_0$ je

$$[x^n](1-\alpha_1 x - \cdots - \alpha_k x^k)A(x) = [x^n] \sum_{m\geq 0} (a_m - \alpha_1 a_{m-1} - \cdots - \alpha_k a_{m-k}) x^m = 0 \ ,$$

takže $(1 - \alpha_1 x - \cdots - \alpha_k x^k)A(x)$ je polynom $p(x)$ stupně nejvýše n_0 a

$$A(x) = \frac{p(x)}{1 - \alpha_1 x - \cdots - \alpha_k x^k} \ .$$

Implikace $2 \Rightarrow 3$. Búno má jmenovatel tvar $q(x) = 1 - \alpha_1 x - \cdots - \alpha_k x^k$. Rozložíme ho na kořenové činitele,

$$q(x) = \prod_{j=1}^{r} (1 - \gamma_j x)^{m_j} \ ,$$

kde $\gamma_j \in \mathbb{C}^*$ jsou různá čísla a násobnosti $m_j \in \mathbb{N}$ splňují $m_1 + m_2 + \cdots + m_r = k$, a použijeme rozklad na parciální zlomky z minulé přednášky:

$$A(x) = \frac{p(x)}{\prod_{j=1}^{r}(1 - \gamma_j x)^{m_j}} = a(x) + \sum_{j=1}^{r} \sum_{i=1}^{m_j} \frac{\beta_{j,i}}{(1 - \gamma_j x)^i}, \ a \in \mathbb{C}[x], \ \beta_{j,i} \in \mathbb{C} \ .$$

Vzpomeneme si opět na zobecněnou geometrickou řadu

$$\frac{1}{(1-x)^{l+1}} = \sum_{n \geq 0} \binom{n+l}{l} x^n =: \sum_{n \geq 0} b_l(n) x^n, \ l \in \mathbb{N}_0 \ ,$$

kde $b_l(x) = \frac{1}{l!}(x+1)(x+2)\dots(x+l)$ je polynom stupně l. Ta se z $\frac{1}{1-x} = 1 + x + x^2 + \dots$ snadno odvodí opakovaným formálním derivováním. Dosazením těchto rozvojů za parciální zlomky dostáváme pro $A(x)$ vyjádření

$$A(x) = a(x) + \sum_{n=0}^{\infty} \left(\sum_{j,i} \beta_{j,i} b_{i-1}(n) \gamma_j^n \right) x^n \ ,$$

kde indexy j, i probíhají výše uvedené obory. Koeficient u x^n v $A(x)$, což je a_n, má tedy pro $n > \deg a(x)$ vyjádření ve tvaru mocninné sumy.

Implikace $3 \Rightarrow 1$. Pro $n > n_0$ je tedy a_n dáno vztahem

$$a_n = \sum_{i=1}^{r} p_i(n) \gamma_i^n \ ,$$

z něhož potřebujeme odvodit C-rekurenci. Dostaneme ji pomocí užitečného lemmatu z lineární algebry:

Lemma. *Každá homogenní lineární soustava (s koeficienty v nějakém tělese), v níž je více neznámých než rovnic, má netriviální řešení, to jest řešení s alespoň jednou nenulovou složkou.*

Důkaz lemmatu ponecháváme jako cvičení. Hledáme $m \in \mathbb{N}$ a neznámá čísla $c_1, c_2, \ldots, c_m \in \mathbb{C}$, ne všechna nulová, aby pro každé $n > n_0$ platila rovnost

$$\sum_{j=1}^{m} c_j a_{n+j} = \sum_{i=1}^{r} \left(\sum_{j=1}^{m} c_j p_i(n+j)\gamma_i^j \right) \gamma_i^n = 0 \ .$$

To bude splněno, bude-li pro každé $i = 1, 2, \ldots, r$ polynom $\sum_{j=1}^{m} c_j p_i(x+j)\gamma_i^j$ identicky nulový (tj. všechny jeho koeficienty budou 0). Tento polynom má nejvýše $1 + \deg p_i$ koeficientů a každý z nich je lineární kombinace neznámých čísel $c_1, c_2, \ldots, c_m$. Podle lemmatu jakmile $m > \sum_{i=1}^{r}(1 + \deg p_i)$, existují hodnoty čísel $c_1, c_2, \ldots, c_m$, alespoň jedna nenulová, pro něž jsou všechny koeficienty ve všech r polynomech nulové a hořejší rovnost tak pro každé $n > n_0$ platí. Z ní už snadnou úpravou, jejímž rozepisováním nebudeme urážet čtenářovu či čtenářčinu inteligenci, dostaneme pro posloupnost $(a_n)_{n \geq 0}$ kýženou C-rekurenci. $\square$

Speciálním případem posloupností splňujících C-rekurence jsou tak zvané *kvazipolynomy*, které se v enumerativní kombinatorice často vyskytují. Funkce respektive posloupnost $f : \mathbb{N} \to \mathbb{C}$ je kvazipolynomem, když existuje modul $m \in \mathbb{N}$ a m polynomů $p_1, p_2, \ldots, p_m \in \mathbb{C}[x]$, že

$$f(n) = p_j(n) \ \text{ pro } \ n \equiv j \pmod{m} \ .$$

Ekvivalentně řečeno,

$$f(n) = a_k(n)n^k + a_{k-1}(n)n^{k-1} + \cdots + a_1(n)n + a_0(n) \ ,$$

kde koeficienty $a_j : \mathbb{N} \to \mathbb{C}$ jsou m-periodické funkce. Příklady kvazipolynomů: $a_n = (-1)^n$ nebo počet rozkladů čísla n na části 1 a 2,

$$p_{\{1,2\}}(n) = \lfloor n/2 \rfloor + 1 = \begin{cases} n/2 + 1 & \ldots \quad \text{pro } n \text{ sudé} \\ n/2 + 1/2 & \ldots \quad \text{pro } n \text{ liché} \ . \end{cases}$$

Dokážeme větu charakterizující kvazipolynomy.

Věta (vlastnosti kvazipolynomů). *Následující dvě vlastnosti posloupnosti $(a_n)_{n \geq 0} \subset \mathbb{C}$ a její GF $A(x) = \sum_{n \geq 0} a_n x^n$ jsou ekvivalentní a vzájemně na sebe jednoduše převeditelné.*

1. *Pro $n > n_0$ je a_n kvazipolynom.*

2. *Existují čísla $a, n \in \mathbb{N}$ a polynom $p \in \mathbb{C}[x]$, že*

$$A(x) = \frac{p(x)}{(1-x^a)^n} \ .$$

Důkaz. Implikace 1 $\Rightarrow$ 2. Nechť je a_n, $n > n_0$, kvazipolynom s periodou m. Búno $a_n = b_k(n)$ pro každé $n \in \mathbb{N}_0$ kongruentní j modulo m a jinak $a_n = 0$, kde $b_k(n) = \binom{n+k}{k}$; obecný kvazipolynom pro $n > n_0$ se dostane jako lineární kombinace takovýchto a přičtením polynomu $a(x)$. Protože pro $\alpha = \exp(2\pi i/m)$ je $\sum_{r=1}^{m} \alpha^{r(n-j)} = m$ pro n kongruentní j modulo m a jinak 0, máme

$$\begin{aligned} \sum_{n\geq 0} a_n x^n &= \frac{1}{m}\sum_{n\geq 0}\left(\sum_{r=1}^{m}\alpha^{r(n-j)}\right)b_k(n)x^n = \sum_{r=1}^{m}\frac{\alpha^{-rj}/m}{(1-\alpha^r x)^{k+1}} \\ &= \frac{p(x)}{(1-x^m)^{k+1}},\ p \in \mathbb{C}[x]\ , \end{aligned}$$

kde jsme použili zobecněnou geometrickou řadu a rozšíření zlomků vhodnými polynomy plynoucími z rovnosti $\prod_{r=1}^{m}(1-\alpha^r x) = 1-x^m$. Lineární kombinace takovýchto zlomků a přičtení $a(x)$ dává opět zlomek stejného typu.

Implikace 2 $\Rightarrow$ 1. To plyne hned z vyjádření a_n pro $n > n_0$ mocninnou sumou (část 3 předchozí věty). Všechny kořeny γ_i jsou teď a-té odmocniny z 1, takže je pro $n > \deg p(x)$ hodnota a_n dána „polynomem“, jehož koeficienty nejsou konstanty ale a-periodické funkce — je to kvazipolynom. □

Typické příklady kvazipolynomů, jak plyne z věty, jsou veličiny $p_A(n)$ počítající rozklady čísla n na části z konečné (multi)množiny A, které známe z minulé přednášky. Později uvidíme další obecnou situaci vedoucí na kvazipolynomy: počty mřížových bodů v nafouknutích nP, tj. $|\mathbb{Z}^k \cap nP|$, kde $P \subset \mathbb{R}^k$ je mnohostěn s vrcholy v $\mathbb{Q}^k$, jsou dány kvazipolynomem v n.

Teď ale popíšeme obecnou situaci vedoucí na racionální GF. Víme, že $\sum_{n\geq 0} x^n$ je racionální, neboť se rovná $\frac{1}{1-x}$. Nahradíme-li konstantní koeficient 1 mocninou a^n, dostaneme opět racionální fmř, protože $\sum_{n\geq 0} a^n x^n = \frac{1}{1-ax}$. Následuje zobecnění tohoto jednoduchého vzorce.

Věta (o přechodové matici). *Nechť $M = (m_{i,j}) \in \mathbb{C}^{k\times k}$ je čtvercová $k \times k$ matice. Pro pevné indexy $1 \leq i, j \leq k$ definujeme $a_n = (M^n)_{i,j}$ (jako položku* *na místě i, j v n-té mocnině matice M). Pak GF posloupnosti $(a_n)_{n\geq 0} \subset \mathbb{C}$ je racionální, přesněji*

$$\sum_{n=0}^{\infty} a_n x^n = (-1)^{i+j} \frac{\det(I - xM \mid j, i)}{\det(I - xM)} ,$$

kde I je jednotková $k \times k$ matice a matice v čitateli vznikne z matice ve jmenovateli vypuštěním j-tého řádku a i-tého sloupce (a $I - xM$ je $k \times k$ matice $(\delta_{i,j} - m_{i,j}x) \in \mathbb{C}[x]^{k\times k}$, kde $\delta_{i,j}$ je Kroneckerovo delta).

Příště to dokážeme a řekneme si kombinatorické aplikace.