Diskrétní matematika B – 11. (zkrácený) týden
Kombinatorické výpočty

Michal Bulant

Masarykova univerzita
Fakulta informatiky

jaro 2014

Obsah přednášky

Doporučené zdroje

- Jan Slovák, Martin Panák, Michal Bulant, *Matematika drsně a svižně*, MU Brno, 2013, 774 s. (též jako e-text).
- *Předmětové záložky v IS MU*
- Donald E. Knuth, **The Art Of Computer Programming**.
- Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, Clifford Stein. **Introduction to Algorithms**, MIT Press, 2009.
- Robert Sedgewick, Philippe Flajolet, **An Introduction to the Analysis of Algorithms**, Addison-Wesley, 1995.
- Ronald L. Graham, Donald E. Knuth, Oren Patashnik, **Concrete Mathematics**, Addison-Wesley, 1994.
- H. S. Wilf, **Generatingfunctionology**, Academic Press, 1994, (rovněž `http://www.math.upenn.edu/~wilf/DownldGF.html`)

Úvodní motivace

Naším cílem nyní bude vybudovat základní prostředky pro řešení úloh obdobných těmto:

odvození Cayleyho formule Určete počet stromů na daných n vrcholech.

Analýza algoritmů Určete očekávaný počet porovnání během algoritmu `Quicksort`.

Quicksort – analýza průměrného případu

Ukázka implementace (*divide and conquer*, rozmyslete, proč není optimální):

```
if L == []: return []
return qsort([x for x in L[1:] if x<L[0]])
       + L[0:1]
       + qsort([x for x in L[1:] if x>=L[0]])
```

1. Počet porovnání při rozdělení (*divide*): $n-1$.
2. (Předpoklad náhodnosti): Pravděpodobnost toho, že prvek $L[0]$ je k-tý největší, je $\frac{1}{n}$.
3. Velikost tříděných polí ve fázi *conquer*: $k-1$ a $n-k$.

Pro střední hodnotu počtu porovnání tak dostáváme rekurentní vztah:

$$C_n = n - 1 + \sum_{k=1}^{n} \frac{1}{n} \left(C_{k-1} + C_{n-k} \right).$$

Zjednodušení rekurence

$$C_n = n - 1 + \sum_{k=1}^{n} \frac{1}{n} \left(C_{k-1} + C_{n-k} \right), \; C_0 = 0.$$

$$C_n = n - 1 + \frac{2}{n} \sum_{k=1}^{n} C_{k-1}$$ *symetrie obou sum*

$$nC_n = n(n-1) + 2 \sum_{k=1}^{n} C_{k-1}$$ *vynásob n*

$$(n-1)C_{n-1} = (n-1)(n-2) + 2 \sum_{k=1}^{n-1} C_{k-1}$$ *tentýž výraz pro C_{n-1}*

$$nC_n = (n+1)C_{n-1} + 2(n-1)$$ *odečteno a upraveno*

Vyřešení rekurence

$$nC_n = (n+1)C_{n-1} + 2(n-1)$$

Přestože jsme již rekurenci výrazně zjednodušili, takže je možné jednoduše iterativně hodnoty C_n dopočítat, je často žádoucí tyto hodnoty konkrétně (nebo alespoň přibližně) vyjádřit explicitně jako funkci n.

Nejprve si pomůžeme drobným trikem, kdy vydělíme obě strany výrazem $n(n+1)$:

$$\frac{C_n}{n+1} = \frac{C_{n-1}}{n} + \frac{2(n-1)}{n(n+1)}$$

Nyní tento vztah „rozbalíme“ (*telescope*, příp. si pomůžeme substitucí $B_n = C_n/(n+1)$):

$$\frac{C_n}{n+1} = \frac{2(n-1)}{n(n+1)} + \frac{2(n-2)}{(n-1)n} + \cdots + \frac{2\cdot 1}{2\cdot 3} + \frac{C_1}{2}$$

Vyřešení rekurence

Odkud

$$\frac{C_n}{n+1} = 2\sum_{k=1}^{n-1} \frac{k}{(k+1)(k+2)}.$$

Výraz sečteme např. pomocí rozkladu na parciální zlomky $\frac{k}{(k+1)(k+2)} = \frac{2}{k+2} - \frac{1}{k+1}$ a dostaneme

$$\frac{C_n}{n+1} = 2\left(H_{n+1} - 2 + \frac{1}{n+1}\right),$$

odkud

$$C_n = 2(n+1)H_{n+1} - 4(n+1) + 2$$

($H_n = \sum_{k=1}^{n} \frac{1}{k}$ je součet prvních n členů harmonické řady). Přitom je možné odhadnout $H_n \sim \int_1^n \frac{\mathrm{d}x}{x} + \gamma$, odkud

$$C_n \sim 2(n+1)(\ln(n+1) + \gamma - 2) + 2.$$

Opakování kombinatorických vztahů

Stručně nyní zopakujme některé důležité kombinatorické pojmy a vztahy:

Aritmetická řada $$\sum_{k=0}^{n} k = \frac{n(n+1)}{2} = \binom{n+1}{2}$$

Geometrická řada $$\sum_{k=0}^{n} x^k = \frac{x^{n+1}-1}{x-1}$$

Binomická věta $$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$$

Horní binomická řada $$\sum_{k=0}^{n} \binom{k}{m} = \binom{n+1}{m+1}$$

Vandermondova konvoluce $$\binom{m+n}{r} = \sum_{k=0}^{r} \binom{m}{k} \binom{n}{r-k}$$

Motto: *spojité a diskrétní modely se vzájemně potřebují a doplňují.*

Příklad

Máme v peněžence 4 korunové mince, 5 dvoukorunových a 3 pětikorunové. Z automatu, který nevrací, chceme minerálku za 22 Kč. Kolika způsoby to umíme, aniž bychom ztratili přeplatek?

Hledáme zjevně čísla i, j a k taková, že $i + j + k = 22$ a zároveň

$$i \in \{0, 1, 2, 3, 4\}, \; j \in \{0, 2, 4, 6, 8, 10\}, \; k \in \{0, 5, 10, 15\}.$$

Uvažme součin polynomů (třeba nad reálnými čísly)

$$(x^0+x^1+x^2+x^3+x^4)(x^0+x^2+x^4+x^6+x^8+x^{10})(x^0+x^5+x^{10}+x^{15}).$$

Mělo by být zřejmé, že hledaný počet řešení je díky (Cauchyovskému) způsobu násobení polynomů právě koeficient u x^{22} ve výsledném polynomu. Skutečně tak dostáváme **čtyři možnosti** $3*5+3*2+1*1$, $3*5+2*2+3*1$, $2*5+5*2+2*1$ a $2*5+4*2+4*1$.

Předchozí příklad asi vypadal spíš jako složitý zápis jednoduchých „backtrackingových úvah“. Následující příklad ukazuje, že tento postup lze ale s výhodou zobecnit.

Nechť I, J jsou konečné množiny nezáporných celých čísel. Potom je pro dané $r \in \mathbb{N}$ počet řešení (i, j) rovnice $i + j = r$ splňujících $i \in I, j \in J$ roven koeficientu u x^r v polynomu $(\sum_{i \in I} x^i)(\sum_{j \in J} x^j)$.

Příklad

Kolika způsoby můžeme pomocí mincí (1, 2, 5, 10, 20 a 50 Kč) zaplatit platbu 100 Kč?

Hledáme přirozená čísla $a_1, a_2, a_5, a_{10}, a_{20}$ a a_{50} taková, že a_i je násobkem i pro všechna $i \in \{1, 2, 5, 10, 20, 50\}$ a zároveň $a_1 + a_2 + a_5 + a_{10} + a_{20} + a_{50} = 100$. Podobně jako výše je vidět, že požadovaný počet lze získat jako koeficient u x^{100} v

$$(1 + x + x^2 + \dots)(1 + x^2 + x^4 + \dots)(1 + x^5 + x^{10} + \dots)$$
$$(1 + x^{10} + x^{20} + \dots)(1 + x^{20} + x^{40} + \dots)(1 + x^{50} + x^{100} + \dots)$$

Podobným způsobem můžeme znovu velmi snadno odvodit některé kombinatorické vztahy, které známe již z dřívějška. Využijeme přitom **binomickou větu.**

Věta (binomická)

Pro $n \in \mathbb{N}$ a $r \in \mathbb{R}$ platí

$$(1+x)^n = \binom{n}{0} + \binom{n}{1}x + \binom{n}{2}x^2 + \cdots + \binom{n}{n}x^n.$$

Na levou stranu se můžeme dívat jako na součin n polynomů, pravá je zápisem polynomu vzniklého jejich roznásobením. Dosazením čísel $x = 1$, resp. $x = -1$ dostáváme známé vzorce:

Důsledek

- $\sum_{k=0}^{n} \binom{n}{k} = 2^n$,
- $\sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0$.

Podíváme se teď na obě strany v binomické větě „spojitýma očima" a s využitím vlastností derivací odvodíme další vztah mezi kombinačními čísly.

Důsledek

Platí

$$\sum_{k=0}^{n} k\binom{n}{k} = n2^{n-1}.$$

Důkaz.

Na obě strany binomické věty se podíváme jako na polynomiální funkce. Derivací levé strany dostaneme $n(1+x)^{n-1}$, derivací pravé strany (člen po členu) pak $\sum_{k=1}^{n} k\binom{n}{k}x^{k-1}$. Dosazením $x=1$ dostaneme tvrzení. $\square$

„Flashback“ do algebry

Ještě upozorněme na vzdálenou souvislost se systémy polynomiálních rovnic, kterým jsme se věnovali minule. Ty lze použít na řešení obdobného typu úloh.

Příklad

Jaký je minimální počet bankovek potřebný k zaplacení 77700 Kč? Uvažujte nejprve, že k dispozici máte bankovky v hodnotě 100 Kč, 200 Kč, 500 Kč, 1000 Kč. Potom předpokládejte, že máte i bankovku 2000 Kč a na konec předpokládejte, že nemáte bankovky 2000 Kč, ale máte bankovky v hodnotě 5000 Kč.

Řešení

Označme si bankovky po řadě proměnnými s, d, p, t, D, P. Platbu bude reprezentovat polynom v těchto proměnných tak, že exponent každé proměnné bude určovat počet použitých příslušných bankovek. Pokud zaplatíme deseti tisícikorunami, deseti pětisetkorunami i stokorunami, pak bude $q = t^{10}p^{10}s^{627}$.

Řešení (pokr.)

Pokud máme pouze bankovky s, d, p, t, pak má ideál popisující vztah jednotlivých bankovek tvar $I_1 = \langle s^2 - d, s^5 - p, s^{10} - t \rangle$. Abychom minimalizovali počet použitých bankovek, spočítáme Gröbnerovu bázi vzhledem ke gradovanému opačnému lexikografickému uspořádání (chceme eliminovat malé bankovky)

$$G_1 = (p^2 - t, s^2 - d, d^3 - sp, sd^2 - p).$$

Nyní vezmeme libovolný polynom reprezentující danou platbu. Redukcí tohoto polynomu vzhledem k bázi G_1 dostaneme polynom, jehož stupeň je vzhledem k našemu monomiálnímu uspořádání nejmenší a je jednoduché si rozmyslet, že to je právě polynom reprezentující optimální platbu. Vezměme tedy např. $q = s^{777}$. Redukce vzhledem ke G_1 je pak $t^{77}pd$. To znamená, že optimální platba v prvním případě je 77 tisícikorun, jedna pětisetkoruna a jedna dvousetkoruna. Dohromady tedy 79 bankovek.

Řešení (pokr.)

V druhém případě, kdy máme i bankovku D, je ideál $I_2 = \langle s^2 - d, s^5 - p, s^{10} - t, s^{20} - D \rangle$ a jeho Gröbnerova báze je

$$G_2 = (t^2 - D, p^2 - t, s^2 - d, d^3 - sp, sd^2 - p).$$

Redukce $q = s^{777}$ vzhledem ke G_2 dá $D^{38}tpd$, takže tentokrát zaplatíme 41 bankovkami. Ve třetím případě je $I_3 = \langle s^2 - d, s^5 - p, s^{10} - t, s^{50} - P \rangle$ a

$$G_3 = (t^5 - P, p^2 - t, s^2 - d, d^3 - sp, sd^2 - p),$$

a redukce je proto rovna $P^{15}t^2pd$. V tomto případě tedy potřebujeme pouze 19 bankovek. $\square$

Tuto jednoduchou úlohu lze samozřejmě vyřešit rychle prostou úvahou. Uvedený postup používající Gröbnerovu bázi ovšem dává univerzální algoritmus. který lze automaticky použít pro vyšší částky a jiné, složitější případy.

(Formální) mocninné řady

Definice

Buď dána nekonečná posloupnost $a = (a_0, a_1, a_2, \ldots)$. Její **vytvořující funkcí** rozumíme (formální) mocninnou řadu tvaru

$$\sum_{i=0}^{\infty} a_i x^i = a_0 + a_1 x + a_2 x^2 + \cdots .$$

Poznámka

O **formální** mocninné řadě hovoříme proto, že se zatím na tuto řadu díváme čistě formálně jako na jiný zápis dané posloupnosti a nezajímáme se o konvergenci. Na druhou stranu to ale znamená, že formální mocninná řada není funkce a nemůžeme do ní dosazovat. To ovšem vzápětí napravíme, když s využitím znalostí z analýzy nekonečných řad přejdeme od formálních mocninnných řad k příslušným funkcím.

Příklad

Posloupnosti samých jedniček odpovídá formální mocninná řada $1 + x + x^2 + x^3 + \cdots$. Z analýzy víme, že stejně zapsaná mocninná řada konverguje pro $x \in (-1, 1)$ a její součet je roven funkci $1/(1 - x)$. Stejně tak obráceně, rozvineme-li tuto funkci do Taylorovy řady v bodě 0, dostaneme zřejmě původní řadu. Takovéto „zakódování“ posloupnosti čísel do funkce a zpět je klíčovým obratem v teorii vytvořujících funkcí.

Jak jsme již zmínili, tento obrat lze ale použít pouze tehdy, pokud víme, že řada alespoň v nějakém okolí 0 konverguje. Často ale „diskrétní“ matematici používají následující „podvod“:

- pomocí formálních mocninných řad odvodí nějaký vztah (formuli, rekurenci,...) bez toho, aby se zajímali o konvergenci
- jinými prostředky (často matematickou indukcí) tento vztah dokážou

Vytvořující funkce v praxi využíváme:

- k nalezení **explicitní formule** pro *n*-tý člen posloupnosti;
- často vytvořující funkce vycházejí z rekurentních vztahů, občas ale díky nim odvodíme rekurentní vztahy nové;
- výpočet průměrů či jiných statistických závislostí (např. průměrná složitost algoritmu);
- důkaz různých identit;
- často je nalezení přesného vztahu příliš obtížné, ale mnohdy stačí vztah přibližný nebo alespoň asymptotické chování.

Exponenciální vytvořující funkce

Kromě výše zmíněných vytvořujících funkcí se v praxi rovněž často objevují jejich tzv. *exponenciální* varianty[1].

$$g(x) = \sum_{n\geq 0} g_n \frac{x^n}{n!}.$$

Poznámka

Jméno vychází z toho, že exponenciální funkce e^x je (exponenciální) vytvořující funkcí pro základní posloupnost $(1, 1, 1, 1, \ldots)$.
V některých případech (např. v důkazu Cayleyho věty) je použití exponenciálních vytvořujících funkcí výhodnější.

[1] Používají se i další typy vytvořujících funkcí (např. v teorii čísel se používají Dirichletovy vytvořující funkce, kde roli faktoru x^n hraje n^{-x}), ale těmi se zde zabývat nebudeme.

Dosazování do mocninných řad

Následující větu znáte z matematické analýzy z loňského semestru:

Věta

Buď $(a_0, a_1, a_2, \dots)$ posloupnost reálných čísel. Platí-li pro nějaké $K \in \mathbb{R}$, že pro všechna $n \geq 1$ je $|a_n| \leq K^n$, pak řada

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

konverguje pro každé $x \in (-\frac{1}{K}, \frac{1}{K})$. Součet této řady tedy definuje funkci na uvedeném intervalu, tuto funkci označujeme rovněž $a(x)$. Hodnotami funkce $a(x)$ na libovolném okolí 0 je jednoznačně určena původní posloupnost, neboť má $a(x)$ v 0 derivace všech řádů a platí

$$a_n = \frac{a^{(n)}(0)}{n!}.$$