MATEMATICKÉ STRUKTURY (NMAI064)
letní semestr 2022/23
přednášející: Martin Klazar

PŘEDNÁŠKA 9 (12. 4. 2023). AXIOM VÝBĚRU A JEHO DŮSLEDKY: NEMĚŘITELNÉ MNOŽINY, VĚTA O DOBRÉM USPOŘÁDÁNÍ, PARADOX PROROKA

• *Axiom výběru*, krátce AC je axiom v teorii množin, který požaduje, aby

$$\forall A \left(\emptyset \not\in A \Rightarrow \exists F \left(F\colon A \to \bigcup A\right) \wedge (B \in A \Rightarrow F(B) \in B)\right) .$$

Jak jistě víte, *suma* $\bigcup A$ *z* A je taková množina $\bigcup A$, že

$$B \in \bigcup A \iff \exists C \in A \left(B \in C\right) .$$

Zápis $F\colon A \to B$, tj. F je *funkce (zobrazení) z* A *do* B, zkracuje fakt, že F je taková množina uspořádaných dvojic (C, D), že vždy $C \in A$, $D \in B$ a pro každé $C \in A$ existuje právě jedno $D \in B$ s $(C, D) \in F$.

Úloha 1 *Ukažte, že* AC *je ekvivalentní s tvrzením, že*

$$\forall \, surjekci \, F\colon A \to B \; \exists G\colon B \to A \left(FG = F \circ G = \mathrm{id}_B\right) .$$

Úloha 2 *Ukažte, že* AC *je ekvivalentní s tvrzením, že pro každý systém množin* $(A_i \mid i \in I)$*, kde vždy* $A_i \neq \emptyset$*, existuje funkce* $F\colon I \to \bigcup_{i\in I} A_i$*, že vždy* $F(i) \in A_i$ *(„vždy“ je* $\forall \, i \in I$*).*

Úloha 3 *Uveďte příklad ukazující, že v první formulaci* AC *nelze obecně mít prostou funkci* F*.*

• *Ekvivalence a rozklady.* Připomeneme si relace ekvivalence a definujeme rozklady. $R \subseteq A \times A$ *je relace ekvivalence (na A)*, pokud je R

- reflexivní $(\forall\, a \in A\, \big(aRa\big))$,
- symetrická $(\forall\, a, b \in A\, \big(aRb \Rightarrow bRa\big))$ a
- tranzitivní $(\forall\, a, b, c \in A\, \big(aRb \wedge bRc \Rightarrow aRc\big))$.

(Množinový) rozklad množiny A je taková množina B, že $\emptyset \notin B$ a

$$(C,\, D \in B \Rightarrow C = D \vee C \cap D = \emptyset) \wedge \bigcup B = A\ .$$

Pro relaci ekvivalence R na množině A definujeme *bloky* R jako množiny

$$[a]_R := \{b \in A \mid aRb\},\ a \in A\ .$$

Úloha 4 *Ukažte, že pro každou množinu A a každou relaci ekvivalence R na A je*

$$A/R := \{[a]_R \mid a \in A\}$$

je rozklad množiny A.

Úloha 5 *Ukažte, že pro každou množinu A a každý rozklad P množiny A je*

$$R(P) := \{(a,\, b) \in A^2 \mid \exists\, B \in P\, \big(a,\, b \in B\big)\}$$

relace ekvivalence na A.

Úloha 6 *Ukažte, že pro každou množinu A, každou relaci ekvivalence S na A a každý rozklad P množiny A paltí, že*

$$R(A/S) = S \quad a \quad A/R(P) = P\ .$$

Úloha 7 *Pro $n \in \mathbb{N} = \{1, 2, \dots\}$ nechť B_n (tzv.* Bellovo číslo[1]*) je počet všech relací ekvivalence na n-prvkové množině X. Proč B_n závisí pouze na mohutnosti X a ne na prvcích X? Dokažte, že pro každé n je*

$$B_n < B_{n+1} \, .$$

- *Neměřitelné množiny.* Nechat

$$S := \{(x,\, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1\}$$

je *jednotková kružnice* v euklidovské rovině $\mathbb{R}^2$. Pro libovolný úhel $\varphi \in [0, 2\pi)$ označíme

$$F_\varphi \colon S \to S, \ \ (x,\, y) \mapsto (?_x,\, ?_y) \, ,$$

rotace proti směru hodinových ručiček kolem počátku o úhel φ; je to bijekce. Úhel $\varphi \in [0, 2\pi)$ je *racionální*, pokud $\varphi/\pi \in \mathbb{Q}$. Množinu racionálních úhlů označíme $[0, 2\pi)_{\mathbb{Q}}$. Je zřejmé, že $[0, 2\pi)_{\mathbb{Q}}$ je spočetná množina.

Úloha 8 *Definujte aditivní abelovskou grupu $([0, 2\pi)_{\mathbb{Q}}, +)$ sčítání modulo 2π. Najděte výše uvedené vzorce $?_x$ a $?_y$ v definici F_φ a ukažte, že pro libovolné úhly $\varphi, \varphi' \in [0, 2\pi)_{\mathbb{Q}}$ je*

$$F_\varphi \circ F_{\varphi'} = F_{\varphi+\varphi'} \, .$$

Ukažte, že pro pevné $x \in S$ je funkce $F_\varphi(x)$ injektivní v proměnné $\varphi \in [0, 2\pi)$.

Pro podmnožinu $X \subseteq \mathcal{P}(S)$ potence množiny S (tj. $\mathcal{P}(S)$ je množina všech podmnožin S) s $S \in X$, říkáme, že funkce

$$\lambda \colon X \to [0,\, +\infty)$$

[1]Pojmenováno po E. T. Bellovi (1883–1960).

je *délka oblouku na* X, pokud platí následující tři podmínky.

1. $\lambda(S) > 0$ – celá jednotková kružnice má kladnou délku oblouku.

2. Pro všechny po dvou disjunktní množiny $A_n \in X$, $n \in \mathbb{N}$, s $\bigcup_{n=1}^{\infty} A_n \in X$ platí, že

$$\lambda(\bigcup_{n=1}^{\infty} A_n) = \sum_{n=1}^{\infty} \lambda(A_n)$$

   – délka oblouku je σ-aditivní.

3. Pro každé $\varphi \in [0, 2\pi)$ a $A \in X$, pokud $F_\varphi[A] \in X$, pak

$$\lambda(F_\varphi[A]) = \lambda(A)$$

   – délka oblouku je při rotacích neměnná.

Věta 9 (problémová množina) *Existuje množina* $X \subseteq S$*, že množina*

$$\{F_\varphi[X] \mid \varphi \in [0, 2\pi)_{\mathbb{Q}}\}$$

je rozklad množiny S*.*

Důkaz. Relace $\sim$ na S, definovaná pomocí

$$a \sim b \iff \exists\, \varphi \in [0,\ 2\pi)_{\mathbb{Q}} \left(F_\varphi(a) = b\right) ,$$

je podle úlohy 10 relace ekvivalence. $X \subseteq S$ definujeme pomocí AC tak, že z každého bloku $\sim$ vezmeme jeden reprezentativní prvek. Ukážeme, že pro φ probíhající $[0, 2\pi)_{\mathbb{Q}}$ jsou množiny $F_\varphi[X]$ disjunktní a rozkládají S. Jejich sjednocení je S, protože každé $s \in S$ leží v nějakém bloku B relace $\sim$ a tedy $F_\varphi(r) = s$ pro nějaký úhel $\varphi \in [0, 2\pi)_{\mathbb{Q}}$ pro reprezentanta $r \in X$ bloku B. Pokud $F_\varphi[X] \cap F_{\varphi'}[X] \neq \emptyset$ pro dva odlišné racionální úhly φ a φ', pak

$$F_\varphi(r) = F_{\varphi'}(r') \text{ pro nějaké } r, r' \in X\ .$$

Potom $r \neq r'$ díky prostotě $F_\varphi(x)$ ve φ pro pevné x (úloha 8). Též

$$F_{\varphi - \varphi'}(r) = r' \ \text{ pro } \ \varphi - \varphi' \in [0,\, 2\pi)_{\mathbb{Q}}$$

(opět úloha 8) a tedy $r \sim r'$, což je nemožné pro dva různé prvky množiny X. Je jasné, že každá množina $F_\varphi[X] \neq \emptyset$. □

Úloha 10 *Dokažte, že relace $\sim$ na S definovaná v předchozím důkazu je relací ekvivalence.*

Důsledek 11 (nemožná délka oblouku) *Neexistuje délka oblouku λ na celé potenci $\mathcal{P}(S)$.*

Důkaz. Předpokládejme pro spor, že

$$\lambda\colon \mathcal{P}(S) \to [0,\, +\infty)$$

je délka oblouku a uvažme množinu $X \subseteq S$ z předchozí věty. Pak dostaneme pomocí věty a pomocí tří vlastností délky oblouku spor, že $\lambda(S) \in (0,\, +\infty)$ se rovná

$$\sum_{\varphi \in [0,\, 2\pi)_{\mathbb{Q}}} \lambda(F_\varphi[X]) = \sum_{\varphi \in [0,\, 2\pi)_{\mathbb{Q}}} \lambda(X) = 0 \ \text{ nebo } \ +\infty\ ,$$

podle toho, zda $\lambda(X) = 0$ nebo je > 0. □

Úloha 12 *Pokud v definici délky oblouku nepožadujeme vlastnost 1, předchozí důsledek neplatí.*

• *Dobré uspořádání.* Relace $\le_X \subseteq X^2$ je *lineární uspořádání (na X)*, je-li reflexivní, tranzitivní, slabě asymetrická ($a \le_X b \wedge b \le_X a \Rightarrow a = b$) a totální ($\forall\, a, b \in X\ \big(a \le_X b \vee b \le_X a\big)$). Lineární pořadí $\le_X$ na X je *dobré*, pokud každá neprázdná množina $Y \subseteq X$ má minimální (tj. nejmenší) prvek $y \in Y$: pro každé $z \in Y$ je $y \le_X z$.

Úloha 13 *Dokažte, že minimální prvky jsou jedinečné (jednoznačné).*

Úloha 14 *Dokažte, že lineární uspořádání* $(X, \leq_X)$ *je dobré, pokud neexistuje nekonečný ostře klesající řetězec* $x_1 >_X x_2 >_X \ldots, x_n \in X$ *(*$x >_X y$ *znamená, že* $y \leq_X x$ *a* $y \neq x$*).*

Úloha 15 *Předpokládejte, že na každé množině existuje dobré lineární uspořádání a odvoďte z toho* AC*.*

Věta 16 (Zermelova věta) *Axiom výběru platí* $\iff$ *každá množina má dobré (lineární) uspořádání.*

Důkaz. Část $\Leftarrow$ je dokázána v úloze 15. Dokážeme druhou implikaci: pokud platí AC, pak každá množina má dobré uspořádání. Nechť $X \neq \emptyset$ a $f \colon \mathcal{P}(X) \setminus \{\emptyset\} \to X$ je *selektor na* X, tj. funkce splňující, že $f(A) \in A$ (tu garantuje AC). Vezmeme množinu

$$L := \{R \mid R \subseteq D(R)^2,\ D(R) \subseteq X,\ R \text{ je lin. usp. na } D(R)\}$$

všech lineárních uspořádání R na podmnožinách $D(R)$ množiny X. Pro libovolné $R \in L$ položíme

$$D_R := \{A \subseteq D(R) \mid x,\, y \in D(R),\, y \in A,\, xRy \Rightarrow x \in A\}\ .$$

D_R je tedy množina všech *dolních množin* v lineárním uspořádání R. Nechte dále

$$C := \{R \in L \mid A \in D_R,\, A \neq D(R) \Rightarrow f(X \backslash A) = \min_R (D(R) \backslash A)\}$$

jsou ty lineární uspořádání R na podmnožinách $D(R)$ množiny X, pro které pro každou vlastní dolní množinu A v R selektor f vybírá z jejího doplňku do X prvek, který je také minimálním prvkem doplňku A do $D(R)$. Ukážeme, že C obsahuje dobré uspořádání celé množiny X. Patrně $C \neq \emptyset$, protože například $\{(f(X), f(X))\}$ je v C.

Nejprve ukážeme, že každá $R \in C$ je dobré uspořádání množiny $D(R)$. Nechť $R \in C$. Pro každou neprázdnou množinu $B \subseteq D(R)$ položíme

$$A = \{y \in D(R) \setminus B \mid x \in B \Rightarrow yRx\} .$$

Množina $D(R) \setminus A$ obsahuje B a je tedy neprázdná. Je zřejmé, že A je dolní množina v R. Tím pádem

$$y := f(X \setminus A) = \min_R(D(R) \setminus A) .$$

Z faktů, že $D(R) \setminus A \supset B$ a že y je minimální prvek v $D(R) \setminus A$, dostaneme yRx pro každé $x \in B$. Pokud $y \notin B$, měli bychom $y \in A$ podle definice A, což je nemožné. Proto y je v B a je minimálním prvkem B, i nadmnožiny $D(R) \setminus A$.

Za druhé ukážeme, že pro každá dvě lineární uspořádání $R, S \in C$ jedno z nich rozšiřuje druhé: $D(R) \in D_S \wedge R \subseteq S$ nebo $D(S) \in D_R \wedge S \subseteq R$. Nechť $R, S \in C$. Definujeme A jako množinu

$$\{x \in D(R) \cap D(S) \mid Rx = Sx \wedge R \cap (Rx \times Rx) = S \cap (Sx \times Sx)\}$$

(zde $Rx = \{y \in D(R) \mid yRx\}$ a podobně pro Sx). Množina A se skládá přesně z prvků, které určují tutéž dolní množinu v R a v S, která je navíc v R a v S uspořádána stejně. Tvrdíme, že $A \in D_R \cap D_S$ – A je dolní množina jak v R, tak v S. Nechť

$$z,\ y,\ x \in X \ \text{ s } \ x \in A \ \text{ a } \ yRx .$$

Potom ySx, protože $Rx = Sx$. Pokud zRy, pak zSy a naopak (v obou případech $y, z \in Rx = Sx$ a tato množina je uspořádána stejným způsobem v R a v S). Tedy $Ry = Sy$. Tato množina je obsažena v $Rx = Sx$, a proto je uspořádána stejným způsobem jak v R, tak v S. Proto $y \in A$ a A je dolní množina v R. Stejně se ukáže, že A je dolní množina v S.

Pokud nyní $D(R) \setminus A$ a $D(S) \setminus A$ nejsou prázdné, $y = f(X \setminus A)$ je minimální prvek $D(R) \setminus A$ vzhledem k R a též minimální prvek $D(S) \setminus A$ vzhledem k S, a tak $Ry = A \cup \{y\} = Sy$. Je také jasné, že R a S uspořádávají $A \cup \{y\}$ stejně (přidají nový prvek y na konec), a tak $y \in A$, což je spor. Tak například $A = D(R)$, $R \subseteq S$ a S rozšiřuje R.

Za třetí ukážeme, že

$$T := \bigcup C \in C \ ,$$

takže C má (jedinečný) maximální prvek vzhledem k inkluzi. Podle předchozího odstavce je T lineární uspořádání na

$$D(T) = \textstyle\bigcup_{R \in C} D(R)$$

a pro $x, y \in D(T)$ máme xTy, právě když xRy pro nějaké $R \in C$ s $x, y \in D(R)$. Zkontrolujeme, že T má vlastnost definující C. Nechť $A \subseteq D(T)$ je vlastní dolní množina v T a $b \in D(T) \setminus A$ je libovolné. Tedy $b \in D(R)$ pro nějakou $R \in C$. Ukážeme, že $A \subseteq D(R)$. Když $a \in A$ je libovolné, pak $a \in D(S)$ pro nějaké $S \in C$. Pokud $D(S) \in D_R$, pak $a \in D(R)$. Pokud $D(R) \in D_S$ a aSb, pak znovu $a \in D(R)$. Případ bSa se nevyskytuje (pak by bylo $b \in A$). Proto $A \subseteq D(R)$ a $D(R) \setminus A \neq \emptyset$. Proto prvek $y = f(X \setminus A)$ je minimální prvek v $D(R) \setminus A$ a yRb. Protože b bylo libovolné, y je minimální prvek v $D(T) \setminus A$ a vidíme, že $T \in C$.

Na závěr ukážeme, že $D(T) = X$, a T je tedy hledané dobré uspořádání množiny X. Pokud $D(T) \neq X$, pak bychom mohli T

rozšířit prvkem $x := f(X \setminus D(T))$ do tohoto R:

$$D(R) := D(T) \cup \{x\} \ \text{ a } \ yRx \ \text{ pro každé } \ y \in D(R) \qquad (1)$$

– do T přidáme nový maximální prvek. Je jasné, že $R \in C$ (úloha 17). Protože R ostře rozšiřuje T, máme spor s maximalitou T. $\square$

Předchozí důkaz je převzat z poznámek prof. A. Pultra.

Úloha 17 *Ukažte, že lineární uspořádání R definované v rovnici* (1) *skutečně patří do C.*

• *Paradox proroka.* Nechť $(X, \leq_X)$ je lineární uspořádání. Pro libovolné $a \in X$ a libovolnou funkci $f\colon X \to Y$ jako $f_{|a}$ označíme zúžení funkce f na množinu

$$\{b \in X \mid b <_X a\}\ .$$

Pro lineární uspořádání $(X, \leq_X)$ a systém $\mathcal{F}$ funkcí $f\colon X \to Y$, je $(X, \mathcal{F})$-*prorok* funkce

$$P\colon \{f_{|a} \mid f \in \mathcal{F},\, a \in X\} \to Y\ .$$

Hodnota $P(f_{|a}) \in Y$ je *odhad P pro $f(a)$*. Prorok se snaží uhodnout z hodnot $f(b)$ pro všechna $b <_X a$ hodnotu $f(a)$. Pokud $P(f_{|a}) = f(a)$, pak P *uhádl* $f(a)$, jinak P *chybuje v* $f(a)$.

Úloha 18 *Nechť $(X, \leq_X) := (\mathbb{R}, \leq)$ jsou reálná čísla se standardním lineárním uspořádáním a nechť*

$$\mathcal{F} = C(\mathbb{R}) := \{f\colon \mathbb{R} \mid f \text{ je spojitá}\}$$

je množina všech reálných funkcí, které jsou spojité na $\mathbb{R}$. Najděte $(\mathbb{R}, C(\mathbb{R}))$ proroka který uhádne $f(a)$ pro každou $f \in C(\mathbb{R})$ a každé $a \in \mathbb{R}$.

Na druhou stranu máme následující stejně jednoduchý výsledek.

Tvrzení 19 (všichni proroci se mýlí) *Pro* $n \in \mathbb{N}$ *nechť*

$$(X, \leq_X) = ([n], \leq) := (\{1, 2, \ldots, n\}, \leq)$$

je standardní lineární pořadí na prvních n *přirozených číslech a nechť*

$$\mathcal{F} := Y^{[n]} = \{\textit{všechny funkce z } [n] \textit{ do } Y\} \ ,$$

kde Y *je množina s alespoň dvěma prvky. Pak platí, že pro každého* $([n], Y^{[n]})$*-proroka* P *existuje taková funkce* $f \in Y^{[n]}$*, že*

$$\forall\, a \in [n] \left(P(f_{|a}) \neq f(a)\right)$$

– P *chybuje v* $f(a)$ *pro každé* $a \in [n]$*.*

Důkaz. Nechť $P\colon \{g \mid g\colon [m] \to Y,\, m \in \{0, 1, \ldots, n-1\}\} \to Y$ je $([n], Y^{[n]})$-prorok; zde $[0] := \emptyset$. Hodnoty $f(m)$ požadované funkce $f\colon [n] \to Y$ definujeme indukcí podle $m = 1, 2, \ldots, n$. Na začátku nastavíme $f(1) \in Y$ tak, že $f(1) \neq P(\emptyset)$ (což je možné díky $|Y| \geq 2$). Pokud $m \in [n]$, $m > 1$ a $f(1), f(2), \ldots, f(m-1)$ jsou již definovány, položíme

$$f(m) \in Y \setminus \{P(f_{|m})\}$$

(opět je to možné díky $|Y| \geq 2$). Je jasné, že P chybuje u funkce f při každém jejím argumentu. $\square$

Úloha 20 *Co se stane, když* $|Y| \leq 1$*?*

Někdo by si mohl myslet, že když se ve cvičení 18 rozšíří rodina spojitých funkcí do rodiny $\mathcal{F} := \mathbb{R}^{\mathbb{R}}$ všech reálných funkcí, získáme výsledek podobný předchozímu tvrzení, totiž že každý prorok se musí kvůli nějaké problematické funkci velmi často mýlit. Překvapivě za předpokladu AC platí opak: existuje prorok, který se pro každou reálnou funkci téměř nikdy nemýlí.

Věta 21 (paradox proroka) *Nechť* $(X, \leq_X) := (\mathbb{R}, \leq)$ *je standardní lineární uspořádání reálných čísel a*

$$\mathcal{F} := \mathbb{R}^{\mathbb{R}} = \{\textit{všechny funkce z } \mathbb{R} \textit{ do } \mathbb{R}\}\ .$$

Pak existuje takový $(\mathbb{R}, \mathbb{R}^{\mathbb{R}})$*-prorok* P*, že*

$$\forall\, f \in \mathbb{R}^{\mathbb{R}} \left(\{a \in \mathbb{R} \mid P \textit{ chybuje v } f(a)\} \textit{ je nejvýše spočetná}\right)\ .$$

Důkaz. P definujeme pomocí dobrého uspořádání

$$\left(\mathbb{R}^{\mathbb{R}}, \preceq\right)\ ,$$

které existuje za předpokladu AC podle věty 16. Pro $g \in \mathbb{R}^{\mathbb{R}}$ a $a \in \mathbb{R}$ položíme

$$P(g_{|a}) := g_0(a), \quad \text{kde} \quad g_0 := \min_{\preceq}(\{h \in \mathbb{R}^{\mathbb{R}} \mid h_{|a} = g_{|a}\})\ .$$

Nyní nechť je dáno $f \in \mathbb{R}^{\mathbb{R}}$. Vezmeme množinu

$$X := \{a \in \mathbb{R} \mid P(f_{|a}) \neq f(a)\}$$

chyb P v $f(a)$. Nechť $a < b$ s $a \in X$ jsou dvě reálná čísla,

$$g_a := \min_{\preceq}(\underbrace{\{g \in \mathbb{R}^{\mathbb{R}} \mid g_{|a} = f_{|a}\}}_{M_a}) \quad \text{a} \quad g_b := \min_{\preceq}(\underbrace{\{g \in \mathbb{R}^{\mathbb{R}} \mid g_{|b} = f_{|b}\}}_{M_b})\ .$$

Z $a < b$ dostaneme, že $M_b \subseteq M_a$ a $g_a \preceq g_b$. Z

$$g_a(a) = P(f_{|a}) \neq f(a) = g_b(a)$$

vidíme, že $g_a \neq g_b$. Tedy $g_a \prec g_b$. Vidíme, že lineární uspořádání $(X, \leq)$ (se standardním uspořádáním $\leq$ reálných čísel) je dobré. Jinak bychom podle úlohy 14 měli v $(X, \leq)$ nekonečný ostře klesající řetězec $a_1 > a_2 > \ldots$, což by podle úvahy výše dalo nekonečný ostře klesající řetězec $g_{a_1} \succ g_{a_2} \succ \ldots$ v $(\mathbb{R}^{\mathbb{R}}, \preceq)$. Ale tento řetězec neexistuje, protože $(\mathbb{R}^{\mathbb{R}}, \preceq)$ je dobře uspořádaná. Protože $(X, \leq)$ je dobré uspořádání, podle úlohy 22 je množina X nejvýše spočetná. $\square$

Úloha 22 *Nechť* $(\mathbb{R}, \leq)$ *je standardní lineární uspořádání a* $X \subseteq \mathbb{R}$ *je taková, že lineární uspořádání*

$$(X, \leq)$$

je dobré. Dokažte, že pak je množina X *nanejvýš spočetná. Nápověda: definujte injekci* $f\colon X \to \mathbb{Q}$.

Poslední věta je převzata z knihy.

> Ch. S. Hardin a A. D. Taylor, *The Mathematics of Coordinated Inference*, Springer, 2013.

DĚKUJI ZA POZORNOST!

Úlohy za dom. cv. jsou: 7, 8, 14 a 22.