0. Lineární rekurence

Martin Mareš, 2010-07-04

V tomto krátkém textu se budeme zabývat lineárními rekurencemi, tj. posloupnostmi definovanými rekurentní rovnicí typu

$$A_{n+k} = c_0 A_n + c_1 A_{n+1} + \ldots + c_{k-1} A_{n+k-1},$$

kde $c_0, \ldots, c_{k-1}$ jsou nějaké (obecně komplexní) konstanty, kterým říkáme *koeficienty* rekurence.

Aby byla posloupnost určena jednoznačně, ještě samozřejmě potřebujeme definovat hodnoty $A_0, \ldots, A_{k-1}$ neboli určit *počáteční podmínky* rekurence.

Přesněji řečeno, budeme studovat převážně homogenní lineární rekurence s konstantními koeficienty. Slovíčko *homogenní* znamená, že neobsahují konstantní členy (nehomogenní by byla třeba rekurence $A_{n+1} = 2A_n + 1$).

Typickým příkladem takové homogenní rekurence je *Fibonacciho posloupnost* definovaná vztahem

$$F_0 = 0, F_1 = 1, F_{n+2} = F_n + F_{n+1}.$$

Studoval ji už ve 12. století Leonardo z Pisy řečený Fibonacci, další generace matematiků objevily i explicitní vzorec pro n-tý člen:

$$F_n = \frac{1}{\sqrt{5}} \cdot \left(\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right).$$

Pokud už tento vzorec známe, není ho nijak těžké dokázat indukcí. Jak na něj ale přijít? Ukážeme, že ho lze snadno objevit pomocí metody vytvořujících funkcí. Navíc analogický postup půjde použít i na libovolnou jinou lineární rekurenci. Obvykle vyjde, že vzorec pro n-tý člen lze zapsat jako nějakou lineární kombinaci exponenciálních funkcí.

Nejprve si ale připomeneme několik tvrzení převážně z matematické analýzy, která budeme cestou potřebovat:

Tvrzení: *(zobecněná binomická věta)* Pro každé $r \in \mathbb{R}$ a $x \in (-1, 1)$ platí $(1+x)^r = \sum_{n=0}^{\infty} \binom{r}{n} x^n$, kde $\binom{r}{n}$ je definováno jako $r \cdot (r-1) \cdot (r-2) \cdot \ldots \cdot (r-n+1)/n!$.

Důkaz: Taylorovým rozvojem funkce $(1+x)^r$ v nule.

Pozorování: *(o zobecněných kombinačních číslech)* Pro $a, b \in \mathbb{N}$ platí:

$$\binom{-a}{b} = \frac{(-a)(-a-1)\ldots(-a-b+1)}{b!} = (-1)^b \cdot \frac{a(a+1)\ldots(a+b-1)}{b!} =$$
$$= (-1)^b \cdot \binom{a+b-1}{b} = (-1)^b \cdot \binom{a+b-1}{a-1}.$$

(rozepsáno podle definice, poslední rovnost platí díky symetrii kombinačních čísel).

Tvrzení: *(o kořenech polynomů)* Každý polynom s koeficienty z $\mathbb{C}$, který není konstantní, má v $\mathbb{C}$ alespoň jeden kořen.

Důkaz: Nesnadný (i když tvrzení vypadá jako snadný algebraický fakt [a proto se mu také někdy říká Základní věta algebry], jsou k jeho důkazu potřeba ne zrovna triviální prostředky komplexní analýzy).

Důsledek: Polynom stupně n nad $\mathbb{C}$ lze zapsat jako $C \cdot (x-\alpha_1)(x-\alpha_2)\dots(x-\alpha_n)$, kde $\alpha_1, \dots, \alpha_n$ jsou kořeny (ne nutně různé). Alternativně lze použít zápis $C \cdot (x-\alpha_1)^{k_1} \dots (x-\alpha_z)^{k_z}$, kde $\alpha_1, \dots, \alpha_z$ jsou navzájem různé kořeny a k_i jejich násobnosti.

Tvrzení: *(o rozkladu na parciální zlomky)* Buďte P a Q polynomy nad $\mathbb{C}$ takové, že stupeň P je menší než stupeň Q. Potom racionální lomenou funkci P/Q lze zapsat jako součet výrazů tvaru $C/(x-\alpha)^j$, kde C je konstanta a α kořen polynomu Q o násobnosti alespoň j.

Důkaz: Indukcí.

Tvrzení: *(o zrcadlových polynomech)* Nechť $P(x) = p_0x^0 + \ldots + p_nx^n$ je nějaký polynom a $\alpha \neq 0$ jeho kořen. Potom je číslo $1/\alpha$ kořenem „zrcadlového“ polynomu $P^*(x) = p_0x^n + p_1x^{n-1} + \ldots + p_nx^0$.

Důkaz: Nechť $P(\alpha) = p_0\alpha^0 + \ldots + p_n\alpha^n = 0$. Jelikož α je nenulové, můžeme rovnost vydělit číslem α^n a získat: $p_0\alpha^{-n} + p_1\alpha^{1-n} + \ldots + p_n\alpha^0 = 0$. Levá strana ovšem není nic jiného než $P^*(1/\alpha)$.

Vytvořující funkce

Ukažme nyní, jak sestrojit vytvořující funkci k zadané lineární rekurenci. Pro každé n má platit

$$A_{n+k} = c_0A_n + c_1A_{n+1} + \ldots + c_{k-1}A_{n+k-1}.$$

To můžeme pro $n \geq k$ přepsat na

$$A_n = c_0A_{n-k} + c_1A_{n-k+1} + \ldots + c_{k-1}A_{n-1}. \qquad (*)$$

Označíme-li G hledanou vytvořující funkci, platí $A_n = [x^n]G(x)$ (kde operátor $[x^n]$ značí koeficient u x^n v mocninné řadě pro danou funkci) a $A_{n-i} = [x^n](G(x) \cdot x^i)$ – vzpomeňte si, že násobení vytvořující funkce mocninou x odpovídá posunutí generované posloupnosti doprava o příslušný počet míst.

Vztah $(*)$ tedy můžeme přepsat na

$$\begin{aligned}[x^n]G(x) &= c_0[x^n](G(x) \cdot x^k) + c_1[x^n](G(x) \cdot x^{k-1}) + \ldots + c_{k-1}[x^n](G(x) \cdot x^1) = \\ &= [x^n]\left(G(x) \cdot (c_0x^k + c_1x^{k-1} + \ldots + c_{k-1}x^1)\right).\end{aligned}$$

Kdyby se koeficienty u x^n rovnaly pro všechna n, plynula by z toho i rovnost vytvořujících funkcí. Pokud se nerovnají pro $n < k$, znamená to, že se funkce na levé a pravé straně mohou lišit o nějaký polynom $P(x)$ stupně menšího než k. Tedy:

$$G(x) = G(x) \cdot (c_0x^k + \ldots + c_{k-1}x^1) - P(x).$$

Z této rovnice už můžeme vyjádřit hledanou funkci G:

$$G(x) = \frac{P(x)}{c_0 x^k + c_1 x^{k-1} + \ldots + c_{k-1} x^1 - 1}.$$

Nalezněme nyní kořeny $\alpha_1, \ldots, \alpha_n$ polynomu $Q(x) = c_0 x^k + \ldots + c_{k-1} x^1 - 1$. Předpokládejme na chvíli, že jsou všechny navzájem různé. Pak má naše vytvořující funkce příjemně jednoduchý rozklad na parciální zlomky:

$$G(x) = \frac{C_1}{x - \alpha_1} + \ldots + \frac{C_k}{x - \alpha_k}.$$

Stačí tedy zjistit, jakou posloupnost generuje funkce $C_i/(x - \alpha_i)$. Pokud čitatele i jmenovatele vydělíme $-\alpha_i$, dostaneme ekvivalentní tvar

$$\frac{-C_i/\alpha_i}{1 - \frac{1}{\alpha_i} x} = \frac{-C_i \lambda_i}{1 - \lambda_i x}, \qquad \text{kde } \lambda_i = 1/\alpha_i.$$

Použitím základních operací s vytvořujícími funkcemi (nebo ze zobecněné binomické věty) zjistíme, že n-tý člen generované posloupnosti musí být $D_i \lambda_i^n$ pro nějakou konstantu D_i.

Nyní sečteme příspěvky od všech členů funkce $G(x)$ a dozvíme se:

$$A_n = [x^n] G(x) = D_1 \lambda_i^n + \ldots + D_k \lambda_k^n.$$

Jinými slovy, n-tý člen zkoumané posloupnosti je lineární kombinací exponenciál λ_i^n, kde λ_i jsou převrácené hodnoty kořenů jakéhosi polynomu odvozeného z koeficientů rekurence. Konstanty D_i závisí na počátečních podmínkách rekurence. (Bylo by možné pro ně odvodit explicitní vztahy, ale vyjdou poměrně složité, takže bývá praktičtější vyřešit soustavu k lineárních rovnic typu $A_j = K_1 \lambda_1^j + \ldots K_k \lambda_k^j$, kde K_i jsou neznámé a A_j a λ_i už známé konstanty.)

Ještě si všimneme, že podle tvrzení o zrcadlových polynomech můžeme čísla λ_i nalézt přímočařeji jako kořeny polynomu $Q^*(x) = x^k - c_{k-1} x^{k-1} - c_{k-2} x^{k-2} - \ldots - c_0 x^0$. Tento polynom se při studiu rekurencí často používá a říká se mu *charakteristický polynom* rekurence.

Násobné kořeny

Komplikovanější situace nastane, když charakteristický polynom (a tedy i původní polynom Q) bude mít násobné kořeny. Pak rozklad na parciální zlomky bude produkovat i členy typu $C_i/(x - \alpha_i)^j$. Ty opět vydělíme $-\alpha_i$, všechny konstanty „shrábneme“ do D_i a s tím, co vznikne, si poradíme pomocí zobecněné binomické věty:

$$[x^n] \frac{C_i}{(x - \alpha_i)^j} = [x^n] \frac{(-\lambda_i)^j C_i}{(1 - \lambda_i x)^j} = D_i \cdot [x^n](1 - \lambda_i x)^{-j} = D_i \cdot \binom{-j}{n} \cdot (-\lambda_i)^n.$$

Ještě si vzpomeneme, co jsme pozorovali o kombinačních číslech se záporným celým číslem nahoře. Díky tomu můžeme celý výraz přepsat na:

$$D_i \cdot (-1)^n \cdot \binom{n+j-1}{j-1} \cdot (-\lambda_i)^n = D_i \cdot \binom{n+j-1}{j-1} \cdot \lambda_i^n.$$

(Všimněte si, že uvedené kombinační číslo je vlastně polynom stupně $j-1$ v proměnné n a že pro $j=1$ tento vztah splývá s tím, který jsme nalezli pro případ bez násobných kořenů.)

Tak jsme odvodili, že pro všechny lineární rekurence platí následující věta:

Věta: *(kuchařka na řešení lineárních rekurencí)* Buď $A_{n+k} = c_0 A_n + \ldots + c_{k-1} A_{n+k-1}$ lineární rekurence s počátečními podmínkami $A_0, \ldots, A_{k-1}$. Dále buď $R(x) = x^k - c_{k-1}x^{k-1} - \ldots - c_0 x^0$ její charakteristický polynom a $\lambda_1, \ldots, \lambda_z$ navzájem různé kořeny tohoto polynomu s násobnostmi po řadě $k_1, \ldots, k_z$. Potom existují konstanty $C_{ij} \in \mathbb{C}$ takové, že

$$A_n = \sum_{i=1}^{z} \sum_{j=0}^{k_i-1} \left(C_{ij} \cdot \binom{n+j}{j} \cdot \lambda_i^n \right).$$

Pokud polynom R nemá násobné kořeny, vztah lze zapsat jednodušeji:

$$A_n = \sum_{i=1}^{n} C_i \lambda_i^n.$$

Poznámka: Jelikož kombinační číslo $\binom{n+j}{j}$ je polynomem stupně j v proměnné n, mohli bychom vzorec pro n-tý člen formulovat i takto (D_{ij} jsou nějaké komplexní konstanty):

$$A_n = \sum_{i=1}^{z} \sum_{j=0}^{k_i-1} \left(D_{ij} \cdot n^j \cdot \lambda_i^n \right).$$

A_n lze tedy vždy vyjádřit jako lineární kombinaci nějakých exponenciál a funkcí typu polynom krát exponenciála. Všimněte si, že to jediné, co závisí na počátečních podmínkách rekurence, jsou koeficienty této lineární kombinace. Funkce, které kombinujeme, jsou dány pouze rekurentní rovnicí samou.

Příklady

Fibonacciho čísla: Z rekurence $A_{n+2} = A_n + A_{n+1}$ získáme charakteristický polynom $x^2 - x - 1$, jehož kořeny jsou $\lambda_{1,2} = (1 \pm \sqrt{5})/2$. Z počátečních podmínek obdržíme rovnice pro konstanty:

$$A_0 = C_1\lambda_1^0 + C_2\lambda_2^0 = 0,$$
$$A_1 = C_1\lambda_1^1 + C_2\lambda_2^1 = 1,$$

Z první rovnice zjistíme, že $C_2 = -C_1$. Dosazením do druhé dostaneme:

$$C_1 \cdot \left(\frac{1+\sqrt{5}}{2} - \frac{1-\sqrt{5}}{2} \right) = 1,$$

tedy $C_1 = 1/\sqrt{5}$, $C_2 = -1/\sqrt{5}$. To je přesně klasická formule, kterou jsme už potkali v úvodu tohoto spisku.

Podívejme se ještě na číselné hodnoty konstant: $\lambda_1 \approx 1.618034$ je známý *zlatý řez*, $\lambda_2 \approx -0.618034$. Z toho vidíme, že λ_2^n velmi rychle konverguje k nule. Číslo F_n se tedy asymptoticky chová jako funkce $\lambda_1^n/\sqrt{5}$, čili roste exponenciálně. (S tímto odhadem se překvapivě často potkáváme v analýze složitosti datových struktur, například AVL stromů nebo Fibonacciho hald.)

Rekurence řádu 3: Uvažujme rekurenci $B_{n+3} = 4B_n - 8B_{n+1} + 5B_{n+2}$ s počátečními podmínkami $B_0 = 0$, $B_1 = 1$, $B_2 = 2$. Jejím charakteristickým polynomem je $x^3 - 5x^2 + 8x^1 - 4x^0 = (x-1)(x-2)^2$. Potkáváme tedy jednoduchý kořen $\lambda_1 = 1$ a dvojnásobný kořen $\lambda_2 = 2$. Naše věta nám říká, že řešení máme hledat ve tvaru

$$B_n = a \cdot 1^n + b \cdot 2^n + c \cdot n \cdot 2^n.$$

Z počátečních podmínek vyplyne soustava rovnic pro konstanty a, b, c:

$$\begin{aligned} B_0 &= a + b = 0, \\ B_1 &= a + 2b + 2c = 1, \\ B_2 &= a + 4b + 8c = 2. \end{aligned}$$

Pomocí první rovnice přepíšeme zbylé dvě na:

$$\begin{aligned} b + 2c &= 1, \\ 3b + 8c &= 2. \end{aligned}$$

Nyní od poslední rovnice odečteme trojnásobek předposlední:

$$2c = -1,$$

takže $c = -1/2$, $b = 2$, $a = -2$ a vzorec pro n-tý člen zní:

$$B_n = 2 \cdot 2^n - \frac{n}{2} \cdot 2^n - 2.$$

Malá odbočka k nehomogenním rekurencím

Nehomogenními rekurencemi jsme se sice neplánovali zabývat, ale přesto k nim na chvilku odbočme. Ukážeme totiž, že se naše kuchařková věta dá po snadné úpravě využít i na ně. Uvažujme nějakou nehomogenní lineární rekurenci ve tvaru

$$A_{n+k} = c_0 A_n + c_1 A_{n+1} + \ldots + c_{k-1} A_{n+k-1} + c. \qquad (\sharp)$$

Odečteme-li od vztahu pro A_{n+k} vztah pro A_{n+k+1}, tedy

$$A_{n+k+1} = c_0 A_{n+1} + c_1 A_{n+2} + \ldots + c_{k-1} A_{n+k} + c,$$

konstanta c anihiluje a získáme:

$$\begin{aligned} A_{n+k+1} - A_{n+k} = &- c_0 A_n \\ &+ (c_0 - c_1)A_{n+1} + (c_1 - c_2)A_{n+2} + \ldots + (c_{k-2} - c_{k-1})A_{n+k-1} \\ &+ c_{k-1}A_{n+k}. \end{aligned}$$

Pokud převedeme A_{n+k} na pravou stranu, vyjde

$$\begin{aligned} A_{n+k+1} = &- c_0 A_n \\ &+ (c_0 - c_1)A_{n+1} + (c_1 - c_2)A_{n+2} + \ldots + (c_{k-2} - c_{k-1})A_{n+k-1} \\ &+ (c_{k-1} + 1)A_{n+k}. \end{aligned}$$

Ejhle, to je homogenní rekurence, kterou už umíme vyřešit (pravda, o 1 vyššího řádu, ale to nevadí). Podívejme se na její charakteristický polynom:

$$R(x) = x^{k+1} - (c_{k-1} + 1)x^k - (c_{k-2} - c_{k-1})x^{k-1} - \ldots - (c_0 - c_1)x^1 + c_0 x^0.$$

Evidentně je jedním z jeho kořenů $x = 1$, takže můžeme vytkout výraz $(x - 1)$:

$$R(x) = (x - 1)(x^k - c_{k-1}x^{k-1} - c_{k-2}x^{k-2} - \ldots - c_0 x_0).$$

Přitom závorka $(x^k - \ldots - c_0 x_0)$ je přesně charakteristický polynom původní rekurence (♯), jaký bychom získali, kdybychom vynechali nehomogenní člen c.

Zjistili jsme tedy, že nehomogenní rekurence můžeme řešit stejně jako jejich homogenní sourozence, pouze mezi kořeny charakteristického polynomu přidáme jedničku. Pokud ani s touto jedničkou nemá polynom násobné kořeny, bude tedy n-tý člen lineární kombinací exponenciál plus nějaká konstanta. Nezapomeňme ovšem, že jako počáteční podmínky musíme použít prvních $k + 1$ členů namísto prvních k, protože popsaná úprava platí až od $n = k + 1$. (Rovněž se až v k-tém členu poprvé projeví existence nenulového c.)

Na scénu přichází lineární algebra

Na naši obecnou větu o řešení rekurencí se můžeme dívat i lineárně algebraicky. Ukažme si ještě alternativní důkaz (pouze pro případ jednoduchých kořenů) založený na přímočaré úvaze o vektorovém prostoru a jeho bázi.

Uvažujme množinu V všech posloupností $a_0, a_1, \ldots$ splňujících zkoumanou rekurenci (každá posloupnost má jiné počáteční podmínky). Všimněme si, že tato množina tvoří vektorový prostor s posloupností samých nul coby nulovým vektorem, sčítáním po složkách (součet dvou posloupností splňujících rekurenci ji také splňuje) a násobením skalárem po složkách (rovněž nemůže platnost rekurentního vztahu porušit).

Jakou má tento vektorový prostor dimenzi? Každá posloupnost je jednoznačně určena svými prvními k členy, takže dimenze musí být stejná jako dimenze k-složkových vektorů komplexních čísel, tedy rovna k.

Jak vypadá báze prostoru? Ukážeme, že lze nalézt bázi z exponenciál. Uvažujme posloupnost $\alpha^0, \alpha^1, \alpha^2, \ldots$, kde α je nějaké nenulové komplexní číslo. Rekurenci tato posloupnost splňuje (a tedy patří do vektorového prostoru) právě tehdy, je-li

$$\alpha^{n+k} = c_0\alpha^n + c_1\alpha^{n+1} + \ldots + c_{k-1}\alpha^{n+k-1}.$$

Po vydělení α^n získáme podmínku

$$\alpha^k = c_0\alpha^0 + \ldots + c_{k-1}\alpha^{k-1},$$

což ovšem neříká nic jiného, než že α je kořenem charakteristického polynomu R.

Pokud jsou všechny kořeny tohoto polynomu navzájem různé, získáváme k různých exponenciálních posloupností ležících ve V. Tvoří bázi? Správný počet jich je, jak ale dokázat, že jsou lineárně nezávislé? Stačilo by ověřit, že determinant

$$D = \begin{vmatrix} \alpha_1^0 & \alpha_1^1 & \alpha_1^2 & \ldots & \alpha_1^{k-1} \\ \alpha_2^0 & \alpha_2^1 & \alpha_2^2 & \ldots & \alpha_2^{k-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \alpha_k^0 & \alpha_k^1 & \alpha_k^2 & \ldots & \alpha_k^{k-1} \end{vmatrix}$$

není nulový (jsou-li posloupnosti zkrácené na prvních k členů nezávislé, tím spíš jsou nezávislé celé). Čtenáři zběhlí v tajích lineární algebry pravděpodobně poznali známý Vandermondův determinant, o němž se ví, že je roven $\prod_{1\le i<j\le n}(\alpha_j - \alpha_i)$. Pokud jsou všechna α_i navzájem různá, nemůže tedy být nulový.

Tento vzorec pro Vandermondův determinant můžeme snadno ověřit indukcí. Pro $k = 1$ je determinant evidentně roven 1, což souhlasí se součinem přes prázdnou množinu dvojic. Pokud $k > 1$, odečteme od každého sloupce determinantu α_1-násobek předchozího sloupce (nejdříve předposlední od posledního, pak předpředposlední od předposledního atd., až nakonec první od druhého). Získáme:

$$D = \begin{vmatrix} 1 & \alpha_1 - \alpha_1 & \alpha_1^2 - \alpha_1^2 & \alpha_1^3 - \alpha_1^3 & \ldots & \alpha_1^{k-1} - \alpha_1^{k-1} \\ 1 & \alpha_2 - \alpha_1 & \alpha_2^2 - \alpha_1\alpha_2^1 & \alpha_2^3 - \alpha_1\alpha_2^2 & \ldots & \alpha_2^{k-1} - \alpha_1\alpha_2^{k-2} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_k - \alpha_1 & \alpha_k^2 - \alpha_1\alpha_k^1 & \alpha_k^3 - \alpha_1\alpha_k^2 & \ldots & \alpha_k^{k-1} - \alpha_1\alpha_k^{k-2} \end{vmatrix}.$$

První řádek tedy obsahuje jedničku a samé nuly, takže ho podle věty o rozvoji determinantu podle řádku můžeme smazat. Z druhého řádku pak můžeme vytknout $(\alpha_2 - \alpha_1)$, takže zbude $\alpha_2^0, \alpha_2^1, \ldots, \alpha_2^{k-1}$ (vzpomeňte si, že násobení řádku konstantou způsobí vynásobení celého determinantu toutéž konstantou, takže výraz $\alpha_2 - \alpha_1$ můžeme přesnout ven z determinantu). Podobně z j-tého řádku pro $3 \le j \le k$ vytkneme $(\alpha_j - \alpha_1)$, čímž dostaneme:

$$D = (\alpha_2 - \alpha_1)(\alpha_3 - \alpha_1)\ldots(\alpha_k - \alpha_1) \cdot \begin{vmatrix} \alpha_2^0 & \alpha_2^1 & \ldots & \alpha_2^{k-1} \\ \alpha_3^0 & \alpha_3^1 & \ldots & \alpha_3^{k-1} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_k^0 & \alpha_k^1 & \ldots & \alpha_k^{k-1} \end{vmatrix}$$

a zbylý determinant není nic jiného než Vandermondův determinant řádu $k - 1$.

Od vzorce k algoritmu

Obecný vzorec pro n-tý člen rekurentně zadané posloupnosti vypadá impozantně a poslouží k odvození mnoha zajímavých vlastností posloupnosti (zejména asymptotického chování). Pro praktický výpočet na počítači je ovšem značně nevhodný, protože v něm typicky vystupují iracionální čísla, která se v algoritmech dají reprezentovat jenom přibližně. Navíc v obecném případě ani nemusíme umět kořeny charakteristického polynomu najít.

Ukážeme si jiný přístup, založený na násobení matic, který nám dá efektivní algoritmus.

Všimněme si následujícího maticového součinu (c_i stále značí koeficienty zkoumané rekurence, matici na levé straně budeme říkat $\mathbf{\Omega}$):

$$\begin{pmatrix} 0 & 1 & 0 & 0 & \dots & 0 \\ 0 & 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 1 \\ c_0 & c_1 & c_2 & c_3 & \dots & c_{k-1} \end{pmatrix} \cdot \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_{k-2} \\ a_{k-1} \end{pmatrix} = \begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ \vdots \\ a_{k-1} \\ \sum_i c_i a_i \end{pmatrix}.$$

Pokud tedy maticí $\mathbf{\Omega}$ vynásobíme vektor $(A_n, A_{n+1}, \dots, A_{n+k-1})$, získáme vektor $(A_{n+1}, A_{n+2}, \dots, A_{n+k})$ – postupným násobením maticí $\mathbf{\Omega}$ můžeme „posouvat okénko velikosti k“ po zkoumané posloupnosti. Označíme-li $\mathbf{a}$ vektor počátečních podmínek $(A_0, \dots, A_{k-1})$, součin $\mathbf{\Omega}^n \mathbf{a} = (A_n, \dots, A_{n+k-1})$ nám prozradí, jak vypadá n-tý člen posloupnosti.

Mocniny matice (nebo i čehokoliv jiného) lze rychle počítat následujícím jednoduchým trikem:

$$\mathbf{\Omega}^{2i} = (\mathbf{\Omega}^i)^2,$$
$$\mathbf{\Omega}^{2i+1} = (\mathbf{\Omega}^i)^2 \cdot \mathbf{\Omega}.$$

Pomocí dvou maticových násobení jsme převedli výpočet $\mathbf{\Omega}^n$ na výpočet $\mathbf{\Omega}^{\lfloor n/2 \rfloor}$, atd. až k $\mathbf{\Omega}^1 = \mathbf{\Omega}$. Celkem nám tedy postačí $\mathcal{O}(\log n)$ maticových násobení, z nichž každé trvá $\mathcal{O}(k^3)$ kroků. Kýžený n-tý člen tudíž dovedeme spočítat v čase $\mathcal{O}(k^3 \log n)$, navíc pokud uvažujeme jednu konkrétní rekurenci, je k konstantní a náš algoritmus dosahuje logaritmické časové složitosti.

Ještě jeden algoritmus

Pro kvadratické rekurence nemusíme zavrhovat ani předchozí postup s kořeny charakteristických polynomů. Na příkladu Fibonacciho čísel si ukážeme, že i ten může vést k efektivnímu algoritmu. Jen se musíme hrozbě počítání s iracionálními čísly elegantně vyhnout. Použijeme k tomu takřka cimrmanovský krok stranou: místo tělesa reálných čísel budeme počítat v tzv. *kvadratickém rozšíření* racionálních čísel.

Podobně jako se zavádějí komplexní čísla, budeme uvažovat výrazy tvaru $a + b\sqrt{5}$, kde a a b jsou racionální. Budeme jim říkat kvadratická čísla. Všimněme si, že

dva výrazy tohoto typu můžeme sečíst nebo odečíst a opět vyjde kvadratické číslo. Pěkně se chová i násobení:

$$(a+b\sqrt{5})(c+d\sqrt{5}) = (ac+5bd)+(ad+bc)\sqrt{5}.$$

Dělení provedeme podobně jako u komplexních čísel vhodným rozšířením zlomku:

$$\frac{a+b\sqrt{5}}{c+d\sqrt{5}} = \frac{(a+b\sqrt{5})(c-d\sqrt{5})}{(c+d\sqrt{5})(c-d\sqrt{5})} = \frac{(ac-5bd)+(bc-ad)\sqrt{5}}{c^2-5d^2}.$$

Jelikož $\sqrt{5}$ není racionální, nabývá výraz c^2-5d^2 nuly pouze v případě $c=d=0$. Jinak je to nenulové racionální číslo, kterým můžeme čitatele vydělit po složkách.

Dokázali jsme tedy, že součet, rozdíl, součin i podíl kvadratických čísel je zase kvadratické číslo. Sčítání i násobení jsou pochopitelně asociativní, komutativní i distributivní, takže kvadratická čísla tvoří těleso.

Kořeny charakteristického polynomu $\alpha_{1,2} = (1\pm\sqrt{5})/2$ přitom patří mezi naše kvadratická čísla a konstanta $1/\sqrt{5}$ jakbysmet, takže celý výpočet výrazu $(\alpha_1^n - \alpha_2^n)/\sqrt{5}$ můžeme provádět v tělese kvadratických čísel, a tedy naprogramovat pomocí operací s racionálními čísly. Umocňovat můžeme na $\mathcal{O}(\log n)$ operací stejným trikem, jakým jsme v předchozím algoritmu mocnili matice.

Navíc si můžeme zjednodušit práci tím, že vzorec přepíšeme na $((1+\sqrt{5})^n - (1-\sqrt{5})^n)/(2^n\sqrt{5})$. Tím jsme zařídili, že všechny mezivýsledky až do konečného dělení mocninou dvojky jsou kvadratická čísla tvaru $a+b\sqrt{5}$, kde a a b jsou celá čísla. Dostaneme tak další elegantní celočíselný algoritmus pracující v čase $\mathcal{O}(\log n)$.

Diagonální trik

Popis rekurencí pomocí matice $\mathbf{\Omega}$, který jsme použili v našem prvním algoritmu, se dá navíc použít i k dalšímu důkazu naší hlavní věty o rekurencích. (Zde si dovolíme předpokládat, že se čtenář již potkal s vlastními čísly matic.)

Zkoumejme případ, kdy má matice $\mathbf{\Omega}$ k různých nenulových vlastních čísel $\beta_1,\ldots,\beta_k$. Tehdy vlastní vektory příslušné k těmto vlastním číslům tvoří bázi vektorového prostoru $\mathbb{C}^k$ a když si matici $\mathbf{\Omega}$ vyjádříme vzhledem k této bázi, dostaneme diagonální matici

$$\mathbf{\Lambda} = \begin{pmatrix} \beta_1 & 0 & 0 & \ldots & 0 \\ 0 & \beta_2 & 0 & \ldots & 0 \\ 0 & 0 & \beta_3 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & \beta_k \end{pmatrix}.$$

Matici $\mathbf{\Omega}$ tedy můžeme vyjádřit ve tvaru $\mathbf{P\Lambda P}^{-1}$, kde $\mathbf{P}$ je matice přechodu mezi bázemi. Tento tvar matice je šikovný pro umocňování, neboť $\mathbf{\Lambda}^n$ je matice, která má na diagonále $\beta_1^n,\ldots,\beta_k^n$ a všude jinde nuly a

$$\mathbf{\Omega}^n = (\mathbf{P\Lambda P}^{-1})^n = (\mathbf{P\Lambda P}^{-1})(\mathbf{P\Lambda P}^{-1})\ldots(\mathbf{P\Lambda P}^{-1}) = \mathbf{P\Lambda}^n\mathbf{P}^{-1}.$$

(Mimochodem, to by nám pro diagonalizovatelnou matici $\mathbf{\Omega}$ dalo algoritmus pro výpočet $\mathbf{\Omega}^n$ v čase $\mathcal{O}(k^2 + k \log n)$, ovšem za předpokladu, že už máme předem spočítanou matici $\mathbf{P}$. Zkuste si ho vymyslet.)

Vraťme se k výpočtu n-tého členu pomocí násobení matic. Víme, že ho umíme získat jako první složku vektoru $\mathbf{b} = \mathbf{\Omega}^n \mathbf{a}$, kde $\mathbf{a}$ je vektor počátečních podmínek. Platí tedy:

$$\mathbf{b} = \mathbf{P}\mathbf{\Lambda}^n\mathbf{P}^{-1}\mathbf{a}.$$

Nyní si všimněme, že $\mathbf{P}^{-1}\mathbf{a}$ je nějaký vektor; označme si ho třeba $\mathbf{d}$. Součin tohoto vektoru s diagonální maticí $\mathbf{\Lambda}^n$ pouze vynásobí i-tou složku vektoru i-tým prvkem na diagonále, tedy číslem β_i^n. Vektor $\mathbf{\Lambda}^n\mathbf{P}^{-1}\mathbf{a}$ tedy bude mít složky $\beta_1^n d_1$, $\beta_2^n d_2$, …, $\beta_k^n d_k$. Násobením tohoto vektoru maticí $\mathbf{P}$ pak vznikne hledaný vektor $\mathbf{b}$, jehož složky budou lineární kombinace čísel $\beta_i^n d_i$.

Dokázali jsme tedy, že n-tý člen posloupnosti je možné zapsat jako lineární kombinaci exponenciál β_i^n, přičemž jednotlivá β_i jsou vlastními čísly matice $\mathbf{\Omega}$ a koeficienty této lineární kombinace lze odvodit z matice $\mathbf{P}$ přechodu k bázi z vlastních vektorů a z vektoru $\mathbf{b}$ počátečních podmínek.

To už je skoro tvrzení naší věty, zbývá jen ukázat, že vlastní čísla matice $\mathbf{\Omega}$ jsou právě kořeny charakteristického polynomu rekurence. Počítejme vlastní čísla standardním způsobem, totiž jako kořeny determinantu[⟨1⟩]

$$\det(\mathbf{\Omega} - \beta\mathbf{E}) = \begin{vmatrix} -\beta & 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & -\beta & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & -\beta & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & -\beta & 1 \\ c_0 & c_1 & c_2 & c_3 & \dots & c_{k-2} & c_{k-1} - \beta \end{vmatrix}.$$

Rozvineme-li tento determinant podle prvního řádku, dostaneme:

$$-\beta \cdot \begin{vmatrix} -\beta & 1 & 0 & \dots & 0 & 0 \\ 0 & -\beta & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & -\beta & 1 \\ c_1 & c_2 & c_3 & \dots & c_{k-2} & c_{k-1} - \beta \end{vmatrix} - \begin{vmatrix} 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & -\beta & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & -\beta & 1 \\ c_0 & c_2 & c_3 & \dots & c_{k-2} & c_{k-1} - \beta \end{vmatrix}.$$

Pravý z těchto dvou determinantů můžeme následně rozvinout podle prvního sloupce a převést na $(-1)^k$ krát determinant trojúhelníkové matice s jedničkami na diagonále, který je nutně jedničkový. Levý determinant je podobného druhu jako ten, se kterým jsme začali, jen s vynechaným prvním řádkem a sloupcem. Nabízí se tedy pokračovat rekurentně.

[⟨1⟩] Jelikož prvky determinantu obsahují mimo čísel ještě proměnnou β, je jeho hodnota nějaký polynom stupně k v proměnné β.

Pokud označíme R_i determinant matice $\mathbf{\Omega} - \beta\mathbf{E}$ omezené na posledních i řádků a sloupců, bude podle předchozí úvahy platit

$$R_i = -\beta R_{i-1} - (-1)^i c_{k-i}.$$

Víme, že $R_1 = c_{k-1} - \beta$. Indukcí pokračujeme:

$$\begin{aligned}
R_2 &= -\beta(c_{k-1} - \beta) - c_{k-2} = \beta^2 - c_{k-1}\beta - c_{k-2},\\
R_3 &= -\beta(\beta^2 - c_{k-1}\beta - c_{k-2}) + c_{k-3} = -\beta^3 + c_{k-1}\beta^2 + c_{k-2}\beta + c_{k-3},\\
&\dots\\
R_i &= (-1)^i \cdot (\beta^i - c_{k-1}\beta^{i-1} - c_{k-2}\beta^{i-2} - \dots - c_{k-i}\beta^0).
\end{aligned}$$

Pro $i = k$ tedy získáme $\det(\mathbf{\Omega} - \beta\mathbf{E}) = R_k = \beta^k - c_{k-1}\beta^{k-1} - c_{k-2}\beta^{k-2} - \dots - c_0\beta^0$, což je přesně charakteristický polynom naší rekurence. Tím jsme pro případ jednoduchých kořenů větu dokázali.

Dar přítele Jordana

Co si počít, když matice $\mathbf{\Omega}$ není diagonalizovatelná? Tehdy nám pomůže nalézt *Jordanův tvar* matice. Ke každé matici lze totiž najít podobnou matici (tzn. lišící se pouze přechodem k jiné bázi), která je téměř diagonální. Přesněji má tvar

$$\begin{pmatrix}
\mathbf{J}_1 & 0 & \dots & 0\\
0 & \mathbf{J}_2 & \dots & 0\\
\vdots & \vdots & \ddots & \vdots\\
0 & 0 & \dots & \mathbf{J}_\ell
\end{pmatrix},$$

kde jednotlivé bloky $\mathbf{J}_i$ jsou tzv. *Jordanovy buňky,* což jsou matice typu

$$\begin{pmatrix}
\beta & 1 & 0 & \dots & 0 & 0\\
0 & \beta & 1 & \dots & 0 & 0\\
0 & 0 & \beta & \dots & 0 & 0\\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots\\
0 & 0 & 0 & \dots & \beta & 1\\
0 & 0 & 0 & \dots & 0 & \beta
\end{pmatrix}.$$

Každá buňka má na diagonále jedno vlastní číslo (dvě buňky mohou mít i totéž), těsně nad diagonálou jedničky a všude jinde nuly.

Jordanův tvar má každá matice (to je standardní věta z lineární algebry, čtenář nám snad promine, že ji nebudeme dokazovat), takže matici $\mathbf{\Omega}$ můžeme zapsat ve tvaru $\mathbf{P\Lambda P}^{-1}$, kde $\mathbf{P}$ je nějaká matice přechodu a $\mathbf{\Lambda}$ matice v Jordanově tvaru.

Umocňování matice $\mathbf{\Omega}$ tedy už zaběhnutým způsobem nahradíme umocňováním matice $\mathbf{\Lambda}$. Blokové matice se mocní po blocích, takže $\mathbf{\Lambda}^n$ musí mít na diagonále bloky $\mathbf{J}_1^n$, $\mathbf{J}_2^n$, …, $\mathbf{J}_\ell^n$. Stačí tedy umět umocnit na n-tou každou Jordanovu buňku.

Prohlédněme si mocniny buňky 3×3:

$$\begin{pmatrix} \beta & 1 & 0 \\ 0 & \beta & 1 \\ 0 & 0 & \beta \end{pmatrix} \quad \begin{pmatrix} \beta^2 & 2\beta & 1 \\ 0 & \beta^2 & 2\beta \\ 0 & 0 & \beta^2 \end{pmatrix} \quad \begin{pmatrix} \beta^3 & 3\beta^2 & 3\beta \\ 0 & \beta^3 & 3\beta^2 \\ 0 & 0 & \beta^3 \end{pmatrix} \quad \begin{pmatrix} \beta^4 & 4\beta^3 & 6\beta^2 \\ 0 & \beta^4 & 4\beta^3 \\ 0 & 0 & \beta^4 \end{pmatrix}.$$

Pod diagonálou se udržují nuly, na diagonále členy β^n, těsně nad diagonálou $n\beta^{n-1}$ a v pravém horním rohu $\binom{n}{2}\beta^{n-2}$.

Nabízí se tedy domněnka, že v n-té mocnině obecné Jordanovy buňky $q \times q$ jsou na diagonále mocniny vlastního čísla, pod diagonálou nuly a ve vzdálenosti t kroků nad diagonálou čísla $\binom{n}{t}\beta^{n-t}$:

$$\mathbf{J}^n = \begin{pmatrix} \beta^n & \binom{n}{1}\beta^{n-1} & \binom{n}{2}\beta^{n-2} & \dots & \binom{n}{q-2}\beta^{n-(q-2)} & \binom{n}{q-1}\beta^{n-(q-1)} \\ 0 & \beta^n & \binom{n}{1}\beta^{n-1} & \dots & \binom{n}{q-3}\beta^{n-(q-3)} & \binom{n}{q-2}\beta^{n-(q-2)} \\ 0 & 0 & \beta^n & \dots & \binom{n}{q-4}\beta^{n-(q-4)} & \binom{n}{q-3}\beta^{n-(q-3)} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & \beta^n & \binom{n}{1}\beta^{n-1} \\ 0 & 0 & 0 & \dots & 0 & \beta^n \end{pmatrix}.$$

Chování čísel na diagonále a pod ní plyne ihned z toho, že matice je horní trojúhelníková. Zbytek dokážeme indukcí. Případ $n = 1$ je triviální, indukční krok od n k $n+1$ provedeme takto: Uvažme prvek ve výšce t nad diagonálou v $\mathbf{J}^{n+1}$, řekněme na souřadnicích $(i, i+t)$. Podle definice násobení matic má být roven $\sum_s \mathbf{J}_{i,s}\mathbf{J}^n_{s,i+t}$. Matice $\mathbf{J}$ má ovšem nenuly pouze na diagonále a ve výšce 1, takže ze sumy zbude pouze

$$\mathbf{J}_{i,i}\mathbf{J}^n_{i,i+t} + \mathbf{J}_{i,i+1}\mathbf{J}^n_{i+1,i+t}.$$

To je podle indukčního předpokladu rovno

$$\beta \cdot \binom{n}{t}\beta^{n-t} + 1 \cdot \binom{n}{t-1}\beta^{n-t+1}.$$

Teď už stačí použít vztah pro součet kombinačních čísel v Pascalově trojúhelníku a získáme $\binom{n+1}{t}\beta^{n-t+1}$, což je přesně to, co potřebujeme.

Umocnit jednu Jordanovou buňku tedy umíme, a tím pádem i celou matici $\mathbf{\Lambda}$. Vraťme se nyní k řešení rekurence. Už víme, že n-tý prvek rekurence lze zapsat jako první složku vektoru $\mathbf{b} = \mathbf{P}\mathbf{\Lambda}^n\mathbf{P}^{-1}\mathbf{a}$ (kde $\mathbf{a}$ je vektor počátečních podmínek) a že tato složka je lineární kombinací prvků matice $\mathbf{\Lambda}^n$. Podle toho, co jsme zjistili o matici $\mathbf{\Lambda}^n$, víme, že je to tedy lineární kombinace výrazů typu $\binom{n}{j}\beta_i^n$, kde β_i je vlastní číslo a j číslo menší než násobnost tohoto vlastního čísla.

Tím jsme tedy dokončili třetí důkaz naší hlavní věty.