

2. sada domácich úloh

Termín odovzdania: **nedeľa 21. 12. 2025, 23:59**

Úloha 1

(2 body) Nech R je relácia na množine $\mathcal{P}(\mathbb{N})$ taká, že pre každé $A, B \in \mathcal{P}(\mathbb{N})$ platí

$$ARB \Leftrightarrow \exists k \in \mathbb{Z}: ((\forall a \in A: \exists b \in B: b = a + k) \wedge (\forall b \in B: \exists a \in A: b = a + k)).$$

Dokážte, že R je reláciou ekvivalencie na množine $\mathcal{P}(\mathbb{N})$ a opíšte rozklad, ktorý indukuje.

Poznámka. Pokiaľ je úloha pre Vás veľmi abstraktná, 1 bod viete získať, ak ju vyriešite pre prípad, keď reláciu R budete miesto množiny $\mathcal{P}(\mathbb{N})$ uvažovať definovanú na množine $\mathcal{P}(\{0, 1, 2, 3, 4\})$. Uznáme Vám aj riešenia založené na overovaní všetkých možností, ak ho dostatočne zaznamenáte. Ak pritom použijete počítačové programy, tak ich pripojte k odovzdávanému PDF súboru do MS Teams.

Dôkaz cez prácu s kvantifikátormi

Najskôr ukážeme dôkaz, ktorý možno spraviť bez toho, aby sme podmienku zo zadania nejako upravovali či zjednodušovali. Na tomto riešení je poučné vidieť, ako sa pracuje s kvantifikovanými výrokmi.

Reflexívnosť. Pre každé $A \in \mathcal{P}(\mathbb{N})$ platí ARA , keďže pre $k = 0$ platí:

- $\forall a \in A: \exists b \in A: b = a + k$, keďže po voľbe $b = a$ máme $a = a + 0$;
- $\forall b \in A: \exists a \in A: b = a + k$, keďže po voľbe $a = b$ máme $b = b + 0$.

Symetrickosť. Nech $A, B \in \mathcal{P}(\mathbb{N})$ a nech ARB . Potom:

$$\begin{aligned} \exists k \in \mathbb{Z}: ((\forall a \in A: \exists b \in B: b = a + k) \wedge (\forall b \in B: \exists a \in A: b = a + k)) \\ \Downarrow \\ \exists k \in \mathbb{Z}: ((\forall a \in A: \exists b \in B: a = b - k) \wedge (\forall b \in B: \exists a \in A: a = b - k)) \\ \Downarrow \\ \exists k \in \mathbb{Z}: ((\forall b \in B: \exists a \in A: a = b - k) \wedge (\forall a \in A: \exists b \in B: a = b - k)) \end{aligned}$$

A keďže $-k$ je tiež celé číslo, tak po jeho nahradení za ℓ máme

$$\exists \ell \in \mathbb{Z}: ((\forall b \in B: \exists a \in A: a = b + \ell) \wedge (\forall a \in A: \exists b \in B: a = b + \ell)),$$

čo je presne podľa definície BRA .

Tranzitívnosť. Nech $A, B, C \in \mathcal{P}(\mathbb{N})$ a nech $ARB \wedge BRC$. Z platnosti ARB máme, že pre nejaké celé číslo k platí

$$\forall a \in A: \exists b \in B: b = a + k, \tag{1}$$

$$\forall b \in B: \exists a \in A: b = a + k. \tag{2}$$

Podobne z BRC máme pre nejaké $\ell \in \mathbb{Z}$

$$\forall b \in B: \exists c \in C: c = b + \ell, \tag{3}$$

$$\forall c \in C: \exists b \in B: c = b + \ell. \tag{4}$$

Teraz dokážeme, že pre $m = k + \ell$ platí:

1. $\forall a \in A: \exists c \in C: c = a + m$: Dôkaz. Pre ľubovoľné $a \in A$ podľa (1) existuje $b_0 \in B$ pre ktoré platí $b_0 = a + k$. Pre toto b_0 podľa (3) máme existenciu $c_0 \in C$ takého, že $c_0 = b_0 + \ell$ (využívame, že ak niečo platí pre všetky b , tak platí aj pre konkrétne b_0), teda $c_0 = b_0 + \ell = a + k + \ell = a + m$. Takto sme pre každé $a \in A$ našli $c = c_0$ pre ktoré platí $c = a + m$. (Pri dôkaze možno pokojne použiť rovno b miesto b_0 . Pre lepšiu názornosť sme však použili iné označenie, keďže vlastne ide o odlišné písmenká. Tak to spravíme aj nižšie.)
2. $\forall c \in C: \exists a \in A: c = a + m$: Dôkaz. Pre ľubovoľné $c \in C$ existuje podľa (4) $b \in B$ spĺňajúce $c = b + \ell$ a pre toto b podľa 2 existuje $a \in A$ také, že $b = a + k$, teda $c = b + \ell = a + k + \ell = a + m$.

Dôkaz cez prepísanie podmienky

Teraz ukážeme, ako si možno dôkazy zjednodušiť, ak si na začiatku podmienku relácie zjednodušíme.

Výroková forma $\exists b \in B: b = a + k$ je ekvivalentná $a + k \in B$. Na základe toho si vieme ARB ekvivalentne prepísať na

$$\exists k \in \mathbb{Z}: ((\forall a \in A: a + k \in B) \wedge (\forall b \in B: b - k \in A)).$$

Toto uvedomenie nám vie zjednodušiť dôkazy. Ešte viac si pomôžeme, keď pre množinu $A \in \mathcal{P}(\mathbb{N})$ a $k \in \mathbb{Z}$ definujeme

$$A + k = \{a + k; a \in A\}.$$

Ukážme, že pre všetky $A, B \in \mathcal{P}(\mathbb{N})$ platí

$$ARB \Leftrightarrow \exists k \in \mathbb{Z}: B = A + k.$$

Podmienka $\forall a \in A: a + k \in B$ je ekvivalentná $A + k \subseteq B$, lebo vraví, že všetky prvky tvaru $a + k$ pre $a \in A$ sa nachádzajú v B . Podmienka $\forall b \in B: b - k \in A$ je zas ekvivalentná $B \subseteq A + k$. Teda

$$ARB \Leftrightarrow \exists k \in \mathbb{Z}: (A + k \subseteq B \wedge B \subseteq A + k) \Leftrightarrow \exists k \in \mathbb{Z}: B = A + k.$$

Reflexívnosť. Pre $k = 0$ platí $A + 0 = \{a; a \in A\} = A$, teda ARA .

Symetrickosť. $ARB \Rightarrow \exists k \in \mathbb{Z}: B = A + k$. Potom

$$B - k = \{b - k; b \in B\} = \{a + k - k; a \in A\} = A,$$

teda BRA .

Tranzitívnosť. $ARB \wedge BRC \Rightarrow \exists k \in \mathbb{Z}: B = A + k \wedge \exists \ell \in \mathbb{Z}: C = B + \ell \Rightarrow C = B + \ell = (A + k) + \ell = \{a + k + \ell; a \in A\} = A + (k + \ell) \Rightarrow C = A + (k + \ell) \Rightarrow ARC$.

Poznámka. Ak chceme byť dôslední. Musíme brať do úvahy, že nemôžeme len tak bez dôkazu využiť, že $(A + k) + \ell = A + (k + \ell)$ alebo $B = A + k \Leftrightarrow B + (-k) = A$. Preto sme aspoň stručne naznačili dôkazy týchto vlastností, keď sme ich používali.

Rozklad malej množiny

Najskôr opíšeme rozklad množiny $\mathcal{P}(\{0, 1, 2, 3, 4\})$. Opakujeme proces, v ktorom si vyberieme nejakú množinu A , ktorú ešte nemáme v rozklade a určíme jej triedu $R[A]$. Tú vieme učiť tak, že si prejdeme zvyšné prvky množiny $\mathcal{P}(\{0, 1, 2, 3, 4\})$ a zistíme, ktoré z nich sú vo vzťahu s prvkom A . Jednoduchšie však je, keď bližšie

pochopte, čo nám podmienka vraví. Napr. tým, že po voľbe k máme len jedného kandidáta na množinu B , pre ktorú môže platiť ARB . Aby sme šli systematicky, tak začneme najprv s prázdnu množinou a určíme

$$R[\emptyset] = \{\emptyset\}.$$

Pokračujeme na jednoprvkové množiny. Tam môžeme začať s

$$R[\{0\}] = \{\{0\}, \{1\}, \{2\}, \{3\}, \{4\}\}.$$

To sme zvolili $k \in \{0, 1, 2, 3, 4\}$. Iné voľby k by nevedli k podmnožine množiny $\{0, 1, 2, 3, 4\}$. Máme už všetky jednoprvkové množiny, tak pokračujeme dvojprvkovými. Začneme s

$$R[\{0, 1\}] = \{\{0, 1\}, \{1, 2\}, \{2, 3\}, \{3, 4\}\}.$$

Ak sme si to neuvedomili na začiatku, tak si teraz vieme všimnúť, že všetky prvky triedy $R[A]$ dostávame tak, že ku každému členu množiny A pripočítame vhodné $k \in \mathbb{Z}$. Vhodné znamená, že stále musí byť výsledkom podmnožina $\{0, 1, 2, 3, 4\}$ (resp. podmnožina $\mathbb{N}$ pri všeobecnom rozklade). Keď týmto systémom budeme pokračovať, tak sa dopracujeme k triedam

$$\begin{aligned} R[\emptyset] &= \{\emptyset\}, \\ R[\{0\}] &= \{\{0\}, \{1\}, \{2\}, \{3\}, \{4\}\}, \\ R[\{0, 1\}] &= \{\{0, 1\}, \{1, 2\}, \{2, 3\}, \{3, 4\}\}, \\ R[\{0, 2\}] &= \{\{0, 2\}, \{1, 3\}, \{2, 4\}\}, \\ R[\{0, 1, 2\}] &= \{\{0, 1, 2\}, \{1, 2, 3\}, \{2, 3, 4\}\}, \\ R[\{0, 3\}] &= \{\{0, 3\}, \{1, 4\}\}, \\ R[\{0, 1, 3\}] &= \{\{0, 1, 3\}, \{1, 2, 4\}\}, \\ R[\{0, 2, 3\}] &= \{\{0, 2, 3\}, \{1, 3, 4\}\}, \\ R[\{0, 1, 2, 3\}] &= \{\{0, 1, 2, 3\}, \{1, 2, 3, 4\}\}, \\ R[\{0, 4\}] &= \{\{0, 4\}\}, \\ R[\{0, 1, 4\}] &= \{\{0, 1, 4\}\}, \\ R[\{0, 2, 4\}] &= \{\{0, 2, 4\}\}, \\ R[\{0, 1, 2, 4\}] &= \{\{0, 1, 2, 4\}\}, \\ R[\{0, 3, 4\}] &= \{\{0, 3, 4\}\}, \\ R[\{0, 1, 3, 4\}] &= \{\{0, 1, 3, 4\}\}, \\ R[\{0, 2, 3, 4\}] &= \{\{0, 2, 3, 4\}\}, \\ R[\{0, 1, 2, 3, 4\}] &= \{\{0, 1, 2, 3, 4\}\}. \end{aligned}$$

Celý rozklad

Využijeme, že $ARB \Leftrightarrow \exists k \in \mathbb{Z}: B = A + k$. Potom priamo s definície je množina A v triede so všetkými množinami tvaru $A + k$ pre $k \in \mathbb{Z}$, ktoré však musia byť podmnožinami $\mathbb{N}$. Teda

$$R[A] = \{A + k; k \in \mathbb{Z} \wedge A + k \subseteq \mathbb{N}\}.$$

Ak za A zvolíme množinu obsahujúcu 0, tak podmienku $A + k \subseteq \mathbb{N}$ nemusíme kontrolovať a stačí nám uvažovať $k \in \mathbb{N}$. Tak sa dostávame k tomu, že náš rozklad je

$$\{\{A + k; k \in \mathbb{N}\}; A \subseteq \mathbb{N} \wedge 0 \in A\} \cup \{\{\emptyset\}\},$$

resp. bez definovania notácie $A + k$ ho vieme vyjadriť ako

$$\{\{\{a + k; a \in A\}; k \in \mathbb{N}\}; A \subseteq \mathbb{N} \wedge 0 \in A\} \cup \{\{\emptyset\}\}.$$

Slovne vyjadrené rozklad obsahuje jednu triedu obsahujúcu $\emptyset$ a potom pre každú podmnožinu množiny $\mathbb{N}$, ktorá obsahuje 0, máme triedu so všetkými jej posunmi o k , kde k je ľubovoľné prirodzené číslo.

Tento rozklad je správny, lebo prázdnu množinu je sama v triede a pre neprázdne množiny platí:

- Každá neprázdná množina $A \in \mathcal{P}(\mathbb{N})$ má najmenší prvok m a je vo vzťahu R s množinou $A + (-m)$, ktorá obsahuje 0.
- Každé dve rôzne množiny $A, B \in \mathcal{P}(\mathbb{N})$ obsahujúce nulu nie sú vo vzťahu R : Z ARB dostávame $B = A + k$, čiže $k = 0$ (lebo inak by B obsahovalo len čísla väčšie ako 0, čo by bol spor), teda $A = B$, čo je spor.

Komentár k častej chybe. Samozrejme, ak by sme uviedli rozklad ako

$$\{\{A + k; k \in \mathbb{Z} \wedge A + k \subseteq \mathbb{N}\}; A \in \mathcal{P}(\mathbb{N})\},$$

tak je formálne správny, je to tá istá množina. Avšak takýto zápis nám nedáva dostatočnú informáciu o tom, ako rozklad vyzerá. Totiž viaceré triedy v ňom uvádzame dvakrát (napr. pre $A = \{2\}$ aj $A = \{7\}$ dostávame tú istú triedu). Napríklad z toho zápisu nevieme jasne povedať, koľko tried má tento rozklad. Preto pri opise hľadáme vhodný *systém reprezentantov* – z každej triedy vyberieme jeden prvok, ktorým ho vieme charakterizovať. Pri tejto úlohe to vedia byť množiny obsahujúce 0 a prázdna množina (ale existujú aj iné). To pekne vieme vidieť na výpise všetkých tried.

Taktiež si to môžeme porovnať aj s programom na ďalšej strane, ktorý nám rozklad pre malý prípad vypíše. Hlavná logika výpisu rozkladu je vo funkcii `main`. Vonkajší for cyklus zodpovedá časti $A \subseteq \mathbb{N} \wedge 0 \in A$ z vonkajšej množiny matematického opisu rozkladu – prechádzame všetky podmnožiny obsahujúce 0 (akurát v prípade programu len podmnožiny $\{0, 1, \dots, n-1\}$). Vnútorň for cyklus zas zodpovedá $k \in \mathbb{N}$ z vnútornej množiny, teda z jednej triedy. Tu nám práve prechádzanie cez množiny s nulou zaručí, že nebudeme vypisovať triedy opakovane – každú vypíšeme práve raz.

```

#include <iostream>
#include <vector>

using namespace std;

// aby sme vedeli vector vypisoavat cez <<
ostream& operator<<(ostream &out, vector<int> v) {
    out << "{";
    for (int i = 0; i < v.size(); i++) {
        if (i > 0) out << ", ";
        out << v[i];
    }
    out << "}";
    return out;
}

// Funkcia, ktora vrati vsetky podmnoziny {0, 1, ..., n} obsahujuce 0
vector<vector<int>> subsets_with_0(int n) {
    vector<vector<int>> result;

    for (int mask = 0; mask < (1 << n); mask++) {
        vector<int> subset = {0};
        int x = mask;
        for (int i = 1; i <= n; i++) {
            if (x % 2 == 1) {
                subset.push_back(i);
            }
            x /= 2;
        }
        result.push_back(subset);
    }
    return result;
}

int main() {
    int n = 4;
    cout << "R[{}] = {}".format("", subsets_with_0(n)) << endl;
    for (vector<int> A : subsets_with_0(n)) {
        cout << "R[" << A << "] = {";
        for (int k = 0; k <= n; k++) {
            vector<int> B(A.size());
            for (int i = 0; i < B.size(); i++) {
                B[i] = A[i] + k;
            }
            if (B.back() > n) break;
            if (k > 0) cout << ", ";
            cout << B;
        }
        cout << "}" << endl;
    }
}

```

Úloha 2

(2 body) Na množine $\mathbb{N} = \{0, 1, 2, \dots\}$ definujeme reláciu $\sqsubseteq$ tak, že pre ľubovoľné $a, b \in \mathbb{N}$ platí

$$a \sqsubseteq b \Leftrightarrow \exists k \in \mathbb{N}: b^2 - a^2 = 9k.$$

Dokážte, že $\sqsubseteq$ je reláciou usporiadania na množine $\mathbb{N}$ a určte všetky jej minimálne, najmenšie, maximálne a najväčšie prvky. Správnosť vašich výsledkov dokážte.

Dôkaz usporiadania

Reflexívnosť. Pre každé $a \in \mathbb{N}$ platí $a^2 - a^2 = 0 = 9 \cdot 0$, teda $a \sqsubseteq a$.

Antisymetrickosť. Pre každé $a, b \in \mathbb{N}$ platí:

$$\begin{aligned} a \sqsubseteq b \wedge b \sqsubseteq a \\ \Downarrow \\ \exists k \in \mathbb{N} b^2 - a^2 = 9k \wedge \exists \ell \in \mathbb{N}: a^2 - b^2 = 9\ell \\ \Downarrow \\ 9k = b^2 - a^2 = -(a^2 - b^2) = -9\ell \\ \Downarrow \\ 9k = -9\ell \\ \Downarrow \\ k + \ell = 0 \end{aligned}$$

Keďže $k, \ell \in \mathbb{N}$, tak z toho vyplýva $k = \ell = 0$, teda $b^2 - a^2 = 0$, čo pre $a, b \in \mathbb{N}$ znamená, že $a = b$.

Tranzitívnosť. Pre každé $a, b, c \in \mathbb{N}$ platí:

$$\begin{aligned} a \sqsubseteq b \wedge b \sqsubseteq c \\ \Downarrow \\ \exists k \in \mathbb{N}: b^2 - a^2 = 9k \wedge \exists \ell \in \mathbb{N}: c^2 - b^2 = 9\ell \\ \Downarrow \\ b^2 - a^2 + c^2 - b^2 = 9k + 9\ell \\ \Downarrow \\ c^2 - a^2 = 9(k + \ell) \\ \Downarrow \\ m = k + \ell \in \mathbb{N} \\ \Downarrow \\ \exists m \in \mathbb{N}: c^2 - a^2 = 9m \\ \Downarrow \\ a \sqsubseteq c \end{aligned}$$

Hasseho diagram

Túto časť nie je nutné uvádzať v riešení. Uvádzame ju pre lepšiu predstavu, ako vyzerá naša usporiadaná množina. Načrtneme si Hasseho diagram, v ktorom prvky rastú zľava doprava.

$$\begin{array}{l}
0-3-6-9-12-\dots \\
1-8-10-17-\dots \\
2-7-11-16-\dots \\
4-5-13-14-\dots
\end{array}$$

Na ňom si môžeme všimnúť pomerne peknú štruktúru našej usporiadanej množiny. Z nej už ľahko vidíme, že minimálne prvky sú 0, 1, 2, 4. Avšak argumentovať diagramom nemôžeme – nemáme ho nakreslený celý. Uvedieme preto dva dôkazy. Jeden úplne nezávislý na tejto štruktúre, v druhom zdôvodníme, že táto usporiadaná množina má štruktúru, akú vidíme na diagrame.

Minimálne prvky sú 0, 1, 2, 4.

Dôkaz minimálnych z definície. Najprv ukážeme, že každý z nich je minimálny:

- $a \sqsubseteq 0 \Rightarrow 0 - a^2 = 9k \Rightarrow a^2 = -9k \Rightarrow a = 0 \wedge k = 0$, keďže $-a^2 \leq 0$.
- $a \sqsubseteq 1 \Rightarrow 1 - a^2 = 9k \Rightarrow a^2 = 1 - 9k \Rightarrow a = 1 \wedge k = 0$, keďže pre $k > 0$ je $1 - 9k < 0$.
- $a \sqsubseteq 2 \Rightarrow 4 - a^2 = 9k \Rightarrow a^2 = 4 - 9k \Rightarrow a = 2 \wedge k = 0$, keďže pre $k > 0$ je $4 - 9k < 0$.
- $a \sqsubseteq 4 \Rightarrow 16 - a^2 = 9k \Rightarrow a^2 = 16 - 9k \Rightarrow a = 4 \wedge k = 0$, keďže pre $k = 1$ máme $a^2 = 7$, čo nemá v prirodzených číslach riešenie, a pre $k \geq 2$ je $16 - 9k < 0$, čo tiež nemá riešenie.

A ešte ukážeme, že iné prvky nie sú minimálne:

- 3 nie je minimálny $\Leftarrow 0 \sqsubset 3 \Leftarrow 3^2 - 0^2 = 9 = 9 \cdot 1$
- $\forall a \in \{5, 6, 7, 8\}$: a nie je minimálny $\Leftarrow 9 - a \sqsubset a \Leftarrow a^2 - (9 - a)^2 = (a + 9 - a)(a - 9 + a) = 9(2a - 9)$, pričom $9 - a$ aj $2a - 9$ sú pre tieto a prirodzené čísla
- $\forall a \in \mathbb{N}, a \geq 9$: a nie je minimálny $\Leftarrow (a - 9) \sqsubset a \Leftarrow a^2 - (a - 9)^2 = (a + a - 9)(a - a + 9) = 9(2a - 9)$, pričom $2a - 9 \in \mathbb{N}$ a aj $a - 9 \in \mathbb{N}$.

Dôkaz minimálnych cez štruktúru usporiadania. Nech platí $\exists k \in \mathbb{N}: b^2 - a^2 = 9k$. Potom:

- $b^2 - a^2$ je deliteľné deviatimi, teda čísla a^2, b^2 majú rovnaký zvyšok po delení deviatimi.
- Keďže $k \in \mathbb{N}$, teda $k \geq 0$, tak aj $b^2 - a^2 \Rightarrow b^2 \geq a^2$, čo v prirodzených číslach znamená $b \geq a$.

Platí to aj opačne: ak máme $b \geq a$ také, že $9 \mid (b^2 - a^2)$, tak nájdené $k = (b^2 - a^2)/9$ bude nezáporné a celé, teda prirodzené.

To znamená, že porovnateľné sú len čísla, ktorých druhé mocniny dávajú rovnaký zvyšok po delení 9 a v tom prípade ich porovnáme na základe bežného usporiadania $\leq$. Zvyšok druhej mocniny prirodzeného čísla a závisí len na jeho zvyšku po delení deviatimi. Vyskúšame všetky možné zvyšky:

$a \bmod 9 =$	0	1	2	3	4	5	6	7	8
$a^2 \bmod 9 =$	0	1	4	0	7	7	0	4	1

Teda druhé mocniny celých čísel dávajú po delení deviatimi len zvyšky 0, 1, 4 a 7. Preto naša usporiadaná množina naozaj vyzerá tak, ako na obrázku. Všetky prirodzené čísla sú rozdelené do 4 množín podľa zvyšku ich druhej mocniny po delení 9 a v rámci týchto množín sú usporiadané podľa veľkosti. Preto sú minimálnymi prvkami čísla 0, 1, 2 a 4.

Najmenší prvok neexistuje, keďže máme aspoň dva minimálne prvky.

Maximálne prvky neexistujú, keďže pre každé $a \in \mathbb{N}$ platí $a \sqsubset a + 9$, keďže $(a + 9)^2 - a^2 = a^2 + 18a + 81 - a^2 = 9(2a + 9)$ a $2a + 9 \in \mathbb{N}$.

Najväčší prvok neexistuje, keďže neexistuje maximálny prvok.

Komentár Chceme upozorniť na problémy pri zdôvodňovaní, že neexistuje najmenší / najväčší prvok:

- „Najmenší prvok neexistuje, lebo existujú neporovnateľné prvky napr. 0 a 1.“ Toto nie je správny dôkaz. Napr. množina $\mathbb{N}$ usporiadaná reláciou $|$ (delí) má najmenší prvok 1 napriek tomu, že prvky 2 a 3 sú neporovnateľné.
- „Najmenší prvok neexistuje, lebo nemáme práve jeden minimálny prvok.“ Toto je správny dôvod, len chceme upozorniť, že ide len o jednosmernú implikáciu. Pokiaľ máme len jeden minimálny prvok, ešte to neznamena, že ide o najmenší (príklad by ste mali byť schopní vymyslieť, je to užitočné cvičenie k príprave na skúšku).
- „Najväčší prvok neexistuje, lebo množina $\mathbb{N}$ je zhora neohraničená.“ Toto je úplne irelevantný argument, lebo hovorí o bežnom usporiadaní $\leq$ a nie o usporiadaní $\sqsubseteq$, o ktorom je úloha. Napr. usporiadaná množina $(\mathbb{N}, |)$ má najväčší prvok 0.

Úloha 3

(1,5 boda) Nech M je množina všetkých nekonečných binárnych postupností (teda každý člen je 0 alebo 1), ktoré neobsahujú tri jednotky vedľa seba a zároveň neobsahujú dve nuly vedľa seba. Rozhodnite a následne dokážte, či je množina M spočítateľná.

Riešenie cez injekciu

Definujme zobrazenie $f: \{0, 1\}^{\mathbb{N}} \rightarrow M$, ktoré každej binárnej postupnosti $a = (a_0, a_1, \dots) \in \{0, 1\}^{\mathbb{N}}$ priradí postupnosť nasledovne: pre každé $i \in \mathbb{N}$ nahradí a_i postupnosťou $(1, 0)$, ak $a_i = 0$, alebo postupnosťou $(1, 1, 0)$, ak $a_i = 1$; potom všetky tieto postupnosti spojí do jednej. Takto dostaneme postupnosť zloženú z blokov $(1, 0)$ a $(1, 1, 0)$, ktorá zjavne neobsahuje $(0, 0)$ ani $(1, 1, 1)$, teda je v množine M . Keďže každý blok sa končí nulou, vieme tieto bloky jednoznačne spätne identifikovať. Ak sa dve postupnosti a, b líšia na i -tom mieste, tak ich obrazy $f(a), f(b)$ sa budú líšiť v i -tom bloku. Preto $a \neq b \Rightarrow f(a) \neq f(b)$, teda zobrazenie f je injektívne. Preto $|M| \geq |\{0, 1\}^{\mathbb{N}}| > \aleph_0$ a teda množina M je nespočítateľná.

Riešenie cez bijekciu

V úlohe sa dala tiež nájsť aj bijekcia. Uvedieme rovno dve, jedným aj druhým smerom, čo využijeme pri zdôvodnení, že naozaj ide o bijekciu.

Definujme zobrazenie $f: \{0, 1\}^{\mathbb{N}} \rightarrow M$, ktoré každej nekonečnej binárnej postupnosti $a = (a_0, a_1, a_2, \dots) \in \{0, 1\}^{\mathbb{N}}$ priradí postupnosť z M tak, že začne s postupnosťou $b = (0)$, ak $a_0 = 0$, alebo s prázdnu postupnosťou $b = ()$, ak $a_0 = 1$. Potom postupne pre každé $i \in \mathbb{N}^+$:

- ak $a_i = 0$, tak na koniec postupnosti b pridá $(1, 0)$;
- ak $a_i = 1$, tak na koniec postupnosti b pridá $(1, 1, 0)$.

Takto vytvorená postupnosť $b = f(a)$ obsahuje len 0 a 1 neobsahuje $(0, 0)$ ani $(1, 1, 1)$: Po prvom kroku môže mať $(1, 0)$, $(1, 1, 0)$, $(0, 1, 0)$, $(0, 1, 1, 0)$, čo sedí. Po prvom a každom ďalšom kroku vytvárania sa končí na

$(1, 0)$, k čomu môžeme pridať aj $(1, 0)$, aj $(1, 1, 0)$ (ak by sme chceli byť veľmi poriadni, tak by sme to mali dokázať indukciou). Teda naozaj ide o zobrazenie do množiny M .

Definujeme zobrazenie $g: M \rightarrow \{0, 1\}^{\mathbb{N}}$, ktoré zobrazí postupnosť $b = (b_0, b_1, \dots) \in M$ na binárnu postupnosť nasledovne. Keďže postupnosť b neobsahuje $(0, 0)$, tak ju nuly delia na niekoľko úsekov jednotiek. Keďže b neobsahuje $(1, 1, 1)$, tak medzi nulami máme vždy jednu alebo dve jednotky. Akurát pred prvou nulou sa môžu nachádzať 0, 1 aj 2 jednotky. Postupnosť b má teda tvar

$$(0, 1^{a_0}, 0, 1^{a_1}, 0, 1^{a_2}, 0, \dots) \quad \text{alebo} \quad (1^{a_0}, 0, 1^{a_1}, 0, 1^{a_2}, 0, \dots),$$

kde $a_i \in \{1, 2\}$ pre každé $i \in \mathbb{N}$ a 1^c značí úsek c jednotiek po sebe. Postupnosť b zobrazíme na

$$g(b) = (c, a_0 - 1, a_1 - 1, a_2 - 1, \dots),$$

kde $c = 0$ ak sa postupnosť b začína nulou, inak $c = 1$.

Lahko overíme, že $f \circ g$ aj $g \circ f$ sú identity, preto sú obe zobrazenia bijekcie [Škoviera, Tvrdenie 2.9].

Riešenie cez diagonálnu metódu

Pre spor predpokladajme, že množina M je spočítateľná. Potom možno všetky jej prvky zoradiť do postupnosti $(a_0, a_1, \dots)$. Prvok na j -tom mieste postupnosti a_i budeme označovať $a_{i,j}$. Teraz definujeme postupnosť b pomocou nasledovného algoritmu. Začneme s postupnosťou $b = (0, 1)$ dĺžky 2. Potom postupne pre každé $n \in \mathbb{N}$ vykonáme nasledovné:

- (i) Nech i je dĺžka doterajšej postupnosti $b = (b_0, b_1, \dots, b_{i-1})$.
- (ii) Ak $a_{n,i} = 0$, tak b predĺžime na postupnosť $(b_0, b_1, \dots, b_{i-1}, 1, 0, 1)$.
- (iii) Ak $a_{n,i} = 1$, tak b predĺžime na postupnosť $(b_0, b_1, \dots, b_{i-1}, 0, 1)$.

Pred každým krokom $n \in \mathbb{N}$ sa postupnosť b končí na $(0, 1)$ a neobsahuje ani tri jednotky po sebe, ani dve nuly po sebe (takejto vlastnosti sa hovorí invariant). To dokážeme priamočiaro matematickou indukciou:

1. Pred krom 0 máme $b = (0, 1)$, čo sedí.
2. Ak pred krokom n sa b končí na $(0, 1)$, tak v krokoch (ii) a (iii) nevytvoríme ani tri jednotky, ani dve nuly. Taktiež sa bude nová postupnosť b (pred krokom $n + 1$) bude končiť na $(0, 1)$.

Keďže b je binárna postupnosť neobsahujúca $(1, 1, 1)$ ani $(0, 0)$, tak patrí do M a teda sa nachádza v postupnosti $(a_0, a_1, \dots)$.

Navyše, krokom (ii) alebo (iii) si zaručíme, že pre každé $n \in \mathbb{N}$ sa postupnosť b líši od postupnosti a_n na indexe i (podľa vtedajšej hodnoty i). Preto sa postupnosť b nenachádza v postupnosti $(a_0, a_1, \dots)$, čo je spor s predošlým odsekom.

Poznámka. Spôsobov, ako tvoriť postupnosť b je mnoho, najmä takýchto algoritmických. Dôležité je uviesť si, že nemusíme ísť čisto po diagonále a vieme ovplyvňovať, ktorý prvok zmeníme z postupnosti a_n .