Jakýsi úvod do diskrétní matematiky

Áďa Klepáčovic

1. února 2023

Obsah

1 | Zajímavé problémy

Jednou z hlavních a oblíbených podmnožin diskrétní matematiky a kombinatoriky je *teorie grafů*. Jednoduše řečeno, graf je množina bodů – vrcholů, mezi některými z nich vedou spojnice – hrany.

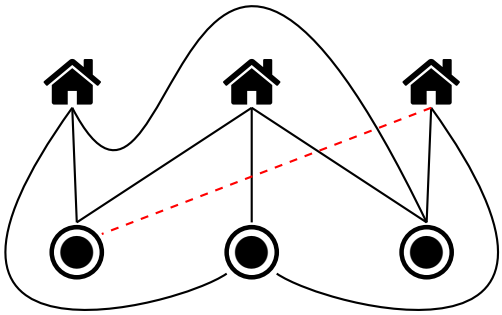
Představíme si pár úloh jako ze života, jak bývá v matematice zvykem, jejichž zdánlivá nevinnost je v rozporu s jejich významem pro rozvoj teorie.

1.1 Problém tří domů a tří studní

V zemi za sedmero horami a sedmero řekami žili byli tři sousedi. Každý z nich vlastnil rodinný domek a dělili se o vodu ze tří blízkých studní. Jednou se ale sousedi po sporu rozkmotřili a už se nechtěli ani vidět. Potřebovali ale pitnou vodu. Každý se odmítl vzdát nároku na nějakou ze studní, tak si jako poslední společný čin najali dvorního architekta, by nechal postavit cesty od každého domu ke každé studni. Cesty se nesměly nikde potkat, aby do sebe sousedi na cestě pro vodu náhodou nenarazili.

Dvorní architekt, probděv tři dny a tři noci hledaje způsob, jak nasupené sousedy uspokojit, klekl nakonec únavou a prohlásil, že cesty bez křížení vystavět nelze.

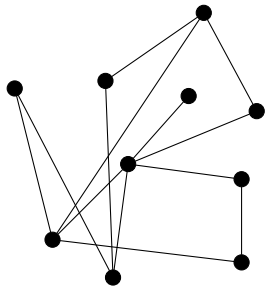
My s ním souhlasíme, ale není lehké najít způsob, jak úlohu matematicky formalizovat, a podat důkaz.



Obrázek 1: Tři domy a tři studně.

1.2 Hrátky s puntíky

Ukážeme si ještě dvě pěkné úlohy s puntíky a čarami. Mějme třeba deset puntíků v rovině a pár z nich spojme čarami, jako na obrázku 2.



Obrázek 2: Náhodný graf na deseti vrcholech.

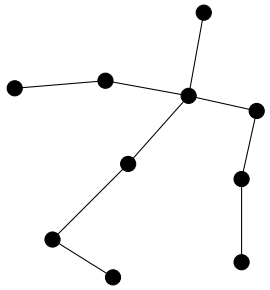
Otázka, kterou se budeme časem zabývat zní „Kolik maximálně mohu nakreslit spojnic, než mi vznikne trojúhelník?“ Trojúhelníkem zde myslíme trojici bodů, z nichž každé dva jsou spojeny. Do tohoto grafu se určitě ještě dají nějaké přikreslit, ale kolik přesně? A jak tuto úlohu řešit obecně pro jakýkoliv počet bodů?

Podobně zajímavá, ale už víc algoritmická otázka, by zněla „Jak poznám, jestli v nějakém grafu existuje trojúhelník?“. Samozřejmě by šlo se prostě podívat na každou jednu trojici bodů, ale jde to i líp?

Ještě na pár odstavců zůstaneme u spojených puntíků. Úloha, která se ukázala jako zásadní v teorii grafů má co dělat s cestami. *Cestou* v grafu nazveme posloupnost bodů – vrcholů, takovou, že mezi sousedními vrcholy na cestě vždycky vede spojnice. Jinak řečeno, mohu se v klidu projít od jednoho vrcholu k druhému, aniž bych musel skákat mezi vrcholy. Naším úkolem je najít takovou množinu spojnic – hran, že se mezi každými dvěma vrcholy dá projít po cestě.

Pro deset vrcholů jedno možné řešení vidíte na obrázku 3.

Je jednoduché si rozmyslet, kolik nejméně hran je třeba nakreslit. Ovšem, co když můžeme vybírat jen z nějaké předem dané množiny? Řešení pak nemusí vždycky existovat (může se totiž stát, že žádné hrany k dispozici nemáme). Dá se nějak efektivně poznat, kdy úlohu lze řešit a kdy ne? A co třeba otázka, kolik existuje řešení s minimálním počtem hran; co řešení, součet přes všechny jehož hrany je nejmenší? V této obecné podobě



Obrázek 3: Minimální kostra grafu na deseti vrcholech.

se úloze (i jejímu řešení) říká *minimální kostra* grafu a v budoucnu ji, stejně jako předchozí dvě úlohy, potkáme.

2 | Úvodní pojmy

Žádná matematická disciplína se neobejde bez pochopení základů logiky a teorie množin. Pro jistotu zde nejnutnější části připomeneme, ale tyto krátké úryvky nezamýšlejí naučit, leč osvěžit.

2.1 Logické spojky a kvantifikátory

Definice 2.1.1 (Výrok)**.** Výrokem nazveme jakoukoli větu, o které lze rozhodnout, zda je pravdivá, či nikoliv.

Příklad. Věty „Je mi zle.“ a „Sumec je drůbež.“ jsou výroky, zatímco „Tvoje máma.“ a „Cos’ dostala z matiky?“ nikoliževěk.

Je též dlužno mít na paměti, že naše znalost pravdivosti věty nemění nic na tom, jestli daná věta je, nebo není výrokem. Třeba „Do pěti století kolonizujeme celou Sluneční soustavu.“ je zcela jistě výrok.

Další text vyžaduje znalost operátorů $\neg, \wedge, \vee, \Rightarrow$ a $\Leftrightarrow$. Je-li x výrok „Prší.“ a y výrok „Vezmu si deštník.“, pak

- výrok $\neg x$ znamená „**Ne**prší.“,

- výrok $x \wedge y$ znamená „Prší **a** vezmu si deštník.“,
- výrok $x \vee y$ znamená „Prší **nebo** si vezmu deštník.“,
- výrok $x \Rightarrow y$ znamená „**Když** prší, **tak** si vezmu deštník.“ a
- výrok $x \Leftrightarrow y$ znamená „Prší, **právě tehdy když** si vezmu deštník.“

Výstraha.

- Logická spojka $\vee$ **není výlučná**. Tedy $x \vee y$ platí v situaci, kdy
  - platí pouze x,
  - platí pouze y,
  - platí x i y.
- Výrok $x \Rightarrow y$ je vždy **pravdivý**, pokud x je **lživý**. Jinak řečeno, $x \Rightarrow y$ platí za situace, kdy
  - platí x i y,
  - neplatí x a platí y,
  - neplatí x a neplatí y.

Jako znalost logických spojek je kritická i znalost kvantifikátorů $\forall$ a $\exists$, které se čtou „pro všechny“ a „existuje“, resp.

Pokud je $p(x)$ výrok závislý na proměnné x (třeba „x je sudé.“), pak výrok

- $\forall x \in \mathbb{N} : p(x)$ zní „Všechna přirozená čísla jsou sudá.“ a
- $\exists x \in \mathbb{N} : p(x)$ zní „Existuje sudé přirozené číslo.“

Budeme rovněž užívat kvantifikátory $\exists!$ a $\nexists$, které znamenají „existuje přesně jeden“ a „neexistuje“.

Podáno intutivně: chci-li tvrdit, že $\forall x \in \mathbb{N} : p(x)$, musím dokázat, že ať mi nepřítel dá **jakékoliv** přirozené číslo x, tak $p(x)$ platí. Naopak, dokázat $\exists x \in \mathbb{N} : p(x)$ je obvykle zásadně jednodušší, neboť musím pouze najít **jedno** přirozené číslo x, pro které $p(x)$ platí.

2.2 Množiny

Požaduji znalost značek $\in, \cap, \cup, \setminus, \times$ a $\subseteq$. Pro připomenutí, jsou-li A, B dvě množiny, pak

- výrok $x \in A$ říká, že „x je prvkem A.“ nebo „ x patří do A.“;
- $A \cap B$ je **průnik** A s B, čili množina obsahující prvky, které patří jak do A, tak do B;
- $A \cup B$ je **sjednocení** A s B, čili množina obsahující prvky, které patří do A nebo do B;
- $A \setminus B$ je **rozdíl** A s B, čili množina obsahující prvky, které patří do A a nepatří do B;
- $A \times B$ je **součin** A s B, čili množina **uspořádaných** dvojic (a, b), kde $a \in A$ a $b \in B$. Uspořádaná dvojice zde znamená, že $(a, b) \neq (b, a)$, tedy záleží na tom, který prvek je první a který druhý;
- výrok $A \subseteq B$ říká, že A je podmnožinou B, tedy, že každý prvek A je rovněž prvkem B.

Pro mnohonásobné a nekonečné verze budeme používat stejné symboly (s výjimkou součinu). Tedy, mám-li množiny $A_1, \ldots, A_n$, pak

- $\bigcap_{i=1}^{n} A_i$ je jejich průnik,
- $\bigcup_{i=1}^{n} A_i$ je jejich sjednocení a
- $\prod_{i=1}^{n} A_i$ je jejich součin.

Když jsou počáteční a koncový index známy z kontextu, budeme je vynechávat a psát pouze třeba $\bigcup A_i$. Součin množiny se sebou samou budeme často zkracovat mocninným zápisem, třeba $A \times A \times A = A^3$.

Příklad. Je-li $A = \{1, 3, 4\}$ a $B = \{2, 4, 5\}$, pak

- $A \cap B = \{4\}$,
- $A \cup B = \{1, 2, 3, 4, 5\}$,
- $A \setminus B = \{1, 3\}$ a

- $A \times B = \{(1,2),(1,4),(1,5),(3,2),(3,4),(3,5),(4,2),(4,4),(4,5)\}$.

Definice 2.2.1. Je-li A množina, pak

- $\#A$ značí **počet prvků** A neboli **velikost** A,
- 2^A značí **množinu všech podmnožin** A, čili

$$2^A := \{B \mid B \subseteq A\}.$$

Pro nekonečné množiny píšeme $\#A = \infty$.

Výstraha. Pojem velikosti takto zavedený není korektně definovaný. Není totiž jasné, co by měl „počet“ prvků znamenat. Pojem *bijekce* ze sekce o zobrazeních tento problém vyřeší.

Tvrzení 2.2.1 (Vlastnosti velikosti množiny)**.**

(1) $\#A \times B = \#A\#B$.

(2) $\#2^A = 2^{\#A}$.

Důkaz.

(1) Pro každý prvek $a \in A$ je v $A \times B$ právě $\#B$ dvojic (a,b), kde $b \in B$. Jelikož prvků $a \in A$ je z definice $\#A$ a každému odpovídá $\#B$ dvojic (a,b), je celkový počet uspořádaných dvojic v $A \times B$ právě $\#A\#B$.

(2) Pro nekonečné množiny tvrzení platí zřejmě. Předpokládejme, že A je konečná.

Očíslujeme si podmnožiny A binárními čísly délky $\#A$. Každá podmnožina A vznikne totiž tak, že procházíme postupně všechny prvky A a u každého se rozhodujeme, zda ho do ní zařadíme či nikoliv. Kladnému rozhodnutí bude odpovídat cifra 1 a zápornému 0. Má-li A řekněme 5 prvků, pak podmnožina očíslovaná číslem 00110 je podmnožina, která obsahuje pouze 3. a 4. prvek z A (při libovolném, **ale fixním**, očíslování samotné množiny A).

Odtud plyne, že A má tolik podmnožin, kolik je různých binárních čísel délky $\#A$. Těch je však $2^{\#A}$, jak jsme chtěli. □

2.3 Relace

Pojem *relace* zobecňuje věci jako zobrazení (se kterým jste se setkali, ale říkali jste mu bůhvíproč funkce) nebo uspořádání (které taky znáte, jen vám bůhvíproč neprozradili, oč jde).

Základní myšlenkou je to, že i relace – vztahy mezi objekty se dají pomocí množin (a jejich součinu) úspěšně definovat. Celá matematika, kterou jste dosud poznali, je založená na *teorii množin*, jinak řečeno, **všechno** je množina.

Definice 2.3.1 (Relace). Jsou-li A, B množiny, pak **relací** mezi A a B nazveme *libovolnou* podmnožinu $A \times B$. Je-li $A = B$, pak R nazýváme relací na A.

Pojem relace v matematice je založen na konceptu, že vztah mezi množinami je dokonale popsán výpisem všech dvojic prvků, které v tom vztahu jsou. To se trochu liší od běžného chápání slova „vztah“. Asi byste nebyli úplně spokojení, kdybychom vám tvrdili, že vztah manželský na množině všech lidí je to samé, co výpis všech manželských párů. Z toho důvodu bude asi lepší se držet latinské verse, „relace“.

Protože nejstarší typy relací, mezi nimi třebas $<$ nebo $=$, lidé používali ještě před vznikem samotné teorie množin, značení je zde trochu matoucí. Fakt, že dvojice $(x, y) \in A \times B$ je v relaci R, nezapisujeme (jak by se čekalo) $(x, y) \in R$, ale spíš xRy. Podobně jako nepíšeme $(x, y) \in <$, ale $x < y$.

Jako spoustu věcí v matematice, relace je dobré si umět vizualizovat. Ukážeme si teď tři standardní způsoby, jak si lidé relace kreslí.

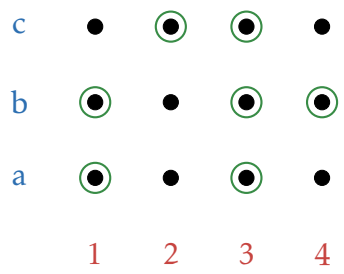
2.3.1 Kreslení relací

Po celou podsekci budeme předpokládat, že máme množiny $A = \{1, 2, 3, 4\}$ a $B = \{a, b, c\}$.

Jedním ze způsobů, jak se dají kreslit relace, je *mříž*. Uvážíme relaci

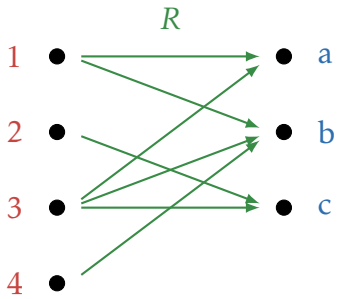
$$R = \{(1,a),(1,b),(2,c),(3,a),(3,b),(3,c),(4,b)\}$$

mezi A a B. Vizualizaci součinu $A \times B$ a relace R pomocí mříže vidíte na obrázku 4.



Obrázek 4: Kreslení relace $R \subseteq A \times B$ pomocí mříže.

Ještě jeden užitečný způsob kreslení, který funguje pro obecné relace, je kreslení pomocí šipek. V zásadě si člověk zobrazí obě množiny jako sloupce bodů a mezi příslušnými body kreslí šipky. Například jako na obrázku 5.



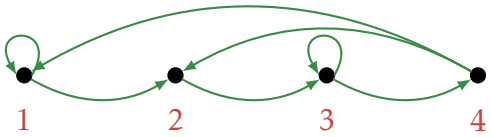
Obrázek 5: Kreslení relace $R \subseteq A \times B$ pomocí šipek.

Tenhle způsob se může zdát méně přehledný než mříž, ale má svoje nesporné využití, především v oblasti *skládání* relací, kterým se budeme zabývat za chvíli.

Ještě před tím si ale ukážeme způsob, jak přehledně kreslit relace na nějaké množině. Řekněme, že tentokrát je třeba

$$R := \{(1,1),(1,2),(2,3),(3,4),(3,3),(4,1),(4,2)\}$$

relace na množině A. Množinu A si nakreslíme jako body v rovině a relaci R jako šipky a smyčky. Vizte obrázek 6.



Obrázek 6: Kreslení relace R na A pomocí šipek a smyček.

2.3.2 Skládání relací

V této podsekci si řekneme, co znamená, že dvě (nebo více) relace složíme dohromady. Tato operace se dá vnímat jako jakési „zobecnění“ skládání zobrazení/funkcí. Jak si ale ukážeme, zobrazení jsou speciálním typem relací, takže tahle představa není úplně vhodná.

Pro jednoduchost se budeme soustředit na relace na nějaké množině A. Tohle ovšem není nutné; mám-li relaci $R \subseteq A \times B$ a relaci $S \subseteq B \times C$, vždy je mohu složit a dostat relaci mezi A a C.

Skládání relací není nijak divoká věc a vztahy (například mezi lidmi) v životě běžně skládáme, ale málokdy se na to asi díváme tímto způsobem. Například, řekněme, že Adéla má přítelkyni Simona a Simona má přítelkyni Terezu. Když složíme relace „býti přítelkyně Adély“ a „býti přítelkyně Simony“ dostaneme relaci, ve které je Tereza přítelkyně Adély. Na druhý příklad, třeba samotné přísloví „Nepřítel mého nepřítele je můj přítel.“, se dá vyložit jako skládání relací.

Teď formálně.

Definice 2.3.2 (Složení relací)**.** Mějme množinu A a relace $R, S \subseteq A \times A = A^2$. Složením relací R a S nazveme množinu

$$\{(x,z) \in A^2 \mid \exists y \in A : xRy \wedge yRz\}$$

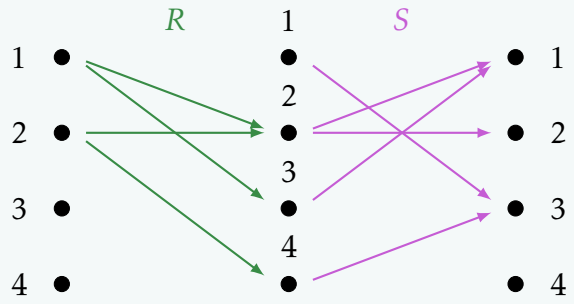
a značíme ji $R \circ S$.

Řečeno asi možná třeba trošku lidštěji, když pro dané $x, z \in A$ najdu takový prvek $y \in A$, že dvojice (x,y) je v relaci R a dvojice (y,z) je v relaci S, pak (x,z) je v relaci $R \circ S$. Vlastně (x,y) a (y,z) slepím dohromady skrze y.

Příklad. Řekněme, že je $A = \{1, 2, 3, 4\}$ a máme relace

$$R := \{(1,2), (1,3), (2,2), (2,4)\},$$
$$S := \{(1,3), (2,1), (2,2), (3,1), (4,3)\}$$

na A. V podsekci o kreslení relací jsme zmínili, že šipky jsou velmi užitečné při skládání. Teď uvidíte proč. Když si obě relace nakreslíme přímo vedle sebe, dostaneme obrázek 7.



Obrázek 7: Složení relací R a S.

V roli x z Definice 2.3.2 je zde první sloupec, v roli y druhý a v roli z třetí. Čili, prvek (x, z) bude v relaci $R \circ S$ jenom tehdy, když najdu v prostředním sloupci prvek y (aspoň jeden, ale klidně víc), přes který dokážu po šipkách dojít z x do z.

Z obrázku je teď už zřejmé, že

$$R \circ S = \{(1,1), (1,2), (2,1), (2,2), (2,3)\}.$$

2.4 Ekvivalence

Jedním speciálním typem relace na množině je tzv. *ekvivalence*. Důvodem pro tenhle název je fakt, že prvky, které jsou v relaci ekvivalence, jde za jisté interpretace považovat za „stejné“. Asi nejobyčejnější příklad užití ekvivalence je při definici množiny racionálních čísel, $\mathbb{Q}$, jak si brzy ukážeme. Nejprve ale definice ekvivalence.

Definice 2.4.1 (Ekvivalence). Relace $R \subseteq A^2$ je

- **reflexivní**, když je každý prvek v relaci sám se sebou, tj.

$$xRx \quad \forall x \in A;$$

- **symetrická**, když ke každé dvojici obsahuje i opačně uspořádanou, tj.

$$xRy \Rightarrow yRx \quad \forall x, y \in A;$$

- **transitivní**, když ke každým dvěma dvojicím, které jdou „slepit přes prostředníka“ (vizte definici skládání) obsahuje i tu slepenou dvojici. Formálně,

$$xRy \wedge yRz \Rightarrow xRz \quad \forall x, y, z \in A.$$

Relace, která je *reflexivní*, *symetrická* a *transitivní* se nazývá **ekvivalence**.

Vlastnosti reflexivity, symetrie a transitivity nejsou principiálně v žádném vztahu. Existují relace, které jsou jen reflexivní, ale nejsou ani symetrické ani transitivní apod. Jeden příklad za všechny.

Příklad. Položme $A := \{1, 2, 3, 4\}$. Relace

- $\{(1,1),(2,2),(3,3),(4,4),(1,2),(2,3)\}$ je reflexivní, ale nikoli symetrická nebo transitivní;
- $\{(1,1),(2,2),(1,2),(2,1),(2,3),(3,2)\}$ je symetrická, ale není reflexivní ani transitivní;
- $\{(1,2),(2,3),(1,3),(3,4),(1,4),(2,4)\}$ je transitivní, ale není reflexivní ani symetrická.

Ekvivalence je velmi přirozený způsob, jak ztotožnit prvky, které bychom, často z technických důvodů, nechtěli považovat za různé. Vrátím-li se k příkladu zlomků, asi bychom nechtěli vidět třeba 1/5 a 2/10 jako dva různé zlomky. Zlomek 1/5 v tomto smyslu je vlastně množina všech zlomků, které představují stejnou hodnotu. Tuto intuici zobecňuje pojem *třídy ekvivalence*.

Definice 2.4.2 (Třída ekvivalence)**.** Mějme ekvivalenci $R \subseteq A^2$ a prvek $x \in A$. **Třídou ekvivalence** prvku x **vzhledem k R** myslíme množinu

$$[x]_R := \{y \in A \mid xRy\},$$

čili množinu všech prvků, které jsou s ním v relaci R. Dolní index R v zápisu $[x]_R$ budeme často vynechávat a psát jen $[x]$. Uvědomme si, že nezáleží na tom, jestli napíšu xRy nebo yRx v definici výše, protože R je symetrická.

Příklad (Racionální čísla)**.** Symbolem $\mathbb{N}$ značím množinu přirozených čísel $\{1, 2, 3, \ldots\}$ a symbolem $\mathbb{Z}$ množinu celých čísel, tj. množinu přirozených čísel, čísel k nim opačných a 0.

Racionální čísla se dají definovat jako všechny možné podíly celého čísla přirozeným. Když si zlomek a/b, kde $a \in \mathbb{Z}$ a $b \in \mathbb{N}$ představím jako uspořádanou dvojici (a, b), tj. (čitatel, jmenovatel), pak množina

$$A := \{(a, b) \mid a \in \mathbb{Z}, b \in \mathbb{N}\}$$

je množina všech zlomků.

Ujasníme si, kdy dva zlomky považujeme za stejné. Snadno úpravou člověk dostane, že

$$\frac{a}{b} = \frac{c}{d} \Leftrightarrow ad = bc,$$

což nám dává návod, jak definovat ekvivalenci na množině všech zlomků, A. Relaci $R \subseteq A^2$ definujeme tím způsobem, že $(a, b)R(c, d)$ právě tehdy, když $ad = bc$. Správně bychom měli dokázat, že to je opravdu ekvivalence, ale tím se nehodláme zdržovat.

Množina racionálních čísel, na kterou jste zvyklí, se pak nejelegantněji definuje jako množina tříd ekvivalence prvků z A vzhledem k R. Konkrétně,

$$\mathbb{Q} := \{[(a, b)]_R \mid a \in \mathbb{Z}, b \in \mathbb{N}\}.$$

Třídy ekvivalence jistým způsobem „parcelují“ množinu A na disjunktní (mající prázdný průnik) množiny. To je obsahem následujícího tvrzení, jehož důkaz je cvičení.

Tvrzení 2.4.1 (Vlastnosti tříd ekvivalence)**.** Nechť A je libovolná množina a R je ekvivalence na A. Pak

(1) $[x] \neq \emptyset$ pro všechna $x \in A$,

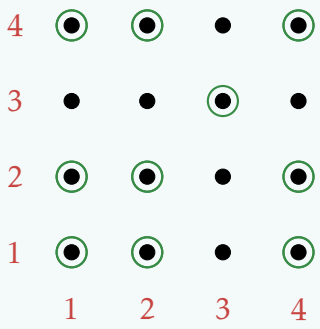
(2) Buď $[x] = [y]$, nebo $[x] \cap [y] = \emptyset$ pro všechna $x, y \in A$.

Důkaz. Cvičení. □

Příklad. Řekněme, že A je naše oblíbená množina $\{1, 2, 3, 4\}$. Snadno ověříme, že

$$R := \{(1,1), (1,2), (1,4), (2,1), (2,2), (2,4), (3,3), (4,1), (4,2), (4,4)\}$$

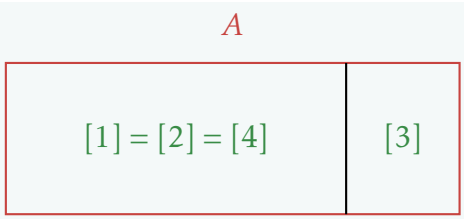
je ekvivalence na A. Její mříž vidíte na obrázku 8.



Obrázek 8: Mříž ekvivalence R na množině A.

Obecně, mříž každé ekvivalence má zaplněnou diagonálu z levého dolního rohu do pravého horního (kvůli reflexivitě) a je symetrická podle této diagonály (kvůli symetrii). Jak na první pohled poznat transitivitu nevím.

Všimněme si, že $1R2$ a $1R4$, takže $2 \in [1]$ a $4 \in [1]$. Podle tvrzení nahoře je $[1] = [2] = [4]$, protože tyto třídy ekvivalence nejsou disjunktní. Naopak, třída $[3]$ **je** disjunktní s každou z nich. Můžeme proto rozdělit množinu A na třídy ekvivalence třeba jako $A = [1] \cup [3]$. Náhled na obrázku 9.



Obrázek 9: Množina A rozdělená na třídy ekvivalence R.

Pár cvičení nakonec.

Cvičení 2.4.1. Dokažte Tvrzení 2.4.1.

Cvičení 2.4.2 (Skládání relací vs. transitivita)**.** Dokažte, že relace (ne nutně ekvivalence!) R je transitivní, právě tehdy když $R \circ R \subseteq R$.

Pozor! Píšeme „právě tehdy, když“, tedy se jedná o (logickou) ekvivalenci. Je třeba dokázat, že když $R \circ R \subseteq R$, pak R je transitivní, a že když je R transitivní, pak $R \circ R \subseteq R$.

2.5 Zobrazení

Druhým ze tří zvláště užitečných typů relace je tzv. *zobrazení*, které spíš znáte pod pojmem *funkce*. Narozdíl od ekvivalence, zobrazení budeme uvažovat jak na množině, tak mezi množinami.

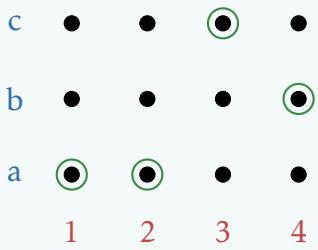
Definující vlastností funkce/zobrazení je fakt, že každý prvek nezobrazí buď na nic (pokud v něm „není definováno“) nebo na jeden jiný prvek. V jazyce relací to znamená, že každý prvek z množiny „nalevo“ je v relaci s maximálně jedním prvkem „napravo“.

Definice 2.5.1 (Zobrazení)**.** Relaci R mezi množinami A a B nazveme **zobrazením**, pokud pro každé $x \in A$ existuje **nejvýše jedno** $y \in B$ takové, že xRy.

Příklad. Mezi množinami $A := \{1,2,3,4\}$ a $B := \{a,b,c\}$ uvažme zobrazení

$$R := \{(1,a),(2,a),(3,c),(4,b)\} \subseteq A \times B.$$

Jeho mříž vypadá následovně.



Obrázek 10: Mříž zobrazení $R \subseteq A \times B$.

Fakt, že relace je zobrazení poznáte z její mříže velmi snadno tak, že (za předpokladu, že prvky levé množiny píšete vždy dole) v každém sloupci je **maximálně** jeden zelený kroužek.

Jelikož lidé přemýšleli o zobrazeních dříve než o relacích, je jejich zápis a názvosloví dost odlišné (a dost zmatené). Budeme je v dalších textu pravidelně užívat, takže vás s ním chca nechca musíme seznámit.

Pro zápis zobrazení se obvykle používají malá písmena latinské abecedy počínaje f (pro **f**unction) nebo malá písmena řecké abecedy počínaje φ (čteno „fí“, opět pro **f**unction). Fakt, že relace $f \subseteq A \times B$ je zobrazení mezi A a B (též říkáme „z A do B“), zapisujeme obvykle jako

$$f : A \to B \quad \text{nebo} \quad A \xrightarrow{f} B.$$

Několik dalších názvů:

- Fakt, že $x f y$ pro $x \in A$ a $y \in B$, zapisujeme jako $f(x) = y$ nebo jako $f : x \mapsto y$. Prvku y říkáme **obraz** prvku x **při zobrazení** f. **Obrazem zobrazení** f pak myslíme množinu všech obrazů prvků z A a značíme ji $\operatorname{im} f$ (z angl. **im**age). Konkrétně,

$$\operatorname{im} f := \{f(x) \mid x \in A\}.$$

- Pro dané $y \in B$ značíme množinu všech $x \in A$ takových, že $f(x) = y$,

jako $f^{-1}(y)$ a říkáme jí **vzor** prvku y **při zobrazení** f. Čili, $x \in f^{-1}(y)$ vyjadřuje fakt, že $f(x) = y$.

- Pokud $f : A \to B$, množině A říkáme **doména zobrazení** f a množině B **kodoména zobrazení** f.

Výstraha. Vzor prvku $y \in B$ při zobrazení f je **množina**. Definice zobrazení mi říká jenom, že jedno $x \in A$ se zobrazí na jedno $y \in B$. To ale nebrání tomu, aby se víc různých prvků z A zobrazilo na **ten samý** prvek z B. Naopak, množina $f^{-1}(y)$ může být i prázdná, pokud se na y nezobrazuje žádný prvek z A.

Příklad (Kvadratická funkce). Kvadratická funkce daná předpisem

$$f(x) := x^2 + 4x + 5$$

je zobrazení $\mathbb{R} \to \mathbb{R}$, čili jeho **doménou** i **kodoménou** jsou reálná čísla. **Obrazem** prvku 3 je $f(3) = 26$, ale **vzorem** prvku 26 je množina $\{-7, 3\}$. Dále třeba vzorem prvku 0 je prázdná množina, což je totéž, co říci, že rovnice

$$x^2 + 4x + 5 = 0$$

nemá v $\mathbb{R}$ řešení. Tradiční zápis f jako relace by vypadal

$$f = \{(x, x^2 + 4x + 5) \mid x \in \mathbb{R}\} \subseteq \mathbb{R} \times \mathbb{R}.$$

Bohužel následuje ještě poslední kus názvosloví, protože pro určité „zajímavé“ typy zobrazení máme zvláštní názvy.

Definice 2.5.2. Zobrazení $f : A \to B$ nazveme

- **prosté** (nebo **injektivní**), pokud se každé dva *různé* prvky v A zobrazují na dva *různé* prvky v B. Formálně, zobrazení f je prosté, když
$$f(x) = f(x') \Rightarrow x = x' \quad \forall x, x' \in A.$$
Ještě jinak řečeno, zobrazení je prosté, když vzorem každého prvku je buď prázdná nebo jednoprvková množina. Fakt, že f

je prosté, často zapisujeme jako $f : A \hookrightarrow B$.

- **na** (nebo **surjektivní**), když má každý prvek z B nějaký vzor v A. Formálně, zobrazení je na, když

$$\forall y \in B \, \exists x \in A : f(x) = y.$$

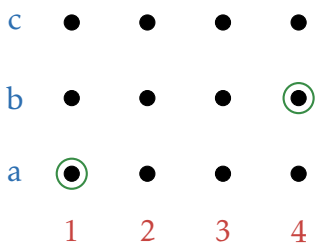
  Ještě jinak řečeno, zobrazení je na, když je vzor každého prvku neprázdná množina. Fakt, že f je na, často symbolicky zapisujeme jako $f : A \twoheadrightarrow B$.

- **vzájemně jednoznačné** (nebo **bijektivní**), když je *prosté* a *na*, čili vzorem každého prvku je přesně jednoprvková množina. Fakt, že f je bijekce, často zapisujeme jako $f : A \leftrightarrow B$ nebo $f : A \cong B$.

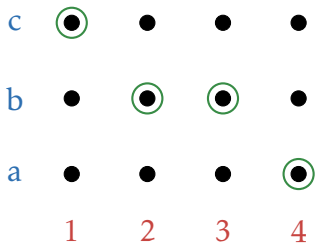
Příklad.

- Zobrazení $f : \mathbb{R} \leftrightarrow \mathbb{R}, x \mapsto 2x + 3$ je **bijektivní**. Obecně, každá lineární funkce je bijektivní zobrazení. Důkaz je ponechán jako cvičení.
- Zobrazení $f : \mathbb{R} \hookrightarrow \mathbb{R}, x \mapsto 3/x$ je **prosté**, ale není na. To proto, že $f^{-1}(0) = \emptyset$.
- Zobrazení $f : \mathbb{R} \twoheadrightarrow \mathbb{R}, x \mapsto (x-2)(x-3)(x+1)$ je **na**, ale není prosté. Třeba $f^{-1}(0) = \{-1, 2, 3\}$.
- Zobrazení $f : \mathbb{R} \to \mathbb{R}, x \mapsto 1 + 2/(x^2 - 1)$ není ani prosté, ani na. Například $f^{-1}(5/3) = \{-2, 2\}$ a $f^{-1}(1) = \emptyset$.

Prostá, surjektivní i bijektivní zobrazení mezi konečnými množinami z jejich mříží poznáte velmi snadno. Prostá zobrazení mají v řádcích maximálně jeden prvek; surjektivní zobrazení mají v každém řádku aspoň jeden prvek; ta bijektivní mají v každém řádku přesně jeden prvek. Pár obrázků.



Obrázek 11: Mříž **prostého** zobrazení $f := \{(1,a),(4,b)\}$.



Obrázek 12: Mříž **surjektivního** zobrazení $f := \{(1,c),(2,b),(3,b),(4,a)\}$.

Bijekce mezi množinami, které mají různý počet prvků existovat nemůže. Důkaz si zkusíte za cvičení. Částečně ho ale dává následující slibovaná definice velikosti množiny pomocí bijektivních zobrazení.

Definice 2.5.3 (Velikost množiny pořádně)**.** Pro přirozené číslo $n \in \mathbb{N}$ označíme symbolem $[n]$ množinu všech přirozených čísel od 1 až do n včetně. Čili,

$$[n] := \{1, 2, \ldots, n\}.$$

Množinu A nazveme **konečnou**, pokud existuje přirozené číslo $n \in \mathbb{N}$ a bijekce $f : [n] \cong A$. V takovém případě číslu n říkáme **velikost** množiny A a značíme $\#A := n$.

Bijekci $f : [n] \cong A$ z definice nahoře můžeme vnímat jako „očíslování“ prvků množiny A čísly od 1 do n. Takových očíslování je samozřejmě mnoho. Kolik?

Příklad. Množina $B := \{a, b, c\}$ má tři prvky. Jedna z možných bijekcí $f : [3] \cong B$ je

$$f := \{(1,c),(2,a),(3,b)\}.$$

Posledním důležitým konceptem je pojem *inverzního zobrazení*. Intuitivně, a vlastně i formálně, inverzní zobrazení je zobrazení, které jde opačným směrem a obrazy posílá zpátky na vzory. Toto samozřejmě vyžaduje například, aby vzor byl vždy nejvýše jeden. Detaily si rozmyslíte jako cvičení.

Definice 2.5.4 (Inverzní zobrazení)**.** Nechť $f : A \to B$ je zobrazení. **Inverzním zobrazením** k f, značeným dost nevhodně f^{-1}, nazveme zobrazení $B \to A$ splňující

$$f^{-1}(f(x)) = x \wedge f(f^{-1}(y)) = y \quad \forall x \in A, y \in \operatorname{im} f.$$

Pozor! Inverzní zobrazení *nemusí existovat*.

Výstraha. Pokud k $f : A \to B$ existuje inverzní zobrazení, značí $f^{-1}(y)$ jak množinu vzorů prvku $y \in B$, tak obraz prvku y při inverzním zobrazení.

Toto však je problém pouze formální. Pokud totiž existuje inverzní zobrazení, pak má množina $f^{-1}(y)$ buď jeden prvek, nebo žádný. V prvním případě tedy akorát ztotožňuji jednoprvkovou množinu s jejím jediným prvkem. To je totéž, co považovat třeba množinu $\{2\}$ a číslo 2 za to samé. Vskutku, problém pouze formální, bez praktických důsledků.

Sekci završíme ku radosti všech párem cvičení.

Cvičení 2.5.1. Vyřešte následující úlohy rozprostřené po sekci. Konkrétně,

- dokažte, že mezi dvěma konečnými množinami různé velikosti neexistuje žádná bijekce.
- pro množinu A velikosti n určete počet různých bijektivních zobrazení $f : [n] \cong A$.
- určete, jakou podmínku splňují zobrazení $f : A \to B$, ke kterým existuje zobrazení inverzní.

Cvičení 2.5.2. Dokažte, že každá lineární funkce $f : \mathbb{R} \to \mathbb{R}$, tedy funkce daná předpisem

$$f(x) = ax + b \quad \text{pro } a, b \in \mathbb{R}, a \neq 0$$

je bijektivní zobrazení.

Cvičení 2.5.3. Nechť A je konečná množina. Zformulujte důkaz, že zobrazení $f : A \to A$, které je definované pro každé $x \in A$, je **prosté, právě tehdy když je na**.

Tento fakt se často též používá v teorii množin jako definice konečné množiny. Je hezčí než naše v tom, že nespoléhá na množinu přirozených čísel. Tedy, množinu A nazvu *konečnou*, když každé zobrazení $f : A \to A$ definované všude je prosté, právě tehdy když je na.

Cvičení 2.5.4. Najděte příklad zobrazení $f : \mathbb{N} \to \mathbb{N}$ definovaného na celém $\mathbb{N}$, které je

(1) prosté, ale není na.

(2) na, ale není prosté.

2.6 Uspořádání

Uspořádání je poslední v jistém smyslu speciální relací, na kterou se podíváme. Podobně jako ekvivalence, uspořádání mezi dvěma množinami nedává úplně smysl, takže se po celou sekci budeme soustředit na relaci na množině.

Určitě nejznámějším typem uspořádání je relace „menší nebo rovno“ (nebo „menší“, „větší nebo rovno“ atd., to je jedno), kterou jistě všichni známe. Tohle je ten příklad uspořádání, který doporučujeme mít na paměti, kdykoli se zdají obecné definice těžko stravitelnými.

Existuje ale samozřejmě spousta jiných druhů uspořádání s rozlišnými spektry užitku. Uveďme například uspořádání dělitelností, zcela zásadní v elementární teorii čísel, nebo lexikografické uspořádání, kterým se řadí

slova ve slovnících a encyklopediích a dá se použít i pro řazení polynomů (například v důkazu slavného Gaussova algoritmu).

Ještě před definicí uspořádání se ale musíme zmínit o pro ni klíčové vlastnosti relací.

Definice 2.6.1 (Antisymetrická relace)**.** Relace R na množině A se nazývá

- **antisymetrická**, pokud $(x,y) \in R \Rightarrow (y,x) \notin R$ pro všechny prvky $x, y \in A$.
- **slabě antisymetrická**, pokud $xRy \wedge yRx \Rightarrow x = y$ pro všechna $x, y \in A$.

Jak název napovídá, vlastnost antisymetrie je opravdu jakýmsi protikladem symetrie.

Přeložena do jazyka aspoň některých lidí, relace je (silně) antisymetrická tehdy, když to, že je prvek x v relaci s prvkem y, zakazuje, aby byl zároveň y v relaci s x. Může se však samozřejmě stát, že x není v relaci s y ani y není v relaci s x. Všimněte si, že vlastnost antisymetrie mimo jiné *nedovoluje, aby daná relace byla reflexivní*.

Příklad. Všeobecně oblíbených příkladem (silně) antisymetrické relace je relace $<$, třeba na množině $\mathbb{R}$. V moment, kdy pro dvě reálná čísla $x, y \in \mathbb{R}$ platí, že $x < y$, pak automaticky **nemůže platit** $y < x$. Zároveň, žádné reálné číslo není nikdy ostře menší než ono samo, tedy $<$ je vskutku antisymetrická a není reflexivní.

Ačkoliv to možná z definice není zřejmé, vlastnost *slabé* antisymetrie je opravdu jen oslabená vlastnost (silné) antisymetrie v tom smyslu, že slabě antisymetrická relace může být reflexivní. Čili, mám-li slabě antisymetrickou relaci R, pak xRy nutně **nezakazuje**, aby yRx, ale jediný prvek y, pro který tato situace může nastat, je x samotné.

Příklad. Asi tušíte, co přijde. Když vám řekneme, abyste zeslabili vztah $<$, prvním takovým přirozeným nápadem je vztah $\leq$, což je skutečně

slabě antisymetrická relace. Vskutku, když $x \leq y$, pak se může stát, že i $y \leq x$, ale to nutně znamená, že $x = y$.

Definice 2.6.2 (Uspořádání)**.** Relace R na množině A se nazývá

- (neostré) **uspořádání**, pokud je *reflexivní*, *slabě antisymetrická* a *transitivní*.
- **ostré uspořádání**, pokud je *antisymetrická* a *transitivní*.

Pokud je R (ostré) uspořádání na A, nazýváme dvojici (A, R) (ostře) **uspořádanou množinou**.

Příklad.

(1) Relace $<$ na $\mathbb{R}$ je **ostré uspořádání**, protože
- (antisymetrie) $x < y \Rightarrow y \not< x$ a
- (transitivita) $x < y \wedge y < z \Rightarrow x < z$

pro všechna čísla $x, y, z \in \mathbb{R}$.

(2) Relace $\leq$ na $\mathbb{R}$ je (neostré) **uspořádání**. Vskutku, platí
- (reflexivita) $x \leq x$,
- (slabá antisymetrie) $x \leq y \wedge y \leq x \Rightarrow x = y$ a
- (transitivita) $x \leq y \wedge y \leq z \Rightarrow x \leq z$

pro všechna $x, y, z \in \mathbb{R}$.

Ještě poslední sousto nomenklatury.

Definice 2.6.3 (Lineární uspořádání)**.** (Ostré) uspořádání R na množině A nazveme **lineárním**, pokud pro každé dva prvky $x, y \in A$ platí, že xRy nebo yRx. Čili, každé dva prvky A spolu *lze porovnat* prostřednictvím R. (Ostré) uspořádání, které *není lineární*, často označujeme jako **částečné**.

Příklad. Jak $<$, tak $\leq$, jsou lineární uspořádání.

Protože základní idea za pojmem „uspořádání“ je, no, uspořádání prvků na množině, ujaly se pro jejich kreslení, spíše než mříže nebo šipky, tzv. *Hasseho diagramy*. Hasseho diagram vypadá tak, že prvky množiny jsou značeny tečkami a mezi porovnatelnými prvky (tj. prvky, které jsou v relaci) se dá dostat po úsečkách (někdy přes více prvků). Navíc, prvky se kreslí zezdola nahoru vzhledem k jejich pozici v rámci daného uspořádání.

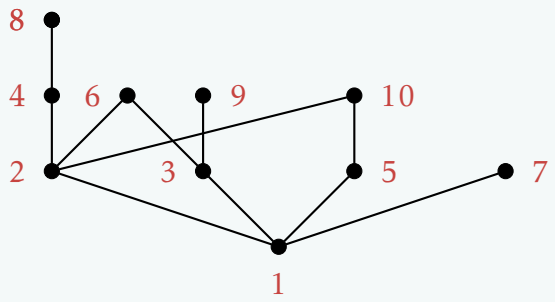
Příklad (Uspořádání velikostí)**.** Již jsme zpozorovali, že $\leq$ je uspořádání. Jeho Hasseho diagram na množině $A := \{1, 2, 3, 4, 5\}$ vidíte na obrázku 13.

Obrázek 13: Hasseho diagram uspořádáné množiny $(A, \leq)$.

Ve skutečnosti, Hasseho diagram **každého** lineárního uspořádání vypadá takto; liší se pouze počet prvků. Detaily si rozmyslíte za cvičení.

Definice 2.6.4 (Dělitelnost)**.** Mějme čísla $m, n \in \mathbb{N}$. Říkáme, že m **dělí** n, když existuje přirozené číslo $k \in \mathbb{N}$ takové, že $n = km$. Tento fakt zapisujeme jako $m \mid n$.

Příklad (Uspořádání dělitelností)**.** Relace $\mid$ z definice dělitelnosti je ve skutečnosti uspořádání (důkaz jako cvičení), které **ale není lineární**. Jeho Hasseho diagram na množině $A := [10]$ je výrazně košatější.



Obrázek 14: Hasseho diagram uspořádané množiny $(A, |)$.

Lexikografické uspořádání je v principu uspořádání na slovech, ale může být úspěšně použito třeba i pro uspořádání polynomů více proměnných. Funguje následovně: slovem délky n nazveme posloupnost $a_1 a_2 \dots a_n$, kde a_i je libovolné písmeno mezi „a“ a „z“. Slovo $a_1 a_2 \dots a_n$ je lexikograficky níž než slovo $b_1 b_2 \dots b_m$, pokud existuje $i \leq \min(n, m)$ takové, že $a_1 = b_1 \wedge a_2 = b_2 \wedge \dots \wedge a_{i-1} = b_{i-1}$ a $b_i > a_i$.

Řečeno lidsky, o slově $a_1 a_2 \dots a_n$ řeknu, že je níž než $b_1 b_2 \dots b_m$, když nějaké jeho písmeno a_i je dřív v abecedě než písmeno b_i na stejném místě ve slově $b_1 b_2 \dots b_m$. Pokud je jedno slovo plně součástí druhého, lexikograficky níž je to kratší. Lexikografické uspořádání se obvykle značí rovněž $\leq$, ale pro přehlednost ho budeme značit třeba $\leq_{\text{lex}}$.

Příklad (Lexikografické uspořádání)**.** Jak si můžete ověřit (ale cvičení to nutně není), lexikografické uspořádání je lineární, takže jeho Hasseho diagram není dvakrát zajímavý. Pro úplnost zde ale přesto ukážeme diagram množiny

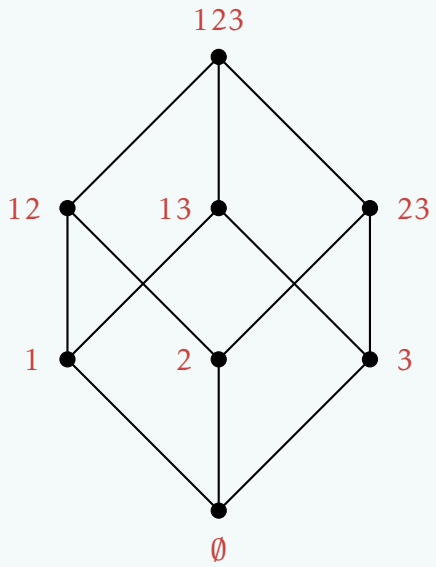
$$A := \{a_1 a_2 \mid a_i \in \{a, b, c\}\},$$

tedy množiny všech dvojpísmenných kombinací písmen „a“ až „c“.

Obrázek 15: Hasseho diagram uspořádané množiny $(A, \leq_{\text{lex}})$.

Velmi pěkné obrázky uspořádání vznikají i na množině všech množin A, tedy na 2^A, kde uspořádání je inkluzí $\subseteq$. Tedy, nejníž je prázdná množina, která leží uvnitř každé množiny, a nejvýš je množina A, ve které je obsažena každá její podmnožina. Jeden malý příklad tu nakreslíme, určitě se vám bude líbit.

Příklad. Mějme množinu $A := \{1, 2, 3\}$. Množinu 2^A uspořádáme inkluzí, čili dvě podmnožiny A jsou v relaci inkluze, když je jedna obsažena v druhé. Jeden příklad za všechny je třeba $\{1\} \subseteq \{1, 3\}$. Hasseho diagram takového uspořádání vidíte níže. V rámci úspory píšeme třeba 12 místo množiny $\{1, 2\}$.



Obrázek 16: Hasseho diagram uspořádané množiny $(2^A, \subseteq)$.

Jako obvykle následuje několik cvičení na závěr sekce.

Cvičení 2.6.1. Udělejte cvičení rozmístěná po sekci. Konkrétně,

(1) dokažte, že Hasseho diagram každého lineárního uspořádání má stejný tvar jako diagram na obrázku 13.

(2) dokažte, že relace dělitelnosti $|$ je uspořádání na každé podmnožině přirozených čísel.

Cvičení 2.6.2. Explicitně popište všechny relace (na libovolné množině), které jsou zároveň ekvivalencí a (částečným) uspořádáním.

Cvičení 2.6.3. Řekněme, že R a S jsou uspořádání na množině A. Které z následujících relací jsou také uspořádáními na A?

- $R \cap S$
- $R \cup S$
- $R \setminus S$
- $R \circ S$

2.7 Matematická indukce

Indukce je základní důkazovou technikou v diskrétní matematice. Je to jeden možný, ale zcela jistě nejoblíbenější, způsob, jak dokazovat libovolná tvrzení o přirozených číslech, která jsou vlastně právě tím číselným oborem, který studuje diskrétní matematika.

Princip indukce spočívá v tom, že přirozená čísla jsou definována v zásadě velmi jednoduše. Libovolná množina, která má nějaký „základní prvek“ (třeba jedničku) a spolu s každým prvkem má i jeho bezprostředního následníka (třeba to číslo o jedna větší), je automaticky „ta samá množina“ jako přirozená čísla.

Pokud byste měli chuť se podívat na formální definici přirozených čísel a dalších souvisejících věcí, doporučujeme vyhledat klíčová slova *Peanova aritmetika*, která je vlastně (možná kecám, ale myslím, že nejmenším možným) systémem axiomů (kategoricky platných výroků), jenž buduje ryze logický základ pro aritmetiku.

My si ale vystačíme s následujícím zjednodušením.

Tvrzení 2.7.1 (Definice přirozených čísel)**.** Nechť A je množina, která splňuje, že

- $1 \in A$,
- je-li $n \in A$, pak rovněž $n+1 \in A$.

Potom $A = \mathbb{N}$.

Důkaz. Nedokazuje se, je to axiom (konkrétně pátý) Peanovy aritmetiky. □

Žádáme, abyste si dali chvíli a zamysleli nad významem tvrzení. Zevrubně řečeno říká, že, pokud umím dokázat, že

- tvrzení platí pro první přirozené číslo a
- za předpokladu, že tvrzení platí pro n, platí pro $n+1$,

pak dané tvrzení platí pro všechna přirozená čísla. Tyhle dva důkazy totiž

dohromady dávají následující (nekonečný) řetězec důkazů:

(1) (Nějaké) tvrzení platí pro $n = 1$.

(2) Jestliže tvrzení platí pro $n = 1$, pak platí pro $n = 2$.

(3) Jestliže tvrzení platí pro $n = 2$, pak platí pro $n = 3$.

$$\vdots$$

Princip indukce asi není přehnaně složitý, ale získat dostatek zkušenosti, aby jej člověk uměl neomylně aplikovat, je výrazně obtížnější. Pár příkladů snad s tímto krokem pomůže. Budeme je záměrně formulovat jako lemmata či tvrzení, jelikož indukce je v prvé řadě důkazová technika. Doporučujeme, abyste důkazy četli se zvýšenou pozorností.

Lemma 2.7.1. Pro každé $n \in \mathbb{N}$ platí

$$\sum_{i=0}^{n} 2^i = 2^{n+1} - 1.$$

Důkaz. Dokazujeme indukcí. Protože suma začíná od 0, je prvním prvkem, pro který musí tvrzení platit, v tomto případě právě $n = 0$. Dosazením zjistíme, že

$$\sum_{i=0}^{0} 2^i = 2^0 = 1 = 2^{0+1} - 1$$

tedy tvrzení platí pro $n = 0$. Předpokládáme, že tvrzení platí pro všechna přirozená čísla až do nějakého $n \in \mathbb{N}$ a z tohoto předpokladu odvodíme, že platí i pro $n + 1$. Počítáme

$$\sum_{i=0}^{n+1} 2^i = \sum_{i=0}^{n} 2^i + 2^{n+1}.$$

Ovšem, z předpokladu dostaneme

$$\sum_{i=0}^{n} 2^i = 2^{n+1} - 1,$$

což dohromady s předchozím výpočtem dává

$$\sum_{i=0}^{n+1} 2^i = \sum_{i=0}^{n} 2^i + 2^{n+1} = 2^{n+1} - 1 + 2^{n+1} = 2 \cdot 2^{n+1} - 1 = 2^{n+2} - 1,$$

jak jsme chtěli ukázat. Důkaz je podle principu indukce ukončen. □

Lemma 2.7.2. Pro všechna $n \in \mathbb{N}$ platí, že

$$3 \mid n \Rightarrow 3 \mid n^2,$$

tedy, pokud 3 dělí n, pak 3 dělí n^2.

Tady by se jistě leckdo rád odvolal třeba na prvočíselné rozklady. Je ale dobré si uvědomit, že fakt, že každé přirozené číslo má jednoznačný rozklad na prvočísla, není samozřejmý. Ve skutečnosti zabere určitou práci toto dokázat. Či vy jste viděli nějaký přímočarý důkaz, že jdou čísla rozkládat na prvočísla? Opravdu lze *každé* číslo rozložit na prvočísla a opravdu to lze *pouze jediným způsobem*?

Důkaz (lemmatu 2.7.2)**.** Dokazujeme indukcí.

První přirozené číslo, pro které má smysl tvrzení dokázat, je $n = 3$. Pak vskutku $3 \mid n = 3$ a $3 \mid n^2 = 9$.

Předpokládejme, že výrok $3 \mid n \Rightarrow 3 \mid n^2$ platí pro nějaké $n \in \mathbb{N}$. Nejbližší další přirozené číslo po n, které je dělitelné 3, je $n+3$. Tedy, víme, že když $3 \mid n$, pak $3 \mid n+3$ a také $3 \mid n^2$. Z těchto dvou faktů odvodíme, že $3 \mid (n+3)^2$.

Máme $(n+3)^2 = n^2 + 6n + 9$. Protože $3 \mid 6$ a $3 \mid 9$, také $3 \mid 6n + 9$. Předpokládáme, že $3 \mid n^2$, dohromady tudíž $3 \mid n^2 + 6n + 9 = (n+3)^2$, jak jsme chtěli. □

Tři cvičení nakonec.

Cvičení 2.7.1. Dokažte indukcí, že

$$\sum_{i=1}^{n} i2^i = (n-1)2^{n+1} + 2.$$

Cvičení 2.7.2 (Fibonacciho čísla a zlatý řez)**.** Tak zvaná *Fibonacciho* posloupnost je definována tak, že další člen dostanu jako součet dvou předchozích. Formálně, $F_0 = 0, F_1 = 1$ a $F_n = F_{n-1} + F_{n-2}$, kde $n \in \mathbb{N}$. Dokažte indukcí, že

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

pro všechna $n \geq 0$.

Číslu $(1+\sqrt{5})/2$ se někdy říká hodnota „zlatého řezu“ (protože je to v jistém smyslu *ideální* poměr mezi délkami dvěma bezprostředních úseček – internet poví víc). Jestli si někdy ukážeme limity, pak dokážeme tento výsledek zdokonalit v tom smyslu, že platí

$$\frac{F_n}{F_{n-1}} \xrightarrow{n\to\infty} \frac{1+\sqrt{5}}{2}.$$

Cvičení 2.7.3. Nakresleme n přímek v rovině, a to tak, že

- žádné 2 nejsou rovnoběžné a
- žádné 3 se neprotínají v jednom bodě.

Dokažte indukcí, že takhle nakreslené přímky rozdělují rovinu na $n(n+1)/2+1$ částí.

3 | Počítání

V této kapitole se naučíme počítat; a ne, doteď jste to neuměli. Snad všechny potěšíme, když zvěstíme, že tahle je kapitola je již skutečným úvodem do problematiky *diskrétní matematiky*. Otázky typů „Kolik je čeho?“,

„Kolika způsoby mohu něco udělat?“ skutečně nikam jinam patřit ani nemohou, protože analytici mají všeho nespočetně mnoho a lineárním algebraikům zas může vadit, že nad přirozenými čísly se žádná rozumná geometrie úplně dělat nedá.

Začneme snad jednoduchým počítáním daných typů zobrazení a podmnožin, poté se posuneme k počtu možností, jak za sebe skládat prvky. V neposlední řadě se budeme věnovat tzv. *principu inkluze a exkluze*, jenž umožňuje elegantně odpovídat třeba na otázky „Kolik je čísel menších než 100, které nejsou dělitelné 2 ani 3?“. Vše završíme notoricky známým *problémem šatnářky*, o kterém raději nic neprozradíme, bychom si udrželi alespoň přirozené číslo čtenářů.

Ty nejzákladnější způsoby, jak určovat počty věcí nebo způsobů, jak něco dělat, jsou obecně dva:

- **přímý** aneb „Vím, co dělám, a umím to spočítat pro libovolné přirozené číslo.“ a
- **indukcí** aneb „Vůbec to nechápu, ale zkusím si to pro pár malejch čísel a pak to nějak ukoulím i pro ty velký.“

Ačkoli by to kolegové z katedry kombinatoriky neradi slyšeli, druhý způsob je zcela jistě ten bohatě nejoblíbenější.

V trochu serióznějším duchu radíme vždy zkusit nejprve přímý důkaz, u kterého je zřejmé, jak jste na vzorec přišli a proč je správný. Důkaz indukcí je totiž z principu *nekonstruktivní*, tj. není z něj vůbec jasné, odkud se vzorec bere. Stačí totiž jen ukázat, že funguje pro jakési první číslo a že když funguje pro nějaké číslo, pak funguje i pro to další. Takový důkaz ale neposkytuje vůbec žádný vhled do problému.

3.1 Zobrazení a podmnožiny

Chvíli se budeme bavit počítáním zobrazení a podmnožin obvykle určených nějakou hezkou podmínkou. Začít právě tady je vhodné z páru důvodů. Zaprvé, není potřeba vymýšlet žádnou novou teorii a zadruhé – snad trochu překvapivě – umět počítat zobrazení a podmnožiny se hodí do spousty dalších matematických disciplín. Zmiňme Čínskou větu o zbytcích, v podstatě jeden ze základních stavebních kamenů teorie čísel, jejíž

důkaz je založen právě na tom, že umíme počítat zobrazení mezi množinami. Dále je tu třeba Burnsideova věta z abstraktní algebry, na jejíž pravdivost spoléhá třeba otáčení obsahu obrazovky na mobilech a jejíž důkaz vyžaduje porovnávání velikostí systémů podmnožin. Konečně, patří sem i latinské čtverce – struktury, jejichž princip stojí za vznikem Sudoku.

Pojďme začít tím nejjednodušším možným tvrzením, tedy o počtu všech zobrazení mezi množinami. Ukážeme si dva důkazy: jeden přímý a jeden indukcí.

Výstraha. Pro stručnost budu v celé kapitole slovem zobrazení myslet **zobrazení definované všude**. Diskrétní matematiku totiž pravdaťúplně netrápí problémy definičních oborů, takže není žádná výhoda v tom uvažovat zobrazení, která nejsou definována pro všechny prvky svých domén.

Tvrzení 3.1.1 (Počet všech zobrazení)**.** Mějme konečné množiny A a B. Počet všech zobrazení $A \to B$ je $\#B^{\#A}$.

Důkaz (tvrzení 3.1.1 přímo)**.** Rozmysleme si nejprve, kdy se dvě zobrazení $f, g : A \to B$ liší. To je přeci tehdy, když existuje nějaký prvek $a \in A$ takový, že $f(a) \neq g(a)$.

Jinak řečeno, každé zobrazení $A \to B$ popíšu tak, že určím obrazy všech prvků z A. Kdykoli mám dvě zobrazení, jejichž obraz byť i jednoho prvku z A se neshoduje, pak jsou to různá zobrazení. Pro každý prvek z A mám přesně $\#B$ prvků, na které ho mohu zobrazit, tedy mám celkem přesně $\#B^{\#A}$ možností, jak zobrazit všechny prvky z A na prvky z B. □

Důkaz (tvrzení 3.1.1 indukcí)**.** Dokážeme předchozí tvrzení užitím indukce podle velikosti množiny A.

Když je A prázdná, čili $\#A = 0$, pak mám právě jedno zobrazení $A \to B$ – to, které nezobrazuje nic na nic. Čili mám vskutku $\#B^{\#A} = \#B^0 = 1$ různých zobrazení $A \to B$.

Předpokládejme, že platí, že zobrazení z A do B je právě $\#B^{\#A}$ a přidejme do množiny A jeden prvek, třeba x. Chceme ukázat, že všech zobrazení $A \cup \{x\} \to B$ je $\#B^{\#A+1}$. Jeden způsob, jak to udělat, je podívat se kolika způsoby můžeme zobrazení $A \to B$ „dodefinovat“ v x.

No, x přeci mohu zobrazit na jakýkoliv prvek z B a každá volba obrazu mi dává jiné zobrazení. Čili, z jednoho zobrazení $A \to B$ mi vznikne právě $\#B$ různých zobrazení $A \cup \{x\} \to B$. To ale znamená, že všech zobrazení $A \cup \{x\} \to B$ je $\#B$-krát víc než zobrazení $A \to B$. Tedy jich je podle předpokladu

$$\#B^{\#A}\#B = \#B^{\#A+1}.$$ □

O něco těžší je počítat zobrazení $A \to B$ omezených vlastností. Samozřejmě bychom si mohli navymýšlet libovolné podmínky, které naše zobrazení musí splňovat; třeba, že musí na každý prvek B zobrazit právě prvočíselný počet prvků z A. Zjistit počet všech takových zobrazení by jistě byla zajímavá úloha, ale asi ne příliš užitečná. Pojďme se soustředit na více obvyklé typy zobrazení.

Tvrzení 3.1.2 (Počet prostých zobrazení)**.** Počet všech **prostých** zobrazení $A \to B$ je

$$\prod_{i=0}^{\#A-1} \#B - i,$$

Důkaz. Předvedeme přímý důkaz. Důkaz indukcí si zkusíte za cvičení.

Princip důkazu je podobný jako při počítání všech zobrazení $A \to B$. Zásadní rozdíl dlí v tom, že na každý prvek z B lze zobrazit maximálně jeden prvek z A. Opět ale platí, že dva různé výběry obrazů prvků z A nám dávají dvě různá zobrazení. Stačí tedy spočítat, kolika způsoby si můžeme zvolit, kam se prvky A zobrazí.

Nu, první prvek z A můžeme zobrazit na $\#B$ různých prvků z B. Pro ten druhý ovšem máme už jen $\#B-1$ možností, protože zobrazení musí být **prosté**, a tedy nelze druhý prvek zobrazit tam, kam ten první. Tenhle princip se opakuje. Pro třetí prvek už máme jen $\#B-2$ možných obrazů atd. Celkem, pro i-tý prvek z A máme jen $\#B - i + 1$ míst, kam ho zobrazit.

Shrnuto, pro každý výběr obrazu prvního prvku máme už jen $\#B - 1$ možných obrazů pro druhý prvek. Pro každý výběr obrazů prvních dvou prvků máme už jen $\#B - 2$ možných obrazů pro třetí prvek. Takhle pokračujeme, dokud nedojdeme až k $\#A$-tému prvku, pro který nám zbývá $\#B - \#A + 1$ nevyužitých prvků B. Sepsáno symbolicky, máme

$$\#B(\#B-1)(\#B-2)\cdots(\#B-\#A+1) = \prod_{i=0}^{\#A-1} \#B - i$$

možností, jak zvolit obrazy všech prvků z A za daných podmínek. Tedy existuje právě tolik prostých zobrazení $A \to B$. □

Na konec sekce si ještě spočítáme nějaké podmnožiny. Už víme, že počet všech podmnožin A je $2^{\#A}$. Je to Tvrzení 2.2.1. Asi nejjednodušší další úlohou je počet všech podmnožin liché a sudé velikosti. Čék by si řek', že jich je fifty-fifty a měl by recht. Ukážeme si důkaz.

Tvrzení 3.1.3 (Počet podmnožin liché velikosti)**.** Všech podmnožin liché velikosti konečné množiny A je $2^{\#A-1}$.

Důkaz. Půjdeme na to trochu jinak. Víme ze sekce o zobrazeních, že mezi konečnými množinami existuje bijekce jenom tehdy, když jsou stejně velké. Vyjměme z A nějaký fixní prvek, třeba $a \in A$. Množinu $A \setminus \{a\}$ označíme $\tilde{A}$. Protože $\tilde{A}$ má $\#A - 1$ prvků, počet jejích podmnožin je $2^{\#A-1}$. Najdeme bijekci mezi všemi podmnožinami množiny $\tilde{A}$ a lichými podmnožinami množiny A.

Definujme zobrazení $f : 2^{\tilde{A}} \to 2^A$ následujícím způsobem. Pozor! Všimněte si, že zobrazení f je definované na podmnožinách. Tedy zobrazuje množiny na množiny.

Každá lichá podmnožina A buď obsahuje a, nebo je neobsahuje. Liché podmnožiny A, které obsahují a, jsou sudými podmnožinami $\tilde{A}$ (protože jsme a odebrali), a ty, které a neobsahují, zůstávají lichými i v $\tilde{A}$. Tedy, definujme

$$f(X) := \begin{cases} X, & \text{pokud } \#X \text{ je liché,} \\ X \cup \{a\}, & \text{pokud } \#X \text{ je sudé.} \end{cases}$$

pro každou podmnožinu $X \subseteq \tilde{A}$. Tím jsme sestrojili bijekci mezi všemi podmnožinami $\tilde{A}$ a lichými podmnožinami A. Odtud plyne, že lichých podmnožin A je $2^{\#A-1} = 2^{\#A}/2$.

Pro sudé podmnožiny lze postupovat obdobně anebo si uvědomit, že všechny ostatní podmnožiny, které nejsou liché, musejí být sudé. Tedy jich je $2^{\#A} - 2^{\#A-1} = 2^{\#A-1}$. □

Předchozí důkaz ilustruje další běžný způsob, jak počítat prvky daných množin: konkrétně tak, že najdeme bijekci mezi množinou, jejíž počet prvků chceme spočítat, a množinou, jejíž počet prvků známe.

Dvě cvičení na závěr.

Cvičení 3.1.1. Dokažte Tvrzení 3.1.2 indukcí podle velikosti množiny A.

Cvičení 3.1.2. Určete počet všech uspořádaných dvojic (A, B), kde $A \subseteq B \subseteq \{1, \ldots, n\}$.

Uspořádaná dvojice znamená, že $(A, B) \neq (B, A)$, tedy záleží na pořadí, v jakém podmnožiny zapíšu.

3.2 Permutace

Permutace jsou vlastně zobrazení, která prohazují prvky množin. Jejich asi hlavním účelem je formalizovat koncept, že „nezáleží na pořadí“ nebo naopak, že všechno dělám pro všechna možná přeuspořádání prvků. Člověk by měl dobrý důvod si myslet, že nejsou dobré k ničemu jinému, než ke zkrášlení zápisu. Opak je pravdou. Permutace mají velmi překvapivé aplikace v oblastech matematiky, kde by je jeden nehledal. Zmiňme tři příklady.

- Důkaz základní věty algebry – tvrzení, že každý komplexní polynom má komplexní kořen – silně využívá tzv. rozklad na symetrické polynomy, založený na vlastnostech permutací.
- Fakt, že kořeny obecných reálných (i komplexních) polynomů nelze zapsat v radikálech (tj. odmocninách), když je stupeň polynomu větší

nebo roven 5 (tj. objevuje se v něm x^5), se opírá o tzv. „neřešitelnost“ permutačních grup (množin permutací na dané množině s binární operací skládání).

- Důkaz, že na každé Riemannově pseudovarietě dimenze 4 (kterou fyzikové používají jako model časoprostoru) existuje nekonečně mnoho neisomorfních Riemannových metrik (tj. v našem vesmíru mohu měřit vzdálenost nekonečně mnoha neekvivalentními způsoby) staví na symetrii tensorů definovaných pomocí permutací.

Takže, o co tu vlastně jde.

Definice 3.2.1 (Permutace)**.** Bijekce $\sigma : X \to X$ konečné množiny X na sebe samu se nazývá *permutace* množiny X.

Množinu všech permutací na X značíme S_X (jako grupa symetrií X).

Jelikož všichni rádi počítáme (xD), určíme si na začátek počet všech permutací na dané množině. Podle cvičení 2.5.3, které jste *všichni* dělali, zobrazení na konečné množině X je prosté právě tehdy, když je na, tedy právě tehdy, když je bijektivní. Tento fakt nám pomůže s důkazem následujícího tvrzení. Jen ještě jedna definice usnadňující zápis.

Definice 3.2.2 (Faktoriál)**.** Pro přirozené číslo $n \in \mathbb{N}$ definujeme

$$n! := \prod_{i=0}^{n-1} n - i.$$

Výraz $n!$ čteme *n faktoriál*.

Tvrzení 3.2.1 (Počet permutací na množině)**.** Ať X je konečná množina. Pak $\#S_X = (\#X)!$.

Důkaz. Podle tvrzení 3.1.2, počet prostých zobrazení $A \to B$ je

$$\prod_{i=0}^{\#A-1} \#B - i.$$

Když $A = B$, pak bijekce $A \to A$ jsou totéž, co prostá zobrazení $A \to A$. Tedy, všech bijekcí $A \to A$ (tj. všech permutací na A) je

$$\prod_{i=0}^{\#A-1} \#A - i = (\#A)!. \qquad \square$$

3.2.1 Zápis permutací

Budeme se chvíli bavit o tom, jak můžeme reprezentovat permutace. Samozřejmě, permutace jsou mimo jiné zobrazení, takže je lze kreslit, jak už jsme to dělali; tj. jako šipky mezi množinami teček.

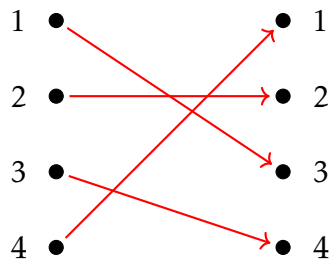
Existují ale chytřejší a přehlednější způsoby, jak je znázornit. Jeden možný způsob je zápisem do řádku. Řekněme, že $X = \{1, 2, 3, 4\}$ a $\sigma \in S_X$. Když napíšeme, že

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix},$$

myslíme tím, že σ je zobrazení, které posílá 1 na 3, 2 na 2, 3 na 4 a 4 na 1. Můžeme navíc předpokládat, že vrchní řádek je vždycky v nějakém předem dohodnutém pořadí a permutaci σ zapsat prostě jako

$$\sigma = \begin{pmatrix} 3 & 2 & 4 & 1 \end{pmatrix}.$$

V obvyklém kreslení permutací bychom σ znázornili, jak vidíte na obrázku níže.

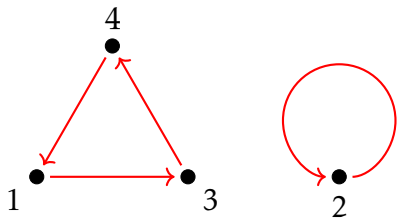


Obrázek 17: Permutace σ zakreslená šipkami.

Ačkoli je tento způsob zápisu intuitivní a podporuje představu permutace jako „proházení“ prvků na množině, mnohem více se používá tzv. zápis

v cyklech. Důvody jsou primárně formální; z cyklického zápisu se velmi snadno totiž pozná, jak „řád“ permutace, tak její rozložení na „transpozice“. Oba pojmy definujeme a vysvětlíme později.

Jelikož permutace jsou bijekce z množiny do téže množiny, můžeme vždy začít v nějakém libovolné prvku a pokračovat po šipkách, dokud se nedostaneme opět na ten samý prvek. Tento přístup formalizuje právě zápis do cyklů. Například zápis permutace $\sigma = (3\ 2\ 4\ 1)$ do cyklů by vypadal takto:



Obrázek 18: Zápis permutace σ do cyklů.

Jak si asi dovedete představit, tento zápis znamená, že permutace σ pošle 1 na 3, pak 3 na 4 a nakonec 4 na 1. Tedy, po třech „iteracích“ permutace σ se dostaneme z prvku 1 opět do prvku 1. Smyčka nad 2 samozřejmě znamená, že 2 se zobrazuje opět na 2.

Zápis na obrázku výše je evidentně dosti neúsporný, a v textu tudíž těžko použitelný. Obvykle se taková permutace zapíše jako $\sigma = (134)(2)$. Tedy, jednotlivé cykly jsou odděleny závorkami a šipky v cyklech vedou zleva doprava, případně z posledního prvku zpět na první.

Konečně, smyčky (tj. zobrazení prvku na sebe sama) se z cyklického zápisu běžně vynechávají. Svoji oblíbenou permutaci $\sigma = (134)(2)$ můžeme proto úplně nejúsporněji zapsat jako $\sigma = (134)$. Zápis permutací v cyklech budeme odteď využívat výhradně.

Výstraha. Zápis permutace pomocí cyklů **není jednoznačný**. Je to proto, že u daného cyklu nelze říct, kde „končí“ a kde „začíná“. Důležité je pouze pořadí prvků. Permutace (134), (341) a (413) jsou tudíž jedna a ta samá.

3.2.2 Skládání permutací

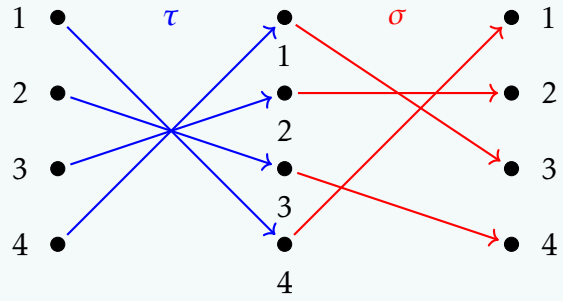
Jelikož permutace jsou speciálně zobrazení, dají se pochopitelně skládat. Navíc, protože doména i kodoména každé permutace na X je právě množina X, mohu je skládat v libovolném pořadí a libovolném množství.

Na výpočet složení dvou permutací $\sigma, \tau \in S_X$ není myslím žádný vyloženě snadný postup. Člověk se musí zkrátka v cyklickém zápisu dočíst, kam posílá první permutace daný prvek, a kam zase druhá permutace posílá obraz tohoto prvku.

Příklad. Ať $X = \{1,2,3,4\}$ a $\sigma, \tau \in S_X, \sigma = (134), \tau = (14)(23)$. Pak

$$\sigma\tau = (243),$$

protože τ pošle 1 na 4 a σ pošle 4 na 1, tedy $\sigma\tau$ pošle 1 na 1. Podobně pro ostatní prvky. V šipkách složení $\sigma\tau$ vypadá takto:



Obrázek 19: Složení permutací $\sigma\tau$ znázorněno v šipkách.

Všimněte si ale, že

$$\tau\sigma = (123).$$

Výstraha. Jak bylo vidno z předchozího příkladu, skládání permutací (jako obecně i relací) **není komutativní**. Dokonce platí, že pouze skládání permutace se sebou samou je komutativní, čili jsou-li $\sigma, \tau \in S_X$, pak

$$\sigma\tau = \tau\sigma \Rightarrow \tau = \sigma$$

za předpokladu, že $\#X \geq 3$.

Nyní si konečně povíme, co znamená „řád“ permutace a že každou permutaci lze rozložit na „transpozice“.

Když $\sigma = c_1 c_2 \cdots c_n$ je rozklad permutace $\sigma \in S_X$ na cykly $c_1, c_2, \ldots, c_n$, pak *délkou cyklu* c_i myslíme počet prvků množiny X, které se v něm vyskytují. Tedy, např. délka cyklu (1324) je 4 a délka cyklu (457) je 3.

Definice 3.2.3 (Transpozice)**.** Permutace $\sigma \in S_X$ se nazývá *transpozice*, když obsahuje právě jeden cyklus délky 2. Lidsky řečeno, transpozice jsou přesně ty permutace, které prohazují dva prvky.

Možná trochu překvapivý výsledek ohledně permutací je, že každou permutaci lze napsat jako složení transpozic. Navíc je algoritmus velmi přímočarý – stačí zkrátka každý cyklus délky k rozložit na $k-1$ transpozic tak, že každý „vnitřní“ prvek cyklu zdvojíme. Zformulujeme si tvrzení a ukážeme si algoritmus na příkladě.

Tvrzení 3.2.2 (Rozklad na transpozice)**.** Ať $\sigma \in S_X$ a $\#X \geq 2$ (jinak bychom neměli dva prvky k prohození). Pak existují transpozice $\tau_1, \ldots, \tau_n$ takové, že

$$\sigma = \tau_1 \tau_2 \cdots \tau_n.$$

Navíc, počet transpozic v rozkladu σ je určen jednoznačně.

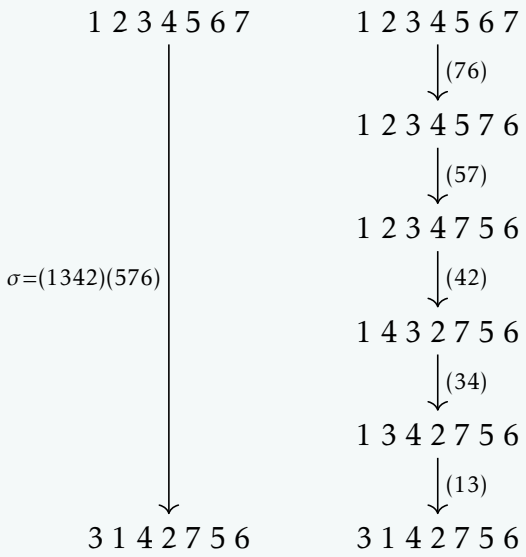
Důkaz. Formální. Vynechám. Ideu si ukážeme na příkladě. □

Příklad. Rozložíme permutaci $\sigma = (1342)(576)$ na transpozice. Každý cyklus vlastně rozdělíme na cykly délky dva (což jsou vlastně transpozice) zdvojením každého vnitřního prvku. Tedy, cyklus (576) se rozdělí na transpozice (57) a (76) a cyklus (1342) se rozdělí na (13), (34) a (42). Pak dostaneme (**pozor na pořadí!**)

$$\sigma = (13) \circ (34) \circ (42) \circ (57) \circ (76),$$

což je rozklad σ na transpozice. Na obrázku vidíte znázornění aplikace permutace σ na množinu $\{1, \ldots, 7\}$ a postupnou aplikaci přísluš-

ných transpozic.



Obrázek 20: Znázornění rozkladu permutace σ na transpozice.

Definice 3.2.4 (Sudá/lichá permutace)**.** Permutaci $\sigma \in S_X$ nazveme *sudou*, když její rozklad na transpozice obsahuje sudý počet transpozic. Jinak ji nazveme *lichou*.

Poslední zajímavý výsledek o permutacích, který zmíníme, říká, že když jednu permutaci složím samu se sebou dostatečněkrát, dostanu identické zobrazení na X. Počtu složení se formálně říká „řád“ permutace.

Definice 3.2.5 (Řád permutace)**.** Mějme $\sigma \in S_X$. Přirozené nenulové číslo $k \in \mathbb{N}$ nazveme *řádem* permutace σ, když

$$\sigma^k = \mathbb{1}_X.$$

Řád permutace značíme $\operatorname{ord}\sigma$ (z angl. **ord**er).

Na konec sekce si rozmyslíme, že každá permutace má konečný řád a jak ho počítat. Uvažme třeba permutaci $\sigma = (143)$. Tahle permutace posílá 1 na 4, 4 na 3 a 3 zpět na 1. To ovšem znamená, že když ji „zopakuji“ třikrát

za sebou, dostanu se rovnou z 1 na 1. Vskutku, můžete si ověřit, že

$$\sigma^3 = (143) \circ (143) \circ (143) = \mathbb{1}_{\{1,2,3,4\}}.$$

Tento pohled napovídá, že když cyklus délky k zopakuji k-krát, zobrazím všechny prvky v tomto cyklu na ony samé.

Co když mám ale permutaci složenou z cyklů různých délek, jako třeba (143)(25)? No, cyklus (143) musím zopakovat třikrát a cyklus (25) dvakrát. Když ale tuto permutaci třikrát zopakuji, nedostanu identické zobrazení, protože cyklus (25) zopakovaný třikrát je zase (25). Když se zamyslíme, zjistíme, že abych dostal z permutace identické zobrazení, musím ji opakovat právě tolikrát, kolik je nejmenší společný násobek délek jejích cyklů, aby se každý cyklus zopakoval nějakým násobkem své délky. Zformulujeme si tento fakt jako tvrzení, ale dokazovat ho nebudeme, protože důkaz je otravně formální.

Tvrzení 3.2.3 (O řádu permutace)**.** Ať $\sigma \in S_X$ a

$$\sigma = c_1 c_2 \cdots c_n$$

je zápis σ v cyklech $c_1, \ldots, c_n$. Označme d_i délku cyklu c_i pro každé $i \leq n$. Pak

$$\operatorname{ord} \sigma = \operatorname{lcm}(d_1, \ldots, d_n),$$

kde lcm (z angl. **l**east **c**ommon **m**ultiple) značí nejmenší společný násobek.

Myslím, že tohle tvrzení je pěkným příkladem přirozeného avšak poměrně silného tvrzení. Kdybyste nevěděli nic o permutacích a řekl bych vám, že máte dokázat fakt, že když bijekci na konečné množině složím samu se sebou hodněkrát, dostanu identické zobrazení, asi byste se zapotili.

3.3 Problém sta vězňů

Za sedmero horami a sedmero řekami, byla nebyla kdysi jedna věznice, ve které bylo žilo a živořilo sto vězňů. Její dozorce, chor a zchřadl, matematik řemeslem a krutovládce povahou, jednoho jitra rozhodl, že vězně propustí – buď do světa, nebo až do toho příštího.

Vyklidiv vězeňskou jídelnu, postavil zde sto dřevěných stolic nesoucích

sto papírových obálek. Mezi obálky rozloučil sto kamení, v každém toporně vyryto různé číslo od jedné do sta.

Rozkázav vězně seřaditi před jídelnu, přičlenil každému rovněž různé číslo od jedné do sta, v pořadí, kterak stáli. Vězni měli po řadě postoupit do jídelny a otevřít padesát obálek. Našli-liž mezi nimi kámen zračící jejich číslo, vrátili jej zpět a směli opustit jídelnu opačným východem.

Podmínka propuštění děla, že každý vězeň musí v jedné z padesáti obálek, které otevřel, zřít své číslo. Pokud byť i jeden vězeň své číslo neobjeví, celé těleso vězňů bude kvapně popraveno.

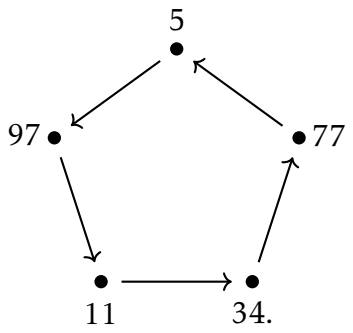
Asi není těžké si rozmyslet, že tohle je úloha na permutace. Pořadí, v jakém jsou umístěny stolice, můžeme vnímat jako množinu přirozených čísel $\{1,\ldots,100\}$ a rozmístění kamenů do obálek jako jednu její náhodně zvolenou permutaci. Tedy, to, že v obálce číslo 6 je kámen s číslem 23 znamená, že tato permutace posílá prvek 6 na prvek 23.

Pokud by vězni vybírali obálky k otevření náhodně, pak má každý z nich na nalezení kamene se svým číslem šanci přesně 1/2. Protože tahle situace se má opakovat stokrát po sobě, šance, že všichni najdou tímto způsobem své číslo, je $(1/2)^{100}$, tedy 1 ku 1 267 650 600 228 229 401 496 703 205 376 – čili pořád větší, než že si MŠMT všimne, že existují počítače – ale přesto malá.

My tvrdíme, že ve skutečnosti existuje strategie, která umožní vězňům uniknout poslednímu dechu s šancí větší než 30 %. Navíc je velmi přímočará. Stačí, aby každý vězeň otevíral obálky v pořadí, které určují kameny v nich obsažené. Konkrétně, každý vězeň otevře jako první obálku na stolici se stejným pořadím, jako je to jeho. Další otevře obálku na stolici s pořadím, které odpovídá číslu na kameni v obálce, kterou právě otevřel. Takhle pokračuje, dokud nenajde své číslo, nebo dokud neprojde padesát různých obálek.

Ilustrujme si postup na příkladě. Do jídelny vstoupí vězeň s číslem 11. Otevře obálku číslo 11 a najde v ní kámen s číslem 34. Dále otevře obálku s číslem 34, v níž je číslo 77. Ještě jednou, v obálce číslo 77 najde číslo 5. V obálce číslo 5 najde kámen s číslem 97. A nakonec – Ejhle! – v obálce číslo 97 najde kámen se svým číslem – 11.

Označme permutaci určenou čísly na kamenech v obálkách třeba κ (jako **k**ámen). Situace v předchozím odstavci znamená, že v κ existuje cyklus



Nyní už si můžeme rozmyslet, za jaké podmínky objeví všichni vězni obálku s kamenem svého čísla. V moment, kdy vězeň otevře první obálku, dostane se tím do jednoho konkrétního cyklu permutace κ. Podle dané strategie bude tento cyklus sledovat až do konce. Pokud je délka daného cyklu třeba d, pak v moment, kdy otevře tento vězeň svoji d-tou obálku, bude v ní kámen s jeho číslem. Samozřejmě, podmínka propuštění říkala, že každý vězeň smí otevřít maximálně 50 obálek. Protože každý vězeň má přiřazeno jiné, určitě čísla všech vězňů dohromady vyčerpají všechny cykly permutace κ. To znamená, že všichni vězni najdou svoje číslo tímto postupem jedině v případě, **kdy permutace κ neobsahuje cyklus délky větší než 50**. Zformulujeme si to jako pozorování.

> **Pozorování.** Problém sta vězňů má řešení (tedy všech sto vězňů bude propuštěno) právě tehdy, když permutace κ, určená čísly na kamenech v obálkách, neobsahuje cyklus délky větší než 50.

Abychom spočítali šanci vězňů na úspěch, zbývá nám umět spočítat počet všech takových permutací, tj. permutací s cykly délky maximálně 50.

Ať $X := \{1,\dots,100\}$. Bude výhodnější řešit opačný problém, tedy hledat počet permutací s cyklem délky aspoň 51, protože (vzhledem k tomu, že množina X má 100 prvků), takový cyklus tam může být nejvýše jeden.

Ať $C_n(S_X)$ značí počet všech permutací na X s aspoň jedním cyklem délky n. Jak jsme právě řekli, pro $n \geq 51$ může mít libovolná permutace takový cyklus jenom jeden. Dále je zřejmé, že počet všech permutací s cyklem délky *aspoň* 51 spočtu tak, že sečtu počty permutací s cyklem délky n pro všechna n od 51 do 100. Když $C_{\geq 51}(S_X)$ značí počet permutací s cyklem

délky aspoň 51, máme

$$C_{\geq 51}(S_X) = \sum_{n=51}^{100} C_n(S_X).$$

Spočítáme $C_n(S_X)$ pro $n \geq 51$. Abychom určili permutace s cyklem délky n, musíme zvolit n z těch 100 čísel, která se v cyklu objeví. Počet způsobů, jak zvolit n čísel ze 100 je $\binom{100}{n}$ (vizte sekci o kombinačních číslech). Čísla v tomto cyklu mohou být uspořádána $n!$ způsoby. **Ovšem, pozor!** Nezapomeňte, že uvnitř cyklu mohu čísla posouvat a cyklus tím nechat stejný. Protože mám v cyklu n čísel, dělá to dohromady n možných posunutí. Tedy mám

$$\frac{\binom{100}{n} n!}{n} = \binom{100}{n} (n-1)!$$

různých způsobů, jak zvolit cyklus délky n.

Konečně, zbývající čísla (tedy ta mimo ten cyklus) můžu přeuspořádat $(100-n)!$ způsoby. Celkem, počet všech permutací s cyklem délky n pro $n \geq 51$ je

$$C_n(S_X) = \binom{100}{n} (n-1)!(100-n)!.$$

Je na čase završit výpočet. Všech možných permutací na 100 číslech je 100!. Počet všech permutací s cyklem délky aspoň 51 je $C_{\geq 51}(S_X)$. Čili šance, že náhodně vybraná permutace na 100 číslech **obsahuje** cyklus délky větší než 50 je

$$\frac{C_{\geq 51}(S_X)}{100!} = \frac{\sum_{n=51}^{100} C_n(S_X)}{100!} = \frac{\sum_{n=51}^{100} \binom{100}{n} (n-1)!(100-n)!}{100!} \approx 0.688,$$

čili 68,8 %. To ovšem znamená, že šance, že náhodná permutace **neobsahuje** cyklus délky větší než 50 je přibližně $1 - 0.688 = 0.312$. Takže při využití této strategie mají vězni přibližně 31.2 % na přežití. O něco lepší než náhodné zkoušení.

Cvičení 3.3.1. Spočtěte složení $\sigma\tau$ a $\tau\sigma$, když

(1) $\sigma = (143)(26), \tau = (146)(253)$,

(2) $\sigma = (14)(25)(36), \tau = (123456)$,

(3) $\sigma = (145)(263), \tau = (154)(236)$.

Cvičení 3.3.2. Určete řád permutace σ, kde

(1) $\sigma = (1345)$,

(2) $\sigma = (1346)(28)(579)$.

Cvičení 3.3.3 (těžké)**.** Určete číslo $C_n(S_X)$, kde $\#X = 100$ a $n \leq 50$, tedy počet všech permutací na 100 číslech s aspoň jedním cyklem délky menší nebo rovné 50.

Cvičení 3.3.4. Ať $\sigma \in S_n$, tedy σ je permutace množiny $\{1,\dots,n\}$. Řekneme, že σ *invertuje* dvojici (i,j), kde $i,j \in \{1,\dots,n\}$, když $i < j$, ale $\sigma(i) > \sigma(j)$.

Definujme

$$I(\sigma) := \{(i,j) \in \{1,\dots,n\}^2 \mid \sigma \text{ invertuje } (i,j)\},$$

čili $I(\sigma)$ je množina všech dvojic (i,j), které σ invertuje. Uvědomme si, že $I(\sigma)$ je podmnožinou $\{1,\dots,n\}^2$, čili relací na $\{1,\dots,n\}$.

(1) Dokažte, že $I(\sigma)$ je transitivní relace na $\{1,\dots,n\}$ pro každou permutaci $\sigma \in S_n$.

(2) * Navrhněte algoritmus, který pro danou permutaci $\sigma \in S_n$ spočte $\#I(\sigma)$.

(3) Spočtěte počet invertovaných dvojic, čili $\#I(\sigma)$, permutací $\sigma = (134)(579)(26)$.