Úvod do diskrétnej matematiky

Množiny
Kombinatorika
Logické funkcie
Teória grafov

prof. RNDr. Martin Škoviera, PhD.

Katedra informatiky, FMFI UK

Bratislava, 2007

Obsah

Kapitola 2

Kombinatorika

Obsah

2.1 Prirodzené čísla a matematická indukcia

Kombinatorika je matematická disciplína, ktorá sa zaoberá úlohami o štruktúrach definovaných na konečných množinách. Najčastejšie ide o podmnožiny, usporiadané n-tice, relácie, zobrazenia, rozklady a množstvo iných objektov, ktoré jednotne nazývame *kombinatorickými konfiguráciami.* Aj keď korene kombinatoriky siahajú hlboko pred náš letopočet, rozvoj kombinatoriky ako modernej disciplíny je úzko spojený s nástupom informatiky. Kombinatrika tvorí jeden zo základných pilierov tohto vedného odboru. Dnešnú kombinatoriku charakterizuje niekoľko všeobecných typov úloh. Spomedzi nich sú najdôležitejšie:

(1) zostrojiť konfigurácie požadovaných vlastností;

(2) nekonštruktívnymi metódami dokázať existenciu alebo neexistenciu konfigurácie istých vlastností;

(3) určiť počet všetkých konfigurácií daného typu;

(4) charakterizovať také konfigurácie pomocou iných pojmov, vlastností a parametrov;

(5) nájsť algoritmus, ktorý umožňuje všetky požadované konfigurácie zostrojiť;

(6) spomedzi všetkých konfigurácií vybrať optimálnu (alebo extremálnu – maximálnu, či minimálnu) podľa daných kriterií.

Spomedzi nich sa v tejto kapitole budeme stretávať s úlohami typu (4) , (3) a (1).

Ako sme povedali, kombinatorika sa zaoberá prevažne konečnými štruktúrami. Je tu však jedna nekonečná množina, ktorá má pre kombinatoriku podstatný význam: množina $\mathbb{N} = \{0, 1, 2, \ldots\}$ všetkých prirodzených čísel. O tejto množine už vieme, že je lineárne usporiadaná bežnou reláciou $\leq$ podľa veľkosti. Toto usporiadanie má jednu veľmi dôležitú vlastnosť (vlastnosť *dobrého usporiadania*): *Každá neprázdna podmnožina množiny* $\mathbb{N}$ *má najmenší prvok.* (To, že prirodzené čísla majú túto vlastnosť sa nahliadne ľahko sporom: keby existovala v $\mathbb{N}$ neprázdna podmnožina M bez najmenšieho prvku, tak by sme ľahko skonštruovali ostro klesajúcu nekonečnú postupnosť $n_0 > n_1 > n_2 > \ldots$ prvkov množiny M. Lenže taká postupnosť v $\mathbb{N}$ očividne neexistuje.)

Ďalšia dôležitá vlastnosť množiny $\mathbb{N}$ je základom metódy matematickej indukcie, ktorá je v kombinatorike prakticky všadeprítomná. Znie takto:

Nech $M \subseteq \mathbb{N}$ *je podmnožina spĺňajúca dve podmienky*:

(I1) $0 \in M$;

(I2) ak $x \in M$, tak potom aj $(x + 1) \in M$.

Potom $M = \mathbb{N}$.

Princíp matematickej indukcie môžeme teraz sformulovať takto.

Teoréma 2.1. *Nech* $(V(n))_{n\in\mathbb{N}}$ *je postupnosť výrokov. Predpokladajme, že*

(i) platí výrok $V(0)$*;*

(ii) pre každé prirodzené číslo n*, ak platí* $V(n)$ *, tak potom platí* $V(n + 1)$*,*

Potom výrok $V(n)$ *platí pre každé prirodzené číslo.*

Poznámka. Bod (i) sa nazýva *báza indukcie* a bod (ii) sa nazýva *indukčný krok*.

Dôkaz. Definujme množinu $A = \{n \in \mathbb{N};\ \text{platí výrok } V(n)\}$. Podmienka (i) našej teorémy znamená, že $0 \in A$. Podmienka (ii) hovorí, že platí implikácia - ak $n \in A$, tak aj $(n + 1) \in A$. To znamená, že sú splnené vyššie spomenuté podmienky (I1) a (I2), a preto $A = \mathbb{N}$. □

Bežne sa využíva niekoľko modifikácií teorémy 2.1. Stáva sa, že vlastnosť $V(n)$ platí iba pre prirodzené čísla $n \geq n_0$ pre nejaké číslo n_0. V tom prípade najprv overíme pravdivosť výroku $V(n_0)$ a potom dokážeme pravdivosť implikácie - pre každé $n \geq n_0$, ak platí $V(n)$, tak platí aj $V(n + 1)$. Tým je potom dokázaná pravdivosť výroku $V(n)$ pre každé $n \geq n_0$. Niekedy je výhodné použiť ďalší variant matematickej indukcie - *úplnú matematickú indukciu.*

Teoréma 2.2. *Predpokladajme, že z platnosti výroku $V(k)$ pre každé $k < n$ vyplýva aj platnosť výroku $V(n)$. Ak platí výrok $V(0)$, tak výrok $V(n)$ platí pre každé prirodzené číslo n.*

Poznamenajme, že overenie platnosti $V(0)$ nemožno vynechať.

2.2 Dirichletov princíp

V tejto časti sa budeme zaoberať jednoduchým no veľmi dôležitým princípom, ktorý má široké použitie pri riešení rozličných problémov a často vedie k prekvapujúcim záverom. Je známy v rôznych formách. Najjednoduchšia je azda táto:

Ak $n+1$ predmetov ukladáme do n priečinkov, tak aspoň jeden priečinok bude obsahovať dva alebo viac predmety.

Exaktnejšie môžeme tento princíp sformulovať takto:

Neexistuje injektívne zobrazenie $(n+1)$-prvkovej množiny do n-prvkovej množiny.

Dokážeme všeobecnejšie tvrdenie

Teoréma 2.3. *Nech A a B sú konečné množiny, pričom $|A| = n$, $|B| = m$ a $n > m$ Potom neexistuje žiadne injektívne zobrazenie $f : A \to B$.*

Dôkaz. Nech S je množina všetkých prirodzených čísel s takých, že existuje s-prvková množina, ktorá sa dá injektívne zobraziť na t - prvkovú, kde $t < s$. Naším cieľom je ukázať, že $S = \emptyset$. Predpokladajme, sporom, že $S \neq \emptyset$. Potom (na základe princípu dobrého usporiadania) S má najmenší prvok - nech n je najmenší prvok množiny S a nech $f : \{a_1, a_2, \ldots, a_n\} = A \to B = \{b_1, b_2, \ldots, b_m\}$ je injekcia, kde $m < n$. Zrejme $m \geq 2$, lebo inak by boli všetky zobrazenia $A \to B$ konštantné, a teda nie injektívne. Predpokladajme, že $f(a_n) = b_r$ pre nejaké $r \in \{1, 2, \ldots, m\}$. Keby každý z prvkov $f(a_1), f(a_2), \ldots, f(a_{n-1})$ bol rôzny od b_m , tak zúženie zobrazenia f na množinu $a_1, a_2, \ldots, a_{n-1}$ by bolo injektívnym zobrazením $A - \{a_n\} \to B - \{b_m\}$. To by však bol spor s voľbou čísla n. Preto musí existovať $j \in \{1, 2, \ldots, n-1\}$, že $f(a_j) = b_m$. Kedže f je injekcia, $f(a_n) \neq b_m$, takže $r \leq m - 1$. No potom zobrazenie $g : A - \{a_n\} \to B - \{b_m\}$ definované predpisom

$$\begin{aligned} g(a_j) &= b_r \\ g(a_i) &= f(a_i) \quad \text{pre } i \neq j,\ i \in \{1, 2, \ldots, n-1\} \end{aligned}$$

je opät injektívne. Znova sme dostali spor s definíciou čísla n, a teda množina S je prázdna. □

Prvýkrát upozornil na tento jednoduchý princíp nemecký matematik 19. storočia P. Dirichlet. Dnes je známy aj ako „holubníkový princíp“ podľa toho, že ak viac ako n holubov používa n holubníkových dier, tak aspoň dva holuby vychádzajú tou istou dierou. Poznamenajme, že tento princíp nedáva nijaký návod ako nájsť dieru používanú viac ako jedným holubom. Preto je tento princíp často existenčný.

Medzi dôsledky Dirichletovho princípu patrí aj skutočnosť, že ak konečná množina má m prvkov aj n prvkov, tak $m = n$.

Príklad 2.1. V Bratislave sa v každom okamihu vyskytujú aspoň dvaja ľudia, ktorí majú rovnaký počet vlasov na hlave. Nech A je množina obyvateľov Bratislavy a $B = \{0, 1, \ldots, 200000\}$. Zobrazenie $f : A \to B$ priraďuje bratislavčanovi x jeho počet vlasov $f(x) \in B$ (počet vlasov človeka neprevyšuje 200 000). Keďže $|A| > 200001$, zobrazenie nemôže byť injektívne. Poznamenajme, že toto zobrazenie sa každú chvíľu mení – stačí sa učesať.

Príklad 2.2. V postupnosti $(a_1, a_2, \ldots, a_n)$ ľubovoľných n prirodzených čísel existuje súvislá podpostupnosť $(a_{k+1}, a_{k+2}, \ldots, a_l)$ taká, že súčet $a_{k+1}, a_{k+2}, \ldots, a_l$ je deliteľný číslom n.

Aby sme sa o tom presvedčili, uvažujme n súčtov $a_1,\ a_1 + a_2, \ldots, a_1 + a_2 + \ldots + a_n$. Ak je medzi nimi niektorý deliteľný číslom n, sme hotoví. Nech preto každý z nich dáva po delení číslom n nenulový zvyšok. Keďže súčtov je n, no možných hodnôt pre zvyšky je len $n - 1$, dva z týchto súčtov povedzme $a_1 + a_2 + \ldots + a_r$ a $a_1 + a_2 + \ldots + a_s$ (pričom $r < s$) dávajú po delení číslom n ten istý zvyšok z. Máme teda

$$\begin{aligned} a_1 + a_2 + \ldots + a_r &= bn + z \\ a_1 + a_2 + \ldots + a_s &= cn + z \end{aligned}$$

pre vhodné $b, c \in \mathbb{Z}$. Odčítaním prvého súčtu od druhého dostávame

$$a_{r+1} + a_{r+2} + \ldots + a_s = (c - b)n,$$

čo znamená, že posledný súčet je deliteľný číslom n.

Uvedieme ešte silnejšiu formu Dirichletovho princípu:

Teoréma 2.4. *Ak $f : A \to B$ je zobrazenie konečných množín také, že $|A| = n$, $|B| = m$ a $n/m > r - 1$ pre nejaké prirodzené číslo r, tak existuje prvok množiny B, na ktorý sa zobrazí aspoň r prvkov množiny A.*

Dôkaz. Nech $B = \{1, 2, \ldots, m\}$ a nech n_i je počet prvkov množiny A, ktoré sa zobrazia na prvok $i \in B$. Keby pre každé z čísel n_i platilo $n_i \leq r - 1$, tak by sme dostali

$$r - 1 < \frac{n}{m} = \frac{n_1 + n_2 + \ldots + n_m}{m} \leq \frac{m(r-1)}{m} = r - 1.$$

Tento spor dokazuje teorému. □

2.3 Základné enumeračné pravidlá

Úloha určiť počet kombinatorických konfigurácií daného typu je jednou z najtypickejších kombinatorických úloh. Existuje obrovské množstvo rôznych druhov kombinatorických konfigurácií, keďže existuje nepreberné množstvo praktických úloh kombinatorického charakteru. Veľká väčšina úloh sa však dá zaradiť do jednej z nasledujúcich tried s dvoma podtriedami:

1. Určiť počet *neusporiadaných konfigurácií*, pričom opakovanie objektov v konfiguráciách je alebo nie je povolené.

2. Určiť počet *usporiadaných konfigurácií*, pričom opakovanie objektov v konfiguráciách je alebo nie je povolené.

Čitateľ iste pozná pojem kombinácií, ktorý spadá pod bod A, a pojem variácií, spadajúci pod bod B. Tieto dva pojmy však na riešenie kombinatorických úloh nestačia, pretože konfigurácie môžu kombinovať usporiadané aj neusporiadané črty. Oveľa dôležitejšie je preto ovládať základné enumeračné pravidlá a ovládnuť umenie „matematizácie“ kombinatorických úloh – čo znamená vedieť vyabstrahovať konfigurácie v podobe podmnožín, usporiadaných k-tic, zobrazení, relácií rozkladov a podobne, a potom na ich zrátanie enumeračné pravidlá použiť.

Prvé z nich je veľmi jednoduché:

Teoréma 2.5 (Pravidlo súčtu)**.** *Nech $X_1,\ X_2,\dots,X_n,\ n \geq 2$ sú navzájom disjunktné podmnožiny konečnej množiny X, pričom $X = X_1 \cup X_2 \cup \ldots \cup X_n$. Potom*

$$|X| = |X_1| + |X_2| + \ldots + |X_n|.$$

Dôkaz. Nech najprv $n = 2$. nech $X_1 = \{a_1, a_2, \dots, a_r\}$ and $X_2 = \{b_1, b_2, \dots, b_s\}$. Keďže $X_1 \cap X_2 = \emptyset$, platí $X_1 \cup X_2 = \{c_1, c_2, \dots, c_r, c_{r+1}, \dots, c_{r+s}\}$, kde $c_i = a_i$ pre $i \in \{1, 2, \dots, r\}$ a $c_j = b_{j-r}$ pre $j \in \{r+1, \dots, r+s\}$. Z tohto už ľahko vidno, že $|X| = |X_1 \cup X_2| = |X_1| + |X_2|$. Pre $n \geq 3$ sa dôkaz ľahko dokončí matematickou indukciou. $\square$

Opakovaným použitím tohto pravidla získavame ďalšie pravidlo. Je zložitejšie, no má častejšie použitie.

Teoréma 2.6 (Pravidlo súčinu)**.** *Nech $X_1,\ X_2,\dots,X_n,\ n \geq 2$, sú ľubovoľné konečné množiny. Potom $|X_1 \times X_2 \times \cdots \times X_n| = |X_1| \cdot |X_2| \cdot \ldots \cdot |X_n|$.*

Dôkaz. Budeme postupovať indukciou vzhľadom na n, pričom v indukčnom kroku použijeme pravidlo súčtu. Tvrdenie teorémy platí aj pre $n = 1$ (ale nič nehovorí) a to využijeme ako bázu indukcie. Nech teraz tvrdenie teorémy platí aj pre nejaké $n \geq 1$. Ukážeme, že platí aj pre $n+1$. Chcem určiť počet prvkov množiny $X_1 \times X_2 \times \ldots \times X_n \times X_{n+1}$. Ak $X_{n+1} = \emptyset$, tak $|X_1 \times X_2 \times \ldots \times X_n \times X_{n+1}| = 0 = |X_1| \cdot |X_2| \cdot \ldots \cdot |X_{n+1}|$. V tomto prípade teraz tvrdenie platí. Nech preto $|X_{n+1}| = s \geq 1$, pričom $X_{n+1} = \{a_1, a_2, \dots, a_s\}$. Položme pre každé $i \in \{1, 2, \dots, s\}$

$$Y_i = X_1 \times X_2 \times \ldots \times X_n \times \{a_i\}.$$

Je zrejmé, že $|Y_i| = |X_1 \times X_2 \times \ldots \times X_n|$ a podľa indukčného predpokladu teda platí

$$|Y_i| = |X_1| \cdot |X_2| \cdot \ldots \cdot |X_n|.$$

Pretože

$$X_1 \times X_2 \times \ldots \times X_n \times X_{n+1} = \bigcup_{k=1}^{s} Y_i.$$

a množiny $Y_1, Y_2, \ldots, Y_s$ sú navzájom disjunktné, z pravidla súčtu dostávame

$$|X_1 \times X_2 \times \ldots \times X_{n+1}| = \sum_{k=1}^{s} |Y_k| = |X_1| \cdot |X_2| \cdot \ldots \cdot |X_n| \cdot |X_{n+1}|.$$

□

Príklad 2.3. Koľko štvorciferných čísel deliteľných piatimi môžeme vytvoriť z cifier 0, 1, 3, 5, 7? Nech $M = \{0, 1, 3, 5, 7\}$. Potom každé hľadané číslo je charakterizované usporiadanou štvoricou, ktorá patrí do množiny $U =$ $= (M - \{0\}) \times M \times M \times \{0, 5\}$. Podľa pravidla súčinu dostávame

$$|U| = 4 \cdot 5 \cdot 5 \cdot 2 = 200.$$

Príklad 2.4. Koľkokrát za deň cifry na digitálnych hodinách ukazujú rastúcu postupnosť? Čas na ukazateli digitálnych množín môžeme zakódovať usporiadanou šesticou prirodzených čísel $x = (x_1, x_2; x_3, x_4; x_5, x_6)$. Predpokladajme, že $x_1 < x_2 < \ldots < x_6$. Hoci vo všeobecnosti čas musí spĺňať $x_1 \leq 2$, vidíme, že $x_1 = 2$ by nevyhnutne viedlo k $x_5 \geq 6$, čo nie je možné. Preto $x_1 \in \{0, 1\}$ a $x_5 \leq 5$. Ak $x_1 = 1$, tak $x_5 = 5$ a ak $x_1 = 0$, tak $x_5 = 4$ alebo 5. Množinu X hľadaných postupností rozdelíme takto

$$\begin{aligned} X_1 &= \{x \in X;\ x_1 = 1\}, \\ X_{04} &= \{x \in X;\ x_1 = 0, x_5 = 4\}, \\ X_{05} &= \{x \in X;\ x_1 = 0, x_5 = 5\}. \end{aligned}$$

V prvej množine sú postupnosti tvaru $(1, 2; 3, 4; 5, x_6)$, z čoho vyplýva $|X_1| =$ $= 4$. V druhej sú postupnosti tvaru $(0, 1; 2, 3; 4, x_6)$, takže $|X_{04}| = 5$. Počet prvkov množiny $|X_{05}|$ spočítame takto: pre (x_2, x_3, x_4) sú len tieto možnosti: $(1, 2, 3), (1, 2, 4), (1, 3, 4), (2, 3, 4)$. Pre x_6 sú možnosti $6, 7, 8, 9$. Každá postupnosť v X_{05} je charakterizovaná usporiadanou dvojicou $((x_2, x_3, x_4), x_6)$, ktorých je podľa pravidla súčinu $4.4 = 16$. Napokon podľa pravidla súčtu dostávame $|X| = |X_1| + |X_{04}| + |X_{05}| = 4 + 5 + 16 = 25$.

2.4 Variácie

Variácie spolu s kombináciami patria medzi najjednoduchšie a najbežnejšie kombinatorické konfigurácie.Zatiaľ čo variácie sú usporiadané štruktúry, kombinácie sú neusporiadané. Ukazuje sa, že jednoduchšie je začat štúdium usporiadaných konfigurácií a na neusporiadané sa dívať ako na triedy ekvivalencie usporiadaných štruktúr.

Ako prvý odvodíme výsledok o počte zobrazení medzi konečnými množinami. Pripomeňme označenie z predchádzajúcej kapitoly: pre lubovolné množiny $\boldsymbol{A}$ a B označujeme symbolom B^A množinu všetkých zobrazení $A \to B$.

Teoréma 2.7. *Ak A a B sú konečné množiny, pričom $|A| = n$ a $|B| = m$, tak*

$$\left|B^A\right| = |B|^{|A|} = m^n$$

Dôkaz. Teorému dokážeme indukciou vzhľadom na n. Pre $n = 0$ (a každé prirodzené císlo $m = |B|$) teoréma platí, lebo $B^\emptyset = \{\emptyset\}$. Predpokladajme teraz, že teoréma platí pre nejaké $n \geq 0$ a všetky prirodzené čísla m. Nech $|A| = n+1$, pričom $A = \{a_1, \ldots, a_n, a_{n+1}\}$. Ak $B = \emptyset$, tak $\emptyset^A = \emptyset$ a tvrdenie platí. Ak $m \geq 1$ a $B = \{b_1, b_2, \ldots, b_m\}$, pre $k \in \{1, 2, \ldots, m\}$ položíme

$$Y_k = \{f \in B^A; f(a_{n+1}) = b_k\}$$

Množiny Y_k sú navzájom disjunktné a $B^A = \cup_{k=1}^m Y_k$. Okrem toho zúženia zobrazení $f \in Y_k$ na množinu $A - \{a_{n+1}\}$ sú po dvoch rôzne a dávajú všetky zobrazenia $\{a_1, a_2, \ldots, a_n\} \to B$, z indukčného predpokladu dostávame $|Y_k| = m^n$. Napokon

$$\left|B^A\right| = \sum_{k=1}^{m} |Y_k| = m \cdot m^n = m^{n+1} = |B|^{|A|}$$

□

Pre $A = \{1, 2, \ldots, n\}$ a $|B| = m$ sa prvky množiny B^A nazývajú *variácie s opakovaním* n-tej triedy z m prvkov (množiny B). V súhlase s označením zavedením v članku **??** namiesto šípkového označenia pre tieto zobrazenia používame označenie sekvenciálne $f : \{1, 2, \ldots, n\} \to B$ označujeme

$(f(1), f(2), \ldots, f(n)) = (f1, f2, \ldots, fn)$. Z tohto vyjadrenia je zrejmé, že existuje bijekcia $B^{\{1,2,\ldots,n\}} \to B \times B \times \ldots \times B$ (n-krát) a teda teoréma 2.7 vyplýva aj priamo z pravidla súčinu.

Napríklad ak $B = \{a, b\}$, tak všetky variácie tretej triedy z množiny B sú (usporiadané lexikograficky):

$$(a, a, a),\ (a, a, b),\ (a, b, a),\ (a, b, b),\ (b, a, a),\ (b, a, b),\ (b, b, a),\ (b, b, b).$$

Poznámka. Teorémy (2.5-2.7) sú základom definície súčtu, súčinu a mocnenia ľubovolných kardinálnych čísel, ako sme ich zaviedli v článku **??**. Tieto definície teda zovšeobecňujú našu praktickú skúsenosť z konečných množín na nekonečné množiny ľubovolnej kardinality.

Teoréma 2.7,5 *Nech* $\boldsymbol{A}$ *je konečná množina,* $|A| = n$*. Potom počet všetkých podmnožín množiny* A *je* $|\mathcal{P}(A)| = 2^n$*.*

Teraz určíme počet všetkých injektívnych zobrazení medzi dvoma množinami.

Teoréma 2.8. *Nech* $\boldsymbol{A}$ *a* B *sú konečné množiny, pričom* $|A| = n$ *a* $|B| = m$*. Potom počet všetkých injektívnych zobrazení z* A *do* B *je*

$$m \cdot (m-1) \dots (m-n+1) = \prod_{i=0}^{n-1} (m-i)$$

Dôkaz. Nech I_B^A označuje počet injekcií $A \to B$. Budeme postupovať indukciou vzhľadom na n. Ak $A = \emptyset$, tak existuje jediná injekcia $A \to B$. V súčine $\prod_{i=0}^{-1}(m-i)$ máme nulový počet činiteľov, a taký súčin sa definitoricky kladie za 1. Teda v tomto prípade výsledok platí. Predpokladajme, že tvrdenie našej teorémy je správne pre nejaké $n \geq 0$ a pre všetky prirodzené čísla m. Nech $|A| = n+1$ a nech $A = \{a_1, a_2, \dots, a_n, a_{n+1}\}$. Ak $B = \emptyset$, tak $B^A = \emptyset$ a tvrdenie platí. Nech teda $m \geq 1$ a $B = \{b_1, b_2, \dots, b_m\}$. Definujme teraz pre $k \in \{1, 2, \dots, m\}$ množinu

$$Y_k = \{f \in B^A; \quad f \text{ je injektívne a } f(a_{n+1}) = b_k\}$$

Množiny $Y_1, Y_2, \dots, Y_m$ sú navzájom disjunktné a každá injekcia $A \to B$ patrí do nejakej z nich. Preto $|Y_1| + |Y_2| + \dots + |Y_m| = I_B^A$
Určíme $|Y_k|$ pre ľubovolné k. Kedže zúžením injekcie je opät injekcia, zúženia zobrazení $f \in Y_k$ a množinu $A - \{a_{n+1}\}$ sú injekcie $A - \{a_{n+1}\} \to B - \{b_k\}$. Naviac medzi zúženiami sa každá taká injekcia vyskytuje práve raz. Preto

$$|Y_k| = I_{B-\{b_k\}}^{A-\{a_{n+1}\}}$$

Podľa indukčného predpokladu

$$|Y_k| = \prod_{i=0}^{n-1}(m-1-i) = \prod_{i=1}^{n}(m-i)$$

Odtiaľ vyplýva, že

$$I_B^A = m\prod_{i=1}^{n}(m-i) = \prod_{i=0}^{n}(m-i)$$

□

Všimnime si, že ak $|A| > |B|$, tak teoréma 2.8 hovorí, že neexistuje žiadna injekcia $A \to B$, čo je obsah teorémy 2.3. Dirichletov princíp je teda dôsledkom teorémy 2.8.

Injekcie z množiny $A = \{1, 2, \dots, n\}$ do množiny B, kde $|B| = m$, sa nazývajú *variácie (bez opakovania) n-tej triedy* z m prvkov (množiny B).

Na označenie počtu variácií bez opakovania n-tej triedy z m prvkov používame symbol $m^{\underline{n}} = m(m-1)\dots(m-n+1)$, pričom v súhlase s teorémou 2.8 platia vzťahy $m^{\underline{0}} = 1$ a $m^{\underline{1}} = m$ číslo $m^{\underline{n}}$ sa nazýva *n-tý klesajúci faktoriál z m.* Číslo $m^{\underline{m}} = m(m-1)\cdot\ldots\cdot 2\cdot 1$ sa označuje $m!$ a nazýva sa *m-faktoriál.*

Príklad 2.5. Máme zostaviť vlajku z troch rovnakých vodorovných farebných prvkov, alebo troch rovnakých zvislých prvkov, pričom máme k dispozícií látky n rôznych farieb (v neobmedzenom množstve) . Nech H je množina vlajok prvého a V množina vlajok druhého druhu. Zrejme $H \cap V = \emptyset$ a $|H| = |V|$. Každú vlajku z množiny H charakterizuje usporiadaná trojica rôznych farieb, čiže injekcia $\{1, 2, 3\} \to F$, kde F je množina farieb. Z teorémy 2.8 vyplýva, že $|H| = n(n-1)(n-2) = n^{\underline{3}}$, a teda počet rôznych vlajok je $2n^{\underline{3}}$.

Napríklad variácie bez opakovania druhej triedy z prvkov množiny $B = \{1, 2, 3\}$ sú (v lexikografickom usporiadaní) $(1, 2), (1, 3), (2, 1), (2, 3), (3, 1), (3, 2)$. Ak $A == \{1, 2, \dots, n\}$ a $|B| = n$, tak variácie n-tej triedy z n prvkov množiny B nie sú nič iné ako bijekcie $A \to B$ a ich počet je podľa teorémy 2.8 $n\cdot(n-1)\cdot\ldots\cdot 2\cdot 1 = n!$. Tieto variácie sa nazývajú *permutáciami množiny B.* (Niekedy je o permutáciach výhodné predpokladať, že $A = B$.)

Zo zápisu permutácie ako postupnosti, v ktorej sa vyskytujú bez opakovania všetky prvky množiny B je zrejmé, že každá permutácia množiny B určuje nejaké lineárne usporiadanie množiny B. Obrátene, každé lineárne usporiadanie množiny B definuje permutáciu f množiny B – ak $b \in B$ je i-ty najmenší prvok množiny B (t.j. i-ty z ľava), stačí položiť $f(i) = b$.

Teoréma 2.9. *Existuje vzájomne jednoznačná korešpondencia medzi permutáciami ľubovolnej množiny B a lineárnymi usporiadaniami množiny B. Preto počet lineárnych usporiadaní n-prvkovej množiny je $n!$*

Na záver vyslovíme ešte *zovšeobecnené pravidlo súčinu*, ktoré je zosilnením teorémy 2.8. Dôkaz indukciou prenechávame čitateľovi.

Teoréma 2.10. *Nech X je konečná množina. Nech $A \subseteq X^k$, $k \geq 2$, je podmnožina karteziánskeho súčinu X^k, ktorej prvky označíme $(x_1, x_2, \dots, x_k)$ a ktorá spĺňa podmienky:*

(1) prvok x_1 je možné z množiny X vybrať n_1 spôsobmi;

(2) pre každé $i \in \{1, \dots, k-1\}$, po akomkoľvek výbere usporiadanej i-tice $(x_1, x_2, \dots, x_i)$ je možné prvok x_{i+1} vybrať vždy n_{i+1} spôsobmi.

Potom $|A| = n_1 \cdot n_2 \cdot \ldots \cdot n_k$

2.5 Kombinácie bez opakovania

Kombinácie bez opakovania sú neusporiadané súbory neopakujúcich sa prvkov - inými slovami podmnožiny nejakej základnej množiny. Presnejšie, *kombinácie (bez opakovania) k-tej triedy z n prvkov* množiny A sú k-prvkové podmnožiny množiny A s mohutnosťou $|A| = n$.

Množina všetkých k-prvkových podmnožín množiny A sa označuje $\mathcal{P}_k(A)$ alebo $\binom{A}{k}$ a ich počet $\binom{n}{k}$. Symbol $\binom{n}{k}$ sa nazýva *kombinačným číslom* alebo *binomickým koeficientom* (dôvody pochopíme neskôr).

Bezprostredne z definície symbolu $\binom{n}{k}$ vyplývajú tieto jeho vlastnosti:

- Pre každé $n \geq 0$ platí $\binom{n}{0} = 1$, lebo každá množina má práve jednu prázdnu množinu.
- Pre každé $n \geq 0$ platí $\binom{n}{n} = 1$, lebo každá n-prvková množina má práve jednu n-prvkovú podmnožinu, totiž samú seba.
- Pre každé $n \geq 0$ platí $\binom{n}{1} = n$, lebo každá n-prvková množina má práve n rôznych 1-prvkových podmnožín.
- Pre každé $k \leq n$ platí $\binom{n}{k} = \binom{n}{n-k}$. Počet k-prvkových podmnožín ľubovoľnej n prvkovej množiny A je ten istý ako počet $(n-k)$-prvkových podmnožín množiny A, lebo zobrazenie $\binom{A}{k} \to \binom{A}{n-k}$, $x \mapsto A - x$ je bijekcia.
- Pre každé $k > n$ platí $\binom{n}{k} = 0$, lebo n-prvková množina nemá podmnožiny s viac ako n prvkami.

Určíme teraz hodnotu symbolu $\binom{n}{k}$.

Teoréma 2.11. *Nech A je konečná množina, pričom $|A| = n$. Potom počet k-kombinácií z množiny A je*

$$|\mathcal{P}_k(A)| = \binom{n}{k} = \frac{n(n-1)\dots(n-k+1)}{k(k-1)\dots1} = \frac{n^{\underline{k}}}{k!}$$

Dôkaz. Nech $K = \{0, 1, \dots, k-1\}$. Budeme skúmať injekcie $K \to A$, čiže na množine I_A^K. Na I_A^K zavedieme binárnu reláciu R takto:

$$f\ R\ g \text{ práve vtedy, keď } f(\{0, 1, \dots, k-1\}) = g(\{0, 1, \dots, k-1\})$$

Potom R je relácia ekvivalencie. Každá trieda ekvivalencie C na množine I_A^K je jednoznačne určená jednou k-prvkovou podmnožinou M, na ktorú zobrazenia z množiny C zobrazia množinu $\{0, 1, \dots, k-1\}$. Ak v týchto zobrazeniach zameníme koobor A za M, dostaneme práve všetky permutácie množiny M. Preto $|C| = k!$. Každá trieda ekvivalencie na I_A^K má $k!$ prvkov. Preto $k!\binom{n}{k} = n^{\underline{k}} = I_A^K$. Počet k-prvkových podmnožín množiny A je teda, podľa teorémy 2.8, $\binom{n}{k} = |I_A^K|/k! = n^{\underline{k}}/k!$. □

Kombinačné čísla majú veľké množstvo zaujímavých vlastností. Uvedieme aspoň niektoré z nich.

Teoréma 2.12. *Pre ľubovoľné prirodzené čísla n a k platí:*

$$\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}$$

Dôkaz. Tvrdenie je možné ľahko dokázať pomocou vyjadrenia $\binom{n}{k} = \frac{n^{\underline{k}}}{k!}$ tak, že úpravou vzťahu na ľavej strane dostaneme kombinačné číslo na pravej strane. My však dokážeme túto rovnosť pomocou množinovej interpretácie. Nech A je množina, ktorá má $|A| = n+1$ a nech $b \in A$ je pevný prvok. Množinu $\binom{A}{k+1}$ rozložíme na dve časti B_0 a B_1: B_0 bude združovať $(k+1)$-podmnožiny, ktoré neobsahujú prvok b, naproti tomu B_1 bude združovať všetky tie, ktoré prvok b obsahujú. Keďže každá množina v B_0 je podmnožinou množiny $A - \{b\}$, dostávame $|B_0| = \binom{n}{k+1}$. Každá množina v B_1 zas určuje k-prvkovú podmnožinu množiny $A - \{b\}$. Preto $|B_1| = \binom{n}{k}$. Odtiaľ

$$\binom{n+1}{k+1} = \binom{A}{k+1} = |B_0| + |B_1| = \binom{n}{k+1} + \binom{n}{k}$$

□

Tento rekurentný vzťah je základom umiestnenia kombinačných čísel v rovine do tvaru trojuholníka, v ktorom je možné postupne vyčísľovať kombinačné čísla s použitím jediného faktu, že $\binom{n}{0} = \binom{n}{n} = 1$ pre každé n.

$$\begin{array}{ccccccc}
 & & & \binom{0}{0} & & & \\
 & & \binom{1}{0} & & \binom{1}{1} & & \\
 & \binom{2}{0} & & \binom{n}{1} & & \binom{2}{2} & \\
\binom{3}{0} & & \binom{3}{1} & & \binom{3}{2} & & \binom{3}{3}
\end{array}
\qquad\qquad
\begin{array}{ccccccc}
 & & & 1 & & & \\
 & & 1 & & 1 & & \\
 & 1 & & 2 & & 1 & \\
1 & & 3 & & 3 & & 1
\end{array}$$

Príklad 2.6. Majme domino (variant známej spoločenskej hry), ktorého každý kameň je rozdelený na dve časti a na každej polovici je vyznačená jedna z hodnôt $0, 1, \ldots, n$; žiadna z dvoch častí sa nedá odlíšiť ako prvá alebo druhá. Aká je pravdepodobnosť toho, že dva náhodne vybrané kamene sa dajú k sebe priložiť, čiže obsahujú rovnakú hodnotu aspoň na jednej strane? (Poznamenajme, že bežné domino má $n = 6$.) Kameň, na ktorom sú napísané hodnoty $i, j \in \in \{0, 1, \ldots, n\}$, môžeme jednoznačne zakódovať množinou $\{i, j\}$. Keďže sa môže stať, že $i = j$ (takým kameňom sa hovorí dublety), máme $1 \leq |\{i, j\}| \leq 2$. Celkový počet kameňov je teda $\binom{n+1}{1} + \binom{n+1}{2} = \binom{n+2}{2}$, podľa teorémy 2.12. Špeciálne pre $n = 6$ dostávame $\binom{8}{2} = 28$. Počet všetkých možných výberov dvoch kameňov je potom

$$\binom{\binom{n+2}{2}}{2} = 28.$$

Určíme teraz počet dvojíc kameňov, ktoré sa daju priložiť k sebe. Toto číslo je zhodné s počtom neusporiadaných dvojíc množín $\{i,j\}, \{k,l\} \in \mathcal{P}_2(\{0,1,\ldots,n\})$ takých, že $\{i,j\} \cap \{k,l\} \neq \emptyset$. Pre každé $i \in \{0,1,\ldots,n\}$ zistíme, aký je počet dvojíc kameňov, ktoré majú spoločnú hodnotu i. Všimnime si, že okrem hodnoty i sa na týchto kameňoch objavujú ešte dve ďalšie hodnoty j a k, pričom $j \neq k$; môže sa však stať, že jedna z týchto hodnôt je totožná s i. Z tohto je jasné, že každú dvojicu kameňov so spoločnou hodnotou i môžeme jednoznačne reprezentovať dvojprvkovou množinou $\{j,k\}$. Takto dostávame $\binom{n+1}{2}$ dvojíc kameňov so spoločnou hodnotou i. Vzhľadom na počet výberov hodnoty i, dostávame $(n+1)\binom{n+1}{2}$ dvojíc kameňov domina, ktoré sa dajú priložiť k sebe. Z toho vyplýva, že pravdepodobnosť javu, že pri náhodnom výbere dvojice kameňov je možné tieto kamene priložiť k sebe, je

$$\frac{(n+1)\binom{n+1}{2}}{\binom{\binom{n+2}{2}}{2}} = \frac{2(n+1)\binom{n+1}{2}}{\binom{n+2}{2}\left(\binom{n+2}{2}-1\right)}.$$

Pre bežné domino ($n=6$) dostávame pravdepodobnosť $7/18 < 0{,}4$.

Dôležitým výsledkom o kombinačných číslach je nasledujúca teoréma, ktorá vysvetľuje, prečo kombinačné čísla nazývajú aj binomické koeficienty.

Teoréma 2.13 (Binomická veta)**.** *Pre každé reálne číslo x a prirodzené číslo n platí*

$$(1+x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k.$$

Dôkaz. Tvrdenie zrejme platí pre $n=0$. Ďalej budeme postupovať indukciou vzhľadom na n. Ak predpokladáme platnosť tvrdenia pre nejaké $n \geq 0$, tak použitím tvrdenia 2.12 dostávame:

$$\begin{aligned}
(1+x)^{n+1} &= (1+x)^n(1+x) \\
&= \left(\sum_{k=0}^{n} \binom{n}{k} x^k\right)(1+x) \\
&= 1 + \left(\binom{n}{0} + \binom{n}{1}\right)x + \left(\binom{n}{1} + \binom{n}{2}\right)x^2 + \ldots \\
&\quad + \left(\binom{n}{n-1} + \binom{n}{n}\right)x^n + x^{n+1} \\
&= \sum_{k=0}^{n+1} \binom{n+1}{k} x^k
\end{aligned}$$

čo bolo treba dokázať. ∎

Poznámka. Definíciu binomického koeficientu $\binom{n}{k}$ môžeme rozšíriť z prirodzeného čísla n na ľubovoľné reálne číslo z, ak na základ jeho rozšírenia zoberieme teorému 2.11.

Položme

$$\binom{z}{k} := \frac{z^{\underline{k}}}{k!} = \frac{z(z-1)\dots(z-k+1)}{k!}$$

Pre takéto binomické koeficienty je možné dokázať analóg binomickej teorémy, ktorý v tomto prípade vyzerá takto:

Pre ľubovoľné $z \in \mathbb{R}$ a pre každé reálne číslo z také, že $|x| < 1$ platí

$$(1+x)^z = \sum_{k=0}^{\infty} \binom{z}{k} x^k$$

Ak $z \in \mathbb{N}$, tak všetky binomické koeficienty pre $k > z$ sú nulové a dostávame opäť tvrdenie teorémy 2.13 (pre $|x| < 1$, čo nie je až také podstatné). Takáto rozšírená binomická teoréma je užitočná pri dokazovaní rozličných vlastností kombinačných čísel. Dôkaz zovšeobecnenej binomickej teorémy presahuje rámec tohto textu.

Dôsledok 2.14. *Platia tieto identity* $(n \geq 1)$

(a) $\displaystyle\sum_{k=0}^{n} \binom{n}{k} = 2^n,$

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

(c) $\displaystyle\sum_{\substack{0\leq k\leq n,\\ k \text{ párne}}} \binom{n}{k} = \sum_{\substack{0\leq k\leq n,\\ k \text{ nepárne}}} \binom{n}{k} = 2^{n-1}.$

Dôkaz. Tvrdenie (a) dostaneme priamo z binomickej teorémy, ak položíme $x = 1$ a (b) dostaneme, ak položíme $x = -1$.

Jednu z rovností v (c) dostaneme, ak sčítame identity (a) a (b) a vydelíme dvoma, druhú rovnosť získame podobne odčítaním.

Identitu (a) môžeme ľahko dokázať aj kombinatorickou úvahou: na pravej strane máme 2^n, čo je $|\mathcal{P}(A)|$, kde $|A| = n$. To isté číslo môžeme vyjadriť aj v tvare súčtu

$$|\mathcal{P}(A)| = \sum_{k=0}^{n} |\mathcal{P}_k(A)|$$

□

Teoréma 2.15 (Cauchyho sčítací vzorec)**.** *Pre všetky prirodzené čísla m a n platí*

$$\sum_{i=0}^{k}\binom{m}{i}\binom{n}{k-i}=\binom{m+n}{k}$$

Dôkaz. Nech A_1 a A_2 sú disjunktné množiny, pričom $|A_1| = m$ a $|A_2| = n$. Položme $A = A_1 \cup A_2$. Nech $X \subseteq A$. Potom $X \cap A = X \cap (A_1 \cup A_2) = (X \cap A_1) \cup (X \cap A_2)$. Označme $X_i = X \cap A_i, i = 1, 2, \ldots$. Potom X_1 a X_2 sú disjunktné podmnožiny A_1 resp. A_2 a $X = X_1 \cup X_2$.

Skúmajme zobrazenie

$$\begin{aligned} f : \mathcal{P}_k(A) \to \cup_{i=0}^{k}(\mathcal{P}_i(A_1) \times \mathcal{P}_{k-i}(A_2)) \\ x \mapsto (x_1, x_2) \end{aligned}$$

Keďže každú podmnožinu X môžeme vyjadriť ako zjednotenie množiny $X_1 = X \cap A_1$ s množinou $X_2 = X \cap A_2$, vidíme, že zobrazenie f je bijektívne. Z teorémy 2.11 a pravidla súčinu vieme, že $|\mathcal{P}_i(A_1)\times\mathcal{P}_{k-i}(A_2)| = \binom{m}{i}\binom{n}{k-i}$.

Požitím pravidla súčtu napokon dostávame

$$\binom{m+n}{k} = |\mathcal{P}_k(A)| = |\cup_{i=0}^{k}\mathcal{P}_i(A_1)\times\mathcal{P}_{k-1}(A_2)| = \sum_{i=0}^{k}\binom{m}{i}\binom{n}{k-i}.$$

Tým je dôkaz skončený. □

Poznámka. Tvrdenie 2.15 môžeme dokázať aj pomocou binomickej teorémy takto. Zrejme platí $(1+x)^{m+n} = (1+x)^m(1+x)^n$. Ak rozpíšeme pravú aj ľavú stranu tejto rovnosti podľa teorémy 2.13, dostáneme

$$\sum_{k=0}^{m+n}\binom{m+n}{k}x^k = \left(\sum_{i=0}^{m}\binom{m}{i}x^i\right)\left(\sum_{j=0}^{n}\binom{n}{j}x^j\right)$$

Súčty na pravej strane roznásobíme podľa distributívneho zákona a roztriedime podľa mocnín premennej x. Zistíme, že pri x^k sa vyskytuje koeficient

$$\sum_{i=0}^{k}\binom{m}{i}\binom{n}{k-i}$$

Na ľavej strane sa pri x^k vyskytuje koeficient $\binom{m+n}{k}$. Keďže dva mnohočleny sa rovnajú práve vtedy, keď pri rovnakých mocninách premennej sa vyskytujú rovnaké koeficienty, musí platiť

$$\sum_{i=0}^{k}\binom{m}{i}\binom{n}{k-i}=\binom{m+n}{k}$$

Rovnakou metódou je možné dokázať celý rad ďalších identít-vzťahov medzi kombinačnými číslami. Čitateľ si môže sám vyskúšať, aká identita vyplýva zo vzťahu $(1+x)^{n+1} = (1+x)^n(1+x)$. Na záver tohto článku sa pozrieme na číslo $\binom{n}{k}$ ako na funkciu premennej k pri pevnom n.

Teoréma 2.16. *Pre každé prirodzené číslo n platí:*

(a) ak n je párne, tak

$$\binom{n}{0} < \binom{n}{1} < \cdots < \binom{n}{n/2-1} < \binom{n}{n/2} > \binom{n}{n/2+1} > \cdots > \binom{n}{n};$$

(b) ak n je nepárne, tak

$$\binom{n}{0} < \binom{n}{1} < \cdots < \binom{n}{(n-1)/2} = \binom{n}{(n+1)/2} > \cdots > \binom{n}{n-1} > \binom{n}{n}.$$

Dôkaz. Skúmajme pomer

$$\frac{\binom{n}{k}}{\binom{n}{k-1}} = \frac{n^{\underline{k}}}{k!}\,\frac{(k-1)!}{n^{\underline{k-1}}} = \frac{n-k+1}{k}$$

Ľahko zistíme, že pre $k \leq n/2$ je tento pomer väčší ako 1, a teda $\binom{n}{k} > \binom{n}{k-1}$. Ak n je nepárne, z rovnosti $\binom{n}{k} = \binom{n}{n-k}$ dostávame rovnosť $\binom{n}{(n-1)/2} = \binom{n}{(n+1)/2}$. Odtiaľ už vyplýva tvrdenie. □

Z tohto tvrdenia vyplýva, že funkcia $\binom{n}{k}$ nadobúda svoju najväčšiu hodnotu v strede celočíselneho intervalu $\langle 0, n \rangle$, pričom ak n je párne sa táto hodnota nadobúda raz, ak n je nepárne – dvakrát. Po túto hodnotu funkcia $\binom{n}{k}$ rastie, od nej potom klesá.

2.6 Kombinácie s opakovaním, permutácie s opakovaním, polynomická veta

Najprv sa budeme venovať kombináciám s opakovaním. Z názvu týchto konfigurácií vyplýva, že ide o konfigurácie, v ktorých sa nerozlišuje poradie, no prvky sa môžu opakovať. Pri ich presnej definícii budeme vychádzať z variácií s opakovaním, teda zobrazení $\{1, 2, \ldots, k\} \to \boldsymbol{A}$. Všimnime si najprv, že na množine $\boldsymbol{A}^{\{1,2,\ldots,k\}}$ všetkých variácií s opakovaním k-tej triedy v množine B môžeme zaviesť reláciu ekvivalencie R takto: Nech $f, g \in \boldsymbol{A}^{\{1,2,\ldots,k\}}$. Položme fRg práve vtedy keď $|f^{-1}(\{x\})| = |g^{-1}(\{x\})|$ pre každý prvok $x \in \boldsymbol{A}$.

Inými slovami, dve variácie s opakovaním budú ekvivalentné práve vtedy, keď v oboch sa rovnaké prvky opakujú rovnaký počet krát.

Kombinácie s opakovaním k-tej triedy z m prvkov množiny $\boldsymbol{A}$ (kde $|\boldsymbol{A}| = m$) sú triedy ekvivalencie R na množine $\boldsymbol{A}^{\{1,2,\ldots,k\}}$.

Ako príklad uvedieme vyššie definovanú ekvivalenciu R na množine $\{a, b\}^{\{1,2,3,4\}}$. Triedy tejto ekvivalencie budú kombinácie s opakovaním štvrtej triedy v množine $\{a, b\}$. Variácie patriace do tej istej triedy rozkladu sú uvedené v tom istom stĺpci. Vnútri každej triedy sú variácie zobrazené lexikograficky. Variácie sú napísané ako slová-bez zátvoriek a čiarok.

aaaa	aaab	aabb	abbb	bbbb
	aaba	abab	babb	
	abaa	abba	bbab	
	baaa	baab	bbba	
		baba		
		bbaa		

Počet kombinácií s opakovaním štvrtej triedy z dvoch prvkov je teda 5.

Teoréma 2.17. *Nech $\boldsymbol{A}$ je n-prvková množina a k prirodzené číslo. Potom počet všetkých kombinácií s opakovaním k-tej triedy v množine $\boldsymbol{A}$ je*

$$\binom{n+k-1}{k}.$$

Dôkaz. Kombinácie s opakovaním k-tej triedy v množine $\boldsymbol{A}$ sú prvky rozkladu množiny $\boldsymbol{A}^{\{1,2,\ldots,k\}}$ indukovaného reláciou ekvivalencie R popísanej vyššie. Bez ujmy na všeobecnosti môžeme predpokladať, že $\boldsymbol{A} = \{1, 2, \ldots, n\}$. Z každej triedy ekvivalencie R, čiže kombinácie s opakovaním, vyberieme slovo, ktoré je lexikograficky najmenšie (to znamená, že v ňom sú prvky množiny $\boldsymbol{A}$ zoradené podľa veľkosti). S trochou nepresnosti budeme toto slovo stotožňovať so samotnou kombináciou s opakovaním. Nech $c_1 c_2 \cdots c_k$ je teda kombinácia s opakovaním k-tej triedy v množine $\boldsymbol{A} = \{1, 2, \ldots, n\}$, pričom $c_1 \leq c_2 \leq \ldots \leq c_k$. Priraďme teraz tejto postupnosti novú postupnosť $d_1 d_2 \cdots d_k$ tak, že položíme

$$f(c_i) = d_i = c_i + i - 1, \quad i = 1, 2, \ldots, k$$

□

Všimnime si, že $d_i \in \{1, 2, \ldots, n + k - 1\}$ a že $d_1 < d_2 < \ldots < d_k$, teda postupnosť $d_1 d_2 \ldots d_k$ reprezentuje kombináciu bez opakovania k-tej triedy z množiny $\{1, 2, \ldots, n + k - 1\}$.

Napr. ak $c_1 c_2 \ldots c_k = 22233$, tak $d_1 d_2 \ldots d_k = 23467$.

Ľahko vidieť, že zobrazenie $c_1 c_2 \ldots c_k \longmapsto d_1 d_2 \ldots d_k$ je injektívne. Z druhej strany, ak
$\{e_1, e_2, \ldots e_k\} \subseteq \{1, 2, \ldots, n + k - 1\}$ je kombinácia bez opakovania k-tej triedy,

môžeme predpokladať, že $e_1 < e_2 < \ldots < e_k$. Postupnosti $e_1e_2\ldots e_k$ priradíme postupnosť $h_1h_2\ldots h_k$ takto:

$$h_i = e_i - i + 1, i = 1, 2, \ldots, k.$$

Ľahko vidno, že $h_1 \leq h_2 \leq \ldots \leq h_k$ a že $h_i \in \{1, 2, \ldots, n\}$. Teda $h_1h_2\ldots h_k$ je kombinácia s opakovaním k-tej triedy z množiny $\boldsymbol{A}$. Okrem toho, $f(h_i) = e_i$. Z uvedeného vyplýva, že zobrazenie

$$c_1c_2\ldots c_k \longmapsto d_1d_2\ldots d_k$$

definuje bijekciu medzi kombináciami k-tej triedy s opakovaním v množine $\{1, 2, \ldots, n\}$ a kombináciami bez opakovania k-tej triedy v množine $\{1, 2, \ldots, n + k - 1\}$. Hľadaný počet kombinácií s opakovaním je preto

$$\binom{n+k-1}{k}$$

Príklad 1. Uvažujme polynómy s viacerými premennými $x_1, x_2, \ldots, x_n$. Polynómy vytvárame z členov tvaru $x_{i_1}^{\alpha} x_{i_2}^{\beta} \ldots x_{i_l}^{\gamma}$, kde $\alpha > 0, \beta > 0, \ldots, \gamma > 0$, ktoré sa nazývajú monómy. Stupeň monómu je číslo $\alpha + \beta + \ldots + \gamma$ (v zápise automaticky predpokladáme, že $i_1, i_2, \ldots, i_l$ sú rôzne prvky množiny $\{1, 2, \ldots, n\}$). Polynóm je tvaru

$$\sum_{l=0}^{n} \sum_{i_1<i_2<\ldots<i_l} a_{i_1i_2\ldots i_l} x_{i_1}^{\varrho} x_{i_2}^{\sigma} \ldots x_{i_l}^{\tau}$$

pričom koeficienty $a_{i_1i_2\ldots i_l}$ sú nejaké čísla (môžu byť aj nuly) a $\varrho, \sigma, \ldots, \tau$ sú kladné exponenty (v rôznych monómoch môžu byť rôzne). Poznamenávame, že vo vnútornej sume sčítame cez všetky kombinácie l-tej triedy z množiny $\{1, 2, \ldots, n\}$.

Koľko je rozličných monómov stupňa k? Ak premenné $x_1, x_2, \ldots, x_n$ medzi sebou komutujú, tak na poradí nezáleží a exponent nad premennou vyjadruje počet opakovaní premennej v monóme - ide teda o kombinácie s opakovaním. Preto sa počet rôznych monómov stupňa k rovná číslu

$$\binom{n+k-1}{k}$$

Ak premenné medzi sebou nekomutujú, na poradí záleží, a potom máme dočinenia s variáciami s opakovaním. V tomto prípade je počet monómov n^k.

Príklad 2. Turista chce z dovolenky poslať k priateľom pohľadnice. Má na výber n druhov pohladníc. Koľkými spôsobmi môže nakúpiť k pohladníc? Koľkými spôsobmi môže nakúpené pohľadnice poslať?

Je očividné, že nakúpené pohľadnice tvoria neusporiadaný súbor a že môžeme z jedného druhu kúpiť viacero kusov pohľadníc (ak $k > n$, zrejme ani inú možnosť nemá). Súbory pohľadníc preto tvoria kombinácie s opakovaním. To znamená, že na nákup má

$$\binom{n+k-1}{k}$$

možností.

Koľkými spôsobmi môže pohľadnice poslať? Keby boli všetky pohľadnice navzájom rôzne, tak pohľadnice sa dajú rozoslať $k!$ spôsobmi, lebo rozoslanie predstavuje bijekciu medzi rôznymi druhmi pohľadníc a ich adresátmi. Ak je však z nejakého druhu viac pohľadníc, tieto sú medzi sebou zameniteľné. Predpokladajme, že v nakúpenom súbore je k_i pohľadníc i-teho druhu, $i = 1, 2, \ldots, n$ ($k_i \geq 0$). Dve bijekcie z množiny nakúpených pohľadníc do množiny priateľov budeme považovať za ekvivalentné, ak v obidvoch ten istý adresát dostane ten istý druh pohľadnice. Ak uvažujeme ľubovoľnú pevnú bijekciu, zámenou pohľadníc v i-tom druhu dostaneme z nej $k_i!$ ekvivaletných bijekcií. Tieto zámeny môžeme vykonať nezávisle v každom druhu. Podľa pravidla súčinu dostávame, že každá trieda ekvivalencie má $k_1!k_2!\ldots k_n!$ prvkov. Počet spôsobov rozoslania pohľadníc je teda

$$\frac{k!}{k_1!k_2!\ldots k_n!}.$$

V predchádzajúcom príklade sme skúmali vlastne takúto všeobecnú situáciu. Máme dve množiny A (pohľadnice) a B (priatelia), pričom $|A| = k = |B|$. Množina A je rozložená na množiny $A_1, A_2, \ldots, A_n$ s mohutnosťami $|A_i| = k_i$. V tomto mieste môžeme trocha porušiť definíciu rozkladu v tom, že pripustíme medzi množinami $A_1, A_2, \ldots, A_n$ aj prázdne množiny. Skúmame teraz bijekcie $A \to B$, pričom dve bijekcie f a g budeme považovať za ekvivalentné, ak pre každý prvok $y \in B$ existuje index $i \in \{1, 2, \ldots, n\}$ taký, že obidva prvky f^{-1} aj g^{-1} patria do tej istej množiny A_i. (V reči predchádzajúceho príkladu: každý adresát y dostal pri rozsielke f aj pri rozsielke g pohľadnicu toho istého druhu – hoci možno nie tú istú). Táto vlastnosť sa dá vyjadriť aj ináč. Nech $p: A \to \{A_1, A_2, \ldots, A_n\}$ je projekcia množiny na svoj rozklad; to znamená, že pre ľubovoľný prvok $a \in A$ platí $p(a) = A_i$ práve vtedy, keď $a \in A_i$. Potom f aj g sú ekvivalentné vtedy a len vtedy, keď $pf^{-1} = pg^{-1}$. Triedy ekvivalencie týchto bijekcií sa nazývajú *permutáciami s opakovaním* z k_1 prvkov prvého druhu, k_2 prvkov druhého druhu, …, k_n prvkov n-tého druhu. Úvahou v predchádzajúcom príklade sme ukázali, že počet takýchto permutácií s opakovaním je

$$\frac{k!}{k_1!k_2!\ldots k_n!}.$$

Tá istá hodnota sa objavuje aj ako počet iných konfigurácií.

Tvrdenie 2.18. *Nech A a B sú konečné množiny, kde $|A| = n$ a $|B| = k$. Nech $B = \{b_1, b_2, \ldots, b_k\}$. Potom počet zobrazení $f: A \to B$ takých, že pre každý prvok b_i platí $|f^{-1}(\{b_i\})| = n_i$, kde n_i sú zadané nezáporné celé čísla so súčtom $n_1 + n_2 + \ldots + n_k = n$, sa rovná*

$$\frac{n!}{n_1!n_2!\ldots n_k!}.$$

Dôkaz. Nech $(a_{i_1}, a_{i_2}, \ldots, a_{i_n})$ je ľubovoľná permutácia množiny A zakódovaná ako usporiadanie. Definujme zobrazenie $A \to B$ tak, že prvých n_1 prvkov množiny A pošleme na b_1, druhých n_2 prvkov na b_2 atď. Prvých n_1 prvkov môžeme však ľubovoľne spermutovať a zobrazenie sa nezmení. Nezávisle môžeme permutovať aj ďalšie skupiny. Z toho dostaneme, že $k_1!k_2!\dots k_n!$ permutácií dáva to isté zobrazenie. Je tiež zrejmé, že každé zobrazenie také, že $|f^{-1}(\{b_i\})| = m_i$ pre každý prvok $b_i \in B$, vznikne hore uvedeným spôsobom. Preto počet týchto zobrazení je $\frac{n!}{n_1!n_2!\dots n_k!}$. □

Čísla $\frac{n!}{n_1!n_2!\dots n_k!}$ sa zvyknú označovať $\binom{n}{n_1,n_2,\dots,n_k}$ a nazývať *polynomické koeficienty.* Ak $k=2$, tak

$$\binom{n}{n_1,n_2} = \binom{n}{n_1} = \binom{n}{n-n_1} = \binom{n}{n_2},$$

čiže polynomické koeficienty sú prirodzeným zovšeobecnením binomických koeficientov. Vysvetlenie názvu týchto čísel poskytuje nasledujúci výsledok.

Teoréma 2.19 (Polynomická veta)**.** *Nech n a k sú kladné prirodzené čísla. Potom*

$$(x_1 + x_2 + \dots + x_k)^n = \sum_{n_1,n_2,\dots,n_k} \binom{n}{n_1,n_2,\dots,n_k} x_1^{n_1}x_2^{n_2}\dots x_k^{n_k}, \quad n_i \geq 0$$

pričom sčítame cez všetky usporiadané n-tice prirodzených čísel $(n_1, n_2, \dots, n_k)$, pre ktoré $n_1 + n_2 + \dots + n_k = n$.

Dôkaz. Vynásobíme n činiteľov $(x_1+x_2+\dots+x_k)$ a združíme rovnaké monómy. Koeficient pri $x_1^{n_1}x_2^{n_2}\dots x_k^{n_k}$ je pritom počet spôsobov, ktorými sa tento monóm pri vynásobení získa. Zrejme $\boldsymbol{M} = x_1^{n_1}x_2^{n_2}\dots x_k^{n_k}$ vznikne vždy, keď x_1 vyberieme z n_1činiteľov,x_2 z n_2 činiteľov atď. Inými slovami, výraz $\boldsymbol{M}$ zodpovedá zobrazeniu z množiny n činiteľov do množiny $x_1, x_2, \dots, x_k$ pričom n_1 činiteľov je zobrazených na x_1, n_2 činiteľov na x_2 atď. Počet takýchto zobrazení je podľa tvrdenia 2.18

$$\frac{n!}{n_1!n_2!\dots n_k!} = \binom{n}{n_1,n_2,\dots,n_k}$$

□

Poznámka. Ľahko sa nahliadne,že

$$\binom{n}{n_1,n_2,\dots,n_k} = \binom{n}{n_1}\binom{n-n_1}{n_2}\dots\binom{n-n_1-n_2-\dots-n_{k-1}}{n_k}$$

Táto rovnosť zodpovedá skutočnosti, že počet spôsobov, ktorými vznikne monóm $x_1^{n_1}x_2^{n_2}\dots x_k^{n_k}$, sa dá popísať aj takto: najprv vyberieme x_1 z n_1 členov $(x_1 + x_2 + \dots + x_n)$, čo môžeme urobiť $\binom{n}{n_1}$ spôsobmi. Potom vyberieme x_2 z n_2 spomedzi zvyšných $n - n_1$ členov, čo môžeme urobiť $\binom{n-n_1}{n_2}$ spôsobmi, atď. kým nevyberieme aj x_k z n_k spomedzi ostávajúcich $n-n_1-n_2\dots-n_{k-1}$ členov, čo môžeme urobiť $\binom{n-n_1-n_2-\dots-n_{k-1}}{n_k}$ spôsobmi.

2.7 Princíp zapojenia a vypojenia

Začneme jednoduchou otázkou. Ak sú dané dve konečné množiny A a B, ako vypočítame počet prvkov ich zjednotenia? Odpoveď je očividná: od súčtu mohutností množín A a B musíme odrátať mohutnosť ich prieniku. Inými slovami,

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

Pre tri množiny je odpoveď podobná:

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|.$$

To znamená, že najprv „zapojíme“ prvky jednotlivých množín, potom „vypojíme“ prvky prienikov dvojíc množín a napokon opäť „zapojíme“ prvky prieniku všetkých troch množín. (Čitateľovi odporúčame presvedčiť sa o platnosti tohto vzťahu s pomocou Vennovho diagramu pre tri prenikajúce sa množiny.)

Princíp *zapojenia a vypojenia* (alebo *inklúzie a exklúzie*) je ďalekosiahlym zavšeobecnením vyššie uvedených vzťahov pre dve a tri množiny.

Nech $M_1, M_2, \ldots, M_n$ sú konečné množiny. Pre ľubovoľné prirodzené číslo k také, že $0 \leq k \leq n$ položme

$$S_k = \sum_{i_1 < i_2 < \ldots < i_k} |M_{i_1} \cap M_{i_2} \cap \ldots \cap M_{i_k}|,$$

pričom súčet prebieha cez všetky kombinácie $\{i_1, i_2, \ldots, i_k\}$ z indexov $\{1, 2, \ldots, n\}$. Pre $k = 0$ dostávame prienik množín M_i z prázdnej množiny indexov, čo podľa dohody z prvej kapitoly je univerzum – základná množina X, v ktorej vedieme všetky úvahy o množinách $M_1, M_2, \ldots, M_n$. Preto

$$S_0 = |X|.$$

Teoréma 2.20 (Princíp zapojenia a vypojenia)**.** *Nech $M_1, M_2, \ldots, M_n$ sú konečné množiny. Potom*

$$\begin{aligned} |M_1 \cup M_2 \cup \ldots \cup M_n| &= \sum_{k=1}^{n} (-1)^{k+1} \sum_{i_1 < i_2 < \ldots < i_k} |M_{i_1} \cap M_{i_2} \cap \ldots \cap M_{i_k}| = \\ &= \sum_{k=1}^{n} (-1)^{k+1} S_k \end{aligned}$$

Dôkaz. Nech x je ľubovoľný prvok z množiny $M_1 \cap M_2 \cap \ldots \cap M_n$. Zaveďme označenie

$$J_x = \{i; x \in M_i\}.$$

Aby sme ukázali, že pravá a ľavá strana rovnosti predstavujú to isté číslo, všimnime si, že prvok x je na ľavej strane zarátaný iba raz. Ak totiž preberáme prvky množiny $M_1 \cap M_2 \cap \ldots \cap M_n$, na x naďabíme len raz. Koľkokrát je započítaný na pravej strane?

Predpokladajme, že prvok x patrí do p množín M_i; to znamená, že $J_x = \{j_1, j_2, \ldots, j_p\} \subseteq \{1, 2, \ldots, n\}$. Z toho vyplýva, že v S_1 je prvok x zarátaný $p = \binom{p}{1}$-krát, totiž v každom sčítanci $|M_{j_1}|, |M_{j_2}|, \ldots, |M_{j_p}|$. V S_2 je x zarátaný $\binom{p}{2}$-krát, raz za každý sčítanec tvaru $|M_{j_i} \cap M_{j_2}|$. Všeobecne - prvok x je zarátaný v S_i $\binom{p}{i}$-krát. Celkove je teda prvok x na pravej strane započítaný toľkokrát:

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

Podľa dôsledku 2.14(b) dostávame

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

čiže prvok x je aj na pravej strane zarátaný práve raz. To dokazuje našu teorému. $\square$

Poznámka. Teorému 2.20 môžeme ľahko dokázať aj matematickou indukciou. Najprv sa presvedčíme o platnosti vzťahu pre dve množiny M_1 a M_2. Nech je vzťah platný pre $n \geq 2$ množín. Zoberme teraz $n+1$ množín $M_1, M_2, \ldots, M_n, M_{n+1}$. Na hľadaný počet $|M_1 \cup M_2 \cup \ldots \cup M_n \cup M_{n+1}|$ použime vzťah pre dve množiny:

$$|M_1 \cup M_2 \cup \ldots \cup M_n \cup M_{n+1}| = |(M_1 \cup M_2 \cup \ldots \cup M_n) \cup M_{n+1}| =$$
$$= \left|\bigcup_{k=1}^{n} M_k\right| + |M_{n+1}| - \left|\left(\bigcup_{k=1}^{n} M_k\right) \cap M_{n+1}\right|.$$

Na tretí sčítanec aplikujeme distributívny zákon, čím z neho dostaneme

$$\left|\bigcup_{k=1}^{n}(M_k \cap M_{n+1})\right|.$$

Potom použijeme indukčný predpoklad na prvý a tretí sčítanec. Po úprave dostaneme požadovaný vzťah pre $n+1$. Podrobnosti prenechávame na čitateľa.

Predpokladajme teraz, že množiny $\boldsymbol{M}_1, \boldsymbol{M}_2, \ldots, \boldsymbol{M}_n$ sú podmnožinami nejakej konečnej množiny $\boldsymbol{X}$. Aký počet má komplement množiny $\boldsymbol{M}_1 \cup \boldsymbol{M}_2 \cup \ldots \cup \boldsymbol{M}_n$ v univerze $\boldsymbol{X}$?

Počítajme

$$|\boldsymbol{X} - (\boldsymbol{M}_1 \cup \boldsymbol{M}_2 \cup \ldots \cup \boldsymbol{M}_n)| = |\boldsymbol{X}| - |\boldsymbol{M}_1 \cup \boldsymbol{M}_2 \cup \ldots \cup \boldsymbol{M}_n|$$
$$= |\boldsymbol{X}| - \sum_{k=1}^{n}(-1)^{k+1}\ S_k = |\boldsymbol{X}| + \sum_{k=1}^{n}(-1)^{k}\ S_k$$
$$= \sum_{k=0}^{n}(-1)^{k}\ S_k.$$

Tým sa dostali k nasledujúcemu výsledku:

Dôsledok 2.21. *Nech $\boldsymbol{M}_1, \boldsymbol{M}_2, \ldots, \boldsymbol{M}_n$ sú podmnožiny konečnej množiny $\boldsymbol{X}$ a nech $\boldsymbol{M}_i'$ je komplement množiny $\boldsymbol{M}_i$ v univerze $\boldsymbol{X}$, $i = 1, 2, \ldots, n$. Potom*

$$|\boldsymbol{M}_1' \cap \boldsymbol{M}_2' \cap \ldots \cap \boldsymbol{M}_n'| = \sum_{k=0}^{n} (-1)^k \; S_k$$

Dôkaz. Výsledok vyplýva z predchádzajúceho výpočtu a z jedného z de Morganových zákonov. ☐

Predchádzajúci výsledok je základom najpoužívanejšej formy princípu zapojenia a vypojenia, ktorú teraz opíšeme.

Majme nejakú základnú množinu $\boldsymbol{X}$, pričom $|\boldsymbol{X}| = N$ a nech $\alpha_1, \alpha_2, \ldots, \alpha_n$ sú nejaké vlastnosti, ktoré prvky množiny môžu, no nemusia, mať. Nech $N\alpha_{i_1}\alpha_{i_2}\ldots\alpha_{i_k}$ je počet prvkov množiny $\boldsymbol{X}$, ktoré majú každú z vlastností $\alpha_{i_1}, \alpha_{i_2}, \ldots, \alpha_{i_k}$ (a prípadne aj iné vlastnosti, no tie nás nezaujímajú). Nech $N(0) = N\alpha_1'\alpha_2'\ldots\alpha_n'$ označuje počet prvkov množiny $\boldsymbol{X}$, ktoré nemajú žiadnu z vlastností $\alpha_1, \alpha_2, \ldots, \alpha_n$. Naším cieľom je vypočítať $N(0)$.

Položme

$$\boldsymbol{M}_i = \{x \in \boldsymbol{X};\ x \text{ má vlastnosť } \alpha_i\}.$$

Potom

$$|\boldsymbol{M}_{i_1} \cap \boldsymbol{M}_{i_2} \cap \ldots \cap \boldsymbol{M}_{i_k}| = N\alpha_{i_1}\alpha_{i_2}\ldots\alpha_{i_k},$$

pričom prienik množín $\boldsymbol{M}_i$ z prázdnej množiny indexov dáva

$$|\cap_{i\in\emptyset} \boldsymbol{M}_i| = |\boldsymbol{X}| = N$$

a

$$|\boldsymbol{M}_1' \cap \boldsymbol{M}_2' \cap \ldots \cap \boldsymbol{M}_n'| = N\alpha_1'\alpha_2'\ldots\alpha_n' = N(0).$$

Z predchádzajúceho dôsledku dostávame

Dôsledok 2.22. *V N-prvkovej množine nech každý prvok má alebo nemá niektoré z vlastností $\alpha_1, \alpha_2, \ldots, \alpha_n$. Nech $N\alpha_{i_1}\alpha_{i_2}\ldots\alpha_{i_k}$ označuje počet prvkov, ktoré majú každú z vlastností $\alpha_{i_1}, \alpha_{i_2}, \ldots, \alpha_{i_k}$ prípadne aj nejaké iné. Nech $N(0) = N\alpha_1'\alpha_2'\ldots\alpha_n'$ označuje počet prvkov uvažovanej množiny, ktoré nemajú žiadnu z vlastností $\alpha_1, \alpha_2, \ldots, \alpha_n$. Potom*

$$N(0) = \sum_{k=0}^{n} (-1)^k S_k = \sum_{k=0}^{n} (-1)^k \sum_{i_1<i_2<\ldots<i_k} N\alpha_{i_1}\alpha_{i_2}\ldots\alpha_{i_k}. \qquad \square$$

Poznámka. Existuje praktický spôsob ako si môžeme ľahko zapamätať predchádzajúci vzorec ako aj množstvo podobných vzťahov. Predpokladajme, že chceme určiť počet prvkov, ktoré majú vlastnosti $\alpha_{i_1}, \alpha_{i_2}, \ldots, \alpha_{i_r}$ a nemajú vlastnosti $\alpha_{j_1}, \alpha_{j_2}, \ldots, \alpha_{j_s}$. Prirodzene predpokladáme, že $\{i_1, i_2, \ldots, i_r, j_1,$

$j_2, \ldots, j_s\} \subseteq \{1, 2, \ldots, n\}$ a že všetky uvažované vlastnosti sú navzájom rôzne. Potom hľadaný počet získame formálnym rozvojom výrazu

$$N\alpha_{i_1}\alpha_{i_2}\ldots\alpha_{i_r}(1-\alpha_{j_1})(1-\alpha_{j_2})\ldots(1-\alpha_{j_s})$$

podľa distributívneho zákona, pričom $N.1 = N$, $N.\alpha_i = N\alpha_i$ a podobne. Napríklad počet prvkov, ktoré majú vlastnosť α_1 a nemajú ani vlastnosť α_2 ani α_3 je

$$\begin{aligned} N\alpha_1(1-\alpha_2)(1-\alpha_3) &= N\alpha_1(1-\alpha_2-\alpha_3+\alpha_2\alpha_3) = \\ &= N\alpha_1 - N\alpha_1\alpha_2 - N\alpha_1\alpha_3 + N\alpha_1\alpha_2\alpha_3. \end{aligned}$$

špeciálne

$$N(0) = N\alpha_1'\alpha_2'\ldots\alpha_n' = N(1-\alpha_1)(1-\alpha_2)\ldots(1-\alpha_n)$$

Rozvinutím posedného výrazu dostávame napokon vzťah z dôsledku 2.22,

$$N(1-\alpha_1)(1-\alpha_2)\ldots(1-\alpha_n) = \sum_{k=0}^{n}(-1)^k \sum_{i_1<i_2<\ldots<i_k} N\alpha_{i_1}\alpha_{i_2}\ldots\alpha_{i_k},$$

o čom sa ľahko presvedčíme matematickou indukciou.

V predchádzajúcom dôsledku sme určili počet $N(0)$ všetkých spomedzi N prvkov, ktoré nemajú žiadnu z uvažovaných vlastností. Tento výsledok je možné zovšeobecniť - dá sa totiž určiť aj počet $N(r)$ všetkých prvkov, ktoré majú práve r vlastnosti, ako aj počet $N(\geq r)$ všetkých prvkov, ktoré majú aspoň r vlastností:

$$N(r) = \sum_{k=r}^{n}(-1)^{k-r}\binom{k}{r}S_k$$

$$N(\geq r) = \sum_{k=r}^{n}\binom{k-1}{r-1}S_k$$

Niekedy je tieto súčty namáhavé presne vypočítať (čo býva pravidlom pri súčtoch so striedavými znamienkami), preto sa vtedy musíme uspokojiť s približnými hodnotami. Namiesto úplného súčtu

$$N(r) = \sum_{k=r}^{n}(-1)^{k-r}\binom{k}{r}S_k$$

s hornou hranicou sčítania n uvažujeme len súčet

$$N(r)_s = \sum_{k=r}^{r+s}(-1)^{k-r}\binom{k}{r}S_k$$

prvých s členov úplného súčtu. Tieto oscilujú okolo hľadanej hodnoty $N(r)$, pričom ak s je nepárne, čiastočný súčet je pod hľadanou hodnotou:

$$N(r)_s \leq N(r).$$

Ak s je párne, čiastočný súčet je nad hľadanou hodnotou :

$$N(r)_s \geq N(r).$$

Tieto vzťahy a odhady nachádzajú svoje praktické uplatnenie pri vyčíslení pravdepodobností rozličných javov. Ich dôkazy však presahujú rámec tohto textu.

Príklad 3. Skupina N pánov sa má zúčastniť večierka. Hostiteľ vyžaduje od účastníkov formálny odev – frak a tvrdý čierny klobúk. Pred vstupom do sály páni odovzdajú svoje klobúky v šatni. Večierok prebehne veľmi úspešne a páni pri svojom odchode nie sú schopní rozoznať svoje klobúky. Aká je pravdepodobnosť toho, že žiaden pán si nezoberie vlastný klobúk?

Ak pánov aj ich klobúky očíslujeme $1, 2, \dots, N$, tak rozmiestnenie klobúkov na hlave predstavuje permutáciu množiny $\{1, 2, \dots, N\}$. Naším cieľom je najprv určiť počet D_N permutácií, ktoré nenechávajú žiaden prvok na mieste. Počet permutácií, ktoré nechávajú na mieste k-prvkovú podmnožinu $\{i_1, i_2, \dots, i_k\}$ je $(N-k)!$. S použitím vyššie zavedených označení dostaneme

$$S_k = \binom{N}{k}(N-k)!,$$

odkiaľ zisťujme, že hľadaný počet permutácií je

$$\begin{aligned} D_N = N(0) = \sum_{k=0}^{N}(-1)^k S_k = \sum_{k=0}^{N}(-1)^k \binom{N}{k}(N-k)! = \\ = \sum_{k=0}^{N}(-1)^k \frac{N!}{k!(N-k)!}(N-k)! = N! \sum_{k=0}^{N} \frac{(-1)^k}{k!} \end{aligned}$$

Keďže všetkých permutácií N prvkov je $N!$, pravdepodobnosť toho, že žiaden pán nemá na hlave svoj klobúk je

$$\frac{N! \sum\limits_{k=0}^{N} \frac{(-1)^k}{k!}}{N!} = \sum_{k=0}^{N} \frac{(-1)^k}{k!}.$$

Z matematickej analýzy poznáme Taylorov rozvoj funkcie e^x, ktorý dáva vzťah

$$e^x = \sum_{k=0}^{\infty} \frac{x^k}{k!},$$

Pre $x = -1$ dostávame rovnosť

$$e^{-1} = \sum_{k=0}^{\infty} \frac{(-1)^k}{k!},$$

z čoho vidno, že nami určená pravdepodobnosť je N-ty čiastočný súčet tohto rozvoja čísla e^{-1}. Ak je číslo N dostatočne veľké, tak hľadaná pravdepodobnosť je približne $1/e$ – o čosi viac ako $1/3$.

Na záver uvedieme ešte dve aplikácie princípu zapojenia a vypojenia. Ich dôkaz ponecháme na čitateľovi.

Dôsledok 2.23. *Počet surjektívnych zobrazení $f\colon A \to B$, kde $|A| = n$ a $|B| = m$, je*

$$S_B^A = \sum_{k=0}^{m} (-1)^k \binom{m}{k} (m-k)^n. \qquad \square$$

Dôsledok 2.24. *Nech $\varphi(n)$ označuje počet kladných prirodzených čísel menších ako prirodzené číslo $n > 1$ a nesúdeliteľných s n. Nech $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$ je kánonický rozklad čísla n na súčin mocnín rôznych prvočísiel $p_1, p_2, \dots, p_r$. Potom*

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_r}\right). \qquad \square$$

Index