

# Úvod do diskrétní matematiky

Doc. RNDr. Miroslav Koucký, CSc.

Liberec, 2020

## Obsah

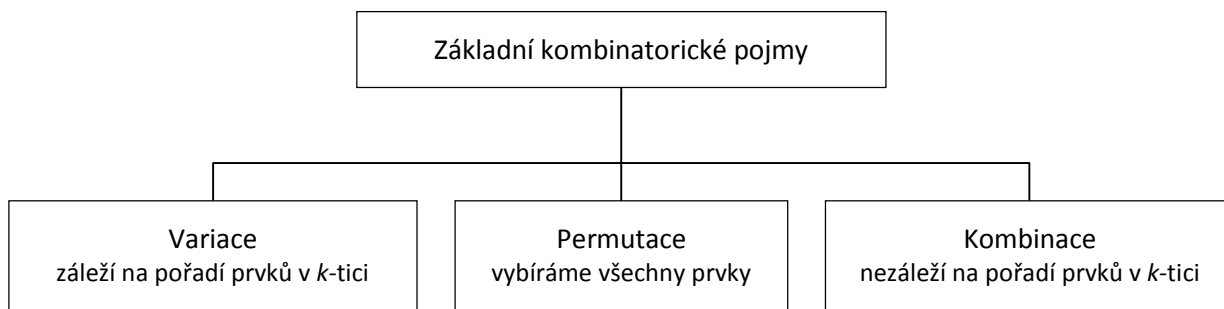
<b>1. Elementární kombinatorika</b>	<b>... 3</b>
1.1. Základní pravidla kombinatoriky	... 3
1.2. Variace, permutace, kombinace	... 5
1.3. Základní kombinatorické identity	... 11
1.4. Subfaktoriály, Catalanova čísla	... 14
1.5. Binomická a multinomická věta, Newtonův vzorec	... 17
<b>2. Rozklady</b>	<b>... 19</b>
2.1. Rozklady nerozlišitelných objektů do rozlišitelných tříd	... 19
2.2. Rozklady nerozlišitelných objektů do nerozlišitelných tříd	... 21
2.3. Stirlingova čísla	... 22
<b>3. Rekurentní vztahy</b>	<b>... 25</b>
3.1. Homogenní lineární rekurentní vztahy a jejich řešení	... 26
3.2. Nehomogenní lineární rekurentní vztahy a jejich řešení	... 28
<b>4. Vytvořující funkce</b>	<b>... 31</b>
4.1. Řešení rekurentních vztahů metodou vytvořujících funkcí	... 35
4.2. Věžové polynomy	... 37
<b>5. Burnside/Pólya enumerační metoda</b>	<b>... 41</b>
5.1. Permutace, symetrická grupa	... 41
<b>6. Symbolika <math>O</math>, <math>\Omega</math>, <math>\Theta</math>, složitost algoritmů</b>	<b>... 46</b>
<b>7. Rekurzivní algoritmy divide and conquer</b>	<b>... 48</b>
<b>8. Přílohy</b>	<b>... 50</b>
8.1. Přehled značení	
8.2. Tabulka hodnot subfaktoriálů	
8.3. Tabulka hodnot Fibonacciho čísel	
8.4. Tabulka hodnot Catalanových čísel	
8.5. Tabulka hodnot Stirlingových čísel 1. druhu	
8.6. Tabulka hodnot Stirlingových čísel 2. druhu	

### Předmluva

Skripta Úvod do diskrétní matematiky jsou úvodem do elementárního kombinatorického počítání a seznamují čtenáře se základními myšlenkami a pojmy z oblasti klasické kombinatoriky. Na tato skripta budou navazují skripta Kombinatorické metody II, která se věnují dalším vybraným tématům zejména teorii grafů.

# 1. Elementární kombinatorika

Systematický rozvoj kombinatoriky lze datovat do 17. století a je spojen se jmény Blaise Pascal, Pierre de Fermat, Christian Huygens a Jacob Bernoulli. Hlavní pozornost se soustředila především na řešení různých otázek spojených s problematikou hazardních her, loterií apod. V tomto kontextu lze nejjednodušší úlohu kombinatoriky formulovat následovně - kolika různými způsoby je možné z  $n$  objektů vybrat  $k$ -tici (tj.  $k$  objektů). V závislosti na podmínkách, které definují různé způsoby výběru, se dostáváme k následujícím základním kombinatorickým pojmům - variace, permutace a kombinace. První představu o obsahu těchto pojmů si lze udělat z následujícího schématu.



## 1.1. Základní pravidla kombinatoriky

Při řešení kombinatorických úloh velmi rychle zjistíme, že většina z nich má tu nepříjemnou vlastnost, že nemůže být řešena metodou „hrubé síly“, kdy hledáme řešení výčtem, resp. vyzkoušením všech možností. Ukazuje se, že tento přístup k řešení kombinatorických úloh je i mimo možnosti současné výpočetní techniky. Z těchto důvodů jsou potřebná základní kombinatorická pravidla a metody, jejichž vhodnou aplikací lze vyřešit většinu běžných, někdy i netriviálních, kombinatorických úloh. Jde především o pravidlo součtu, pravidlo součinu, Dirichletův princip a princip inkluze a exkluze.

### Pravidlo součtu

Nechť množina  $A = \{a_1, \dots, a_m\}$  obsahuje  $m$  různých prvků a množina  $B = \{b_1, \dots, b_n\}$  obsahuje  $n$  různých prvků, navíc  $A \cap B = \emptyset$ . Potom jeden prvek z množiny  $A \cup B$  lze vybrat  $m + n$  různými způsoby.

Důkaz.

Vzhledem k předpokladu  $A \cap B = \emptyset$ , je pravidlo součtu ekvivalentní s tvrzením  $|A \cup B| = |A| + |B|$ .

### Pravidlo součinu

Nechť množina  $A = \{a_1, \dots, a_m\}$  obsahuje  $m$  různých prvků a množina  $B = \{b_1, \dots, b_n\}$  obsahuje  $n$  různých prvků. Potom uspořádanou dvojici prvků  $(a_i, b_j)$ , kde  $a_i \in A, b_j \in B$  lze vybrat  $m \cdot n$  různými způsoby.

Důkaz.

Pravidlo součinu je ekvivalentní se zřejmým tvrzením  $|A \times B| = |A| \cdot |B|$ , kde symbol  $\times$  označuje kartézský součin. Schematicky lze toto pravidlo znázornit maticí

$$A \times B = \left\{ \begin{array}{cccc} (a_1, b_1) & (a_1, b_2) & \cdots & (a_1, b_n) \\ (a_2, b_1) & (a_2, b_2) & \cdots & (a_2, b_n) \\ \vdots & \vdots & \cdots & \vdots \\ (a_m, b_1) & (a_m, b_2) & \cdots & (a_m, b_n) \end{array} \right\}$$

typu  $m, n$ , která obsahuje (právě jednou) všechny uspořádané dvojice  $(a_i, b_j), i = 1, \dots, m, j = 1, \dots, n$ .

## Poznámky

- Pravidlo součtu lze snadno zobecnit na případ více množin. Jsou-li  $A_1, \dots, A_n$  po dvou disjunktní množiny (tj.  $\forall i \neq j A_i \cap A_j = \emptyset$ ), dostáváme

$$|A_1 \cup A_2 \cup \dots \cup A_n| = |A_1| + |A_2| + \dots + |A_n|.$$

V případě, kdy není splněna podmínka disjunktnosti po dvou, pravidlo součtu nelze aplikovat a je třeba použít princip inkluze a exkluze (viz poznámka dále).

- Pravidlo součinu lze také zobecnit na případ více (konečných) množin. Dostáváme tak

$$|A_1 \times A_2 \times \dots \times A_n| = |A_1| \cdot |A_2| \cdot \dots \cdot |A_n|.$$

## Princip inkluze a exkluze (princip IE)

Označme  $N$  celkový počet objektů, které mohou mít některé z vlastností  $\alpha_1, \dots, \alpha_n$ . Označme dále  $N(\alpha_{i_1}, \dots, \alpha_{i_k})$  počet všech objektů z celkového počtu  $N$ , které mají vlastnosti uvedené v závorce, tj.  $\alpha_{i_1}, \dots, \alpha_{i_k}$  (a to bez ohledu na to, zda mají některé další vlastnosti). Potom pro počet  $N(\bar{\alpha}_1, \dots, \bar{\alpha}_n)$  objektů, které nemají žádnou z uvedených vlastností  $\alpha_1, \dots, \alpha_n$  platí

$$N(\bar{\alpha}_1, \dots, \bar{\alpha}_n) = N - [\sum_{i=1}^n N(\alpha_i)] + [\sum_{1 \leq i_1 < i_2 \leq n} N(\alpha_{i_1}, \alpha_{i_2})] - [\sum_{1 \leq i_1 < i_2 < i_3 \leq n} N(\alpha_{i_1}, \alpha_{i_2}, \alpha_{i_3})] + \dots + (-1)^k [\sum_{1 \leq i_1 < \dots < i_k \leq n} N(\alpha_{i_1}, \dots, \alpha_{i_k})] + \dots + (-1)^n N(\alpha_1, \alpha_2, \dots, \alpha_n)$$

Důkaz.

Matematickou indukci dle počtu vlastností, tj. dle  $n$ .

Pro  $n = 1$  má princip IE triviálně platný tvar  $N(\bar{\alpha}_1) = N - N(\alpha_1)$ .

Předpokládejme nyní jeho platnost pro libovolnou skupinu předmětů a  $(n - 1)$  vlastností, tj.

$$N(\bar{\alpha}_1, \dots, \bar{\alpha}_{n-1}) = N - [\sum_{i=1}^{n-1} N(\alpha_i)] + [\sum_{1 \leq i_1 < i_2 \leq n-1} N(\alpha_{i_1}, \alpha_{i_2})] + \dots + (-1)^k [\sum_{1 \leq i_1 < \dots < i_k \leq n-1} N(\alpha_{i_1}, \dots, \alpha_{i_k})] + \dots + (-1)^{n-1} N(\alpha_1, \alpha_2, \dots, \alpha_{n-1})$$

Aplikací tohoto předpokladu na skupinu předmětů majících vlastnost  $\alpha_n$  dostáváme

$$N(\bar{\alpha}_1, \dots, \bar{\alpha}_{n-1}, \alpha_n) = N(\alpha_n) - [\sum_{i=1}^{n-1} N(\alpha_i, \alpha_n)] + [\sum_{1 \leq i_1 < i_2 \leq n-1} N(\alpha_{i_1}, \alpha_{i_2}, \alpha_n)] + \dots + (-1)^k [\sum_{1 \leq i_1 < \dots < i_k \leq n-1} N(\alpha_{i_1}, \dots, \alpha_{i_k}, \alpha_n)] + \dots + (-1)^{n-1} N(\alpha_1, \alpha_2, \dots, \alpha_{n-1}, \alpha_n)$$

Dále zřejmě platí

$$N(\bar{\alpha}_1, \dots, \bar{\alpha}_n) = N(\bar{\alpha}_1, \dots, \bar{\alpha}_{n-1}) - N(\bar{\alpha}_1, \dots, \bar{\alpha}_{n-1}, \alpha_n).$$

Po dosazení výše uvedených vztahů a elementární úpravě dostáváme dokazované tvrzení.

## Poznámky

- Množinově bývá princip IE zapisován ve tvaru

$$|\cup_{i=1}^n A_i| = \sum_{i=1}^n |A_i| - [\sum_{1 \leq i_1 < i_2 \leq n} |A_{i_1} \cap A_{i_2}|] + \dots + (-1)^{k+1} [\sum_{1 \leq i_1 < \dots < i_k \leq n} |A_{i_1} \cap \dots \cap A_{i_k}|] + \dots + (-1)^{n+1} |A_1 \cap \dots \cap A_n|$$

- Speciálně v případě  $n = 2$  dostáváme

$$N(\bar{\alpha}_1, \bar{\alpha}_2) = N - N(\alpha_1) - N(\alpha_2) + N(\alpha_1, \alpha_2), \text{ resp. } |A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|.$$

V případě  $n = 3$  dostáváme

$$N(\bar{\alpha}_1, \bar{\alpha}_2, \bar{\alpha}_3) = N - N(\alpha_1) - N(\alpha_2) - N(\alpha_3) + N(\alpha_1, \alpha_2) + N(\alpha_1, \alpha_3) + N(\alpha_2, \alpha_3) - N(\alpha_1, \alpha_2, \alpha_3)$$

$$\text{resp. } |A_1 \cup A_2 \cup A_3| = |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| + |A_1 \cap A_2 \cap A_3|.$$

(případy  $n = 2, 3$  lze přehledně znázornit Vennovými diagramy).

### Dirichletův princip (P. G. L. Dirichlet, 1805 – 1859)

Při libovolném rozmístění  $n$  objektů do  $k$  přihrádek obsahuje alespoň jedna z nich nejméně  $\lceil n/k \rceil$  objektů.  
Důkaz.

Sporem. Předpokládejme, že každá přihrádka obsahuje nejvýše  $\lceil n/k \rceil - 1$  objektů. Z definice  $\lceil x \rceil$  dostáváme  $n \leq k(\lceil n/k \rceil - 1) < k(n/k) = n$ . Spor - alespoň jedna přihrádka obsahuje alespoň  $\lceil n/k \rceil$  objektů.

### Příklad

Určete minimální počet obyvatel města, jestliže víte, že alespoň 15 lidí má ve stejný den a měsíc narozeniny (k roku nepřihlížíme a předpokládáme 365 dní v roce).

Řešení.

Dny v roce reprezentují „přihrádky“, tj.  $k = 365$ . V alespoň jedné má být 15 objektů (osob se stejným datem narození). Z Dirichletova principu plyne, že hledáme nejmenší přirozené  $n$  takové, aby  $\lceil n/365 \rceil \geq 15$ . Odtud  $n = 5\,111$ .

### Poznámka

Dirichletův princip lze formulovat také následovně: Uvažujme  $k$  libovolných kladných přirozených čísel  $n_1, \dots, n_k$ . Pokud rozmístíme  $n_1 + \dots + n_k - k + 1$  objektů do  $k$  skupin, potom existuje  $i \in \{1, \dots, k\}$  a alespoň jedna skupina, která obsahuje alespoň  $n_i$  objektů. (důkaz snadné cvičení)

## 1.2. Variace, permutace, kombinace

Nyní se vrátíme k exaktnějšímu vymezení základních kombinatorických pojmů - variace, permutace a kombinace. Připomeňme, že pro  $n \in \mathbb{N}$  označujeme součin  $1 \cdot 2 \cdot \dots \cdot n$  symbolem  $n!$  (čteme  $n$  faktoriál), kde definujeme  $0! = 1$ .

### Definice - variace bez opakování

Označme  $M$  množinu obsahující  $n$  různých prvků. Variací  $k$ -té třídy z  $n$  prvků (resp. na  $n$ -prvkové množině  $M$ ) nazýváme každou uspořádanou  $k$ -tici navzájem různých prvků množiny  $M$ . Počet všech variací  $k$ -té třídy z  $n$  prvků označíme  $A_n^k$ .

Stručně lze variace bez opakování charakterizovat jako uspořádané  $k$ -tice (tj. záleží na pořadí prvků ve vybrané  $k$ -tici), ve které se jednotlivé prvky nesmí opakovat. Dvě variace (bez opakování) považujeme tedy za různé, pokud se liší na alespoň jedné pozici.

### Tvrzení

Pro libovolné  $k, n \in \mathbb{N}, k \leq n$  platí

$$A_n^k = n \cdot (n - 1) \cdot \dots \cdot (n - k + 1) = \frac{n!}{(n - k)!}$$

Důkaz.

Počty prvků, které jsou na „výběr“ při obsazování jednotlivých pozic ve variaci (bez opakování), jsou zřejmě dány následující tabulkou:

1. pozice	2. pozice	...	$k$ -tá pozice
$n$	$n - 1$	...	$n - k + 1$

Dle pravidla součinu tak dostáváme platnost tvrzení.

### Definice - variace s opakováním

Mějme  $k$  dispozici  $n$  různých druhů prvků, každý druh v libovolném množství. Variací  $k$ -té třídy z  $n$  prvků s opakováním nazýváme každou uspořádanou  $k$ -tici vytvořenou z prvků uvedených druhů. Počet všech variací  $k$ -té třídy z  $n$  prvků s opakováním označíme  $\bar{A}_n^k$ .

Stručně lze variace s opakováním charakterizovat jako uspořádané  $k$ -tice, ve které se jednotlivé druhy prvků mohou opakovat. Dvě variace s opakováním považujeme za různé, pokud se liší na alespoň jedné pozici.

### Tvrzení

Pro libovolné  $k, n \in \mathbb{N}$  platí

$$\bar{A}_n^k = n^k.$$

Důkaz.

Počty prvků, kterými lze obsadit jednotlivé pozice ve variaci s opakováním, jsou zřejmě dány následující tabulkou (druhy se mohou opakovat!)

1. pozice	2. pozice	...	$k$ -tá pozice
$n$	$n$		$n$

Dle pravidla součinu tak dostáváme platnost tvrzení.

### Poznámky

Variace  $k$ -té třídy z  $n$  prvků lze definovat pomocí pojmu zobrazení. Označme  $K = \{1, 2, \dots, k\}$  a  $A = \{a_1, \dots, a_n\}$  množinu obsahující  $n$  různých prvků.

- Variace  $k$ -té třídy z  $n$  prvků bez opakování ( $k \leq n$ ) odpovídají všem prostým zobrazením  $K$  do  $A$ .
- Variace  $k$ -té třídy z  $n$  prvků s opakováním odpovídají všem zobrazením  $K$  do  $A$ .

### Příklad

Určete počet všech podmnožin libovolné  $n$  prvkové množiny  $A$ .

Řešení.

Označme  $A = \{a_1, \dots, a_n\}$ . Každé podmnožině  $B \subseteq A$  lze přiřadit uspořádanou  $n$ -tici  $(x_1, \dots, x_n)$ , nazývanou charakteristický vektor podmnožiny  $B$  tak, že

$$x_i = \begin{cases} 1, & a_i \in B \\ 0, & a_i \notin B \end{cases}$$

Podmnožiny tak jednoznačně odpovídají výše uvedeným variacím  $n$ -té třídy s opakováním ze dvou prvků 0, 1. Naopak, každá variace  $n$ -té třídy z 2 prvků (s opakováním) jednoznačně definuje jistou podmnožinu množiny  $A$ , proto počet všech podmnožin  $n$ -prvkové množiny je roven počtu variací  $n$ -té třídy z 2 prvků s opakováním, tj.  $\bar{A}_2^n = 2^n$ .

### Poznámka

Systém všech podmnožin množiny  $A$  se běžně označuje některým z následujících symbolů  $P(A)$ ,  $2^A$  a nazývá se potenční množina množiny  $A$ . Jak plyne z výše uvedeného příkladu, pro konečnou množinu  $A$  platí

$$|P(A)| = 2^{|A|}.$$

Uvedme např., že  $P(\emptyset) = \{\emptyset\}$ ,  $P(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}$ ,  $P(\{\emptyset, \{\emptyset\}\}) = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$ .

### Definice - permutace bez opakování

Označme  $M$  množinu obsahující  $n$  různých prvků. Permutací řádu  $n$  (resp. na množině  $M$ ) nazveme libovolnou uspořádanou  $n$ -tici vytvořenou z prvků množiny  $M$ . Počet všech permutací řádu  $n$  označíme  $P(n)$ , resp.  $P_n$ .

## Poznámky

- Permutace řádu  $n$  (bez opakování) jsou speciálním případem variací bez opakování, totiž variace  $n$ -té třídy z  $n$  prvků, tj.  $P(n) = A_n^n$ .
- Permutace na množině  $M$  odpovídají všem vzájemně jednoznačným zobrazením množiny  $M$  na sebe (tzv. bijektivní zobrazení, tj. prosté a na).
- Platí následující rekurentní vztahy
  - $P(n) = n \cdot P(n - 1)$ , kde  $P(0) = 1$ ,
  - $P(n) = (n - 1) \cdot (P(n - 1) + P(n - 2))$ , kde  $P(0) = P(1) = 1$ .

S prvním z výše uvedených vztahů se ještě setkáme v celé řadě souvislostí. V této chvíli uveďme jeho možnou kombinatorickou interpretaci. Množinu všech permutací na  $\{a_1, \dots, a_n\}$  rozložíme do  $n$  tříd  $A_1, \dots, A_n$  tak, že  $A_i$  obsahuje právě všechny permutace, které mají na první pozici prvek  $a_i$ . Snadno zjistíme, že takto definované třídy tvoří rozklad (třídy jsou po dvou disjunktní a jejich sjednocení obsahuje všechny uvažované permutace) a navíc ze zřejmých důvodů mají stejný počet prvků, tj.  $\forall i, j \ |A_i| = |A_j|$ . Z definice jednotlivých tříd pak vyplývá, že  $|A_i| = P(n - 1)$ , tedy  $P(n) = \sum_{i=1}^n |A_i| = nP(n - 1)$ .

## Tvrzení

Pro libovolné  $n \in \mathbb{N}$  platí

$$P(n) = n!$$

kde definujeme  $0! = 1$ .

Důkaz.

Počet možností jak obsadit jednotlivé pozice v permutaci jsou zřejmě dány tabulkou:

1. pozice	2. pozice	...	$n$ -tá pozice
$n$	$n - 1$		1

Podle pravidla součinu dostáváme platnost tvrzení.

## Definice - permutace s opakováním

Nechť množina  $M$  obsahuje  $n_1$  stejných prvků 1. druhu,  $n_2$  stejných prvků 2. druhu až  $n_k$  stejných prvků  $k$ -tého druhu. Potom každé uspořádání prvků této množiny (tj. každou uspořádanou  $n$ -tici těchto prvků, kde  $n = n_1 + \dots + n_k$ ) nazveme permutací s opakováním řádu  $(n_1, \dots, n_k)$ . Počet všech permutací s opakováním řádu  $(n_1, \dots, n_k)$  označíme  $P(n_1, \dots, n_k)$ , resp.  $P_{n_1, \dots, n_k}$ .

## Tvrzení

Pro libovolná přirozená čísla  $n_1, \dots, n_k$  platí

$$P(n_1, \dots, n_k) = \frac{(n_1 + \dots + n_k)!}{n_1! \cdot \dots \cdot n_k!}$$

Důkaz.

Označme  $M = \{\underbrace{a, \dots, a}_{n_1}, \underbrace{b, \dots, b}_{n_2}, \dots, \underbrace{r, \dots, r}_{n_k}\}$ , kde  $n = n_1 + \dots + n_k$  množinu prvků, ze kterých budou vytvářeny permutace. Každá permutace s opakováním je zřejmě invariantní vzhledem k permutacím prvků jednotlivých druhů. Prvky  $i$ -tého druhu lze permutovat  $n_i!$  způsoby, tedy dle pravidla součinu dostáváme

$$P(n_1 + \dots + n_k) = P(n_1, \dots, n_k) \cdot n_1! \cdot \dots \cdot n_k!$$

odkud je platnost tvrzení zřejmá.

## Příklad

Kolik různých slov (bez ohledu na smysl) lze sestavit při využití všech písmen slova POPOKATEPETL.

Řešení.

Evidentně jde o permutace s opakováním na množině  $M = \{A, E, E, K, L, O, O, P, P, P, T, T\}$ , tedy hledaný počet slov je roven  $P(1,2,1,1,2,3,2) = \frac{12!}{1! \cdot 2! \cdot 1! \cdot 1! \cdot 2! \cdot 3! \cdot 2!} = 9\,979\,200$ .

**Definice** - kombinace bez opakování

Označme  $M$  množinu obsahující  $n$  různých prvků. Kombinací  $k$ -té třídy z  $n$  prvků (resp. na  $n$ -prvkové množině  $M$ ) nazýváme každou neuspořádanou  $k$ -tici navzájem různých prvků množiny  $M$ . Počet kombinací  $k$ -té třídy z  $n$  prvků (bez opakování) budeme značit  $C_n^k$ .

**Poznámky**

- Dvě kombinace považujeme za různé, pokud se liší v zastoupení některého prvku (bez ohledu na pozici).
- Číslo  $C_n^k$  se v závislosti na kontextu nazývá kombinační číslo, resp. binomický koeficient a označuje se také symbolem  $\binom{n}{k}$ , který čteme „ $n$  nad  $k$ “.

**Tvrzení**

Pro libovolná přirozená  $k, n \in N, k \leq n$  platí

$$C_n^k = \frac{n!}{k!(n-k)!}$$

Důkaz.

Z každé kombinace (neuspořádané  $k$ -tice) dostaneme  $k!$  různých variací (uspořádané  $k$ -tice) lišící se pouze pořadím prvků, tedy  $A_n^k = k! \cdot C_n^k$ , odtud je platnost tvrzení zřejmá.

**Tvrzení** - základní vlastnosti kombinačních čísel

Pro  $k, n \in N, k \leq n$  platí:

- $C_n^k = C_n^{n-k}$ , (symetrie)
- $C_n^k = C_{n-1}^{k-1} + C_{n-1}^k$ , (Pascalova identita)
- $C_n^k = P(k, n-k)$ ,
- $\sum_{k=0}^n C_n^k = 2^n$ .

Důkaz – kombinatorický.

Označme  $M = \{a_1, \dots, a_n\}$ .

- Každá kombinace  $k$ -té třídy z  $n$  prvků jednoznačně definuje doplňkovou kombinaci  $(n-k)$ -té třídy (zbylé prvky) a tedy jejich počty musí být stejné, tj.  $C_n^k = C_n^{n-k}$ .
- Množinu kombinací  $k$ -té třídy na  $M$  rozložíme na disjunktní množiny  $A_1, A_2$ , kde  $A_1$  tvoří všechny kombinace obsahující  $a_1$ ,  $A_2$  všechny ostatní. Zřejmě  $C_n^k = |A_1| + |A_2|$ . Pro počet kombinací v  $A_1$  platí  $|A_1| = C_{n-1}^{k-1}$  (kombinace obsahují  $a_1$ , ostatních  $(k-1)$  prvků vybíráme libovolně z  $(n-1)$  zbývajících). Počet kombinací v  $A_2$  je  $|A_2| = C_{n-1}^k$  (vybíráme  $k$  prvků z  $(n-1)$ , neboť nesmíme použít  $a_1$ ).
- Každé kombinaci  $k$ -té třídy z  $n$  prvků přiřadíme charakteristický vektor, tj. uspořádanou  $n$ -tici  $(x_1, \dots, x_n)$ , kde  $x_i = 1$ , pokud  $a_i$  je v dané kombinaci, resp.  $x_i = 0$ , pokud  $a_i$  není v dané kombinaci. Vztah mezi kombinacemi a jejich charakteristickými vektory, je vzájemně jednoznačný, proto jsou jejich počty stejné. Charakteristické vektory jsou permutace s opakováním z  $k$  prvků prvního druhu (1) a  $(n-k)$  prvků druhého druhu (0) a tudíž  $C_n^k = P(k, n-k)$ .
- Pravá strana rovnosti udává počet variací  $n$ -té třídy ze dvou prvků, např. 0,1. Množinu všech těchto variací rozložíme do  $(n+1)$  tříd  $A_0, \dots, A_n$ , kde  $A_i$  definujeme jako množinu všech variací obsahující právě  $i$  jedniček a  $(n-i)$  nul. Zřejmě platí  $|A_i| = P(i, n-i) = C_n^i$  a vzhledem k tomu, že množiny  $A_i$  jsou disjunktní po dvou, dostáváme  $2^n = |A_0| + \dots + |A_n|$ , což bylo třeba dokázat.



Uspořádejme nyní kombinační čísla do tzv. Pascalova trojúhelníku (schéma z následujícího obr.), jehož  $n$ -tý řádek obsahuje právě všechna kombinační čísla  $C_n^k, 0 \leq k \leq n$ .

$C_0^k$	...	1	$0 \leq k$						
$C_1^k$	...	1	1						
$C_2^k$	...	1	2	1					
$C_3^k$	...	1	3	3	1				
$C_4^k$	...	1	4	6	4	1			
$C_5^k$	...	1	5	10	10	5	1		
$C_6^k$	...	1	6	15	20	15	6	1	
$C_7^k$	...	1	7	21	35	35	21	7	1
		$0 \leq n$							

Vztah části a) předchozího tvrzení lze interpretovat jako symetrii řádků (tj.  $k$ -té číslo zleva se rovná  $k$ -tému číslu zprava). Vztah b) vyjadřuje skutečnost, že každé číslo ve schématu (které není „krajní“) je součtem dvou čísel z předcházejícího řádku umístěných v daném a předcházejícím sloupci. Vztah c) udává, že součet  $n$ -tého řádku je roven  $2^n$ .

Dále lze odhalit i kombinatoricky jinak méně evidentní zákonitosti, např. číslo z  $n$ -tého řádku a  $k$ -tého sloupce (který není „krajní“) je rovno součtu čísel na diagonále  $[n - 1, k] \rightarrow [n - k - 1, 0]$  (první číslo v dvojici určuje řádek a druhé sloupec). Platí tedy

$$C_n^k = C_{n-k-1}^0 + C_{n-k-2}^1 + \dots + C_{n-1}^k.$$

Pomocí Pascalovy identity lze dodefinovat hodnoty  $C_n^k$  pro  $k, n \in \mathbb{Z}$  (tzv. rozšířený, resp. zobecněný binomický koeficient), čímž dostáváme následující schéma, které se nazývá rozšířený Pascalův trojúhelník.

$C_{-7}^k$	...	0	0	1	-7	28	-84	210	-462	924	-1716
$C_{-6}^k$	...	0	0	1	-6	21	-56	126	-252	462	-792
$C_{-5}^k$	...	0	0	1	-5	15	-35	70	-126	210	-330
$C_{-4}^k$	...	0	0	1	-4	10	-20	35	-56	84	-120
$C_{-3}^k$	...	0	0	1	-3	6	-10	15	-21	28	-36
$C_{-2}^k$	...	0	0	1	-2	3	-4	5	-6	7	-8
$C_{-1}^k$	...	0	0	1	-1	1	-1	1	-1	1	-1
$C_0^k$	...	0	0	1	0	0	0	0	0	0	0
$C_1^k$	...	0	0	1	1	0	0	0	0	0	0
$C_2^k$	...	0	0	1	2	1	0	0	0	0	0
$C_3^k$	...	0	0	1	3	3	1	0	0	0	0
$C_4^k$	...	0	0	1	4	6	4	1	0	0	0
$C_5^k$	...	0	0	1	5	10	10	5	1	0	0
$C_6^k$	...	0	0	1	6	15	20	15	6	1	0
$C_7^k$	...	0	0	1	7	21	35	35	21	7	1
				$n$							

### Definice – rozšířené binomické koeficienty

Pro libovolná přirozená čísla  $k, n \in \mathbb{N}$  definujeme hodnoty rozšířených binomických koeficientů (kombinačních čísel) následovně:

- $C_n^k = \frac{n!}{(n-k)! \cdot k!}$  pro  $0 \leq k \leq n$ ,
- $C_n^k = 0$ , pro  $0 \leq n < k$ ,
- $C_{-n}^k = (-1)^k C_{n+k-1}^k$ , pro  $0 \leq k, 0 < n$ ,
- $C_n^{-k} = C_{-n}^{-k} = 0$ , pro  $0 < k, 0 \leq n$ .

Jak uvidíme později, odpovídá tato definice vlastnostem binomických koeficientů (kombinačních čísel) v kontextu jejich širšího využití.

### Definice - kombinace s opakování

Mějme k dispozici  $n$  různých druhů prvků, každý v libovolném množství. Kombinací  $k$ -té třídy z  $n$  prvků s opakováním ( $0 \leq k, n$ ) nazveme libovolnou neuspořádanou  $k$ -tici sestavenou z prvků uvedených druhů. Dvě kombinace s opakováním považujeme za různé, jestliže se liší v počtu zastoupení prvků některého druhu. Počet kombinací  $k$ -té třídy z  $n$  prvků s opakováním budeme značit  $\bar{C}_n^k$ .

### Tvrzení

Pro libovolná  $n, k \in \mathbb{N}$  platí

$$\bar{C}_n^k = C_{n+k-1}^k.$$

Důkaz.

Každou kombinaci  $k$ -té třídy z  $n$  prvků  $\{a_1, \dots, a_n\}$  s opakováním lze jednoznačně reprezentovat bitovým řetězcem délky  $(n + k - 1)$  obsahujícím  $k \times 1$  a  $(n - 1) \times 0$ . Prvky 0 tvoří oddělovače jednotlivých druhů a 1 zastupují prvky vyskytující se v kombinaci. Je zřejmé, že všem kombinacím  $k$ -té třídy z  $n$  prvků s opakováním odpovídají právě všechny permutace s opakováním z  $k \times 1$  a  $(n - 1) \times 0$ , tj.  $\bar{C}_n^k = P(k, n - 1) = C_{n+k-1}^k$ .

### Poznámka

Po definici pojmů variace, kombinace a permutace lze přistoupit k některým ukázkám jejich využití, např. ve statistické fyzice. Základní úlohou statistické fyziky je určit, jak se vzhledem ke svým vlastnostem rozdělují fyzikální částice. Předpokládejme, že zkoumaný systém obsahuje  $k$  částic a existuje  $n$  různých fázových stavů, ve kterých se tyto částice mohou vyskytovat. V závislosti na jejich vlastnostech dostáváme následující modely.

- a) Maxwell-Boltzmannův model - nachází uplatnění v klasické fyzice (např. kinetická teorie plynů) a předpokládá, že částice jsou vzájemně rozlišitelné a každá z nich se může se stejnou pravděpodobností vyskytovat v libovolném fázovém stavu. Pro počet možných rozdělení částic tak dostáváme  $\bar{A}_n^k = n^k$ .
- b) Bose-Einsteinův model.  
Tento model nachází uplatnění např. v kvantové fyzice a předpokládá, že částice (nazývané bosony) jsou vzájemně nerozlišitelné. Rozhodující je pouze počet částic v jednotlivých fázových stavech, proto počet možných rozdělení uvažovaných částic je  $\bar{C}_n^k$ .
- c) Fermi-Diracův model.  
Tento model nachází uplatnění v atomové fyzice a lze ho považovat za Bose-Einsteinův model omezený Pauliovým vylučovacím principem. Předpokládá, že každý fázový stav může obsahovat nejvýše jednu částici (nazývanou fermion). Pro počet možných rozdělení částic tak dostáváme  $C_n^k$ .

### 1.3. Základní kombinatorické identity

Kombinatorické úlohy lze řešit v zásadě třemi následujícími způsoby:

- Přímá metoda – spočívá ve vhodné úpravě výrazů a využití různých obecně platných vztahů. Bývá technicky velmi náročná a je rozumně využitelná pouze v jednoduchých případech.
- Kombinatorická metoda – založena na kombinatorických úvahách. Názorná, technicky velmi jednoduchá a prakticky využitelná i ve složitějších případech.
- Metody využívající vytvářející funkce, resp. rekurentní vztahy - obecné a velmi účinné metody, využitelné i ve složitých případech a důkazech. Těmto metodám se budeme věnovat v navazujících skriptech.

#### Tvrzení

Platí

a)  $\sum_{k=0}^n (-1)^k C_n^k = 0,$

b)  $C_{n+k}^{n+1} = \sum_{i=0}^{k-1} C_{n+i}^n,$

c)  $C_{m+n}^k = \sum_{i=0}^k C_m^i C_n^{k-i}, k \leq \min\{m, n\}$  (Vandermondeova identita).

Důkaz.

ad a) Uvedený vztah je zřejmě ekvivalentní s tvrzením, že počet všech kombinací sudého řádu z  $n$  prvků  $\{a_1, \dots, a_n\}$  je roven počtu kombinací lichého řádu. Zvolme libovolně jeden prvek, např.  $a_1$ , a následně provedme proceduru, při které ze všech kombinací obsahujících prvek  $a_1$  tento prvek odebereme a naopak do kombinací, které ho původně neobsahovaly, tento prvek přidáme. Je zřejmé, že opět dostaneme všechny kombinace  $k$ -té třídy z  $n$  prvků, navíc všechny kombinace lichého řádu přejdou na kombinace sudého řádu a opačně (ve všech kombinacích změníme počet prvků o jeden).

ad b) Množinu všech kombinací  $(k-1)$ . třídy z  $(n+2)$  prvků  $\{a_1, \dots, a_{n+2}\}$  s opakováním rozložíme do  $k$  tříd  $A_0, \dots, A_{k-1}$ , kde  $A_i$  je třída obsahující všechny kombinace  $(k-1)$ . třídy s opakováním, ve kterých se vyskytuje prvek  $a_i$  právě  $i$ -krát. Zřejmě tak platí

$$\bar{C}_{n+2}^{k-1} = \bar{C}_{n+1}^{k-1} + \bar{C}_{n+1}^{k-2} + \dots + \bar{C}_{n+1}^1 + \bar{C}_{n+1}^0.$$

Využitím vztahu pro výpočet kombinací s opakováním pomocí kombinací bez opakování dostáváme dokazované tvrzení.

ad c) Množinu všech kombinací  $k$ -té třídy z  $(m+n)$  prvků  $\{a_1, \dots, a_m\} \cup \{b_1, \dots, b_n\}$  rozložíme podle počtu prvků z množiny  $\{a_1, \dots, a_m\}$  do  $(k+1)$  tříd  $A_0, \dots, A_k$ , kde  $A_i$  je třída obsahující všechny kombinace, ve kterých je právě  $i$  prvků z množiny  $\{a_1, \dots, a_m\}$  a  $(k-i)$  prvků z množiny  $\{b_1, \dots, b_n\}$ . Zřejmě platí  $C_{m+n}^k = \sum_{i=0}^k |A_i|$ , kde  $|A_i| = C_m^i C_n^{k-i}$ .

Výše uvedené identity nachází využití při řešení celé řady různých úloh. Jako příklad uvedeme vztahy pro výpočet součtů mocnin přirozených čísel.

- Ve vztahu b) položíme  $n = 1$ . Dostáváme tak  $C_1^1 + C_2^1 + \dots + C_k^1 = C_{k+1}^2$ . Odtud

$$1 + 2 + \dots + k = \frac{k(k+1)}{2}.$$

(Součet lze stanovit i jednodušší úvahou, kterou použil C. F. Gauss. Návod – sčítejte vhodné dvojice čísel.)

- Pro výpočet součtu druhých mocnin využijeme opět vztah b), kde položíme  $n = 2$ . Dostáváme tak  $C_2^2 + C_3^2 + \dots + C_{k+1}^2 = C_{k+2}^3$  a po rozepsání

$$1 \cdot 2 + 2 \cdot 3 + \dots + k(k+1) = \sum_{i=1}^k i + \sum_{i=1}^k i^2 = \frac{k(k+1)(k+2)}{3}.$$

Pro součet druhých mocnin tak dostáváme

$$1^2 + \dots + k^2 = \frac{k(k+1)(2k+1)}{6}.$$

Analogicky lze pokračovat i v případě výpočtu součtu vyšších mocnin (volíme  $n = 3, \dots$ ).

## Tvrzení

Platí

$$a) P(k_1, k_2, \dots, k_r) = C_n^{k_1} \cdot C_{n-k_1}^{k_2} \cdot \dots \cdot C_{n-k_1-\dots-k_{r-2}}^{k_{r-1}}$$

$$b) \sum_{k_1+\dots+k_r=n} P(k_1, k_2, \dots, k_r) = r^n.$$

kde se sčítá přes všechny uspořádané  $r$ -tice  $(k_1, \dots, k_r)$  přirozených čísel, jejichž součet je roven  $n$  (tj. přes všechny rozklady čísla  $n$  na  $r$  sčítanců, na jejichž pořadí záleží).

Důkaz.

ad a) Všechny permutace s opakováním z  $k_1$  prvků 1. druhu,  $k_2$  prvků 2. druhu, ...,  $k_r$  prvků  $r$ -tého druhu lze sestavit následovně. Nejprve vybereme  $k_1$  míst pro prvky 1. druhu, což lze provést  $C_n^{k_1}$  různými způsoby (všechny pozice jsou zatím volné). Následně vybereme  $k_2$  míst pro prvky 2. druhu. Tato místa již vybíráme z  $(n - k_1)$  volných pozic, tj.  $C_{n-k_1}^{k_2}$  způsoby. Analogicky postupujeme i v případě prvků ostatních druhů. Aplikací pravidla součinu pak dostáváme dokazovaný vztah.

ad b) Pravá strana b) je zřejmě rovna počtu všech variací  $n$ -té třídy s opakováním z  $r$  prvků  $\{a_1, \dots, a_r\}$ . Všechny zmíněné variace lze rozložit podle počtu prvků jednotlivých druhů do tříd. Počet tříd je zřejmě roven počtu uspořádaných  $r$ -tic přirozených čísel  $(k_1, \dots, k_r)$ , kde  $k_1 + \dots + k_r = n$  a v každé takové třídě je  $P(k_1, \dots, k_r)$  variací.

Pro potřeby počítačového modelování je třeba mít k dispozici algoritmy, které umožní efektivně a systematicky (tj. v jasně definovaném pořadí) generovat permutace, kombinace, resp. variace. Závěrečná část této kapitoly je věnována právě této problematice.

## Definice - lexikografické uspořádání

Nechť  $A = \{a_1, \dots, a_n\}$  je uspořádaná abeceda, kde  $a_1 < a_2 < \dots < a_n$ . Potom uspořádání  $\leq$  na množině  $A^*$  konečných slov nad  $A$  definované pro  $\mathbf{x}, \mathbf{y} \in A^*$ , kde  $\mathbf{x} = x_1 \dots x_m, \mathbf{y} = y_1 \dots y_k$  vztahy:

$$i) \mathbf{x} = \mathbf{y} \leftrightarrow (m = k) \wedge [\forall i \in \{1, \dots, m\} (x_i = y_i)],$$

$$ii) \mathbf{x} < \mathbf{y} \leftrightarrow (x_1 < y_1) \vee$$

$$[\exists l \in \{2, \dots, \min\{m, k\}\} (x_1 = y_1, \dots, x_{l-1} = y_{l-1}) \wedge (x_l < y_l)] \vee$$

$$[(m < k) \wedge (\forall i \in \{1, \dots, m\} x_i = y_i)]$$

nazýváme lexikografické uspořádání na  $A^*$ .

Lexikografické uspořádání je uspořádání, které odpovídá běžnému řazení slov ve slovníku. Právě v tomto pořadí bude následující algoritmus generovat permutace na množině  $\{1, 2, \dots, n\}$ .

## Algoritmus generování permutací řádu $n$ v lexikografickém pořadí

$(x_1, x_2, \dots, x_n) := (1, 2, \dots, n)$ ; (\* generování startuje od nejmenší (lexikograficky) permutace \*)

while  $(x_1, x_2, \dots, x_n) \neq (n, \dots, 2, 1)$  do

$k := \max_{1 \leq i \leq n-1} \{i \mid x_i < x_{i+1}\}$ ; (\* v aktuální permutaci určí poslední pozici následovanou větším prvkem \*)

$x'_1 := x_1; \dots; x'_{k-1} := x_{k-1}$ ; (\* prvky na pozicích  $1, \dots, k-1$  se v nově generované permutaci nemění \*)

$x'_k := \min_{k+1 \leq i \leq n} \{x_i \mid x_i > x_k\}$ ; (\* v nově generované permutaci umístí na  $k$ -tou pozici nejmenší prvek

aktuální permutace, který je větší než  $x_k$  a který následuje za  $k$ -tou pozici \*)

$(x'_{k+1}, \dots, x'_n) :=$  „zbývající prvky seřazené vzestupně“;

$(x_1, x_2, \dots, x_n) := (x'_1, x'_2, \dots, x'_n)$ ; print  $(x_1, x_2, \dots, x_n)$ ;

wend;

### Příklad

- Vygenerujte prvních třináct (v lexikografickém uspořádání) permutací na množině  $\{1,2,3,4\}$ :  
(1,2,3,4) → (1,2,4,3) → (1,3,2,4) → (1,3,4,2) → (1,4,2,3) → (1,4,3,2) → (2,1,3,4) → (2,1,4,3) → (2,3,1,4) → (2,3,4,1) → (2,4,1,3) → (2,4,3,1) → (3,1,2,4) → ...  
(tučně označený prvek odpovídá pozici  $k$ )
- Vygenerujte dvě bezprostředně po sobě jdoucí permutace (v lexikografickém uspořádání) následující permutaci (3,1,4,2,7,6,5):  
(3,1,4,2,7,6,5) → (3,1,4,5,2,6,7) → (3,1,4,5,2,7,6)

Při generování kombinací je třeba vzít v úvahu skutečnost, že kombinace je množina, tj. nezáleží na pořadí prvků a proto nelze použít lexikografické uspořádání. Budeme je proto generovat v pořadí definovaném následujícím uspořádáním.

Pro libovolné konečné číselné množiny  $A, B$  definujeme:  $A < B \leftrightarrow \min\{(A \cup B) - (A \cap B)\} \in A$ .

(např. pro  $A = \{6,3,2,5,7,8\}, B = \{7,3,2,4,8\}$  platí  $B < A$ )

### Algoritmus generování kombinací řádu $k$ na množině $\{1, 2, \dots, n\}$

(přesto, že jsou kombinace neuspořádané  $k$ -tice, budeme je zapisovat jako uspořádané  $k$ -tice, tj. do okrouhlých závorek)

$(x_1, \dots, x_k) := (1, \dots, k)$ ; (\* generování startuje od nejmenší kombinace, dle výše definovaného uspořádání \*)

while  $(x_1, \dots, x_k) \neq (n - k + 1, \dots, n)$  do

$m := \max_{1 \leq i \leq k} \{i \mid \exists j \notin (x_1, \dots, x_k) \wedge (j > x_i)\}$ ; (\* v aktuální permutaci určí poslední pozici  $i \in \{1, \dots, k\}$  s vlastností - existuje prvek větší než  $x_i$ , který není v aktuální kombinaci \*)

$x'_1 := x_1; \dots; x'_{m-1} := x_{m-1}$ ; (\* prvky na pozicích  $1, \dots, m - 1$  se v nově generované kombinaci nemění \*)

$x'_{m+i} := x_m + (i + 1), i = 0, 1, \dots, k - m$ ; (\* obsazení zbývajících pozic v nově generované kombinaci \*)

$(x_1, \dots, x_k) := (x'_1, \dots, x'_k)$ ; print( $x_1, \dots, x_k$ );

wend;

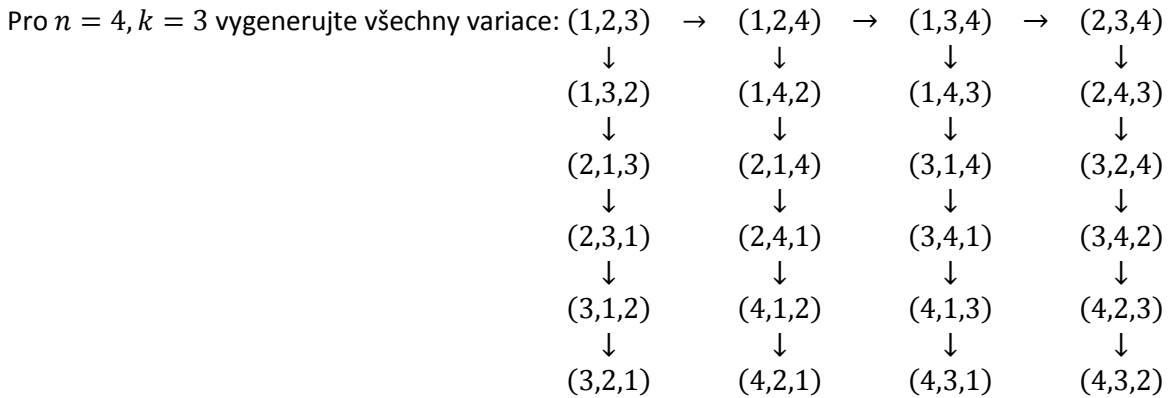
### Příklad

- Pro  $n = 5, k = 3$  vygenerujte všechny kombinace:  
(1,2,3) → (1,2,4) → (1,2,5) → (1,3,4) → (1,3,5) → (1,4,5) → (2,3,4) → (2,3,5) → (2,4,5) → (3,4,5)
- Pro  $n = 8, k = 5$  vygenerujte dvě kombinace bezprostředně následující kombinaci (1,2,4,7,8):  
(1,2,4,7,8) → (1,2,5,6,7) → (1,2,5,6,8)

### Algoritmus generování variací řádu $k$ na množině $\{1, 2, \dots, n\}$

Při generování variací  $k$ -té třídy z  $n$  prvků postupujeme následovně - postupně generujeme kombinace  $k$ -té třídy z  $n$  prvků a pro každou kombinaci vygenerujeme všechny její permutace. Popsaný způsob negeneruje variace v lexikografickém pořadí, nicméně jde o generování variací v jasně definovaném pořadí.

### Příklad



## 1.4. Subfaktoriály, Catalanova čísla

V následující části odstavce se budeme věnovat několika kombinatorickým úlohám s omezujícími podmínkami. Při jejich řešení budou využívány postupy, které mají obecný charakter a jsou významné pro řešení celé řady dalších úloh.

### Tvrzení

a) Označme  $D(n)$  počet permutací řádu  $n$ , ve kterých nezůstává žádný prvek na svém místě. Potom platí

$$D(n) = n! \left[ 1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \dots + (-1)^n \frac{1}{n!} \right].$$

b) Označme  $D_k(n)$  počet permutací řádu  $n$ , ve kterých právě  $k$  ( $0 \leq k \leq n$ ) prvků, zůstává na svém místě. Potom platí

$$D_k(n) = C_n^k D(n-k).$$

Důkaz.

ad a) Označme  $N(\alpha_{i_1}, \dots, \alpha_{i_k})$  počet permutací, ve kterých prvky  $\alpha_{i_1}, \dots, \alpha_{i_k}$  zůstávají na svém místě a  $N(\bar{\alpha}_1, \dots, \bar{\alpha}_n)$  počet permutací, kdy žádný prvek nezůstává na svém místě. Aplikací principu IE dostáváme

$$D(n) = N(\bar{\alpha}_1, \dots, \bar{\alpha}_n) = N - [\sum_{1 \leq i \leq n} N(\alpha_i)] + [\sum_{1 \leq i_1 < i_2 \leq n} N(\alpha_{i_1}, \alpha_{i_2})] + \dots \\ \dots + (-1)^k [\sum_{1 \leq i_1 < \dots < i_k \leq n} N(\alpha_{i_1}, \dots, \alpha_{i_k})] + \dots + (-1)^n N(\alpha_1, \alpha_2, \dots, \alpha_n)$$

Pro jednotlivé počty permutací zřejmě platí:

- |   |   |
|---|---|
| $N = n!$  | ... celkový počet permutací řádu $n$ ,  |
| $N(\alpha_i) = (n-1)!$                          | ... počet permutací, ve kterých zůstává prvek $\alpha_i$ na svém místě, zbývajících $(n-1)$ prvků lze umístit libovolně,                        |
| $N(\alpha_{i_1}, \alpha_{i_2}) = (n-2)!$        | ... počet permutací, ve kterých prvky $\alpha_{i_1}, \alpha_{i_2}$ zůstávají na svém místě, zbývajících $(n-2)$ prvků lze umístit libovolně,    |
| $N(\alpha_{i_1}, \dots, \alpha_{i_k}) = (n-k)!$ | ... počet permutací, ve kterých $k$ prvků $\alpha_{i_1}, \dots, \alpha_{i_k}$ zůstává na svém místě, zbývajících $(n-k)$ lze umístit libovolně, |
| $N(\alpha_1, \alpha_2, \dots, \alpha_n) = 0!$   | ... počet permutací, kde zůstávají všechny prvky na svém místě.   |

Odtud

$$D(n) = n! - C_n^1(n-1)! + C_n^2(n-2)! + \dots + C_n^k(n-k)! + \dots + C_n^n 0!$$

a po snadné úpravě

$$D(n) = n! \left[ 1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \dots + (-1)^n \frac{1}{n!} \right].$$

ad b) Prvky (v počtu  $k$ ), které zůstávají na svém místě lze vybrat  $C_n^k$  způsoby, zbývajících  $(n - k)$  prvků je možné umístit  $D(n - k)$  způsoby tak, že nejsou na svém místě. Aplikací pravidla součinu pak dostáváme dokazovaný vztah.

Pozorný čtenář si jistě uvědomí, že hranatá závorka ve vztahu pro  $D(n)$  obsahuje prvních  $(n + 1)$  členů rozvoje  $e^{-1}$ . Jelikož řada uvedená v závorce konverguje rychle, lze pro  $n \geq 2$  použít k výpočtům vztah

$$D(n) = \text{round}\left(\frac{n!}{e}\right),$$

kde  $\text{round}(\quad)$  je funkce zaokrouhlení.

### Definice - subfaktoriály

Čísla  $D(n)$ ,  $n \in \mathbb{N}$  definovaná ve výše uvedeném tvrzení nazýváme subfaktoriálem (řádu  $n$ ).

Jak vyplývá z níže uvedeného tvrzení, mají subfaktoriály  $D(n)$  mnohé vlastnosti podobné faktoriálům  $P(n)$ .

### Tvrzení

Platí:

- $D(n) = (n - 1)[D(n - 1) + D(n - 2)]$ , kde  $D(0) = 1, D(1) = 0$ ,
- $D(n) = nD(n - 1) + (-1)^n$ , kde  $D(0) = 1$ ,
- $P(n) = \sum_{k=0}^n C_n^k D(n - k)$ .

Důkaz.

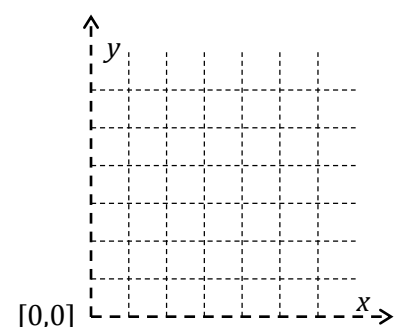
- ad a) Označme  $A$  množinu všech permutací na  $\{a_1, \dots, a_n\}$ , ve kterých nezůstává žádný prvek na svém místě. Tuto množinu lze rozložit do  $(n - 1)$  tříd  $A_2, \dots, A_n$ , kde  $A_i$  obsahuje právě všechny permutace z  $A$ , které mají na první pozici prvek  $a_i$ . Vzhledem k tomu, že všechny třídy mají stejný počet prvků (důsledek „symetrie“), pro libovolné  $i$  platí  $D(n) = (n - 1)|A_i|$ . Nyní stačí určit počet permutací, např. ve třídě  $A_2$ . Třidu  $A_2$  rozložíme na dvě podmnožiny  $A_2^0, A_2^1$ , kde  $A_2^0$  obsahuje všechny permutace z  $A_2$ , ve kterých je na druhé pozici  $a_1$  a na zbývajících  $(n - 2)$  pozicích není žádný prvek na svém místě. Odtud  $|A_2^0| = D(n - 2)$ . Podmnožina  $A_2^1$  obsahuje všechny zbývající permutace z  $A_2$  (na první pozici je  $a_2$ , na druhé není  $a_1$  a na zbývajících pozicích není žádný prvek na svém místě). Odtud  $|A_2^1| = D(n - 1)$  a tedy platnost dokazovaného tvrzení je zřejmá.
- ad b) Označme  $h_n = D(n) - nD(n - 1)$ . Snadnou úpravou (dosazením do a)) dostáváme  $h_n = (-1)h_{n-1}$ , tedy  $h_n = (-1)^{n-2}h_2$ , kde  $h_2 = D(2) - 2D(1) = 1$ . Odtud  $D(n) - nD(n - 1) = (-1)^n$  a po zřejmé úpravě dostáváme dokazovaný vztah.
- ad c) Množinu všech permutací řádu  $n$  lze rozložit do  $(n + 1)$  tříd  $A_0, \dots, A_n$ , kde  $A_i$  obsahuje všechny permutace, kde zůstává právě  $i$  prvků na svém místě. Odtud s ohledem na předchozí tvrzení dostáváme  $P(n) = \sum_{k=0}^n D_k(n) = \sum_{k=0}^n C_n^k D(n - k)$ .

### Příklad

Uvažujme rovinnou síť znázorněnou na sousedním obrázku a předpokládejme, že pohyb v síti je realizován pouze pomocí dvou typů tahů  $[x, y] \rightarrow [x + 1, y]$  a  $[x, y] \rightarrow [x, y + 1]$ . Spočítejte, kolik existuje různých cest z bodu  $[0, 0]$  do bodu  $[m, n]$ .

Řešení.

Pro potřeby důkazu označme tah  $[x, y] \rightarrow [x + 1, y]$  symbolem 0 a tah typu  $[x, y] \rightarrow [x, y + 1]$  symbolem 1. Nyní je zřejmé, že každé cestě (používající pouze tahy typu 0 a 1) lze jednoznačně přiřadit bitový řetězec



délky  $(m + n)$ , který obsahuje právě  $m$  nul a  $n$  jedniček. Naopak, každý bitový řetězec obsahující  $m$  nul a  $n$  jedniček definuje jedinou cestu z bodu  $[0,0]$  do bodu  $[m, n]$  a proto počet uvažovaných cest je roven počtu všech permutací s opakováním, které se skládají z  $m$  nul a  $n$  jedniček, tj.  $P(m, n) = C_{m+n}^m$ .

### Příklad

Uvažujme rovinnou síť z předcházejícího příkladu, ve které se pohybujeme pomocí stejných typů kroků, tj.  $0: [x, y] \rightarrow [x + 1, y]$  a  $1: [x, y] \rightarrow [x, y + 1]$ . Spočítejte, kolik existuje různých cest z bodu  $[0,0]$  do bodu  $[n, n]$ , které nepřekročí diagonálu.

(Diagonálu tvoří body  $[x, y]$ , pro které  $x = y$ , tj. nepřekročíme diagonálu, pokud pro souřadnice  $[x, y]$  všech bodů cesty platí  $x \geq y$ ).

Řešení.

Hledaný počet povolených cest (nepřekročí diagonálu a vedou z  $[0,0]$  do  $[n, n]$ ) označíme  $C_n$  a určíme ho jako doplněk počtu zakázaných cest  $Z_n$  (cesta překročí diagonálu). Platí proto  $C_n = C_{2n}^n - Z_n$ . Počet  $Z_n$  určíme následující kombinatorickou úvahou. Označme  $a_1, \dots, a_k, \dots, a_{2n}$  bitový řetězec reprezentující zakázanou cestu a  $k$  index, kde cesta prvně překročí diagonálu. V tomto okamžiku je poprvé počet jedniček v prefixu  $a_1, \dots, a_k$  o jedničku větší než počet nul (číslo  $k$  je proto liché). V této chvíli přidejme na začátek uvažovaného bitového řetězce 0. Tím dostáváme bitový řetězec  $0, a_1, \dots, a_k, \dots, a_{2n}$ , který má v prefixu  $0, a_1, \dots, a_k$  stejný počet 1 i 0. Dále v uvažovaném prefixu zaměňme 0 a 1. Dostáváme tak bitový řetězec  $1, \bar{a}_1, \dots, \bar{a}_k, a_{k+1}, \dots, a_{2n}$ , kde  $\bar{a}_i = 0$ , jestliže  $a_i = 1$  a  $\bar{a}_i = 1$  v ostatních případech. Tento nový bitový řetězec začíná 1, obsahuje  $(n + 1)$  nul a  $n$  jedniček. Snadno nahlédneme, že každé zakázané cestě lze takto jednoznačně přiřadit bitový řetězec uvedených vlastností (dvěma různými zakázaným cestám zřejmě odpovídají i různé bitové řetězce). Nyní je podstatné si uvědomit, že každý bitový řetězec  $b_0, b_1, \dots, b_k, \dots, b_{2n}$  uvedených vlastností (tj. začíná 1, obsahující  $(n + 1)$  nul a  $n$  jedniček) definuje zakázanou cestu, kterou lze zkonstruovat následovně. Necht  $k$  označuje pozici, kde se poprvé vyrovná počet 1 a 0 (tato situace musí nutně nastat - zdůvodněte). Nyní v prefixu  $b_0, b_1, \dots, b_k$  zaměňme 0 a 1 a odstraníme úvodní 0. Získáme tak bitový řetězec  $\bar{b}_1, \dots, \bar{b}_k, b_{k+1}, \dots, b_{2n}$ , který reprezentuje zakázanou cestu (poprvé překročí diagonálu na pozici  $k$ ). Tím jsme také dokázali, že počet zakázaných cest je roven počtu bitových řetězců délky  $(2n + 1)$ , které začínají 1, obsahují  $(n + 1)$  nul a  $n$  jedniček, tj.  $Z_n = P(n - 1, n + 1) = C_{2n}^{n-1}$ . Pro počet povolených cest tak dostáváme  $C_n = C_{2n}^n - C_{2n}^{n-1} = \frac{1}{n+1} C_{2n}^n$ .

### Definice - Catalanova posloupnost

Catalanovou posloupností budeme nazývat posloupnost  $\{C_n\}_{n=0}^{\infty}$ , kde

$$C_n = \frac{1}{n+1} C_{2n}^n$$

a její členy budeme nazývat Catalanovými čísly.

### Poznámky

Catalanova posloupnost patří mezi „prominentní“ kombinatorické posloupnosti a je řešením celé řady úloh.

- Snadno nahlédneme, že počet způsobů jak správně uzavřít součin  $x_0 \cdot x_1 \cdot \dots \cdot x_n$  je roven  $C_n$ . (Řádně zdůvodněte. Návod - každou levou závorku reprezentujte symbolem 0 a pravou symbolem 1.)

Speciálně pro  $n = 3$  dostáváme  $C_3 = 5$  následujících možností:

$$\begin{array}{ccc} ((x_0 \cdot x_1) \cdot x_2) \cdot x_3 & (x_0 \cdot x_1) \cdot (x_2 \cdot x_3) & ((x_0 \cdot (x_1 \cdot x_2)) \cdot x_3) \\ (x_0 \cdot ((x_1 \cdot x_2) \cdot x_3)) & (x_0 \cdot (x_1 \cdot (x_2 \cdot x_3))) & \end{array}$$

- Počet permutací řádu  $n$ , které lze realizovat pomocí zásobníku (do zásobníku jsou postupně vkládána čísla  $1, 2, \dots, n$  a mohou být kdykoliv vybírána), je roven  $C_n$ . (Řádně zdůvodněte. Návod - každou operaci PUSH reprezentujte symbolem 0 a POP symbolem 1.)



## 1.5. Binomická a multinomická věta, Newtonův vzorec

Velmi důležitou „kombinatorickou identitou“ je známá binomická věta a její zobecnění ve formě multinomické věty a Newtonova vzorce.

**Tvrzení** - binomická a multinomická věta

a) Binomická věta - pro libovolná reálná  $x, y$  a přirozené  $n$  platí

$$(x + y)^n = \sum_{i=0}^n C_n^i x^i y^{n-i}.$$

b) Multinomická věta - pro libovolná reálná  $x_1, \dots, x_r$  a přirozené  $n$  platí

$$(x_1 + \dots + x_r)^n = \sum_{n_1 + \dots + n_r = n} P(n_1, \dots, n_r) \cdot x_1^{n_1} \cdot \dots \cdot x_r^{n_r},$$

kde součet se provádí přes všechny uspořádané  $r$ -tice přirozených čísel  $(n_1, \dots, n_r)$ , jejichž součet je roven  $n$ , tj.  $n_1 + \dots + n_r = n$ .

Důkaz.

ad a) Roznásobením výrazu  $\underbrace{(x + y)}_{1. \text{ člen}} \cdot \underbrace{(x + y)}_{2. \text{ člen}} \cdot \dots \cdot \underbrace{(x + y)}_{n. \text{ člen}}$  dostaneme  $2^n$  členů obsahujících  $n$  symbolů (z každé závorky právě jeden) a tvořící zřejmě všechny variace  $n$ -té třídy s opakováním ze dvou prvků  $x, y$ . Dále je evidentní, že počet členů ve kterých se vyskytuje  $i$ -krát symbol  $x$  a  $(n - i)$ -krát symbol  $y$  je roven  $P(i, n - i)$ . Po jejich sloučení dostáváme jako koeficient u  $x^i y^{n-i}$  právě  $P(i, n - i) = C_n^i$ .

ad b) Zcela analogický k části a).

Roznásobením výrazu  $\underbrace{(x_1 + \dots + x_r)}_{1. \text{ člen}} \cdot \underbrace{(x_1 + \dots + x_r)}_{2. \text{ člen}} \cdot \dots \cdot \underbrace{(x_1 + \dots + x_r)}_{n. \text{ člen}}$  dostáváme všechny variace  $n$ -té třídy s opakováním z  $r$  prvků  $x_1, \dots, x_r$ . Po sloučení členů se stejnými mocninami dostáváme jako koeficient u  $x_1^{n_1} \cdot \dots \cdot x_r^{n_r}$  počet permutací s opakováním řádu  $(n_1, \dots, n_r)$ , tj.  $P(n_1, \dots, n_r)$ .

### Příklad

Uvažujte rozvinutý tvar výrazu  $(2x - \frac{\sqrt{y}}{3})^{10}$ . Určete koeficient: i) u členu  $x^4 y^3$ , ii) u členu  $(xy)^5$ , iii) u členu obsahujícího  $x^3$ .

Řešení.

ad i) Z binomické věty plyne, že člen obsahující  $x^4 y^3$  má tvar  $C_{10}^4 (2x)^4 \left(-\frac{\sqrt{y}}{3}\right)^6$  a tedy hledaný koeficient je

$$C_{10}^4 \cdot 2^4 \cdot \left(\frac{-1}{3}\right)^6 = \frac{1120}{243} \doteq 4,60905.$$

ad ii) Uvedený člen se v rozvoji nevyskytuje, tedy koeficient je roven 0.

ad iii) V rozvoji daného výrazu existuje jediný člen obsahující  $x^3$ , který má tvar  $x^3 y^3 \sqrt{y}$ . Snadno tak

$$\text{dopočteme, že hledaný koeficient je } C_{10}^3 \cdot 2^3 \cdot \left(\frac{-1}{3}\right)^7 = -\frac{320}{729} \doteq -0,43896.$$

### Příklad

Uvažujte rozvinutý tvar výrazu  $(5x + (2y)^2 - 3\sqrt{u})^6$ .

Určete: a) koeficient u členu  $xy^2 u^2$ , b) součet koeficientů u členů obsahujících  $y^8$ .

Řešení.

$$\text{ad a) } P(1,1,4) \cdot 5 \cdot 2^2 \cdot (-3)^4 = 48\,600$$

$$\left. \begin{array}{l} \text{ad b) } P(2,4,0) \cdot 5^2 \cdot (2^2)^4 = 96000 \\ P(1,4,1) \cdot 5 \cdot (2^2)^4 \cdot (-3) = -115200 \\ P(0,4,2) \cdot (2^2)^4 \cdot (-3)^2 = 34560 \end{array} \right\} \rightarrow 15360$$

### Poznámka

Binomická a multinomická věta (jak uvidíme později, jde o vytvořující funkce) má velmi široké možnosti využití, např. jako účinný nástroj při řešení celé řady méně triviálních úloh. Pro ilustraci uvedeme důkazy vztahů a), c) z prvního tvrzení odstavce 1.3.

ad a) Dosazením  $x = -1, y = 1$  do binomické věty dostáváme

$$0 = (-1 + 1)^n = \sum_{i=0}^n C_n^i \cdot (-1)^i \cdot 1^{n-i} = \sum_{i=0}^n (-1)^i C_n^i.$$

ad c) Aplikací binomické věty na zřejmou identitu  $(1+x)^{m+n} = (1+x)^m(1+x)^n$  dostáváme

$$\sum_{i=0}^{m+n} C_{m+n}^i \cdot x^i = \left(\sum_{i=0}^m C_m^i \cdot x^i\right) \left(\sum_{j=0}^n C_n^j \cdot x^j\right).$$

Porovnáním koeficientů u  $x^k$  na obou stranách dostáváme  $C_{m+n}^k = \sum_{i=0}^k C_m^i C_n^{k-i}, k \leq \min\{m, n\}$ .

Binomická věta je speciálním případem následujícího tvrzení, které bývá označované jako Newtonův vzorec.

### Tvrzení - Newtonův vzorec

Pro libovolná  $x, \alpha \in R, |x| < 1$  platí

$$(1+x)^\alpha = 1 + \alpha x + \frac{\alpha(\alpha-1)}{2!} x^2 + \dots + \frac{\alpha(\alpha-1) \cdot \dots \cdot (\alpha-k+1)}{k!} x^k + \dots$$

Snadno ověříme, že pro  $\alpha = n \in N$  je koeficient u  $x^k$  roven právě binomickému koeficientu  $C_n^k$  (koeficienty všech členů  $x^k, k > n$  jsou nulové, tudíž dostáváme binomickou větu). V případě, kdy exponent je záporné celé číslo, budeme psát  $\alpha = -n$ , kde  $n \in N^+$  a (1.27) má tvar

$$(1+x)^{-n} = 1 - C_n^1 x + C_{n+1}^2 x^2 + \dots + (-1)^k C_{n+k-1}^k x^k + \dots$$

Koeficient u  $x^k$  je tedy roven  $C_{-n}^k$ , což plně odpovídá již dříve uvedené definici rozšířených binomických koeficientů.

### Příklad

Uvažujte rozvoj výrazu  $\sqrt[3]{(5-4x^3)^2}$ . Určete: a) koeficient u  $x^{12}$ , b) koeficient u  $x^{13}$ .

Řešení.

$$\text{Zřejmě } \sqrt[3]{(5-4x^3)^2} = 5^{2/3} \left(1 - \frac{4}{5} x^3\right)^{2/3}$$

ad a) Využitím Newtonova vzorce dostáváme ( $\alpha = 2/3$ ) pro hledaný koeficient

$$5^{2/3} \cdot \frac{\binom{2/3}{4} \cdot \binom{2/3-1}{3} \cdot \binom{2/3-2}{3} \cdot \binom{2/3-3}{3}}{4!} \cdot \left(-\frac{4}{5}\right)^4 = -\frac{1792}{30375\sqrt[3]{5}} \doteq -0,0345$$

ad b) Uvedený člen se v rozvoji nevyskytuje, tedy koeficient je roven 0.

## 2. Rozklady

Základní úlohu z oblasti rozkladů lze formulovat následovně – určete počet rozkladů dané konečné množiny. V závislosti na „omezujících“ podmínkách, např. prvky množiny (alternativně označované také jako objekty) jsou (ne)rozdílitelné, třídy rozkladu považujeme za (ne)rozdílitelné, (ne)zadán počet tříd rozkladu, omezení počtu prvků v jednotlivých třídách apod., dostáváme následující základní typy rozkladových úloh.

### 2.1. Rozklady nerozlišitelných objektů do rozlišitelných tříd

Úloha - určete počet rozkladů množiny obsahující  $n$  nerozlišitelných objektů do rozlišitelných tříd.

#### Tvrzení

- a) Počet rozkladů množiny obsahující  $n$  nerozlišitelných objektů do  $k$  rozlišitelných tříd, jestliže připouštíme i prázdné třídy rozkladu, je roven počtu řešení diofantické rovnice

$$x_1 + \dots + x_k = n,$$

kteřá vyhovují podmínkám  $\forall i x_i \in N$ .

- b) Počet řešení výše uvedené rovnice je roven  $P(n, k - 1) = C_{n+k-1}^{k-1}$ .

Důkaz.

ad a) Zřejmé, pokud  $x_i$  interpretujeme jako počet objektů v  $i$ -té třídě rozkladu.

ad b) Každý rozklad lze jednoznačně reprezentovat bitovým řetězcem délky  $n + k - 1$ , který obsahuje  $(k - 1)$  bitů nastavených na 0 (tvoří oddělovače pro  $k$  tříd rozkladu) a  $n$  bitů nastavených na 1, kde každá 1 zastupuje právě jeden objekt v dané třídě rozkladu.

Další variantou této úlohy je situace, kdy předepíšeme minimální počty objektu v jednotlivých třídách. V tomto případě platí následující tvrzení.

#### Tvrzení

- a) Počet rozkladů množiny obsahující  $n$  nerozlišitelných objektů do  $k$  rozlišitelných tříd, jestliže požadujeme, aby  $i$ -tá třída ( $1 \leq i \leq k$ ) rozkladu obsahovala alespoň  $a_i$  objektů, je roven počtu celočíselných řešení diofantické rovnice

$$x_1 + \dots + x_k = n,$$

kteřá vyhovují podmínkám  $\forall i 0 \leq a_i \leq x_i$ .

- b) Počet řešení výše uvedené rovnice je roven  $P(n - \sum_{i=1}^k a_i, k - 1) = C_{n+k-1-\sum_{i=1}^k a_i}^{k-1}$ .

Důkaz.

Analogicky k důkazu předchozího tvrzení interpretujeme  $(k - 1)$  nulových bitů jako oddělovače  $k$  tříd, které nejprve „naplníme“ povinným minimálním počtem objektů  $a_i$ . Následně rozdělíme zbývajících  $n - \sum_{i=1}^k a_i$  objektů (reprezentované 1) libovolně do  $k$  tříd.

Obecnou variantou předchozích úloh je situace, kdy zadáme dolní i horní omezení počtu objektů v jednotlivých třídách rozkladu. V tomto případě hledáme počet celočíselných řešení diofantické rovnice

$$x_1 + \dots + x_k = n,$$

kteřá vyhovují podmínkám  $\forall i a_i \leq x_i \leq b_i$  ( $a_i, b_i \in Z$ ).

#### Poznámka

Počet celočíselných řešení výše uvedené rovnice stanovíme obvykle následovně:

Nejprve převedeme podmínky  $\forall i a_i \leq x_i \leq b_i$  na tvar  $\forall i 0 \leq x_i - a_i \leq b_i - a_i$ .

Označíme-li nyní  $y_i = x_i - a_i$ ,  $c_i = b_i - a_i$  a  $m = n - \sum_{i=1}^k a_i$ , dostáváme se k ekvivalentní rovnici

$$y_1 + \dots + y_k = m,$$

s podmínkami  $\forall i \ 0 \leq y_i \leq c_i$ .

Hledaný počet řešení pak stanovíme pomocí principu inkluze a exkluze, tj. dle vztahu

$$N(\bar{\alpha}_1, \dots, \bar{\alpha}_k) = N - \left[ \sum_{i=1}^k N(\alpha_i) \right] + \left[ \sum_{1 \leq i_1 < i_2 \leq k} N(\alpha_{i_1}, \alpha_{i_2}) \right] - \left[ \sum_{1 \leq i_1 < i_2 < i_3 \leq k} N(\alpha_{i_1}, \alpha_{i_2}, \alpha_{i_3}) \right] + \dots + (-1)^k N(\alpha_1, \dots, \alpha_k),$$

kde  $\alpha_i: c_i + 1 \leq y_i, i = 1, \dots, k$ ,

$\bar{\alpha}_i: 0 \leq y_i \leq c_i$ ,

$N(\alpha_{i_1}, \dots, \alpha_{i_j}), j = 1, \dots, k$  označuje počet řešení vyhovující podmínkám  $\alpha_{i_1}, \dots, \alpha_{i_j}$  a

$N(\bar{\alpha}_1, \dots, \bar{\alpha}_k)$  je počet hledaných řešení, tj. vyhovujících podmínkám  $\bar{\alpha}_1, \dots, \bar{\alpha}_k$ .

### Příklad

Nalezněte počet celočíselných řešení rovnice

$$x_1 + x_2 + x_3 + x_4 + x_5 = 8,$$

kde  $0 \leq x_1, -4 < x_2 < 5, 2 \leq x_3 \leq 6, -4 \leq x_4 < -1, 0 < x_5 \leq 7$ .

Řešení.

Nejprve omezující podmínky transformujeme na ekvivalentní tvar s dolní mezí rovnou 0. Dostáváme

$$0 \leq x_1, 0 \leq x_2 + 3 \leq 7, 0 \leq x_3 - 2 \leq 4, 0 \leq x_4 + 4 \leq 2, 0 \leq x_5 - 1 \leq 6.$$

Nyní provedeme substituci  $y_1 = x_1, y_2 = x_2 + 3, y_3 = x_3 - 2, y_4 = x_4 + 4, y_5 = x_5 - 1$ , která převede původní rovnici na tvar

$$y_1 + y_2 + y_3 + y_4 + y_5 = 12 \quad (*)$$

s podmínkami  $0 \leq y_1, 0 \leq y_2 \leq 7, 0 \leq y_3 \leq 4, 0 \leq y_4 \leq 2, 0 \leq y_5 \leq 6$ .

Pro potřeby principu inkluze a exkluze použijme následující označení (negace omezujících podmínek s definovanou horní mezí):  $\alpha_1: 8 \leq y_2, \alpha_2: 5 \leq y_3, \alpha_3: 3 \leq y_4, \alpha_4: 7 \leq y_5$ . Hledáme tedy počet řešení  $N(\bar{\alpha}_1, \bar{\alpha}_2, \bar{\alpha}_3, \bar{\alpha}_4)$  rovnice (\*), která nesplňují žádnou z podmínek  $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ . Z principu inkluze a exkluze dostáváme

$$N(\bar{\alpha}_1, \bar{\alpha}_2, \bar{\alpha}_3, \bar{\alpha}_4) = N - \sum_{i=1}^4 N(\alpha_i) + \sum_{1 \leq i_1 < i_2 \leq 4} N(\alpha_{i_1}, \alpha_{i_2}) - \sum_{1 \leq i_1 < i_2 < i_3 \leq 4} N(\alpha_{i_1}, \alpha_{i_2}, \alpha_{i_3}) + N(\alpha_1, \alpha_2, \alpha_3, \alpha_4),$$

kde  $N$  je počet všech řešení ( $0 \leq y_i$ ),

$N(\alpha_i)$  je počet řešení vyhovující podmínce  $\alpha_i$ , jinde  $0 \leq y_j$  pro  $j \neq i$ ,

$N(\alpha_{i_1}, \alpha_{i_2})$  je počet řešení vyhovující podmínkám  $\alpha_{i_1}, \alpha_{i_2}$ , jinde  $0 \leq y_j$  pro  $j \neq i_1, i_2$ ,

$N(\alpha_{i_1}, \alpha_{i_2}, \alpha_{i_3})$  je počet řešení vyhovující podmínkám  $\alpha_{i_1}, \alpha_{i_2}, \alpha_{i_3}$ , jinde  $0 \leq y_j$  pro  $j \neq i_1, i_2, i_3$ ,

$N(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$  je počet řešení vyhovující podmínkám  $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ .

Pro výše uvedené dostáváme (viz předchozí věta) následující hodnoty

$$N = P(4, 12) = 1820;$$

$$N(\alpha_1) = P(4, 12 - 8) = 70; \quad N(\alpha_2) = P(4, 12 - 5) = 330;$$

$$N(\alpha_3) = P(4, 12 - 3) = 715; \quad N(\alpha_4) = P(4, 12 - 7) = 126;$$

$$N(\alpha_1, \alpha_2) = N(\alpha_1, \alpha_4) = 0; \quad N(\alpha_1, \alpha_3) = P(4, 12 - 8 - 3) = 5;$$

$$N(\alpha_2, \alpha_3) = P(4, 12 - 5 - 3) = 70; \quad N(\alpha_2, \alpha_4) = P(4, 12 - 5 - 7) = 1;$$

$$N(\alpha_3, \alpha_4) = P(4, 12 - 3 - 7) = 15;$$

$$N(\alpha_1, \alpha_2, \alpha_3) = N(\alpha_1, \alpha_2, \alpha_4) = N(\alpha_1, \alpha_3, \alpha_4) = N(\alpha_2, \alpha_3, \alpha_4) = N(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = 0;$$

Tedy pro hledaný počet řešení platí  $N(\bar{\alpha}_1, \bar{\alpha}_2, \bar{\alpha}_3, \bar{\alpha}_4) = 670$

## 2.2. Rozklady nerozlišitelných objektů do nerozlišitelných tříd

Úloha - určete počet rozkladů množiny obsahující  $n$  nerozlišitelných objektů do nerozlišitelných tříd.

### Tvrzení

Počet rozkladů množiny obsahující  $n$  nerozlišitelných objektů do nerozlišitelných tříd (jejichž počet není předepsán), je roven:

- Počtu rozkladů přirozeného čísla  $n$  na součet přirozených sčítanců.
- Počtu řešení diofantické rovnice

$$x_1 + 2x_2 + 3x_3 + \dots + nx_n = n$$

v oboru přirozených čísel (tj.  $\forall i x_i \in N$ ).

Důkaz.

ad a) Zřejmé - každý sčítanec reprezentuje počet prvků třídy rozkladu (nezáleží na pořadí sčítanců, neboť sčítání je komutativní, sčítanci se stejnou hodnotou jsou nerozlišitelní).

ad b) S ohledem na a) stačí označit počet sčítanců o velikosti  $i$  symbolem  $x_i$  ( $1 \leq i \leq n$ ).

Další variantou výše uvedené úlohy o rozkladu přirozeného čísla  $n$  na kladné sčítance je předepsání hodnot, kterých sčítanci mohou nabývat (v základní variantě to jsou hodnoty  $1, 2, \dots, n$ ).

### Tvrzení

Počet rozkladů přirozeného čísla  $n$  na sčítance rovné některým z přirozených čísel  $a_1, a_2, \dots, a_k$ , je roven počtu řešení diofantické rovnice

$$a_1x_1 + a_2x_2 + \dots + a_kx_k = n$$

v oboru přirozených čísel (tj.  $\forall i x_i \in N$ ).

Důkaz.

Analogicky předchozímu tvrzení stačí interpretovat  $x_i$  jako počet sčítanců rovných číslu  $a_i$ .

### Poznámka

Je zřejmé, že přirozené číslo  $n$  nemusí být vždy rozložitelné na součet využívající pouze zadaných sčítanců  $a_1, \dots, a_k$ . Snadno se přesvědčíme, že např. číslo 353 nelze vyjádřit ve tvaru součtu, kde sčítance se mohou opakovat, ale mohou být rovny pouze některým z čísel 9, 12, 21, 33. Připomeňme, že kritériem řešitelnosti je v tomto případě podmínka  $NSD(a_1, \dots, a_k) | n$ , kde  $NSD$  označuje největšího společného dělitele.

### Příklad

Určete počet způsobů, jak lze vyplatit částku  $5n$  Kč pomocí mincí v hodnotě 5 Kč, 10 Kč, 20 Kč.

Řešení.

Úloha je zřejmě ekvivalentní s úlohou určit počet řešení rovnice  $5x_1 + 10x_2 + 20x_3 = 5n$  ( $n \in N$ ) v oboru přirozených čísel. Snadno zjistíme, že zadaným podmínkám vyhovují uspořádané trojice tvaru

$$(x_1, x_2, x_3) = (n - 2t - 4u, t, u),$$

kde  $0 \leq n - 2t - 4u$  a  $t, u \in N$ . Odtud pro hledaný počet způsobů jak rozměnit zadanou částku  $5n$  Kč pomocí mincí v hodnotě 5 Kč, 10 Kč, 20 Kč dostáváme vztah

$$\sum_{t=0}^{\lfloor n/2 \rfloor} \left( \left\lfloor \frac{n-2t}{4} \right\rfloor + 1 \right) = (\lfloor n/4 \rfloor + 1)(\lfloor n/2 \rfloor - \lfloor n/4 \rfloor + 1),$$

kde  $\lfloor \cdot \rfloor$  označuje funkci dolní celá část. Např. částku 500 Kč lze rozměnit pomocí 5, 10, 20 Kč mincí 676 různými způsoby.

## 2.3. Stirlingova čísla

Další třídu rozkladových úloh tvoří problematika rozkladu množiny rozlišitelných prvků. Základní výsledky jsou obsahem tohoto odstavce a stručně pojednávají o tzv. Stirlingových číslech.

**Definice** – Stirlingova čísla 2. druhu

Počet, kolika způsoby lze rozložit množinu obsahující  $n$  různých prvků do  $k$  neprázdných tříd, kde na pořadí tříd ani prvků v třídách nezáleží, značíme  $S(n, k)$  a nazýváme Stirlingovo číslo 2. druhu řádu  $n, k$ .

### Poznámky

- V kontextu rozkladů se místo pojmu Stirlingovo číslo 2. druhu běžně používá termín Stirling subset number (řádu  $n, k$ ) a značí se  $\left\{ \begin{matrix} n \\ k \end{matrix} \right\}$ , tj.  $S(n, k) = \left\{ \begin{matrix} n \\ k \end{matrix} \right\}$ . Oba názvy i symboly budeme běžně používat jako ekvivalenty. Nicméně označení pomocí složených závorek budeme preferovat, neboť je návodné a zdůrazňuje skutečnost, že jde o třídy rozkladu, které chápeme jako množiny, tedy nezáleží na pořadí prvků v třídách rozkladu (na rozdíl od níže zavedených Stirling cycle numbers).

- Pro některé hodnoty  $n, k \in N$  je snadné určit  $\left\{ \begin{matrix} n \\ k \end{matrix} \right\}$  explicitně. Platí:

$$\begin{aligned} \left\{ \begin{matrix} 0 \\ 0 \end{matrix} \right\} &= 1, & \left\{ \begin{matrix} n \\ 0 \end{matrix} \right\} &= 0, \text{ pro } n \in N^+, & \left\{ \begin{matrix} n \\ 1 \end{matrix} \right\} &= 1, \text{ pro } n \in N^+, \\ \left\{ \begin{matrix} n \\ 2 \end{matrix} \right\} &= 2^{n-1} - 1, \text{ pro } 2 \leq n, & \left\{ \begin{matrix} n \\ n-1 \end{matrix} \right\} &= \frac{n(n-1)}{2}, \text{ pro } n \in N^+, & \left\{ \begin{matrix} n \\ n \end{matrix} \right\} &= 1, \text{ pro } n \in N. \end{aligned}$$

(řádně zdůvodněte!)

### Tvrzení

Pro Stirlingova čísla 2. druhu (Stirling subset numbers) platí pro  $1 \leq k \leq n$  rekurentní vztah

$$\left\{ \begin{matrix} n \\ k \end{matrix} \right\} = \left\{ \begin{matrix} n-1 \\ k-1 \end{matrix} \right\} + k \left\{ \begin{matrix} n-1 \\ k \end{matrix} \right\}.$$

(s počátečními podmínkami uvedenými v předchozí poznámce)

Důkaz.

Označme  $M = \{a_1, \dots, a_n\}$  množinu rozkládanou do  $k$  neprázdných tříd. Uvažované rozklady rozdělíme do dvou disjunktních skupin následovně – první obsahuje rozklady, kde libovolný pevně zvolený prvek, např.  $a_1$ , tvoří samostatnou třídu rozkladu a druhou zbývající rozklady (tj. rozklady, kde prvek  $a_1$  je obsažen ve třídě rozkladu obsahující alespoň 2 prvky). Snadno zjistíme, že v první skupině existuje  $\left\{ \begin{matrix} n-1 \\ k-1 \end{matrix} \right\}$  rozkladů (prvek  $a_1$  tvoří samostatnou třídu rozkladu a je proto třeba rozložit  $n-1$  zbývajících prvků do  $k-1$  tříd). Počet rozkladů ve druhé skupině je zřejmě roven  $k \left\{ \begin{matrix} n-1 \\ k \end{matrix} \right\}$ . Všechny prvky kromě  $a_1$  (tj. celkem  $n-1$  prvků) rozložíme do  $k$  tříd a následně prvek  $a_1$  přidáme k některé z  $k$  již existujících tříd.

**Poznámka** - trojúhelník Stirlingových čísel 2. druhu/Stirling subset numbers

Stirlingova čísla 2. druhu  $\left\{ \begin{matrix} n \\ k \end{matrix} \right\}$ ,  $0 \leq k \leq n$  lze uspořádat do schématu uvedeného v příloze - tabulka 3.6, které je analogií Pascalova trojúhelníku pro kombinační čísla  $C_n^k$ ,  $0 \leq k \leq n$ . Hodnoty počítáme z výše uvedeného rekurentního vztahu (a z počátečních podmínek).

**Definice** - Bellova čísla

Počet všech rozkladů konečné  $n$ -prvkové množiny značíme  $B_n$ ,  $n \in N$  a nazýváme Bellovo číslo.

### Poznámka

- Každý rozklad množiny jednoznačně definuje relaci ekvivalence na této množině a tedy Bellova čísla  $B_n, n \in \mathbb{N}$  lze interpretovat také jako počet ekvivalencí na  $n$ -prvkové množině.
- Je zřejmé, že pro Bellova čísla platí  $B_n = \sum_{k=0}^n \left\{ \begin{matrix} n \\ k \end{matrix} \right\}$ , tj.  $B_n$  je součtem  $n$ -tého řádku výše uvedeného trojúhelníka Stirlingových čísel 2. druhu.

### Definice – Stirling cycle numbers

Počet, kolika způsoby lze rozložit množinu obsahující  $n$  různých prvků do  $k$  neprázdných cyklů značíme  $\left[ \begin{matrix} n \\ k \end{matrix} \right]$  a nazýváme Stirling cycle number<sup>1</sup> řádu  $n, k$ .

### Poznámky

- Jak Stirling subset numbers  $\left\{ \begin{matrix} n \\ k \end{matrix} \right\}$ , tak i Stirling cycle numbers  $\left[ \begin{matrix} n \\ k \end{matrix} \right]$  se vztahují k rozkladům  $n$ -prvkové množiny na  $k$  neprázdných nerozlišitelných tříd, resp. do  $k$  cyklů. Rozdíl spočívá v tom, že v případě Stirling subset numbers nezáleží na pořadí prvků v jednotlivých třídách rozkladu, kdežto v případě Stirling cycle numbers jsou prvky každé třídy rozkladu uspořádány na kružnici a tedy záleží na tom, jak jsou na kružnici uspořádány. Pro libovolná  $0 \leq k \leq n$  proto zřejmě platí  $0 \leq \left\{ \begin{matrix} n \\ k \end{matrix} \right\} \leq \left[ \begin{matrix} n \\ k \end{matrix} \right]$ .
- Stirling cycle number  $\left[ \begin{matrix} n \\ k \end{matrix} \right]$  lze interpretovat jako počet permutací na  $n$ -prvkové množině, které lze zapsat pomocí  $k$  disjunktních cyklů, tudíž platí  $\sum_{k=0}^n \left[ \begin{matrix} n \\ k \end{matrix} \right] = n!$
- Pro některé hodnoty  $n, k \in \mathbb{N}$  je snadné určit  $\left[ \begin{matrix} n \\ k \end{matrix} \right]$  explicitně. Platí:

$$\begin{aligned} \left[ \begin{matrix} 0 \\ 0 \end{matrix} \right] &= 1, & \left[ \begin{matrix} n \\ 0 \end{matrix} \right] &= 0, \text{ pro } n \in \mathbb{N}^+, & \left[ \begin{matrix} n \\ 1 \end{matrix} \right] &= (n-1)!, \text{ pro } n \in \mathbb{N}^+, \\ \left[ \begin{matrix} n \\ n-1 \end{matrix} \right] &= \frac{n(n-1)}{2}, \text{ pro } n \in \mathbb{N}^+, & \left[ \begin{matrix} n \\ n \end{matrix} \right] &= 1, \text{ pro } n \in \mathbb{N}. & & \text{(řádně zdůvodněte!)} \end{aligned}$$

### Tvrzení

Pro Stirling cycle numbers platí pro  $1 \leq k \leq n$  rekurentní vztah

$$\left[ \begin{matrix} n \\ k \end{matrix} \right] = \left[ \begin{matrix} n-1 \\ k-1 \end{matrix} \right] + (n-1) \left[ \begin{matrix} n-1 \\ k \end{matrix} \right].$$

(s počátečními podmínkami uvedenými v předchozí poznámce)

Důkaz.

Zcela analogický důkaz předchozího tvrzení, tj. spočteme počet rozkladů, kde prvek  $a_1$  tvoří samostatný cyklus, plus počet rozkladů, kde prvek  $a_1$  je součástí cyklu délky alespoň 2.

### Definice - padající faktoriál

Nechť  $x \in \mathbb{R}, n \in \mathbb{N}$ . Potom symbolem  $x^{\underline{n}}$  označujeme tzv. padající faktoriál (faktorial power, falling power) definovaný vztahem

$$x^{\underline{n}} = x \cdot (x-1) \cdot \dots \cdot (x-n+1),$$

kde definujeme  $x^{\underline{0}} = 1$

### Poznámky – Stirlingova čísla 1. a 2. druhu

- Je zřejmé, že padající faktoriál  $x^{\underline{n}}$  je polynom stupně  $n$  a lze ho proto psát ve tvaru

$$x^{\underline{n}} = \sum_{k=0}^n s(n, k) \cdot x^k.$$

Koeficienty  $s(n, k)$  se nazývají Stirlingova čísla 1. druhu.

---

<sup>1</sup> Vzhledem k tomu, že v češtině není dosud ustálen vhodný překlad, budeme dále používat anglickou terminologii.

Mezi Stirlingovými čísly 1. druhu a Stirling cycle numbers platí vztah

$$s(n, k) = (-1)^{n-k} \left[ \begin{matrix} n \\ k \end{matrix} \right],$$

tedy

$$x^n = \sum_{k=0}^n (-1)^{n-k} \left[ \begin{matrix} n \\ k \end{matrix} \right] \cdot x^k.$$

- Snadno lze ukázat i obrácené tvrzení, že mocninu  $x^n, n \in \mathbb{N}$  lze jednoznačně vyjádřit ve tvaru lineární kombinace padajících faktoriálů  $x^k, k = 0, 1, \dots, n$ , tj. ve tvaru

$$x^n = \sum_{k=0}^n S(n, k) \cdot x^k.$$

Koeficienty  $S(n, k)$  se jsou právě Stirlingova čísla 2. druhu, resp. Stirling subset numbers a platí již zmíněný vztah  $S(n, k) = \left\{ \begin{matrix} n \\ k \end{matrix} \right\}$ , takže lze také psát  $x^n = \sum_{k=0}^n \left\{ \begin{matrix} n \\ k \end{matrix} \right\} \cdot x^k$ .

### Příklad

a) Vyjádřete  $x^7$  ve tvaru polynomu.

b) Vyjádřete  $x^7$  ve tvary lineární kombinace padajících faktoriálů.

Řešení.

ad a) Z výše uvedené poznámky dostáváme

$$x^7 = x^7 - 21x^6 + 175x^5 - 735x^4 + 1624x^3 - 1764x^2 + 720x.$$

Správnost ověřte z definice, tj. roznásobením výrazu  $x^7 = x(x-1)(x-2)(x-3)(x-4)(x-5)(x-6)$ .

ad b) Vzhledem k výše uvedené poznámce dostáváme

$$x^7 = x^7 + 21x^6 + 140x^5 + 350x^4 + 301x^3 + 63x^2 + x^1.$$

Správnost ověřte dosazením výrazů pro  $x^k, k = 1, \dots, 7$  a následným roznásobením.



### 3. Rekurentní vztahy

Posloupnost je jedním ze základních pojmů, který budeme v těchto skriptech používat. V následující poznámce proto tento pojem (a pojmy související) stručně připomeneme.

#### Poznámky

- Posloupností rozumíme libovolné zobrazení množiny přirozených čísel  $N$  do množiny reálných (resp. komplexních čísel). Posloupnost budeme obvykle značit  $\{a_n\}_{n=0}^{\infty}$ , resp.  $(a_n)_{n=0}^{\infty}$  (členy číslujeme od 0).
- Na množině všech posloupností se zavádí operace sčítání posloupností a násobení posloupnosti skalárem (reálným, resp. komplexním číslem) následovně:

$$\{a_n\}_{n=0}^{\infty} + \{b_n\}_{n=0}^{\infty} = \{a_n + b_n\}_{n=0}^{\infty}, \quad (\text{tj. posloupnosti sčítáme člen po členu})$$

$$\alpha\{a_n\}_{n=0}^{\infty} = \{\alpha a_n\}_{n=0}^{\infty}. \quad (\text{tj. každý člen posloupnosti vynásobíme číslem } \alpha)$$

V této souvislosti připomeňme, že množina všech posloupností tvoří vektorový prostor nad tělesem reálných, resp. komplexních čísel. Této skutečnosti budeme využívat a běžně používat následující pojmy (známé z lineární algebry): vektorový prostor/podprostor, lineární kombinace posloupností, lineárně (ne)závislá množina posloupností, báze, dimenze atd.

- Posloupnost můžeme definovat v zásadě třemi způsoby - zadáním explicitního výrazu pro její  $n$ -tý člen (např.  $a_n = 2n - 1$ ), pomocí rekurentního vztahu (alternativně pomocí diferenční rovnice) nebo pomocí vytvořující funkce.

#### Definice – rekurentní vztah, řešení

Rekurentním vztahem posloupnosti  $\{a_n\}_{n=0}^{\infty}$  označujeme rovnici

$$\Phi(a_n, a_{n-1}, \dots, a_0, n) = 0,$$

kde  $\Phi$  označuje funkci s proměnnými  $a_0, a_1, \dots, a_n, n$ , která  $\forall n \geq n_0$  ( $n_0$  pevně dané) umožňuje vypočítat hodnotu  $a_n$  pomocí předchozích členů posloupnosti (tj.  $a_{n-1}, \dots, a_0$ ) a hodnoty  $n$ . Libovolnou posloupnost  $\{a_n\}_{n=0}^{\infty}$  takovou, že  $\forall n \geq n_0$  po do sazení hodnot  $a_n, a_{n-1}, \dots, a_0, n$  platí  $\Phi(a_n, a_{n-1}, \dots, a_0, n) = 0$  nazýváme řešením daného rekurentního vztahu.

Rekurentní vztahy lze rozdělit do následujících základních kategorií:

- Rekurentní vztah označujeme jako homogenní, jestliže nulová posloupnost, tj.  $\{0\}_{n=0}^{\infty}$ , je řešením daného vztahu. Ostatní rekurentní vztahy označujeme jako nehomogenní (někdy méně vhodně jako rekurentní vztahy s nenulovou pravou stranou).
- Rekurentní vztah označujeme jako lineární, jestliže  $\Phi$  je lineární funkcí členů  $a_n, a_{n-1}, \dots, a_0$ . Ostatní rekurentní vztahy označujeme jako nelineární. Např.  $a_n = a_0 a_{n-1} + a_1 a_{n-2} + \dots + a_{n-1} a_0$  je ukázkou důležitého homogenního nelineárního rekurentního vztahu. V další části se budeme zabývat především řešením homogenních i nehomogenních lineárních rekurentních vztahů.

#### Poznámky – difference, diferenční rovnice

S rekurentními vztahy velmi úzce souvisí tzv. diferenční rovnice, které definují posloupnost pomocí tzv. diferencí.

- Nechť  $\{a_n\}_{n=0}^{\infty}$  je posloupnost. Potom symbolem  $\Delta a_n$  označujeme 1. diferenci posloupnosti  $\{a_n\}_{n=0}^{\infty}$  v bodě  $n$  a definujeme ji vztahem

$$\Delta a_n = a_{n+1} - a_n.$$

Je zřejmé, že  $\Delta a_n$  je definováno pro libovolné  $n \in N$  a tedy 1. difference tvoří posloupnost  $\{\Delta a_n\}_{n=0}^{\infty}$  nazývanou posloupností 1. diferencí posloupnosti  $\{a_n\}_{n=0}^{\infty}$ .

Analogicky lze postupovat i v případě posloupnosti  $\{\Delta a_n\}_{n=0}^{\infty}$ , jejímž diferencováním dostáváme posloupnost  $\{\Delta^{(2)} a_n\}_{n=0}^{\infty}$  nazývanou posloupností 2. diferencí posloupnosti  $\{a_n\}_{n=0}^{\infty}$ , kde

$$\Delta^{(2)}a_n = \Delta(\Delta a_n) = \Delta a_{n+1} - \Delta a_n = (a_{n+2} - a_{n+1}) - (a_{n+1} - a_n) = a_{n+2} - 2a_{n+1} + a_n.$$

Diference vyšších řádu definujeme rekurentně vztahem

$$\Delta^{(k)}a_n = \Delta(\Delta^{(k-1)}a_n),$$

kde  $\Delta^{(0)}a_n = a_n$ .

- Diferenční rovnici rozumíme výraz

$$\Psi(\Delta^{(k)}a_n, \Delta^{(k-1)}a_n, \dots, \Delta a_n, n) = 0,$$

kde  $\Delta^{(i)}a_n, i = 1, \dots, k$  označuje  $i$ -tou diferenci posloupnosti  $\{a_n\}_{n=0}^\infty$ .

- Každou diferenční rovnici lze převést na rekurentní vztah tak, že diference jednotlivých řádů rozepíšeme dle zřejmého vztahu  $\Delta^{(k)}a_n = \sum_{i=0}^k (-1)^i C_k^i a_{n+k-i}$ . Obráceně, každý rekurentní vztah lze převést na diferenční rovnici, neboť platí  $a_{n+k} = \sum_{i=0}^k C_k^i \Delta^{(i)}a_n$ .

### 3.1. Homogenní lineární rekurentní vztahy a jejich řešení

#### Definice

Homogenním lineárním rekurentním vztahem (dále HLR vztah) řádu  $k$  s konstantními koeficienty rozumíme výraz

$$C_k a_{n+k} + C_{k-1} a_{n+k-1} + \dots + C_0 a_n = 0, \quad (*)$$

kde  $C_i \in R (i = 0, \dots, k)$  a  $C_0 C_k \neq 0$ .

Řešením HLR (\*) rozumíme libovolnou posloupnost  $\{a_n\}_{n=0}^\infty$  takovou, že  $\forall n \in N$  po dosazení hodnot  $a_{n+k}, a_{n+k-1}, \dots, a_n$  platí rovnost  $C_k a_{n+k} + C_{k-1} a_{n+k-1} + \dots + C_0 a_n = 0$ .

Základní výsledky vztahující se k problematice řešení HLR vztahů jsou uvedeny v následujícím tvrzení.

#### Tvrzení

- HLR vztah řádu  $k \geq 1$  má nekonečně mnoho řešení. Je-li však předepsáno  $k$  počátečních podmínek (tj.  $k$  po sobě jdoucích hodnot  $a_i, \dots, a_{i+k-1}$ , obvykle hodnoty  $a_0, \dots, a_{k-1}$ ), potom existuje jediné řešení, které tyto podmínky splňuje.
- Jsou-li posloupnosti  $\{a_n\}_{n=0}^\infty, \{b_n\}_{n=0}^\infty$  řešením HLR vztahu, potom pro libovolné konstanty  $K, L$  je řešením také posloupnost  $\{K a_n + L b_n\}_{n=0}^\infty$ .
- Množina všech řešení HLR vztahu řádu  $k$  tvoří vektorový prostor dimenze  $k$ . Existuje proto  $k$  lineárně nezávislých posloupností  $\{a_n^{(1)}\}_{n=0}^\infty, \dots, \{a_n^{(k)}\}_{n=0}^\infty$ , které jsou řešením, přičemž obecným řešením rozumíme lineární kombinaci těchto  $k$  lineárně nezávislých řešení. Je-li tedy  $\{b_n\}_{n=0}^\infty$  libovolné řešení HLR vztahu, potom existují jediné konstanty  $K_1, \dots, K_k$  takové, že  $\forall n \in N \quad b_n = \sum_{i=1}^k K_i a_n^{(i)}$ .

(Tvrzení dokažte jako cvičení.)

Jak plyne z výše uvedeného, řešení HLR vztahu spočívá v nalezení  $k$  lineárně nezávislých řešení. Pokud hledáme řešení vyhovující zadaným počátečním podmínkám, dopočteme hodnoty koeficientů  $K_1, \dots, K_k$  vyskytujících se v obecném řešení (vyřešíme soustavu  $k$  lineárních algebraických rovnic o  $k$  neznámých).

#### Definice

Charakteristickým polynomem příslušným HLR vztahu (\*) rozumíme polynom

$$C_k x^k + C_{k-1} x^{k-1} + \dots + C_1 x + C_0.$$

Nyní se snadno přesvědčíme, že pokud  $r$  je kořen charakteristického polynomu, potom posloupnost  $\{r^n\}_{n=0}^{\infty}$  je řešením příslušného HLR vztahu. Navíc, pokud  $r$  je  $m$  násobný kořen charakteristického polynomu, potom posloupnosti  $\{r^n\}_{n=0}^{\infty}, \{nr^n\}_{n=0}^{\infty}, \dots, \{n^{m-1}r^n\}_{n=0}^{\infty}$  jsou lineárně nezávislá řešení příslušného HLR vztahu. Jako bezprostřední důsledek pak dostáváme následující tvrzení.

### Tvrzení

Nechť  $r_1, \dots, r_l$  jsou kořeny charakteristického polynomu a  $m_1, \dots, m_l$  jsou jejich násobnosti, potom posloupnost  $\{a_n\}_{n=0}^{\infty}$ , kde

$$\begin{aligned} a_n = & r_1^n \left( K_1^{(1)} + K_2^{(1)}n + \dots + K_{m_1}^{(1)}n^{m_1-1} \right) + \\ & r_2^n \left( K_1^{(2)} + K_2^{(2)}n + \dots + K_{m_2}^{(2)}n^{m_2-1} \right) + \\ & \vdots \\ & r_l^n \left( K_1^{(l)} + K_2^{(l)}n + \dots + K_{m_l}^{(l)}n^{m_l-1} \right), \end{aligned}$$

$K_1^{(1)}, \dots, K_{m_l}^{(l)}$  jsou libovolné konstanty,

je obecným řešením HLR vztahu (\*).

### Poznámka

Vzhledem k tomu, že koeficienty uvažovaného HLR vztahu jsou reálná čísla, jsou kořeny charakteristického polynomu reálná čísla nebo dvojice komplexně sdružených čísel  $r_1 = a + ib, r_2 = a - ib$ . Využijeme-li goniometrický tvar komplexních čísel a známou Moivreovu větu  $(\cos \varphi \pm i \sin \varphi)^n = \cos(n\varphi) \pm i \sin(n\varphi)$ , lze dvojici lineárně nezávislých posloupností generovaných komplexně sdruženými kořeny nahradit dvojicí lineárně nezávislých reálných posloupností, tj.

$$K_1(a + ib)^n + K_2(a - ib)^n = (\sqrt{a^2 + b^2})^n (C_1 \cos(n\varphi) + C_2 \sin(n\varphi)), \text{ kde } \varphi = \arctan(b/a).$$

### Příklad

Uvažujte rekurentní vztah  $a_{n+4} - 3a_{n+3} + 4a_{n+2} - 3a_{n+1} + a_n = 0$ . a) Nalezněte obecné řešení.

b) Nalezněte řešení vyhovující podmínkám  $a_0 = 3, a_1 = 5 - 2\sqrt{3}, a_2 = 6 - 2\sqrt{3}, a_3 = 8$ .

Řešení.

a) Jde o homogenní lineární rekurentní vztah 4. řádu, jehož charakteristický polynom má tvar

$$x^4 - 3x^3 + 4x^2 - 3x + 1 = (x - 1)^2(x^2 - x + 1).$$

Jako kořeny  $r_i$  a jejich násobnosti  $m_i$  dostáváme

$$r_1 = 1, m_1 = 2; r_2 = \frac{1}{2} + i\frac{\sqrt{3}}{2}, m_2 = 1; r_3 = \frac{1}{2} - i\frac{\sqrt{3}}{2}, m_3 = 1.$$

Obecné řešení má tvar

$$a_n = K_1 + K_2n + K_3 \left( \frac{1}{2} + i\frac{\sqrt{3}}{2} \right)^n + K_4 \left( \frac{1}{2} - i\frac{\sqrt{3}}{2} \right)^n.$$

Nyní dvojici lineárně nezávislých komplexních posloupností  $\left\{ \left( \frac{1}{2} + i\frac{\sqrt{3}}{2} \right)^n \right\}_{n=0}^{\infty}, \left\{ \left( \frac{1}{2} - i\frac{\sqrt{3}}{2} \right)^n \right\}_{n=0}^{\infty}$  nahradíme dvojicí reálných lineárně nezávislých posloupností tvořících také řešení. Jelikož

$$\frac{1}{2} + i\frac{\sqrt{3}}{2} = \cos \frac{\pi}{3} + i \sin \frac{\pi}{3} \text{ a } \frac{1}{2} - i\frac{\sqrt{3}}{2} = \cos \frac{\pi}{3} - i \sin \frac{\pi}{3}$$

dostáváme

$$\left( \frac{1}{2} + i\frac{\sqrt{3}}{2} \right)^n = \cos \frac{\pi n}{3} + i \sin \frac{\pi n}{3}, \left( \frac{1}{2} - i\frac{\sqrt{3}}{2} \right)^n = \cos \frac{\pi n}{3} - i \sin \frac{\pi n}{3}$$

a uvedenou dvojici komplexních posloupností nahradíme dvojicí posloupností  $\left\{ \cos \frac{\pi n}{3} \right\}_{n=0}^{\infty}, \left\{ \sin \frac{\pi n}{3} \right\}_{n=0}^{\infty}$ .

Obecné řešení má proto tvar

$$a_n = L_1 + L_2 n + L_3 \cos \frac{\pi n}{3} + L_4 \sin \frac{\pi n}{3}.$$

b) S ohledem na počáteční podmínky dostáváme následující soustavu

$$\begin{aligned} L_1 + L_3 &= 3 & \text{. Vyřešením dostáváme } a_n = 1 + 3n + 2 \cos \frac{\pi n}{3} - 4 \sin \frac{\pi n}{3}. \\ L_1 + L_2 + \frac{L_3}{2} + L_4 \frac{\sqrt{3}}{2} &= 5 - 2\sqrt{3} \\ L_1 + 2L_2 - \frac{L_3}{2} + L_4 \frac{\sqrt{3}}{2} &= 6 - 2\sqrt{3} \\ L_1 + 3L_2 - L_3 &= 8 \end{aligned}$$

### Poznámky

- Fibonacciho posloupnost

Posloupnost  $\{F_n\}_{n=0}^{\infty}$  definovanou lineárním homogenním rekurentním vztahem řádu 2

$$F_{n+2} = F_{n+1} + F_n$$

a vyhovující počátečním podmínkám  $F_0 = 0, F_1 = 1$ , nazýváme Fibonacciho posloupností (její prvky nazýváme Fibonacciho čísla). Vyřešením dostáváme

$$F_n = \frac{1}{\sqrt{5}} \left[ \left( \frac{1+\sqrt{5}}{2} \right)^n - \left( \frac{1-\sqrt{5}}{2} \right)^n \right], n \in N.$$

- Lucasova posloupnost

Posloupnost  $\{L_n\}_{n=0}^{\infty}$  definovanou lineárním homogenním rekurentním vztahem řádu 2

$$L_{n+2} = L_{n+1} + L_n$$

a vyhovující počátečním podmínkám  $L_0 = 2, L_1 = 1$ , nazýváme Lucasovou posloupností (její prvky nazýváme Lucasova čísla). Vyřešením dostáváme

$$L_n = \left( \frac{1+\sqrt{5}}{2} \right)^n + \left( \frac{1-\sqrt{5}}{2} \right)^n, n \in N.$$

Tabulku obsahující několik prvních členů Fibonacciho a Lucasovy posloupnosti lze nalézt v příloze.

## 3.2. Nehomogenní lineární rekurentní vztahy a jejich řešení

### Definice

Nehomogenním lineárním rekurentním vztahem (dále NHLR vztah) řádu  $k$  s konstantními koeficienty rozumíme výraz

$$C_k a_{n+k} + C_{k-1} a_{n+k-1} + \dots + C_0 a_n = p_n, \quad (**)$$

kde  $C_i \in R (i = 0, \dots, k), C_0 C_k \neq 0$ ,

$\{p_n\}_{n=0}^{\infty}$  je posloupnost taková, že  $\exists i \in N p_i \neq 0$ .

Řešením NHLR (\*\*\*) rozumíme libovolnou posloupnost  $\{a_n\}_{n=0}^{\infty}$  takovou, že  $\forall n \in N$  po dosazení hodnot  $a_{n+k}, a_{n+k-1}, \dots, a_n$  platí rovnost  $C_k a_{n+k} + C_{k-1} a_{n+k-1} + \dots + C_0 a_n = p_n$ .

Výraz  $C_k a_{n+k} + \dots + C_0 a_n = 0$  označujeme jako HLR vztah příslušný NHLR vztahu (\*\*).

Základní výsledky vztahující se k problematice řešení NHLR vztahů jsou uvedeny v následujícím tvrzení.

### Tvrzení

- NHLR vztah řádu  $k \geq 1$  má nekonečně mnoho řešení.
- Obecné řešení  $\{a_n\}_{n=0}^{\infty}$  NHLR vztahu má tvar

$$a_n = a_n^{(p)} + a_n^{(h)},$$

kde  $\{a_n^{(p)}\}_{n=0}^{\infty}$  je tzv. partikulární řešení (jedna konkrétní posloupnost vyhovující danému NHLR vztahu),  
 $\{a_n^{(h)}\}_{n=0}^{\infty}$  je obecné řešení HLR vztahu příslušného NHLR vztahu.

- Je-li předepsáno  $k$  počátečních podmínek (tj.  $k$  po sobě jdoucích hodnot  $a_i, \dots, a_{i+k-1}$ ), potom existuje jediné řešení NHLR vztahu, které těmto podmínkám vyhovuje.

Vzhledem ke znalosti metod řešení HLR vztahů je zřejmé, že řešení NHLR vztahu se redukuje na schopnost nalézt jeho partikulární řešení. V následující části se tak změříme na způsob nalezení partikulárního řešení pro speciální tvary pravých stran  $\{p_n\}_{n=0}^{\infty}$ .

Postup nalezení partikulárního řešení NHLR vztahu se speciální pravou stranou lze popsat takto - nejprve sestavíme tzv. zkušební řešení  $\{t_n\}_{n=0}^{\infty}$ , které je ve tvaru pravé strany. Na základě tohoto zkušebního řešení sestrojíme partikulární řešení  $\{a_n^{(p)}\}_{n=0}^{\infty}$  následovně:

- Je-li pravá strana NHLR vztahu ve tvaru uvedeném v sloupci  $p_n$  níže uvedené tabulky, potom zkušební řešení je ve tvaru uvedeném v příslušném řádku sloupce  $t_n$ .
- Je-li pravá strana NHLR vztahu ve tvaru lineární kombinace členů uvedených ve sloupci  $p_n$ , potom zkušební řešení je ve tvaru lineární kombinace členů uvedených v příslušných řádcích sloupce  $t_n$ .
- Jestliže žádný ze sčítanců zkušebního řešení není řešením příslušného HLR vztahu, potom partikulární řešení je ve tvaru zkušebního řešení, tj.  $a_n^{(p)} = t_n$ .
- Jestliže některý ze sčítanců zkušebního řešení je řešením příslušného HLR vztahu, potom partikulární řešení je ve tvaru  $a_n^{(p)} = n^s t_n$ , kde  $s$  je nejmenší přirozené číslo takové, že již žádný ze sčítanců výrazu  $n^s t_n$  (po roznásobení) není řešením příslušného HLR vztahu.

$p_n$	$t_n$
$K$ (konstanta)	$A$ (konstanta)
$n^t, t \in \mathbb{N}$	$A_0 + A_1 n + \dots + A_t n^t$
$r^n, r \in \mathbb{R}$	$A r^n$
$r^n n^t$	$r^n (A_0 + A_1 n + \dots + A_t n^t)$
$\cos(\alpha n)$	$A \cos(\alpha n) + B \sin(\alpha n)$
$\sin(\beta n)$	$A \cos(\beta n) + B \sin(\beta n)$
$r^n \cos(\alpha n)$	$r^n (A \cos(\alpha n) + B \sin(\alpha n))$
$r^n \sin(\beta n)$	$r^n (A \cos(\beta n) + B \sin(\beta n))$

Tabulka zkušebních řešení

### Příklad

Nalezněte řešení rekurentního vztahu  $a_{n+2} + 4a_n = 25n$ , kde  $a_0 = -1, a_1 = 5$ .

Řešení.

Jde o NHLR vztah 2. řádu. Nejprve nalezneme obecné příslušného HLR vztahu  $a_{n+2} + 4a_n = 0$  majícího charakteristický polynom  $x^2 + 4 = (x + 2i)(x - 2i)$ . Jeho kořeny násobnosti 1 jsou  $r_1 = 2i = 2 \left( \cos\left(\frac{\pi}{2}\right) + i \sin\left(\frac{\pi}{2}\right) \right), r_2 = -2i = 2 \left( \cos\left(\frac{\pi}{2}\right) - i \sin\left(\frac{\pi}{2}\right) \right)$ . Obecné řešení příslušného HLR vztahu je

$$a_n^{(h)} = 2^n \left( K_1 \cos\left(\frac{\pi n}{2}\right) + K_2 \sin\left(\frac{\pi n}{2}\right) \right).$$

Zkušební řešení má tvar pravé strany, tj.  $t_n = An + B$ . Jelikož žádný ze sčítanců  $t_n$  není řešením příslušného HLR vztahu dostáváme  $a_n^{(p)} = 5n - 2$ . Obecné řešení zadaného NHLR vztahu je

$$a_n = 5n - 2 + 2^n \left( K_1 \cos\left(\frac{\pi n}{2}\right) + K_2 \sin\left(\frac{\pi n}{2}\right) \right).$$

Nyní využijeme počáteční podmínky a dopočteme konstanty  $K_1, K_2$ . Dostáváme tak

$$a_n = 5n - 2 + 2^n \left( \cos\left(\frac{\pi n}{2}\right) + \sin\left(\frac{\pi n}{2}\right) \right).$$

## 4. Vytvořující funkce

Vytvořující funkce jsou efektivním nástrojem pro práci s posloupnostmi a tedy i velmi silným nástrojem řešení celé řady netriviálních kombinatorických úloh.

**Definice** - obyčejná vytvořující funkce

Nechť  $\{a_n\}_{n=0}^{\infty}$  je reálná, resp. komplexní posloupnost. Algebraický výraz (formální mocninnou řadu)

$$f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n + \dots = \sum_{n=0}^{\infty} a_nx^n,$$

resp. jakýkoliv s ním ekvivalentní tvar, nazveme (obyčejnou) vytvořující funkcí posloupnosti  $\{a_n\}_{n=0}^{\infty}$ .

**Poznámka**

Vytvořující funkci ve tvaru mocninné řady  $\sum_{n=0}^{\infty} a_nx^n$  označujeme jako otevřený, resp. rozvinutý tvar. Ostatní „konečné“ výrazy s ním ekvivalentní označujeme jako uzavřený tvar. Např.  $f(x) = \sum_{n=0}^{\infty} (2x/3)^n$  je rozvinutý tvar vytvořující funkce posloupnosti  $\{(2/3)^n\}_{n=0}^{\infty}$ , kdežto  $f(x) = \frac{3}{3-2x}$  je její uzavřený tvar.

**Tvrzení**

a) Existuje vzájemně jednoznačný vztah mezi posloupností  $\{a_n\}_{n=0}^{\infty}$  a její vytvořující funkcí  $f(x)$ . Platí

$$a_n = f^{(n)}(0)/n!,$$

kde  $f^{(n)}(0)$  označuje hodnotu  $n$ -té derivace funkce  $f(x)$  v bodě 0.

b) Nechť  $f(x)$  je vytvořující funkce posloupnosti  $\{a_n\}_{n=0}^{\infty}$  a  $g(x)$  posloupnosti  $\{b_n\}_{n=0}^{\infty}$ . Potom následující operace s vytvořujícími funkcemi (sloupec „Vytvořující funkce“ níže uvedené tabulky) definují posloupnosti uvedené ve sloupci „Posloupnost“. (Dokažte jako cvičení.)

Vytvořující funkce	Posloupnost
$\alpha f(x) + \beta g(x)$	$\{\alpha a_n + \beta b_n\}_{n=0}^{\infty}$
$x^k f(x)$	$\underbrace{0, \dots, 0}_{k \times 0}, a_0, a_1, a_2, \dots$
$f(x) - (\sum_{i=k}^n a_i x^i)$	$a_0, \dots, a_{k-1}, \underbrace{0, \dots, 0}_{(n-k+1) \times 0}, a_{n+1}, a_{n+2}, \dots$
$f(x^k)$	$a_0, \underbrace{0, \dots, 0}_{(k-1) \times 0}, a_1, \underbrace{0, \dots, 0}_{(k-1) \times 0}, a_2, \underbrace{0, \dots, 0}_{(k-1) \times 0}, a_3, 0, \dots$
$\frac{f(x) - \sum_{i=0}^{k-1} a_i x^i}{x^k}$	$a_k, a_{k+1}, a_{k+2}, \dots$ , tj. $\{a_{k+n}\}_{n=0}^{\infty}$
$\frac{f(x)}{1-x}$	$a_0, a_0 + a_1, a_0 + a_1 + a_2, \dots$ , tj. $\{\sum_{i=0}^n a_i\}_{n=0}^{\infty}$
$f'(x)$	$a_1, 2a_2, 3a_3, \dots, na_n, \dots$ , tj. $\{(n+1)a_{n+1}\}_{n=0}^{\infty}$
$\int_0^x f(t) dt$	$0, a_0, \frac{a_1}{2}, \frac{a_2}{3}, \dots, \frac{a_n}{n+1}, \dots$
$f(x)g(x)$	$a_0b_0, a_0b_1 + a_1b_0, a_0b_2 + a_1b_1 + a_2b_0, \dots$ , tj. $\{\sum_{i=0}^n a_i b_{n-i}\}_{n=0}^{\infty}$

**Poznámka**

Připomeňme, že  $\{\sum_{i=0}^n a_i\}_{n=0}^{\infty}$  se nazývá posloupnost částečných součtů posloupnosti  $\{a_n\}_{n=0}^{\infty}$ . Posloupnost  $\{\sum_{i=0}^n a_i b_{n-i}\}_{n=0}^{\infty}$  se nazývá konvoluce posloupností  $\{a_n\}_{n=0}^{\infty}$  a  $\{b_n\}_{n=0}^{\infty}$  a značí se  $\{a_n * b_n\}_{n=0}^{\infty}$ , resp.  $\{a_n\}_{n=0}^{\infty} * \{b_n\}_{n=0}^{\infty}$ .

### Příklad

Označme  $f(x)$  vytvořující funkci posloupnosti  $\{a_n\}_{n=0}^{\infty}$ . Určete vytvořující funkci posloupnosti  $\{c_n\}_{n=0}^{\infty}$ , kde  $c_n = \sum_{i=1}^{n+1} i \cdot a_i, n \in N$ .

Řešení.

$\{c_n\}_{n=0}^{\infty}$  je zřejmě posloupnost částečných součtů posloupnosti  $\{(n+1)a_{n+1}\}_{n=0}^{\infty}$ , která má (viz výše uvedená tabulka) vytvořující funkci  $f'(x)$  a tedy  $f'(x)/(1-x)$  je uzavřený tvar hledané vytvořující funkce.

Následující tabulka obsahuje přehled vybraných posloupností a jim odpovídajících uzavřených tvarů (obyčejných) vytvořujících funkcí.

Posloupnost	Vytvořující funkce
$\{q^n\}_{n=0}^{\infty}$ (geometrická posloupnost)	$\frac{1}{1-qx}$
$\{1/n!\}_{n=0}^{\infty}$	$e^x$
$0, 1, 1/2, 1/3, \dots$	$-\ln(1-x)$
$0, 1, -1/2, 1/3, -1/4, 1/5, \dots$	$\ln(1+x)$
$\{n\}_{n=0}^{\infty}$	$\frac{x}{(1-x)^2}$
$\{n^2\}_{n=0}^{\infty}$	$\frac{x+x^2}{(1-x)^3}$
$\{n^3\}_{n=0}^{\infty}$	$\frac{x+4x^2+x^3}{(1-x)^4}$
$\{C_n^k\}_{k=0}^{\infty}, n \in Z$ (binomické koeficienty)	$(1+x)^n$
$\{\bar{C}_n^k\}_{k=0}^{\infty}, n \in Z$ (kombinace s opakováním)	$(1-x)^{-n}$
$\{F_n\}_{n=0}^{\infty}$ (Fibonacciho čísla)	$\frac{x}{1-x-x^2}$
$\{L_n\}_{n=0}^{\infty}$ (Lucasova čísla)	$\frac{2-x}{1-x-x^2}$
$\{C_n\}_{n=0}^{\infty}$ (Catalanova čísla)	$\frac{1-\sqrt{1-4x}}{2x}$
$a_{2n} = 0, a_{2n+1} = \frac{(-1)^n}{(2n+1)!}, n \in N$	$\sin x$
$a_{2n} = \frac{(-1)^n}{(2n)!}, a_{2n+1} = 0, n \in N$	$\cos x$

### Poznámky

Vytvořující funkce lze využít při řešení úloh o rozkladech. Zdůvodněte, že platí následující:

- Rozkladům množiny nerozlišitelných objektů do  $k$ -rozlišitelných tříd, kde třída může zůstat prázdná, odpovídá vytvořující funkce

$$f(x) = (1 + x + x^2 + \dots)^k = 1/(1-x)^k.$$



- Rozkladům množiny nerozlišitelných objektů do  $k$ -rozlišitelných tříd, kde  $i$ -tá třída obsahuje alespoň  $a_i$  objektů, odpovídá vytvořující funkce

$$f(x) = \prod_{i=1}^k (x^{a_i} + x^{a_i+1} + \dots) = x^{\sum_{i=1}^k a_i} / (1-x)^k.$$

- Rozkladům množiny nerozlišitelných objektů do  $k$ -rozlišitelných tříd, kde  $i$ -tá třída obsahuje alespoň  $a_i$  a nejvýše  $b_i$  objektů, odpovídá vytvořující funkce

$$f(x) = \prod_{i=1}^k (x^{a_i} + x^{a_i+1} + \dots + x^{b_i}) = x^{\sum_{i=1}^k a_i} / (1-x)^k \cdot \prod_{i=1}^k (1-x^{b_i-a_i+1}).$$

- Rozkladům přirozeného čísla  $n$  na kladné sčítance (tj. rozkladům nerozlišitelných objektů do nerozlišitelných tříd), odpovídá vytvořující funkce

$$f(x) = \prod_{i=1}^n \frac{1}{1-x^i}.$$

V případě, že sčítanci se nemohou opakovat, má vytvořující funkce tvar  $f(x) = \prod_{i=1}^n (1+x^i)$

- Rozkladům přirozeného čísla  $n$  na kladné sčítance rovné některým z čísel  $a_1, \dots, a_k$ , odpovídá vytvořující funkce

$$f(x) = \prod_{i=1}^k \frac{1}{1-x^{a_i}}.$$

V případě, že sčítanci se nemohou opakovat, má vytvořující funkce tvar  $f(x) = \prod_{i=1}^k (1+x^{a_i})$ .

Na závěr ještě poznamenejme, že kromě obyčejných vytvořujících funkcí existují i další typy vytvořujících funkcí. V následující části se stručně zmíníme o exponenciálních vytvořujících funkcích (nacházejí uplatnění např. v kombinatorických úlohách, kde záleží na pořadí, tj. v úlohách vedoucích na variace, resp. permutace).

#### Definice - exponenciální vytvořující funkce

Nechť  $\{a_n\}_{n=0}^{\infty}$  je reálná, resp. komplexní posloupnost. Algebraický výraz (formální mocninnou řadu)

$$f(x) = a_0 + a_1 \frac{x}{1!} + a_2 \frac{x^2}{2!} + \dots + a_n \frac{x^n}{n!} + \dots = \sum_{n=0}^{\infty} a_n \frac{x^n}{n!},$$

resp. jakýkoliv s ním ekvivalentní tvar, nazveme exponenciální vytvořující funkcí posloupnosti  $\{a_n\}_{n=0}^{\infty}$ .

#### Tvrzení

- a) Existuje vzájemně jednoznačný vztah mezi posloupností  $\{a_n\}_{n=0}^{\infty}$  a její exponenciální vytvořující funkcí  $f(x)$ . Platí totiž

$$a_n = f^{(n)}(0),$$

kde pravá strana označuje hodnotu  $n$ -té derivace funkce  $f(x)$  v bodě 0.

- b) Nechť  $f(x)$ , resp.  $g(x)$  jsou exponenciální vytvořující funkce posloupnosti  $\{a_n\}_{n=0}^{\infty}$ , resp.  $\{b_n\}_{n=0}^{\infty}$ . Potom exponenciální vytvořující funkce uvedené ve sloupci „Vytvořující funkce“ níže uvedené tabulky reprezentují posloupnosti uvedené ve sloupci „Posloupnost“.

Vytvořující funkce	Posloupnost
$\alpha f(x) + \beta g(x)$	$\{\alpha a_n + \beta b_n\}_{n=0}^{\infty}$
$f'(x)$	$a_1, a_2, a_3, \dots, a_n, \dots$ , tj. $\{a_{n+1}\}_{n=0}^{\infty}$
$\int_0^x f(t) dt$	$0, a_0, a_1, a_2, \dots, a_n, \dots$
$xf(x)$	$0, a_0, 2a_1, 3a_2, \dots, (n+1)a_n, \dots$

$x^k f(x)$	$\underbrace{0, \dots, 0}_{k \times 0}, C_{2k}^k a_0, C_{2k+1}^k a_1, C_{2k+2}^k a_2, \dots, C_{2k+n}^k a_n, \dots$
$f(x)g(x)$	$C_0^0 a_0 b_0, C_1^0 a_0 b_1 + C_1^1 a_1 b_0, C_2^0 a_0 b_2 + C_2^1 a_1 b_1 + C_2^2 a_2 b_0, \dots$ , tj. $\left\{ \sum_{i=0}^n C_n^i a_i b_{n-i} \right\}_{n=0}^{\infty}$

### Příklad

Nalezněte uzavřený tvar exponenciální vytvořující funkce posloupnosti subfaktoriálů  $\{D_n\}_{n=0}^{\infty}$ .

Řešení.

Jelikož

$$D_n = n! \left( \sum_{i=0}^n \frac{(-1)^i}{i!} \right) = \sum_{i=0}^n \frac{n!}{i!(n-i)!} \cdot (-1)^i \cdot (n-i)! = \sum_{i=0}^n C_n^i \cdot (-1)^i \cdot (n-i)!,$$

vidíme, že  $D_n$  je binomickou konvolucí posloupnosti  $\{(-1)^n\}_{n=0}^{\infty}$  mající exponenciální vytvořující funkci  $e^{-x}$  a posloupnosti  $\{n!\}_{n=0}^{\infty}$  s exponenciální vytvořující funkcí  $\frac{1}{1-x}$  a tedy uzavřený tvar exponenciální vytvořující funkce subfaktoriálů má tvar  $f(x) = e^{-x}/(1-x)$ .

Následující tabulka obsahuje přehled uzavřených tvarů exponenciálních vytvořujících funkcí několika vybraných posloupností.

Posloupnost	Exponenciální vytvořující funkce
$\{1\}_{n=0}^{\infty}$	$e^x$
$\{n\}_{n=0}^{\infty}$	$x e^x$
$\{A_n^k\}_{k=0}^n$	$(1+x)^n$
$\{D_n\}_{n=0}^{\infty}$	$\frac{e^{-x}}{1-x}$
$\left\{ \binom{0}{n}, \dots, \binom{n}{n}, \binom{n+1}{n}, \dots \right\}$	$\frac{(e^x - 1)^n}{n!}$
$\left[ \binom{0}{n}, \dots, \binom{n}{n}, \binom{n+1}{n}, \dots \right]$	$\frac{(-\ln(1-x))^n}{n!}$

### Příklad

Uvažujte řetězce nad abecedou  $\{a, b, c\}$ . Určete počet řetězců: a) délky 9, které obsahují lichý počet znaků  $a$  a současně alespoň jeden znak  $c$ . b) délky 10, které neobsahují žádný znak právě jednou.

Řešení.

ad a) Vytvořující funkce má zřejmě tvar

$$f(x) = \left( x + \frac{x^3}{3!} + \frac{x^5}{5!} + \dots \right) \left( 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \dots \right) \left( x + \frac{x^2}{2!} + \frac{x^3}{3!} + \dots \right),$$

kde první činitel reprezentuje výskyt znaku  $a$  (lichý počet), druhý činitel reprezentuje výskyt znaku  $b$  (bez omezení) a třetí činitel reprezentuje výskyt znaku  $c$  (alespoň jeden). Využitím obecně známého rozvoje  $e^{ax} = \sum_{n=0}^{\infty} a^n \frac{x^n}{n!}$  dostáváme

$$f(x) = \left( \frac{e^x - e^{-x}}{2} \right) \cdot e^x \cdot (e^x - 1) = \frac{1}{2} (e^{3x} - e^{2x} - e^x + 1).$$

Nyní určíme rozvinutý tvar

$$f(x) = \frac{1}{2} \left( \sum_{n=0}^{\infty} 3^n \frac{x^n}{n!} - \sum_{n=0}^{\infty} 2^n \frac{x^n}{n!} - \sum_{n=0}^{\infty} \frac{x^n}{n!} + 1 \right).$$

Hledaný počet řetězců tvoří koeficient u členu  $\frac{x^9}{9!}$ , tj.  $\frac{1}{2} (3^9 - 2^9 - 1^9) = 9\,585$ .

ad b) Vytvořující funkce má zřejmě tvar

$$f(x) = \left(1 + \frac{x^2}{2!} + \frac{x^3}{3!} + \dots\right)^3 = (e^x - x)^3 = e^{3x} - 3xe^{2x} + 3x^2e^x - x^3.$$

Nyní určíme rozvinutý tvar

$$\begin{aligned} f(x) &= \sum_{n=0}^{\infty} \frac{3^n x^n}{n!} - 3 \sum_{n=0}^{\infty} \frac{2^n x^{n+1}}{n!} + 3 \sum_{n=0}^{\infty} \frac{x^{n+2}}{n!} - x^3 = \\ &= \sum_{n=0}^{\infty} 3^n \frac{x^n}{n!} - 3 \sum_{n=1}^{\infty} 2^{n-1} n \frac{x^n}{n!} + 3 \sum_{n=2}^{\infty} n(n-1) \frac{x^n}{n!} - x^3. \end{aligned}$$

Hledaný počet řetězců tvoří koeficient u členu  $\frac{x^{10}}{10!}$ , tj.  $3^{10} - 3 \cdot 2^9 \cdot 10 + 3 \cdot 10 \cdot 9 = 43\,959$ .

#### 4.1. Řešení rekurentních vztahů metodou vytvořujících funkcí

V následující části bude popsán důležitý způsob využití vytvořujících funkcí při řešení rekurentních vztahů a jejich soustav. Cílem je nalézt explicitní vyjádření  $n$ -tého členu posloupnosti tvořící řešení rekurentního vztahu jako funkce  $n$ . Postup řešení popíšeme pro NHLR vztah (\*\*), přičemž analogicky postupujeme i v ostatních případech.

Označme  $\{a_n\}_{n=0}^{\infty}$  posloupnost, která je řešením zadaného NHLR vztahu (\*\*) a  $f(x)$  její vytvořující funkci.

1. Vynásobíme obě strany rekurentního vztahu nejvyšší mocninou  $x^{n+k}$ . Dostáváme rovnici, která je platná pro každé  $n \in \mathbb{N}$ , tj. dostáváme „nekonečně“ mnoho rovnic.
2. Nyní uvedené rovnice sčítáme přes  $n = 0, 1, \dots$ , čímž na levé straně získáme výrazy tvaru  $\sum_{n=0}^{\infty} a_{n+i} x^{n+i}$ , které vyjádříme pomocí symbolu pro vytvořující funkci, tj.  $f(x)$ . Dostáváme tak rovnici, jejíž neznámou je právě vytvořující funkce  $f(x)$  hledané posloupnosti.
3. Vyřešíme výše zmíněnou rovnici, čímž získáme uzavřený tvar vytvořující funkce  $f(x)$ .
4. Nalezneme rozvinutý tvar  $f(x)$ , přičemž koeficient u  $x^n$  je hledané explicitní vyjádření  $a_n$ .

##### Příklad

Vyřešte rekurentní vztah  $a_{n+2} = a_{n+1} + 2a_n + (-1)^n$ , kde  $a_0 = a_1 = 1$ .

Řešení.

Jde o nehomogenní lineární rekurentní vztah 2. řádu, který nejprve převedeme do tvaru

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

a obě strany vynásobíme  $x^{n+2}$  a následně sčítáme přes  $n = 0, 1, \dots$ . Dostáváme tak

$$\sum_{n=0}^{\infty} a_{n+2} x^{n+2} - x \sum_{n=0}^{\infty} a_{n+1} x^{n+1} - 2x^2 \sum_{n=0}^{\infty} a_n x^n = x^2 \sum_{n=0}^{\infty} (-x)^n.$$

Označíme-li vytvořující funkci hledané posloupnosti  $f(x) = \sum_{n=0}^{\infty} a_n x^n$  a nahradíme-li nekonečné součty, dostaneme rovnici

$$(f(x) - a_0 - a_1 x) - x(f(x) - a_0) - 2x^2 f(x) = \frac{x^2}{1+x}, \text{ tj. } f(x) - xf(x) - 2x^2 f(x) = \frac{x^2+x+1}{1+x}.$$

Jako řešení dostáváme uzavřený tvar vytvořující funkce hledané posloupnosti

$$f(x) = \frac{1+x+x^2}{(1+x)^2(1-2x)}.$$

Využitím rozkladu na parciální zlomky získáme tvar

$$f(x) = \frac{1}{3} \frac{1}{(1+x)^2} - \frac{1}{9} \frac{1}{1+x} + \frac{7}{9} \frac{1}{1-2x},$$

ze kterého snadno dostaneme rozvinutý tvar

$$f(x) = \frac{1}{3} \sum_{n=0}^{\infty} (-1)^n (n+1) x^n - \frac{1}{9} \sum_{n=0}^{\infty} (-1)^n x^n + \frac{7}{9} \sum_{n=0}^{\infty} 2^n x^n,$$

tj.

$$a_n = \frac{1}{9} [(-1)^n (2 + 3n) + 7 \cdot 2^n].$$

### Poznámka

Důležitým příkladem nelineárního rekurentního vztahu je rekurentní vztah, který definuje nám již známou Catalanovu posloupnost  $\{C_n\}_{n=0}^{\infty}$ . Při jeho odvození vyjdeme z interpretace, že  $C_n$  je rovno počtu způsobů jak správně uzavřít výraz  $x_0 \cdot \dots \cdot x_n$ . Všechny způsoby uzavřování rozdělíme do tříd podle toho, který součin je realizován (tedy uzavřován) jako poslední (označíme ho symbolem  $*$ ). Dostáváme tak  $(n - 1)$  tříd, které odpovídají následujícím schémataům uzavřování:

1. třída:  $((x_0) * (x_1 \cdot \dots \cdot x_n))$  ... celkem  $C_0 C_{n-1}$  způsobů uzavřování,
2. třída:  $((x_0 \cdot x_1) * (x_2 \cdot \dots \cdot x_n))$  ... celkem  $C_1 C_{n-2}$  způsobů uzavřování,
- ⋮
- $(n - 1)$ . třída:  $((x_0 \cdot \dots \cdot x_{n-1}) * (x_n))$  ... celkem  $C_{n-1} C_0$  způsobů uzavřování,

tedy

$$C_n = C_0 C_{n-1} + C_1 C_{n-2} + \dots + C_{n-1} C_0, \text{ resp. } C_{n+1} = C_0 C_n + C_1 C_{n-1} + \dots + C_n C_0, \text{ kde } C_0 = 1.$$

K vyřešení uvedeného rekurentního vztahu použijeme metodu vytvořujících a označíme  $f(x) = \sum_{n=0}^{\infty} C_n x^n$ . Dostáváme tak

$$\sum_{n=0}^{\infty} C_{n+1} x^{n+1} = x \sum_{n=0}^{\infty} (C_0 C_n + C_1 C_{n-1} + \dots + C_n C_0) x^n,$$

tedy (výraz v závorce na pravé straně rovnosti je  $n$ -tý člen konvoluce posloupnosti  $\{C_n\}_{n=0}^{\infty}$  sama se sebou)

$$f(x) - C_0 = x f^2(x)$$

a jako řešení dostáváme dvě funkce (jde o kvadratickou rovnici)

$$f(x) = \frac{1 \pm \sqrt{1-4x}}{2x},$$

z nichž je samozřejmě pouze jedna vytvořující funkcí Catalanovy posloupnosti. Vzhledem k tomu, že musí platit  $\lim_{x \rightarrow 0} f(x) = C_0 = 1$  dostáváme uzavřený tvar

$$f(x) = \frac{1 - \sqrt{1-4x}}{2x}.$$

Z uvedeného uzavřeného tvaru  $f(x)$  je zřejmé, že  $C_n$  je až na multiplikativní konstantu  $(-1/2)$  rovno koeficientu u  $x^{n+1}$  v rozvoji  $\sqrt{1-4x}$  a je zřejmě roven (viz Newtonův vzorec)

$$C_n = \left(-\frac{1}{2}\right) \frac{\frac{1}{2}(\frac{1}{2}-1) \dots (\frac{1}{2}-n)}{(n+1)!} (-4)^{n+1},$$

což po snadné úpravě dává nám již známý tvar  $C_n = \frac{1}{n+1} C_{2n}^n$ .

### Poznámka

Metodu vytvořujících funkcí lze využít i k řešení soustav rekurentních vztahů, přičemž postup je zcela analogický případu řešení jednoho rekurentního vztahu. Zjednodušeně řečeno, každý rekurentní vztah soustavy vynásobíme výrazem  $x^{n+k}$  s vhodným  $k$  a následně sčítáme přes  $n = 0, 1, \dots$ . Nekonečné součty obsahující členy hledaných posloupností vyjádříme pomocí symbolů jejich vytvořujících funkcí, čímž dostaneme soustavu rovnic, kde neznámé jsou právě vytvořující funkce hledaných posloupností. Vyřešením soustavy dostaneme uzavřené tvary vytvořujících funkcí. Na závěr pak nalezneme jejich rozvinutý tvar.

### Příklad

Nalezněte řešení soustavy rekurentních vztahů  $a_{n+1} = 2a_n + b_n$ ,  $b_{n+1} = 3a_n$ , kde  $a_0 = 1$ ,  $b_0 = 2a_0$ .  
Řešení.

Jde o soustavu dvou lineárních homogenních rekurentních vztahů 1. řádu.

Vynásobením obou vztahů soustavy výrazem  $x^{n+1}$  a součtováním dostáváme

$$\sum_{n=0}^{\infty} a_{n+1} x^{n+1} - 2x \sum_{n=0}^{\infty} a_n x^n - x \sum_{n=0}^{\infty} b_n x^n = 0 \text{ a } -3x \sum_{n=0}^{\infty} a_n x^n + \sum_{n=0}^{\infty} b_{n+1} x^{n+1} = 0.$$

Označme-li  $f(x) = \sum_{n=0}^{\infty} a_n x^n$ ,  $g(x) = \sum_{n=0}^{\infty} b_n x^n$ , dostáváme

$$(f(x) - a_0) - 2xf(x) - xg(x) = 0 \text{ a } -3xf(x) + (g(x) - b_0) = 0$$

Po úpravě získáme lineární nehomogenní soustavu dvou rovnic o neznámých  $f(x)$ ,  $g(x)$  a s maticí soustavy

$$\begin{pmatrix} 1-2x & -x \\ -3x & 1 \end{pmatrix} \begin{pmatrix} f(x) \\ g(x) \end{pmatrix} = \begin{pmatrix} a_0 \\ b_0 \end{pmatrix}.$$

Soustavu vyřešíme např. Cramerovým pravidlem, dále využijeme rozklad na parciální zlomky. Dostáváme tak

$$f(x) = \frac{1+2x}{(1+x)(1-3x)} = -\frac{1}{4} \frac{1}{1+x} + \frac{5}{4} \frac{1}{1-3x}, \quad g(x) = \frac{2-x}{(1+x)(1-3x)} = \frac{3}{4} \frac{1}{1+x} + \frac{5}{4} \frac{1}{1-3x}.$$

Jako řešení pak dostáváme

$$a_n = \left(-\frac{1}{4}\right)(-1)^n + \frac{5}{4}3^n, \quad b_n = \frac{3}{4}(-1)^n + \frac{5}{4}3^n.$$

## 4.2. Věžové polynomy

Důležitým typem úloh (pro pochopení některých kombinatorických principů, ale i z hlediska aplikačního) jsou úlohy na šachovnici. Jedna třída těchto úloh souvisí s problematikou rozmístování figur na šachovnici tak, že se vzájemně (ne)ohrožují, další pak souvisí s pohybem figur po šachovnici. V následující části se stručně zaměříme na úlohy související s rozmístováním věží na šachovnici.

**Definice** - šachovnice

Šachovnicí typu  $(m, n)$ , kde  $m, n \in \mathbb{N}^+$ , rozumíme obdélníkové schéma skládající se z  $m \cdot n$  čtvercových polí uspořádaných do  $m$  řádků a  $n$  sloupců. Na šachovnici mohou existovat tzv. zakázaná pole (ostatní pole označujeme jako povolená nebo také přípustná). Šachovnici budeme značit symbolem  $C$ , resp.  $C_1, C_2, \bar{C}$  apod.

Základní úlohu lze nyní formulovat následovně – určete, kolika různými způsoby lze na přípustná pole dané šachovnice  $C$  rozmístit  $k$  nerozlišitelných věží tak, že se vzájemně neohrožují<sup>2</sup> (tj. žádné dvě věže nestojí ve stejném řádku ani sloupci a současně nestojí na zakázaných polích).

**Definice** - věžový polynom (rook polynomial)

Nechť  $C$  je šachovnice typu  $(m, n)$ . Věžovým polynomem šachovnice  $C$  rozumíme polynom

$$r(x; C) = r_0(C) + r_1(C)x + r_2(C)x^2 + \dots + r_l(C)x^l,$$

kde  $l = \min\{m, n\}$  a

$r_k(C)$  je počet, kolika způsoby lze na přípustná pole šachovnice  $C$  rozmístit  $k$  nerozlišitelných věží tak, že se neohrožují.

**Poznámky**

- Uvědomme si, že věžový polynom je obyčejná vytvořující funkce posloupnosti koeficientů  $\{r_i(C)\}_{i=0}^{\min\{m,n\}}$  a lze tak využívat poznatky z kapitoly o vytvořujících funkcích.
- Snadno nahlédneme, že z požadavku „věže se nesmí ohrožovat“ vyplývá, že na šachovnici typu  $(m, n)$  nelze umístit více věží než je  $\min\{m, n\}$ , a to bez ohledu na případnou existenci zakázaných polí. Odtud  $r_i(C) = 0$  pro  $i > \min\{m, n\}$ .
- Pro libovolnou šachovnici zřejmě platí  $r_0(C) = 1$  a  $r_1(C) =$  počet přípustných polí. Při výpočtu ostatních koeficientů  $r_k(C)$  využíváme následující pravidla.
- Zřejmou (a mnohdy využívanou) vlastností věžových polynomů je, že jsou invariantní vzhledem k permutacím řádků, resp. sloupců šachovnice.

<sup>2</sup> Nejde o hru v šachy, ve které se věže stejné barvy (tj. nerozlišitelné) neohrožují.

### Pravidlo 1

Nechť  $C$  je šachovnice, která se skládá z podšachovnic  $C_1, C_2$ , které jsou řádkově i sloupcově disjunktní, tj. žádné povolené pole podšachovnice  $C_1$  neleží ve stejném řádku ani sloupci jako povolené pole podšachovnice  $C_2$ . Potom pro koeficienty  $r_k(C)$  platí

$$r_k(C) = \sum_{i=0}^k r_i(C_1)r_{k-i}(C_2),$$

resp. pro věžový polynom  $r(x; C)$  platí

$$r(x; C) = r(x; C_1)r(x; C_2).$$

Důkaz.

Vzhledem k tomu, že  $C_1, C_2$ , jsou řádkově i sloupcově disjunktní je zřejmé, že žádná věž umístěná na  $C_1$  se neohrožuje s žádnou věží umístěnou na  $C_2$ . Odtud dostáváme vztah pro koeficient  $r_k(C)$ . Nyní si stačí uvědomit, že  $r_k(C)$  je konvolucí koeficientů příslušných podšachovnicím  $C_1, C_2$  a tedy  $r(x; C)$  je součinem věžových polynomu podšachovnic.

### Poznámka

Pravidlo 1 lze zobecnit na případ více podšachovnic: jsou-li  $C_1, \dots, C_h$  po dvou disjunktní (tj. každá dvojice různých podšachovnic je disjunktní ve smyslu výše uvedeného pravidla) podšachovnice šachovnice  $C$ , potom

$$r(x; C) = \prod_{i=1}^h r(x; C_i).$$

Vzhledem k tomu, že předpokladem výše uvedeného pravidla je disjunktnost podšachovnic (po dvou), je třeba si umět poradit i v případě, že předpoklad splněn není. V této situaci využijeme tzv. faktorizaci popsanou v následujícím pravidle 2.

### Pravidlo 2

Nechť  $C$  je šachovnice,  $p$  libovolné její přípustné pole,  $C_1$  je podšachovnice vzniklá z  $C$  vynecháním pole  $p$  a  $C_2$  je podšachovnice vzniklá z  $C$  vynecháním řádku a sloupce, v jejichž průsečíku leží pole  $p$ . Potom pro koeficienty  $r_k(C)$  platí

$$r_k(C) = r_k(C_1) + r_{k-1}(C_2),$$

resp. pro věžový polynom  $r(x; C)$  platí

$$r(x; C) = r(x; C_1) + x \cdot r(x; C_2).$$

Důkaz.

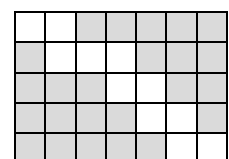
Je-li  $p$  zvolené přípustné pole, máme pouze dvě možnosti - buď na  $p$  věž neumístíme (tj. pole vynecháme), nebo umístíme (tj. vynecháme příslušný řádek a sloupec). Odtud platnost prvního dokazovaného vztahu pro  $r_k(C)$ . Nyní stačí na již dokázaný rekurentní vztah aplikovat metodu vytvořujících funkcí, tj. obě strany vynásobit  $x^k$  a sčítat přes  $k = 0, \dots, \min\{m, n\}$ . Odtud dostáváme platnost druhého vztahu týkajícího se věžových polynomů.

### Poznámka

Jako pole  $p$  zmíněné v pravidle 2 lze zvolit libovolné přípustné pole, nicméně některá pole mohou být vhodnější než jiná (např. pokud odstraněním zvoleného pole vzniknou disjunktní podšachovnice).

### Příklad

Sestavte věžový polynom pro zobrazenou šachovnici (zakázaná políčka jsou šedá).



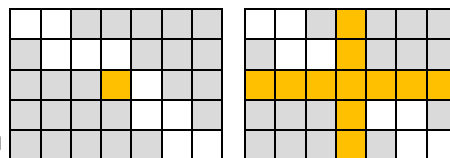
Řešení.

Aplikujeme pravidlo 2 a za pole  $p$  zvolíme průnik 3. řádku a 4. sloupce (toto pole rozdělí šachovnici na dvě disjunktní podšachovnice).

Dostáváme tak

$$r(x; C) = r(x; C_1) + x \cdot r(x; C_2),$$

kde podšachovnice  $C_1, C_2$  jsou znázorněny na vedlejším obrázku (vynechané pole u  $C_1$  i sloupce/řádky u  $C_2$  jsou zbarvená okrově).



Podšachovnice  $C_1$  se skládá ze dvou disjunktních podšachovnic malého rozměru, pro které snadno sestavíme příslušný věžový polynom (jinak bychom na  $C_1$  opět aplikovali výše uvedená pravidla)

$$r(x; C_1) = (1 + 5x + 5x^2)(1 + 5x + 6x^2 + x^3) = 1 + 10x + 36x^2 + 56x^3 + 35x^4 + 5x^5.$$

Podšachovnice  $C_2$  se skládá také ze dvou disjunktních podšachovnic malého rozměru a tedy snadno sestavíme příslušný věžový polynom (jinak bychom na  $C_2$  opět aplikovali výše uvedená pravidla)

$$r(x; C_2) = (1 + 4x + 3x^2)^2 = 1 + 8x + 22x^2 + 24x^3 + 9x^4.$$

Jako věžový polynom původní šachovnice tak dostáváme

$$r(x; C) = (1 + 10x + 36x^2 + 56x^3 + 35x^4 + 5x^5) + x(1 + 8x + 22x^2 + 24x^3 + 9x^4),$$

tj.

$$r(x; C) = 1 + 11x + 44x^2 + 78x^3 + 59x^4 + 14x^5.$$

### Poznámka

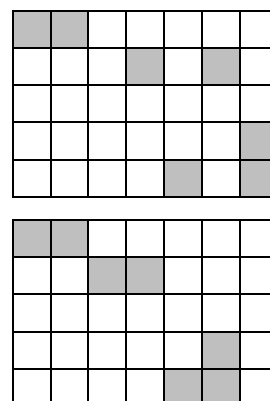
V některých situacích nás zajímá hodnota pouze jednoho koeficientů  $r_k(C)$  a je proto zbytečné počítat věžový polynom. V tomto případě se kromě uvedených pravidel 1 a 2 užívá (zejména v situaci, kdy zakázaných polí je málo, resp. mají jednoduchou strukturu) i princip inkluze a exkluze.

### Příklad

Určete, kolika různými způsoby lze na danou šachovnici rozmístit maximální možný počet věží tak, že se neohrožují a nestojí na zakázaných (šedých) polích.

Řešení.

Na přípustná pole dané šachovnice lze zřejmě rozmístit maximálně 5 neohrožujících se věží, tedy hledáme  $r_5(C)$ . Pro větší přehlednost provedeme transpozici 3. a 6. sloupce 6. a 7. sloupce (věžový polynom je invariantní na permutace sloupců/řádků). Tím dostáváme šachovnici, ze které je patrné, že zakázaných polí je málo a navíc mají jednoduchou strukturu. Z tohoto důvodu je efektivnější využít princip inkluze a exkluze a vyjádřit počet rozmístění na přípustná pole pomocí rozmístování věží na zakázaná pole.



Označíme-li  $\bar{C}$  šachovnici zakázaných polí, vidíme, že se skládá ze tří po dvou disjunktních podšachovnic  $\bar{C}_1, \bar{C}_2, \bar{C}_3$ , tedy

$$r(x; \bar{C}) = r(x; \bar{C}_1)r(x; \bar{C}_2)r(x; \bar{C}_3) = (1 + 2x)^2(1 + 3x + x^2) = 1 + 7x + 17x^2 + 16x^3 + 4x^4.$$

Připomeňme, že koeficient u  $x^k$  polynomu  $r(x; \bar{C})$  je počet, kolika způsoby lze na zakázaná pole zadané šachovnice rozmístit  $k$  věží tak, že se neohrožují. Nyní použijeme princip inkluze a exkluze. Dostáváme

$$r_5(C) = N - \sum_{i=1}^5 N(\alpha_i) + \sum_{1 \leq i_1 < i_2 \leq 5} N(\alpha_{i_1}, \alpha_{i_2}) - \sum_{1 \leq i_1 < i_2 < i_3 \leq 5} N(\alpha_{i_1}, \alpha_{i_2}, \alpha_{i_3}) + \sum_{1 \leq i_1 < i_2 < i_3 < i_4 \leq 5} N(\alpha_{i_1}, \alpha_{i_2}, \alpha_{i_3}, \alpha_{i_4}) - \sum_{1 \leq i_1 < i_2 < i_3 < i_4 < i_5 \leq 5} N(\alpha_{i_1}, \alpha_{i_2}, \alpha_{i_3}, \alpha_{i_4}, \alpha_{i_5}),$$

kde  $N = r_0(\bar{C}) \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 = 2520$  ... počet všech rozmístění 5 neohrožujících se věží (bez omezení zakázanými poli);

$$\sum_{i=1}^5 N(\alpha_i) = r_1(\bar{C}) \cdot 6 \cdot 5 \cdot 4 \cdot 3 = 2520$$
 ... počet rozmístění 5 neohrožujících se věží tak, že 1 stojí na zakázaném poli, zbylé 4 bez omezení;

$$\sum_{1 \leq i_1 < i_2 \leq 5} N(\alpha_{i_1}, \alpha_{i_2}) = r_2(\bar{C}) \cdot 5 \cdot 4 \cdot 3 = 1020$$
 ... počet rozmístění 5 neohrožujících se věží tak, že 2 stojí na zakázaných polích, zbylé 3 bez omezení;

$\sum_{1 \leq i_1 < i_2 < i_3 \leq 5} N(\alpha_{i_1}, \alpha_{i_2}, \alpha_{i_3}) = r_3(\bar{C}) \cdot 4 \cdot 3 = 192$  ... počet rozmístění 5 neohrožujících se věží tak,  
že 3 stojí na zakázaných polích, zbylé 2 bez omezení;

$\sum_{1 \leq i_1 < i_2 < i_3 < i_4 \leq 5} N(\alpha_{i_1}, \alpha_{i_2}, \alpha_{i_3}, \alpha_{i_4}) = r_4(\bar{C}) \cdot 3 = 12$  ... počet rozmístění 5 neohrožujících se věží tak,  
že 4 stojí na zakázaných polích, zbývající 1 bez omezení;

$\sum_{1 \leq i_1 < i_2 < i_3 < i_4 < i_5 \leq 5} N(\alpha_{i_1}, \alpha_{i_2}, \alpha_{i_3}, \alpha_{i_4}, \alpha_{i_5}) = r_5(\bar{C}) \cdot 1 = 0$  ... počet rozmístění 5 neohrožujících se  
věží tak, že všechny stojí na zakázaných polích, zbývajících 0 bez omezení;

tj.

$$r_5(C) = 2520 - 2520 + 1020 - 192 + 12 - 0 = 840.$$



## 5. Burnside/Pólyaova enumerační metoda

Burnside/Pólyaova enumerační metoda je nástroj, který umožňuje určit počet různých „konfigurací“ objektů, u kterých je třeba brát v úvahu jejich symetrie (rovinné, prostorové, ...). Nachází uplatnění např. při určení počtu izomérů chemických sloučenin, při určení počtu obarvení různých objektů apod.

Před studiem této kapitoly si ještě připomeněte základní pojmy a fakta o grupách, zejména o symetrických grupách.

### 5.1. Permutace, symetrická grupa

**Definice** (permutace)

Nechť  $A$  je  $n$ -prvková množina, tj.  $|A| = n$ . Potom permutací na množině  $A$  rozumíme libovolné vzájemně jednoznačné zobrazení  $A$  na  $A$ .

**Poznámky**

- Permutací na množině  $A$  lze interpretovat jako uspořádání prvků množiny  $A$ , přesněji jako libovolnou uspořádanou  $n$ -tici tvořenou právě všemi prvky množiny  $A$ .
- Permutace budeme značit symboly  $\pi, \rho, \sigma, \dots$  a pro jejich zápis budeme využívat nejprve tzv. dvouřádkový zápis, později zápis ve tvaru součinu (obvykle disjunktních) cyklů.

Dvouřádkový zápis permutace na množině  $A = \{1, 2, \dots, n\}$  má tvar

$$\pi = \begin{pmatrix} 1 & 2 & \dots & n \\ \pi(1) & \pi(2) & \dots & \pi(n) \end{pmatrix},$$

kde horní řádek obsahuje vzory a dolní řádek obsahuje jim odpovídající obrazy. Je zřejmé, že při zápisu permutace není podstatné pořadí sloupců, podstatné je pouze přiřazení obrazů vzorům. Z tohoto pohledu např. zápisy  $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 2 & 5 & 1 \end{pmatrix}$  a  $\begin{pmatrix} 3 & 1 & 5 & 2 & 4 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix}$  definují stejnou permutaci.

Označíme-li  $S_n$  množinu všech permutací na  $n$ -prvkové množině, lze na  $S_n$  definovat operaci násobení permutací  $\pi, \rho \in S_n$  jako skládání zobrazení, tj. následovně:

$$\pi\rho = \begin{pmatrix} 1 & 2 & \dots & n \\ \rho(\pi(1)) & \rho(\pi(2)) & \dots & \rho(\pi(n)) \end{pmatrix}.$$

Je-li např.  $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 1 & 2 & 4 \end{pmatrix}$ ,  $\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 5 & 4 & 3 \end{pmatrix}$ , dostáváme  $\pi\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 2 & 1 & 4 \end{pmatrix}$ ,  $\rho\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 2 & 1 \end{pmatrix}$ .

Nyní snadno ověříme (permutace je vzájemně jednoznačné zobrazení), že  $(S_n, \cdot)$  je grupa, tj. platí:

$$\text{i) } \forall \pi, \rho, \tau \in S_n \quad (\pi \cdot \rho) \cdot \tau = \pi \cdot (\rho \cdot \tau), \quad (\text{asociativita})$$

$$\text{ii) } \exists id \in S_n \quad \forall \pi \in S_n \quad id \cdot \pi = \pi \cdot id = \pi, \quad (\text{existence jednotkového prvku})$$

$$\text{iii) } \forall \pi \in S_n \quad \exists \pi^{-1} \in S_n \quad \pi \cdot \pi^{-1} = \pi^{-1} \cdot \pi = id. \quad (\text{existence inverzního prvku})$$

Konkrétně  $id = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}$  a je-li  $\pi = \begin{pmatrix} 1 & 2 & \dots & n \\ \pi(1) & \pi(2) & \dots & \pi(n) \end{pmatrix}$ , potom  $\pi^{-1} = \begin{pmatrix} \pi(1) & \pi(2) & \dots & \pi(n) \\ 1 & 2 & \dots & n \end{pmatrix}$ .

Např. pro  $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 2 & 5 & 1 \end{pmatrix}$  dostáváme  $\pi^{-1} = \begin{pmatrix} 4 & 3 & 2 & 5 & 1 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 2 & 1 & 4 \end{pmatrix}$ .

**Definice** (symetrická/permutační grupa)

Grupu  $(S_n, \cdot)$  nazýváme symetrickou grupou na  $n$ -prvkové množině. Každou podgrupu grupy  $(S_n, \cdot)$  nazýváme permutační grupou.

## Poznámka

Symetrická grupa  $(S_n, \cdot)$  je řádu  $n!$  a pro  $n \geq 3$  není komutativní.

## Definice - cyklus

Řekneme, že permutace  $\pi \in (S_n, \cdot)$  je cyklus délky  $k$ , jestliže:

- i)  $\exists \{i_1, \dots, i_k\} \subseteq \{1, \dots, n\}$  taková, že  $\forall j \in \{1, \dots, k-1\} [\pi(i_j) = i_{j+1}] \wedge [\pi(i_k) = i_1]$ ,
- ii)  $\forall i \notin \{i_1, \dots, i_k\} \pi(i) = i$ .

V tomto případě píšeme  $\pi = (i_1, \dots, i_k)$ . Speciálně, cyklus délky 2 se nazývá transpozice.

Např. permutace  $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 7 & 3 & 2 & 4 & 6 & 8 & 1 \end{pmatrix}$  je cyklus délky 6 a zapisujeme ho  $\pi = (1,5,4,2,7,8)$ , resp. obširněji  $\pi = (1,5,4,2,7,8)(3)(6)$ .

## Poznámky

- Je dobré si uvědomit, že z definice cyklu vyplývá, že jeho zápis není jednoznačný. Lze ho totiž interpretovat jako umístění prvků uspořádané  $k$ -tice  $(i_1, \dots, i_k)$  na kružnici. Zjednodušeně řečeno, nezáleží na tom, kde cyklus začíná, ale na tom, jaký prvek následuje za daným prvkem při pohybu (např. ve směru hodinových ručiček) po kružnici. Z tohoto pohledu např. platí  $(1,5,4,2,7,8) = (8,1,5,4,2,7) = (7,8,1,5,4,2) = (2,7,8,1,5,4) = (4,2,7,8,1,5) = (5,4,2,7,8,1)$ .
- Cyklus je speciální permutace a proto lze cykly násobit.  
Např.  $(1,5,3,2)(4,3) = (1,5,4,3,2)$ , kdežto  $(4,3)(1,5,3,2) = (1,5,3,4,2)$ .
- Řekneme, že cykly  $\pi, \rho \in S_n$ , kde  $\pi = (i_1, \dots, i_k), \rho = (j_1, \dots, j_l)$  jsou disjunktní, jestliže  $\{i_1, \dots, i_k\} \cap \{j_1, \dots, j_l\} = \emptyset$ .  
S výhodou se využívá zřejmá skutečnost, že součin disjunktních cyklů je komutativní!

## Tvrzení

- i) Každou permutaci lze zapsat, až na pořadí jednoznačně, ve tvaru součinu disjunktních cyklů.
- ii) Každý cyklus lze zapsat ve tvaru součinu transpozic s tím, že toto vyjádření není jednoznačné, ale platí, že každou permutaci lze zapsat vždy jako součin pouze sudého, nebo pouze lichého počtu transpozic.

## Poznámky

- Identická permutace  $id \in S_n$  má jako součin disjunktních cyklů zápis  $id = (1)(2) \dots (n)$ .
- Je-li  $\pi = (i_1, i_2, \dots, i_{k-1}, i_k)$  cyklus, potom  $\pi^{-1}$  je také cyklus a má tvar  $\pi^{-1} = (i_k, i_{k-1}, \dots, i_2, i_1)$ . Např.  $(1,5,4,3,2)^{-1} = (2,3,4,5,1)$ . Navíc, každá transpozice je zřejmě inverzní sama k sobě, tedy  $(i_1, i_2)^{-1} = (i_1, i_2)$ .
- Cyklus  $(i_1, i_2, i_3, \dots, i_k)$  lze zapsat ve tvaru součinu transpozic následovně  $(i_1, i_2, i_3, \dots, i_k) = (i_1, i_2)(i_1, i_3) \cdot \dots \cdot (i_1, i_k)$ .
- Je-li  $\pi$  permutace zapsaná ve tvaru disjunktních cyklů, potom inverzní permutace  $\pi^{-1}$  má tvar součinu inverzních cyklů tvořících permutaci  $\pi$  (vzhledem k jejich disjunktnosti nezáleží na jejich pořadí).  
Např. pro  $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 5 & 2 & 6 & 7 & 4 & 3 & 1 & 8 \end{pmatrix} = (198)(2573)(46)$  dostáváme  $\pi^{-1} = (891)(3752)(46)$ .

## Definice – sudá, lichá permutace

Permutaci nazveme sudou, jestliže ji lze zapsat ve tvaru součinu sudého počtu transpozic. Ostatní permutace nazýváme liché.

## Poznámky

- Snadno se přesvědčíme, že součin sudých permutací je opět sudá permutace, inverzní permutace k sudé je také sudá a identita je sudá (0 transpozic). Označíme-li tedy  $A_n$  množinu všech sudých permutací na  $n$ -prvkové množině, je zřejmé, že  $A_n$  je uzavřená vzhledem k násobení permutací a tedy  $(A_n, \cdot) \cong (S_n, \cdot)$ . Grupa  $(A_n, \cdot)$  se nazývá alternující grupa, je řádu  $n!/2$  (polovina permutací je sudých a polovina lichých) a pro  $n \geq 4$  je nekomutativní.
- Důležité příklady permutačních grup jsou tzv. dihedralní grupy  $D_n, n \geq 2$ , které popisují prostorové symetrie pravidelných  $n$ -úhelníků (jejich vrcholy pro tyto účely očíslovíme  $1, \dots, n$ ). Dihedralní grupa  $D_n$  je řádu  $2n$  (obsahuje  $n$  otočení a  $n$  osových symetrií).
- Symetrie obdélníka (vrcholy číslováme  $1, 2, 3, 4$ ) tvoří tzv. Kleinovu čtyřgrupu (Felix Klein, 1849-1925). Obsahuje následující permutace:
  - (13)(24) ... otočení o  $180^\circ$ ,
  - (1)(2)(3)(4) ... otočení o  $360^\circ$ ,
  - (12)(34) ... překlopení kolem osy procházející středy stran 12 a 34,
  - (14)(23) ... překlopení kolem osy procházející středy stran 14 a 23.

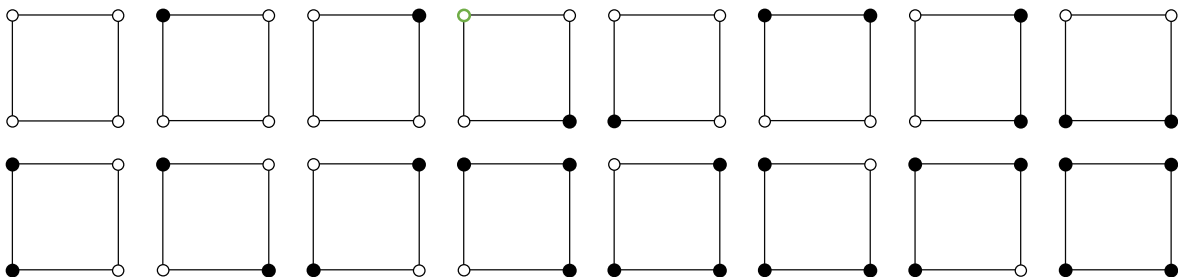
## Příklad

Určete, kolika různými způsoby lze obarvit vrcholy čtverce pomocí nejvýše 2 zadaných barev.

Řešení.

Nejprve je nutné vymežit formulaci „obarvit pomocí nejvýše 2 barev“.

Pod obarvením pomocí nejvýše 2 barev rozumíme, že kterýkoliv vrchol čtverce bude obarven právě jednou ze dvou zadaných barev a to bez ohledu na obarvení ostatních vrcholů. Připouštíme tak i situaci, kdy všechny vrcholy budou obarveny stejnou barvou. Všechny možnosti obarvení vrcholů čtverce pomocí nejvýše 2 barev (bílá, černá), jsou zobrazeny níže.



Nyní je třeba vyjasnit formulaci „různé způsoby obarvení“. Uvažujeme-li čtverec umístěný v rovině, potom je zřejmé, že např. 2., 3., 4. a 5. čtverec 1. řádku se liší pouhým otočením (o  $90^\circ$ ,  $180^\circ$ ,  $270^\circ$ , resp.  $360^\circ$ ) a je proto rozumné je považovat za stejně obarvené. Analogicky 6., 7. 8. čtverec 1. řádku a 1. čtverec 2. řádku, dále 2. a 3. čtverec 2. řádku, resp. 4., 5. 6. a 7. čtverec 2. řádku se liší pouhým otočením. Celkem tak dostáváme 6 různých obarvení vrcholů čtverce nejvýše 2 barvami.

Uvědomme si, že při vymezení pojmu různá obarvení čtverce hrají důležitou roli jeho symetrie, tj. takové transformace čtverce, které ho „nemění“ (např. otočení o  $90^\circ$ ).

## Příklad

Určete: a) 2D symetrie čtverce, b) 3D symetrie čtverce.

Řešení.

Vrcholy čtverce postupně očíslováme  $1, 2, 3, 4$ .

ad a) 2D symetrie čtverce odpovídají postupnému otáčení o  $90^\circ$  a lze je proto popsat následujícími permutacemi: (1234) ... otočení o  $90^\circ$  (13)(24) ... otočení o  $180^\circ$

(1432) ... otočení o 270° (1)(2)(3)(4) ... otočení o 360°

Odtud  $P_{2D} = \{(1)(2)(3)(4), (1234), (13)(24), (1432)\}$ .

ad b) 3D symetriím čtverce (tvoří tzv. dihedrální grupa  $D_4$ ) odpovídají, kromě jeho 2D symetrií, ještě 4 osové symetrie, které lze popsat následujícími permutacemi:

(12)(34) ... překlopení kolem osy procházející středy stran 1-2 a 3-4,

(14)(23) ... překlopení kolem osy procházející středy stran 1-4 a 2-3,

(1)(24)(3) ... překlopení kolem osy procházející vrcholy 1 a 3,

(13)(2)(4) ... překlopení kolem osy procházející vrcholy 2 a 4.

Odtud

$P_{3D} = \{(1)(2)(3)(4), (1234), (13)(24), (1432), (12)(34), (14)(23), (1)(24)(3), (13)(2)(4)\}$ .

Řádně zdůvodněte, že množiny  $G_{2D}, G_{3D}$  tvoří permutační grupy (podgrupy  $(S_4, \cdot)$ ), navíc  $G_{2D} \subseteq G_{3D}$ .

Nyní výše prezentovaný přístup zobecníme a formalizujeme.

**Definice** (cycle-structure, cycle-index polynom)

Nechť  $G = (N, P)$ <sup>3</sup> je permutační grupa na množině  $N = \{1, \dots, n\}$ .

a) Je-li  $\pi \in G$ , potom symbolem  $\text{cyc\_str}(\pi)$  označujeme formální výraz (tzv. „cycle-structure“) popisující strukturu disjunktních cyklů permutace  $\pi$  (tj. délku a jejich počet). Definujeme ho vztahem

$$\text{cyc\_str}(\pi) = x_1^{\alpha_1} \cdot \dots \cdot x_n^{\alpha_n},$$

kde  $x_i$  reprezentuje cyklus délky  $i$  a

$\alpha_i$  je počet cyklů délky  $i$ .

b) Symbolem  $P_G(x_1, x_2, \dots, x_n)$  označujeme tzv. cycle-index polynom permutační grupy  $G$  a definujeme ho vztahem

$$P_G(x_1, x_2, \dots, x_n) = \frac{1}{|G|} \sum_{\pi \in P} \text{cyc\_str}(\pi),$$

kde  $|G|$  označuje řád (počet prvků) permutační grupy.

(vzhledem k tomu, že dosud není ustálena vhodná česká terminologie, budeme používat „anglickou terminologii“, tj. cycle-structure a cycle-index polynom)

### Příklad

Určete cycle-index polynom a) 2D symetrií čtverce, b) 3D symetrií čtverce.

Řešení.

Vzhledem k výše uvedenému příkladu hned dostáváme:

a)  $\text{cyc\_str}((1)(2)(3)(4)) = x_1^4$ ,  $\text{cyc\_str}((13)(24)) = x_2^2$ ,  $\text{cyc\_str}(1234) = \text{cyc\_str}(1432) = x_4$ , tedy

$$P_{2D}(x_1, x_2, x_3, x_4) = \frac{1}{4}(x_1^4 + x_2^2 + 2x_4).$$

b)  $\text{cyc\_str}((12)(34)) = \text{cyc\_str}((14)(23)) = x_2^2$ ,  $\text{cyc\_str}((1)(24)(3)) = \text{cyc\_str}(13)(2)(4) = x_1^2 x_2$ , tedy

$$P_{3D}(x_1, x_2, x_3, x_4) = \frac{1}{8}(x_1^4 + 2x_1^2 x_2 + 3x_2^2 + 2x_4).$$

### Tvrzení

Nechť  $N = \{1, \dots, n\}$  je množina reprezentující  $n$ -prvkový objekt, jehož symetrie jsou definovány permutační grupou  $G = (N, P)$ . Potom počet různých obarvení daného  $n$ -prvkového objektu pomocí nejvýše  $m$  barev, je rovno hodnotě cycle-index polynomu  $P_G(x_1, x_2, \dots, x_n)$  permutační grupy  $G$  pro  $x_1 = x_2 = \dots = x_n = m$ , tj.

$$P_G(m, \dots, m).$$

<sup>3</sup>  $P$  je množina permutací na  $N$ , která obsahuje identickou permutaci, je uzavřená na inverzi a násobení permutací.

## Poznámky

- Dvě obarvení považujeme za stejná, pokud existuje symetrie, která převádí jedno obarvení na druhé. Exaktněji: Nechť  $G = (N, P)$  je permutační grupa symetrií  $n$ -prvkového objektu  $N = \{1, 2, \dots, n\}$ . Dvě obarvení  $(b_1^{(1)}, \dots, b_n^{(1)})$  a  $(b_1^{(2)}, \dots, b_n^{(2)})$  považujeme za stejná, jestliže

$$\exists \pi = \begin{pmatrix} 1 & 2 & \dots & n \\ \pi(1) & \pi(2) & \dots & \pi(n) \end{pmatrix} \in P \text{ tak, že } \forall i \in \{1, 2, \dots, n\} \text{ platí } b_i^{(1)} = b_{\pi(i)}^{(2)}$$

(tj. v prvním způsobu obarvení je prvek  $i$  obarven stejně jako prvek  $\pi(i)$  v druhém způsobu obarvení)

- Zdůrazněme ještě, že pod obarvením pomocí nejvýše  $m$  barev rozumíme takové obarvení, kdy libovolný prvek objektu je obarven kteroukoliv z uvedených  $m$  barev a to bez ohledu na obarvení ostatních prvků objektu.

## Příklad

Počet 2D obarvení vrcholů čtverce pomocí nejvýše  $m$  barev je rovno  $P_{2D}(m) = \frac{1}{4}(m^4 + m^2 + 2m)$ , kdežto ve 3D je rovno  $P_{3D}(m) = \frac{1}{8}(m^4 + 2m^3 + 3m^2 + 2m)$ . Speciálně dostáváme

$m$	2	3	4	5	10	50	100
$P_{2D}(m)$	6	24	70	165	2 530	1 563 150	25 002 550
$P_{3D}(m)$	6	21	55	120	1 540	813 450	12 753 775

Předešlé tvrzení odpovídá na otázku počtu obarvení daného objektu pomocí nejvýše  $m$  barev. Dalším logickým krokem je proto vyřešení otázky počtu obarvení daného objektu pomocí předepsaného počtu použitých jednotlivých barev. Např. z výše uvedeného příkladu víme, že vrcholy čtverce lze pomocí nejvýše 3 barev (např.  $b, c, m$ ) obarvit 24 způsoby, pokud uvažujeme 2D symetrie čtverce. Lze si v této souvislosti klást otázku, v kolika případech jde o obarvení, kdy použijeme právě  $1 \times b, 0 \times c, 3 \times m$ .

## Tvrzení

Nechť  $N = \{1, \dots, n\}$  je množina reprezentující  $n$ -prvkový objekt, jehož symetrie jsou definovány permutační grupou  $G = (N, P)$ . Potom počet různých obarvení daného  $n$ -prvkového objektu pomocí  $m$  zadaných barev  $\{b_1, \dots, b_m\}$ , kde barva  $b_i$  ( $i = 1, \dots, m$ ) je použita na obarvení  $k_i$  prvků ( $k_1 + \dots + k_m = n$ ), je rovno koeficientu u členu  $b_1^{k_1} \cdot \dots \cdot b_m^{k_m}$  v rozvoji cykle-index polynomu  $P_G(x_1, x_2, \dots, x_n)$ , kde za  $x_i$  ( $i = 1, \dots, n$ ) dosadíme výraz  $b_1^i + \dots + b_m^i$ .

## Příklad

Uvažujte 2D symetrie čtverce a určete rozložení počtu různých obarvení jeho vrcholů pomocí nejvýše 3 barev např.  $b, c, m$ .

Řešení.

Stačí určit rozvoj cycle-index polynomu  $P_{2D}(x_1, x_2, x_3, x_4) = \frac{1}{4}(x_1^4 + x_2^2 + 2x_4)$ , do kterého za  $x_i$  dosadíme  $b^i + c^i + m^i$ . Po dosazení a dalších úpravách dostáváme

$$\begin{aligned} P_{2D}(b + c + m, b^2 + c^2 + m^2, b^3 + c^3 + m^3, b^4 + c^4 + m^4) &= \\ &= b^4 + c^4 + m^4 + \\ &\quad + b^3c + b^3m + c^3b + c^3m + m^3b + m^3c + \\ &\quad + 2b^2c^2 + 2b^2m^2 + 2c^2m^2 + 3b^2cm + 3c^2bm + 3m^2bc. \end{aligned}$$

Z uvedeného rozvoje např. vidíme, že existují 2 různá obarvení vrcholů čtverce, kdy právě 2 vrcholy jsou  $b$  a 2 vrcholy jsou  $c$ , dále existují 3 různá obarvení vrcholů čtverce, kdy právě 2 vrcholy mají barvu  $b$  a ze zbývajících dvou vrcholů je jeden  $c$  a druhý  $m$ .

## 6. Symbolika $O$ , $\Omega$ , $\Theta$ , složitost algoritmů

Standardním nástrojem využívaným k popisu chování algoritmů (jako funkce velikosti vstupu  $n$ ) je tzv. symbolika „velké o“, „velké omega“ a „velké théta“, která charakterizuje asymptotické chování funkcí, resp. posloupností (tj. charakterizuje jejich chování pro „dostatečně velké“ hodnoty argumentu  $n$ ).

Jedním ze standardních přístupů k hodnocení efektivnosti algoritmů je analýza jejich paměťové a časové složitosti. Paměťovou složitostí budeme rozumět, zjednodušeně řečeno, odhad velikost paměti potřebné k realizaci výpočtu pomocí daného algoritmu pro úlohu

### Definice

Nechť  $f, g: N \rightarrow R$  jsou reálné posloupnosti. Potom:

- $O(g(n)) = \{f(n) | (\exists K > 0)(\exists n_0 \in N)(\forall n \geq n_0) 0 \leq |f(n)| \leq K|g(n)\}$
- $\Omega(g(n)) = \{f(n) | (\exists K > 0)(\exists n_0 \in N)(\forall n \geq n_0) 0 \leq Kg(n) \leq f(n)\}$
- $\Theta(g(n)) = \{f(n) | (\exists K_1, K_2 > 0)(\exists n_0 \in N)(\forall n \geq n_0) 0 \leq K_1g(n) \leq f(n) \leq K_2g(n)\}$

### Poznámky

- Symbol  $O$  zavedl matematik P. Bachmann (1837-1920) a ve svých pracích zpopularizoval E. Landau (neplést s fyzikem L. D. Landauem, nositelem Nobelovy ceny za fyziku (1962)). Symboly  $\Omega, \Theta$  zavedl respektovaný matematik a informatik D. Knuth (1938), autor vynikající třídílné knihy The Art of Computer Programming Vol. 1: Fundamental Algorithms, Vol. 2: Seminumerical Algorithms a Vol. 3: Sorting and Searching, se kterou by se měl seznámit každý programátor.
- Jako  $g(n)$  se často uvažují následující funkce: 1 (konstanta);  $n$ ;  $n \log n$ ;  $n^2$ ;  $n^2 \log n$ ; ...;  $2^n$ ;  $n!$ ;  $n^n$ . Platí:  $O(1) \subset O(n) \subset O(n \log n) \subset O(n^2) \subset O(n^2 \log n) \subset \dots \subset O(2^n) \subset O(n!) \subset O(n^n)$ .
- $O(g(n))$  je množina všech reálných posloupností, které až na kladnou multiplikativní konstantu nerostou rychleji než posloupnost  $g(n)$ . Píšeme  $f(n) \in O(g(n))$ , resp. méně přesně  $f(n) = O(g(n))$ .
- $\Omega(g(n))$  je množina všech reálných posloupností, které až na kladnou multiplikativní konstantu rostou alespoň tak rychle jako posloupnost  $g(n)$ . Píšeme  $f(n) \in \Omega(g(n))$ , resp. méně přesně  $f(n) = \Omega(g(n))$ .
- $\Theta(g(n))$  je množina všech reálných posloupností, které až na kladnou multiplikativní konstantu rostou stejně rychle jako posloupnost  $g(n)$ . Píšeme  $f(n) \in \Theta(g(n))$ , resp. méně přesně  $f(n) = \Theta(g(n))$ .
- Např. platí:

$$3n^2 + 17^{235} 139 \in O(n^2)$$

$$3n^2 + 17^{235} 139 \notin O(n)$$

$$3n^2 + 17^{235} 139 \in O(n^3)$$

$$3n^2 + 17^{235} 139 \notin \Theta(n^3)$$

$$\sin x \in O(1)$$

$$\sin x \notin \Omega(n)$$

$$\frac{17n^8 - 375n^7 + 5n^2 + 100^{1734}}{531n^3 + n + 5} \in O(n^5)$$

$$\frac{17n^8 - 375n^7 + 5n^2 + 100^{1734}}{531n^3 + n + 5} \in \Theta(n^5)$$

$$\sum_{i=1}^n i \in O(n^2)$$

$$\sum_{i=1}^n \frac{1}{i} \in O(\log n)$$

Následující tvrzení shrnuje základní vlastnosti zavedených symbolů.

### Tvrzení

Platí:

- $f \in O(g) \rightarrow Kf \in O(g)$ , kde  $K$  je konstanta,
- $f_1, f_2 \in O(g) \rightarrow f_1 + f_2 \in O(g)$ ,
- $f_1 \in O(g_1), f_2 \in O(g_2) \rightarrow (f_1 + f_2) \in O(g_1 + g_2), (f_1 + f_2) \in O(\max(|g_1|, |g_2|)), (f_1 f_2) \in O(g_1 g_2)$ ,

- $f \in O(g) \leftrightarrow g \in \Omega(f)$
- $f \in \Theta(g) \leftrightarrow (f \in O(g) \wedge f \in \Omega(g)) \leftrightarrow (f \in O(g) \wedge g \in O(f))$
- $a, b > 1 \rightarrow O(\log_a n) = O(\log_b n)$ ,
- Je-li  $f$  polynom stupně  $n$ ,  $g$  polynom stupně  $m$ , kde  $n \geq m$  potom  $f \in O(x^n)$ ,  $f/g \in O(x^{n-m})$ .

Důkaz - proveďte jako samostatné cvičení.

## 7. Rekurzivní algoritmy divide and conquer

Rekurzivní algoritmy divide and conquer jsou významným typem algoritmů využívaným k řešení široké třídy úloh (nejenom kombinatorických). Strategie řešení je založena na opakovaném rozdělování řešené úlohy na podúlohy stejného typu, ale menšího rozsahu (přibližně stejného). Dělení na podúlohy opakujeme do doby, než dostaneme úlohy „dostatečně“ malého rozsahu, jejichž řešení snadno zvládneme.

Otázkou, kterou se budeme krátce zabývat, je analýza časové složitosti těchto algoritmů. Nejprve však výše uvedený neformální popis formalizujeme, tj. převedeme do matematické podoby.

Označíme-li

- $f(n)$  ... časová složitost algoritmu aplikovaného na vyřešení úlohy o rozsahu  $n \in N^+$   
(obvykle vyjádřená počtem „základních“ operací nutných k vyřešení úlohy o rozsahu  $n$ ),  
 $a$  ... počet podúloh ( $1 \leq a < n$ ), na které převádíme řešení původní úlohy,  
 $\lfloor n/b \rfloor$ <sup>4</sup> ... rozsah podúlohy ( $1 < b < n$ ).

dostáváme pro časovou složitost rekurentní vztah

$$f(n) = af\left(\lfloor n/b \rfloor\right) + h(n),$$

s počáteční podmínkou  $f(1) = c$ .

Interpretace uvedeného rekurentního vztahu je zřejmá - řešení úlohy o rozsahu  $n$  převádíme na řešení  $a$  podúloh téhož typu, každá o rozsahu  $\lfloor n/b \rfloor$ , kde  $h(n)$  vyjadřuje časovou složitost rozdělení na podúlohy a zpětného převedení řešení podúloh na řešení původní úlohy.

Nyní uvážíme dva základní tvary funkce  $h(n)$ , totiž konstantu  $c$  a přirozenou mocninu  $n$ .

a) Předpokládejme  $h(n) = c$

(rozdělení na podúlohy a sestavení řešení původní úlohy z řešení podúloh trvá konstantní čas, nezávislý na rozsahu úlohy)

Základní představu o chování časové složitosti  $f(n)$  získáme tím, že o rozsahu úlohy budeme předpokládat, že je přirozenou mocninou  $b$ , tj. omezíme se na  $n \in S_b = \{b^k | k \in N\}$ . Tím se „zbavíme“ funkce dolní celá část a řešíme rekurentní vztah

$$f(n) = af\left(\frac{n}{b}\right) + c, f(1) = c,$$

kde  $n \in S_b = \{b^k | k \in N\}$ ,  $a, b, c \in N^+$ ,  $b \geq 2$ .

Vzhledem k  $n = b^k$  snadno nalezneme explicitní řešení, neboť  $f(n) = c(a^k + \dots + a + 1)$ , tj.

$$f(n) = \begin{cases} c(k+1), & a = 1 \\ c \frac{a^{k+1}-1}{a-1}, & a \geq 2 \end{cases}$$

Výše uvedené upravíme tak, abychom získali výrazy s proměnnou  $n$  (dostaneme tvary, z nichž bude evidentní chování  $f(n)$ ). Jelikož  $n = b^k$ , je  $k = \log_b n$ , dále  $a^k = (b^{\log_b a})^{\log_b n}$ , tj.  $a^k = n^{\log_b a}$  dostáváme

$$f(n) = \begin{cases} c(\log_b n + 1), & a = 1 \\ c \frac{an^{\log_b a}-1}{a-1}, & a \geq 2 \end{cases}$$

---

<sup>4</sup> Symbol  $\lfloor \ ]$  označuje dolní celou část.



Důsledkem je následující tvrzení.

### Tvrzení

Nechť  $f(n)$  je rostoucí na  $N^+$ , pro kterou na množině  $S_b = \{b^k | k \in N\}$  platí

$$f(n) \leq af\left(\frac{n}{b}\right) + c, f(1) \leq c,$$

kde  $a, b, c \in N^+, b \geq 2$ , potom

$$f(n) \in O(\log_b n) \text{ pro } a = 1 \text{ a } f(n) \in O(n^{\log_b a}) \text{ pro } a \geq 2.$$

### Poznámka

Je dobré si uvědomit, že ve výše uvedeném tvrzení (i v následujícím) jde věcně o  $\log_b$  tj. logaritmus se základem  $b$ , nicméně vzhledem k tomu, že zkoumáme asymptotické chování  $f(n)$ , tj. využíváme symboliku „velké  $O$ “, lze použít jako základ libovolné reálné číslo větší než 1.

### Příklad

Určete časovou složitost algoritmu vyhledávání v binárním vyhledávacím stromu.

Řešení.

Označíme-li  $f(n)$  funkci časové složitosti vyhledávání v binárním vyhledávacím stromu o velikosti  $n$ , zřejmě platí (zdůvodněte)

$$f(n) = f\left(\frac{n}{2}\right) + 2,$$

kde  $f(1) = 2$ .

Dostáváme tak hodnoty  $a = 1, b = 2, c = 2$  a pro časovou složitost proto dle výše uvedeného tvrzení platí

$$f(n) \in O(\log_2 n).$$

b) Předpokládejme  $h(n) = rn^d, r \in R^+, d \in N^+$

### Tvrzení

Nechť  $f(n)$  je rostoucí na  $N^+$ , pro kterou na množině  $S_b = \{b^k | k \in N\}$  platí

$$f(n) \leq af\left(\frac{n}{b}\right) + rn^d, f(1) \leq c,$$

kde  $a, b, c \in N^+, b \geq 2$ , potom

$$f(n) \in O(n^d) \text{ pro } a < b^d,$$

$$f(n) \in O(n^d \log n) \text{ pro } a = b^d,$$

$$f(n) \in O(n^{\log a}) \text{ pro } a > b^d$$

### Příklad

Určete časovou složitost řadícího algoritmu označovaného jako merge sort.

Řešení.

Označíme-li  $f(n)$  funkci časové složitosti řadícího algoritmu merge sort pracujícího nad daty o rozsahu  $n$ , zřejmě platí (zdůvodněte)

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

kde  $f(1) = 0$ .

Dostáváme tak hodnoty  $a = 2, b = 2, c = 0$  a pro časovou složitost proto dle výše uvedeného tvrzení platí

$$f(n) = O(n \log_2 n).$$

## 8. Přílohy

### 8.1. Přehled značení

$\wedge$	... logická spojka „a“ (konjunkce)
$\vee$	... logická spojka „nebo“ (disjunkce)
$\rightarrow$	... implikace (jestliže ... potom)
$\leftrightarrow$	... ekvivalence (právě když)
$\bar{\quad}$ , resp. $\neg$	... negace
$N$	... množina přirozených čísel 0,1,2, ...
$N^+$	... množina kladných přirozených čísel
$Z$	... množina celých čísel
$Q$	... množina racionálních čísel
$R$	... množina reálných čísel
$C$	... množina komplexních čísel
$\{a_1, \dots, a_n\}$	... neuspořádaná $n$ -tice, tj. množina skládající se z prvků $a_1, \dots, a_n$
$(a_1, \dots, a_n)$	... uspořádaná $n$ -tice
$\{a V(a)\}$	... množina prvků s vlastností $V$
$A \cap B$	... průnik množin $A, B$
$A \cup B$	... sjednocení množin $A, B$
$A - B$	... rozdíl množin $A, B$
$\bar{A}$	... doplněk množiny $A$
$A \times B$	... kartézský součin množin $A, B$
$P(A)$	... potenční množina (systém všech podmnožin množiny $A$ )
$ A $	... počet prvků (mohutnost, kardinalita) množiny $A$
$f(a)$	... hodnota funkce $f$ v bodě $a$
$\{a_n\}_{n=0}^{\infty}$ , resp. $(a_n)_{n=0}^{\infty}$	... číselná posloupnost
$[x]$	... horní celá část reálného čísla $x$
$\lfloor x \rfloor$	... dolní celá část reálného čísla $x$
$\{x\}$	... lomená část $x$
$C_n^k, \binom{n}{k}$	... rozšířený binomický koeficient ( $k, n \in Z$ ), resp. kombinační číslo ( $0 \leq k \leq n$ )
$\bar{C}_n^k$	... počet kombinací $k$ -té třídy z $n$ prvků s opakováním ( $0 \leq k, n$ )
$A_n^k$	... počet variací $k$ -té třídy z $n$ prvků bez opakování ( $0 \leq k \leq n$ )
$\bar{A}_n^k$	... počet variací $k$ -té třídy z $n$ prvků s opakováním ( $0 \leq k, n$ )
$P(n), P_n$	... počet permutací $n$ -tého řádu/třídy (bez opakování)
$P(n_1, \dots, n_k), P_{n_1, \dots, n_k}$	... počet permutací s opakováním ( $n_1$ prvků 1. druhu, ..., $n_k$ prvků $k$ -tého druhu)
$D(n), D_n$	... subfaktoriál $n$ -tého řádu (permutace, kde nezůstává žádný prvek na svém místě)
$D_k(n), D_{n,k}$	... počet permutací $n$ -tého řádu, ve kterých zůstává právě $k$ prvků na svém místě
$C_n$	... Catalanovo číslo
$\left\{ \begin{matrix} n \\ k \end{matrix} \right\}$	... Stirling subset number ( $0 \leq k \leq n$ )
$s(n, k)$	... Stirlingova čísla 1. druhu
$\left[ \begin{matrix} n \\ k \end{matrix} \right]$	... Stirling cycle number ( $0 \leq k \leq n$ )
$S(n, k)$	... Stirlingova čísla 2. druhu

## 8.2. Tabulka hodnot subfaktoriálů

$n$	$D_n$	$n$	$D_n$
0	1	11	14 684 570
1	0	12	176 214 841
2	1	13	2 290 792 932
3	2	14	32 071 101 049
4	9	15	481 066 515 734
5	44	16	7 697 064 251 745
6	265	17	130 850 092 279 664
7	1 854	18	2 355 301 661 033 953
8	14 833	19	44 750 731 559 645 106
9	133 496	20	895 014 631 192 902 121
10	1 334 961	21	18 795 307 255 050 944 540

## 8.3. Tabulka hodnot Fibonacciho čísel

$n$	$F_n$	$n$	$F_n$	$n$	$F_n$
0	0	15	610	30	832 040
1	1	16	987	31	1 346 269
2	1	17	1 597	32	2 178 309
3	2	18	2 584	33	3 524 578
4	3	19	4 181	34	5 702 887
5	5	20	6 765	35	9 227 465
6	8	21	10 946	36	14 930 352
7	13	22	17 711	37	24 157 817
8	21	23	28 657	38	39 088 169
9	34	24	46 368	39	63 245 986
10	55	25	75 025	40	102 334 155
11	89	26	121 393	41	165 580 141
12	144	27	196 418	42	267 914 296
13	233	28	317 811	43	433 494 437
14	377	29	514 229	44	701 408 733

## 8.4. Tabulka hodnot Catalanových čísel

$n$	$C_n$	$n$	$C_n$	$n$	$C_n$
0	1	7	429	14	2 674 440
1	1	8	1 430	15	9 694 845
2	2	9	4 862	16	35 357 670
3	5	10	16 796	17	129 644 790
4	14	11	58 786	18	447 638 700
5	42	12	208 012	19	1 767 263 190
6	132	13	742 900	20	6 564 120 420

### 8.5. Tabulka hodnot Stirlingových čísel 1. druhu $s(n, k)$

$n$	0	1	2	3	4	5	6	7	8	9	10
0	1										
1	0	1									
2	0	-1	1								
3	0	2	-3	1							
4	0	-6	11	-6	1						
5	0	24	-50	35	-10	1					
6	0	-120	274	-225	85	-15	1				
7	0	720	-1 764	1 624	-735	175	-21	1			
8	0	-5 040	13 068	-13 132	6 769	-1 960	322	-28	1		
9	0	40 320	-109 584	118 124	-67 284	22 449	-4 536	546	-36	1	
10	0	-362 880	1 026 576	-1 172 700	723 680	-269 325	63 273	-9 450	870	-45	1

### 8.6. Tabulka hodnot Stirlingových čísel 2. druhu $S(n, k)$

(Stirling subset numbers  $\left\{ \begin{matrix} n \\ k \end{matrix} \right\}$ )

$n$	0	1	2	3	4	5	6	7	8	9	10
0	1										
1	0	1									
2	0	1	1								
3	0	1	3	1							
4	0	1	7	6	1						
5	0	1	15	25	10	1					
6	0	1	31	90	65	15	1				
7	0	1	63	301	350	140	21	1			
8	0	1	127	966	1 701	1 050	266	28	1		
9	0	1	255	3 025	7 770	6 951	2 646	462	36	1	
10	0	1	511	9 330	34 105	42 525	22 827	5 880	750	45	1