Do nekonečna a ještě dál

Nikdo nás nebude moci vyhnat z ráje, který pro nás vytvořil Cantor. (David Hilbert)

Díl první – Svět nekonečen

Pojmem nekonečna se zabývali filosofové a matematici již od dob, kdy rozdíl mezi filosofií a matematikou byl pramalý. My si zde předvedeme až výsledky matematiků 19. a 20. století počínaje Georgem Cantorem. Ti na své cestě vyzkoušeli řadu slepých uliček a nejednoho z nich to stálo duševní zdraví. Výsledkem však je krásná teorie, nyní všeobecně uznávaná za základ takřka veškeré vysokoškolské matematiky.

Název celého seriálu *Do nekonečna a ještě dál* je mimo jiné odkazem na sérii animovaných filmů Příběh hraček. Jedná se o slavnou hlášku hračky Buzze Rakeťáka – superastronauta, který létá z planety na planetu a zachraňuje svět. Dítě, které si z Buzzem hraje, je nadšené z toho, že s ním létá „do nekonečna a ještě dál“, a to ani nemá ponětí, o čem vlastně mluví. Cílem seriálu, který taktéž bude místy pojat pohádkově či hravě, je tuto otázku objasnit a přitom neubrat nekonečnu nic z jeho kouzla.

V odborných publikacích nese téma tohoto seriálu suché označení *Teorie množin*. Důvod, proč tomu tak je, bude patrný zejména z druhého dílu *Pevné základy*. Nicméně ani vysokoškoláci neztrácejí hravost a ohromení z nekonečna, což reflektuje fakt, že běžným slangovým označením pro teorii množin je zkratka TeMno. ;-)

První nástrahy nekonečna

Než se pustíme do nekonečna, dohodneme se na jednom základním značení: Množinu přirozených čísel značíme ω a **nulu budeme považovat za přirozené číslo.**[1] Toto značení je v teorii množin obvyklé a důvody jeho používání budou více patrné z druhého dílu seriálu. Mimo jiné se nám bude hodit, aby šlo říci „Konečné množiny jsou právě ty množiny, jejichž velikost vyjadřuje nějaké přirozené číslo.“ a nevyřadit tím z konečných množin prázdnou množinu. Nicméně pozor, tato úmluva platí pouze zde a v úlohách patřících k tomuto seriálu, v jiných středoškolských úlohách se nula za přirozené číslo běžně nepovažuje.

Zatímco nula je přirozeným číslem, nekonečno žádným číslem není. Nekonečno ve skutečnosti ani není nějaký matematický objekt, je to jen vlastnost. Přímka je nekonečná, posloupnost může být nekonečná, množina může být nekonečná. Jedná se o opak konečnosti, kde konečnost přesně znamená, že se velikost dané množiny nebo posloupnosti dá vyjádřit přirozeným číslem. Nekonečná množina pak je taková, jejíž velikost se žádným přirozeným číslem vyjádřit nedá, je na to „příliš velká“. Existují i další důvody, proč se nekonečno nepovažuje za přirozené číslo – chová se totiž úplně jinak.

[1] Řecké písmenko ω je malá omega, zatímco velká omega vypadá takto: Ω.

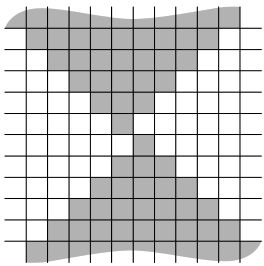
Příklad. Kdykoli si vezmeme konečnou množinu reálných čísel, najdeme v ní největší i nejmenší prvek. U nekonečné množiny se to stát může, ale nemusí. Například uzavřený interval $\langle 0, 1\rangle$ má nejmenší prvek 0 a největší prvek 1, zatímco otevřený interval $(0, 1)$ nemá ani nejmenší, ani největší prvek.

Další příklad ukazuje, že když něco může být libovolně velké, ještě to neznamená, že to může být nekonečné.

Příklad. Existuje libovolně dlouhá klesající posloupnost přirozených čísel. Pokud si usmyslíme, že chceme posloupnost délky n, sestrojíme ji coby $n, (n-1), \ldots, 2, 1$. Naopak nekonečná klesající posloupnost $a_0, a_1, a_2, \ldots$ přirozených čísel existovat nemůže.

Dále tu máme malý paradox.

Příklad. Nekonečnou čtverečkovou síť lze celou obarvit dvěma barvami, šedou a bílou, tak, aby každý řádek obsahoval jen konečně mnoho šedých políček a každý sloupec jen konečně bílých políček. Lze to udělat třeba takto:



Znázornění obarvené mřížky podle zadání

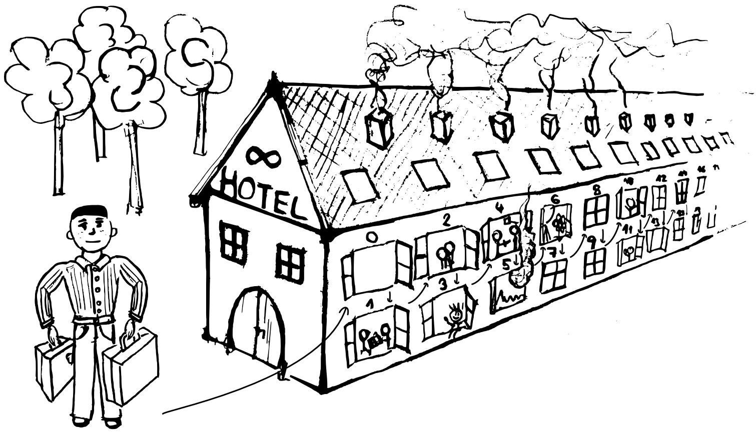
Na druhou stranu, kdyby byly řádky omezeny konkrétním přirozeným číslem, například „v řádku může být nanejvýš 2015 šedých políček“, už by takové obarvení nešlo najít. Proč? Představme si obarvenou mřížku a z ní vyjměme 2016 sloupečků. Pak by v každém řádku muselo být alespoň jedno bílé políčko. To je dohromady nekonečně mnoho bílých políček v konečně mnoha sloupečcích, takže by v některém sloupečku muselo být nekonečně mnoho bílých políček.

A jako poslední příklad, jak se nekonečno chová odlišně od konečna, uvedeme tradiční (leč převyprávěnou) pohádku, která v úvodu do nekonečna nesmí chybět. Dokonce můžeš najít její anglickou video verzi na stránkách `www.hotel-infinity.com`.

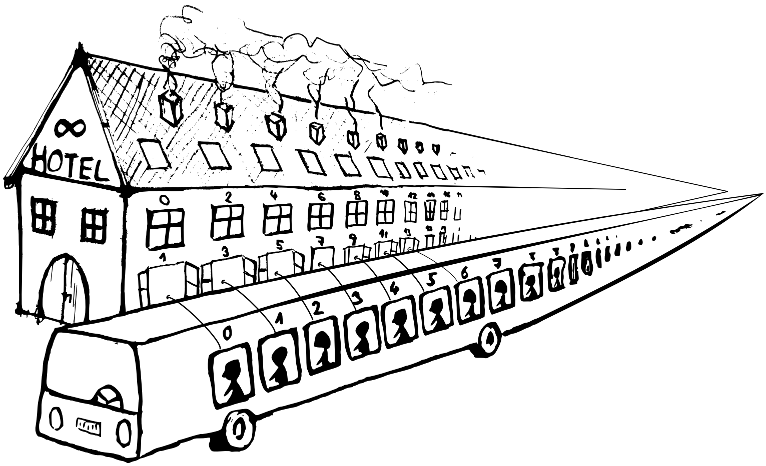
Pohádka o Hilbertově hotelu

Byl nebyl jeden turista. Ten cestoval přes devatero hor a devatero řek, až přišel do jednoho městečka. Doufal, že by si po náročné cestě mohl odpočinout v některém z tamních ubytovacích zařízení. Přišel k jednopokojovému apartmánu. „Mohl bych se tu ubytovat?“ zeptal se. „Kdepak,“ odvětil majitel, „teď tu někoho máme.“ Turista tedy šel dál, až přišel k hotelu s tisícem pokojů. „Panečku, to je velký hotel,“ pomyslil si, „tady pro mne určitě budou mít místo.“ Záhy však byl recepcí zklamán: „Bohužel, všechny pokoje jsou obsazené.“ „A nešlo by třeba ty hosty nějak přeuspořádat? Víte, cestoval jsem přes …“ „Ani omylem,“ odvětila recepční, „jak chcete nacpat 1001 hostů do 1000 pokojů? Copak neznáte Dirichletův princip?“

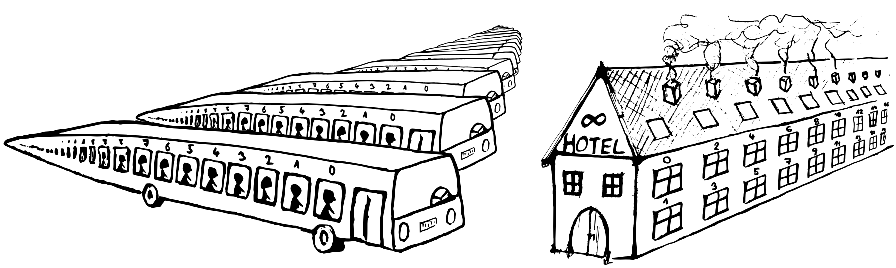
A tak šel náš cestovatel dál, až přišel k dalšímu hotelu, k Hilbertovu hotelu. Hilbertův hotel není obyčejný hotel. Je to kouzelný hotel, má totiž nekonečně mnoho pokojů. V tomto hotelu jsou pokoje číslované přirozenými čísly, a pod každým číslem se skrývá některý pokoj. „Tady nemáte všechny pokoje obsazené, že ne?“ ujišťoval se turista při pohledu na to neskutečné množství pokojů. „Máme,“ odpověděl majitel hotelu David Hilbert, „to víte, je hlavní turistická sezona.“ „Ach jo, tak já zase půjdu,“ řekl zklamaně turista. „Ale, ale, kam byste chodil?“ Hilbert na to, „určitě tu pro vás místo najdeme.“ Vzal do ruky mikrofon a hotelovým rozhlasem zaznělo: „Pozor, pozor! Žádáme všechny hosty, aby se přesunuli do pokoje s číslem o jedna vyšším, než ve kterém právě bydlí.“ Pak se Hilbert obrátil k našemu turistovi: „No vidíte, teď se můžete nastěhovat do prázdného pokoje číslo nula a hotel bude zase plný.“ Turista vešel do svého pokoje. Spokojeně; ještě netušil, kolikrát se bude muset stěhovat.



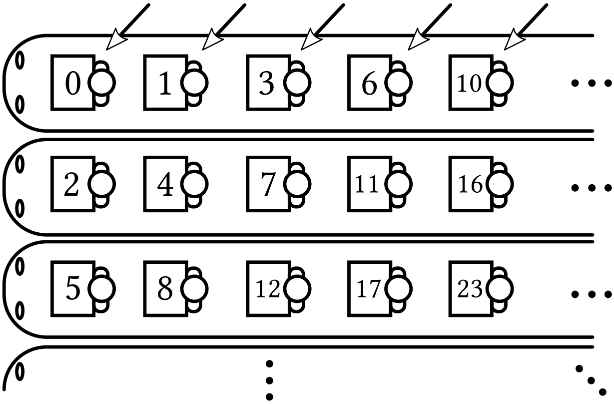
Pak k hotelu přijel autobus se sto lidmi, kteří se zde chtěli ubytovat. To pro hoteliéra Hilberta nebyl žádný problém: „Pokud číslo vašeho pokoje je k, tak se přestěhujte do čísla $k + 100$.“ A hned se zas uvolnilo 100 míst. Když pak ale přijel k hotelu autobus, který měl stejnou kapacitu jako Hilbertův hotel, tedy zaplněná sedadla se všemi přirozenými čísly, byl to již trochu oříšek. Není možné říct „posuňte se o nekonečno míst dál“ – neexistuje přirozené číslo, které by bylo o nekonečno větší než nula nebo jednička. Proto bylo třeba provést trochu rafinovanější operaci: „Ten, kdo bydlí v pokoji s číslem k, se přestěhuje do pokoje s číslem $2k$. Ten, kdo sedí v autobuse na sedadle s číslem k, se nastěhuje do pokoje s číslem $2k + 1$.“



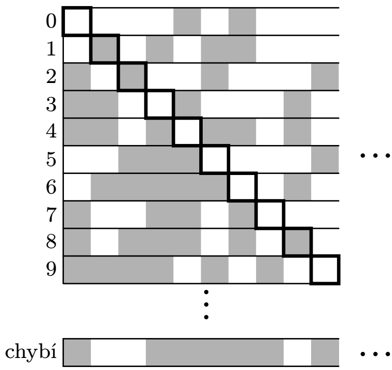
To byl šrumec, panečku; kufry létaly, zámky cvakaly, ale nakonec se povedlo do hotelu umístit celý nekonečný autobus. A jen co autobus odjel, ani hosté se ještě pořádně neusadili, řítí se k hotelu nekonečně mnoho takových autobusů – opět číslovaných přirozenými čísly.



Ještě jsme nezmínili, že David Hilbert byl (ještě než jsme jej usadili do jeho vlastní pohádky) matematik. A matematici rádi převádí problém na předchozí případ. Pokud by se podařilo rozdat lidem v autobusech lístečky s různými přirozenými čísly, jednalo by se o stejnou situaci jako v případě, kdy přijel jen jeden nekonečný autobus s očíslovanými sedadly. Zbývá otázka, jak to provést. Pokud by Hilbert začal postupně rozdávat čísla $0, 1, 2, \ldots$ lidem v autobuse 0, na cestující v ostatních autobusech by se nedostalo. Stejně tak, kdyby začal s tím, že by v každém autobuse rozdal jeden lísteček cestujícímu na sedadle 0, na cestující na ostatních sedadlech by se nedostalo. Nakonec však David Hilbert přišel na to, jak lístečky rozdat: Uspořádá si cestující primárně podle součtu čísel autobusu a sedadla a sekundárně podle čísla autobusu. Jinými slovy rozdá lístečky po zpětných úhlopříčkách, jak je naznačeno na následujícím obrázku.



Pak přijel k hotelu další nekonečný autobus. Ten však neměl sedadla číslovaná přirozenými čísly, nýbrž nekonečnými posloupnostmi bílých a šedých čtverečků. To znamená, že každé sedadlo bylo označeno nějakou nekonečnou posloupností čtverečků, přičemž každé dvě posloupnosti se lišily a naopak i každá možná posloupnost připadla nějakému sedadlu. „Když jsem už ubytoval nekonečno autobusů, jeden autobus navíc nemůže být problém," pomyslel si Hilbert a opět se jal vymýšlet nějaký chytrý způsob, jak taková sedadla očíslovat přirozenými čísly. Přemýšlel tuze dlouho. Ubytovaní hosté už šli spát, byli rádi, že to stěhování utichlo, a Hilbert stále na nic nepřišel. A byl by nad tím dumal dodnes, kdyby nezjistil, že teď už opravdu prohrál. Hosté z tohoto autobusu se do Hilbertova hotelu nevejdou. Proč? Protože ať rozdá lístečky s přirozenými čísly cestujícím jakkoli, vždy se najde cestující, na kterého se nedostalo. Jednoho takového odhalíme například takto:[2] Nakreslíme pod sebe posloupnosti bílých a šedých čtverečků v tom pořadí, v jakém jim byly přiřazeny kartičky s přirozenými čísly. Následně se podíváme na úhlopříčku a vytvoříme z ní novou posloupnost čtverečků, kterou následně invertujeme – nahradíme bílou barvu za šedou a obráceně. Tím dostaneme novou posloupnost, která se liší od všech v tabulce (od posloupnosti s číslem n přinejmenším na pozici n), což znamená, že příslušný cestující nedostal lísteček.



Znázornění Cantorovy diagonální metody

[2]Tento postup se běžně nazývá Cantorovou diagonální metodou.

Porovnávání nekonečen

Z pohádky plynou dvě poučení. První poučení je, že nekonečno je hodně nafukovací, a druhé je, že přesto není nafukovací nade všechny meze. Nyní se pokusíme pohádku více zasadit do matematického rámce. Konečné množiny mezi sebou porovnávat umíme: Spočítáme, kolik prvků má první množina, kolik prvků má druhá množina a za větší prohlásíme tu množinu, jejíž počet prvků je vyšší přirozené číslo. Naším cílem je toto porovnávání množin zobecnit, aby jej bylo možné použít i pro nekonečné množiny. Klíčovým nástrojem pro porovnávání množin je zobrazení neboli funkce.

Definice. *Zobrazení* (nebo též *funkce*) f je předpis, který na vstupu dostane matematický objekt x a na základě něj vytvoří výstupní objekt $f(x)$ (také nazývaný *obraz* bodu x). Tento předpis může ale také dané x nezpracovat (říkáme, že $f(x)$ nemá smysl).

(i) *Definiční obor* funkce f je množina objektů x, pro které má $f(x)$ smysl. Obecně značením $f\colon A \to B$ říkáme, že definičním oborem funkce f je množina A a každé $f(a)$ leží v množině B. Slovy lze také říci, že se jedná o funkci z A do B, případně, že je tato funkce definovaná na množině A.

Symbol $\mathbb{R}$ značí množinu všech reálných čísel. Příkladem funkce $f\colon \mathbb{R} \to \mathbb{R}$ může být funkce daná předpisem $f(x) = x^2$.

(ii) Funkce je *prostá*, pokud dvěma různým prvkům nikdy nepřiřadí stejný prvek. Například v pohádce vždy Hilbert hledal zobrazení z množiny hostů do množiny pokojů, a to navíc prosté, tedy takové, aby žádní dva hosté neskončili ve stejném pokoji.

(iii) *Bijekce* $f\colon A \to B$ je prostá funkce, pro kterou je každý prvek množiny B reprezentovaný nějakým $f(a)$. Jde tedy o popárování prvků množiny A s prvky množiny B.

(iv) Uvažme funkci f definovanou na množině A a podmnožinu A' této množiny. Pak *zúžení* funkce f na množinu A' značíme $f \restriction A'$. Jedná se o funkci, která má za definiční obor A' a chová se na něm stejně jako f. Tedy $(f \restriction A')(x) = f(x)$ pro x z A'. Například funkce definovaná v bodě (i) není prostá, ale její zúžení na množinu kladných čísel už je prosté.

(v) Mějme funkci $f\colon A \to B$ a na obou množinách A i B mějme zavedené uspořádání (tedy definované, co znamená $x < y$). Říkáme, že f je *rostoucí*, pokud zachovává toto uspořádání, tedy pro libovolné $a_0 < a_1$ z A platí $f(a_0) < f(a_1)$.

Nyní již můžeme říci, jak se množiny porovnávají. Mějme množiny A a B. Říkáme, že:

(i) Množiny A a B mají *stejnou mohutnost* (značíme $|A| = |B|$), pokud existuje nějaká bijekce $f\colon A \to B$.

(ii) Mohutnost A je *menší nebo rovna mohutnosti* B (značíme $|A| \leq |B|$), pokud existuje prosté zobrazení $f\colon A \to B$.

(iii) Mohutnost množiny A je ostře menší než mohutnost množiny B (značíme $|A| < |B|$), pokud $|A| \leq |B|$, ale neplatí $|B| \leq |A|$.

A nakonec okolo množin definujeme ještě několik dalších pojmů.

(i) Pokud množina A splňuje $|A| \leq |\omega|$, říkáme, že je *spočetná*, v opačném případě říkáme, že je *nespočetná*. Spočetná množina je tedy taková, která se vejde do Hilbertova hotelu.

(ii) Pro dvě množiny A, B definujeme jejich *kartézský součin* $A \times B$ jako množinu všech uspořádaných dvojic[3] (a, b), kde a je prvek množiny A a b je prvek množiny B. Jsou-li obě množiny A, B konečné, je počet prvků množiny $A \times B$ roven součinu mohutností množin A a B coby přirozených čísel.

(iii) Pro množinu A definujeme její *potenci* (značíme $P(A)$) jako množinu všech jejích podmnožin včetně prázdné množiny a A samotné. Potence je tedy konkrétní příklad takového

[3] Kulatými závorkami zde budeme běžně značit uspořádané dvojice. Kdyby se mělo jednat o interval, bude to explicitně řečeno.

zobrazení, že $\mathcal{P}(X)$ má smysl na všech množinách. Je-li množina A konečná, n-prvková, je počet prvků množiny $\mathcal{P}(A)$ roven 2^n.

V pohádce jsme popsali bijekci mezi množinou cestujících v nekonečně mnoha autobusech a ω. Každý takový cestující je určený dvěma čísly: číslem autobusu a číslem sedadla. Jedná se tedy vlastně o bijekci z $\omega \times \omega$ do ω, takže platí $|\omega \times \omega| = |\omega|$. Z toho plyne, že sjednocení spočetně mnoha spočetných množin je spočetné.

Příklad. Množina S všech sudých přirozených čísel má stejnou mohutnost jako ω, není tedy „dvakrát menší“, jak by se mohlo na první pohled zdát. Příslušná bijekce $f\colon \omega \to S$ může být například daná předpisem $f(x) = 2x$. Obecně má každá nekonečná podmnožina X množiny ω stejnou mohutnost jako ω, tedy dá se říci, že ω je nejmenší nekonečná množina. Příslušná bijekce $\omega \to X$ může vypadat takto: Číslu 0 přiřaď nejmenší prvek X, číslu 1 přiřaď druhý nejmenší prvek X atd.

Příklad. Množina $\mathbb{Q}$ je spočetná.[4]

Důkaz. Nejprve ukážeme, že množina $\mathbb{Z}$ všech celých čísel je spočetná. Existuje totiž bijekce $f\colon \mathbb{Z} \to \omega$, například definovaná předpisem $f(n) = 2n$ pro přirozená čísla n a $f(m) = -2m - 1$ pro záporná čísla m. Snadno se ověří, že takové zobrazení je skutečně bijekce.

Díky tomu je spočetná i množina všech zlomků tvaru $\frac{n}{1}$, kde n je celé číslo. Stejně tak množina všech zlomků tvaru $\frac{n}{2}$, stejně tak množina všech zlomků tvaru $\frac{n}{3}$ atd. Množina $\mathbb{Q}$ je pak sjednocením těchto spočetně mnoha spočetných množin, a proto je spočetná. $\square$

Příklad. *Polynom s racionálními koeficienty* je funkce $f\colon \mathbb{R} \to \mathbb{R}$ daná předpisem tvaru

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0,$$

kde n je přirozené číslo a $a_0, \ldots, a_n$ jsou racionální čísla (říkáme jim *koeficienty*). Polynomů s racionálními koeficienty je spočetně mnoho (neboli množina těchto polynomů je spočetná).

Důkaz. Polynom může mít libovolný konečný počet koeficientů. Pro dané n budeme symbolem $\mathbb{Q}^n[x]$ značit množinu všech (racionálních) polynomů pouze s koeficienty $a_0, \ldots, a_n$. Polynomy z množiny $\mathbb{Q}^0[x]$ mají jen koeficient a_0, a proto $|\mathbb{Q}^0[x]| = |\mathbb{Q}| = |\omega|$. Polynomy z množiny $\mathbb{Q}^1[x]$ mají dva koeficienty, tedy $|\mathbb{Q}^1[x]| = |\mathbb{Q} \times \mathbb{Q}| = |\omega \times \omega| = |\omega|$. Dále polynomy z množiny $\mathbb{Q}^2[x]$ mají o jeden racionální koeficient více než prvky $\mathbb{Q}^1[x]$, proto $|\mathbb{Q}^2[x]| = |\mathbb{Q} \times \mathbb{Q}^1[x]| = |\omega \times \omega| = |\omega|$. Podobně $|\mathbb{Q}^3[x]| = |\mathbb{Q} \times \mathbb{Q}^2[x]| = |\omega \times \omega| = |\omega|$ a tak dále, obecně vždy odvodíme $|\mathbb{Q}^n[x]| = |\mathbb{Q} \times \mathbb{Q}^{n-1}[x]| = |\omega \times \omega| = |\omega|$. Takto dostaneme, že všechny množiny $\mathbb{Q}^n[x]$ jsou spočetné. Navíc jich je spočetně mnoho, takže je spočetné i jejich sjednocení čili množina všech polynomů s racionálními koeficienty. $\square$

A teď nás čeká první nespočetné cvičení.

Cvičení 1. Označme symbolem $\check{C}$ množinu všech nekonečných posloupností bílých a šedých čtverečků jako v pohádce. Rozmysli si, že $|\check{C}| = |\mathcal{P}(\omega)|$.

Obecně můžeme říci, že potence je nástroj na výrobu větších nekonečen, čímž myslíme, že pro každou množinu A platí $|A| < |\mathcal{P}(A)|$. Důkaz se opírá o závěr pohádky, ale je obecnější a dívá se na záležitost trochu jinými pojmy, takže si jej raději předvedeme:

Pro důkaz tvrzení $|A| < |\mathcal{P}(A)|$ potřebujeme ukázat, že existuje prostá funkce $A \to \mathcal{P}(A)$, ale neexistuje prostá funkce $\mathcal{P}(A) \to A$. Funkci $f\colon A \to \mathcal{P}(A)$ jednoduše sestrojíme tak, aby každému prvku přiřadila jednoprvkovou množinu obsahující právě tento prvek, tedy $f(a) = \{a\}$.

Druhou část dokážeme sporem – předpokládejme, že existuje prostá funkce $g\colon \mathcal{P}(A) \to A$. Sestrojíme podmnožinu S množiny A podle následujícího pravidla: Pro každou podmnožinu B množiny A

[4]Symbolem $\mathbb{Q}$ značíme množinu všech racionálních čísel neboli čísel vyjádřitelných jako podíl dvou celých čísel.

se podíváme, zda je $g(B)$ prvkem B. Pokud není, umístíme $g(B)$ do S, v opačném případě jej tam nedáme. Jinými slovy je S množina obrazů těch podmnožin, které neobsahují svůj obraz. Protože S je také množina, určitě má i sama obraz $g(S)$. Ale zdalipak je $g(S)$ prvkem S? Kdyby bylo prvkem S, tak bychom jej do S ale nemohli dát (ani za jinou podmnožinu, protože g je prostá), a naopak kdyby nebylo, tak bychom jej do S museli dát – dostáváme spor, a proto funkce g nemůže existovat.

Kolem porovnávání nekonečen nám zatím zůstává řada otazníků.

(i) Musí vždy nastat alespoň jedna z možností $|A| \leq |B|$ nebo $|B| \leq |A|$?

(ii) Pokud $|A| \leq |B|$ a současně $|B| \leq |A|$, musí už nutně $|A| = |B|$?

(iii) Pokud platí $|A| \leq |B|$ a současně $|B| \leq |C|$, musí už nutně $|A| \leq |C|$? A pokud je navíc některá z původních nerovností ostrá, musí už nutně $|A| < |C|$?

(iv) Když už je ω nejmenší nekonečná množina, je $\mathcal{P}(\omega)$ nejmenší nespočetná množina?

A abychom se měli na co těšit, nastíníme stručně odpovědi.

(i) Ano, ale není to lehké dokázat, bude to ukázáno ve třetím díle.

(ii) Ano, toto bychom mohli dokázat elementárně, ale počkáme si na třetí díl, kde to ukážeme spolu s (i). Můžeš to zkusit už teď dokázat coby těžší cvičení, případně si vyhledat Schröder–Bernstein theorem na anglické Wikipedii.

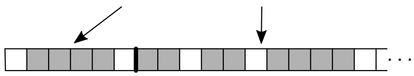
(iii) Oboje platí, rozmysli si to jako cvičení. ;-)

(iv) Tato otázka byla dlouho nevyřešená a říká se jí *hypotéza kontinua*. Nakonec se ukázalo, že hypotézu kontinua není možné dokázat ani vyvrátit; pochopit, proč tomu tak je, ale vyžaduje znalosti nad rámec tohoto seriálu. Přesto si ve druhém díle sestrojíme nejmenší nespočetnou množinu, jen nebude jasné, zda má stejnou mohutnost jako $\mathcal{P}(\omega)$.

Příklad. Označme opět symbolem $\check{C}$ množinu všech nekonečných posloupností bílých a šedých čtverečků jako v pohádce. Popíšeme prosté zobrazení $f\colon \mathbb{R} \to \check{C}$, takže ukážeme, že $|\mathbb{R}| \leq |\check{C}| = |\mathcal{P}(\omega)|$. Zobrazení dostane reálné číslo x. Pak najdeme nejvyšší celé číslo, které nepřevyšuje x (dolní celá část), značíme jej $\lfloor x \rfloor$. Je-li číslo $\lfloor x \rfloor$ kladné, zakreslíme takový počet šedých čtverečků, jak velké toto číslo je, a následně jeden bílý čtvereček. Je-li nekladné (nula nebo záporné), zakreslíme jeden bílý čtvereček, pak $-\lfloor x \rfloor$ šedých čtverečků a nakonec opět jeden bílý čtvereček.

Zbývá zakódovat necelou část reálného čísla x, tedy $x - \lfloor x \rfloor$. To je nezáporné reálné číslo menší než jedna. Ve dvojkové soustavě[5] tak bude tvaru $0.\langle$posloupnost nul a jedniček$\rangle$. Nulu zapíšeme jako bílý čtvereček, jedničku jako šedý čtvereček a doplníme takto zbylé čtverečky. Snadno ověříme, že toto kódování popisuje prosté zobrazení.

$$-\pi = -4 + .110110111100^{\mathrm{BIN}} \ldots$$



Cvičení 2.

(i) Rozmysli si, že se v předchozím příkladu nedostane přesně na ty prvky $\check{C}$, které obsahují jen konečně mnoho bílých čtverečků. (Vzpomeň si, že $0,\overline{9} = 1$.)

(ii) Ukaž, že množina prvků $\check{C}$, na které se nic nezobrazilo, je spočetná.

(iii) Na základě předchozího bodu uprav zobrazení $f\colon \mathbb{R} \to \mathcal{P}(\omega)$, aby se jednalo o bijekci.

Cvičení 3. Dokaž, že množina všech nekonečných posloupností přirozených čísel má stejnou mohutnost jako $\check{C}$. Pozor na ty prvky $\check{C}$, které obsahují pouze konečně mnoho čtverečků od jedné barvy.

[5] Pokud ses ještě nesetkal(a) s jinou číselnou soustavou než s desítkovou, můžeš se podívat například na `www.matematika.cz/prevod`.

Potence nám dává nástroj na výrobu větších a větších nekonečen, pojďme si s ní ještě trochu pohrát a pokusit se sestrojit co možná největší nekonečnou množinu. Platí

$$|\omega| < |\mathcal{P}(\omega)| < |\mathcal{P}(\mathcal{P}(\omega))| < |\mathcal{P}(\mathcal{P}(\mathcal{P}(\omega)))| < \cdots .$$

Dále můžeme sestrojit sjednocení A_0 všech těchto množin. Množina A_0 tedy obsahuje každý prvek, jenž se vyskytuje v některé množině tvaru

$$\underbrace{\mathcal{P}(\mathcal{P}(\cdots\mathcal{P}(}_{n}\omega)\cdots)) \quad \text{pro přirozené číslo } n.$$

Tato A_0 je ostře větší než každá z předchozích množin. Proč? Uvažme jednu z předchozích množin X. Množina $\mathcal{P}(X)$ je stejně jako X podmnožinou A_0, takže $|X| < |\mathcal{P}(X)| \leq |A_0|$, z čehož už plyne $|X| < |A_0|$.

Můžeme pokračovat. Máme

$$|A_0| < |\mathcal{P}(A_0)| < |\mathcal{P}(\mathcal{P}(A_0))| < |\mathcal{P}(\mathcal{P}(\mathcal{P}(A_0)))| < \cdots .$$

A opět můžeme sestrojit sjednocení všech těchto množin, které nazveme A_1. Analogicky sestrojíme

$$|A_0| < |A_1| < |A_2| < |A_3| < \cdots .$$

Na závěr sestrojíme sjednocení B všech těchto A_n. Samozřejmě bychom dále mohli pokračovat $|B| < |\mathcal{P}(B)| < \cdots$, ale je na čase se podívat trochu hlouběji, co se tu vlastně děje.

Pravá podstata rekurze a indukce

Rekurzivní definice a důkazy indukcí jsi už pravděpodobně potkal(a). Jestli ne, můžeš se podívat třeba na stránku `www.matematika.cz/matematicka-indukce`.

Rekurzivní definice je například následující definice Fibonacciho čísel:

$$F_0 = 0, \quad F_1 = 1, \quad F_{n+2} = F_n + F_{n+1} \text{ (pro přirozené číslo } n).$$

Prvním dvěma rovnostem říkáme *počáteční podmínka* a poslední je *rekurzivní předpis*. Indukce je technika, kterou lze využít například v důkazu následujícího tvrzení.

Příklad. Každé přirozené n lze rozložit na součet několika Fibonacciho čísel, jejichž indexy (v posloupnosti F) se vždy liší alespoň o 2.

Důkaz. Nulu napíšeme jako součet jednoho Fibonacciho čísla. Nyní půjdeme po přirozených číslech a dokážeme platnosti tvrzení pro $1, 2, 3, 4, \ldots$ Jsme v obecném n-tém kroku, kdy vlastnost dokazujeme pro číslo n. Přitom ale víme, že pro všechna nižší čísla $0, 1, \ldots, n-1$ už jsme tuto vlastnost dokázali. Zvolme Fibonacciho číslo F_i tak, aby $F_i \leq n$ a index i byl největší možný. Protože $n \geq 1$, bude $i \geq 2$. Navíc $F_{i+1} > n$, neboli

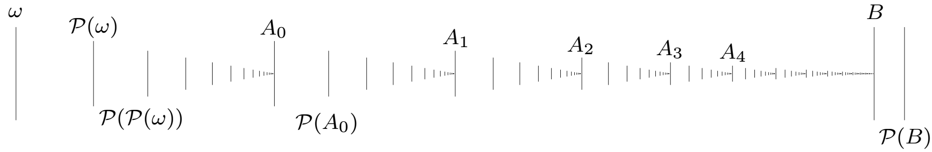
$$n - F_i < F_{i+1} - F_i = F_{i-1}.$$

V druhé rovnosti jsme použili rekurzivní předpis pro F_{i+1}. Nyní využijeme toho, že dokazujeme úlohu postupně, takže číslo $n - F_i$ již umíme rozložit podle zadání. Navíc tento rozklad neobsahuje číslo F_{i-1} (protože samotné rozkládané číslo je ostře menší), takže k tomuto rozkladu můžeme přidat číslo F_i a získat rozklad čísla n podle zadání.

Důkaz úlohy pro číslo 0 se nazývá *první krok indukce*. Důkaz pro obecné číslo n, kde předpokládáme, že pro všechna čísla menší než n tvrzení platí, se nazývá *indukční krok*. Využívaný předpoklad, že tvrzení platí pro všechna čísla menší než n, se nazývá *indukční předpoklad*.

Poznámka. V běžných středoškolských úlohách často není třeba v indukčním kroku využít toho, že je úloha dokázaná pro všechna čísla menší než n. Stačí pouze vědět, že tvrzení platí pro $n-1$. Taková indukce se nazývá *slabá indukce* a v úvodních povídáních o indukci bývá vydávaná za tu pravou indukci. My naopak budeme za tu pravou indukci považovat indukci, která může využívat platnost pro kterékoli předchozí hodnoty; ta se jinak nazývá *silná indukce*. Další rozdíl silné a slabé indukce spočívá v tom, že v silné indukci může být první krok považován za součást indukčního kroku, indukční předpoklad je totiž pro $n = 0$ automaticky splněn.[6] V příkladu jsme vyřešili první krok zvlášť jen proto, že pro $n = 0$ bychom nenašli nenulové $F_i \leq n$ a $n - F_n$ by tak nebylo ostře menší než n.

Intuitivně je tedy indukce „postupné dokazování“ a rekurze je „postupné definování“. Na konci předchozí kapitoly jsme rekurzivně definovali velkou množinu B. Jenže tato rekurze se nezastavila na přirozených číslech, ve skutečnosti šlo o rekurzi po zhruba takovýchto krocích:



Motivační obrázek

Podobným způsobem lze rozšířit i rekurzi a takto rozšířená indukce resp. rekurze se běžně nazývá *transfinitní indukce* resp. *transfinitní rekurze.* Na druhou stranu ne na každé množině můžeme dokazovat indukcí. Představme si například nezáporná reálná čísla a zkusme dokázat, že každé nezáporné číslo je přirozené. První krok: Nula je přirozené číslo. Indukční krok: Uvažme kladné reálné číslo x. Číslo $x/2$ je menší než x, takže jsme o něm již dokázali, že je přirozené. Proto je přirozený i jeho dvojnásobek, tedy x. Dokázali jsme, že každé reálné číslo je přirozené, no ne? :-) No, dobrá, je to podvod. Na reálných číslech indukce nefunguje.

Naším cílem bude pochopit, jak se poznají **množiny, na kterých indukce a rekurze funguje**. K tomu je třeba ještě trochu jiný pohled na tyto pojmy.

Začneme s indukcí, která je (možná překvapivě) jednodušší. Proč tedy indukce funguje? **Indukce je jen speciální případ důkazu sporem.** Princip je následující: Pro spor předpokládáme, že dokazované tvrzení neplatí pro některé přirozené číslo, a zvolíme n nejmenší takové, pro které tvrzení neplatí. Pak tvrzení platí pro všechna $k < n$, a je tak splněn indukční předpoklad. Jenže potom z indukčního kroku plyne, že tvrzení platí i pro n, což je spor a důkaz je hotov.

Ukážeme to stručně na příkladu s rozkladem na Fibonacciho čísla. Předpokládejme, že existuje přirozené číslo, které nelze rozložit na Fibonacciho čísla. Zvolme nejmenší takové n. Nulu zapsat jako součet lze, takže $n > 0$. Dále najdeme $F_i \leq n$ s největším možným i. Potom je $n - F_i$ menší než n, takže $n - F_i$ lze rozložit na součet Fibonacciho čísel dle zadání. Jenže pak přidáním F_i k tomuto rozkladu dostáváme rozklad čísla n. Dostali jsme spor s tím, že n nelze rozložit.

V celé úvaze jsme využili jedinou (klíčovou) vlastnost přirozených čísel: Mohli jsme nalézt nejmenší n, pro které tvrzení neplatilo. To nás vede k následující definici.

Definice. Mějme množinu D, na které máme definováno, kdy pro dvojici prvků a, b z množiny D platí $a < b$ (ekvivalentně $b > a$). Řekneme, že D je *dobře uspořádaná*[7], pokud platí následující

[6] Žádné přirozené číslo menší než $n = 0$ neexistuje a výroky, kde kvantifikace probíhá prázdnou množinu (například „Všichni opravdoví vodníci jsou růžoví.“) jsou v matematické logice považovány za pravdivé.

[7] Jakkoli se pojem „dobře uspořádaný“ může zdát podobně provizorním jako pojmy „zajímavý“ či „pěkný“, které se občas objeví v zadání či v řešení některé z úloh, pojem „dobře uspořádaný“ (anglicky *well ordered*) je skutečně oficiální termín používaný v teorii množin.

tři podmínky:

(i) Jakmile $a < b$ a $b < c$, tak nutně $a < c$. (tranzitivita)

(ii) Pro libovolné dva prvky a, b platí právě jedna z následujících tří možností: $a < b$, $a = b$, $a > b$. (linearita)

(iii) V každé neprázdné podmnožině X množiny D existuje nejmenší prvek, tedy a takové, že pro všechny ostatní prvky b z množiny X je $a < b$. (dobré uspořádání)

Pokud D splňuje pouze první dvě podmínky, říkáme, že je *lineárně uspořádaná*. Pojem dobře uspořádané množiny budeme zkracovat jako *DUM*.

V klasické indukci se často případ dělí na první krok a indukční krok, protože má prvek 0 poněkud odlišné vlastnosti od ostatních. V obecné DUMě máme dokonce tři typy prvků.

Definice. Mějme DUMu a její prvek x. Prvek x nazýváme

(i) *nulový*, pokud je to nejmenší prvek této DUMy;

(ii) *izolovaný*, pokud existuje jeho bezprostřední předchůdce, tedy největší prvek menší než x;

(iii) *limitní*, pokud nenastane ani jedna z předchozích situací.

Příklad.

(i) Množina reálných čísel je lineárně uspořádaná, ale není DUM, protože nemá nejmenší prvek.

(ii) Množina nezáporných reálných čísel je lineárně uspořádaná a má nejmenší prvek, ale není DUM, protože množina kladných reálných čísel nemá nejmenší prvek.

(iii) Každá konečná lineárně uspořádaná množina je dobře uspořádaná.

(iv) Množina přirozených čísel je dobře uspořádaná.

(v) DUMu D vyobrazenou na motivačním obrázku můžeme sestrojit následovně. Za množinu D zvolíme $\omega \times \omega$. Prvky $(0, 0)$ a $(0, 1)$ označíme jako *velké*, ostatní označíme jako *malé*. Uspořádání definujeme tak, že velké prvky jsou vždy větší než malé. Pokud jsou oba prvky malé nebo oba velké, porovnáme je lexikograficky[8], tedy $(a, b) < (c, d)$, pokud $a < c$ nebo platí současně $a = c$ a $b < d$.

Cvičení 4. Rozděl prvky DUMy z předchozího příkladu (v) na nulový, limitní a izolované.

Cvičení 5. Ukaž, že následující podmnožiny reálných čísel (s obvyklým uspořádáním) **nejsou** dobře uspořádané.

(i) Množina celých čísel,

(ii) množina nezáporných racionálních čísel,

(iii) uzavřený interval $\langle 10, 20 \rangle$,

(iv) Cantorova množina, tedy množina těch čísel z intervalu $\langle 0, 1 \rangle$, která ve svém zápisu v trojkové soustavě obsahují jen nuly a dvojky (případně jednu jedničku na konci, protože ta je nahraditelná nulou následovanou samými dvojkami).

Cvičení. Rozmysli si, že když k DUMě přidáme prvek ∞ větší než všechny ostatní prvky, bude se stále jednat o DUMu.[9]

Cvičení 6. Rozmysli si, že lineárně uspořádaná množina je DUMou právě tehdy, když v ní není možné najít nekonečnou ostře klesající posloupnost.

---

[8] Porovnávat lexikograficky znamená „jako ve slovníku“.

[9] Značka ∞ v seriálu nic konkrétního neznamená. Jde jen o pojmenování toho prvku a naznačuje, že je tento prvek nad ostatními.

Dobře uspořádanou množinu jsme definovali právě tak, aby na ní šlo provádět indukci. Dále ukážeme, že na DUMách funguje i rekurze. K tomu je třeba pochopit, co je to vlastně rekurze a co je to samotný rekurzivní předpis. Stejně jako silná indukce nemusí rekurze využívat jen předchozí dvě hodnoty, ale může vzít v úvahu všechny předešlé.

Definice. Uvažme DUMu D a její prvek x. Pak symbolem $D \leftarrow x$ značíme množinu všech prvků D ostře menších než x. *Rekurzivní předpis* na množině D je zobrazení, které pro každý prvek x množiny D a každou funkci definovanou na množině $D \leftarrow x$ přiřadí další hodnotu (pro bod x).

O funkci f říkáme, že *splňuje* rekurzivní předpis p, pokud pro všechny prvky x množiny D splňuje

$$f(x) = p(f \restriction (D \leftarrow x)).$$

Slovy řečeno, uvažme zúžení funkce f jen na množinu $D \leftarrow x$. Pokud tuto zúženou funkci zobrazíme rekurzivním předpisem, musíme dostat $f(x)$.

Příklad. (Fibonacciho čísla) Definujeme rekurzivní předpis na ω následovně: Uvažme přirozené číslo x a funkci $f\colon (\omega \leftarrow x) \to \omega$. Pokud je $x \leq 1$, ignoruje rekurzivní předpis funkci f a vrátí samotné x (počáteční podmínka). V opačném případě rekurzivní předpis vrátí hodnotu $f(x-2) + f(x-1)$.

Opět obecná definice rekurzivního předpisu a funkce dané rekurzivním předpisem nedává příliš jasnou odpověď na otázky: Musí funkce splňující rekurzivní předpis vždy existovat? A je vůbec dána jednoznačně? Odpověď na obě tyto otázky je kladná, ale je třeba to dokázat:

Nejprve dokážeme jednoznačnost – (transfinitní) indukcí. V indukčním kroku stačí ukázat, že jakmile se dvě funkce dané rekurzivním předpisem shodují na množině $D \leftarrow x$, tak se shodují i v bodě x. To je ovšem jasné, protože v takovém okamžiku je hodnota v bodě x rekurzivním předpisem jednoznačně určena.

Zbývá ukázat, že taková funkce opravdu existuje. Sestrojíme DUMu D' tak, že k DUMě D přidáme jeden další bod ∞ větší než všechny původní. Stačí ukázat, že existuje funkce definovaná na $D' \leftarrow \infty$ splňující rekurzivní předpis. Opět indukcí dokážeme, že pro každé x z množiny D' existuje funkce definovaná na $D' \leftarrow x$ splňující rekurzivní předpis. Mohou nastat tři možnosti:

(i) Prvek x je nulový. V takovém případě je vyhovující f na $D' \leftarrow x$ prázdná funkce definovaná na prázdné množině.

(ii) Prvek x je izolovaný a má bezprostředního předchůdce y. V takovém případě z indukčního předpokladu existuje funkce definovaná na $D' \leftarrow y$ splňující rekurzivní předpis. Pomocí rekurzivního předpisu tuto funkci můžeme dodefinovat v bodě y a získáváme funkci definovanou na množině $D' \leftarrow x$ splňující rekurzivní předpis.

(iii) Prvek x je limitní. V takovém případě existují funkce definované na $D' \leftarrow y$ pro všechna $y < x$. Navíc pro každý prvek $z < x$ najdeme y ležící ostře mezi z a x. Funkce definovaná na $D' \leftarrow y$ tak bude definovaná v z. Už jsme si dokázali jednoznačnost funkce splňující rekurzivní předpis a tato jednoznačnost platí i na množinách $D' \leftarrow y$. Pro každé y je tak tato funkce jednoznačná a její hodnota v bodě z nezávisí na volbě y. Takto najdeme hodnotu pro každé z z množiny $D' \leftarrow x$ a výsledná funkce bude splňovat rekurzivní předpis, protože jej splňují jednotlivá zúžení na $D' \leftarrow y$.

Příklad. Motivační obrázek v úvodu této kapitoly znázorňoval, jak může vypadat rekurze, která se nezastaví na přirozených číslech. Množinu, na které se tato rekurze odehrává, jsme již popsali v bodě (v) příkladu na stránce 11. Nyní popíšeme rekurzivní předpis: Uvažme prvek x množiny D a funkci f definovanou na množině $D \leftarrow x$. Rozebereme tři případy.

(i) Pokud je x nulový prvek, rekurzivní předpis vrátí množinu ω.
(ii) Pokud je x izolovaný prvek, má bezprostředního předchůdce y. Rekurzivní předpis vrátí množinu $\mathcal{P}(f(y))$.
(iii) Pokud je x limitní prvek, vrátí rekurzivní předpis sjednocení všech hodnot funkce f.

Operace na DUMách

Předpis z předchozího příkladu je možné použít zcela obecně, takže se hledání množiny s co největší mohutností přetavilo v hledání co „nejdelší“ dobře uspořádané množiny. K tomu bychom si ale měli ujasnit, jak délku dobře uspořádaných množin porovnávat.

Definice. Řekneme, že dvě DUMy A, B jsou *stejného typu* (značíme $A \simeq B$), pokud mezi nimi existuje rostoucí bijekce $f\colon A \to B$.

Povšimněme si, že porovnávání typů je jemnější než porovnávávání velikostí. Pokud je $A \simeq B$, tak už nutně $|A| = |B|$, ale obráceně to neplatí. Jak vyplyne z následujícího tvrzení, kdykoli k nekonečné spočetné DUMě přidáme nový prvek větší než všechny ostatní, bude mít výsledná DUM jiný typ. Na druhou stranu bude mít stále stejnou mohutnost jako ω.

Tvrzení. *Nechť A, B jsou dvě libovolné DUMy. Pak nastane právě jedna z následujících možností:*

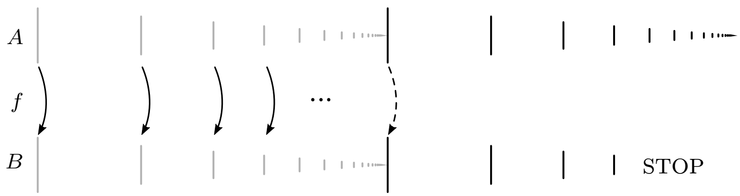
(i) $A \simeq B$.

(ii) $A \simeq (B \leftarrow x)$ *pro nějaký prvek x z B.*

(iii) $(A \leftarrow x) \simeq B$ *pro nějaký prvek x z A.*

Pokud nastane možnost (ii) nebo (iii), je dokonce prvek x jednoznačně určen a ve všech třech případech je jednoznačně určena příslušná rostoucí bijekce. Pokud je navíc A jen podmnožinou DUMy B, určitě nenastane možnost (iii).

Důkaz. Rekurzivně sestrojíme zobrazení f, které každému prvku množiny A přiřadí prvek množiny B nebo značku STOP. Rekurzivní předpis je následující: Funkci f už máme definovanou na množině $A \leftarrow x$. Pokud tato funkce na každý prvek množiny B již něco zobrazila, přiřadíme prvku x značku STOP. V opačném případě přiřadíme x ten nejmenší prvek B, na který se dosud nic nezobrazilo.



Znázornění konstrukce f

Z konstrukce se žádným dvěma prvkům A nepřiřadí stejný prvek B a mimo prvky zobrazené na STOP je f rostoucí.

Mohou nastat tři možnosti:

(i) Žádnému prvku nebylo přiřazeno STOP a $f\colon A \to B$ je rostoucí bijekce $A \to B$, tedy $A \simeq B$.

(ii) Žádnému prvku nebylo přiřazeno STOP a f není bijekce. Můžeme zvolit nejmenší prvek x množiny B, na který se nic nezobrazilo. V takovém případě se na základě konstrukce f nic nemohlo zobrazit na žádný prvek větší než x, zatímco všechny prvky menší než x jsou z definice prvku x funkcí f pokryty. Proto je f hledaná rostoucí bijekce mezi A a $B \leftarrow x$.

(iii) Některému prvku bylo přiřazeno STOP. Vezměme nejmenší takový prvek x. Pak zúžení $f \upharpoonright x$ je hledaná rostoucí bijekce mezi $A \leftarrow x$ a B.

Už jsme dokázali, že nastane jedna alespoň jedna z uvedených situací, a zkonstruovali jednu konkrétní bijekci. Existuje ale i opačný proces, který z informace, která varianta (i)–(iii) nastala, prvku x a rostoucí bijekce rekonstruuje funkci f splňující popsaný rekurzivní předpis: V případech (i) resp. (ii) stačí použít coby funkci f samotnou rostoucí bijekci $A \to B$ resp. $A \to (B \leftarrow x)$.

V případě (iii) stejně, jen je třeba dodefinovat rostoucí bijekci $(A \leftarrow x) \to B$ na prvcích $y \geq x$ předpisem $f(y) = \mathrm{STOP}$.

Proto jsou varianta (i)–(iii), prvek x a rostoucí bijekce určeny jednoznačně funkcí f splňující rekurzivní předpis. I tato funkce je však určena jednoznačně z vlastností rekurze, takže máme dokázanou jednoznačnost.

Pro poslední doplňující fakt, že v případě, kdy A je podmnožinou B, nenastane možnost (iii), si stačí uvědomit, že v takovém případě pro každý prvek a množiny A platí $f(a) \leq a$.

Definice. Pokud platí $A \simeq (B \leftarrow x)$ pro nějaký prvek x z B, říkáme, že B má *větší typ* než A (značíme $A < B$).

Cvičení 7.

(i) Uvědom si, že předchozí věta říká, že pro dvě DUMy A, B nastane právě jedna z možností $A < B$, $A \simeq B$, $A > B$.

(ii) Ukaž, že když DUMy A, B_0, B_1, C splňují $A < B_0 < C$ a $B_0 \simeq B_1$, tak $A < B_1 < C$.

(iii) Ukaž, že když DUMy A, B, C splňují $A < B$ a $B < C$, tak $A < C$.

(iv) Nechť X je množina nekonečně mnoha DUM. Dokaž, že v množině X lze nalézt takovou DUMu A, že pro každou jinou DUMu B z množiny X platí $A < B$ nebo $A \simeq B$.

Cvičení 8. Najdi DUMu B a její vlastní[10] podmnožinu A, aby stále platilo $A \simeq B$.

Nyní umíme porovnávat jednotlivé DUMy. Ještě si ukážeme dvě základní operace, jak vytvářet nové DUMy s větším typem. Základní DUM, ze které můžeme stavět, je ω. Dále přirozené číslo n na místě DUMy budeme považovat za n-prvkovou DUMu.

Definice. Pro dvě DUMy A a B definujeme

(i) DUMu $A + B$ coby množinu všech uspořádaných dvojic tvaru $(a, 0)$ nebo $(b, 1)$, kde a je z A a b je z B;

(ii) DUMu $A \cdot B$ coby kartézský součin $A \times B$.

V obou případech definujeme porovnávání dvojic následovně: Pokud se dvojice liší na druhém místě, rozhodne o tom, která dvojice je větší, druhé místo (pro sčítání DUM uvažujeme $0 < 1$). V případě shody na druhé pozici rozhodne první.

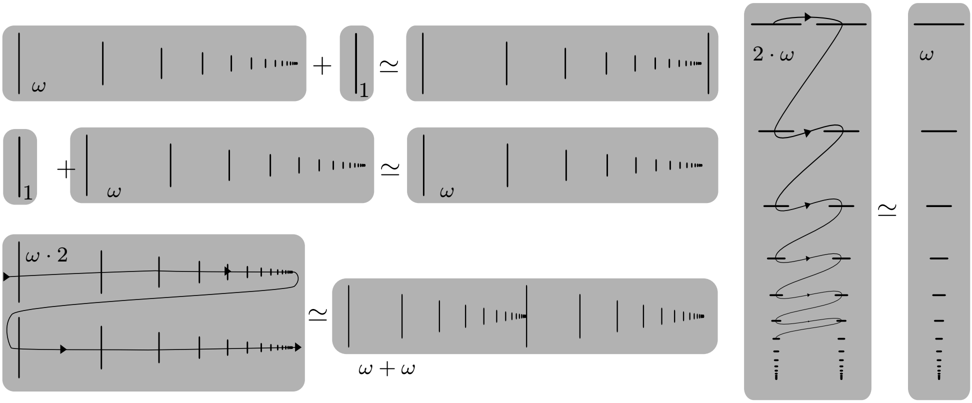
Ukážeme, že takto definované uspořádání je dobré – uvažme nějakou neprázdnou množinu dvojic a označme ji X. Množina všech možných druhých souřadnic je podmnožina DUMy, takže najdeme nejmenší druhou souřadnici y. Nyní se omezíme jen na ty dvojice z množiny X, jejichž druhá souřadnice je y. První souřadnice opět probíhá DUMu, takže najdeme nejmenší z nich, x. Dvojice (x, y) je nejmenší prvek množiny X.

Sčítání DUM odpovídá skládání DUM za sebe. Násobení $A \cdot B$ lze ilustrovat tak, že kartézský součin $A \times B$ (v každém řádku je A, v každém sloupci B) přečteme po řádcích. Odpovídá to tomu, když v B nahradíme každý jednotlivý prvek kopií DUMy A.

Příklad. DUMu z motivačního obrázku můžeme sestrojit jako $\omega \cdot \omega + 2$.

Příklad. Na rozdíl od sčítání a násobení reálných čísel zde záleží na pořadí. Například $\omega + 1$ odpovídá přidání nového největšího prvku do ω a je tak $\omega + 1 > \omega$, dále $\omega \cdot 2 \simeq \omega + \omega > \omega$. Na druhou stranu $1 + \omega \simeq \omega$ a taky $2 \cdot \omega \simeq \omega$. Operace jsou znázorněny na obrázku.

[10] Vlastní podmnožina množiny A je taková, která není rovna A. Jedná se tedy o ekvivalent pojmu ostře menší prvek v uspořádání.



Cvičení 9. Předchozí příklad ukazuje, že výsledek součtu či součinu může vyjít jako druhý sčítanec resp. činitel. Ukaž, že u prvního sčítance resp. činitele se toto až na degenerované případy nestane, tedy konkrétně pro DUMy A, B platí

(i) $A < A + B$, pokud je B neprázdná;

(ii) $A < A \cdot B$, pokud je B alespoň dvouprvková.

A to je z teorie prvního dílu vše. Zbývá se pustit do řešení úloh. Nevěš hlavu, jestli se Ti prozatím nepovedlo pochopit těžší důkazy s transfinitní rekurzí – ty jsou v seriálu uvedeny spíše pro úplnost a úlohy lze řešit i bez nich. Ale pokud Tě naopak zklamalo, že seriál šel sice do nekonečna, ale zatím málo „dál“, pak právě pro Tebe je tu závěrečná kapitola.

Čokoládová výzva

Čokoládová výzva je soutěž, jejíž výherce dostane čokoládu.[11] V každém díle seriálu bude jedna čokoládová výzva, tedy dohromady se bude soutěžit o tři čokolády. V příštích dvou dílech se bude jednat o co nejrychlejší vyřešení nějaké úlohy a poslání řešení e-mailem, takže doporučujeme se na další díly seriálu podívat co nejdříve.

První výzva je o poznání kreativnější.

Úloha. Sestroj **spočetnou** DUMu s co největším typem.

Ten, jehož DUM bude největší, vyhraje čokoládu. Při vzácné shodě (ale ta snad nenastane, stačilo by přeci přičíst jedničku) čokoládu rozdělíme. Konstrukce musí být formálně jasná, ale není například potřeba dokazovat, že se jedná o DUMu (pokud to bude pravda). Svou konstrukci pošli společně se seriálovou sérií (posíláš-li poštou), případně pro ni najdeš příslušnou kolonku v submitovátku.

A v příštím díle si předvedeme nespočetnou DUMu. ;-)

[11] Ale nejde o soutěžní úlohu, takže za ni nelze získat žádné body.

Seznam symbolů a pojmů

Na této stránce jsou stručně uvedeny všechny důležité pojmy prvního dílu seriálu. U každého pojmu je uvedeno, na které stránce byl definován.

str 1. ω neboli množina všech přirozených čísel (včetně nuly).
str 6. *Zobrazení* neboli *funkce* $f\colon A \to B$.
str 6. $\mathbb{R}$ neboli množina všech reálných čísel.
str 6. *Definiční obor*, *obraz bodu*.
str 6. *Prostá* funkce, *bijekce*, *rostoucí* funkce.
str 6. $f \restriction A$ neboli zúžení funkce f na množinu A.
str 6. $|A| = |B|$ neboli množina A má *stejnou mohutnost* jako B.
str 6. $|A| \leq |B|$ neboli množina A má *mohutnost menší nebo rovnu* mohutnosti B.
str 6. $|A| < |B|$ neboli množina A má *menší mohutnost* než B.
str 6. *Spočetná* množina, *nespočetná* množina.
str 6. *Kartézský součin* $A \times B$.
str 6. $\mathcal{P}(X)$ neboli *potence* množiny X.
str 7. $\mathbb{Q}$ neboli množina všech racionálních čísel.
str 11. *DUM* neboli *dobře uspořádaná* množina.
str 11. *Nulový*, *izolovaný*, *limitní* prvek v DUMě.
str 12. $D \leftarrow x$
str 12. *Rekurzivní předpis*, funkce *splňující* rekurzivní předpis.
str 13. $A \simeq B$ neboli DUMy A, B jsou *stejného typu*.
str 14. $A < B$ neboli DUM B má *větší typ* než A.
str 14. *Součet* DUM $A + B$.
str 14. *Součin* DUM $A \cdot B$.

Návody

1. Očísluj čtverečky a vezmi množinu šedých čtverečků.

2. (ii) Představ si místo každého přirozeného čísla jeho binární zápis (včetně nekonečné posloupnosti nul na začátku). (iii) Vezmi jakoukoli spočetnou množinu, která je pokrytá, a proveď postup obrácený k tomu, když se do Hilbertova hotelu nacpal autobus.

3. Bílá políčka oddělují jednotlivé členy posloupnosti, délka souvislých šedých úseků udává velikost čísla. S případem, kdy je bílých čtverečků jen konečně mnoho, se vypořádej stejně jako v předchozím cvičení.

4. $(0, 2)$ nulový, $(n, 0)$ limitní pro všechna n, ostatní izolované.

5. (i) Nemá minimum, (ii), (iv) po odstranění nuly nemá minimum, (iii) otevřený interval $(10, 20)$ nemá minimum.

6. Když existuje posloupnost, tvoří množinu bez minima. Při důkazu opačného směru máme neprázdnou množinu bez minima. Z ní vezmeme libovolný prvek x_0, to není minimum, najdeme $x_1 < x_0$, dále $x_2 < x_1$ atd.

7. (iv) Vezmi libovolnou DUMu D z množiny X, porovnej ji se všemi ostatními a využij toho, že D je dobře uspořádaná.

8. Prohlédni si pozorně část o sčítání a násobení DUM.

9. Sestroj rostoucí bijekci mezi A a začátkem $A + B$ resp $A \cdot B$. Věta o porovnávání pak už říká vše potřebné.

Do nekonečna a ještě dál

Na počátku bylo slovo, a to slovo bylo od Matematika, a to slovo bylo „množina“.

Díl druhý – pevné základy

V tomto díle si ukážeme, jak se matematika asi před sto dvaceti lety rozbila, a především to, jak ji následně opravili. Nenavážeme tedy na první díl hned, ale až zhruba v polovině seriálu.

Možná totiž v prvním díle nebylo jasné, proč při snaze sestrojit obrovské množiny používáme tak rafinované konstrukce namísto toho, abychom prostě úplně všechny množiny naházeli do jednoho pytle. To už bude určitě největší množina. Nic většího nevyrobíme. Jenže v tom je právě ta potíž, vždyť jsme si ukázali, že vždycky můžeme sestrojit větší množinu pomocí potence. Jak to? Když si vzpomeneme na důvod, proč je potence větší než původní množina, dostáváme Russelův paradox:

Russel: „Existuje množina všech množin?“

Intuice: „Ovšem že ano. Proč by měla neexistovat?“

Russel: „A obsahuje tato množina sama sebe?“

Intuice: „Jasně, obsahuje přece všechny množiny.“

Russel: „A existuje množina všech množin, které neobsahují samy sebe?“

Intuice: „Jasně, stačí z množiny všech množin vyhodit ty prvky, které samy sebe obsahují.“

Russel: „A obsahuje tato množina sama sebe?“

Intuice: „Jejda.“

Problém spočívá v tom, že z definice množiny všech množin neobsahujících samu sebe vyplývá, že tato množina se obsahuje právě tehdy, když se neobsahuje. Obě varianty vedou ke sporu.

Matematika ale nesmí vést sama o sobě ke sporu. Když jsme dostali spor, znamená to, že jsme ji špatně vybudovali. Po objevu Russelova paradoxu matematici bádali nad tím, jak zařídit, aby fungovala veškerá dosud vybudovaná matematika, ale již nikoli Russelův paradox.

S řešením přišli pánové Zermelo a Fraenkel. Sestavili pro matematiku sadu axiomů – to jsou tvrzení, která se bez důkazu považují za pravdivá, jedná se tedy o základní kameny matematiky. Podle těchto axiomů není množinou jen tak ledaco, axiomy dávají pro tvorbu množin striktní pravidla. Nemůžeme si tedy jen tak vzít množinu všech množin. Naopak Russelův paradox sporem dokazuje, že žádná množina všech množin ve skutečnosti neexistuje.

Jazyk teorie množin

Napřed si představíme formální jazyk, ve kterém jsou axiomy psané. Jedná se o jazyk hovořící o množinách, žádné jiné matematické objekty v něm zastoupeny nejsou. Možná si říkáš: „No moment, a co prvky těch množin? O těch se mluvit nedá? Co přirozená čísla? Co body v rovině? Co posloupnosti? Co funkce?“ Inu, vše tohle budou zase množiny.[1] Časem si definujeme, která množina

[1] Se situací, kdy prvky množiny byly opět množiny, ses v minulém díle setkal(a) například u potence $\mathcal{P}(X)$ – prvky potence jsou podmnožiny X, tedy množiny.

je přirozeným číslem, která bodem v rovině, a tak podobně. V základním jazyku teorie množin si však vystačíme s následujícími symboly.

(i) Závorky a klasické logické spojky[2]: $\neg$ (není pravda, že), $\wedge$ (a zároveň), $\vee$ (nebo), $\Rightarrow$ (implikuje), $\Leftrightarrow$ (právě tehdy, když).
(ii) Proměnné – písmenka, která zastupují nějakou množinu.
(iii) Kvantifikátory: Symbol $(\forall x)$ (pro všechna x) znamená, že následující výrok platí, ať za x dosadíme kteroukoli množinu, a symbol $(\exists x)$ (existuje x) znamená, že je možné v následujícím výroku dosadit za x nějakou množinu tak, aby byl splněn.
(iv) Rovnítko $x = y$ značí, že x a y jsou tytéž množiny.
(v) Náležítko $x \in y$ značí, že množina x je prvkem množiny y. **Pozor!** Prvek množiny a podmnožina množiny jsou zásadně odlišné pojmy. Prvky množiny často nebývají jejími podmnožinami. Je rozdíl mezi množinou x a jednoprvkovou množinou obsahující x jako prvek.

Z koncepce tohoto jazyka je patrné, proč se o množinách říká, že „Prvky množiny jsou neuspořádané a nemohou se opakovat“. Samotný jazyk totiž neumožňuje zjistit, v jakém pořadí prvky v množině jsou a kolikrát. Jediné, na co se lze ptát, je, zda $x \in y$, či nikoli.

Pomocí těchto symbolů pak lze skládat takzvané *formule* – to je něco jako výroky. Formule jsou takové nápisy, které jdou smysluplně přečíst. Formulí je třeba $(x = y) \wedge (\exists z)(z \in x)$, což se přečte jako „$x$ je stejná množina jako y a zároveň existuje z, které je prvkem množiny x.“ Zato například $\exists\neg) {=}{\in}\, x$ formulí není, protože je to zkrátka blbost. Exaktně můžeme formuli definovat jako to, co vznikne opakovaným použitím následujících pravidel:

(i) Formulemi jsou $x \in y$ a $x = y$ (případně s jinými proměnnými).
(ii) Nechť φ je formule.[3] Pak přidáním kvantifikace na začátek vznikne opět formule. Tedy $(\forall x)(\varphi)$ a $(\exists x)(\varphi)$ jsou formule.
(iii) Aplikováním logických spojek na formule opět vzniknou formule. Tedy z formulí φ, ψ vzniknou například formule $\neg(\varphi)$ nebo $(\varphi) \Rightarrow (\psi)$.

Pokud nedojde k nejednoznačnosti, lze závorky v zápisu vynechat. Ke kvantifikátoru v takovém případě náleží jen to, co po něm bezprostředně následuje: $(\exists x)(\varphi) \wedge (\psi)$ znamená $\big((\exists x)(\varphi)\big) \wedge (\psi)$.

Příklad. Ukážeme konstrukci formule $(x = y) \Rightarrow (\forall z)(x \in z \Leftrightarrow y \in z)$. Z bodu (i) jsou formulemi formální nápisy $x = y$, $x \in z$ a $y \in z$. Aplikováním bodu (iii) získáme formuli $x \in z \Leftrightarrow y \in z$. Dále z bodu (ii) je formulí $(\forall z)(x \in z \Leftrightarrow y \in z)$ a nakonec opět z bodu (iii) dostaneme formuli

$$x = y \Rightarrow (\forall z)(x \in z \Leftrightarrow y \in z).$$

Ještě přeložme tuto formuli do češtiny: „Pokud jsou x a y stejné objekty $(x = y)$, tak pro libovolnou množinu z platí, že x je prvkem množiny z právě tehdy, když y je prvkem množiny z.“ Říká tedy jen to, že když jsou x, y stejné prvky, tak leží ve stejných množinách. To platí v každém případě, čili tato formule platí obecně, pro libovolnou volbu[4] x, y. Zato formule, které jsme vytvořili cestou (například $x \in z$) nejsou obecně pravdivé.

Příklad. Chceme napsat formuli „Množina x je jednoprvková.“ Formule se může opírat pouze o to, které prvky leží v této množině, tedy „Existuje jeden prvek y množiny x takový, že každý prvek z množiny x musí být roven onomu jednomu prvku y.“ To lze říci ještě formálněji: „Existuje y takové, že y je prvkem x a zároveň pro každé z platí, že pokud je z prvkem x, tak je z rovno y.“ Toto již lze přímočaře přepsat do řeči symbolů:

$$(\exists y)(y \in x \wedge (\forall z)(z \in x \Rightarrow z = y)).$$

[2] Logické spojky jsou popsány například na `http://www.matematika.cz/vyroky`.

[3] Řecké písmenko φ označující nějakou formuli se čte „fí“. Dále budeme pro formule používat písmenko „psí“ ψ.

[4] Pokud zvolíme x, y různé, tak vyjde formule pravdivá z toho důvodu, že není splněn předpoklad implikace.

O něco stručnější způsob zápisu by mohl být: „Existuje objekt y takový, že pro každý objekt z je z prvkem x právě tehdy, když je z roven y.“ Formule vypadá takto:

$$(\exists y)\big(\forall z)(z \in x \Leftrightarrow z = y\big).$$

Cvičení 1. Napiš formuli, která říká: „Množina x' obsahuje stejné prvky jako x a ještě jeden navíc.“

Abychom nemuseli všude psát samá náležitka, zavedeme ještě běžně používané zkratky.

(i) $x \notin y$ resp. $x \neq y$ znamená $\neg(x \in y)$ resp. $\neg(x = y)$.
(ii) $x \subset y$ (x je podmnožinou množiny y) znamená $(\forall z)(z \in x \Rightarrow z \in y)$.
(iii) Pokud za $\forall x$ okamžitě následuje požadavek na x, například $(\forall x \in y)(\ldots)$, jedná se o zkratku za to, že příslušný požadavek je předpokladem implikace, tedy $(\forall x)\big((x \in y) \Rightarrow (\ldots)\big)$.
(iv) Pokud za $\exists x$ okamžitě následuje požadavek na x, například $(\exists x \subset y)(\ldots)$, jedná se o zkratku za to, že příslušný požadavek je současně vyžadován, tedy $(\exists x)\big((x \subset y) \wedge (\ldots)\big)$.
(v) Zápis $(\forall x, y, z)$ je jen zkratka za sled kvantifikátorů $(\forall x)(\forall y)(\forall z)$, obdobně pro existenční kvantifikátor.
(vi) Zápis $y = \{x : \varphi(x)\}$ (*množina daná předpisem*), kde $\varphi(x)$ je formule,[5] značí, že y je množina těch prvků x, které splňují formuli φ. Jedná se tedy o formuli $(\forall x)(x \in y \Leftrightarrow \varphi(x))$.

Pozastavíme se u posledního bodu. Ten dává návod, jak interpretovat $y = \{x : \varphi(x)\}$, ale již neříká, jak do základního jazyka přeložit samotnou množinu danou předpisem, tedy samotné $\{x : \varphi(x)\}$. Pokud se ve formuli vyskytne taková množina, přeložíme ji do jazyka teorie množin tak, že založíme novou proměnnou y, která se ve formuli dosud nevyskytuje. Tou nahradíme (jeden) výskyt $\{x : \varphi(x)\}$ a před vzorec s tímto výskytem připíšeme $(\exists y = \{x : \varphi(x)\})$.

Příklad. Přepíšeme do základního jazyka formuli

$$\{x : x \in A \wedge x \in B\} = \{x : x \in C \wedge x \in D\}.$$

Nejprve nahradíme první výskyt do tvaru

$$(\exists y = \{x : x \in A \wedge x \in B\})(y = \{x : x \in C \wedge x \in D\})$$

neboli

$$(\exists y)\big((y = \{x : x \in A \wedge x \in B\}) \wedge (y = \{x : x \in C \wedge x \in D\})\big).$$

Nyní již můžeme nahradit výrazy podle bodu (vi):

$$(\exists y)\Big((\forall x)\big(x \in y \Leftrightarrow (x \in A \wedge x \in B)\big) \wedge (\forall x)\big(x \in y \Leftrightarrow (x \in C \wedge x \in D)\big)\Big).$$

Poznámka. Skutečnost, že můžeme množinu danou předpisem napsat, ještě nezaručuje její existenci a jednoznačnost. Jednoznačnost vyplyne z axiomu extensionality, existence v některých případech nebude možná vůbec (jak ukazuje Russelův paradox). Pokud si tedy například formálně rozepíšeme tvrzení $a \in \{x : x = x\}$, zjistíme, že jsme dostali nepravdivou formuli (kde nepravdivost vyplývá z neexistence množiny všech množin, která vyplyne až z axiomu vydělení).

Za často používané typy množin daných předpisem zavedeme další zkratky. V těchto případech z axiomů vyplyne dokonce existence.

(i) $\{x_0, \ldots, x_n\}$ (*množina zadaná výčtem prvků*) značí $\{z : z = x_0 \vee \cdots \vee z = x_n\}$.
(ii) $x \cap y$ (*průnik x a y*) značí množinu $\{z : z \in x \wedge z \in y\}$.
(iii) $x \setminus y$ (*množinový rozdíl x minus y*) značí množinu $\{z : z \in x \wedge z \notin y\}$.
(iv) $x \cup y$ (*sjednocení x a y*) značí množinu $\{z : z \in x \vee z \in y\}$.
(v) $\mathcal{P}(x)$ (*potence x*) značí množinu $\{y : y \subset x\}$.

[5] To, že se tato formule jmenuje $\varphi(x)$, a ne jen φ, naznačuje, že se x v této formuli nejspíše bude vyskytovat, a že tedy na x závisí její platnost.

Příklad. Formule $a \in \{c, \{d\}\}$ se do základního jazyka přepíše takto:

$$(\exists y_0)(\exists y_1)\Big(a \in y_1 \wedge (\forall z)(z \in y_0 \Leftrightarrow z = d) \wedge (\forall z)\big(z \in y_1 \Leftrightarrow (z = c \vee z = y_0)\big)\Big).$$

Pokud před dvojtečku napíšeme složitější výraz než jednu proměnnou, značíme množinu všech možných hodnot takového výrazu. Například pokud máme zafixované množiny x a y, značí $\{\{a, b\} : a \in x, b \in y\}$ množinu $\{c : (\exists a \in x)(\exists b \in y)(c = \{a, b\})\}$.

Nyní již se takřka můžeme pustit do axiomů, tedy formulí, jejichž platnost se v teorii množin automaticky předpokládá. Poslední věc, kterou je třeba o těchto axiomech pochopit, je, že se nejedná o axiomy logiky. K logice budeme přistupovat intuitivně – například chápeme, že když $x = y$, tak můžeme ve formuli nahradit x za y a nezmění se tím její platnost. Nebo že když platí $\varphi \vee \psi$ a neplatí φ, tak platí ψ. Popsat a vysvětlit axiomy logiky a formální dedukci by bylo na mnohem delší povídání. Axiomy teorie množin jsou od toho, aby jasně definovaly, jak se chová náležítko, a tedy, co přesně můžeme dělat s množinami.

Axiomy

Za každým axiomem je vysvětleno, co říká a k čemu slouží. Ale v principu by tento doprovodný text nemusel být třeba. Jestli si chceš popřemýšlet, zkus nejprve pokaždé pochopit axiom bez něj.

(0) Axiom existence:

$$(\exists x)(\forall y)(y \notin x).$$

Česky řečeno: Existuje množina x taková, že pro žádnou[6] množinu y není y prvkem množiny x. Jinými slovy x nemá žádný prvek. Tuto množinu x budeme nazývat *prázdná* množina a budeme ji značit $\emptyset$.

(1) Axiom extensionality:

$$(\forall z)(z \in x \Leftrightarrow z \in y) \Rightarrow (x = y).$$

Tento axiom říká, že množina není dána ničím jiným než svými prvky. Tedy například prázdná množina, průnik, sjednocení, potence, množina zadaná výčtem prvků či obecná množina zadaná předpisem je (pokud existuje) dána jednoznačně. Opačná implikace – že stejné množiny obsahují stejné prvky – také platí. Ta vyplývá přímo z axiomů logiky, považujeme ji tedy za ještě samozřejmější než axiomy teorie množin.

(2) Axiom dvojice:

$$(\forall x, y)(\exists d)(d = \{x, y\})$$

neboli pro každé dvě zadané množiny existuje množina, která obsahuje právě je. Tento axiom mimo jiné zaručuje i existenci jednoprvkových množin $\{x\}$, protože $\{x\} = \{x, x\}$.

Cvičení 2. Dokaž „opak extensionality“: $(\forall z)(x \in z \Leftrightarrow y \in z) \Rightarrow (x = y)$.

(3) Schéma axiomů vydělení: To, že se jedná o schéma, znamená, že za jistý kus axiomu je možné dosadit skoro jakoukoli formuli a dá se říci, že takto vlastně vyrobíme nekonečně mnoho axiomů. V tomto případě je možné za $\varphi(z)$ dosadit formuli, která v sobě neobsahuje y. Pak je axiomem

$$(\forall x)(\exists y)(\forall z)\big(z \in y \Leftrightarrow (z \in x \wedge \varphi(z))\big).$$

Jinými slovy toto schéma zaručuje existenci množiny y dané předpisem $\{z : z \in x \wedge \varphi(z)\}$. Jedná se o vydělení těch prvků z množiny x, které splňují formuli $\varphi(x)$, výslednou množinu budeme značit i $\{z \in x : \varphi(z)\}$. Použitím axiomu vznikne vždy podmnožina nějaké existující množiny, takže ke konstrukci množiny všech množin tento axiom použít nelze.

[6] V češtině má slovo „žádná“ takřka stejný význam jako slovo „každá“. Sloveso rozhoduje, které z těchto dvou slov se má použít. Divně se zde chová čeština, nikoli formální jazyk.

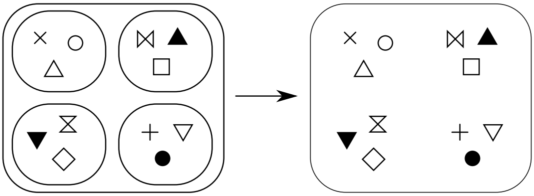
Příklad. Axiom vydělení je možné použít i ke konstrukci průniku $a \cap b$. Za formuli $\varphi(z)$ zvolíme $z \in b$. Dále za x dosadíme a a použijeme axiom. Dostáváme y splňující $(\forall z)\big(z \in y \Leftrightarrow (z \in a \wedge z \in b)\big)$. Tedy $y = a \cap b$.

Cvičení 3. Odvoď pomocí axiomu vydělení existenci množiny $a \setminus b$.

(4) Axiom sjednocení:

$$(\forall x)(\exists s)(\forall z)\big(z \in s \Leftrightarrow (\exists y \in x)(z \in y)\big).$$

Tento axiom říká, že kdykoli máme množinu x, můžeme sjednotit všechny množiny, které v x leží. Toto sjednocení s značíme $\bigcup x$. Použití axiomu dvojice a následně axiomu sjednocení zaručuje existenci sjednocení dvou množin $x \cup y$.



x $\qquad$ $\bigcup x$

Navíc můžeme pokračovat a sestavit pomocí tohoto axiomu libovolně velkou konečnou množinu danou výčtem $\{x_0, x_1, \ldots, x_{n-1}\}$. Existují totiž jednoprvkové množiny $\{x_0\}, \{x_1\}, \ldots, \{x_{n-1}\}$ a postupným aplikováním sjednocení dvou množin z nich dostáváme $\{x_0, x_1\}, \{x_0, x_1, x_2\}, \ldots$, až nakonec získáme $\{x_0, x_1, \ldots, x_{n-1}\}$.

(5) Axiom potence:

$$(\forall x)(\exists y)(y = \mathcal{P}(x)).$$

Cvičení 4. Přepiš axiom potence (tedy tvrzení „existuje potence x") jen pomocí základního jazyka teorie množin.

(6) Schéma axiomů nahrazení: Mějme formuli $\psi(x, y)$, která v sobě neobsahuje b, y_0 ani y_1. Symbolem $\psi(x, y_0)$ resp. $\psi(x, y_1)$ značíme úpravu formule $\psi(x, y)$, ve které nahradíme proměnnou y za proměnnou y_0 resp. y_1. Pak je axiomem

$$(\forall x, y_0, y_1)\big((\psi(x, y_0) \wedge \psi(x, y_1)) \Rightarrow (y_0 = y_1)\big) \Rightarrow (\forall a)(\exists b)(\forall y)\big(y \in b \Leftrightarrow (\exists x \in a)(\psi(x, y))\big).$$

I když je tohle schéma na první pohled opravdu nestravitelné, překvapivě to s ním není až tak hrozné. Nechť f je zobrazení, které množině x přiřadí množinu y, aby platilo $\psi(x, y)$. Celá první závorka je jen podmínka požadující, aby f bylo jednoznačně určené zobrazení, tedy aby bylo k jednomu x přiřazeno jen jedno y. Axiom pak říká, že obrazy prvků množiny a (přesněji té její části, která leží v definičním oboru) v zobrazení f opět tvoří množinu.

Pokud budeme chápat zápis $f(x) = y$ jako formální $\psi(x, y)$ můžeme axiom přepsat do tvaru

$$(\forall x, y_0, y_1)\big(((f(x) = y_0) \wedge (f(x) = y_1)) \Rightarrow (y_0 = y_1)\big) \Rightarrow (\forall a)(\exists b)(b = \{f(x) : x \in a\}).$$

(7) Axiom fundovanosti (nebo též regularity):

$$(\forall x \neq \emptyset)(\exists y \in x)(\forall z \in y)(z \notin x).$$

Tento axiom požaduje, aby každá neprázdná množina obsahovala prvek, který je s ní disjunktní[7]. Není to intuitivní požadavek a my nebudeme tento axiom příliš potřebovat. Smyslem tohoto axiomu je vyloučit existenci divných množin.

[7] Slovo disjunktní znamená neprotínající se, tedy že dané množiny mají prázdný průnik.

Cvičení 5.

(i) Ukaž, že nemůže existovat množina a splňující $a \in a$.
(ii) Ukaž, že nemohou existovat množiny a, b takové, že $(a \in b) \wedge (b \in a)$.

(8) Axiom nekonečna:

$$(\exists m)\big(\emptyset \in m \wedge (\forall x \in m)(x \cup \{x\} \in m)\big).$$

Tento axiom zaručuje existenci nekonečné množiny m jistou konkrétní konstrukcí, ačkoli jednoznačně množina m určená není. Podstata tohoto axiomu spočívá v sestrojení alespoň nějaké uchopitelné nekonečné množiny. Se vzniklou množinou se setkáme při konstrukci množiny všech přirozených čísel.

Cvičení 6. Přepiš axiom nekonečna jen pomocí základního jazyka teorie množin.

(9) Axiom výběru:

$$(\forall a)\big((\forall x \in a, y \in a)(x \neq y \Leftrightarrow x \cap y = \emptyset) \Rightarrow (\exists b)(\forall x \in a)(\exists y)(x \cap b = \{y\})\big).$$

Tento axiom říká, že pokud máme množinu a neprázdných disjunktních množin, tak je možné z každé množiny vybrat po jednom prvku a sestavit z těchto prvků množinu b. Intuitivně tento axiom říká, že je možné provést nekonečně mnoho nahodilých výběrů najednou. Podrobněji se mu budeme věnovat v příštím díle.

Tato (obvykle používaná) sada axiomů trochu překvapivě není minimální – tři axiomy by bylo možné vyškrtnout, aniž bychom o jejich platnost přišli, jak ukazuje následující cvičení.

Cvičení 7.

(i) Uvědom si, že platnost axiomu existence plyne z axiomu nekonečna.
(ii) Odvoď schéma axiomů vydělení ze schématu axiomů nahrazení.
(iii) Odvoď axiom dvojice z axiomů existence, potence a nahrazení.

To, že se uvádějí i nadbytečné axiomy, je dáno historickými a pedagogickými důvody – přeci jen je snazší pochopit axiom dvojice než axiom nahrazení. Dalším důvodem je, že se občas uvažují jiné teorie množin bez axiomu potence či bez axiomu nahrazení, ale těmito verzemi se zabývat nebudeme.

Dvojice a kartézský součin

Nyní si ukážeme, jak pomocí množin vytvořit některé známé struktury, které se od běžných množin liší.

Neuspořádaná dvojice obsahující prvky a a b je množina $\{a, b\}$. Obecně se tedy jedná o dvouprvkovou nebo jednoprvkovou množinu.

Uspořádaná dvojice (a, b) je množina $\{\{a\}, \{a, b\}\}$.

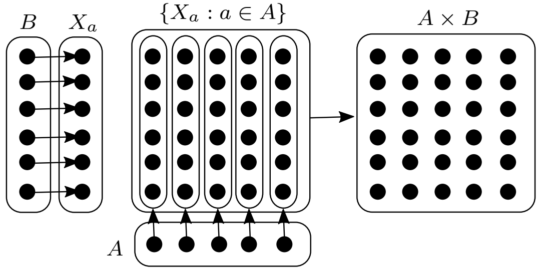
Cvičení 8. Ukaž, že uspořádaná dvojice $(\emptyset, \{\emptyset\})$ je prvkem $\mathcal{P}(\mathcal{P}(\mathcal{P}(\mathcal{P}(\emptyset))))$.

Následující cvičení říká, že uspořádané dvojice se chovají tak, jak bychom chtěli, tedy že jednoznačně určují svůj první i druhý prvek.

Cvičení 9. Ověř, že pokud $(a_0, b_0) = (a_1, b_1)$, tak už nutně $a_0 = a_1$ a $b_0 = b_1$.

Kartézský součin $A \times B$ je množina obsahující všechny uspořádané dvojice (a, b), kde $a \in A$, $b \in B$, lze jej tedy zapsat jako $\{(a, b) : a \in A, b \in B\}$.

Příklad. Ukážeme z axiomů, že pro libovolné dvě množiny A, B existuje kartézský součin $A \times B = \{(a, b) : a \in A, b \in B\}$. Pro každé a, b plyne existence dvojice (a, b) z trojnásobného použití axiomu dvojice.[8] Dále zafixujeme a a definujeme formuli $\psi(x,y)$ jako $y=(a,x)$. Díky axiomu nahrazení existuje množina obrazů všech $b \in B$ v tomto zobrazení, tedy množina $X_a = \{(a,b) : b \in B\}$. Tím už jsme skoro hotovi, stačí sjednotit množiny X_a pro $a \in A$. Množina X_a existuje, ať zvolíme kterékoli a. Uvažme jinou formuli $\psi(x,y)$, a to $y = \{(x,b) : b \in B\}$ (neboli $y = X_x$). Použitím axiomu nahrazení na množinu A dostáváme množinu $\{X_a : a \in A\}$. Aplikováním axiomu sjednocení na tuto množinu dostáváme $A \times B$.



Cvičení 10. Dokaž existenci kartézského součinu bez použití axiomu nahrazení.

Třídy a dvojí pohled na zobrazení

V prvním díle jsme definovali zobrazení (neboli funkci) jako předpis, jak přeměnit jeden typ objektů na jiný. Toto lze formálně přepsat pomocí formule jako v axiomu nahrazení: Uvažme formuli $\psi(x,y)$, která neobsahuje proměnné y_0, y_1, a navíc pro ni platí

$$(\forall x, y_0, y_1)\big((\psi(x,y_0) \wedge \psi(x,y_1)) \Rightarrow (y_0 = y_1)\big).$$

Pak taková formule určuje *třídovou funkci* f_ψ, kde zápisem $f_\psi(x)$ rozumíme ten jediný prvek y, který splňuje $\psi(x,y)$ (existuje-li). Takto popsaná funkce je formulí, nikoli množinou. Další formule ale mohou mluvit jen o množinách. Nelze tedy například napsat formuli, která by znamenala „existuje zobrazení“, což je například pro porovnávání mohutností množin celkem podstatný problém. Proto definujeme funkci coby množinu.

Množinovou funkcí $f\colon A \to B$, kde A, B jsou množiny, myslíme nějakou podmnožinu součinu $f \subset A \times B$, takovou, že pro každé $a \in A$ existuje právě jedno $b \in B$ splňující $(a,b) \in f$. I zde píšeme $f(a) = b$.

Jakmile máme takovou množinu f, můžeme pomocí ní napsat odpovídající formuli $\psi(x,y)$ coby $(x,y) \in f$. Takto jsme převedli množinové zobrazení f na *třídové* zobrazení f_ψ, problém je, že obráceně to nemusí být možné provést. Pro lepší uchopení si objasníme pojem třídy.

Vraťme se k Russelovu paradoxu. Ten vzešel z toho, že jsme s množinami začali zacházet způsobem, na který původně nebyly stavěny. Pokud bychom zůstali u množin coby „souhrnného označení pro nějaký typ bodů v rovině, časových okamžiků, lidí na Zeměkouli, …“, tak bychom Russelův paradox nedostali. Problém nastal, když jsme množiny opět prohlásili za matematické objekty a začali strkat množiny do množin. V takovém okamžiku se ukázalo, že za množinu nemůžeme prohlásit jen tak něco, nýbrž jen to, co sestrojíme pomocí axiomů. Občas se ale hodí používat opět množiny v jejich původním významu, tedy jen coby souhrnné označení pro nějaký typ objektů. Jenže slovo množina je již zabrané. Proto budeme souhrnnému označení pro nějaký typ množin říkat *třída*.

Formálně je *třída* T vždy reprezentovaná nějakou formulí $\varphi(x)$. Za prvky třídy T pak prohlásíme přesně ty množiny x, pro které $\varphi(x)$ platí.

[8] Jedno použití vytvoří množinu $\{a\}$, druhé množinu $\{a,b\}$ a poslední žádanou množinu.

Příklad.

(i) Třída všech množin je reprezentovaná formulí $x = x$. Z Russelova paradoxu plyne, že tato třída neodpovídá žádné množině. Třídy, které neodpovídají žádné množině, budeme nazývat *vlastní*.
(ii) Pro libovolnou množinu A můžeme popsat třídu se stejnými prvky formulí $x \in A$. Každá množina je tedy i třídou. Axiom vydělení navíc říká, že kdykoli jsou všechny prvky třídy T obsaženy v jedné množině, je tato třída opět množinou. Proto si lze třídy představovat jako „příliš velké na to, aby byly množinami“.
(iii) Třída všech jednoprvkových množin je reprezentovaná formulí $(\exists y)(x = \{y\})$.

Cvičení 11. Dokaž, že třída všech jednoprvkových množin je vlastní.

V některých případech se třídy chovají oproti množinám benevolentněji, v některých stejně, v jiných zas striktněji. Stejně jako v množinách můžeme pro libovolné dvě třídy T, U reprezentované formulemi φ, ψ napsat

(i) $T \cup U$ (třída reprezentovaná formulí $\varphi(x) \vee \psi(x)$),
(ii) $T \cap U$ (třída reprezentovaná formulí $\varphi(x) \wedge \psi(x)$),
(iii) $T \subset U$ (neboli $(\forall x)(\varphi(x) \Rightarrow \psi(x))$).

Na rozdíl od množin ale

(i) vlastní třída nemůže být prvkem množiny ani třídy,
(ii) třídy nelze kvantifikovat (tedy ptát se, zda existuje třída či zda něco platí pro každou třídu). Ve výjimečných případech, kdy se tak děje (například ve schématech vydělení a nahrazení), se nejedná o formuli, ale pouze o „metatvrzení“, těmito nuancemi se však nebudeme příliš zabývat.

Nyní je zřejmé, proč zobrazení určené formulí nazýváme třídovým. Platí ještě jedno metatvrzení dávající do souvislosti třídy a zobrazení.

Tvrzení. *Třídové zobrazení lze zapsat množinově právě tehdy, když jeho definiční obor je množina.*

Důkaz. Pokud lze zobrazení napsat množinově, je jeho definiční obor množina z definice množinového zobrazení. Naopak předpokládejme, že máme třídové zobrazení, jehož definiční obor je množina A. Z axiomu nahrazení je tak i jeho obor hodnot množina, označme ji B. Hledané množinové zobrazení dostaneme vydělením z kartézského součinu $A \times B$. □

Příklad. Potence je třídová funkce, kterou nelze vyjádřit množinou, protože je definovaná na všech množinách.

Třídová a množinová zobrazení nebudeme důsledně rozlišovat, nicméně pokud to bude možné, budeme chápat zobrazení jako množinová.

Ordinální čísla – typy DUM

Podobně jako jsme zavedli funkci f coby množinu, můžeme zavést DUMu. DUM coby objekt v sobě musí mít uloženou nejenom nosnou množinu, ale i informaci o tom, jak se prvky nosné množiny porovnávají. Formálně proto definujeme DUMu jako dvojici (D, U), kde D je nosná množina a $U \subset D \times D$ je uspořádání na ní. Uspořádání U pak funguje tak, že značením $d_0 < d_1$ rozumíme $(d_0, d_1) \in U$. Aby (D, U) byla DUM, požadujeme po U vlastnosti dobrého uspořádání.

Jak se ukázalo v minulém díle, není pro DUMu důležitá ani tak její nosná množina, jako spíš jen její „typ“. Prozatím si typ představujeme naivně jako „zapomenutí konkrétních prvků“, ale daleko vhodnější bude jej definovat jako konkrétní množinu. To se standardně provede takto:

Definice. Mějme DUMu (D, U). Transfinitní rekurzí definujeme na D zobrazení f předpisem $f(x) = \{f(d) : d < x\}$, speciálně pro nulový prvek $d_0 \in D$ vyjde $f(d_0) = \emptyset$. Nakonec definujeme *typ* této DUMy jako $\mathrm{typ}(D,U) = \{f(d) : d \in D\}$. Množiny, které lze získat jako $\mathrm{typ}(D,U)$ nějaké DUMy (D,U), nazveme *ordinálními čísly* (stručně *ordinály*).

Příklad. Pro libovolnou trojprvkovou DUMu (D,U) na nosné množině $\{d_0, d_1, d_2\}$, kde $d_0 < d_1 < d_2$, se chová definice typu takto:

$$f(d_0) = \emptyset, \quad f(d_1) = \{\emptyset\}, \quad f(d_2) = \{\emptyset, \{\emptyset\}\}, \quad \mathrm{typ}(D,U) = \Big\{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\Big\}.$$

Ještě dodejme, v jaké formě jsme použili transfinitní rekurzi. Rekurzivní předpis je třídové zobrazení definované na všech množinových funkcích, jejichž definičním oborem je $D \leftarrow x$ pro nějaké $x \in D$. Výsledná funkce pak je opět množinová. Jelikož někdy neumíme předem omezit třídu všech možných částečných množinových funkcí množinou, není tvrzení o existenci funkce dané transfinitní rekurzí tvrzením popsatelným formulí, ale metatvrzením, do kterého teprve můžeme dosazovat různé rekurzivní předpisy.

Cvičení 12. Projdi důkaz existence funkce dané transfinitní rekurzí (z minulého dílu) a rozmysli si, které axiomy jsou potřeba pro tvrzení, že každá DUM má typ.

Nyní si uvědomíme, jak vypadají typy DUM. Každý z postupně přidávaných prvků $f(x) = \{f(d) : d < x\}$ obsahuje všechny prvky $f(d)$ pro $d < x$. A také naopak žádný z těchto prvků $f(d)$ prvek $f(x)$ neobsahuje – to plyne z axiomu fundovanosti.[9] Celkově dostáváme, že funkce f zobrazila nosnou množinu DUMy (D,U) na $\alpha = \mathrm{typ}(D,U)$ takovým způsobem, že

$$(d_0 < d_1) \Leftrightarrow (f(d_0) \in f(d_1)).$$

Pokud se budeme dívat na náležítko coby na znaménko uspořádání, vidíme, že f je rostoucí bijekcí mezi DUMami (D,U) a $(\alpha, \in)$, platí tedy $(D,U) \simeq (\alpha, \in)$.

Ano, používání náležítka k porovnávání zprvu vypadá jako nehorázná zhůvěřilost, k tomu přeci vůbec nebylo stavěné. Na druhou stranu je náležítko to nejjednodušší, co v jazyce teorie množin máme, a ukáže se být zcela postačujícím a dokonce praktickým. Na prvcích ordinálního čísla bude proto náležítko plnit roli menšítka $<$.

Další věc, které si můžeme všimnout rovnou z definice funkce typ, je $f(x) = \mathrm{typ}(D \leftarrow x, U)$. Prvky ordinálního čísla jsou tedy opět ordinály – typy všech menších DUM. Tato skutečnost usnadňuje jejich porovnávání. Konkrétně pro ordinály α, β platí

(i) $(\alpha, \in) \simeq (\beta, \in)$ právě tehdy, když $\alpha = \beta$,
(ii) $(\alpha, \in) < (\beta, \in)$ právě tehdy, když $\alpha \in \beta$,
(iii) $(\alpha, \in) \leq (\beta, \in)$ právě tehdy, když $\alpha \subset \beta$.

Definice. Označme $\mathbb{O}n$ třídu všech ordinálních čísel.

Později ukážeme, že třída $\mathbb{O}n$ nemůže být množinou. Chová se však jako „největší ordinál“, konkrétně:

(i) $(\forall \alpha \in \mathbb{O}n)(\alpha \subset \mathbb{O}n)$.
(ii) $\mathbb{O}n$ je dobře uspořádaná náležítkem. Dokonce v tom smyslu, že kdykoli popíšeme neprázdnou podtřídu $T \subset \mathbb{O}n$, tak tato podtřída má nejmenší prvek. Proč? Uvažme libovolný ordinál $\alpha \in T$. Jedná-li se o nejmenší prvek T, jsme hotovi. V opačném případě je množina $\alpha \cap T$ neprázdná a najdeme nejmenší prvek tohoto průniku díky dobrému uspořádání na α.
(iii) Na $\mathbb{O}n$ lze definovat třídová zobrazení pomocí transfinitní rekurze. Rekurzivní předpis v takovém případě musí být třídové zobrazení, které je definované na všech množinových funkcích f s definičním oborem $\alpha \in \mathbb{O}n$. Transfinitní rekurze pak určuje třídovou funkci F definovanou na všech ordinálech. Formálně napsané Ti to možná zní děsivě, ale jak uvidíš na příkladu ω_α na konci seriálu, samotné použití je docela přirozené.

[9] Případně to lze ukázat i bez něj volbou nejmenšího x, pro které se tato vlastnost porušila.

Zatím jsme si ukázali, že každé ordinální číslo je množina všech menších ordinálů. Následující tvrzení říká, že to platí i obráceně.

Tvrzení. *Nechť $X \subset \mathbb{O}n$ je množina taková, že kdykoli obsahuje ordinální číslo α, tak obsahuje i všechna ordinální čísla $\beta < \alpha$. Pak X je ordinál.*

Důkaz. Z dobrého uspořádání třídy $\mathbb{O}n$ (bod (ii)) plyne, že i X je dobře uspořádaná náležítkem. Navíc dle zadání splňuje pro každý prvek $\alpha \in X$ podmínku $\alpha = \{\beta \in X : \beta < \alpha\}$. To znamená, že funkce $f(\alpha) = \alpha$ splňuje rekurzivní předpis pro definici typu DUMy $(X, \in)$, takže $\mathrm{typ}(X, \in) = X$, čili X je ordinální číslo.

Důsledek. *Pro libovolnou množinu $X \subset \mathbb{O}n$ je $\bigcup X$ ordinální číslo.*

Důsledek. *$\mathbb{O}n$ je vlastní třída.*

Důkaz. Kdyby $\mathbb{O}n$ byla množina, tak by byla ordinálem. To by ale znamenalo $\mathbb{O}n \in \mathbb{O}n$, což je sporu s fundovaností.[10] □

Cvičení 13. Ukaž, že množina X je ordinální číslo právě tehdy, když platí následující dvě podmínky.

(i) Pro každé dva různé prvky $x, y \in X$ platí $x \in y$ nebo $y \in x$.
(ii) Každý prvek $x \in X$ je podmnožinou X.

Definice. Ordinály dělíme na *nulový, izolované* a *limitní* podle toho, jaké prvky reprezentují v uspořádané třídě $\mathbb{O}n$. Konkrétně:

(i) *Nulový* ordinál je jen prázdná množina $\emptyset$.
(ii) *Izolovaný* ordinál α je takový, který má největší prvek $\beta \in \alpha$ v uspořádání náležítkem.
(iii) *Limitní* ordinály jsou ty, které nejsou nulové ani izolované.

Přirozená a reálná čísla

Nyní definujeme přirozená čísla coby množiny. Přirozená čísla jsou od toho, aby udávala velikosti konečných množin. Je proto vhodné, aby každé přirozené číslo mělo tolik prvků, kolik je ono samo. Tedy 0 bude prázdná množina, 1 bude jednoprvková množina, 2 bude dvouprvková, a tak dále. Prázdná množina je určena jednoznačně $0 = \emptyset$, ale které prvky dát do dalších přirozených čísel? Musí se jednat o již dříve definované množiny, tak dává smysl, aby to byla přímo předchozí přirozená čísla:

$$1 = \{0\}, \quad 2 = \{0, 1\}, \quad 3 = \{0, 1, 2\}, \quad 4 = \{0, 1, 2, 3\}, \ldots$$

Přesně takto se ale staví i ordinální čísla. Přirozená čísla jsou tedy jen počátečními ordinálními čísly – těmi konečnými. Formálně popíšeme, které ordinály považujeme za *konečné.*

Definice. *Konečné* ordinální číslo (nebo též *přirozené číslo*) α je takové, které není limitní a ani žádný menší ordinál není limitní. Symbolem ω značíme množinu všech konečných ordinálních čísel.

Z toho snadno plyne, že kdykoli je ordinál n konečný, jsou i všechny ordinály $k < n$ konečné. Množina ω je tak současně ordinálem, a to nejmenším nekonečným – všechny menší jsou konečné a ω nemůže obsahovat samu sebe.

Musíme ale dokázat, že ω existuje (tedy že se nejedná o vlastní třídu). Zvolme libovolnou množinu m z axiomu nekonečna a vydělme z ní množinu $\omega' = \{n \in m : n \text{ je konečný ordinál}\}$. Dokážeme, že ω' obsahuje všechny konečné ordinály, a je tak hledanou ω. Zvolme pro spor nejmenší konečný ordinál $n \notin \omega'$. Nulový ordinál v ω' leží, takže je n izolovaný a existuje jeho předchůdce $n' \in \omega'$. Jenže $n = n' \cup \{n'\}$, a tak $n \in m$ z podmínky pro m. Proto i $n \in \omega'$.

[10]Kdybychom nechtěli použít axiom fundovanosti (který se občas vypouští), mohli bychom argumentovat i tím, že pro DUMu nemůže nastat $\mathbb{O}n < \mathbb{O}n$.

Na ordinálech, a tudíž i na přirozených číslech, zavedeme operace sčítání a násobení pomocí sčítání a násobení na DUMách. Pouze s tím rozdílem, že na výsledek aplikujeme zobrazení typ, abychom získali opět ordinální číslo, tedy $\alpha \cdot \beta = \mathrm{typ}\big((\alpha, \in) \cdot (\beta, \in)\big)$.

Cvičení. Rozmysli si, že součet i součin přirozených čísel je opět přirozené číslo.

Na základě přirozených čísel definujeme celá čísla. Množinou celých čísel $\mathbb{Z}$ bude $(\{0,1\} \times \omega) \setminus \{(1,0)\}$. Celé číslo pak je vždy dvojice (z, n), kde n je přirozené číslo určující absolutní hodnotu celého čísla a $z \in \{0,1\}$ určuje jeho znaménko (0 znamená plus). Z množiny celých čísel vyjímáme dvojici $(1,0)$, která by reprezentovala číslo „-0“.

Dále definujeme racionální čísla (zlomky) coby dvojice (a, b), kde a je celé číslo a b je nenulové přirozené číslo nesoudělné s a. Tuto dvojici interpretujeme jako zlomek $\frac{a}{b}$. Operace na celých a racionálních číslech se definují klasicky, ale bylo by nudné to zde rozepisovat.

Poznámka. Při takto definovaném rozšiřování čísel je 42 coby přirozené číslo jiné než 42 coby celé číslo, a to je jiné než 42 coby racionální číslo. Tento formalistický problém ale matematiky nikdy příliš nevzrušoval a běžně jsou přirozená čísla chápána jako podmnožina celých a ta zase jako podmnožina racionálních, ačkoli tomu tak formálně vzato zcela není.

Předvedeme ještě elegantní definici nezáporných reálných čísel, kterou lze snadno rozšířit na definici všech reálných čísel. Bylo by možné je definovat pomocí nekonečného desetinného (či binárního) rozvoje, avšak v takovém případě by bylo nesnadné například definovat násobení, proto to uděláme jinak.

Definice. Nechť $\mathbb{Q}_0^+$ značí množinu nezáporných racionálních čísel. O množině $R \subset \mathbb{Q}_0^+$ řekneme, že to je nezáporné reálné číslo, pokud

(1) s každým prvkem obsahuje všechny menší, tedy $(\forall r \in R)(\forall s \in \mathbb{Q}_0^+)(s < r \Rightarrow s \in R)$,
(2) nemá největší prvek,
(3) $R \neq \mathbb{Q}_0^+$.

Nezáporné reálné číslo tedy charakterizujeme výčtem všech racionálních čísel, která jsou menší. Racionální číslo $q \in \mathbb{Q}_0^+$ odpovídá reálnému číslu $\{r \in \mathbb{Q}_0^+ : r < q\}$. Operace v reálných číslech definujeme následovně:

(i) pro nezáporná reálná čísla R, S definujeme $R + S = \{r + s : r \in R, s \in S\}$,
(ii) pro nezáporná reálná čísla R, S definujeme $R \cdot S = \{r \cdot s : r \in R, s \in S\}$,
(iii) pro nezáporná reálná čísla R, S definujeme $R \leq S$ jako $R \subset S$.

Množinu nezáporných reálných čísel značíme $\mathbb{R}_0^+$.

Poznámka. Tato konstrukce reálných čísel je nejbližší konstrukci pomocí Dedekindových řezů. Standardní konstrukce Dedekindovými řezy definuje rovnou všechna reálná čísla (nikoli jen nezáporná). V takovém případě je třeba ještě zakázat prázdnou množinu a věnovat větší péči násobení reálných čísel.

Cvičení 14. Dokaž, že množiny popsané v bodech (i), (ii), tedy součet a součin dvou nezáporných čísel, odpovídají definici nezáporného reálného čísla.

Cvičení 15. Najdi nespočetnou množinu $X \subset \mathcal{P}(\omega)$ tak, aby pro libovolné dva prvky $x, y \in X$ platilo $x \subset y$ nebo $y \subset x$.

Z takto definovaných nezáporných reálných čísel plynou klíčové vlastnosti reálných čísel, které popisují jejich vztah k číslům racionálním:

(i) Pro každá dvě různá nezáporná reálná čísla existuje racionální číslo, které leží mezi nimi. (hustota racionálních čísel)
(ii) Uvažme neprázdnou množinu čísel $X \subset \mathbb{R}_0^+$. Řekneme, že X je omezená číslem $r \in \mathbb{R}_0^+$, pokud $(\forall x \in X)(x \leq r)$. Pokud nějaké číslo $r \in \mathbb{R}_0^+$ omezuje X, tak lze najít jedno nejmenší možné číslo, které omezuje X (tímto číslem je $\bigcup X$). (existence suprema)

Nezáporná reálná čísla lze rozšířit na všechna reálná čísla obdobně jako přirozená čísla na celá. Vlastnost hustoty racionálních čísel i existence suprema v nich zůstane zachována.

Příklad. O množině $X \subset \mathbb{R}$ řekneme, že je *diskrétní*, pokud pro každé $x \in X$ existuje otevřený interval[11] I, který splňuje $I \cap X = \{x\}$. Platí, že každá diskrétní množina je spočetná.

Důkaz. Uvažme $x \in X$ a otevřený interval $I = (a, b)$, který splňuje $I \cap X = \{x\}$. Pak je možné najít racionální číslo p uvnitř intervalu (a, x) a racionální číslo q uvnitř intervalu (x, b). Možných dvojic racionálních čísel (p, q) je jenom spočetně mnoho, protože $|\mathbb{Q} \times \mathbb{Q}| = \omega$. Na druhou stranu lze zpětně z dvojice (p, q) rekonstruovat číslo x tím, že najdeme průnik intervalu (p, q) a množiny X. Proto je v množině X jenom spočetně mnoho čísel. □

Cvičení 16. Najdi funkci $f\colon \mathbb{R}\times\mathbb{R} \to \omega$ takovou, že $f(x, y) = f(y, z)$ nastává jedině pro $x = y = z$.

Nespočetný ordinál

Rozšíření přirozených čísel směrem k reálným byla odbočka demonstrující, že pomocí teorie množin lze stavět i známé matematické objekty. Nyní se vrátíme k výpravě do nekonečna a ještě dál a sestrojíme nespočetné ordinální číslo.

Nechť ω_1 značí množinu všech spočetných ordinálních čísel. Určitě nemůže být ω_1 spočetná – to plyne ze stejného argumentu, z jakého $\mathbb{O}n$ není množina a ω je nekonečná; musela by obsahovat sama sebe, což je ve sporu s fundovaností. Rovněž analogicky je ω_1 nejmenší nespočetný ordinál. Nemusí ale být jasné, proč tato množina existuje, neboli proč není vlastní třídou.

To plyne z axiomu nahrazení pro funkci typ. Začneme s množinou $\{\omega\} \times \mathcal{P}(\omega \times \omega)$, čili množinou všech dvojic (ω, U), kde $U \subset \omega \times \omega$. V některých případech určuje U dobré uspořádání na ω, v takovém případě můžeme najít $\mathrm{typ}(\omega, U)$. Množinu ω_1 sestrojíme jako množinu těchto typů (existuje díky axiomu nahrazení), kterou nakonec ještě sjednotíme s ω (abychom tam dostali i konečné ordinály).

Příklad. Neexistuje rostoucí funkce $f\colon \omega_1 \to \mathbb{R}$.

Důkaz. Pro spor předpokládejme takovou funkci f. Pak pro každé $\alpha \in \omega_1$ najdeme racionální číslo $g(\alpha)$ v otevřeném intervalu $(f(\alpha), f(\alpha + 1))$. Funkce g je rostoucí, tedy prostá, a dostáváme tak $|\omega_1| \le |\mathbb{Q}|$, což je spor. □

Dále ω_1 vykazuje řadu analogií s množinou přirozených čísel ω:

ω : Každý prvek $n \in \omega$ dělí ω na konečně mnoho menších a nekonečno větších prvků.
ω_1 : Každý prvek ω_1 dělí ω_1 na spočetně mnoho menších a nespočetně mnoho větších prvků.
Proč? Menších prvků je spočetně, protože to jsou prvky spočetného ordinálu, a větších (ostatních) prvků je nespočetně mnoho, protože ω_1 sama je nespočetná.

ω : Každá množina $X \subset \omega$ je konečná nebo má stejný typ jako ω.
ω_1 : Každá množina $X \subset \omega_1$ je spočetná nebo má stejný typ jako ω_1.
Proč? Plyne z věty o porovnání typů z minulého dílu – buď $\mathrm{typ}(X) \in \omega_1$, a tak je X spočetná, nebo $\mathrm{typ}(X) = \omega_1$.

ω : Množina $X \subset \omega$ je konečná právě tehdy, když $\bigcup X \in \omega$.
ω_1 : Množina $X \subset \omega_1$ je spočetná právě tehdy, když $\bigcup X \in \omega_1$.
Proč? Když je X spočetná a každý prvek $x \in X$ je spočetný ordinál, tak množina $\bigcup X$ je spočetná, a tedy prvek ω_1. Pro opačnou implikaci si stačí uvědomit $X \subset (\bigcup X) + 1 \in \omega_1$.

[11] Otevřený interval (a, b) je množina daná předpisem $\{x \in \mathbb{R} : a < x < b\}$ pro dané $a, b \in \mathbb{R}$, $a < b$.

Aby to ale nevypadalo, že se ω_1 chová úplně stejně jako přirozená čísla, nabízíme opět ilustrační pohádku.

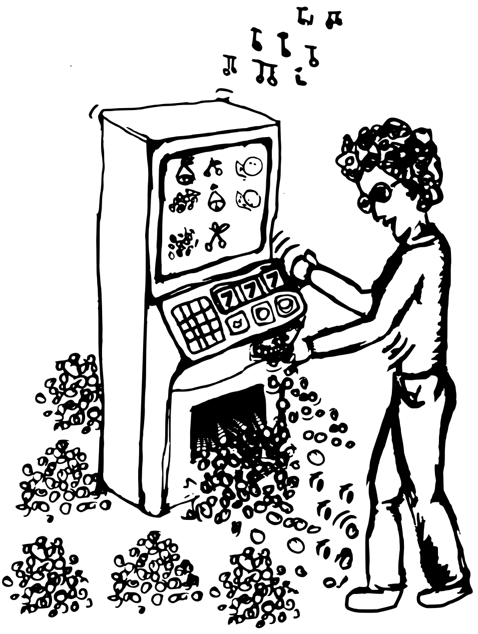
Pohádka o nespočetném gamblerovi

Ve světě teorie množin, kde čas běží po ordinálních číslech, se jistý pan Loudal neustále hádal se svou ženou. Sice před časem nalezl poklad, ale v teorii množin je času nekonečně (a ještě víc), a tak už stihl skoro všechen majetek prosázet v loterii, za což ho Loudalka právě napomínala: „Měl bys s tím sázením skončit v konečným čase a čím dřív, tím líp. Nekonečně mincí se vyhrát nedá, to je dokázaný! Važ si tý jedný mince, co ti zbyla!“ „Ale na mne se jednou usměje štěstí a budeme mít nekonečně peněz,“ snil si Loudal svou.

Navíc tou dobou do vesnice přivezli výherní automat. A nebyl to jen tak kdejaký hrací automat, jaké možná znáte z obyčejného světa. Obyčejné automaty většinou sežerou minci a nic z toho. Kdykoli tento automat obdržel minci, vypadly z něho dvě nové mince stejné hodnoty. Od něčeho tak lákavého Loudalka Loudala zadržet nedokázala. Hodil do něj minci m_0, vypadly dvě další mince m_1, m_2, hodil do něj minci m_1, vypadly další dvě mince m_3, m_4, vhodil mince m_2, vypadly mince m_5, m_6. A takto Loudal pokračoval až do ω, kdy do automatu naházel všechny mince a žádná mu nezbyla.

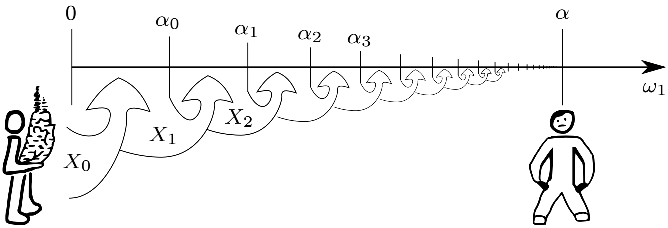
To nebylo to pravé ořechové, pomyslel si Loudal s jednou kapsou prázdnou a druhou vysypanou. Loudalka ho přivítala zčásti vítězoslavně, zčásti pekelně naštvaně, ale unavený Loudal ji ani moc neposlouchal a šel spát. V noci dostal nápad. Hned vyskočil z postele a šel ještě za tmy na ryby, aby si vydělal nějakou tu kačku do automatu. Jakmile se mu to povedlo, vydělanou minci m_0 hodil do automatu a vypadly opět mince m_1, m_2. Minci m_1 si nechal a do automatu hodil až druhou vydělanou minci m_2. Minci m_3 si opět nechal a hodil do automatu m_4, … Takto měl v čase ω od vhození první mince nekonečně mnoho mincí. „No vidíš,“ povídá ráno Loudalce, „já věděl, že se to musí podařit.“

Dalšího dne pak automat vyměnili za nový. Nový automat, kdykoli dostane minci, vyhodí zpátky ω mincí. „No teda,“ pomyslí si Loudal, „teď někomu stačí hodit do automatu jednu minci a bude stejně bohatý jako já, jaká nespravedlnost!“ A hned se mu v hlavě zrodil plán, že kdyby na automatu hrál až do kroku ω_1, mohl by vyhrát nespočetně mnoho mincí. Marně ho Loudalka napomínala, že v tom bude zase nějaká čertovina, akorát se ohradil: „Že dostanu nekonečně mnoho mincí, tos mi taky nevěřila, a jakej jsem byl!“ Loudal vzal svých ω mincí a začal je házet do automatu. Opět se pokoušel si vybírat mince šikovně do zásoby, ale ať se snažil, jak se snažil, ještě dříve, než se dostal do kroku ω_1, byl opět bez peněz. Nespočetně mnoho mincí pomocí takového automatu totiž získat nelze. O tom, jak mu pak Loudalka vyhubovala, raději taktně pomlčíme.



A proč z automatu nelze získat nespočetně mnoho mincí? Dokážeme, že už v některém spočetném kroku Loudal nebude mít do automatu co hodit. Můžeme tedy pro jednoduchost předpokládat, že se Loudal nerozhodl žádnou minci ušetřit do kroku ω_1 (když chceme dokázat, že se do toho kroku stejně nedostane).

Označme X_0 množinu všech kroků, při nichž vhodil do automatu některou z mincí, které měl na začátku. To je spočetná podmnožina ω_1, tedy existuje ordinál $\alpha_0 \in \omega_1$, který je ostře větší než všechny prvky X_0 (například můžeme zvolit $\alpha_0 = \bigcup X_0 + 1$). Před α_0 proběhlo spočetně mnoho kroků a v každém z automatu vypadlo spočetně mnoho mincí. Celkem to je opět spočetně mnoho vypadlých mincí. Označme X_1 množinu všech kroků, během kterých Loudal hodil do automatu některou z nich. Opět najdeme α_1, které je větší než všechny prvky X_1, a opakováním postupu sestrojíme X_n a α_n pro každé přirozené číslo n. Nakonec definujeme spočetný ordinál $\alpha = \bigcup\{\alpha_n : n \in \omega\}$. V kroku α už Loudalovi žádná mince nezbyla. Každou minci, kterou vydělal před krokem α, totiž vydělal před některým krokem α_n. Jenže to znamená, že ji hodil do automatu před krokem α_{n+1}.



Poznámka. Nepohádková verze tohoto tvrzení se nazývá Pressing down lemma a zní: „Nechť f je funkce $\omega_1 \to \omega_1$. Předpokládejme, že pro všechny nenulové $\alpha \in \omega_1$ platí $f(\alpha) < \alpha$. Pak se nemůže stát, že by všechny množiny $X_\beta = \{\alpha \in \omega_1 : f(\alpha) = \beta\}$ byly spočetné.“ Jak toto tvrzení souvisí s pohádkou? Z Pressing down lemmatu lze přímočaře dokázat nemožnost výhry ω_1 mincí a naopak.

Nejprve ukážeme, že kdyby se Loudal dostal až do kroku ω_1, nemůže platit Pressing down lemma. V každém kroku α si Loudal musí vzít minci z některého předchozího kroku, označíme jej $f(\alpha)$. Množina X_β pro takto definovanou f pak obsahuje všechny kroky, ve kterých hodil do automatu některou minci vydělanou v kroku β. Je tedy spočetná, protože vydělaných mincí z každého kroku je spočetně.

Nyní naopak mějme funkci f, pro kterou jsou všechna X_β spočetná, a ukažme, že se Loudal může dostat do kroku ω_1. V kroku α vezme Loudal minci z kroku $f(\alpha)$. Navíc mějme zafixované očíslování množiny $X_{f(\alpha)}$ a Loudal si vezme tolikátou minci z kroku $f(\alpha)$, kolikátý je prvek $\alpha \in X_{f(\alpha)}$ v tomto očíslování. Tím nebude potřebovat žádnou minci hodit do automatu vícekrát a vždy bude mít minci, kterou do automatu hodí. Dostane se tedy až do kroku ω_1.

A ještě dál

Postup pro sestrojení ω_1 coby množiny všech spočetných ordinálů lze zobecnit a definovat ω_α pro obecný ordinál α rekurzivním předpisem:

(i) $\omega_0 = \omega$,
(ii) $\omega_{\alpha+1}$ je množina všech ordinálů β splňujících $|\beta| \leq |\omega_\alpha|$,
(iii) $\omega_\alpha = \bigcup\{\omega_{\alpha'} : \alpha' < \alpha\}$ pro α limitní.

Takto definované ordinály ω_α mají všechny různou mohutnost, což dává odpověď na otázku, kolik je různě velkých nekonečen. Různě velká nekonečna tvoří vlastní třídu, tedy je jich tolik, že se ani nevejdou do množiny.

Příklad. Pokud bychom chtěli sestrojit hodně velké nespočetné ordinální číslo (resp. DUMu), můžeme uvážit ordinály

$$\omega_0, \quad \omega_{\omega_0}, \quad \omega_{\omega_{\omega_0}}, \quad \omega_{\omega_{\omega_{\omega_0}}}, \quad \ldots$$

a nakonec vzít jejich sjednocení.

Čokoládová výzva

Za následující čokoládovou úlohu na řešitele čeká geometrická **nekonečná posloupnost čokolád**. Ten, kdo ji vyřeší nejrychleji, dostane čokoládu. Ten, kdo ji vyřeší po něm, dostane půlku čokolády, další čtvrtku čokolády, atd. Tak s chutí do řešení! Úloha se týká toho, jak lze mohutnost ω_n charakterizovat i bez použití rekurze či dobrých uspořádání.

Úloha. Nechť α je ordinál a n přirozené číslo. Označme $[\alpha]^n$ množinu všech n-prvkových podmnožin α a $[\alpha]^{<\omega}$ množinu všech konečných podmnožin α. O zobrazení $f\colon [\alpha]^n \to [\alpha]^{<\omega}$ řekneme, že je *čokoládové*, pokud existuje $(n+1)$-prvková množina $X \subset \alpha$ taková, že

$$(\forall x \in X)(x \notin f(X \setminus \{x\})).$$

Dokaž, že následující dvě tvrzení jsou ekvivalentní.

(i) Všechna zobrazení $f\colon [\alpha]^n \to [\alpha]^{<\omega}$ jsou čokoládová.
(ii) $\alpha \geq \omega_n$.

Minulou čokoládovou výzvu vyhrál Danil Koževnikov s následující konstrukcí: Pro DUMy A, B definujeme mocninu A^B jako množinu všech funkcí $B \to A$, které jsou pouze na konečně mnoha místech nenulové. Dvě takové funkce f, g porovnáme tak, že se podíváme na nejvyšší prvek $b \in B$, pro který $f(b) \neq g(b)$, a hodnota v tomto bodě rozhodne, která funkce je větší. Danil takto vymyslel mocnění DUM, které se běžně používá, a s přehledem by vyhrál už jen s DUMou $\omega^{(\omega^\omega)}$.

On však šel dál a zbytek byl mírně zamlžený, tak jej popíšeme pomocí ordinálních čísel a standardní notace ε_α. Stejně jako u sčítání a násobení rozšíříme mocnění na ordinální čísla. Pak transfinitní rekurzí definujeme ε_α předpisem:

(i) $\varepsilon_0 = \omega \cup \omega^\omega \cup \omega^{(\omega^\omega)} \cup \ldots$,
(ii) $\varepsilon_{\alpha+1} = \varepsilon_\alpha \cup \varepsilon_\alpha^{\varepsilon_\alpha} \cup \varepsilon_\alpha^{(\varepsilon_\alpha^{\varepsilon_\alpha})} \cup \ldots$,
(iii) $\varepsilon_\alpha = \bigcup\{\varepsilon_\beta : \beta < \alpha\}$ pro α limitní.

DUMou, kterou Danil vsadil, je $\varepsilon_{(\omega^\omega)}$. Ještě poznamenejme, že v zadání předchozí čokoládové úlohy bylo cílem popsat co možná největší spočetnou DUMu, takže i Danilova DUM je spočetná. Oproti tomu DUM popsaná v předchozí kapitole je nespočetná vzhledem k tomu, že už ω_1 je nespočetná.

Seznam symbolů a pojmů

Na této stránce jsou stručně uvedeny všechny důležité pojmy druhého dílu seriálu. U každého pojmu z tohoto dílu je uvedeno, na které stránce byl definován.

str 2. Logické spojky $\neg$, $\wedge$, $\vee$, $\Rightarrow$, $\Leftrightarrow$
str 2. Kvantifikátory $\forall$, $\exists$
str 2. *Náležítko* $\in$
str 2. *Formule* – výroky ve formálním jazyce
str 3. Zkratky $\notin$ (neleží), $\neq$ (nerovná se), $\subset$ (je podmnožinou)
str 3. $\{x : \ldots\}$ – *množina daná předpisem*
str 3. $\{x_0, \ldots, x_n\}$ – *množina daná výčtem prvků*
str 3. $x \cap y$ – *průnik* množin x a y
str 3. $x \cup y$ – *sjednocení* množin x a y
str 3. $x \setminus y$ – *množinový rozdíl* x minus y
str 3. $\mathcal{P}(x)$ – *potence* množiny x
str 4. $\emptyset$ – *prázdná* množina
str 5. $\bigcup X$ – sjednocení všech prvků množiny X
str 6. (a, b) – *uspořádaná dvojice*
str 7. $A \times B$ – *kartézský součin*
str 7. *Třídová funkce*
str 7. *Množinová funkce*
str 7. *Třída* – souhrnnné označení pro všechny množiny s nějakou vlastností
str 8. *Vlastní* třída – třída, která není množinou
str 8. DUM coby dvojice (D, U)
str 8. typ(D, U) čili *ordinální* číslo (stručně *ordinál*) udávající typ DUMy (D, U)
str 9. $\mathbb{O}n$ – třída všech ordinálů
str 10. Ordinál *nulový*, *izolovaný*, *limitní*
str 10. *Přirozené číslo* neboli *konečné* ordinální číslo
str 10. ω – první nekonečný ordinál
str 10. $\alpha + \beta, \alpha \cdot \beta$ pro $\alpha, \beta \in \mathbb{O}n$ – operace na ordinálech
str 11. $\mathbb{R}_0^+$ neboli množina všech *nezáporných reálných čísel*
str 12. ω_1 – první nespočetný ordinál
str 14. ω_α – ordinální číslo α-té nekonečné mohutnosti

Důležité pojmy z minulého dílu: zobrazení (funkce), spočetno, nespočetno, porovnávání mohutností $|A| \leq |B|$, $|A| = |B|$, DUM (dobře uspořádaná množina), operace na DUMách $A + B$, $A \cdot B$, porovnávání DUM $A < B$, $A \simeq B$.

Návody

1. $(\exists y)\Big(\big(\neg(y \in x)\big) \wedge (\forall z)\big(z \in x' \Leftrightarrow (z = y \vee z \in x)\big)\Big)$.

2. Zvol $z = \{x\}$.

3. $a \setminus b = \{z \in a : z \notin b\}$. Stačí tedy volit $\varphi(z)$ jako $z \notin b$.

4. $(\forall x)(\exists y)(\forall z)\big(z \in y \Leftrightarrow (\forall u)(u \in z \Rightarrow u \in x)\big)$.

5. (i) Existence množiny $\{a\}$ je ve sporu s axiomem fundovanosti. (ii) Stejný argument s $\{a, b\}$.

6. (Zatím není rozepsané kompletně)

$$(\exists m)(\exists e)\Bigg((\forall z)\big(z \notin e\big) \wedge (e \in m) \wedge (\forall x)\Big(x \in m \Rightarrow (\exists y \in m)\big(\forall z\big)\big((z \in y) \Leftrightarrow (z \in x \vee z = x)\big)\Big)\Bigg).$$

7. (i) Axiom nekonečna vyžaduje existenci množiny, jejímž prvkem je prázdná množina. Tedy prázdná množina sama o sobě musí existovat. (ii) $\psi(x, y)$ definujeme jako $\varphi(x) \wedge (x = y)$. (iii) $\mathcal{P}(\mathcal{P}(\emptyset))$ je dvouprvková množina $\{\emptyset, \{\emptyset\}\}$. Pak definujeme $\psi(x, y)$ jako $(x = \emptyset \wedge y = s) \vee (x = \{\emptyset\} \wedge y = t)$ a dostaneme množinu $\{s, t\}$.

8. Postupné kroky:

(i) $\emptyset \in \mathcal{P}(\emptyset)$, $\emptyset \in \mathcal{P}(\mathcal{P}(\emptyset))$,
(ii) $\{\emptyset\} \in \mathcal{P}(\mathcal{P}(\emptyset))$, $\{\emptyset\} \in \mathcal{P}(\mathcal{P}(\mathcal{P}(\emptyset)))$ z (i),
(iii) $\{\emptyset, \{\emptyset\}\} \in \mathcal{P}(\mathcal{P}(\mathcal{P}(\emptyset)))$ z (i) a (ii),
(iv) $(\emptyset, \{\emptyset\}) = \{\{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} \in \mathcal{P}(\mathcal{P}(\mathcal{P}(\mathcal{P}(\emptyset))))$ z (ii) a (iii).

9. Dvojice (a, b) je jednoprvková množina právě tehdy, když $a = b$. V takovém případě je $\{a\}$ jednoznačně určený prvek této množiny. Pokud je (a, b) dvouprvková, obsahuje jednu jednoprvkovou a jednu dvouprvkovou množinu. Prvek té jednoprvkové musí být a. Současně a musí být jedním z prvků dvouprvkové množiny, ten druhý pak musí být b.

10. Je třeba si vzpomenout na definici uspořádané dvojice. Součin $A \times B$ pak lze dostat vydělením z množiny $\mathcal{P}(\mathcal{P}(A \cup B))$.

11. Sporem: Kdyby to byla množina, tak z axiomu sjednocení existuje množina všech množin. Alternativa: Nechť množina A obsahuje všechny jednoprvkové množiny. Pak obsahuje i množinu $\{A\}$, což je sporu s fundovaností.

12. To, že je rekurzivní předpis jednoznačně definován pro každou částečnou funkci, zaručují axiom nahrazení a extensionality. Pro využívání vlastnosti dobrého uspořádání vždy potřebujeme axiom vydělení: Existuje prvek, který splňuje podmínku, vydělíme tedy množinu všech prvků, které ji splňují, a v té najdeme nejmenší. Dále rozlišíme tři možnosti z důkazu v minulém dílu:

(i) Když x je nulový, stačí axiom existence.
(ii) Když x je izolovaný, používáme axiomy dvojice a sjednocení pro rozšíření f o jeden prvek. Alternativně by stačilo popsat toto rozšířené zobrazení třídově a použít axiom nahrazení stejně jako v bodě (iii).
(iii) Když x je limitní, umíme (jednoznačně) popsat hodnotu pro všechna $y < x$. Stačí tedy použít axiom nahrazení k tomu, že třídové zobrazení, jehož definiční obor je množina, lze reprezentovat množinou.

13. Dopředná implikace byla dokázaná v textu. Předpokládejme (i) a (ii) a dokažme, že X je ordinál. Z (i) vyplyne přímočarou aplikací axiomu fundovanosti (zde se bez jeho využití neobejdeme), že X je dobře uspořádaná náležítkem. Důkaz se dokončí postupem z důkazu předchozího tvrzení.

14. (i) Když $x < r + s$, tak $x = r' + s$, kde $r' = x - s < r$. Z toho snadno odvodíme potřebné vlastnosti. (ii) Analogicky k (i).

15. Přejmenuj prvky nezáporných reálných čísel (coby množin) pomocí bijekce mezi $\mathbb{Q}_0^+$ a ω.

16. Uvaž bijekci $g\colon \mathbb{Q} \to \omega$. Pak lze volit $f(x, x) = 0$. Pro $x < y$ pak $f(x, y) = 2g(q) + 1$, $f(y, x) = 2g(q) + 2$, kde q leží v intervalu (x, y).

Do nekonečna a ještě dál

Axiom výběru očividně platí, princip dobrého uspořádání očividně neplatí, a Zornovo lemma – těžko říct. – Jerry Bona

Díl třetí – Síla volby

aneb Nač ten humbuk okolo axiomu výběru

V minulém díle jsme představili sadu deseti axiomů teorie množin, které se v současnosti běžně používají. Jeden z nich, axiom výběru, mezi nimi ale z počátku chyběl. Skutečnost, že se matematikům nedaří dokázat něco tak zřejmého jako „je možné provést nekonečně mnoho nahodilých výběrů najednou“, způsobila pozdvižení. Obzvlášť poté, co shledali, že na jednu stranu lze z axiomu výběru odvodit různé pochybně vzhlížející důsledky, ale na druhou stranu jej již mimoděk používají ve svých důkazech. Obava, krátce poté, co se zbavili Russelova paradoxu, byla pochopitelná. Opravdu si můžeme jen tak dovolit přidat nový axiom? Nemůže se s ním teorie zas rozbít? Nakonec problém rozsekli podobně jako hypotézu kontinua[1] (použitím obdobných pokročilých nástrojů). Axiom výběru není možné pomocí ostatních axiomů dokázat ani vyvrátit.

Rozdíl mezi axiomem výběru a hypotézou kontinua spočívá v tom, jak k této nezávislosti na ostatních axiomech matematici přistoupili. Zatímco u hypotézy kontinua se smířili s tím, že se holt nikdy nezjistí, jak to s ní „doopravdy“ je, axiom výběru uznali za natolik intuitivní a zřejmý, že jej zařadili mezi ostatní axiomy. Tento přístup není povinností – kdokoli si může zvolit svou sadu axiomů, kterou bude uznávat. Jde jen o všeobecně rozšířenou praxi, které se držíme i zde.

V tomto díle seriálu se axiomu výběru podíváme na zoubek. Dozvíš se, k čemu potřeba není, jak vypadá jeho takřka přehlédnutelné použití, jak s ním umravnit porovnávání mohutností, i jaké paradoxy[2] z něj jdou odvodit.

Co axiom výběru je a co není

Axiom výběru říká

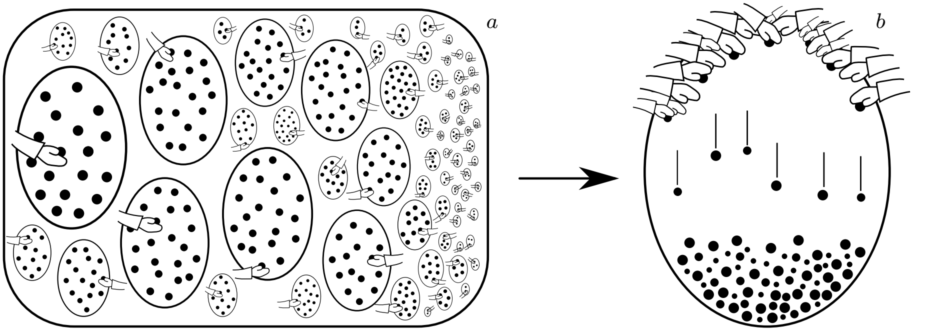
$$(\forall x \in a)(\forall y \in a)(x \neq y \Leftrightarrow x \cap y = \emptyset) \Rightarrow (\exists b)(\forall x \in a)(\exists y)(x \cap b = \{y\}).$$

Slovy: Kdykoli máme množinu a, jejíž prvky jsou navzájem disjunktní (tj. neprotínající se) neprázdné množiny, umíme vybrat z každého prvku x množiny a jednoho reprezentanta $y \in x$ a sestavit množinu reprezentantů b.

Laický, avšak výstižný popis axiomu výběru zní: **Lze provést nekonečně mnoho nahodilých výběrů najednou.** Je dobré si uvědomit, proč jsou v tomto popisu pojmy „nahodilý“ a „nekonečně mnoho“. Důvodem jsou následující dvě tvrzení, z nichž první říká „Nenahodilé výběry lze provádět i bez axiomu výběru.“ a druhé „Konečně mnoho výběrů lze taktéž provést bez axiomu výběru.“.

[1] Připomínáme, že hypotéza kontinua je výrok $|\omega_1| = |\mathbb{R}|$, který nelze dokázat ani vyvrátit. Ví se pouze, že $|\omega_1| \leq |\mathbb{R}|$.

[2] Zde myslíme překvapivá tvrzení, nikoli spor jako v případě Russelova paradoxu.



Tvrzení. *Pokud máme předpis (formuli), jak z jednotlivých množin $x \in a$ najít reprezentanta $y \in x$, plyne existence množiny reprezentantů z axiomu nahrazení.*

Axiom výběru je tedy potřeba jenom v případě, kdy takový předpis nemáme. Poznamenejme, že předpis máme například v situaci, kdy všechny množiny x obsahují přirozená (či obecněji ordinální) čísla. V takovém případě může předpis znít „vezmi nejmenší číslo z dané množiny".

Tvrzení. *Pokud je množina a konečná, lze najít množinu reprezentantů bez axiomu výběru. Axiom výběru tedy je třeba až v okamžiku, kdy je a nekonečná množina.*

Důkaz. Dokážeme to (obyčejnou, nikoli transfinitní) indukcí podle velikosti a. V okrajovém případě, kdy je a prázdná množina, je správnou odpovědí prázdná množina reprezentantů. Označme dále n počet prvků množiny a a předpokládejme, že lze najít množinu reprezentantů v každé $(n-1)$-prvkové množině. Dokážeme, že ji lze najít i v množině a. Uvažme jeden prvek x množiny a (existuje, protože a je neprázdná) a dále prvek $y \in x$ (existuje, protože x je neprázdná množina). Dále z indukčního předpokladu najdeme množinu b reprezentantů z $a \setminus \{x\}$. Kýžená množina reprezentantů pro a pak je například $b \cup \{y\}$. $\square$

Tento důkaz nelze transfinitně zobecnit, protože se v něm opíráme o indukční předpoklad na předchozím prvku, který u limitních ordinálů neexistuje. Pro následující tvrzení z minulého dílu již axiom výběru potřeba je.

Tvrzení. *Kdykoli máme spočetnou množinu X, jejíž prvky jsou spočetné množiny, tak i množina $\bigcup X$ je spočetná.*

Důkaz. Množina X je spočetná, takže existuje prostá funkce $f\colon X \to \omega$. Každý prvek $x \in X$ je spočetná množina, takže existuje prostá funkce $g_x\colon x \to \omega$. Abychom ukázali, že $Y = \bigcup X$ je spočetná množina, musíme ukázat, že existuje prostá funkce $g\colon Y \to \omega$. Pro $y \in Y$ vždy najdeme $x \in X$, které obsahuje prvek y. Pak definujeme

$$g(y) = 2^{f(x)} \cdot 3^{g_x(y)}.$$

Prostota funkce g vyplývá z jednoznačnosti prvočíselného rozkladu: Z hodnoty $g(y)$ jednoznačně určíme exponent u dvojky, a protože je f prostá funkce, můžeme určit i samotné x. Z exponentu u trojky (a na základě prostoty funkce g_x) nakonec určíme samotné y. $\square$

Kde byl potřeba axiom výběru? Jeden náznak vybírání v důkaze je, když si pro prvek y vybereme nějaké $x \in X$, které jej obsahuje. V tomto okamžiku ale axiom výběru nezbytný není – můžeme totiž napsat předpis, který x určí jednoznačně: Zvolíme x takové, pro které je $f(x)$ nejmenší možné. Možnost přiřadit každému $y \in Y$ příslušné $x \in X$ tedy plyne z axiomu nahrazení, jak jsme již uváděli.

Axiom výběru byl však klíčový v jiném momentě – když jsme volili funkce g_x. Možností, jak zobrazit x do ω, je nekonečně (a typicky nespočetně) mnoho. My jsme si však vybrali jen jednu, a to pro každý z prvků množiny X, kterých mohlo být nekonečně mnoho. Formální použití axiomu výběru by vypadalo třeba takto:

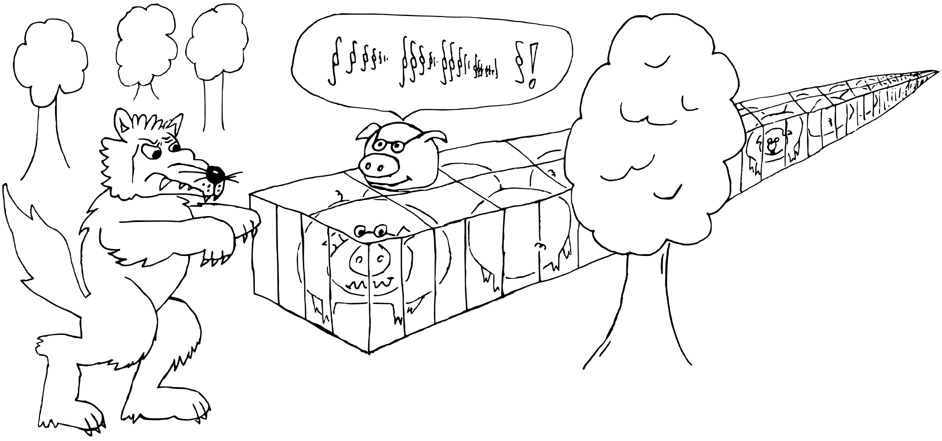
Nechť $G_x \subset \mathcal{P}(x \times \omega)$ je množina všech prostých zobrazení $x \to \omega$ pro $x \in X$. Jednotlivé množiny G_x jsou jednak neprázdné, protože všechny $x \in X$ jsou spočetné, a jednak disjunktní, protože z funkce lze poznat její definiční obor. Pak na $a = \{G_x : x \in X\}$ aplikujeme axiom výběru, čímž dostaneme množinu reprezentantů b. Nakonec definujeme g_x jako onen jediný prvek průniku $G_x \cap b$.

Opět by ale axiom výběru potřeba nebyl, kdybychom měli daný předpis pro funkce g_x. Popravdě se moc často nestává, že bychom měli spočetnou množinu spočetných množin a neměli při nich i seznam prostých funkcí do ω. Například v důkaze spočetnosti množiny $\mathbb{Q}$ se bez axiomu výběru obejdeme. Někdy se ale může stát, že o prvcích množiny víme, že jsou spočetné, ale nemáme předepsáno, jak – například ve druhém díle, když jsme dokazovali, že sjednocení spočetné množiny prvků ω_1 stále leží v ω_1.

Předešlé použití axiomu výběru působí neškodně a ukazuje, jak ho mohli matematici snadno přehlédnout. Je to také tím, že jsme axiom výběru použili jen na spočetnou množinu a, kde je ještě konstrukce příslušné množiny reprezentantů docela představitelná. Co je tedy na tom axiomu tak kontroverzního? Následující dva příklady již demonstrují moc axiomu výběru v plné síle.

Dobrodružství nekonečně mnoha prasátek

Před nekonečně mnoha lety, za nekonečně mnoha horami a řekami, potulovala se družinka nekonečně (ale spočetně) mnoha prasátek. Šla poklidně lesem a neměla ponětí, že na ně má spadeno zlý vlk. Na tuhle chvíli čekal už nekonečně dlouho – už dávno měl nachystanou past. Ještě kousek… A klap! Všechna prasátka byla v kleci.



„Tak, a teď vás všechna sním," liboval si vlk. Už měl rozpočítáno, jak sežere každý den nekonečně mnoho prasátek, a dokonce mu to vyjde na nekonečně mnoho dní. Ale prasátka nehodlala prodat svou kůži lacino. Jak jich bylo hodně, našlo se mezi nimi prasátko-právník, které dobře vědělo, proč je jezení prasátek nejen nesprávné, ale dokonce ilegální: „Podle paragrafu 58072 královy vyhlášky $\omega \cdot \omega + 5$ sbírky je konzumace sebeuvědomělých bytostí ztotožněna se skutkovou podstatou trestného činu vraždy, jak je uvedena v trestním zákoníku …" „Jaké sebeuvědomění?! Jste obyčejná prasata – zvířata!" čílil se vlk a už přehodnocoval své plány. Radši je všechna sežere už zítra, takovéhle diskuze nemá zapotřebí.

„Podle paragrafu ω téže vyhlášky je sebeuvědomělá bytost taková, která prokáže svou schopnost splnit úkol intelektuální podstaty…" sypalo ze sebe prasátko-právník. „Jó takhle," pomyslel si vlk

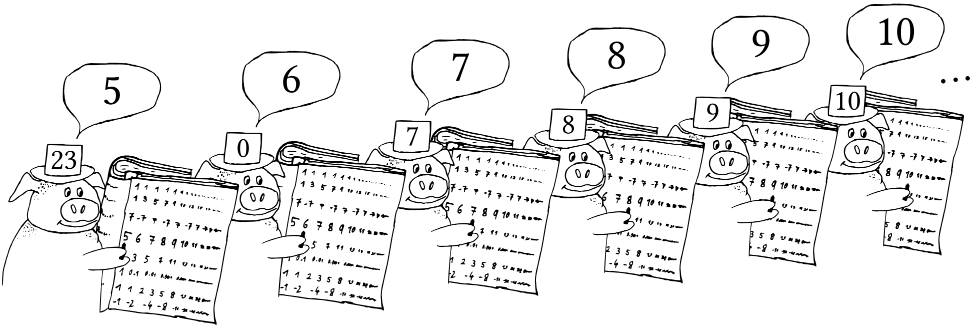
– na vymýšlení nesplnitelných úkolů byli pohádkoví záporáci vždy odborníky (nebo si to o sobě aspoň mysleli). Takto vypadal úkol pro prasátka: Další den se mají seřadit na přirozená čísla. Poté vlk na jejich hlavy posadí klobouky a každý klobouk bude mít barvu nějakého odstínu šedi (reálné číslo). Prasátka neuvidí barvu svého klobouku, jen barvy klobouků prasátek před sebou (stojících na vyšších přirozených číslech). Pak každé prasátko pošeptá vlkovi tip na barvu svého klobouku. Pokud se splete jen konečně mnoho prasátek, vlk je všechna pustí na svobodu. Jakmile se jich však zmýlí nekonečně mnoho, vlk všechna prasátka sežere. „Po právní stránce je vše v pořádku," vypísklo prasátko-právník a schoulilo se do kouta klece.

Každé jednotlivé prasátko v duchu uvažovalo: „Pokud vlk nasadí každému z nás klobouk náhodné barvy, nebude žádná cesta, jak by mi informace o barvách klobouků přede mnou mohla prozradit něco o tom, co mám já. Takže šance, že se strefím do náhodného reálného čísla bez sebemenší nápovědy, je nulová. Stejně tak mají nulovou šanci ostatní prasátka, tedy je mizivá pravděpodobnost, že se vůbec někdo strefí. A že bychom se měla strefit všechna s výjimkou konečně mnoha z nás? Tady už pomůže jedině zázrak…"

Někdo tomu říká zázrak, jiný axiom výběru. A protože bylo prasátek dohromady docela hodně, našlo se mezi nimi jedno, které na to přišlo. Za pomoci axiomu výběru se totiž v jakkoli náhodném rozestavění klobouků dá najít „pravidelnost", přesněji řečeno reprezentant.

Vlkovo rozdání klobouků interpretujeme jako funkci $f\colon \omega \to \mathbb{R}$, kde hodnota $f(n)$ určuje barvu klobouku prasátka stojícího na čísle n. Uvažme množinu M všech možných takových funkcí f. Dále řekneme, že dvě funkce $f, g \in M$ si jsou podobné (značíme $f \sim g$), pokud se liší jen na konečně mnoha pozicích. Nakonec pro $f \in M$ nazveme *ocasem funkce* f množinu $[f] = \{g \in M : g \sim f\}$.

Všimneme si, že kdykoli $g \in [f]$, tak je $[g] = [f]$. Z toho plyne, že jednotlivé ocasy funkcí jsou vždy buď stejné, nebo disjunktní. Na množinu $a = \{[f] : f \in M\}$ tak můžeme použít axiom výběru a získat množinu reprezentantů R. Množina R bude tvořit základ strategie prasátek – jednu takovou množinu reprezentantů R si prasátka vyberou a každé si ji napíše do notýsku.



Když vlk posadí klobouky podle funkce f, nebude sice žádné prasátko znát f, ale každému prasátku do znalosti f chybí jen konečně mnoho hodnot, takže každé prasátko bude znát její ocas $[f]$. V notýsku pak najde jediného reprezentanta $g \in [f] \cap R$, a stojí-li na přirozeném čísle n, pošeptá vlkovi $g(n)$. Takto se zmýlí jen konečně mnoho prasátek, protože $g \sim f$. Všimněme si, že kdyby bylo prasátek jen konečně mnoho, skutečně by se s největší pravděpodobností spletla všechna. Když jich ale je nekonečně mnoho, už se jich většina strefí. Barvu, kterou mají říct, určují pomocí klobouků, které vidí před sebou – i když je jasné, že „barvy jednotlivých klobouků spolu nijak nesouvisejí". To je první ze slibovaných paradoxů.

Neměřitelná množina

Další příklad použití axiomu výběru již není pohádkový, ale takový, na který matematici skutečně narazili. Přáli si zobecnit pojem obsahu a objemu a tento zobecněný obsah nazvali *míra*. Pro jednoduchost si to ukážeme na reálných číslech. Míra by měla být zobrazení, které podmnožině reálných čísel přiřadí číslo z $\mathbb{R}_0^+ \cup \{\infty\}$ udávající, „jak je tato množina dohromady dlouhá“. Matematici si usmysleli, že by po míře chtěli následující vlastnosti:

(i) Míra (neprázdného) otevřeného intervalu (a, b) je jeho délka $b - a$.
(ii) Pokud $A \subset B \subset \mathbb{R}$, tak je míra A menší nebo rovna míře B (prvek ∞ zde pokládáme za vyšší než všechna reálná čísla).
(iii) Pokud posuneme množinu $A \subset \mathbb{R}$ po reálné ose, neměla by se změnit její míra. Formálně řečeno je pro každé (pevné) reálné číslo r míra množiny $\{a + r : a \in A\}$ stejná jako míra množiny A.
(iv) Jsou-li $A, B \subset \mathbb{R}$ disjunktní množiny, dostaneme míru $A \cup B$ jako součet měr A a B.
(v) Sjednocení spočetně mnoha množin nulové míry je stále množina nulové míry.

Jsou tyto požadavky přirozené, či přehnané? Přinejmenším s axiomem výběru lze ukázat, že není možné je všechny splnit a definovat míru všem podmnožinám $\mathbb{R}$.

Pro reálné číslo x definujeme jeho *iracionální část* coby množinu $S_x = \{x+q : q \in \mathbb{Q}\}$. Všimněme si, že $x \in S_x$ a jakmile $y \in S_x$, tak $S_y = S_x$. Z toho plyne, že jednotlivé množiny S_x jsou vždy buď stejné, nebo disjunktní. Na množinu $\mathcal{S} = \{S_x : x \in \mathbb{R}\}$ tak můžeme použít axiom výběru. Ještě předtím ale každou z nich pronikneme s intervalem $(0, 1)$ – axiom výběru nám tak dá množinu reprezentantů $R \subset (0, 1)$. Množina R má tu vlastnost, že pokud ji posuneme o racionální číslo, získáme množinu disjunktní s původní. Na druhou stranu, pokud ji posuneme o všechna možná racionální čísla, pokryjeme celou reálnou osu. (Prvek x posunutý o všechna racionální čísla totiž pokryje celou množinu S_x.)

Jakou by ale množina R měla mít míru? Je podmnožinou intervalu $(0, 1)$, míra tedy bude rovna nejvýše jedné. Kdyby měla nulovou míru, pak by i každé její posunutí o racionální číslo mělo nulovou míru. Všech možných posunutí o racionální číslo je spočetně mnoho, takže i jejich sjednocení by mělo mít nulovou míru. To je ale spor – celá reálná osa nulovou míru jistě nemá (musí mít míru ∞).

Míra R tak musí být kladné číslo r. V intervalu $(0, 1)$ existuje nekonečně mnoho racionálních čísel – nám jich bude stačit konečně mnoho, víc než $\frac{2}{r}$. Posunutí množiny R o tato racionální čísla jsou navzájem disjunktními podmnožinami intervalu $(0, 2)$. Jejich sjednocení tak je také podmnožinou intervalu $(0, 2)$, ale míra tohoto sjednocení je větší než $r \cdot \frac{2}{r} = 2$. Opět jsme dostali spor, proto nemůžeme množině R přiřadit žádnou míru.

Poznámka. Když jsme popsali problém, tak i nastíníme, jak z něho ven. Matematici po míře stále požadují všechny zmíněné vlastnosti, ale již nepožadují, aby byla míra definovaná na všech podmnožinách $\mathbb{R}$. Musí být ale definovaná pro všechny „měřitelné množiny“, což jsou skoro jakékoli konstruktivně popsané množiny. Například je měřitelná i množina těch reálných čísel, která v desítkovém zápisu neobsahují číslici 2 na žádné prvočíselné pozici za desetinnou čárkou. Přesná definice měřitelných množin však přesahuje rámec tohoto seriálu.

Poznámka. Ve třírozměrném prostoru (formálně $\mathbb{R} \times \mathbb{R} \times \mathbb{R}$) lze jít ještě dál a rozdělit kouli na jen konečně mnoho (čtyři základní a několik pomocných pro doladění detailů) disjunktních množin, tyto množiny otočit a posunout a poskládat z nich dvě nové koule, obě stejně velké jako ta původní. Tento jev se nazývá Banach–Tarského paradoxem a demonstruje nemožnost zavedení objemu všech třírozměrných množin ještě silněji, než jsme předvedli zde pro míru na $\mathbb{R}$.

Tato použití axiomu výběru byla víceméně přímočará. Další zajímavosti se budou dít, když si budeme vybírat „postupně“. Napřed ale musíme umět takové postupné vybírání formálně uchopit.

Postupné vybírání

Postupné vybírání není nic nového, ostatně bylo použito již v prvním díle. Coby příklad ukážeme dvě jednoduchá tvrzení, která nejprve dokážeme ne zcela formálně, a následně se zamyslíme, jak by bylo možné tyto důkazy formalizovat. V další kapitole pak tato tvrzení rozšíříme do překvapivější podoby.

Tvrzení. (kritérium pro dobré uspořádání) *Nechť lineárně uspořádaná množina A je neprázdná a nelze v ní najít nekonečnou klesající posloupnost jejích prvků $x_0 > x_1 > x_2 > \cdots$. Pak má množina A nejmenší prvek.*

Důkaz. Pro spor předpokládáme, že A nemá nejmenší prvek, a najdeme v A nekonečnou klesající posloupnost. Zvolme první prvek x_0. Ten nemůže být nejmenší, najdeme tedy menší prvek $x_1 < x_0$. Ani x_1 nemůže být nejmenší, takže najdeme $x_2 < x_1$. Takto můžeme pokračovat stále, takže nakonec získáme nekonečnou klesající posloupnost $x_0 > x_1 > x_2 > \cdots$. □

Tvrzení. (minimalita ω mezi nekonečnými mohutnostmi) *Uvažme množinu X. Pak buď existuje bijekce mezi X a některým přirozeným číslem, nebo existuje nekonečná posloupnost různých prvků $x_0, x_1, \ldots$*

Důkaz. Budeme postupně volit x_n coby různé prvky množiny X. Nejprve zvolíme $x_0 \in X$, pak $x_1 \in X \setminus \{x_0\}$, $x_2 \in X \setminus \{x_0, x_1\}$, a tak dále. Pokud se v průběhu X vyprázdní, neboli nemůžeme zvolit $x_n \in X \setminus \{x_0, x_1, \ldots, x_{n-1}\}$, tak jsme právě popsali bijekci $n \to X$ a X je n-prvková konečná množina. V opačném případě se povede sestrojit celou nekonečnou posloupnost různých prvků $x_0, x_1, x_2, \ldots$ □

V obou případech jsme postupně sestrojili posloupnost prvků $x_0, x_1, \ldots$ Posloupnost coby objekt teorie množin by měla být množina (nebo přinejhorším třída). V tomto případě nazveme *posloupností* (prvků z Y délky X) zobrazení $X \to Y$, jehož definičním oborem je ordinál (nebo $\mathbb{O}n$,[3] v předešlých příkladech byla definičním oborem ω). Hodnoty posloupnosti značíme indexem x_n na rozdíl od běžného zobrazení, kde se značí závorkami $x(n)$.

Již v minulém díle jsme se setkali s posloupností ω_α délky $\mathbb{O}n$. Technicky jde téměř o třetí synonymum ke slovům zobrazení a funkce, rozdíl spočívá hlavně v intuitivním vnímání – zatímco funkci si člověk představí jako proces, jak z x vzniká $f(x)$, posloupnost si představí jako za sebou jdoucí prvky $x_0, x_1, x_2, \ldots$

Postupné definování jsme se už naučili provádět rekurzí. Jenže v předešlých dvou důkazech nemáme exaktní pravidlo pro výběr následujícího členu, a (transfinitní) rekurze stojí na tom, že známe následující prvek přesně. Jinak totiž není funkce daná rekurzivním předpisem jednoznačná. Tato jednoznačnost je navíc potřeba i pro důkaz existence – v limitním kroku. Opět není problém ukázat, že existuje odpovídající posloupnost délky n pro libovolné přirozené číslo n. Pokud si však začátky těchto posloupností neodpovídají, nedokážeme je skloubit do jedné nekonečné posloupnosti. V některých případech to ani nejde – například v přirozených číslech najdeme libovolně dlouhou konečnou klesající posloupnost, avšak nikoli nekonečnou.

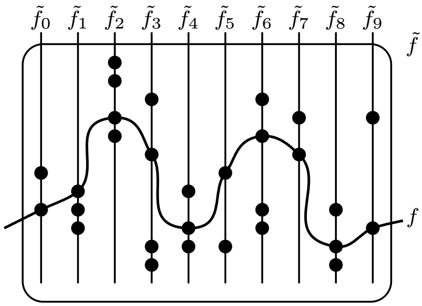
Řešením bude sestrojit ještě před spuštěním rekurze pomocnou funkci, se kterou již bude rekurzivní předpis jednoznačný.

Definice. Nechť X, Y jsou množiny. *Víceznačná funkce z X do Y* je množina $\tilde{f} \subset X \times Y$ taková, že $(\forall x \in X)(\exists y \in Y)\big((x, y) \in \tilde{f}\big)$. Od obyčejné funkce se tedy liší tím, že jednomu x může odpovídat více y.

Tvrzení. *Nechť $\tilde{f}$ je víceznačná funkce z X do Y. Pak existuje funkce $f\colon X \to Y$ taková, že $f \subset \tilde{f}$. Tento proces nazýváme vybráním funkce f z víceznačné funkce $\tilde{f}$.*

Důkaz. Pro $x \in X$ označme $\tilde{f}_x = \tilde{f} \cap (\{x\} \times Y)$ a dále $a = \{\tilde{f}_x : x \in X\}$. Protože je $\tilde{f}$ víceznačná funkce, je každá $\tilde{f}_x$ neprázdná, a proto můžeme na množinu a použít axiom výběru. Výsledkem bude funkce $f\colon X \to Y$ splňující $f \subset \tilde{f}$. □

[3] Připomínáme, že symbolem $\mathbb{O}n$ myslíme (vlastní) třídu všech ordinálů.



Cvičení 1. Nechť existuje (ne nutně prosté) zobrazení $f\colon A \to B$ takové, že každé $b \in B$ lze dostat jako nějaké $f(a)$ (říkáme, že f je *surjektivní* nebo též *na* B). Dokaž, že existuje prosté zobrazení $g\colon B \to A$.

Poznámka. Analogicky by bylo možné zavést i třídovou víceznačnou funkci, avšak v takovém okamžiku již axiom výběru nepostačuje k tomu, aby se z třídové víceznačné funkce vybrala třídová funkce. Pro takový výběr by byl potřeba tzv. *axiom silného výběru*, kterým se v tomto textu nebudeme zabývat.

Nyní můžeme důkazy obou tvrzení formalizovat.

Důkaz. (kritérium pro dobré uspořádání) Předpokládáme, že žádný prvek A není nejmenší. To znamená, že máme víceznačnou funkci $\tilde{f}$ z A do A, která každému $a \in A$ přiřadí menší prvky. Formálně

$$\tilde{f} = \{(x, y) : x \in A, y \in A, y < x\}.$$

Z víceznačné funkce $\tilde{f}$ vybereme funkci f, která každému prvku přiřadí nějaký menší prvek. Nakonec si zvolme jeden prvek $s \in A$ pro začátek a rekurzivně definujeme nekonečnou klesající posloupnost předpisem $x_0 = s$, $x_{n+1} = f(x_n)$. $\square$

Důkaz. (minimalita ω mezi nekonečnými mohutnostmi) Nechť STOP je prvek různý od všech prvků množiny X. Dále uvažme víceznačnou funkci $\tilde{f}$ z $\mathcal{P}(X)$ do $X \cup \{\text{STOP}\}$, která každé neprázdné množině přiřadí její prvky a prázdné množině přiřadí STOP. Formálně

$$\tilde{f} = \{(x, y) : x \in \mathcal{P}(X), y \in x\} \cup \{(\emptyset, \text{STOP})\}.$$

Vybereme z ní funkci f, ta každé neprázdné podmnožině množiny X přiřadí jeden její prvek a prázdné množině přiřadí STOP. Pak definujeme rekurzivně posloupnost $x_n = f(X \setminus \{x_i : i < n\})$. Speciálně vyjde $x_0 = f(X)$. Z vlastností funkce f budou x_n nejprve různé prvky množiny X a následně už jen samá STOP.

Mohou nastat dvě možnosti. Pokud je nějaké $x_n = \text{STOP}$, zvolme nejmenší takové n. Zúžení x na n je pak bijekce $n \to X$, takže je X konečná množina. V opačném případě jsme sestrojili nekonečnou posloupnost různých prvků. $\square$

Kombo axiomu výběru a transfinitní rekurze

Zatímco z formálního hlediska je mezi rekurzí a transfinitní rekurzí minimální rozdíl, jinak je tomu z pohledu lidské intuice. Možná sis u minulé kapitoly říkal(a), proč se už zase pipláme s dokazováním něčeho zřejmého, a kvůli formalismům to děláme malinko nešikovně a složitě. V této kapitole provedeme takřka stejné úvahy, jen namísto rekurze na přirozených číslech použijeme rekurzi na všech ordinálech.

Tím najednou místo banálních tvrzeníček získáme silné nástroje teorie množin – Zornovo[4] lemma a princip dobrého uspořádání. Jestli Ti budou jejich důkazy připadat aspoň zpola tak intuitivní jako v předchozí kapitole, seriál splnil své poslání ;-).

[4] Čti [cornovo]; taktéž je známé pod pojmem *princip maximality*.

Tvrzení. (Zornovo lemma) *Mějme množinu X. O množině $\mathcal{R} \subset \mathcal{P}(X)$ řekneme, že se jedná o řetězec, pokud pro každé dvě množiny $A, B \in \mathcal{R}$ platí $A \subset B$ nebo $B \subset A$.*

Nechť $\mathcal{S} \subset \mathcal{P}(X)$ je neprázdná množina splňující následující podmínku: Pro každý řetězec $\mathcal{R} \subset \mathcal{S}$ platí $\bigcup \mathcal{R} \in \mathcal{S}$. Pak existuje maximální množina $M \in \mathcal{S}$. (Maximální množinou rozumíme takovou, že pro žádnou jinou množinu $A \in \mathcal{S}$ neplatí $M \subset A$.)

Navíc můžeme volit $M \supset Y$ pro předem zvolenou $Y \in \mathcal{S}$.

Důkaz. Pro spor předpokládejme, že taková maximální množina neexistuje. To znamená, že kdykoli uvážíme množinu $M \in \mathcal{S}$, najdeme její vlastní[5] nadmnožinu $A \in \mathcal{S}$. Z víceznačné funkce vybereme funkci $f\colon \mathcal{S} \to \mathcal{S}$, která každé množině z $\mathcal{S}$ přiřadí nějakou vlastní nadmnožinu z $\mathcal{S}$. Dále víme, že $\mathcal{S}$ je neprázdná, vezměme si tedy prvek $Y \in \mathcal{S}$ a definujme posloupnost S_α délky $\mathbb{O}n$ rekurzivním předpisem:

(i) $S_0 = Y$,
(ii) $S_{\alpha+1} = f(S_\alpha)$,
(iii) $S_\alpha = \bigcup\{S_\beta : \beta \in \alpha\}$ pro α limitní.

Slovy řečeno vystartujeme na Y a na izolovaných ordinálech skáčeme na nadmnožiny pomocí funkce f. Na limitním ordinálu si všimneme, že jsme dosud prošli řetězec prvků z $\mathcal{S}$, můžeme tedy použít jeho sjednocení. Takto jsme definovali rostoucí posloupnost S_α různých prvků z $\mathcal{S}$. Představíme si inverzní zobrazení k posloupnosti S_α – takové, které prvek S_α pošle na ordinál α. Pomocí něj a axiomu nahrazení z množiny $\mathcal{S}$ sestrojíme množinu všech ordinálních čísel, což je spor, protože $\mathbb{O}n$ tvoří vlastní třídu. $\square$

Poznámka. Důkaz je v pořádku, ale protože jsme se v seriálu příliš nevěnovali transfinitní rekurzi na všech ordinálech, předvedeme ještě, jak by bylo možné využití třídy všech ordinálů obejít. Zvolme množinu γ všech typů dobře uspořádaných řetězců v $\mathcal{S}$ (uspořádání stále chápeme tak, že větší prvek znamená nadmnožinu). To je množina ordinálních čísel, která s každým ordinálním číslem obsahuje i všechna menší, tedy je to ordinál. Nyní namísto rekurze na $\mathbb{O}n$ spustíme rekurzi jen na ordinálu γ. Posloupnost S_α nám dá rostoucí bijekci mezi γ a řetězcem v $\mathcal{S}$. Z toho plyne, že typ tohoto řetězce je γ, z čehož plyne spor $\gamma \in \gamma$.

Příklad. Nechť A, B jsou disjunktní množiny. Pak existuje prostá funkce $A \to B$ nebo $B \to A$.

Důkaz. Označme $\mathcal{S}$ množinu všech takových množin S, které obsahují navzájem disjunktní dvojice tvaru $\{a, b\}$, kde $a \in A$, $b \in B$. Ukážeme, že $\mathcal{S}$ splňuje podmínku Zornova lemmatu. Je třeba ověřit, že když uvážíme řetězec $\mathcal{R} \subset \mathcal{S}$ a sjednotíme jej $R = \bigcup \mathcal{R}$, budou stále všechny dvojice z R navzájem disjunktní. Pro spor předpokládejme, že v R leží dvě dvojice $d_0 = \{a_0, b_0\}$, $d_1 = \{a_1, b_1\}$, které se protínají. Protože je R sjednocením řetězce $\mathcal{R}$, musí v $\mathcal{R}$ ležet množiny R_0, R_1 takové, že $d_0 \in R_0$, $d_1 \in R_1$. Protože je $\mathcal{R}$ řetězec, nastane $R_0 \subset R_1$ nebo $R_1 \subset R_0$. Větší z těchto množin tak musí obsahovat obě dvojice d_0, d_1, což je spor s tím, že tato větší množina leží v $\mathcal{S}$. Tím je podmínka Zornova lemmatu ověřena.

Proto z Zornova lemmatu najdeme maximální množinu $M \in \mathcal{S}$. Pak musí $\bigcup M$ pokrýt celou A nebo celou B. V opačném případě bychom totiž mohli vzít $a \in A \setminus \bigcup M$, $b \in B \setminus \bigcup M$ a zvětšit M přidáním dvojice $\{a, b\}$. Pokud pokryje celou A, definujeme prostou funkci $f\colon A \to B$ tak, že každému $a \in A$ přiřadíme to $b \in B$, které je s ním ve dvojici. Pokud nastane druhá možnost, definujeme analogicky $f\colon B \to A$.

V kapitole o kardinálních číslech dostaneme předešlý výsledek znovu a v silnější podobě. Na následujících cvičeních si můžeš podobné použití Zornova lemmatu samostatně vyzkoušet.

Cvičení 2. Dokaž, že existuje systém množin $\mathcal{S} \subset \mathcal{P}(\omega)$ splňující následující dvě podmínky:

(i) Pro každou nekonečnou množinu $X \subset \omega$ existuje $S \in \mathcal{S}$ taková, že $X \cap S$ je nekonečný.
(ii) Průnik každých dvou různých množin z $\mathcal{S}$ je konečný.

[5] Vlastní nadmnožinou myslíme jen to, že má být různá od původní M.

Cvičení 3. Dokaž axiom výběru zpětně z Zornova lemmatu.

Poznámka. Na základě předešlého cvičení se někdy označuje Zornovo lemma (stejně jako následující princip dobrého uspořádání) za ekvivalent axiomu výběru. Zornovo lemma je sice netriviální věta, ale je shodou okolností natolik obecná, že z ní vyplývá nějaký axiom.

Tvrzení. (Princip dobrého uspořádání) *Pro každou množinu X lze najít uspořádání $U \subset X \times X$ takové, aby (X, U) tvořila DUMu.*

Poznámka. V důkaze použijeme stejný argument se třídou všech ordinálních čísel jako v důkaze Zornova lemmatu. Stejně jako předtím lze tento argument obejít – místo $\mathbb{O}n$ by stačila množina typů všech DUM (Y, U'), kde $Y \subset X$ a U' tvoří na Y dobré uspořádání.

Důkaz. Stačí ukázat, že existuje posloupnost x_α (nějaké délky), která obsahuje každý prvek množiny X právě jednou. Uspořádání pak vyčteme z ordinálů skrze bijektivní posloupnost x_α, tedy stanovíme $x_\alpha < x_\beta$ pro $\alpha < \beta$. Zbývá najít takovou posloupnost.

To provedeme tak, že se pokusíme definovat posloupnost délky $\mathbb{O}n$ předpisem: „Vezmi libovolný dosud nepoužitý prvek $x_\alpha \in X$." Formálně to provedeme úplně stejně jako v důkaze minimality ω. Pomocí axiomu výběru sestrojíme funkci $f\colon \mathcal{P}(X) \to X \cup \{\mathrm{STOP}\}$, která pro všechny neprázdné množiny $Y \subset X$ splňuje $f(Y) \in Y$ a $f(\emptyset) = \mathrm{STOP}$, přičemž STOP je prvek neležící v X. Následně rekurzivně definujeme posloupnost $x_\alpha = f(X \setminus \{x_\beta : \beta \in \alpha\})$. Jen se nezastavíme na ω, ale pokračujeme přes všechny ordinály. Pokud jsme někdy dostali $f(\alpha) = \mathrm{STOP}$, stačí zvolit nejmenší takové α a dostáváme po zúžení na α kýženou bijektivní posloupnost.

Zbývá ukázat, proč se nemohlo stát, že bychom každému ordinálnímu číslu přiřadili nějaký prvek X. V takovém případě bychom totiž měli posloupnost délky $\mathbb{O}n$, jejíž prvky jsou různé a všechny leží v jedné množině. To je stejně jako v důkaze Zornova lemmatu ve sporu s tím, že $\mathbb{O}n$ tvoří vlastní třídu. □

Cvičení 4. Dokaž axiom výběru zpětně z principu dobrého uspořádání.

Poznámka. Tímto cvičením máme trojici ekvivalentních podmínek kompletní. Je tedy jedno, jestli si k původním axiomům (0) až (8) přidáme axiom výběru, Zornovo lemma, či princip dobrého uspořádání, výsledek bude stejný. Za axiom ale běžně považujeme axiom výběru ze dvou důvodů. Zaprvé k jeho vysvětlení stačí ty nejzákladnější pojmy a mohli jsme jej formulovat už mezi axiomy, kdy jsme ještě ani neměli formálně definovanou funkci, natožpak řetězec či dobré uspořádání.

Druhým důvodem je, že axiom výběru vypadá jako něco, co by podle intuice vážně mělo platit. Zato princip dobrého uspořádání působí spíše opačným dojmem – už na těch nejjednodušších nespočetných množinách, například $\mathbb{R}$ nebo $\mathcal{P}(\omega)$, je dobré uspořádání nepředstavitelné. Drobné vodítko sice dávají nespočetné ordinály $\omega_1, \omega_2, \ldots$, je ale zrada, že se ani nedá dokázat (a dokonce se dá dokázat, že se nedá dokázat), jestli má $\mathbb{R}$ mohutnost stejnou jako ω_1, nebo ω_2, nebo dokonce mnohem větší než všechna takhle sestrojitelná ordinální čísla.

A co se týče Zornova lemmatu, jak naznačuje úvodní motto, jedná se o příliš abstraktní nástroj na to, aby se dalo na základě intuice říci, zda by mělo, nebo nemělo platit. V jednoduchých případech působí celkem uvěřitelně, ve složitějších (jako v následujícím cvičení či v příští kapitole) už to zdaleka tak jasné není.

Cvičení 5. Dokaž princip dobrého uspořádání pomocí Zornova lemmatu místo transfinitní rekurze s axiomem výběru.

Ve zbytku seriálu si předvedeme, k čemu všemu se uvedené dva nástroje dají použít.

Netriviální řešení Cauchyho rovnice

Jako příklad použití Zornova lemmatu si předvedeme skutečné řešení následující slavné funkcionální rovnice.

Úloha. (Cauchyho rovnice) Nalezněte všechny funkce $f\colon \mathbb{R} \to \mathbb{R}$ splňující pro každou dvojici čísel $x, y \in \mathbb{R}$ rovnici

$$f(x) + f(y) = f(x + y).$$

Zřejmě tuto rovnici splňují funkce $f(x) = 0$, $f(x) = x$ a obecně $f(x) = cx$, kde $c \in \mathbb{R}$ je konstanta. Ale jsou všechny funkce splňující zadanou rovnici takového tvaru?

Dosazováním různých hodnot za x a y můžeš dospět k tomuto výsledku:

Cvičení 6. Ukaž, že každá funkce f, která vyhovuje Cauchyho rovnici, splňuje pro každou dvojici čísel $q \in \mathbb{Q}$, $x \in \mathbb{R}$ rovnost $f(qx) = qf(x)$.

Pro reálná čísla q už taková rovnost platit nemusí. Při sebechytřejším dosazování za x, y do Cauchyho rovnice se například nepovede odvodit žádný vztah mezi hodnotami $f(1)$ a $f(\sqrt{2})$. Tyto hodnoty jsou totiž na sobě skutečně nezávislé – když zvolíme libovolně hodnoty $f(1)$ a $f(\sqrt{2})$, stále půjde najít příslušné řešení Cauchyho rovnice.

Není ale snadné takové řešení sestrojit. Abychom to dokázali, musíme umět tuto nezávislost formálně uchopit. K tomu použijeme aparát lineární algebry. Lineární algebra pracuje s vektory x_i, s jejich násobky $\alpha_i x_i$ a s jejich konečnými součty, které jsou obecně ve tvaru

$$\alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n.$$

Koeficienty α_i se berou z množiny skalárů, což bude v našem příkladě množina $\mathbb{Q}$. Vektory budou v našem příkladě (poněkud neobvykle) prvky množiny $\mathbb{R}$. Výše uvedený vzorec se (zhruba) nazývá lineární kombinace vektorů. Přesněji chápeme *lineární kombinaci* jako přiřazení koeficientů α_i konečně mnoha reálným číslům (vektorům). Přitom si můžeme představovat, že všem ostatním reálným číslům přidělíme nulový koeficient. *Vyhodnocení* lineární kombinace pak spočteme pomocí vzorce uvedeného výše. Nyní zavedeme přesné definice.

Definice. Mějme množinu $X \subset \mathbb{R}$.

(i) *Lineární kombinace* prvků množiny $X \subset \mathbb{R}$ je zobrazení $k\colon X \to \mathbb{Q}$, které je nenulové jen v konečně mnoha bodech.

(ii) Dvě lineární kombinace k_0, k_1 můžeme sčítat nebo odčítat. Součtem / rozdílem $k = k_0 \pm k_1$, rozumíme lineární kombinaci danou předpisem $k(x) = k_0(x) \pm k_1(x)$. Povšimneme si, že stačí vykonat tuto práci jen v konečně mnoha bodech, ostatní hodnoty zůstávají nulové.

(iii) *Vyhodnocení* lineární kombinace k značíme $k(X)$ a spočteme jej coby součet všech konečně mnoha $k(x) \cdot x$, kde $x \in X$ a $k(x) \neq 0$.

(iv) O lineární kombinaci k řekneme, že je *triviální*, pokud je $k(x) = 0$ pro všechna $x \in X$. Všechny ostatní lineární kombinace nazýváme *netriviální*. Triviální lineární kombinace se vždy vyhodnotí na nulu.

(v) O množině $X \subset \mathbb{R}$ řekneme, že je *lineárně závislá*, pokud se některé dvě různé lineární kombinace jejích prvků vyhodnotí stejně. V opačném případě říkáme, že je X *lineárně nezávislá.*

Příklad. Jednoprvková množina je lineárně závislá právě tehdy, když je její prvek nulový. Dvouprvková množina je lineárně závislá právě tehdy, když je podíl jejích prvků racionální číslo.

Příklad. Množina $X = \{1, \sqrt{2}, \sqrt{8} - 1\}$ je lineárně závislá, protože lineární kombinace k_0 daná předpisem $k_0(\sqrt{8} - 1) = 1$ (a na zbytku nula) se vyhodnotí stejně jako lineární kombinace daná předpisem $k_1(1) = -1$, $k_1(\sqrt{2}) = 2$ (a jinak nula):

$$k_0(X) = 1 \cdot (\sqrt{8} - 1) = 2\sqrt{2} - 1 = -1 \cdot (1) + 2 \cdot (\sqrt{2}) = k_1(X).$$

Na druhou stranu například nekonečné množiny $\{\sqrt{n} : n \text{ je bezčtvercové}[6] \text{ číslo}\}$ nebo $\{e^n : n \in \omega\}$ lineárně nezávislé jsou.

---

[6] Bezčtvercová jsou ta přirozená čísla, která nejsou dělitelná žádnou druhou mocninou celého čísla vyšší než 1.

Důkazy, že uvedené dvě množiny jsou lineárně nezávislé, by vyžadovaly nemalé množství další teorie. Pro následující jednodušší verzi stačí vědět, že $\sqrt{n}$ je za předpokladu, že n není druhou mocninou přirozeného čísla, iracionální číslo.

Cvičení 7. Dokaž, že množiny $\{1, \sqrt{2}\}$ a $\{1, \sqrt{2}, \sqrt{3}\}$ jsou lineárně nezávislé.

Učiníme ještě jedno pozorování: Pokud existují dvě různé lineární kombinace k_0, k_1 se stejným vyhodnocením, jejich odečtením sestrojíme jinou než triviální lineární kombinaci $k = k_0 - k_1$, která se vyhodnotí na nulu. Lineární závislost tedy lze popsat výrokem: „I některá netriviální lineární kombinace se vyhodnotí na nulu."

Příklad. Aplikujeme-li toto pozorování na předchozí příklad lineárně závislé množiny, dostáváme netriviální lineární kombinaci k s předpisem $k(1) = 1, k(\sqrt{2}) = -2, k(\sqrt{8} - 1) = 1$. Ta se vyhodnotí na nulu:

$$1 \cdot 1 - 2 \cdot \sqrt{2} + 1 \cdot (\sqrt{8} - 1) = 0.$$

Nechť $\mathcal{S} \subset \mathcal{P}(\mathbb{R})$ je množina všech lineárně nezávislých množin. Ukážeme, že $\mathcal{S}$ splňuje podmínku Zornova lemmatu: Uvažme řetězec $\mathcal{R} \subset \mathcal{S}$ lineárně nezávislých množin. Předpokládejme pro spor, že $\bigcup \mathcal{R}$ je lineárně závislá množina, existuje tedy netriviální lineární kombinace $k \colon \bigcup \mathcal{R} \to \mathbb{Q}$, která se vyhodnotí na nulu. Funkce k smí být nenulová jen v konečně mnoha bodech, označme je $x_0, x_1, \ldots, x_{n-1}$. Tyto prvky leží v množině $\bigcup \mathcal{R}$, proto najdeme množiny $R_0, R_1, \ldots, R_{n-1} \in \mathcal{R}$ tak, aby $x_i \in R_i$. Vezmeme největší z množin R_i, a ta již musí obsahovat všechny $x_0, \ldots, x_{n-1}$. To ale znamená, že ani tato $R_i \in \mathcal{R}$ nebyla lineárně nezávislá. Dostáváme spor, takže podmínka Zornova lemmatu platí.

Nyní použijeme Zornovo lemma a najdeme maximální lineárně nezávislou množinu M. Prozkoumejme její vlastnosti. Ukážeme, že každé reálné číslo lze získat vyhodnocením právě jedné lineární kombinace prvků M. Protože je M lineárně nezávislá, nebude existovat více kombinací, které se vyhodnotí stejně. Zbývá ukázat, že pro každé číslo $t \in \mathbb{R}$ najdeme odpovídající lineární kombinaci. Kdyby t již leželo v M, stačí lineární kombinace, která t přiřadí jedničku a zbytku nuly. Dále předpokládáme $t \notin M$. Protože je M maximální, nemůže být $M \cup \{t\}$ lineárně nezávislá, existuje tedy netriviální lineární kombinace k, která se vyhodnotí na nulu. Musí ale $k(t) \neq 0$, jinak by ani M nebyla lineárně nezávislá. Pak i lineární kombinace $k_1(x) = -k(x)/k(t)$ se vyhodnotí na nulu a $k_1(t) = -1$. Tedy lineární kombinace[7] $k_1 \restriction M$ prvků množiny M se vyhodnotí na t.

Množině M s vlastností „každé reálné číslo lze reprezentovat právě jedním způsobem jako vyhodnocení lineární kombinace prvků množiny M" budeme říkat *báze.* Zatím jsme pomocí Zornova lemmatu ukázali, že lze najít nějakou bázi.

Cvičení 8.

(i) Ukaž, že žádná báze neobsahuje nulu.
(ii) Ukaž, že každá báze může obsahovat nejvýše jedno racionální číslo.
(iii) Ukaž, že existuje báze, která neobsahuje žádné racionální číslo.

Cvičení 9.

(i) Ukaž, že báze musí mít alespoň dva prvky.
(ii) Ukaž, že báze musí být nespočetná.

Konečně se dostáváme k řešení Cauchyho rovnice.

Tvrzení. *Mějme bázi M a funkci $f_0 \colon M \to \mathbb{R}$. Pak f_0 lze právě jedním způsobem rozšířit na funkci $f \colon \mathbb{R} \to \mathbb{R}$ tak, aby f splňovala Cauchyho rovnici.*

Důkaz. Pro lineární kombinaci k prvků M označme jako $k \cdot f_0$ součet všech $k(x) f_0(x)$, kde $x \in M$ a $k(x) \neq 0$. To si lze představovat jako „vyhodnocení k až poté, co X upravíme funkcí f_0". Dále

[7] Značením $k_1 \restriction M$ rozumíme zúžení funkce k_1 na množinu M. V tomto případě tedy jen zahodíme hodnotu -1 v bodě t.

pro $x \in \mathbb{R}$ označme k_x tu jedinou lineární kombinaci, která splňuje $k_x(M) = x$. Ukážeme, že jednoznačné rozšíření funkce f je

$$f(x) = k_x \cdot f_0. \tag{$\star$}$$

Rovnost ($\star$) musí platit pro $x \in M$ – pak je totiž k_x definována předpisem $k_x(x) = 1$ a na zbytku nula, tedy $k_x \cdot f_0 = f_0(x)$. Protože každá funkce splňující Cauchyho rovnici musí splňovat $f(qx) = qf(x)$ pro $q \in \mathbb{Q}, x \in \mathbb{R}$, musí rovnost ($\star$) platit i pro $x = mq$, kde $m \in M, q \in \mathbb{Q}$. Nakonec díky vztahu $f(x+y) = f(x) + f(y)$ musí být rovnice ($\star$) splněna pro vyhodnocení všech lineárních kombinací prvků M, tedy pro všechna reálná čísla.

Zbývá ověřit, že funkce daná předpisem ($\star$) splňuje Cauchyho rovnici. K tomu si uvědomíme, že lineární kombinace se dají roznásobovat a vytýkat. Uvážíme-li $x, y \in \mathbb{R}$, platí $k_x(M) = x$ a $k_y(M) = y$, a tak i $(k_x + k_y)(M) = x + y$. Z toho plyne $k_{x+y} = (k_x + k_y)$. Obdobně také platí $(k_x + k_y) \cdot f_0 = k_x \cdot f_0 + k_y \cdot f_0$. Dohromady dostáváme

$$f(x + y) = k_{x+y} \cdot f_0 = (k_x + k_y) \cdot f_0 = k_x \cdot f_0 + k_y \cdot f_0 = f(x) + f(y). \qquad \square$$

Právě dokázané tvrzení odpovídá na otázku, jak vypadají všechna řešení Cauchyho rovnice. Mějme pevně zvolenou bázi M. Pak každé řešení Cauchyho rovnice je jednoznačně určeno svými hodnotami na M, přičemž tyto hodnoty lze volit libovolně. S tímto pohledem již není těžké sestrojit jiné řešení než $f(x) = cx$, stačí, aby hodnoty v prvcích báze nesplňovaly tento předpis.

Předvedeme ještě trochu konkrétnější příklad takového řešení Cauchyho rovnice. Při použití Zornova lemmatu jsme mohli začít s libovolnou lineárně nezávislou množinou, tedy například $\{1, \sqrt{2}\}$. Získáme tedy bázi obsahující tato dvě čísla. Pak definujeme $f_0(1) = 1$ a $f_0(x) = 0$ pro $x \in M \setminus \{1\}$. Když takovou f_0 rozšíříme na řešení f, bude platit $f(1) = 1$ a $f(\sqrt{2}) = 0$, tedy určitě toto řešení není tvaru $f(x) = cx$. Můžeme se ještě zeptat, jakou hodnotu má $f(\sqrt{3})$. Sice víme, že všechny ostatní prvky báze mají nulovou hodnotu, ale nevíme (dosud jsme si to nezvolili, protože nám to bylo jedno), jestli $\sqrt{3}$ leží v bázi. Pokud ano, tak $f(\sqrt{3}) = 0$. Pokud ale místo $\sqrt{3}$ leží v bázi například číslo $\sqrt{3} - 1$, máme hodnotu $f(\sqrt{3}) = f(1) + f(\sqrt{3} - 1) = 1 + 0 = 1$.

Vidíme, že při konstrukci netriviálního řešení Cauchyho rovnice máme ohromnou volnost, co si lze zvolit. Rozhodně se nedá říct, že by bylo těžké najít netriviální řešení, protože by byla příliš vzácná. Spíše naopak – je jich příliš mnoho a volnost je příliš velká na to, aby se do nich dalo systematicky proniknout. A to jsou přesně ty chvíle, kdy pomáhá axiom výběru.

Cvičení 10.

(i) Najdi alespoň tři řešení Cauchyho rovnice splňující navíc $f(f(x)) = x$ pro všechna $x \in \mathbb{R}$.
(ii) Najdi nějaké řešení Cauchyho rovnice splňující navíc $f(f(1)) = -1$.
(iii) Ukaž, že bázi lze popárovat, tedy rozložit na množinu disjunktních dvojic.
(iv) Najdi nějaké řešení Cauchyho rovnice splňující navíc $f(f(x)) = -x$ pro všechna reálná x.
(v) Najdi nějaké řešení Cauchyho rovnice, které je prosté, ale není bijekce $\mathbb{R} \to \mathbb{R}$.

Kardinální čísla – mohutnosti množin

Při definici ordinálního čísla jsme z obecné DUMy sestrojili množinu stejného typu, která nezávisela na nosné množině původní DUMy. Podobně bychom chtěli popsat nějaké množiny, které budou reprezentovat mohutnosti obecných množin. Jenže jaké si vymyslet „obecné prvky“ množiny?

Snadno se obecné prvky popsat nedají, a proto se na mohutnosti jde malinko oklikou – přes ordinální čísla. Díky principu dobrého uspořádání dokážeme na jakékoli množině X najít dobré uspořádání U. To znamená, že X má stejnou mohutnost jako $\mathrm{typ}(X, U)$. Jenže různá ordinální čísla mohou mít stejnou mohutnost – například $|\omega| = |\omega \cdot \omega + 5|$. Vybereme proto jen některá ordinální čísla.

Definice. *Kardinální číslo* (stručně kardinál) je nejmenší ordinální číslo své mohutnosti. Jde tedy o takové ordinální číslo α, že pro žádné $\beta < \alpha$ neplatí $|\beta| = |\alpha|$.

Kardinální číslo vypadá jako nový pojem, ale ve skutečnosti jsi „všechna“ kardinální čísla už potkal(a) v minulém díle. Za prvé jde o přirozená čísla, která udávají mohutnosti konečných množin, a za druhé jde o ordinály ω_α pro $\alpha \in \mathbb{O}n$, což jsou všechny nekonečné kardinály. Dokážeme si jejich základní vlastnosti.

Tvrzení. *Nechť α je kardinál a $\beta < \alpha$ je ordinál. Pak $|\beta| < |\alpha|$.*

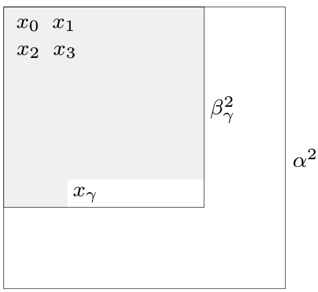
Důkaz. Na základě definice porovnávání mohutností potřebujeme ověřit dvě podmínky. Jednak, že $|\beta| \leq |\alpha|$, a za druhé, že neexistuje prosté zobrazení $\alpha \to \beta$. První část snadno plyne z toho, že $\beta \subset \alpha$. Ve druhé pro spor předpokládejme prostou funkci $f\colon \alpha \to \beta$. Množina $X = \{f(x) : x \in \alpha\}$ je pak podmnožinou ordinálu β, takže $\mathrm{typ}(X, \in) \leq \beta < \alpha$. Jenže $|\mathrm{typ}(X, \in)| = |X| = |\alpha|$, což je ve sporu s tím, že α je nejmenší ordinální číslo své mohutnosti. □

Tvrzení. *Pro každé nekonečné ordinální číslo α platí $|\alpha| = |\alpha \times \alpha|$.*

Důkaz. Množinu $X \times X$ budeme stručně značit X^2. Tvrzení dokážeme indukcí přes nekonečné ordinální číslo α. Pokud není α kardinální číslo, tak existuje menší ordinál $\beta < \alpha$ stejné mohutnosti, pro který platí $|\beta| = |\beta^2|$. Proto i $|\alpha| = |\alpha^2|$.

Když α je kardinálem, ukážeme napřed $|\beta^2| < |\alpha|$ pro všechna $\beta < \alpha$. Pro konečná β je tomu tak proto, že i β^2 je konečná množina. Je-li β nekonečné ordinální číslo, plyne z indukčního předpokladu $|\beta^2| = |\beta|$ a z předchozího tvrzení $|\beta| < |\alpha|$, celkem $|\beta^2| < |\alpha|$. Ještě si uvědomíme, že kvůli tomu musí být α limitní ordinál – pro $\beta < \alpha$ a větší než jedna totiž $|\beta^2| \geq |\beta + 1|$, a tak $\beta + 1 < \alpha$.

Nyní pro kardinál α dokážeme $|\alpha^2| = |\alpha|$. Postupně budeme vybírat z množiny α^2 vzájemně různé prvky a sestavíme z nich posloupnost délky α. Budeme ji značit x_γ a vybírání bude založeno na následujícím předpisu. Uvažme $\gamma \in \alpha$. Protože $|\gamma| < |\alpha| \leq |\alpha^2|$, nejsou dosud v posloupnosti všechny prvky α^2. Protože je navíc α limitní, najdeme $\beta_\gamma < \alpha$ takové, že v posloupnosti dosud chybí některý prvek množiny β_γ^2, přičemž volíme β_γ nejmenší možné. Prvek x_γ pak volíme z množiny β_γ^2.



Takto popsaná posloupnost musí projít všechny prvky α^2. Kdyby ne, neprošla by ani všechny prvky součinu β^2 pro nějaké $\beta < \alpha$. Tím bychom dostali prosté zobrazení $\alpha \to \beta \times \beta$, které nemůže existovat. Posloupnost x_γ tak tvoří bijekci $\alpha \to \alpha^2$. □

Poznámka. V důkaze jsme nepopsali přesně, v jakém pořadí prvky α^2 bereme, takže se může zdát, že jsme potřebovali použít axiom výběru. V tomto případě však není nutný, protože na α^2 máme dobré uspořádání, které může s vybíráním dalšího prvku pomoci.

Definice. Nechť X je množina. Pak díky principu dobrého uspořádání existuje alespoň jedno ordinální číslo stejné mohutnosti jako X. Protože je třída ordinálních čísel dobře uspořádaná, najdeme mezi nimi to nejmenší – jediné kardinální číslo této mohutnosti. Toto kardinální číslo nazýváme *mohutností* X a značíme $|X|$. Kardinální číslo $|\mathcal{P}(\omega)|$ budeme nazývat *kontinuum* a značit $\mathfrak{c}$. Tento kardinál je významný i proto, že udává mohutnost množiny $\mathbb{R}$.

Poznámka. Definice výrazů $|X| < |Y|$ a $|X| \leq |Y|$ nyní vypadá na první pohled nejednoznačně – jednak se může jednat o dosud používané porovnávání mohutností zavedené v prvním díle, současně může jít o porovnání odpovídajících kardinálů coby ordinálních čísel. První tvrzení v této kapitole ale přímo říká, že v případě, když X, Y jsou kardinály, je porovnávání přes ordinály i přes mohutnosti totožné. Následně lze tuto skutečnost rozšířit na obecné množiny, protože množiny X a $|X|$ mají stejnou mohutnost (ve smyslu původní definice).

Když jsme převedli porovnávání mohutností na porovnávání ordinálů, snadno již pro libovolné množiny X, Y dostáváme:

(i) Pokud $|X| \leq |Y|$ a $|Y| \leq |X|$, tak $|X| = |Y|$.
(ii) Platí $|X| \leq |Y|$ nebo $|Y| \leq |X|$.
(iii) Jsou-li X, Y nekonečné množiny, platí $|X \times X| = |X|$. Obecněji $|X \times Y| = \max(|X|, |Y|)$.

Díky tomu skoro všechny „normální" geometrické objekty – křivka, obdélník, sféra, apod. – obsahují kontinuum bodů. Každý z nich je totiž podmnožinou $\mathbb{R}^2$ resp. $\mathbb{R}^3$, takže má mohutnost nejvýše kontinuum. Současně do takového objektu lze zobrazit prostou funkcí interval, takže má mohutnost alespoň kontinuum.

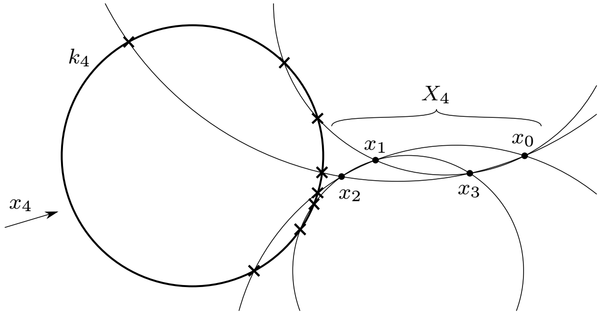
Pomocí kardinálů můžeme provést transfinitní rekurzi silnějším způsobem než rekurzí na všech ordinálních číslech. Pokud projdeme prvky množiny X transfinitní rekurzí na kardinálu $|X|$, máme v průběhu rekurze navíc jistotu, že dosud prošlých kroků je v každém okamžiku ostře méně než $|X|$.

Příklad. Existuje množina bodů v rovině[8], kterou každá kružnice protne právě ve třech bodech.

Důkaz. Každá kružnice je určená svým středem (prvek množiny $\mathbb{R} \times \mathbb{R}$) a poloměrem (prvek $\mathbb{R}^+$). Počet všech kružnic tedy je $|\mathbb{R} \times \mathbb{R} \times \mathbb{R}^+| = |\mathbb{R}| = \mathfrak{c}$. Očíslujeme si všechny kružnice prvky kontinua – to znamená, že sestrojíme posloupnost k_α délky $\mathfrak{c}$, která obsahuje všechny kružnice. Navíc to provedeme tak, aby každá kružnice byla v této posloupnosti právě třikrát (to lze, protože $|3 \times \mathfrak{c}| = \mathfrak{c}$).

Kýženou množinu sestrojíme postupně transfinitní rekurzí coby posloupnost bodů x_α. Tato posloupnost bude délky $\mathfrak{c}$ a body volíme tak, aby vždy $x_\alpha \in k_\alpha$. Rekurzivní předpis probíhá následovně.

Chceme popsat x_α. Označme množinu dosud vybraných bodů $X_\alpha = \{x_\beta : \beta < \alpha\}$ a její průnik s kružnicí jako $P_\alpha = X_\alpha \cap k_\alpha$. Pokud již $|P_\alpha| = 3$, je kružnice k_α uspokojená; nechceme přidat nový bod, a volíme tedy $k_\alpha \in P_\alpha$. V opačném případě máme $|P_\alpha| < 3$, takže najdeme nový bod $x_\alpha \in k_\alpha \setminus P_\alpha$. Musíme ale zajistit, abychom nevytvořili čtyři body na některé jiné kružnici.



Jak je to možné zajistit? Jediné, čemu je třeba se vyhnout, je položení bodu x_α na kružnici, která již prochází třemi body z X_α. Množina X_α má mohutnost maximálně $|\alpha| < \mathfrak{c}$. I množina všech trojic bodů z X_α má tedy mohutnost menší než kontinuum. Každé takové trojici lze opsat nanejvýš jednu kružnici, takže všech kružnic, které prochází třemi body z X_α, je méně než kontinuum. Každá taková kružnice protne k_α nanejvýš ve dvou bodech, takže zakázaných bodů je méně než kontinuum. Kružnice k_α (i po odebrání konečného P_α) obsahuje kontinuum bodů, takže zbývá bod, který můžeme zvolit.

[8] Rovinu formálně považujeme za množinu $\mathbb{R} \times \mathbb{R}$, kde bod je určený svými souřadnicemi.

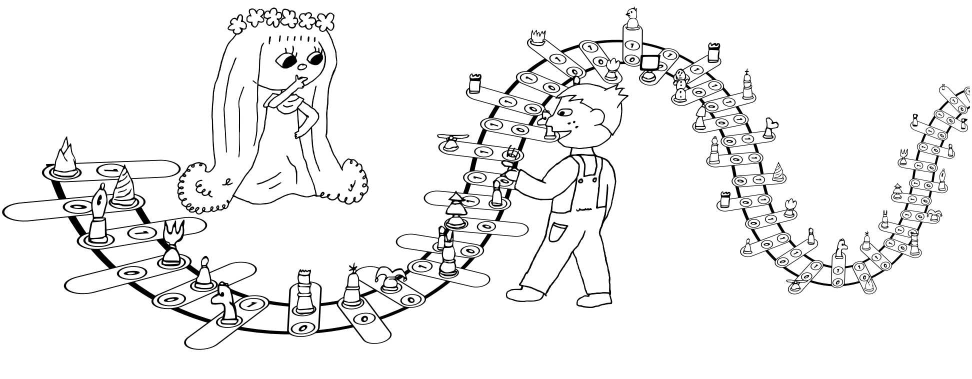
Takto zajistíme, že na každé kružnici budou ve finální množině $X = \{x_\alpha : \alpha \in \mathfrak{c}\}$ nejvýše tři body. Současně na každé budou alespoň tři body, protože jsme v průběhu rekurze každou kružnici potkali třikrát a vždy, když na ní ještě nebyly tři body, jsme na ni bod přidali. Množina X tak každou kružnici protíná právě ve třech bodech. □

Skutečnost, že jsme v transfinitní rekurzi probíhali kardinál a ne něco většího, byla klíčová. Při volbě kružnic a bodů se totiž opíráme o axiom výběru, a tak nemáme příliš kontrolu nad tím, které body bereme. Kdybychom nepoužili kardinál, mohlo by se během rekurze náhodou stát, že jsou v některém okamžiku vybrány přesně všechny body z jedné přímky a ještě jeden mimo ni. Pak sice na každé kružnici leží nejvýše tři body, ale nelze přidat žádný další bod tak, aby tato vlastnost zůstala splněna. Přitom přímka s bodem zjevně není řešením úlohy. Tím, že jsme použili kardinál $\mathfrak{c}$, jsme takové situaci zabránili – v průběhu se nikdy nemohlo stát, že bychom měli vybrány všechny body některé přímky, protože je v každém okamžiku vybráno méně než kontinuum bodů.

Pro lepší pochopení, co se v předchozím důkaze dělo, si můžeš představit pouze spočetnou verzi tohoto tvrzení – „existuje množina racionálních bodů $S \subset \mathbb{Q} \times \mathbb{Q}$, která má tříprvkový průnik s každou kružnicí s racionálním středem a poloměrem“ – a projít důkaz znovu. V takové verzi bychom použili namísto $\mathfrak{c}$ jen ω. „Méně než kontinuum“ by pak znamenalo jednoduše „konečně mnoho“ a přiřazování bodů x_n by probíhalo obyčejnou (netransfinitní) rekurzí. Na druhou stranu je pak v důkaze navíc potřeba znalost faktu, že každá kružnice s racionálním středem i poloměrem obsahuje nekonečně mnoho racionálních bodů.

Hra bez neprohrávající strategie

V této kapitole předvedeme další kuriózní objekt sestrojitelný pomocí transfinitní rekurze na kardinálu: Hru dvou hráčů, kteří se střídají v tazích, oba mají úplnou informaci, a přitom ani jeden z nich nemá neprohrávající strategii. Možná ses setkal(a) s tvrzením, že „v každé konečné hře dvou hráčů s úplnou informací má alespoň jeden z nich neprohrávající strategii“. Pro nekonečné hry to již platit nemusí. Sestrojit takovou hru není snadné, ale s dosavadní teorií již toho příliš nechybí.



Ve hře budou hrát dva hráči – Amálka (A) a Budulínek (B). Oba postupně plní posloupnost $a_0, a_1, \ldots \in \{0, 1\}$ délky ω. Amálka rozhodne hodnotu a_0, Budulínek rozhodne hodnotu a_1, Amálka hodnotu a_2 atd. Po sestrojení této posloupnosti se na základě pravidel (která popíšeme později) určí, kdo vyhrál.

Závěrečným stavem hry tedy rozumíme posloupnost nul a jedniček délky ω. Nechť Z je množina všech závěrečných stavů hry. Pravidly pak rozumíme zobrazení $p\colon Z \to \{A, B\}$. Pravidla se podívají na závěrečný stav hry $z \in Z$ a odpovědí, zda vyhrála Amálka ($p(z) = A$), či Budulínek ($p(z) = B$).

Protože tato hra nikdy nedopadne remízou, znamená neprohrávající strategie totéž co vítězná strategie. Budeme proto raději mluvit o vítězné strategii. Abychom mohli najít pravidla, pro něž nemá ani jeden z hráčů vítěznou strategii, musíme ještě přesně popsat, co to vůbec je strategie.

Definice. *Částečným stavem hry pro Amálku* nazveme posloupnost nul a jedniček sudé (konečné) délky. *Strategií pro Amálku* rozumíme zobrazení $C_A \to \{0, 1\}$, kde C_A je množina všech částečných stavů hry pro Amálku. Na základě stavu hry tedy strategie vždy řekne, zda má Amálka napsat nulu, nebo jedničku. *Vítězná* strategie pro Amálku je taková, že hraje-li Amálka přesně podle této strategie, vyhraje, ať hraje Budulínek jakkoli. Analogicky definujeme množinu C_B částečných stavů hry pro Budulínka jako množinu posloupností nul a jedniček liché délky, a vítěznou strategii pro Budulínka.

Tvrzení. *Existují pravidla, se kterými ani jeden z hráčů nemá vítěznou strategii.*

Důkaz. Všech částečných stavů hry je nekonečně, ale jen spočetně mnoho. Strategie tak jsou zobrazení ze spočetné množiny do dvouprvkové množiny. Proto když označíme S množinu všech strategií (pro oba hráče), máme $|S| = \mathfrak{c}$. Očíslujeme tedy množinu $S = \{s_\alpha : \alpha \in \mathfrak{c}\}$. Rekurzivně definujeme posloupnost délky kontinua $p_\alpha = (z_\alpha, h_\alpha)$, kde z_α je závěrečný stav hry a $h_\alpha \in \{A, B\}$. Přitom všechna z_α budou navzájem různá a hráč h_α dokáže dosáhnout závěrečného stavu z_α za předpokladu, že druhý hráč hraje podle strategie s_α. Z toho plyne, že zvolíme-li pravidla $P \supset \{p_\alpha\}$, nebude strategie s_α vítězná.

Nutně tak je h_α ten hráč, kterému nepatří strategie s_α. V hledání z_α předpokládejme, že s_α patří Amálce, a tedy $h_\alpha = B$. Opačný případ se ošetří analogicky.

Když Amálka hraje podle strategie s_α, může stále Budulínek libovolně rozhodnout, jaká čísla dá na liché pozice. Hra tedy může v závislosti na hře Budulínka dopadnout kontinuum mnoha způsoby. Dosud jsme ale přiřadili vítěze jen k $|\alpha| < \mathfrak{c}$ závěrečným stavům z_β, kde $\beta < \alpha$. Mezi závěrečnými stavy, kterých může Budulínek dosáhnout, když Amálka hraje podle s_α, tak stále bude nějaký nový. Ten použijeme coby z_α.

Tímto postupem zajistíme, že na základě zobrazení $\{p_\alpha : \alpha \in \mathfrak{c}\}$ nebude žádná strategie vítězná. Může se ale stát, že některým závěrečným stavům dosud není přiřazený žádný hráč. Pro zkompletování pravidel můžeme takové stavy přisoudit třeba Amálce, a máme požadovanou hru. □

Čokoládová výzva

Čokoládovou výzvu z předchozího dílu dosud nikdo nevyřešil. Nezveřejníme tak prozatím její řešení – stále platí: kdo první pošle správné řešení na mail `mirek zavináč olsak tečka net`, dostane velkou čokoládu, případně druhý polovinu, třetí čtvrtinu atd. O nezávislou posloupnost malých čokolád stále mohou soutěžit organizátoři.

A krom minulé čokoládové výzvy přichází poslední, třetí čokoládová výzva. Její pravidla jsou stejná jako v případě té minulé – první, kdo pošle řešení následující úlohy na mail `mirek zavináč olsak tečka net`, dostane velkou čokoládu, druhý půlku, třetí čtvrtku atd.

Poslední čokoládová úloha zobecňuje dobrodružství nekonečně mnoha prasátek na obecnou DUMu. Věříme, že bude schůdnější než ta předchozí ;-).

Úloha. Množina (blíže neurčené velikosti) prasátek nastoupí na všechny prvky předem určené DUMy. Každé ví, na kterém prvku stojí, a vidí jen prasátka na vyšších prvcích. Dále každé dostane na hlavu černý nebo bílý klobouk, a jen na základě klobouků, které vidí před sebou, si tipne barvu svého klobouku. Ukaž, že ať je tato DUM jakákoli, existuje strategie, se kterou se při jakémkoli rozložení klobouků splete jen konečně mnoho prasátek.

Rozloučení

Nekonečno je fascinující, ale ve skutečném světě jej příliš nepotkáš. Z tohoto důvodu končí i náš nekonečný seriál. Doufáme, že se Ti mezi nekonečny líbilo a že se k nim budeš myšlenkami rád(a) vracet. Na druhou stranu doporučujeme se z nich nezbláznit. Přeci jen je pro teorií množin nedotčené lidi nespočetný ordinál mnohem větší nesmysl než růžový vodník a nemá cenu je přesvědčovat, že nespočetné ordinály opravdu existují… Měj se nekonečně!

Mirek Olšák

Seznam symbolů a pojmů

Na této stránce jsou stručně uvedeny všechny důležité pojmy třetího dílu seriálu. U každého pojmu z tohoto dílu je uvedeno, na které stránce byl definován.

str 6. *Posloupnost* $x_0, x_1, \ldots$ délky α
str 6. *Víceznačná funkce*, *vybrání* funkce z víceznačné funkce
str 8. *Řetězec* množin $\mathcal{R} \subset \mathcal{P}(X)$ – každé dva prvky $A, B \in \mathcal{R}$ musí splňovat $A \subset B$ nebo $B \subset A$
str 8. Zornovo lemma – když v $\mathcal{S}$ leží sjednocení každého řetězce, tak v $\mathcal{S}$ je maximální prvek
str 9. Princip dobrého uspořádání – každou množinu lze dobře uspořádat
str 10. *Lineární kombinace* prvků množiny $X \subset \mathbb{R}$
str 10. *Vyhodnocení* $k(X)$ lineární kombinace k prvků množiny X – součet všech $k(x) \cdot x$
str 10. *Triviální* lineární kombinace – všude nulová
str 10. *Lineárně nezávislá množina* – různé lineární kombinace dávají různá vyhodnocení
str 11. *Báze* – maximální lineárně nezávislá množina
str 12. *Kardinální číslo* – nejmenší ordinální číslo své mohutnosti
str 13. $|X|$ neboli *mohutnost* X – kardinální číslo, které má stejnou mohutnost jako X
str 13. $\mathfrak{c}$ neboli *kontinuum* – mohutnost množiny reálných čísel

Důležité pojmy z předchozích dílů: zobrazení (funkce), spočetno, nespočetno, porovnávání mohutností $|A| \leq |B|$, $|A| = |B|$, množina, třída, potence $\mathcal{P}(A)$, kartézský součin $A \times B$, ordinální číslo, množina přirozených čísel ω, třída ordinálních čísel $\mathbb{O}n$, transfinitní rekurze.

Návody

1. $\tilde{g} = \{(b, a) : f(a) = b\}$.

2. Pomocí Zornova lemmatu najdi maximální systém množin splňující bod (ii). Z maximality vyplyne bod (i).

3. Za $\mathcal{S}$ vol množinu takových podmnožin $\bigcup a$, které protínají každý prvek a jen v jednom bodě.

4. Uvaž dobré uspořádání na $\bigcup a$ a z něj odvoď předpis pro výběr reprezentantů.

5. Za $\mathcal{S}$ zvol množinu všech prostých zobrazení $\alpha \to X$, kde α je ordinální číslo. Jedná se o množinu (a ne o vlastní třídu), protože α je vždy typem nějaké podmnožiny množiny X s přidaným uspořádáním.

6. Postupně ukaž $f(0) = 0$, $f(-x) = -f(x)$, $f(nx) = nf(x)$ pro každé x reálné a n celé. Nakonec zjednoduš hodnotu $d \cdot f(qx)$, kde $q = \frac{n}{d}$ a n, d jsou nenulová celá čísla.

7. $\{1, \sqrt{2}\}$: Nechť $p = q\sqrt{2}$ a $q \neq 0$, pak $\sqrt{2} = \frac{p}{q}$. $\{1, \sqrt{2}, \sqrt{3}\}$: Když $p + q\sqrt{2} = r\sqrt{3}$, tak umocněním dostaneš $2pq\sqrt{2} = 3r^2 - p^2 - 2q^2$. Protože je $\sqrt{2}$ iracionální, musí být $pq = 0$. Zbytek se rozebere podobně jako v předchozím případě.

8. (i) Kdyby M obsahovala nulu, vyhodnotila by se na nulu netriviální lineární kombinace daná předpisem $k(0) = 1$, $k(x) = 0$ pro $x \neq 0$. M by tak nebyla lineárně nezávislá. (ii) Kdyby M obsahovala racionální čísla p, q, měla by nulové vyhodnocení netriviální lineární kmbinace daná předpisem $k(p) = q$, $k(q) = -p$, $k(x) = 0$ pro $x \neq p, q$. (iii) Stačí například doplnit na bázi lineárně nezávislou množinu $\{1 + \sqrt{2}, \sqrt{2}\}$. Obecně můžeš libovolnou bázi s racionálním číslem q upravit na bázi bez racionálního čísla – vezmi ještě jeden její iracionální prvek x a nahraď q za $q + x$.

9. (i) Kdyby obsahovala jen jeden prvek $x \neq 0$, nebylo by možné vyjádřit $x\sqrt{2}$ jako racionální násobek x. (ii) Kdyby byla báze M spočetná, tak by i počet lineárních kombinací byl spočetný – ze stejného důvodu jako počet polynomů s racionálními koeficienty v kapitole Porovnávání nekonečen prvního dílu seriálu.

10. (i) Klasická řešení jsou $f(x) = x$, $f(x) = -x$. Dále se na takové řešení doplní například tyto dvě funkce definované na bázi: $f_0(x) = x$ s výjimkou $f_0(1) = -1$ nebo $f_1(x) = x$ s výjimkami $f_1(1) = \sqrt{2}$ a $f_1(\sqrt{2}) = 1$. (ii) $f_0(1) = \sqrt{2}$, $f_0(\sqrt{2}) = -1$. (iii) Z Zornova lemmatu existuje maximální množina P disjunktních párů z M. To znamená, že buď $\bigcup P = M$, nebo v $\bigcup P$ chybí jeden prvek. Úpravou spočetně mnoha dvojic se začlení i tento poslední zbývající prvek. Alternativně lze využít princip dobrého uspořádání a popsat párování na DUMě. (iv) Z párů v (iii) vytvoř uspořádané dvojice a definuj na nich f_0 jako v bodě (ii). (v) Stačí najít pro bázi M libovolné zobrazení $M \to M$, které je prosté, ale není na.