Milé čtenářky, milí čtenáři,

vypadá to, že pravděpodobnost není objektivní vlastností světa, ale konstrukcí založenou na osobním nebo kolektivním úsudku. Hodím-li minci na stůl a rychle ji zakryju, pak subjektivní pravděpodobnost, že padla panna, je jiná pro toho, kdo si výsledku před zakrytím stihl všimnout (0 nebo 100 procent) a jiná pro toho, kdo výsledek neviděl (50 procent). A objektivní pravděpodobnost? Ta pravděpodobně neexistuje.

Tak nějak uvažuje David Spiegelhalter ve svém eseji *Why probability probably does not exist (but it is useful to act like it does)* uveřejněném v časopisu Nature. V nejnovějším dvojčísle Kvaternionu se v úvodním článku Mateje Benka přesvědčíme, že pravděpodobnostní pohled může být užitečný i v proslulém problému, jejž česká wikipedie označuje za pravděpodobně nejznámější příklad parciální diferenciální rovnice parabolického typu: v rovnici vedení tepla.

Druhý článek Kvaternionu autora Jiřího Klašky se zabývá kubickými a kvartickými polynomy: konkrétně úlohou Borise Deloneho zformulovanou v roce 1940: jak najít všechny normované kubické polynomy s celočíselnými koeficienty mající daný diskriminant – a její analogií pro stupeň 4.

Kuželosečky se studují už od časů Platónových; ovšem zásadní impuls k jejich zkoumání dodal Johannes Kepler učiniv je „klíčem k nebesům“. A že stále nejde o téma vyčerpané, dokazuje i článek Pavla Loučky věnující se konstrukcím kuželoseček ze skupin bodů.

Studentskou prací do dvojčísla přispěla Alžběta Kočendová za drobné asistence autora této předmluvy: představuje užití Schurových doplňků pro výpočet inverzní matice. Možná vhodné rozšiřující téma pro lineární algebru. Posledním příspěvkem nového Kvaternionu jsou zajímavé příklady z internetové matematické soutěže MATHING, které přesvědčivě objasňuje a špatné postupy vyvrací Viera Štoudková Růžičková.

Milé čtenářky a milí čtenáři, subjektivní pravděpodobnost jevu, že se Vám dostane do rukou dvojčíslo Kvaternionu 2024, v tuto chvíli znáte. Za celý redakční kolektiv Vám přeju jeho obohacující a podnětné čtení, které vás bude co nejvíc inspirovat.

Miroslav Kureš

RÔZNE POHĽADY NA ROVNICU VEDENIA TEPLA

MATEJ BENKO

Abstrakt. V tomto článku diskutujeme tri rôzne interpretácie rovnice vedenia tepla (parabolická parciálna diferenciálna rovnica). Najskôr ukážeme, že pozdĺž každého jej slabého riešenia klesá funkcionál, ktorý reprezentuje energiu systému. Pokračujeme úvahou, že pokiaľ jej riešenie reprezentujeme ako hustotu pravdepodobnosti a uvažujeme priestor pravdepodobnostných mier, riešenie môžeme interpretovať ako krivky, ktoré generujú gradientný tok po funkcionáli, ktorý reprezentuje zápornú Boltzmannovu entropiu. Toto zodpovedá fyzikálnym zákonom. Na záver si ukážeme, že riešenie tejto rovnice vieme tiež interpretovať ako hustotou pravdepodobnosti riešenia stochastického procesu (konkrétne Brownovho pohybu).

1. Úvod

Budeme študovať rovnicu vedenia tepla s počiatočnou podmienkou, uvažujeme teda úlohu

$$\begin{cases} \dfrac{\partial \varrho}{\partial t} = \Delta \varrho, \\ \varrho(\cdot, 0) = \varrho_0. \end{cases} \tag{1.1}$$

Funkcia ϱ predstavuje teplotu v bode x a v čase t. Riešenie úlohy (1.1) hľadáme na množine $\mathbb{R}^d \times [0, T)$, kde $T < +\infty$, a uvažujeme ho v *slabom zmysle*.

Rovnicu z každej strany vynásobíme testovacou funkciou φ z priestoru $C_c^\infty(\mathbb{R}^d \times [0, T))$, ktorý obsahuje funkcie s kompaktným nosičom majúce parciálne derivácie všetkých rádov. Túto funkciu spojito dodefinujeme tak, že $\varphi(\cdot, T) = 0$. Obe strany zintegrujeme a dostaneme

$$\int_0^T \int_{\mathbb{R}^d} \varphi \frac{\partial \varrho}{\partial t} \,\mathrm{d}x \,\mathrm{d}t = \int_0^T \int_{\mathbb{R}^d} \varphi \,\Delta \varrho \,\mathrm{d}x \,\mathrm{d}t \qquad \forall \varphi \in C_c^\infty(\mathbb{R}^d \times [0, T)).$$

Na ľavej strane zameníme poradie integrácie a integrujeme per partes:

$$\begin{aligned} \int_0^T \int_{\mathbb{R}^d} \varphi \,\frac{\partial \varrho}{\partial t} \,\mathrm{d}x \,\mathrm{d}t &= \int_{\mathbb{R}^d} \int_0^T \varphi \,\frac{\partial \varrho}{\partial t} \,\mathrm{d}t \,\mathrm{d}x \\ &= \int_{\mathbb{R}^d} \left(\varrho(\cdot, T)\varphi(\cdot, T) - \varrho(\cdot, 0)\varphi(\cdot, 0) - \int_0^T \varrho \,\frac{\partial \varphi}{\partial t} \,\mathrm{d}t \right) \mathrm{d}x \end{aligned}$$

2010 *MSC.* Primární 60H30, 60J65, 35K05; Sekundární 49J50, 60H05.

Klíčová slova. Gradientný tok, parabolická parciálna diferenciálna rovnica, stochastická diferenciálna rovnica.

$$= -\int_{\mathbb{R}^d} \varphi(\cdot,0)\varrho_0 \,\mathrm{d}x - \int_0^T \int_{\mathbb{R}^d} \varrho \,\frac{\partial \varphi}{\partial t} \,\mathrm{d}x \,\mathrm{d}t.$$

Podobne na pravej strane použijeme Greenovu vetu a získame

$$\int_0^T \int_{\mathbb{R}^d} \varphi \,\Delta\varrho \,\mathrm{d}x \,\mathrm{d}t = -\int_0^T \int_{\mathbb{R}^d} \nabla\varphi \cdot \nabla\varrho \,\mathrm{d}x \,\mathrm{d}t.$$

Porovnaním upravenej ľavej a pravej strany získame slabú formuláciu problému. Riešením úlohy (1.1) budeme chápať „rozumnú“ funkciu ϱ, ktorá spĺňa

$$-\int_{\mathbb{R}^d} \varphi(\cdot,0)\,\varrho_0 \,\mathrm{d}x = \int_0^T \int_{\mathbb{R}^d} \varrho \,\frac{\partial \varphi}{\partial t} \,\mathrm{d}x \,\mathrm{d}t - \int_0^T \int_{\mathbb{R}^d} \nabla\varphi \cdot \nabla\varrho \,\mathrm{d}x \,\mathrm{d}t \qquad \forall \varphi \in C_c^\infty(\mathbb{R}^d \times [0,T)). \tag{1.2}$$

V prvej z našich úvah slovami „rozumná funkcia“ chápeme funkciu ϱ takú, že pre skoro každé t je funkcia $\varrho(\cdot,t)$ z priestoru $W_0^{1,2}(\mathbb{R}^d)$. Je to *Sobolevov priestor* funkcií na $\mathbb{R}^d$, ktoré v „nekonečne“ idú k nule a ich slabé derivácie prvého rádu sú Lebesgueovsky integrovateľné v druhej mocnine. Je známe, že také riešenie úlohy (1.1) existuje, ak $\varrho_0 \in W_0^{1,2}(\mathbb{R}^d)$.

V ďalších dvoch úvahách budeme hľadať riešenie ϱ tak, že pre skoro každé t bude $\varrho(\cdot,t)$ hustotou pravdepodobnosti. Hustoty musia dostatočne rýchlo klesať v „nekonečne“ k nule, aby sa zabezpečil jednotkový integrál hustoty cez celý priestor.

V našej prvej úvahe chceme rozumieť funkcii teploty ϱ tak, že príroda sa snaží minimalizovať energiu uvažovaného systému. To znamená, že riešenie ϱ budeme interpretovať ako krivku v abstraktnom priestore, ktorá predstavuje najrýchlejšie klesanie energie telesa. Takúto krivku budeme nazývať *gradientný tok*.

Zavedieme pojem gradientného toku na Hilbertovom priestore. Dostaneme sa k prvému výsledku. Ten hovorí, že na Hilbertovom priestore rovnica vedenia tepla generuje gradientný tok po Dirichletovej energii (ktorú reprezentujeme ako funkcionál na Hilbertovom priestore).

Následne definujeme gradientný tok na metrickom priestore náhodných veličín s tzv. Wassersteinovou metrikou (tento priestor nie je lineárny) a ukážeme, že riešenie rovnice vedenia tepla generuje gradientný tok po záporne vzatej Boltzmannovej entropii. V tomto prípade môžeme interpretovať riešenie ϱ v rôznych časoch ako hustoty pravdepodobnosti.

Na záver nadviažeme na myšlienku reprezentácie riešenia ako pravdepodobnostnej miery, resp. náhodnej veličiny. Ukážeme si, že riešenie ϱ v slabej formulácii je ekvivalentné riešeniu stochastickej diferenciálnej rovnice. V tomto prípade Brownovmu pohybu, ktorý sa v teórii stochastických procesov tiež nazýva Wienerov proces.

V nasledujúcej kapitole diskutujeme gradientný tok na Hilbertovom priestore $L^2(\mathbb{R}^d)$. Pre názornosť si teraz uvedieme gradientný tok na Euklidovom priestore. Nech má funkcia $f\colon \mathbb{R}^d \to \mathbb{R}$ spojité parciálne derivácie prvého rádu (t.j. $f \in C^1(\mathbb{R}^d)$). Potom pre každé $x_0 \in \mathbb{R}^d$ je fázová trajektória riešenia $x\colon [0,+\infty) \to \mathbb{R}^d$

počiatočnej úlohy

$$\begin{cases} \dot{x} = -\nabla f(x), \\ x(0) = x_0 \end{cases} \tag{1.3}$$

krivkou v priestore $\mathbb{R}^d$, ktorú nazývame *gradientný tok* na $\mathbb{R}^d$ po funkcii f.

Všimnime si, že dotykový vektor $\dot{x}(t)$ gradientného toku v bode $x(t)$ je rovný zápornе vzatému gradientu $-\nabla f(x(t))$ a preto určuje smer najstrmšieho klesania funkcie f.

2. Gradientný tok na $L^2(\mathbb{R}^d)$

Pojem gradietný tok na $\mathbb{R}^d$ zovšeobecníme, zavedieme pojem gradietný tok na priestore $L^2(\mathbb{R}^d)$. Pre súlad s literatúrou (a tiež kvôli tomu, že smerujeme k popisu gradientného toku na abstraktnejších priestoroch), budeme namiesto s pojmom gradient funkcie pracovať s pojmom subdiferenciál funkcionálu.

Definujme teda najskôr subdiferenciál na všeobecnom Hilbertovom priestore H.

Definícia 2.1 (Fréchetov subdiferenciál na H)**.** Nech je H Hilbertov priestor a $F\colon H \to \mathbb{R} \cup \{+\infty\}$ je funkcionál definovaný na celom H. *Fréchetovym subdiferenciálom* nazývame viachodnotový operátor $\partial F\colon H \to 2^H$ definovaný vzťahom

$$\partial F[u] = \left\{ \xi \in H;\ F[v] \geq F[u] + \langle \xi, v - u \rangle \ \forall v \in H \right\} \quad \text{pre } u \in H.$$

Teraz, definujeme gradientný tok na $L^2(\mathbb{R}^d)$.

Definícia 2.2 (Gradientný tok na $L^2(\mathbb{R}^d)$)**.** Abstraktnú funkciu $u\colon [0,T) \to L^2(\mathbb{R}^d)$ nazveme *gradientným tokom* na $L^2(\mathbb{R}^d)$ po funkcionáli $F\colon L^2(\mathbb{R}^d) \to \mathbb{R}$ s počiatočným bodom $u_0 \in L^2(\mathbb{R}^d)$, ak pre skoro všetky $t \in [0,T)$ existuje $\dot{u}(t)$, $\partial F[u(t)] \neq \emptyset$ a platí

$$-\dot{u}(t) \in \partial F[u(t)] \quad \text{pre s. v. } t \in [0,T), \quad u(0) = u_0.$$

Pristúpime k výsledku našej prvej úvahy a to, že každé riešenie rovnice vedenia tepla generuje gradientný tok po tzv. Dirichletovej energii.

Veta 2.3. *Na $L^2(\mathbb{R}^d)$ uvažujme funkcionál*

$$F[u] := \begin{cases} \frac{1}{2} \int_{\mathbb{R}^d} \|\nabla u\|^2 \,\mathrm{d}x & \text{pre } u \in W_0^{1,2}(\mathbb{R}^d), \\ +\infty & \text{inak}, \end{cases} \tag{2.1}$$

ktorý popisuje tzv. Dirichletovu energiu. Potom pre každé $u \in W_0^{1,2}(\mathbb{R}^d)$ platí

$$\partial F[u] \neq \emptyset \quad \Leftrightarrow \quad \Delta u \in L^2(\mathbb{R}^d).$$

Ak $u \in W_0^{1,2}(\mathbb{R}^d)$ a $\Delta u \in L^2(\mathbb{R}^d)$, potom

$$\partial F[u] = \{-\Delta u\}.$$

Dôsledok 2.4. *Každý gradientný tok po funkcionáli F definovaným vzťahom* (2.1) *na priestore $L^2(\mathbb{R}^d)$ generuje nejaké riešenie rovnice vedenia tepla v slabom zmysle a naopak.*

Pre ukážku aparátu používaného v teórii gradientných tokov na priestore $L^2(\mathbb{R}^d)$ uvedieme dôkaz vety 2.3.

Dôkaz vety 2.3. „⇒“: Nech $u \in W_0^{1,2}(\mathbb{R}^d)$ a funkcia $\xi \in L^2(\mathbb{R}^d)$ je prvkom subdiferenciálu $\partial F[u]$. Potom podľa definície 2.1 platí

$$F[v] \geq F[u] + \langle \xi, v - u \rangle \quad \forall v \in L^2(\mathbb{R}^d). \tag{2.2}$$

Zoberieme funkciu $v = u + \varepsilon w$, kde $w \in W_0^{1,2}(\mathbb{R}^d)$ a $\varepsilon > 0$. Dosadíme do nerovnosti v (2.2), všimneme si, že $v - u = \varepsilon w$ a získame vzťah

$$\frac{1}{2}\int_{\mathbb{R}^d} \|\nabla(u + \varepsilon w)\|^2 \,\mathrm{d}x - \frac{1}{2}\int_{\mathbb{R}^d} \|\nabla u\|^2 \,\mathrm{d}x \geq \varepsilon \int_{\mathbb{R}^d} \xi w \,\mathrm{d}x. \tag{2.3}$$

Úpravou

$$\|\nabla(u + \varepsilon w)\|^2 = \|\nabla u + \varepsilon \nabla w\|^2 = \|\nabla u\|^2 + 2\varepsilon \nabla u \cdot \nabla w + \varepsilon^2 \|\nabla w\|^2$$

a dosadením do (2.3) získame

$$\varepsilon \int_{\mathbb{R}^d} \nabla u \cdot \nabla w \,\mathrm{d}x + \frac{\varepsilon^2}{2}\int_{\mathbb{R}^d} \|\nabla w\|^2 \,\mathrm{d}x \geq \varepsilon \int_{\mathbb{R}^d} \xi w \,\mathrm{d}x.$$

Vydelíme ε, prejdeme k limite pre $\varepsilon \to 0$ a získame tak

$$\int_{\mathbb{R}^d} \nabla u \cdot \nabla w \,\mathrm{d}x \geq \int_{\mathbb{R}^d} \xi w \,\mathrm{d}x \quad \forall w \in W_0^{1,2}(\mathbb{R}^d),$$

čo je možné s využitím Greenovej vety na ľavej strane nerovnosti prepísať do tvaru

$$-\int_{\mathbb{R}^d} w \Delta u \,\mathrm{d}x \geq \int_{\mathbb{R}^d} \xi w \,\mathrm{d}x \quad \forall w \in W_0^{1,2}(\mathbb{R}^d). \tag{2.4}$$

Keďže nerovnosť v (2.4) platí pre ľubovoľnú funkciu z priestoru $W_0^{1,2}(\mathbb{R}^d)$, môžeme uvažovať tiež funkciu $-w \in W_0^{1,2}(\mathbb{R}^d)$ (pretože je lineárnym priestorom) a získame

$$\int_{\mathbb{R}^d} w \Delta u \,\mathrm{d}x \geq -\int_{\mathbb{R}^d} \xi w \,\mathrm{d}x \quad \forall w \in W_0^{1,2}(\mathbb{R}^d). \tag{2.5}$$

Porovnaním nerovností (2.4) a (2.5) získame

$$\int_{\mathbb{R}^d} w \Delta u \,\mathrm{d}x = -\int_{\mathbb{R}^d} \xi w \,\mathrm{d}x \quad \forall w \in W_0^{1,2}(\mathbb{R}^d).$$

Odtiaľ plynie $\xi = -\Delta u$, a preto $-\Delta u \in \partial \mathcal{F}[u]$ a $\Delta u \in L^2(\mathbb{R}^d)$.

„⇐“: Predpokladajme, že $u \in W_0^{1,2}(\mathbb{R}^d)$ je také, že $\Delta u \in L^2(\mathbb{R}^d)$. Potom podľa (2.1) pre každé $w \in W_0^{1,2}(\mathbb{R}^d)$ platí

$$\begin{aligned} F[u + w] - F[u] &= \frac{1}{2}\int_{\mathbb{R}^d} \|\nabla(u + w)\|^2 \,\mathrm{d}x - \frac{1}{2}\int_{\mathbb{R}^d} \|\nabla u\|^2 \,\mathrm{d}x \\ &= \int_{\mathbb{R}^d} \nabla u \cdot \nabla w \,\mathrm{d}x + \frac{1}{2}\int_{\mathbb{R}^d} \|\nabla w\|^2 \,\mathrm{d}x \\ &\geq \int_{\mathbb{R}^d} \nabla u \cdot \nabla w \,\mathrm{d}x = -\int_{\mathbb{R}^d} w \Delta u \,\mathrm{d}x. \end{aligned}$$

V prípade, že $w \in L^2(\mathbb{R}^d)$, avšak $w \notin W_0^{1,2}(\mathbb{R}^d)$, z (2.1) je zrejmé, že

$$F[u+w] = +\infty \geq F[u] - \int_{\mathbb{R}^d} w\Delta u \,\mathrm{d}x.$$

Dokázali sme, že

$$F[u+w] - F[u] \geq -\int_{\mathbb{R}^d} w\Delta u \,\mathrm{d}x = \langle -\Delta u, w\rangle \quad \forall w \in L^2(\mathbb{R}^d)$$

a teda podľa definície subdiferenciálu je $-\Delta u \in \partial F[u]$. □

3. Wassersteinova metrika

V tejto kapitole zavedieme metriku na priestore pravdepodobnostných mier, ktorý označíme $\mathscr{P}(\mathbb{R}^d)$. Pravdepodobnostné miery určujú náhodné veličiny na $\mathbb{R}^d$, t.j. $X \sim \mu$, kde $\mu \in \mathscr{P}(\mathbb{R}^d)$. Poznačme, že je možné (nad rámec tohoto článku) nahradiť $\mathbb{R}^d$ Hilbertovym priestorom H. V tomto prípade miery určujú rozdelenie stochastických procesov. Priestor H však nie je tzv. *lokálne kompaktný* a teda tieto miery nemajú hustotu, resp. pravdepodobnostnú funkciu.

Kvôli prehľadnosti sa obmedzíme na priestor absolútne spojitých pravdepodobnostných mier voči Lebesgueovej miere, ktorý budeme značiť $\mathscr{P}^{\mathrm{ac}}(\mathbb{R}^d)$. Tento podpriestor určuje rozdelenie spojitých náhodných veličín. Toto má niekoľko dôvodov. Po prvé, popísať vlastnosti, ktoré plánujeme na tomto podpriestore je názornejšie a stručnejšie, ale je možné (avšak technicky náročnejšie) popis rozšíriť na všetky pravdepodobnostné miery. Po druhé, je možné ukázať, že riešenie rovnice vedenia tepla v slabej formulácii určuje v skoro každom čase hustotu absolútne spojitej pravdepodobnostnej miery.

Uvažujeme mieru $\mu \in \mathscr{P}^{\mathrm{ac}}(\mathbb{R}^d)$ s hustotou ϱ. Potom pre každú merateľnú množinu $A \subseteq \mathbb{R}^d$ máme

$$\mu(A) = \int_A \varrho(x)\,\mathrm{d}x\,; \qquad \varrho = \frac{\mathrm{d}\mu}{\mathrm{d}x}\,, \tag{3.1}$$

kde výraz $\mathrm{d}\mu/\mathrm{d}x$ značí tzv. *Radonovu-Nikodýmovu deriváciu* [3, Section 1.6.1]. Keďže hustota ϱ jednoznačne určuje mieru μ, stotožníme označenie miery a hustoty.

Uvedieme si pojem moment náhodnej veličiny, s ktorým budeme pracovať.

Definícia 3.1 (Moment náhodnej veličiny)**.** Nech je rozdelenie náhodnej veličiny X určené hustotou ϱ. Potom jej *moment cez funkciu* $f\colon \mathbb{R}^d \to \mathbb{R}$ definujeme vzťahom

$$\mathbb{E}[f(X)] := \int_{\mathbb{R}^d} f(x)\,\varrho(x)\,\mathrm{d}x.$$

Uvažujeme miery s konečným druhým momentom, $\mathscr{P}_2^{\mathrm{ac}}(\mathbb{R}^d) \subset \mathscr{P}(\mathbb{R}^d)$, t.j.

$$\mathscr{P}_2^{\mathrm{ac}}(\mathbb{R}^d) := \left\{ \varrho \in \mathscr{P}^{\mathrm{ac}}(\mathbb{R}^d);\ \int_{\mathbb{R}^d} \|x\|^2\,\varrho(x)\,\mathrm{d}x < +\infty \right\},$$

ekvivalentne

$$\mathscr{P}_2^{\mathrm{ac}}(\mathbb{R}^d) := \left\{ \varrho \in \mathscr{P}^{\mathrm{ac}}(\mathbb{R}^d);\ \varrho = \mathrm{Law}(X),\ \mathbb{E}\big[\|X\|^2\big] < +\infty \right\}.$$

Teraz si popíšeme, čo je *push-forward operátor*. Určuje transformáciu mier, resp. zobrazenie medzi nimi. V reči klasickej štatistiky sa jedná zobrazenie náhodných veličín. Ak máme náhodnú veličinu $X \sim \varrho$ a jej transformáciu danú zobrazením T, potom hustotou pravdepodobnosti náhodnej veličiny $T(X)$ značíme $T_{\#}\varrho$ a operátor $T_{\#}$ nazývame push-forward operátor cez zobrazenie T. To znamená, že $T_{\#}$ popisuje transformáciu náhodných veličín v reči pravdepodobnostných mier.

Veta 3.2 (Zmena premenných)**.** *Nech je $T : X \to Y$ zobrazenie, $\varrho \in \mathscr{P}^{\mathrm{ac}}(\mathbb{R}^d)$ hustota pravdepodobnosti a $T_{\#}\varrho$ je jej push-forward hustota pravdepodobnosti cez zobrazenie T. Potom pre všetky prípustné funkcie $f : Y \to \mathbb{R} \cup \{+\infty\}$ platí*

$$\int_{\mathbb{R}^d} f(x)\, T_{\#}\varrho(x)\,\mathrm{d}x = \int_{\mathbb{R}^d} f(T(x))\,\varrho(x)\,\mathrm{d}x.$$

Popíšeme si formu charakterizácie push-forward operátora pomocou vety o substitúcii integrálu. Túto charakterizáciu využijeme neskôr pri určovaní subdiferenciálu konkrétneho funkcionálu (entropie), viď str. 11.

Veta 3.3 (Zmena premenných cez jakobián)**.** *Nech je $T : \mathbb{R}^d \to \mathbb{R}^d$ zobrazenie, $\varrho \in \mathscr{P}^{\mathrm{ac}}(\mathbb{R}^d)$ je hustota pravdepodobnosti a $\varphi = T_{\#}\varrho$. Ak $\det \nabla T > 0$, potom platí*

$$\varphi(T(x))\,\det \nabla T(x) = \varrho(x) \quad \forall x \in \mathbb{R}^d.$$

Dôkaz. Z vety 3.2 o zmene premenných plynie pre všetky prípustné funkcie $f : Y \to \mathbb{R} \cup \{+\infty\}$

$$\int_{\mathbb{R}^d} f(y)\,\varphi(y)\,\mathrm{d}y = \int_{\mathbb{R}^d} f(y)\,\mathrm{d}T_{\#}\varrho(y)\,\mathrm{d}y = \int_{\mathbb{R}^d} f(T(y))\,\varrho(y)\,\mathrm{d}y.$$

Vykonáme transformáciu $y = T(x)$ v integráli na ľavej strane predchádzajúceho vzťahu a z vety o substitúcii tak dostaneme

$$\int_{\mathbb{R}^d} f(T(x))\varphi(T(x))\det \nabla T(x)\,\mathrm{d}x = \int_{\mathbb{R}^d} f(T(x))\varrho(x)\,\mathrm{d}x.$$

Keďže funkcia f je ľubovoľná, získame $\varphi(T(x))\,\det \nabla T(x) = \varrho(x)$ pre každé $x \in \mathbb{R}^d$. □

Definovali sme všetky potrebné pojmy a môžeme pristúpiť k definícii Wassersteinovej vzdialenosti.

Definícia 3.4 (Wassersteinova vzdialenosť)**.** *Wassersteinova vzdialenosť* medzi dvoma pravdepodobnostnými mierami $\varrho^1, \varrho^2 \in \mathscr{P}_2^{\mathrm{ac}}(\mathbb{R}^d)$ je definovaná vzťahom

$$W_2(\varrho^1, \varrho^2) := \sqrt{\inf\left\{\mathbb{E}\left[\|X - Y\|^2\right];\ X \sim \varrho^1, Y \sim \varrho^2\right\}}\,.$$

Poznámka 3.5 (W_2 je optimálna cena prepravy). Wassersteinovu vzdialenosť W_2 vieme interpretovať ako optimálnu cenu prepravy tovaru, ktorý je rozdelený podľa hustoty ϱ^1 na nové miesta (napr. z tovární do predajní), ktoré sú rozdelené podľa hustoty ϱ^2. Keďže pracujeme s hustotami pravdepodobnosti, množstvo tovaru je stále konštantné (integrál pravdepodobnostnej miery cez celý priestor je 1).

Uvažovaním diskrétnych mier (nie náš prípad) by integrálna formulácia prešla na sumu a variačný problém na klasický problém optimalizácie prepravy tovaru s cenou prepravy, ktorá zodpovedá druhej mocnine Euklidovskej vzdialenosti medzi miestami $\|x_i - y_i\|^2$.

Veta 3.6 ([2, Theorem 2.2])**.** *Wassersteinova vzdialenosť W_2 je metrika na priestore pravdepodobnostných mier s konečným druhým momentom $\mathscr{P}_2^{\mathrm{ac}}(\mathbb{R}^d)$.*

4. Subdiferenciál na priestore $(\mathscr{P}_2^{\mathrm{ac}}(\mathbb{R}^d), W_2)$

V predchádzajúcej kapitole sme ukázali, že na množine $\mathscr{P}_2^{\mathrm{ac}}(\mathbb{R}^d)$ vieme zaviesť metriku W_2 a získame metrický priestor. Priestor $\mathscr{P}_2^{\mathrm{ac}}(\mathbb{R}^d)$ však nie je ani lineárnym priestorom (pre $d > 1$) a je preto potrebné definovať subdiferenciál iným spôsobom než v kapitole 2.

Felix Otto v článku [8] popísal tento priestor ako istý typ slabej nekonečne rozmernej Riemannovskej variety. Ku každému prvku $\nu \in \mathscr{P}_2^{\mathrm{ac}}(\mathbb{R}^d)$ zostrojil dotykový priestor (bundle) ako podmnožinu váhového Hilbertovho priestoru $L^2(\nu; \mathbb{R}^d)$, tento priestor je zavedený na str. 10. S takouto úvahou potom bolo možné definovať subdiferenciál ako podmnožinu dotykového priestoru. S použitím subdiferenciálu potom vieme ukázať spojitosť medzi riešeniami niektorých parabolických parciálnych diferenciálnych rovníc (v našom prípade rovnica vedenia tepla) a gradientných tokov na priestore $\mathscr{P}_2^{\mathrm{ac}}(\mathbb{R}^d)$.

Budeme pracovať s konečným časom $T < +\infty$, avšak rovnaké výsledky sa dajú ukázať aj pre $T \to +\infty$. Najskôr zavedieme pojem absolútne spojitá krivka na metrickom priestore $(\mathscr{P}_2^{\mathrm{ac}}(\mathbb{R}^d), W_2)$.

Definícia 4.1. Abstraktná funkcia $u\colon [0,T) \to \mathscr{P}_2^{\mathrm{ac}}(\mathbb{R}^d)$ sa nazýva *lokálne absolútne spojitá* vzhľadom k metrike W_2, ak existuje $m \in L_{\mathrm{loc}}([0,T))$ tak, že platí

$$W_2(u(s), u(t)) \le \int_s^t m(r)\,\mathrm{d}r \quad \text{pre každé } 0 \le s \le t < T.$$

Systém funkcií $\{u(t)\}_{t\in[0,T)}$ budeme nazývať (lokálne) *absolútne spojitou krivkou* na metrickom priestore $(\mathscr{P}_2^{\mathrm{ac}}(\mathbb{R}^d), W_2)$.

Uvažujme rovnicu kontinuity

$$\frac{\partial \varrho}{\partial t} + \operatorname{div}(v\varrho) = 0, \tag{4.1}$$

kde $v\colon \mathbb{R}^d \times [0,T) \to \mathbb{R}^d$ je daná vektorová funkcia, ktorá predpisuje vektor rýchlosti hmoty v čase t a bode x. Riešenie tejto rovnice budeme chápať v zmysle distribúcií, t.j. riešením rovnice (4.1) nazývame funkciu $\varrho\colon \mathbb{R}^d \times [0,T) \to \mathbb{R}$ takú, že pre skoro všetky $t \in [0,T)$ je funkcia $\varrho(\cdot,t)$ z priestoru $\mathscr{P}_2^{\mathrm{ac}}(\mathbb{R}^d)$ a spĺňa

$$-\int_{\mathbb{R}^d} \varphi(\cdot,0)\,\varrho(\cdot,0)\,\mathrm{d}x = \int_0^T \int_{\mathbb{R}^d} \varrho \frac{\partial \varphi}{\partial t}\,\mathrm{d}x\,\mathrm{d}t - \int_0^T \int_{\mathbb{R}^d} v \cdot \nabla\varphi\,\varrho\,\mathrm{d}x\,\mathrm{d}t \qquad \forall \varphi \in C_c^\infty(\mathbb{R}^d \times [0,T)). \tag{4.2}$$

Rovnica kontinuity popisuje v hydromechanike šírenie nestlačiteľnej kvapaliny. Keďže transformácia náhodnej veličiny zachováva objem (integrál cez celý priestor je vždy 1), je prirodzené očakávať, že každá absolútne spojitá krivka na priestore pravdepodobnostných mier je generovaná nejakým riešením rovnice (4.1). Pri uvažovaní miery v súvislosti s riešeniami rovnice kontinuity je integrálna podmienka (4.2) prirodzená, pretože miera sama je integrál hustoty, viď (3.1).

Definujme najskôr priestor, ktorého v je prvkom. Z dôsledku [2, Remark 1.22] Brenierovej vety [5, Theorem 2.5.10] plynie, že každý prvok μ (dostatočne malého) okolia hustoty $\nu \in \mathscr{P}_2^{\mathrm{ac}}(\mathbb{R}^d)$ v metrike W_2 je tvaru $\mu = (\mathsf{Id} + \varepsilon\nabla\varphi)_{\#}\nu$, kde funkcia φ je z priestoru $C_c^\infty(\mathbb{R}^d)$ a $\varepsilon \in \mathbb{R}$, pričom symbolom Id značíme identitu na $\mathbb{R}^d$. Týmto komentárom sme chceli naznačiť dôvod, prečo priestor vektorových funkcií popisujúcich zmenu hustoty ν definujeme ako uzáver množiny gradientov hladkých funkcií, viď nasledujúca definícia.

Poznamenajme ešte, že pre každé $\nu \in \mathscr{P}_2^{\mathrm{ac}}(\mathbb{R}^d)$ označíme $L^2(\nu;\mathbb{R}^d)$ Hilbertov priestor vektorových polí $w\colon \mathbb{R}^d \to \mathbb{R}^d$ takých, že $x \mapsto w(x)\cdot w(x)$ je lebesgueovsky integrovateľná na $\mathbb{R}^d$, pričom skalárny súčin v tomto priestore je definovaný vzťahom

$$\langle u, w\rangle_\nu := \int_{\mathbb{R}^d} u(x)\cdot w(x)\,\nu(x)\,\mathrm{d}x.$$

Definícia 4.2 (Dotykový priestor)**.** Nech je $\nu \in \mathscr{P}_2^{\mathrm{ac}}(\mathbb{R}^d)$ hustota. Potom *dotykový priestor* $\mathrm{Tan}_\nu(\mathscr{P}_2^{\mathrm{ac}}(\mathbb{R}^d))$ na $\mathscr{P}_2^{\mathrm{ac}}(\mathbb{R}^d)$ v ν definujeme vzťahom

$$\mathrm{Tan}_\nu(\mathscr{P}_2^{\mathrm{ac}}(\mathbb{R}^d)) := \overline{\{\nabla\varphi\colon \varphi \in C_c^\infty(\mathbb{R}^d)\}}^{L^2(\nu;\mathbb{R}^d)}.$$

Je možné dokázať, že $\mathrm{Tan}_\nu(\mathscr{P}_2^{\mathrm{ac}}(\mathbb{R}^d))$ je podpriestor priestoru $L^2(\nu;\mathbb{R}^d)$. V nasledujúcej vete ukážeme vzťah medzi absolútne spojitými krivkami na priestore $(\mathscr{P}_2^{\mathrm{ac}}(\mathbb{R}^d), W_2)$ a riešeniami rovnice kontinuity (4.1).

Veta 4.3 ([2, Theorem 2.29])**.** *Ak je $\{u(t)\}_{t\in[0,T)}$ absolútne spojitá krivka na metrickom priestore $(\mathscr{P}_2^{\mathrm{ac}}(\mathbb{R}^d), W_2)$, potom funkcia $\varrho\colon \mathbb{R}^d\times[0,T)\to\mathbb{R}$ taká, že $\varrho(\cdot,t) = u(t)$ pre skoro všetky $t\in[0,T)$, je riešením rovnice (4.1) v zmysle distribúcií, v ktorej $v(\cdot,t)\in \mathrm{Tan}_{u(t)}(\mathscr{P}_2^{\mathrm{ac}}(\mathbb{R}^d))$ pre skoro všetky $t\in[0,T)$.*

Opačne, keď ϱ je riešením rovnice (4.1) v zmysle distribúcií, potom je systém funkcií $\{\varrho(\cdot,t)\}_{t\in[0,T)}$ absolútne spojitá krivka na $(\mathscr{P}_2^{\mathrm{ac}}(\mathbb{R}^d), W_2)$.

Teraz pristúpime k definícii Fréchetovho subdiferenciálu na metrickom priestore $(\mathscr{P}_2^{\mathrm{ac}}(\mathbb{R}^d), W_2)$.

Definícia 4.4 (Fréchetov subdiferenciál na priestore $(\mathscr{P}_2^{\mathrm{ac}}(\mathbb{R}^d), W_2)$)**.** Nech je $\mathcal{G}\colon \mathscr{P}_2^{\mathrm{ac}}(\mathbb{R}^d)\to\mathbb{R}\cup\{+\infty\}$ funkcionál. *Fréchetovym subdiferenciálom* nazývame viachodnotový operátor $\partial\mathcal{G}\colon \mathscr{P}_2^{\mathrm{ac}}(\mathbb{R}^d)\to 2^{\mathscr{P}_2^{\mathrm{ac}}(\mathbb{R}^d)}$ definovaný vzťahom

$$\partial\mathcal{G}[\nu] = \left\{\xi\in\mathrm{Tan}_\nu(\mathscr{P}_2^{\mathrm{ac}}(\mathbb{R}^d));\ \mathcal{G}[\mu]-\mathcal{G}[\nu]\geq\langle\xi, T_\nu^\mu - \mathsf{Id}\rangle_\nu\ \forall\mu\in\mathscr{P}_2^{\mathrm{ac}}(\mathbb{R}^d)\right\}$$

pre $\nu\in\mathscr{P}_2^{\mathrm{ac}}(\mathbb{R}^d)$, kde vektorové pole T_ν^μ spĺňa $\mu = (T_\nu^\mu)_{\#}\nu$.

Poznámka 4.5. Vyššie sme uviedli, že $\mathrm{Tan}_\nu(\mathscr{P}_2^{\mathrm{ac}}(\mathbb{R}^d)) \subseteq L_2(\nu;\mathbb{R}^d)$, pravá strana nerovnice v definícii 4.4 je teda definovaná vzťahom $\langle \xi, T_\nu^\mu - \mathsf{Id}\rangle_\nu = \int_{\mathbb{R}^d} \xi(x) \cdot (T_\nu^\mu(x) - x)\,\nu(x)\,\mathrm{d}x$ a vektorové pole T_ν^μ transformuje hustotu ν na hustotu μ.

Teraz zavedieme gradientný tok na metrickom priestore $(\mathscr{P}_2^{\mathrm{ac}}(\mathbb{R}^d), W_2)$ tak, aby analogicky ako v priestore $L^2(\mathbb{R}^d)$, bol v ľubovoľnom bode každý dotykový vektor záporne vzatý prvok subdiferenciálu daného funkcionálu.

Definícia 4.6 (Charakterizácia gradientného toku pomocou subdiferenciálu, [1, Definition 11.1.1])**.** Povieme, že absolútne spojitá krivka $\{u(t)\}_{t\in[0,T)}$ na metrickom priestore $(\mathscr{P}_2^{\mathrm{ac}}(\mathbb{R}^d), W_2)$ je *gradientný tok*, ak pre skoro každé $t \in [0,T)$ platí

$$-w \in \partial\mathcal{G}[u(t)] \quad \forall w \in \mathrm{Tan}_{u(t)}(\mathscr{P}_2^{\mathrm{ac}}(\mathbb{R}^d)).$$

Bez dôkazu uvedieme tvrdenie, ktoré využijeme pri určovaní subdiferenciálu. Toto tvrdenie sa nazýva reťazové pravidlo na $(\mathscr{P}_2^{\mathrm{ac}}(\mathbb{R}^d), W_2)$.

Tvrdenie 4.7 ([1, Propoposition 10.3.18])**.** *Nech $\nu \in \mathscr{P}_2^{\mathrm{ac}}(\mathbb{R}^d)$ a $\varphi \in C_c^\infty(\mathbb{R}^d)$. Položme $\nu^\varepsilon = (\mathsf{Id}+\varepsilon\nabla\varphi)_\#\nu$ pre každé $\varepsilon \in \mathbb{R}$. Potom pre každé $w \in L^2(\nu;\mathbb{R}^d)$ platí*

$$\frac{\mathrm{d}}{\mathrm{d}\varepsilon}\mathcal{F}[\nu^\varepsilon]\Big|_{\varepsilon=0} = \langle w, \nabla\varphi\rangle_\nu \quad \Leftrightarrow \quad w \in \partial\mathcal{F}[\nu].$$

Pristúpime k výsledku, kvôli ktorému sme teóriu gradientných tokov na priestore pravdepodobnostných mier s Wassersteinovou metrikou budovali. Uvažujeme funkcionál popisujúci tzv. vnútornú energiu (resp. záporne vzatú Boltzmannovu entropiu) daný vzťahom

$$\mathcal{F}_e[\nu] = \int_{\mathbb{R}^d} \nu \ln \nu \,\mathrm{d}x \quad \text{pre } \nu \in \mathscr{P}_2^{\mathrm{ac}}(\mathbb{R}^d).$$

V nasledujúcej vete určíme hodnoty subdiferenciálu funkcionálu $\mathcal{F}_e$ pre všetky prvky priestoru $(\mathscr{P}_2^{\mathrm{ac}}(\mathbb{R}^d), W_2)$.

Veta 4.8 (Subdiferenciál funkcionálu $\mathcal{F}_e$)**.** *Nech je $\nu \in \mathscr{P}_2^{\mathrm{ac}}(\mathbb{R}^d)$ také, že $\nu \neq 0$ a gradient $\nabla\nu$ je spojitý na $\mathbb{R}^d$. Potom*

$$\partial\mathcal{F}_e[\nu] = \Big\{\frac{\nabla\nu}{\nu}\Big\}.$$

Myšlienka dôkazu. Položme $\nu^\varepsilon = (\mathsf{Id}+\varepsilon\nabla\varphi)_\#\nu$ pre každé $\varepsilon \in \mathbb{R}$. Z vety o substitúcii cez jakobián (viď veta 3.3) získame

$$\nu = \nu^\varepsilon(\mathsf{Id}+\varepsilon\nabla\varphi)\det\nabla(\mathsf{Id}+\varepsilon\nabla\varphi) \quad \Rightarrow \quad \nu^\varepsilon(\mathsf{Id}+\varepsilon\nabla\varphi) = \frac{\nu}{\det(I_d+\varepsilon\nabla^2\varphi)},$$

kde I_d je jednotková matica a $\nabla^2\varphi$ značí Hessovu maticu funkcie φ. Pretože pre maticu $A \in \mathbb{R}^{d\times d}$ platí

$$\frac{\mathrm{d}}{\mathrm{d}\varepsilon}\det(I_d+\varepsilon A) = \mathrm{tr}\,A + o(\varepsilon),$$

dostaneme

$$\frac{\mathrm{d}}{\mathrm{d}\varepsilon}\det(I_d+\varepsilon\nabla^2\varphi) = \Delta\varphi + o(\varepsilon),$$

keďže $\operatorname{tr}\nabla^2\varphi = \Delta\varphi$. Pre prehľadnosť položíme $u(z) = z\ln z$ pre $z > 0$. Potom máme

$$\begin{aligned}\frac{\mathrm{d}}{\mathrm{d}\varepsilon}\mathcal{F}_e[\nu^\varepsilon] &= \frac{\mathrm{d}}{\mathrm{d}\varepsilon}\int_{\mathbb{R}^d} u(\nu^\varepsilon)\,\mathrm{d}y \\ &= \frac{\mathrm{d}}{\mathrm{d}\varepsilon}\int_{\mathbb{R}^d} u(\nu^\varepsilon(\mathsf{Id}+\varepsilon\varphi))\,\det(I_d+\varepsilon\nabla^2\varphi)\,\mathrm{d}x \\ &= \frac{\mathrm{d}}{\mathrm{d}\varepsilon}\int_{\mathbb{R}^d} u\Big(\frac{\nu}{\det(I_d+\varepsilon\nabla^2\varphi)}\Big)\,\det(I_d+\varepsilon\nabla^2\varphi)\,\mathrm{d}x \\ &= \int_{\mathbb{R}^d}\frac{\mathrm{d}}{\mathrm{d}\varepsilon}u\Big(\frac{\nu}{\det(I_d+\varepsilon\nabla^2\varphi)}\Big)\,\det(I_d+\varepsilon\nabla^2\varphi)\,\mathrm{d}x.\end{aligned}$$

Spočítame deriváciu vnútri integrálu nasledovne:

$$\begin{aligned}&\frac{\mathrm{d}}{\mathrm{d}\varepsilon}\,u\Big(\frac{\nu}{\det(I_d+\varepsilon\nabla^2\varphi)}\Big)\det(I_d+\varepsilon\nabla^2\varphi) \\ &\qquad= u'\Big(\frac{\nu}{\det(I_d+\varepsilon\nabla^2\varphi)}\Big)\frac{-\nu}{\det^2(I_d+\varepsilon\nabla^2\varphi)}\big(\Delta\varphi+o(\varepsilon)\big) \\ &\qquad\quad+u\Big(\frac{\nu}{\det(I_d+\varepsilon\nabla^2\varphi)}\Big)\big(\Delta\varphi+o(\varepsilon)\big).\end{aligned}$$

Dosadením $\varepsilon = 0$ získame

$$\frac{\mathrm{d}}{\mathrm{d}\varepsilon}\mathcal{F}_e[\nu^\varepsilon]\Big|_{\varepsilon=0} = \int_{\mathbb{R}^d}\Big(u'(\nu)(-\nu\Delta\varphi)+u(\nu)\,\Delta\varphi\Big)\,\mathrm{d}x$$

a použitím Greenovej vety dostaneme

$$\frac{\mathrm{d}}{\mathrm{d}\varepsilon}\mathcal{F}_e[\nu^\varepsilon]\Big|_{\varepsilon=0} = \int_{\mathbb{R}^d}\nabla\big(u'(\nu)\nu-u(\nu)\big)\cdot\nabla\varphi\,\mathrm{d}x. \tag{4.3}$$

Keďže

$$\nabla(\nu u'(\nu)-u(\nu)) = u'(\nu)\,\nabla\nu+\nu\,\nabla u'(\nu)-u'(\nu)\,\nabla\nu = \nu\,\nabla u'(\nu),$$

z (4.3) získame

$$\frac{\mathrm{d}}{\mathrm{d}\varepsilon}\mathcal{F}_e[\nu^\varepsilon]\Big|_{\varepsilon=0} = \int_{\mathbb{R}^d}\nabla u'(\nu)\cdot\nabla\varphi\,\nu\,\mathrm{d}x = \langle\nabla u'(\nu),\nabla\varphi\rangle_\nu\,.$$

S využitím tvrdenia 4.7 odtiaľ plynie $\nabla u'(\nu)\in\partial\mathcal{F}_e[\nu]$. Zrejme $u'(z) = \ln z + 1$ pre $z > 0$ a preto $\nabla u'(\nu) = \nabla\nu/\nu$, t.j. sme ukázali, že $\nabla\nu/\nu\in\partial\mathcal{F}_e[\nu]$. □

Dôsledok 4.9. *Nech je ϱ riešením problému* (1.1) *v slabom zmysle s počiatočnou podmienkou $\varrho_0\in\mathscr{P}_2^{\mathrm{ac}}(\mathbb{R}^d)$. Potom $\{\varrho(\cdot,t)\}_{t\in[0,T)}$ je gradientným tokom na $(\mathscr{P}_2^{\mathrm{ac}}(\mathbb{R}^d),W_2)$ po funkcionáli $\mathcal{F}_e$ daným vzťahom*

$$\mathcal{F}_e[\nu] = \int_{\mathbb{R}^d}\nu\ln\nu\,\mathrm{d}x \quad \textit{pre } \nu\in\mathscr{P}_2^{\mathrm{ac}}(\mathbb{R}^d).$$

Dôkaz. Z vety 4.8 plynie $\partial \mathcal{F}_e[\varrho(\cdot,t)] = \left\{ \frac{\nabla \varrho(\cdot,t)}{\varrho(\cdot,t)} \right\}$ pre skoro každé $t \in [0,T)$. Dosadením $\frac{\nabla \varrho(\cdot,t)}{\varrho(\cdot,t)}$ za v do vzťahu (4.2), ktorý charakterizuje riešenie rovnice kontinuity v zmysle distribúcií, po vykrátení $\varrho(\cdot,t)$ dostaneme slabú formuláciu riešenia rovnice vedenia tepla (1.2). □

Poznámka 4.10. Teória gradientných tokov na priestore $(\mathscr{P}_2^{\mathrm{ac}}(\mathbb{R}^d), W_2)$ je podrobne popísaná v knihe [1] a tiež [10]. Medzi klasické výsledky tejto teórie patrí, že riešenia parciálnej diferenciálnej rovnice

$$\frac{\partial \varrho}{\partial t} = \nabla \cdot (\varrho \nabla V) + \nabla \cdot (\varrho \nabla W * \varrho) + \Delta(\varrho^m); \quad m > \frac{1}{d} \tag{4.4}$$

generujú gradientné toky po funkcionáli popisujúceho voľnú energiu. Prvý sčítanec na pravej strane rovnice reprezentuje potenciálnu energiu (potenciál V reprezentuje napr. gravitačnú energiu), druhý sčítanec interakčnú energiu (sila, ktorou sa priťahujú častice hmoty medzi sebou) a posledný vnútornú energiu (difúziu a pre $m \neq 1$ tzv. nelineárnu difúziu). Podotknime, že kvôli konvolučnému členu a nelineárnej difúzii sa doteraz nepodarilo odvodiť rády konvergencie klasických numerických metód, napr. metódy konečných prvkov alebo konečných objemov pre túto rovnicu.

5. Diskretizácia gradientného toku

Teória popísaná v kapitolách 3 a 4 bola vytvorená na základe pozorovania nemeckého matematika Felixa Otta koncom 90. rokov minulého storočia. Pomocou časovej diskretizácie zistil, že riešenia rovnice vedenia tepla generujú gradientné toky na metrickom priestore pravdepodobnostných mier. Toto pozorovanie si popíšeme na diskretizácii gradientného toku na Euklidovom priestore $\mathbb{R}^d$ po hladkej konvexnej funkcii f a následne ho zovšeobecníme na priestor pravdepodobnostných mier. Uvažujme spätnú/implicitnú Eulerovu diskretizáciu systému obyčajných diferenciálnych rovníc v (1.3) s časovým krokom τ:

$$\begin{aligned} \frac{x_{k+1}-x_k}{\tau} = -\nabla f(x_{k+1}) \quad &\Rightarrow \quad \frac{x_{k+1}-x_k}{\tau} + \nabla f(x_{k+1}) = 0 \\ &\Rightarrow \quad \nabla \left(\frac{\|x-x_k\|^2}{2\tau} + f(x) \right) \Big|_{x=x_{k+1}} = 0. \end{aligned}$$

Uvedomme si, že f je konvexná funkcia a výraz $\frac{\|x-x_k\|^2}{2\tau}$ je rýdzo konvexný. Z toho plynie, že výraz $\frac{\|x-x_k\|^2}{2\tau} + f(x)$ je rýdzo konvexný a v bode, kde je jeho gradient nulový, má tento výraz jediné minimum. Teda spätnú Eulerovu diskretizáciu počiatočnej úlohy (1.3) vieme zapísať ako

$$x_{k+1} := \arg\min_{x \in \mathbb{R}^d} \left\{ \frac{\|x-x_k\|^2}{2\tau} + f(x) \right\} \quad k = 0, 1, 2, \ldots \tag{5.1}$$

Poznámka 5.1. Diskretizáciu vo vzťahu (5.1) môžeme písať v tvare $x_{k+1} := \mathrm{prox}_\tau^f(x_k)$, kde prox je tzv. proximálny operátor známy z teórie optimalizácie konvexných funkcií, viď [9].

Je známy výsledok numerických metód, že problém (5.1) konverguje v norme $\|\cdot\|$ k presnému riešeniu úlohy (1.3). Znovu si môžeme všimnúť, že na definovanie tohoto problému potrebujeme len metriku na priestore $\mathbb{R}^d$. Prirodzene tak môžeme navrhnúť časovú diskretizáciu problému gradientného toku na Hilbertovom priestore $L^2(\mathbb{R}^d)$ v definícii 2.2:

$$u_{k+1} := \arg\min_{u\in L^2(\mathbb{R}^d)} \left\{ \frac{\|u-u_k\|_{L^2}^2}{2\tau} + F[u] \right\} \quad k = 0, 1, 2, \dots \tag{5.2}$$

V knihe [4, Section 9.6, Theorem 2] je ukázané, že diskretizácia (5.2) konverguje v norme priestoru $L^2(\mathbb{R}^d)$ k presnému riešeniu.

Teraz prejdime k spomínanému spojeniu s priestorom $\mathscr{P}_2^{\mathrm{ac}}(\mathbb{R}^d)$ absolútne spojitých pravdepodobnostných mier určených hustotou ϱ. Jordan, Kindelehrer a Otto ukázali v článku [6], že časová diskretizácia (ktorej dnes hovoríme JKO schéma)

$$\varrho_{k+1} := \arg\min_{\varrho\in\mathscr{P}_2^{\mathrm{ac}}(\mathbb{R}^d)} \left\{ \frac{W_2^2(\varrho,\varrho_k)}{2\tau} + \int_{\mathbb{R}^d} \varrho\ln\varrho\,\mathrm{d}x \right\} \quad k = 0, 1, 2, \dots \tag{5.3}$$

konverguje k slabému riešeniu rovnice vedenia tepla $\frac{\partial\varrho}{\partial t} = \Delta\varrho$ vo Wassersteinovej metrike W_2. Hlavným argumentom pre význam tohoto tvrdenia je, že integrál $-\int \varrho\ln\varrho\,\mathrm{d}x$ je Boltzmannova entropia a príroda sa skutočne pri zanedbaní ostatných vplyvov podľa fyzikálnych zákonov snaží túto entropiu čo najrýchlejšie navýšiť, t.j. čo najstrmšie klesať po funkcionáli vo vzťahu (5.3).

Keďže JKO schéma (5.3) napodobňuje spätnú/implicitnú diskretizáciu gradientného toku na Euklidovom, resp. Hilbertovom priestore, intuitívne by sa dalo očakávať, že by mala predstavovať diskretizáciu gradientného toku na priestore pravdepodobnostných mier s Wassersteinovou metrikou. Toto pozorovanie viedlo k podrobnejšiemu štúdiu jednak Wassersteinovej metriky [10] a jednak gradientných tokov. Tu je významná kniha [1], kde sa v kapitolách 1–4 opisujú toky na všeobecných metrických priestoroch a v kapitolách 5–12 na konkrétnom priestore pravdepodobnostných mier s Wassersteinovou metrikou.

6. Stochastické diferenciálne rovnice

V kapitole 4 sme ukázali, že riešenia rovnice vedenia tepla v zmysle distribúcií generujú absolútne spojité krivky na priestore pravdepodobnostných mier. Ukážeme, že riešeniam stochastických diferenciálnych rovníc odpovedajú riešenia niektorých parabolických parciálnych diferenciálnych rovníc. Budeme pracovať s pojmom normálne rozdelenie, takže si tento pojem zavedieme. Pre jednoduchosť a názornosť budeme v celej tejto kapitole pracovať v jednorozmernom prípade, t.j. uvažujeme $d = 1$.

Definícia 6.1 (Normálne rozdelenie, Gaussovská miera)**.** Povieme, že náhodná veličina X určená hustotou $\varrho \in \mathscr{P}_2^{\mathrm{ac}}(\mathbb{R})$, t.j. $X \sim \varrho$, má normálne rozdelenie (ϱ je Gaussovská miera) ak

$$\varrho(x) = \frac{1}{\sqrt{2\pi\sigma^2}}\,\exp\Big(-\frac{(x-\mu)^2}{2\sigma^2}\Big) \quad \text{pre } x\in\mathbb{R},$$

kde $\mu \in \mathbb{R}$ a $\sigma > 0$. Píšeme

$$X \sim \mathsf{N}(\mu, \sigma^2) \qquad \text{alebo} \qquad \varrho = \mathsf{N}(\mu, \sigma^2).$$

Veta 6.2 (Momenty náhodnej veličiny)**.** *Ak je* $X \sim \mathsf{N}(\mu, \sigma^2)$*, potom*

$$\mathbb{E}[X] = \mu \qquad a \qquad \mathbb{E}[X^2] = \sigma^2 + \mu^2.$$

V tejto časti intuitívne popíšeme dôležité vlastnosti stochastických obyčajných diferenciálnych rovníc. Medzi klasické motivačné príklady patrí nasledujúca úloha (viď [7]). Ak v obyčajnej diferenciálnej rovnici

$$\frac{\mathrm{d}x}{\mathrm{d}t} = Ax$$

uvažujeme parameter A ako normálne rozdelenú náhodnú veličinu $A \sim \mathsf{N}(a, \sigma^2)$, dostaneme Itôovu stochastickú diferenciálnu rovnicu

$$\mathrm{d}X_t = a\, X_t\, \mathrm{d}t + \sigma\, X_t\, \mathrm{d}B_t\,,$$

kde B_t predstavuje Brownov pohyb (inak povedané Wienerov proces). Stochastická rovnica teda hovorí, že systém sa v každom bode správa približne podľa rovnice $\mathrm{d}X/\mathrm{d}t = a$ s odchýlkou popísanou šumom $\sigma\, \mathrm{d}B_t$. Poznamenajme, že tento zápis sa užíva preto, nakoľko Brownov pohyb nie je diferencovateľný (viď jeho definícia neskôr).

Príklad 6.3 (Stochastický gradientný tok)*.* Gradientný tok na Euklidovom priestore $\mathbb{R}$ generovaný počiatočnou úlohou (1.3) s $d = 1$, ktorý sa vychyľuje v každom bode o šum (t.j. sa pohybuje len približne v smere najväčšieho klesania funkcie) sa dá popísať stochastickou rovnicou

$$\mathrm{d}X_t = -\nabla f(X_t)\, \mathrm{d}t + \sqrt{2}\, \sigma\, \mathrm{d}B_t\,.$$

Ak je funkcia f rýdzo konvexná, potom existuje jediné $x_\star := \arg\min_{x \in \mathbb{R}}\{f(x)\}$, ktoré je zároveň stacionárnym riešením skalárnej obyčajnej diferenciálnej rovnice $\dot{x} = -\nabla f(x)$. V prípade stochastických diferenciálnych rovníc stacionárnym riešením nie je presne tento bod, ale rozdelenie pravdepodobnosti dané hustotou ϱ_∞ (tak, že $X_\infty \sim \varrho_\infty$), ktorej modus je práve hodnota $x_\star$. Je možné ukázať, že táto hustota má tvar

$$\varrho_\infty(x) = \frac{\exp(-\frac{1}{\sigma} f(x))}{\int_{\mathbb{R}} \exp(-\frac{1}{\sigma} f(x))\, \mathrm{d}x} \quad \text{pre } x \in \mathbb{R}.$$

Tu si môžeme všimnúť, že čím je hodnota σ väčšia, tým je rozptyl rozdelenia ϱ_∞ väčší. Toto je konzistentné s intuitívnym očakávaním, že čím zavádzame väčšiu neurčitosť do modelu, tým s väčšou nepresnosťou dosiahneme minimum funkcie f.

V prípade, že funkcia f je daná vzťahom $f(x) = \frac{x^2}{2}$ pre $x \in \mathbb{R}$, stacionárne rozdelenie ϱ_∞ je Gaussovská miera $\varrho_\infty = \mathsf{N}(0, 1)$.

Teraz definujeme Brownov pohyb, ktorý sa tiež nazýva Wienerov proces.

Definícia 6.4 (Brownov pohyb na $\mathbb{R}$)**.** Stochastický proces $\{B_t\}_{t \geq 0}$ sa nazýva Brownov pohyb (tiež Wienerov proces), ak spĺňa nasledujúce podmienky:

1. (počiatočná podmienka) $B_0 = 0$;

2. (nezávislosť prírastkov) Pre všetky hodnoty $0 < t_1 < \cdots < t_k$ sú náhodné premenné $B_{t_1}, B_{t_2} - B_{t_1}, \ldots, B_{t_k} - B_{t_{k-1}}$ vzájomne nezávislé;
3. (rozdelenie prírastkov) Pre všetky $0 \leq s < t < +\infty$ platí
$$B_t - B_s \sim \mathsf{N}(0, t-s)\,;$$
4. (spojitosť) Skoro iste je zobrazenie $t \mapsto B_t$ spojité.

Poznámka 6.5. Píšeme
$$\int_s^t \mathrm{d}B_t = B_t - B_s \sim \mathsf{N}(0, t-s).$$
Keďže
$$\int_0^t \mathrm{d}B_t = B_t \sim \mathsf{N}(0,t), \quad \text{platí} \quad \mathbb{E}[B_t] = 0\,,\ \mathbb{E}[B_t^2] = t.$$

Nasledujúca lemma je základným prvkom stochastického počtu. Na prvý pohľad je zvláštna, pretože podľa nej v prvom diferenciáli transformovanej náhodnej veličiny vystupuje nenulová druhá priestorová derivácia transformačnej funkcie. Toto vychádza z vlastnosti Brownovho pohybu, druhý moment $\mathbb{E}[B_t^2]$ je totiž rádu t. Jej dôkaz spočíva v použití Taylorovho rozvoja a následnom využití spomenutej vlastnosti $\mathrm{d}B_t^2 \approx \mathrm{d}t$.

Lemma 6.6 (Itôova, [7, Theorem 4.1.2])**.** *Nech $a \in \mathbb{R}$, $b \in \mathbb{R}_0^+$ a X_t je riešenie Itôovej stochastickej diferenciálnej rovnice*
$$\mathrm{d}X_t = a\,\mathrm{d}t + b\,\mathrm{d}B_t$$
s jednorozmerným Brownovym pohybom B_t. Nech ďalej $f\colon \mathbb{R} \times [0,+\infty) \to \mathbb{R}$ je dostatočne hladká funkcia. Potom
$$Y_t = f(X_t, t)$$
je riešením stochastickej diferenciálnej rovnice
$$\mathrm{d}Y_t = \Big(\frac{\partial f}{\partial t} + a\frac{\partial f}{\partial x} + \frac{b^2}{2}\frac{\partial^2 f}{\partial x^2}\Big)\mathrm{d}t + b\,\frac{\partial f}{\partial x}\,\mathrm{d}B_t\,.$$

Teraz si ukážeme prepojenie Brownovho pohybu (jednoduchej SDR) a rovnice vedenia tepla (opäť pre jednorozmerný prípad, všetky výsledky sa dajú samozrejme získať aj pre vyššie dimenzie).

Veta 6.7. *Nech je X_t riešenie stochastickej diferenciálnej rovnice*
$$\mathrm{d}X_t = \sqrt{2}\,\mathrm{d}B_t, \tag{6.1}$$
kde B_t je jednorozmerný Brownov pohyb. Potom funkcia $\varrho\colon \mathbb{R}\times[0,T) \to \mathbb{R}$ taká, že $X_t \sim \varrho(\cdot,t)$ pre skoro všetky $t \in [0,T)$, je riešením rovnice vedenia tepla v slabom zmysle.

Dôkaz. Položme $Y_t = \varphi(X_t, t)$, kde $\varphi \in C_c^\infty(\mathbb{R}\times[0,T))$. Spojito dodefinujeme $\varphi(\cdot,T) = 0$, aplikujme Itôovu lemmu (v ktorej $a = 0$, $b = \sqrt{2}$) a zistíme, že Y_t je riešením stochastickej diferenciálnej rovnice
$$\mathrm{d}Y_t = \Big(\frac{\partial \varphi}{\partial t} + \frac{\partial^2 \varphi}{\partial x^2}\Big)\,\mathrm{d}t + \sqrt{2}\,\frac{\partial \varphi}{\partial x}\,\mathrm{d}B_t\,.$$

Uvažujeme integrálnu formuláciu SDR (obe strany zintegrujeme na $[0,T]$):

$$\int_0^T \mathrm{d}Y_t = \int_0^T \Big(\frac{\partial\varphi}{\partial t} + \frac{\partial^2\varphi}{\partial x^2}\Big)\,\mathrm{d}t + \int_0^T \sqrt{2}\,\frac{\partial\varphi}{\partial x}\,\mathrm{d}B_t,$$

$$Y_T - Y_0 = \int_0^T \Big(\frac{\partial\varphi}{\partial t} + \frac{\partial^2\varphi}{\partial x^2}\Big)\,\mathrm{d}t + \int_0^T \sqrt{2}\,\frac{\partial\varphi}{\partial x}\,\mathrm{d}B_t,$$

$$\varphi(X_T,T) - \varphi(X_0,0) = \int_0^T \Big(\frac{\partial\varphi}{\partial t} + \frac{\partial^2\varphi}{\partial x^2}\Big)\,\mathrm{d}t + \int_0^T \sqrt{2}\,\frac{\partial\varphi}{\partial x}\,\mathrm{d}B_t.$$

Teraz spočítame na oboch stranách strednú hodnotu vzhľadom k X_t, vynásobíme teda jednotlivé členy ϱ a integrujeme cez $\mathbb{R}$. Vzhľadom k vlastnosti Brownovho pohybu bude stredná hodnota integrálu úplne vpravo nulová. Získame teda

$$-\int_{\mathbb{R}} \varphi(\cdot,0)\varrho(\cdot,0)\,\mathrm{d}x = \int_0^T\int_{\mathbb{R}} \frac{\partial\varphi}{\partial t}\,\varrho\,\mathrm{d}x\,\mathrm{d}t + \int_0^T\int_{\mathbb{R}} \frac{\partial^2\varphi}{\partial x^2}\,\varrho\,\mathrm{d}x\,\mathrm{d}t.$$

Odtiaľ integráciou per partes dostávame

$$-\int_{\mathbb{R}} \varphi(\cdot,0)\varrho(\cdot,0)\,\mathrm{d}x = \int_0^T\int_{\mathbb{R}} \frac{\partial\varphi}{\partial t}\,\varrho\,\mathrm{d}x\,\mathrm{d}t - \int_0^T\int_{\mathbb{R}} \frac{\partial\varphi}{\partial x}\,\frac{\partial\varrho}{\partial x}\,\mathrm{d}x\,\mathrm{d}t$$
$$\forall\varphi \in C_c^\infty(\mathbb{R}\times[0,T)),$$

pretože funkcia φ bola ľubovoľná. Ukázali sme teda, že funkcia ϱ je riešením rovnice vedenia tepla v slabom zmysle (1.2). □

Dôsledok 6.8. *Nech je ϱ riešením rovnice vedenia tepla v slabom zmysle s počiatočnou podmienkou $\varrho_0 \sim \mathsf{N}(0,a_0)$, kde $a_0 \in \mathbb{R}^+$. Potom pre skoro každé $t>0$ platí $\varphi(\cdot,t) \sim \mathsf{N}(0,a_0+2t)$.*

Dôkaz. Prevedieme (6.1) do integrálnej formulácie a využijeme vlastnosti Brownovho pohybu (viď definícia 6.4) a druhého momentu (resp. rozptylu) náhodnej veličiny. □

Poznámka 6.9. Parciálne diferenciálne rovnice tvaru (4.4) majú svoju stochastickú interpretáciu v tvare tzv. McKean-Vlasovej SDR

$$\mathrm{d}X_t = -\big(\nabla V(X_t) + \nabla W(X_t) * \varrho(\cdot,t)\big)\,\mathrm{d}t + \sqrt{2\varrho^{m-1}}\,\mathrm{d}B_t\,; \quad X_t \sim \varrho(\cdot,t).$$

7. Záver

V tomto článku sme pracovali s rôznymi interpretáciami rovnice vedenia tepla.

Najskôr sme definovali pojem gradientného toku na Hilbertovom priestore lebesgueovsky integrovateľných funkcií a ukázali sme, že riešenia rovnice vedenia tepla generujú gradientné toky po Dirichletovej energii.

Intuícia nemeckého matematika Felixa Otta viedla k tomu, že priestor pravdepodobnostných mier by mohol byť vhodným na popis riešenia rovnice vedenia tepla. Pozoroval, že riešenie tejto rovnice konverguje k minimalizácií funkcionálu

záporne vzatej Boltzmannovej entropie, ktorý má fyzikálny význam pre túto rovnicu (teplo sa skutočne šíri tak, aby maximalizovalo Boltzmannovu entropiu). Toto viedlo na štúdium metrického priestoru mier, ktorého základné vlastnosti sme si popísali. Ďalej sme ukázali, že riešenia rovnice vedenia tepla generujú gradientné toky po funkcionáli zápornej Boltzmannovej entropie.

Pozorovanie, že riešenie parciálnej diferenciálnej rovnice môžeme rozumieť ako krivku na priestore náhodných veličín nás posunulo k úvahe, že by táto krivka mohla byť zároveň riešením stochastického procesu (stochastickej diferenciálnej rovnice). Ukázali sme, že riešenie Brownovho pohybu (Wienerovho procesu), konkrétne jeho hustota, je slabým riešením rovnice vedenia tepla.

Poďakovanie

Autor ďakuje kolegom za cenné pripomienky a návrhy na výrazné vylepšenie textu.

Literatúra

[1] L. Ambrosio, N. Gigli, G. Savaré: *Gradient flows: in metric spaces and in the space of probability measures*, Lectures in mathematics ETH Zürich, Basel: Birkhäuser, 2008.
[2] L. Ambrosio, N. Gigli: *User's guide to optimal transport*, Modelling and Optimisation of Flows on Networks, Lecture Notes in Mathematics, Berlin, Springer, 2013, 1–155.
[3] L. Evans: *Measure Theory and Fine Properties of Functions*, Revised Edition, Boca Raton: CRC Press, Taylor & Francis Group, 2015.
[4] L. Evans: *Partial differential equations*, Graduate studies in mathematics, Providence, Rhode Island: American Mathematical Society, 2022.
[5] A. Figalli, F. Glaudo: *An Invitation to Optimal Transport, Wasserstein Distances, and Gradient Flows*, Berlin: European Mathematical Society, 2021.
[6] R. Jordan, D. Kinderlehrer, F. Otto: *The Variational Formulation of the Fokker–Planck Equation*, SIAM Journal on Mathematical Analysis, 1998, roč. 29, č. 1, 1–17.
[7] B. Øksendal: *Stochastic differential equations: an introduction with applications*, Heidelberg: Springer, 2013.
[8] F. Otto: *The Geometry of dissipative evolution equations: The porous medium equation*, Communications in Partial Differential Equations, 2001, roč. 26, č. 1–2, 101–174.
[9] N. Parikh: *Proximal Algorithms*, Foundations and Trends in Optimization, 2014, roč. 1, č. 3, s. 127–239.
[10] C. Villani: *Optimal transport: old and new*, Grundlehren der mathematischen Wissenschaften, A series of comprehensive studies in Mathematics, Berlin: Springer, 2009.

Matej Benko, Ústav matematiky, Fakulta strojního inženýrství, Vysoké učení technické v Brně, Technická 2, 616 69 Brno, Česká republika,
e-mail: Matej.Benko@vutbr.cz

APLIKACE CELOČÍSELNÝCH BODŮ ELIPTICKÝCH KŘIVEK V TEORII KUBICKÝCH A KVARTICKÝCH POLYNOMŮ

JIŘÍ KLAŠKA

Věnováno profesoru Michalu Křížkovi

Abstrakt. V 16. století došlo k průlomovým objevům, které umožnily nalézt řešení kubických a kvartických rovnic. I když od vydání slavné Cardanovy knihy Ars Magna uplynulo téměř 500 let, některé otázky související s kubickými a kvartickými polynomy jsou stále aktuální. V následující přehledové studii seznámíme čtenáře s několika zajímavými výsledky, které byly dosaženy v teorii kubických a kvartických polynomů s daným diskriminantem.

1. Úvod

Ve 14. a 15. století vynaložili někteří matematici velké úsilí, aby nalezli obecný postup pro řešení kubické rovnice. K těmto matematikům patřili Maestro Biaggio, Antonio de' Mazzinghi, Maestro Benedetto da Firenze, Maestro Dardi a Piero della Francesca. V roce 1494 vydal italský františkánský mnich Luca Pacioli (1445–1517) knihu *Summa de arithmetica, goeometria, proportioni at proportionalita*[1] (Souhrn vědomostí o aritmetice, geometrii, poměrech a úměrnosti), ve které sděluje, že řešení kubické rovnice nebylo doposud objeveno. Toto sdělení se stalo intelektuální výzvou pro nejlepší matematiky 16. století. Vydáním Pacioliho knihy začal zajímavý a spletitý příběh, ve kterém se v průběhu následujících století objevovala jména nejvýznamnějších matematických osobností. Jejich lidské osudy jsou často stejně zajímavé jako jejich objevy. V období let 1515–1540 došlo k významnému pokroku a metoda řešení kubických rovnic byla nalezena. Na vyřešení problému se podíleli

Scipione del Ferro	(1465–1526),
Niccolò Fontana Tartaglia	(1499–1557),
Gerolamo Cardano	(1501–1576),
Lodovicco Ferrari	(1522–1565).

Příběh Ferro – Tartaglia – Cardano – Ferrari je jedním z nejkontroverznějších příběhů dějin matematiky. Sled neobyčejných a dramatických událostí týkajících

2020 *MSC.* Primární 11D25; Sekundární 11D45.

Klíčová slova. Kubický polynom, kvartický polynom, diskriminant, eliptická křivka, Mordellova rovnice.

[1]Pro zajímavost uveďme, že jeden výtisk Pacioliho knihy vlastní Moravská zemská knihovna v Brně.

se objevu řešení kubické rovnice je poutavě popsán ve třetí kapitole knihy *The Equation That Couldn't Be Solved – How Mathematical Genius Discovered the Language of Symmetry*, jejímž autorem je Mario Livio. Kniha byla publikována v roce 2005 a český překlad této knihy vyšel v roce 2008 pod názvem *Neřešitelná rovnice*.

V roce 1545 Cardano publikoval knihu *Artis magnae sive de reguli algebraicis liber unus* (Velké umění neboli první kniha pravidel algebry), ve které byl poprvé uveden postup pro řešení kubické rovnice. Tato kniha, dnes známá jako *Ars Magna*, je považována za počátek moderní algebry. Cardanova kniha obsahuje rovněž řešení kvartické rovnice, které objevil v roce 1540 Lodovicco Ferrari. Podrobnou historii kubických a kvartických rovnic může čtenář nalézt také v knize *Rasskazy o fizikach i matematikach*, kterou napsal Semjon Grigorjevič Gindikin v roce 1981. V angličtině tato kniha vyšla v roce 1988 pod názvem *Tales of Physicists and Mathematicians*.

Dnes, téměř 500 let od vydání *Ars Magna*, je velmi obtížné si představit jak lidé v Cardanově době žili a přemýšleli. Díky Cardanovu životopisu *De Vita Propria Liber*, který Cardano napsal v průběhu posledního roku svého života, můžeme získat zajímavý pohled na dobu, kdy *Ars Magna* vznikla. Životopisné pojednání *De Vita Propria Liber* bylo poprvé publikováno v Paříži roku 1653. V roce 1914 byl Cardanův životopis přeložen do němčiny pod názvem *Des Girolamo Cardano von Mailand eigene Lebensbeschreibung* a v roce 1929 také do angličtiny pod názvem *The Book of My Life*. Český překlad z němčiny byl publikován v roce 2021 pod názvem *Můj život*.

Z historického hlediska je zajímavé připomenout, že téměř žádný z dnes běžně používaných matematických symbolů v Cardanově době ještě neexistoval. Pro lepší představu uveďme přehled autorů různých symbolů, používaných dnes v algebře, spolu s letopočtem prvního použití symbolu v tisku.

$+, -$	Widmann	(1489)
$(\ ,\ )$	Tartaglia	(1556)
$\cdot$	Clavius	(1593)
$\times$	Oughtread	(1631)
$:$	Johnson	(1633)
$\surd$	Rudolff	(1525)
$=$	Recorde	(1557)
$<, >$	Harriot	(1631)
$\leq\ ,\ \geq$	Bougere	(1734)
$i = \sqrt{-1}$	Euler	(1794)

Po nalezení postupu pro řešení kubických a kvartických rovnic bylo zřejmé, že další problém, který na matematiky čeká, je řešení kvintických rovnic. Příběh hledání vzorce pro řešení kvintické rovnice trval od smrti Cardana přibližně dalších 250 let. Tento problém byl však nesrovnatelně obtížnější. Na problému řešení kvintických rovnic pracovala v průběhu následujících století celá řada významných matematiků. Uveďme alespoň některé:

Rafael Bombelli	(1526–1572),
François Viète	(1540–1603),
Thomas Harriot	(1560–1621),
James Gregory	(1638–1675),
Ehrenfried Walther von Tschirnhaus	(1651–1708),
Étienne Bézout	(1730–1783),
Leonhard Paul Euler	(1777–1783),
Erland Samuel Bring	(1736–1798),
George Birch Jerrard	(1804–1863),
Alexandre–Théophile Vandermonde	(1735–1796),
Edward Waring	(1736–1798),
Joseph–Louis Lagrange	(1736–1813),
Johann Carl Friedrich Gauss	(1777–1855),
Paolo Ruffini	(1765–1822),
Niels Henrik Abel	(1802–1829),
Évariste Galois	(1811–1829).

Teprve objevy Abela a Galoise[2] uzavřely období velkého a marného úsilí nalézt řešení kvintické rovnice. Jejich objevy přinesly překvapující a znepokojivou odpověď. Žádný vzorec pro řešení kvintické rovnice, který by využíval pouze čtyři základní aritmetické operace a operaci odmocňování, nemůže existovat.

Důkaz, že kvintické rovnice není možné vyřešit podobným způsobem jako rovnice kubické a kvartické, ale neznamená, že by kvintické rovnice nemohly být řešeny pomocí jiných, složitějších metod, například pomocí eliptických funkcí. Touto problematikou se v následujícím období zabývali

Charles Hermite	(1922–1901),
Leopold Kronecker	(1823–1891),
Felix Christian Klein	(1849–1925).

Vývoj teorie rovnic od této chvíle pokračoval různými směry, v nichž hrála stále důležitější úlohu teorie grup. Vraťme se ale k problematice kubických rovnic. V roce 1940 Boris Nikolajevič Delone[3] (1890–1980) a Dmitrij Konstantinovič Faddějev (1907–1989) předložili následující problém:

Problém 1.1 (1940)**.** Nechť $D \in \mathbb{Z}$. Nalezněte metodu, která umožní určit všechny normované kubické polynomy s celočíselnými koeficienty mající diskriminant D.

Problém 1.1 byl poprvé publikován ve známé monografii [3, str. 313], která byla v roce 1964 přeložena do angličtiny. Pro zajímavost uveďme, že na anglickém překladu [4] se podstatně podílela Emma Lehmer (1906–2007). V [4] může čtenář nalézt Problém 1.1 na straně 412. Dále je vhodné poznamenat, že autorem Problému 1.1 je zřejmě pouze Boris Nikolajevič Delone, který se nalezením metody zabýval již před rokem 1928. Některé dílčí Deloneho výsledky, týkající se Problému 1.1,

[2]Tragické životní příběhy Abela a Galoise jsou podrobně popsány v kapitolách 4 a 5 v knize *Neřešitelná rovnice*.

[3]Delone publikoval některé články pod jménem Delaunay.

byly publikovány v článku [2]. V [2, str. 25] Delone nalezl všechny normované ireducibilní kubické polynomy s celočíselnými koeficienty pro 16 konkrétních hodnot diskriminantu D a sestavil jejich tabulku. Tato tabulka byla rovněž publikována v [3, str. 318] a [4, str. 418]. Metoda, kterou Delone k sestavení tabulky použil, byla založena na dvou podstatných předpokladech:

(i) Diskriminant D je záporný.
(ii) Polynomy jsou ireducibilní nad tělesem racionálních čísel $\mathbb{Q}$.

Deloneho postup tedy není možné aplikovat na případ diskriminantů $D \in \mathbb{Z}$, kde $D \geq 0$. Navíc, Deloneho postup neumožňuje určit kubické polynomy, které jsou reducibilní nad $\mathbb{Q}$. Obecná metoda, která je řešením Problému 1.1, byla poprvé publikována v roce 2021 v článku [20]. Tato metoda úzce souvisí s řešením diofantické rovnice

$$Y^2 = X^3 + k, \tag{1.1}$$

kde k je libovolné celé nenulové číslo. Rovnice (1) má velmi dlouhou a zajímavou historii, která sahá až do 17. století k práci francouzského matematika Gasparda Bacheta (1581–1638). Diofantická rovnice (1.1) se často nazývá Mordellova rovnice[4] na počest Louise Joela Mordella (1888–1972), který významně přispěl k objasnění některých vlastností této rovnice. Eliptická křivka odpovídající Mordellově rovnici se pak nazývá Mordellova křivka.

První objevy týkající se Mordellovy rovnice je možno nalézt v knize *History of the Theory of Numbers – Diophantine Analysis* [5, str. 533–539], jejímž autorem je americký matematik Leonard Eugene Dickson (1874–1954). Literatura týkající se Mordellovy rovnice je poměrně rozsáhlá. Čtenáři lze doporučit například publikace [1, 6, 11, 12, 19, 25, 26, 27, 28].

Důležitým výsledkem Louise Mordella je tvrzení, že každá rovnice (1.1) má nejvýše konečně mnoho celočíselných řešení. Je zřejmé, že je-li $[X_0, Y_0]$ je řešení rovnice (1.1), pak rovněž $[X_0, -Y_0]$ je řešení (1.1). Pro $Y_0 \neq 0$, budeme řešení $[X_0, Y_0]$ a $[X_0, -Y_0]$ považovat za různá. Konečně je vhodné připomenout, že v současné době existuje rozsáhlá literatura týkající se problematiky polynomů majících daný diskriminant. Významné výsledky v tomuto oboru dosáhli zejména maďarský matematik Kálmán Győry (*1940) a holandský matematik Jan–Hendrik Evertse (*1958). Z prací těchto autorů připomeňme alespoň publikace [7, 8, 9, 10, 13, 14, 15, 16, 17, 18].

V následující kapitole uvedeme hlavní výsledky dosažené v článku [20], které poskytují řešení Problému 1.1.

2. Řešení Deloneho problému kubických polynomů

Nechť $D \in \mathbb{Z}$ a nechť

$$C(D) = \{f(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x] : D(f) = D\},$$

kde $D(f) = a^2b^2 + 18abc - 4a^3c - 4b^3 - 27c^2$ je diskriminant $f(x)$. Je zřejmé, že problém určit množinu $C(D)$, pro dané $D \in \mathbb{Z}$, je ekvivalentní problému nalézt

[4]Rovnice (1.1) se někdy nazývá Bachetova rovnice.

všechna celočíselná řešení diofantické rovnice

$$a^2b^2 + 18abc - 4a^3c - 4b^3 - 27c^2 = D.$$

Řešení Deloneho problému můžeme rozdělit do několika částí.

2.1. Ekvivalence na množině $C(D)$

Nechť $f(x) = x^3 + ax^2 + bx + c \in C(D)$. Pro každé $w \in \mathbb{Z}$ definujme polynom $f_w(x) = f(x+w)$. Přímým výpočtem můžeme ověřit, že pro libovolné $w \in \mathbb{Z}$ platí

$$D(f_w) = D(f). \tag{2.1}$$

Z rovnosti (2.1) snadno plyne následující lemma.

Lemma 2.1. *Nechť $D \in \mathbb{Z}$. Je-li $C(D) \neq \emptyset$, pak množina $C(D)$ je nekonečná.*

Dále je možné dokázat, že pro polynomy $f_w(x)$ platí hezká a užitečná identita

$$f_w(x) = x^3 + \frac{f''(w)}{2!}x^2 + \frac{f'(w)}{1!}x + f(w), \tag{2.2}$$

ve které výrazy $f'(w)$ a $f''(w)$ označují první a druhou derivaci $f(x)$ v bodě w.

Nechť $C(D) \neq \emptyset$. Pro $f(x), g(x) \in C(D)$ položme

$$f(x) \sim g(x) \Longleftrightarrow \exists\, w \in \mathbb{Z} : g(x) = f(x+w) = f_w(x).$$

Lemma 2.2. *Relace $\sim$ je ekvivalence na množině $C(D)$.*

Nechť $f(x) = x^3 + ax^2 + bx + c \in C(D)$. Pak existují jednoznačně určená čísla $w \in \mathbb{Z}$ a $e \in \{0, 1, 2\}$ tak, že $a = 3w + e$. Položme

$$r(x) = f(x-w) = x^3 + ex^2 + (b - 3w^2 - 2ew)x + 2w^3 + ew^2 - bw + c. \tag{2.3}$$

Polynom $r(x)$ budeme nazývat kanonický reprezentant třídy

$$[f(x)] = \{g(x) \in C(D) : g(x) \sim f(x)\} \in C(D)/\sim .$$

Bude užitečné zavést následující konvenci.

Konvence 2.3. Pro zápis polynomu $f(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]$ budeme rovněž požívat stručnější vyjádření ve tvaru uspořádané trojice koeficientů $[a, b, c]$.

Příklad 2.4. Nechť $f(x) = x^3 - 3x^2 - x + 6$. Protože $D(f) = 13$ je $C(13) \neq \emptyset$. Podle Lemma 2.1 je množina $C(13)$ nekonečná a z rovnosti (2.2) plyne, že polynomu $f(x)$ odpovídá třída rozkladu

$$[f(x)] = \{x^3 + (3w-3)x^2 + (3w^2 - 6w - 1)x + w^3 - 3w^2 - w + 6 : w \in \mathbb{Z}\}.$$

Aplikací vztahu (2.3) obdržíme, že kanonický reprezentant třídy $[f(x)]$ je polynom $r(x) = x^3 - 4x + 3$ a podle Konvence 2.3 můžeme $r(x)$ zapsat ve tvaru $[0, -4, 3]$.

Použití Konvence 2.3 může být také užitečné pro kratší formulace některých tvrzení.

Lemma 2.5. *Nechť $[a, b, c], [a', b', c'] \in C(D)$. Jestliže $[a, b, c] \sim [a', b', c']$, pak*

$$a \equiv a' \pmod 3.$$

Pomocí protipříkladu není obtížné dokázat, že opačná implikace neplatí. Zřejmě

$$[1,0,-1],[1,2,1] \in C(-23) \text{ a } [1,0,-1] \not\sim [1,2,1].$$

Následující Věta 2.6 má pro řešení Deloneho problému zásadní význam.

Věta 2.6. *Nechť $0 \neq D \in \mathbb{Z}$ a nechť $C(D) \neq \emptyset$. Pak $C(D)/\sim$ má konečně mnoho tříd.*

Věta 2.6 je důsledkem obecnějšího tvrzení, které dokázal v roce 1973 Kálmán Győry v článku [13, str. 419]. Viz také [8, str. 109] a [18, str. 475]. Alternativní důkaz Věty 2.6 může čtenář nalézt v článku [20, str. 107–108]. Tento důkaz je založen na následujícím významném výsledku Louise Mordella [27].

Věta 2.7 (L. J. Mordell, 1920)**.** *Nechť $0 \neq k \in \mathbb{Z}$. Pak Mordellova rovnice*

$$Y^2 = X^3 + k \tag{2.4}$$

má nejvýše konečně mnoho celočíselných řešení.

Pro nalezení všech celočíselných řešení rovnice (2.4) je možné použít metodu s níž se čtenář může podrobně seznámit v knize [30]. V současnosti je tato metoda implementována například v programech Magma a Sage.

Pro formulaci dalších výsledků budeme potřebovat několik označení. Předně, je-li A konečná množina, pak symbolem $\#A$ budeme označovat počet prvků množiny A. Dále, pro libovolné $0 \neq D \in \mathbb{Z}$, položme

$$c(D) = \begin{cases} \#C(D)/\sim, & \text{je-li } C(D) \neq \emptyset, \\ 0, & \text{je-li } C(D) = \emptyset. \end{cases}$$

Konečně, symbolem $R_C(D)$ označme množinu všech kanonických reprezentantů tříd rozkladu množiny $C(D)/\sim$. Množina $R_C(D)$ se nazývá úplný systém kanonických reprezentantů množiny $C(D)/\sim$. Je zřejmé, že platí

$$\#R_C(D) = \#C(D)/\sim = \ c(D).$$

Některé základní vlastnosti množiny $R_C(D)$ popisuje následující věta.

Věta 2.8. *Nechť $0 \neq D \in \mathbb{Z}$. Pak platí:*

(i) $[0,u,v] \in R_C(D)$ *právě tehdy, když* $[0,u,-v] \in R_C(D)$.
(ii) $[1,u,v] \in R_C(D)$ *právě tehdy, když* $[2,u+1,u-v] \in R_C(D)$.

Jestliže $v \neq 0$, pak v části (i) Věty 2.8 platí $[0,u,v] \not\sim [0,u,-v]$. Podobně v části (ii) platí $[1,u,v] \not\sim [2,u+1,u-v]$ pro libovolné u,v. Dále je možné dokázat, že část (ii) Věty 2.8 může být formulována v následujícím ekvivalentním tvaru

$$[2,r,s] \in R_C(D) \text{ právě tehdy, když } [1,r-1,r-s-1] \in R_C(D).$$

Je zřejmé, že vztahy (i) a (ii) uvedené ve Větě 2.8 mají praktický význam. Například, pokud víme, že $[1,-3077,64681] \in R_C(-76)$, pak také $[2,-3076,-67758] \in R_C(-76)$.

2.2. Případ množin $C(0)$ a $R_C(0)$

Množiny $C(0)$ a $R_C(0)$ tvoří výjimku celé teorie, kterou je nutné vyřešit samostatně. Úplný popis množin $C(0)$ a $R_C(0)$ uvedeme ve Větě 2.9.

Věta 2.9. *Nechť $f(x) = x^3+ax^2+bx+c \in \mathbb{Z}[x]$. Pak $f(x) \in C(0)$ právě tehdy, když existují $e \in \{0,1,2\}$, $v, w \in \mathbb{Z}$ tak, že*

$$\begin{aligned} f(x) &= x^3 + (3w+e)x^2 + (3w^2+2ew-3v^2-2ev)x + w^3 + ew^2 \\ &\quad - (3v^2+2ev)w + 2v^3 + ev^2 \\ &= (x+w-v)^2(x+w+2v+e). \end{aligned}$$

Rozklad $C(0)/\sim$ má nekonečně mnoho tříd a množina všech kanonických reprezentantů $R_C(0)$ může být zapsána ve tvaru

$$R_C(0) = \{[e, -3v^2-2ev, 2v^3+ev^2] : e \in \{0,1,2\}, v \in \mathbb{Z}\}.$$

Důkaz Věty 2.9 lze nalézt v [20, str. 110].

2.3. Mordellova rovnice $Y^2 = X^3 - 432D$

Základní souvislost mezi množinou $C(D)$ a Mordellovou rovnicí $Y^2 = X^3 - 432D$ poskytuje Věta 2.10.

Věta 2.10. *Nechť $0 \neq D \in \mathbb{Z}$. Jestliže Mordellova rovnice*

$$Y^2 = X^3 + k, \quad \text{kde} \quad k = -432D = -2^4 3^3 D$$

nemá celočíselné řešení, pak $C(D) = \emptyset$.

Důkaz této věty lze nalézt v [20, str. 106].

Příklad 2.11. (i) Nechť $D \in \{-1,-2,-5,-6,-9,-10\}$. Pak žádná z Mordellových rovnic $Y^2 = X^3 - 432D$ nemá celočíselné řešení. Podle Věty 2.10 pak platí

$$C(-1) = C(-2) = C(-5) = C(-6) = C(-9) = C(-10) = \emptyset.$$

(ii) Nechť $D \in \{2,6,7,9,10\}$. Pak žádná z Mordellových rovnic $Y^2 = X^3 - 432D$ nemá celočíselné řešení. Podle Věty 2.10 pak platí

$$C(2) = C(6) = C(7) = C(9) = C(10) = C(11) = \emptyset.$$

Kombinací Lemma 2.1 a Příkladu 2.11 obdržíme Větu 2.12.

Věta 2.12. *Pro každé $D \in \mathbb{Z}$ nastane právě jedna z možností: množina $C(D)$ je buď prázdná, nebo nekonečná.*

Pro každé $0 \neq D \in \mathbb{Z}$ položme

$$M_C(D) = \{[X_0, Y_0] : X_0, Y_0 \in \mathbb{Z}, Y_0^2 = X_0^3 - 432D\} \text{ a } m_C(D) = \#M_C(D).$$

Zaměřme nyní krátce pozornost na aritmetické vlastnosti celočíselných řešení rovnice $Y^2 = X^3 - 432D$, kde $D \neq 0$. Speciální tvar koeficientu $-432D$ způsobuje, že rovněž celočíselná řešení této rovnice mají některé speciální vlastnosti. Například pro každé $[X_0, Y_0] \in M_C(D)$ platí $X_0 \equiv 0 \pmod 2$ právě tehdy, když $Y_0 \equiv 0 \pmod 2$. Můžeme tedy zavést následující definici.

(i) Řešení $[X_0, Y_0] \in M_C(D)$ budeme nazývat liché, když X_0 a Y_0 jsou lichá.
(ii) Řešení $[X_0, Y_0] \in M_C(D)$ budeme nazývat sudé, když X_0 a Y_0 jsou sudá

Zkoumání celkového počtu lichých a sudých řešení rovnice $Y^2 = X^3 - 432D$ odhalilo následující skutečnost. Nechť

$$G = \{D \in \mathbb{Z} : 0 \neq |D| \leq 1000\} \quad \text{a} \quad H = \bigcup_{D \in G} M_C(D).$$

Pak v množině H existuje přibližně 33% lichých řešení a 67% sudých řešení. Tento objev vede k zajímavé hypotéze, totiž že asymptotický poměr počtu lichých a sudých řešení Mordellovy rovnice $Y^2 = X^3 - 432D$ je roven 1/2. Podrobnější informace může čtenář nalézt v [20, str. 112].

Při konstrukci množiny $C(D)$ hraje důležitou roli také Lemma 2.13.

Lemma 2.13. *Nechť $X_0, Y_0 \in \mathbb{Z}$. Pak existuje nejvýše jedno číslo $e \in \{0, 1, 2\}$ splňující soustavu kongruencí*

$$4e^2 - X_0 \equiv 0 \pmod{12}, \quad 4e^3 - 3eX_0 + Y_0 \equiv 0 \pmod{108}. \tag{2.5}$$

Pro formulaci Věty 2.14 bude vhodné zavést následující označení. Nechť

$$E_C(D) = \big\{[[X_0, Y_0], e] \in M_C(D) \times \{0, 1, 2\} : 4e^2 - X_0 \equiv 0 \pmod{12},\\ 4e^3 - 3eX_0 + Y_0 \equiv 0 \pmod{108}\big\}.$$

Věta 2.14. *Nechť $0 \neq D \in \mathbb{Z}$ a nechť $f(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]$. Pak $f(x) \in C(D)$ právě tehdy, když existují $w \in \mathbb{Z}$ a $[[X_0, Y_0], e] \in E_C(D)$ tak, že*

$$a = 3w + e,$$

$$b = 3w^2 + 2ew + \frac{4e^2 - X_0}{12},$$

$$c = w^3 + ew^2 + \frac{4e^2 - X_0}{12}w + \frac{4e^3 - 3eX_0 + Y_0}{108}.$$

Navíc, pokud $f(x) \in C(D)$, pak

$$r(x) = f(x - w) = x^3 + ex^2 + \frac{4e^2 - X_0}{12}x + \frac{4e^3 - 3eX_0 + Y_0}{108}$$

je kanonický reprezentant třídy $[f(x)]$.

Z Věty 2.14 ihned plyne, že lichá řešení $[X_0, Y_0] \in M_C(D)$ nemohou splňovat podmínku $[[X_0, Y_0], e] \in E_C(D)$ pro žádné $e \in \{0, 1, 2\}$. V následujícím příkladu ukážeme, že i když množina $M_C(D)$ obsahuje sudá řešení, množina $C(D)$ může být prázdná.

Příklad 2.15. Uvažujme Mordellovu rovnici $Y^2 = X^3 - 432D$, kde $D = 33$. Pak $M_C(33) = \big\{[25, \pm 37], [36, \pm 180], [108, \pm 1116], [180, \pm 2412], [2113, \pm 97129]\big\}$ a $m_C(33) = 10$. Aplikací Věty 2.14 obdržíme, že $C(33) = \emptyset$ a $c(33) = 0$.

2.4. Metoda konstrukce množiny $C(D)$

Na základě předchozích výsledků můžeme vytvořit postup, pomocí kterého je možné určit množinu $C(D)$ pro libovolné $0 \neq D \in \mathbb{Z}$. Postup lze formálně rozdělit do čtyř následujících kroků:

1) Nechť $0 \neq D \in \mathbb{Z}$. Nejprve nalezneme množinu $M_C(D)$ všech celočíselných řešení $[X_0, Y_0]$ Mordellovy rovnice $Y^2 = X^3 - 432D$. Podle Věty 2.7 je množina $M_C(D)$ konečná. Je-li $M_C(D) = \emptyset$, pak výpočet končí. Z Věty 2.14 totiž plyne, že $C(D) = \emptyset$.
2) Předpokládejme, že $M_C(D) \neq \emptyset$. Ve druhém kroku určíme množinu $E_C(D)$. Pro každé $[X_0, Y_0] \in M_C(D)$ rozhodneme, zda existuje číslo $e \in \{0, 1, 2\}$, splňující soustavu kongruencí (2.5). Podle Lemma 2.13 vyhovuje této soustavě nejvýše jedno číslo $e \in \{0, 1, 2\}$. Protože $\#E_C(D) = \#C(D)/\!\sim$, platí, že $C(D) = \emptyset$ právě tehdy, když $E_C(D) = \emptyset$.
3) Předpokládejme, že $E_C(D) \neq \emptyset$. Ve třetím kroku určíme množinu $R_C(D)$, tj. úplný systém kanonických reprezentantů množiny $C(D)/\!\sim$. Vzhledem k Větě 2.14 platí

$$R_C(D) = \left\{ \left[e, \frac{4e^2 - X_0}{12}, \frac{4e^3 - 3eX_0 + Y_0}{108} \right] : [[X_0, Y_0], e] \in E_C(D) \right\}. \tag{2.6}$$

4) Ve čtvrtém, závěrečném kroku nalezneme množinu $C(D)$. Aplikací vzorce (2.2) pro všechna $r(x) \in R_C(D)$ obdržíme

$$C(D) = \bigcup_{r(x) \in R_C(D)} \left\{ x^3 + \frac{r''(w)}{2!}x^2 + \frac{r'(w)}{1!}x + r(w) : w \in \mathbb{Z} \right\}. \tag{2.7}$$

Výše uvedený postup budeme demonstrovat na Příkladu 2.16.

Příklad 2.16. Nechť $D = 29$. Nalezněte množinu $C(29)$.
Nejprve určíme množinu $M_C(29)$. Rovnice $Y^2 = X^3 - 12528$ má 10 řešení a

$$M_C(29) = \big\{[24, \pm 36], [33, \pm 153], [112, \pm 1180], [384, \pm 7524], [528, \pm 12132]\big\}.$$

Dále, pro každé $[X_0, Y_0] \in M_C(29)$ nalezneme řešení soustavy kongruencí (2.5) a určíme množinu $E_C(29)$.

$$E_C(29) = \big\{[[112, -1180], 1], [[112, 1180], 2]\big\}.$$

Aplikací vztahu (2.6) obdržíme množinu $R_C(29)$, tj. úplný systém kanonických reprezentantů množiny $C(29)/\!\sim$.

$$R_C(29) = \{x^3 + x^2 - 9x - 14,\ x^3 + 2x^2 - 8x + 5\}.$$

Odtud plyne, že $c(29) = \#C(29)/\!\sim\ = \#R_C(29) = 2$. Podle Konvence 2.3 můžeme množinu $R_C(29)$ zapsat stručně ve tvaru $R_C(29) = \big\{[1, -9, -14], [2, -8, 5]\big\}$. Konečně aplikací vzorce (2.7) nalezneme

$$\begin{aligned} C(29) = \{&x^3 + (3w+1)x^2 + (3w^2 + 2w - 9)x + w^3 + w^2 - 9w - 14 : w \in \mathbb{Z}\} \cup \\ &\{x^3 + (3w+2)x^2 + (3w^2 + 4w - 8)x + w^3 + 2w^2 - 8w + 5 : w \in \mathbb{Z}\}. \end{aligned}$$

2.5. Tabulky kanonických reprezentantů tříd rozkladu množiny $C(D)/\sim$

V roce 2022 byla metoda konstrukce množiny $C(D)$ použita pro sestavení tabulek kanonických reprezentantů tříd rozkladu množiny $C(D)/\sim$ pro všechna $D \in \mathbb{Z}$, kde $1 \leq |D| \leq 1000$. Dosažené výsledky byly prezentovány v publikaci [21]. V roce 2023 se podařilo tabulky [21] rozšířit pro všechna $D \in \mathbb{Z}$, kde $1 \leq |D| \leq 10000$. Rozšířená verze tabulek byla publikována v [23].

3. Problém kvartických polynomů a jeho řešení

Je zřejmé, že analogický problém k Problému 1.1 je možné formulovat také pro případ kvartických polynomů. Pro libovolné $D \in \mathbb{Z}$ definujme množinu

$$Q(D) = \big\{f(x) = x^4 + ax^3 + bx^2 + cx + d \in \mathbb{Z}[x] : D(f) = D\big\},$$

kde $D(f)$ označuje diskriminant polynomu $f(x)$. Je dobře známo, že pomocí koeficientů a, b, c, d lze diskriminant $D(f)$ vyjádřit ve tvaru

$$\begin{aligned} D(f) = {} & a^2b^2c^2 - 4a^2b^3d - 4a^3c^3 + 18a^3bcd - 27a^4d^2 - 4b^3c^2 \\ & + 16b^4d + 18abc^3 - 80ab^2cd - 6a^2c^2d + 144a^2bd^2 \\ & - 27c^4 + 144bc^2d - 128b^2d^2 - 192acd^2 + 256d^3. \end{aligned} \tag{3.1}$$

Problém 3.1 (2022)**.** Nechť $D \in \mathbb{Z}$. Nalezněte metodu, která umožní určit všechny normované kvartické polynomy s celočíselnými koeficienty mající diskriminant D.

Je zřejmé, že problém určit množinu $Q(D)$ je ekvivalentní problému nalézt všechna celočíselná řešení diofantické rovnice $D(f) = D$. Hlavním cílem této kapitoly je poskytnout čtenáři základní informace o řešení Problému 3.1, které bylo nalezeno v článku [22].

3.1. Ekvivalence na množině $Q(D)$

Nechť $f(x) = x^4 + ax^3 + bx^2 + cx + d \in Q(D)$. Pro každé $w \in \mathbb{Z}$ definujme polynom $f_w(x) = f(x+w)$. Podobně, jako v případě kubických polynomů, můžeme ověřit, že pro libovolné $w \in \mathbb{Z}$ platí rovnost $D(f_w) = D(f)$, jejímž důsledkem je Lemma 3.2.

Lemma 3.2. *Nechť $D \in \mathbb{Z}$. Je-li $Q(D) \neq \emptyset$, pak množina $Q(D)$ je nekonečná.*

Dále je možné dokázat, že pro polynomy $f_w(x)$ platí identita

$$f_w(x) = x^4 + \frac{f'''(w)}{3!}\,x^3 + \frac{f''(w)}{2!}\,x^2 + \frac{f'(w)}{1!}\,x + f(w), \tag{3.2}$$

ve které výrazy $f'(w)$, $f''(w)$ a $f'''(w)$ označují první, druhou a třetí derivaci $f(x)$ v bodě w. Nechť $Q(D) \neq \emptyset$. Pro $f(x), g(x) \in Q(D)$ položme

$$f(x) \sim g(x) \iff \exists\, w \in \mathbb{Z} : g(x) = f(x + w).$$

Lemma 3.3. *Relace $\sim$ je ekvivalence na množině $Q(D)$.*

Nechť $f(x) = x^4 + ax^3 + bx^2 + cx + d \in Q(D)$. Pak existují jednoznačně určená čísla $w \in \mathbb{Z}$ a $e \in \{0, 1, 2, 3\}$ tak, že $a = 4w + e$. Položme $r(x) = f(x - w) =$

$$x^4+ex^3+(b-6w^2-3ew)x^2+(c+8w^3+3ew^2-2bw)+d-3w^4-ew^3+bw^2-cw. \quad (3.3)$$

Polynom $r(x)$ budeme nazývat kanonický reprezentant třídy

$$[f(x)] = \{g(x) \in Q(D) : g(x) \sim f(x)\} \in Q(D)/\sim .$$

Konvence 3.4. Pro zápis kvartického polynomu $f(x) = x^4+ax^3+bx^2+cx+d \in \mathbb{Z}[x]$ budeme používat stručnější vyjádření ve tvaru uspořádané čtveřice koeficientů $[a, b, c, d]$.

Příklad 3.5. Nechť $f(x) = x^4 - x^3 + 2x^2 - x + 1$. Z (3.1) plyne, že $D(f) = 12$, a tedy $Q(12) \neq \emptyset$. Podle Lemma 3.2 je množina $Q(12)$ nekonečná a třída rozkladu obsahující polynom $f(x)$ je tvaru $[f(x)] = \big\{x^4 + (4w - 1)x^3 + (6w^2 - 3w + 2)x^2 + (4w^3 - 3w^2 + 4w - 1)x + w^4 - w^3 + 2w^2 - w + 1 : w \in \mathbb{Z}\big\}$. Aplikací vztahu (3.3) obdržíme, že kanonický reprezentant třídy $[f(x)]$ je polynom $r(x) = x^4 + 3x^3 + 5x^2 + 4x + 2$ a podle Konvence 3.4 můžeme $r(x)$ zapsat ve tvaru $[3, 5, 4, 2]$.

Lemma 3.6. *Nechť $[a, b, c, d], [a', b', c', d'] \in Q(D)$. Jestliže platí $[a, b, c, d] \sim [a', b', c', d']$, pak*

$$a \equiv a' \pmod 4.$$

Pomocí protipříkladu není obtížné dokázat, že opačná implikace neplatí. Zřejmě

$$[1, -5, 4, -1], [1, -6, -3, 10] \in Q(-23) \quad \text{a} \quad [1, -5, 4, -1] \not\sim [1, -6, -3, 10].$$

Následující věta má pro řešení problému kvartických polynomů zásadní význam.

Věta 3.7. *Nechť $0 \neq D \in \mathbb{Z}$ a nechť $Q(D) \neq \emptyset$. Pak $Q(D)/\sim$ má konečně mnoho tříd.*

Věta 3.7 je rovněž důsledkem obecnějšího tvrzení, které dokázal Kálmán Győry v článku [13, str. 419]. Alternativní důkaz Věty 3.7 může čtenář nalézt v [22, str. 42]. Důkaz prezentovaný v [22] využívá podstatného rozšíření Mordellova výsledku formulovaného ve Větě 2.7. Toto rozšíření provedl v roce 1929 německý matematik Carl Ludwig Siegel (1896–1981) v článku [29]. Speciálním případem Siegelova výsledku je Věta 3.8.

Věta 3.8 (C. L. Siegel, 1929)**.** *Nechť $\alpha, \beta \in \mathbb{Z}$ a nechť $4\alpha^3 + 27\beta^2 \neq 0$. Pak eliptická rovnice*

$$\eta^2 = \xi^3 + \alpha\xi + \beta \quad (3.4)$$

má nejvýše konečně mnoho celočíselných řešení.

Pro nalezení všech celočíselných řešení rovnice (3.4) je možné použít, podobně jako v případě Mordellovy rovnice (2.4), metodu popsanou v knize [30] a implementovanou v programech Magma a Sage.

Pro formulaci dalších výsledků budeme potřebovat následující označení. Pro libovolné $0 \neq D \in \mathbb{Z}$, položme

$$q(D) = \begin{cases} \#Q(D)/\sim, & \text{je-li } Q(D) \neq \emptyset, \\ 0, & \text{je-li } Q(D) = \emptyset, \end{cases}$$

a symbolem $R_Q(D)$ označme množinu všech kanonických reprezentantů tříd rozkladu množiny $Q(D)/\sim$. Množinu $R_Q(D)$ budeme nazývat úplný systém kanonických reprezentantů množiny $Q(D)/\sim$. Je zřejmé, že $\#R_Q(D) = \#Q(D)/\sim = q(D)$.

3.2. Souvislost mezi Mordellovou rovnicí a množinou $Q(D)$

Základním objevem, který umožňuje určit všechny prvky množiny $Q(D)$ je nalezení souvislosti mezi množinou $Q(D)$ a Mordellovou rovnicí (1.1) pro speciální hodnotu koeficientu k. Tuto souvislost popisuje následující věta.

Věta 3.9. *Nechť $0 \neq D \in \mathbb{Z}$. Jestliže Mordellova rovnice*

$$Y^2 = X^3 + k, \quad kde \quad k = -1769472D = -2^{16}3^3D \tag{3.5}$$

nemá celočíselné řešení, pak $Q(D) = \emptyset$.

Pro každé $0 \neq D \in \mathbb{Z}$ položme

$$M_Q(D) = \left\{[X_0, Y_0] : X_0, Y_0 \in \mathbb{Z}, Y_0^2 = X_0^3 - 2^{16}3^3D\right\} \quad \text{a} \quad m_Q(D) = \#M_Q(D).$$

Je možné dokázat, že opačná implikace k Větě 3.9 neplatí. Z předpokladu $M_Q(D) \neq \emptyset$ tedy obecně neplyne $Q(D) \neq \emptyset$.

Příklad 3.10.
(i) Nechť $D = 2$. Pak $M_Q(2) = \emptyset$ a podle Věty 3.9 platí, že $Q(2) = \emptyset$.
(ii) Nechť $D = -7$. Pak $M_Q(-7) = \{[-192, \pm 2304], [16, \pm 3520], [960, \pm 29952]\}$, a tedy $m_Q(-7) = 6$. Přesto ale $Q(-7) = \emptyset$. Skutečnost, že $Q(-7) = \emptyset$ je možné dokázat pomocí Věty 3.12, která bude uvedena v následujícím odstavci.

3.3. Eliptická rovnice $\eta^2 = \xi^3 - 108X_0\xi + 432Y_0$

Při konstrukci množiny $Q(D)$ hraje důležitou roli Lemma 3.11.

Lemma 3.11. *Nechť $\xi_0, \eta_0 \in \mathbb{Z}$. Pak existuje nejvýše jedno číslo $e \in \{0, 1, 2, 3\}$ splňující soustavu kongruencí $\xi_0 \equiv 36e^2 \pmod{96}$, $\eta_0 \equiv 9e\xi_0 - 108e^3 \pmod{1728}$.*

Následující Věta 3.12 je nejdůležitějším tvrzením celé teorie. Poskytuje nutnou a postačující podmínku pro $Q(D) \neq \emptyset$. Věta 3.12 má konstruktivní charakter, tj. umožňuje určit konkrétní tvary kanonických reprezentantů množiny $Q(D)/\sim$.

Věta 3.12. *Nechť $0 \neq D \in \mathbb{Z}$ a nechť $M_Q(D) \neq \emptyset$. Pak $Q(D) \neq \emptyset$ právě tehdy, když existuje $[X_0, Y_0] \in M_Q(D)$ tak, že eliptická rovnice*

$$\eta^2 = \xi^3 - 108X_0\xi + 432Y_0 \tag{3.6}$$

má aspoň jedno celočíselné řešení $[\xi_0, \eta_0]$ splňující soustavu kongruencí

$$36e^2 - \xi_0 \equiv 0 \pmod{96}, \tag{3.7}$$

$$108e^3 - 9e\xi_0 + \eta_0 \equiv 0 \pmod{1728}, \tag{3.8}$$

$$432e^4 - \xi_0^2 - 72e^2\xi_0 + 16e\eta_0 + 144X_0 \equiv 0 \pmod{110592} \tag{3.9}$$

pro nějaké $e \in \{0,1,2,3\}$. *Pak polynom*

$$r(x) = x^4 + ex^3 + \frac{36e^2 - \xi_0}{96}\,x^2 + \frac{108e^3 - 9e\xi_0 + \eta_0}{1728}\,x + \frac{432e^4 - \xi_0^2 - 72e^2\xi_0 + 16e\eta_0 + 144X_0}{110592}$$

leží v množině $Q(D)$.

Nechť $0 \neq D \in \mathbb{Z}$ a nechť $M_Q(D) \neq \emptyset$. Pak pro každé $[X_0, Y_0] \in M_Q(D)$ definujeme množinu $\mathscr{E}(D, X_0, Y_0) = \{[X_0, Y_0, \xi_0, \eta_0] : \xi_0, \eta_0 \in \mathbb{Z}, \eta_0^2 = \xi_0^3 - 108X_0\xi_0 + 432Y_0\}$ a klademe $e(D, X_0, Y_0) = \#\mathscr{E}(D, X_0, Y_0)$. Dále položme

$$\mathscr{E}(D) = \bigcup_{[X_0,Y_0]\in M_Q(D)} \mathscr{E}(D, X_0, Y_0), \quad e(D) = \#\mathscr{E}(D),$$

$$E_Q(D) = \big\{[[X_0, Y_0, \xi_0, \eta_0], e] \in \mathscr{E}(D) \times \{0,1,2,3\} : e \in \{0,1,2,3\} \text{ splňuje pro } [X_0, Y_0, \xi_0, \eta_0] \text{ soustavu kongruencí (3.7)–(3.9)}\big\}.$$

Věta 3.13 je důsledkem Věty 3.12.

Věta 3.13. *Nechť* $0 \neq D \in \mathbb{Z}$ *a nechť* $f(x) = x^4 + ax^3 + bx^2 + cx + d \in \mathbb{Z}[x]$. *Pak* $f(x) \in Q(D)$ *právě tehdy, když existují* $[[X_0, Y_0, \xi_0, \eta_0], e] \in E_Q(D)$ *a* $w \in \mathbb{Z}$ *tak, že*

$$\begin{aligned} a &= 4w + e, \\ b &= 6w^2 + 3ew + \frac{36e^2 - \xi_0}{96}, \\ c &= 4w^3 + 3ew^2 + \frac{36e^2 - \xi_0}{48}w + \frac{108e^3 - 9e\xi_0 + \eta_0}{1728}, \\ d &= w^4 + ew^3 + \frac{36e^2 - \xi_0}{96}\,w^2 + \frac{108e^3 - 9e\xi_0 + \eta_0}{1728}\,w \\ &\quad + \frac{432e^4 - \xi_0^2 - 72e^2\xi_0 + 16e\eta_0 + 144X_0}{110592}. \end{aligned}$$

3.4. Metoda určení množiny $Q(D)$

Na základě teoretických výsledků prezentovaných v předchozích odstavcích můžeme vytvořit postup umožňující určit množinu $Q(D)$ pro každé $0 \neq D \in \mathbb{Z}$. Tento postup může být formálně rozdělen do pěti následujících kroků.

1) Nechť $0 \neq D \in \mathbb{Z}$. Nejprve nalezneme množinu $M_Q(D)$ všech celočíselných řešení $[X_0, Y_0]$ Mordellovy rovnice $Y^2 = X^3 - 2^{16}3^3D$. Podle Věty 2.7 je $M_Q(D)$ konečná množina a podle Věty 3.9 platí, že pokud $M_Q(D) = \emptyset$, pak $Q(D) = \emptyset$.
2) Nechť $M_Q(D) \neq \emptyset$. Pro každé $[X_0, Y_0] \in M_Q(D)$ sestavíme eliptickou rovnici $\eta^2 = \xi^3 - 108X_0\xi + 432Y_0$ a určíme množinu $\mathscr{E}(D, X_0, Y_0)$. Z Věty 3.8 plyne, že $\mathscr{E}(D, X_0, Y_0)$ je konečná množina pro každé $[X_0, Y_0] \in M_Q(D)$.

Sjednocením všech množin $\mathscr{E}(D, X_0, Y_0)$ obdržíme množinu $\mathscr{E}(D)$. Je-li $\mathscr{E}(D) = \emptyset$, pak $Q(D) = \emptyset$.

3) Nechť $\mathscr{E}(D) \neq \emptyset$. Pro každou čtveřici $[X_0, Y_0, \xi_0, \eta_0] \in \mathscr{E}(D)$ provedeme test, zda existuje číslo $e \in \{0, 1, 2, 3\}$ splňující soustavu kongruencí (3.7)–(3.9). Na základě těchto testů určíme množinu $E_Q(D)$. Je-li $E_Q(D) = \emptyset$, pak $Q(D) = \emptyset$.

4) Nechť $E_Q(D) \neq \emptyset$ a $\#E_Q(D) = n$. Každému prvku $\big[[X_0, Y_0, \xi_0, \eta_0], e\big] \in E_Q(D)$ přiřadíme polynom

$$\begin{aligned} r(x) &= x^4 + ex^3 + \frac{36e^2 - \xi_0}{96}x^2 + \frac{108e^3 - 9e\xi_0 + \eta_0}{1728}x \\ &\quad + \frac{432e^4 - \xi_0^2 - 72e^2\xi_0 + 16e\eta_0 + 144X_0}{110592} \\ &= \left[e, \frac{36e^2 - \xi_0}{96}, \frac{108e^3 - 9e\xi_0 + \eta_0}{1728}, \right. \\ &\qquad \left. \frac{432e^4 - \xi_0^2 - 72e^2\xi_0 + 16e\eta_0 + 144X_0}{110592}\right] \end{aligned} \tag{3.10}$$

Podle Věty 3.12 leží polynom $r(x)$ v množině $R_Q(D)$ a přiřazení je bijektivním zobrazením mezi množinami $E_Q(D)$ a $R_Q(D)$. Tímto způsobem obdržíme úplný systém kanonických reprezentantů množiny $Q(D)/\!\sim$. Nechť $R_Q(D) = \{r_1(x), \ldots, r_n(x)\}$.

5) V závěrečném kroku konstrukce množiny $Q(D)$ přiřadíme každému $r_i(x) \in R_Q(D)$ třídu $[r_i(x)] = \{r_i(x + w) : w \in \mathbb{Z}\}$. Podle (3.2) platí, že

$$\begin{aligned} [r_i(x)] &= \left\{x^4 + \frac{r_i'''(w)}{3!}\,x^3 + \frac{r_i''(w)}{2!}\,x^2 + \frac{r_i'(w)}{1!}\,x + r_i(w) : w \in \mathbb{Z}\right\} \\ &= \left\{\left[\frac{r_i'''(w)}{3!}, \frac{r_i''(w)}{2!}, \frac{r_i'(w)}{1!}, r_i(w)\right] : w \in \mathbb{Z}\right\}. \end{aligned} \tag{3.11}$$

Sjednocením všech tříd $[r_i(x)]$ obdržíme množinu $Q(D)$.

$$Q(D) = \bigcup_{i=1}^{n} [r_i(x)] = \bigcup_{i=1}^{n}\left\{\left[\frac{r_i'''(w)}{3!}, \frac{r_i''(w)}{2!}, \frac{r_i'(w)}{1!}, r_i(w)\right] : w \in \mathbb{Z}\right\}.$$

Výše uvedený postup budeme demonstrovat na dvou příkladech.

Příklad 3.14. Nechť $D = 5$. Pak Mordellova rovnice (3.5) má tvar $Y^2 = X^3 - 8847360$. Tato rovnice má 6 celočíselných řešení

$$M_Q(5) = \{[256, \pm 2816], [384, \pm 6912], [5136, \pm 368064]\} \quad \text{a} \quad m_Q(5) = 6.$$

Ke každému ze šesti prvků množiny $M_Q(5)$ sestavíme odpovídající eliptickou rovnici (3.6) a tu vyřešíme. Řešením eliptických rovnic obdržíme následující množiny:

$$\mathscr{E}(5, 256, -2816) = \{[256, -2816, -48, 0]\},$$

$$\begin{aligned}
\mathscr{E}(5,256,2816) &= \{[256,2816,-96,\pm 1728],[256,2816,48,0],\\
&\qquad [256,2816,192,\pm 1728]\}\\
\mathscr{E}(5,384,-6912) &= \{[384,-6912,-144,0]\},\\
\mathscr{E}(5,384,6912) &= \{[384,6912,0,\pm 1728],[384,6912,144,0]\},\\
\mathscr{E}(5,5136,-368064) &= \{[5136,-368064,-432,0],[5136,-368064,-428,\pm 8],\\
&\qquad [5136,-368064,864,\pm 2592],\\
&\qquad [5136,-368064,103897,\pm 33488317]\},\\
\mathscr{E}(5,5136,368064) &= \{[5136,368064,432,0]\}.
\end{aligned}$$

Odtud plyne, že

$$\begin{aligned}
\mathscr{E}(5) = \{&[256,-2816,-48,0],[256,2816,-96,\pm 1728],[256,2816,48,0],\\
&[256,2816,192,\pm 1728],[384,-6912,-144,0],[384,6912,0,\pm 1728],\\
&[384,6912,144,0],[5136,-368064,-432,0],[5136,-368064,-428,\pm 8],\\
&[5136,-368064,864,\pm 2592],[5136,-368064,103897,\pm 33488317],\\
&[5136,368064,432,0]\},
\end{aligned}$$

a tedy, $e(5) = \#\mathscr{E}(5) = 18$. Dále, pro každý z osmnácti prvků množiny $\mathscr{E}(5)$ provedeme test, zda existuje číslo $e \in \{0,1,2,3\}$ splňující soustavu kongruencí (3.7)–(3.9). Na základě těchto testů zjistíme, že soustavě vyhovují pouze tři prvky množiny $\mathscr{E}(5)$. Z těchto prvků sestavíme množinu $E_Q(5)$.

$$\begin{aligned}
E_Q(5) = \{&[[256,2816,192,-1728],0],[[256,2816,192,1728],0],\\
&[[384,6912,144,0],0]\}.
\end{aligned}$$

Každému prvku množiny $E_Q(5)$ nyní přiřadíme uspořádanou čtveřici čísel definovanou vztahem (3.10). Tímto způsobem vytvoříme množinu $R_Q(5)$.

$$R_Q(5) = \{[2,0,-1,0],[0,-2,-1,0],[0,-2,1,0]\}.$$

Na základě Konvence 3.4 můžeme každou uspořádanou čtveřici ležící v množině $R_Q(5)$ interpretovat jako polynom. Platí tedy, že $R_Q(5) = \{r_1(x), r_2(x), r_3(x)\}$, kde

$$r_1(x) = x^4 + 2x^3 - x, \quad r_2(x) = x^4 - 2x^2 - x, \quad r_3(x) = x^4 - 2x^2 + x.$$

Polynomy $r_1(x)$, $r_2(x)$, $r_3(x)$ tvoří úplný systém kanonických reprezentantů množiny $Q(5)/\sim$. Platí tedy, že $\#R_Q(5) = \#Q(5)/\sim = q(5) = 3$. V závěrečném kroku postupu aplikujeme vztah (3.11), pomocí kterého každému reprezentantu $r_i(x) \in R_Q(5)$ přiřadíme třídu rozkladu $[r_i(x)]$. Sjednocením všech tříd $[r_i(x)]$ pak obdržíme množinu $Q(5)$.

$$\begin{aligned}
Q(5) = \{&[4w, 6w^2+3, 4w^3+6w-1, w^4+2w^3-w],\\
&[4w, 6w^2-2, 4w^3-4w-1, w^4-2w^2-w],\\
&[4w, 6w^2-2, 4w^3-4w+1, w^4-2w^2+w] : w \in \mathbb{Z}\}.
\end{aligned}$$

Příklad 3.15. Nechť $D = -87$. Pak Mordellova rovnice (3.5) má tvar $Y^2 = X^3 + 153944064$. Tato rovnice má 6 celočíselných řešení.

$$M_Q(-87) = \{[-320, \pm 11008], [-92, \pm 12376], [448, \pm 15616]\}.$$

Ke každému prvku množiny $M_Q(-87)$ sestavíme odpovídající eliptickou rovnici (3.6) a tu vyřešíme. Řešením těchto eliptických rovnic obdržíme následující množiny:

$$\begin{aligned}
\mathscr{E}(-87, -320, 11008) = \{&[-320, 11008, -80, \pm 1216], [-320, 11008, -48, \pm 1728],\\
&[-320, 11008, 240, \pm 5184], [-320, 11008, 384, \pm 8640],\\
&[320, 11008, 8592, \pm 796608]\},\\
\mathscr{E}(-87, -320, -11008) = \emptyset,&\\
\mathscr{E}(-87, -92, 12376) = \{&[-92, 12376, -156, 0]\},\\
\mathscr{E}(-87, -92, -12376) = \{&[-92, -12376, 156, 0]\},\\
\mathscr{E}(-87, 448, 15616) = \{&[448, 15616, -156, \pm 3240], [448, 15616, 96, \pm 1728]\},\\
\mathscr{E}(-87, 448, -15616) = \emptyset.&
\end{aligned}$$

Odtud plyne, že $e(-87) = \#\mathscr{E}(-87) = 16$. Pro každý z prvků množiny $\mathscr{E}(-87)$ provedeme test, zda existuje číslo $e \in \{0, 1, 2, 3\}$ splňující soustavu kongruencí (3.7)–(3.9). Na základě těchto testů zjistíme, že soustavě vyhovují pouze čtyři prvky množiny $\mathscr{E}(-87)$. Z těchto prvků sestavíme množinu $E(-87)$.

$$\begin{aligned}
E_Q(-87) = \{&[[-320, 11008, 240, 5184], 2], [[-320, 11008, 240, -5184], 2],\\
&[[448, 15616, -156, -3240], 1], [[448, 15616, -156, 3240], 3]\}.
\end{aligned}$$

Každému prvku množiny $E_Q(-87)$ přiřadíme uspořádanou čtveřici čísel definovanou vztahem (3.10). Tímto způsobem vytvoříme množinu

$$R_Q(-87) = \{[2, -1, 1, 0], [2, -1, -5, -3], [1, 2, -1, 0], [3, 5, 6, 3]\}.$$

Na základě Konvence 3.4 můžeme každou uspořádanou čtveřici ležící v množině $R_Q(-87)$ interpretovat jako polynom. Platí tedy, že

$$R_Q(-87) = \{r_1(x), r_2(x), r_3(x), r_4(x)\},$$

kde

$$\begin{aligned}
r_1(x) &= x^4 + 2x^3 - x^2 + x, \quad r_2(x) = x^4 + 2x^3 - x^2 - 5x - 3,\\
r_3(x) &= x^4 + x^3 + 2x^2 - x, \quad r_4(x) = x^4 + 3x^3 + 5x^2 + 6x + 3.
\end{aligned}$$

Polynomy $r_1(x), r_2(x), r_3(x), r_4(x)$ tvoří úplný systém kanonických reprezentantů množiny $Q(-87)/\!\sim$. Odtud plyne, že $\#R_Q(-87) = \#Q(-87)/\!\sim = q(-87) = 4$. V závěrečném kroku postupu aplikujeme vztah (3.11), pomocí kterého každému reprezentantu $r_i(x) \in R_Q(-87)$ přiřadíme třídu rozkladu $[r_i(x)]$. Sjednocením všech tříd $[r_i(x)]$ pak obdržíme množinu

$$\begin{aligned}
Q(-87) = \big\{&[4w + 2, 6w^2 + 6w - 1, 4w^3 + 6w^2 - 2w + 1, w^4 + 2w^3 - w^2 + w],\\
&[4w + 2, 6w^2 + 6w - 1, 4w^3 + 6w^2 - 2w - 5,
\end{aligned}$$

$$w^4 + 2w^3 - w^2 - 5w - 3],$$
$$[4w + 1, 6w^2 + 3w + 2, 4w^3 + 3w^2 + 4w - 1, w^4 + w^3 + 2w^2 - w],$$
$$[4w + 3, 6w^2 + 9w + 5, 4w^3 + 9w^2 + 10w + 6,$$
$$w^4 + 3w^3 + 5w^2 + 6w + 3] : w \in \mathbb{Z}\big\}.$$

3.5. Tabulky kanonických reprezentantů tříd rozkladu množiny $Q(D)/\sim$

V roce 2024 byla metoda konstrukce množiny $Q(D)$ použita pro sestavení tabulek kanonických reprezentantů tříd rozkladu množiny $Q(D)/\sim$ pro všechna $D \in \mathbb{Z}$, kde $1 \leq |D| \leq 1000$. Dosažené výsledky byly prezentovány v publikaci [24].

3.6. Sudá a lichá řešení Mordellovy rovnice $Y^2 = X^3 - 2^{16}3^3D$

V následujícím lemmatu uvedeme některé základní vlastnosti celočíselných řešení Mordellovy rovnice $Y^2 = X^3 - 2^{16}3^3D$.

Lemma 3.16. *Nechť $0 \neq D \in \mathbb{Z}$ a nechť $[X_0, Y_0] \in M_Q(D)$. Pak platí:*

(i) *Jestliže $2|X_0$, pak $4|X_0$, $8|Y_0$.*
(ii) *Jestliže $2|Y_0$, pak $4|X_0$, $8|Y_0$.*
(iii) *Jestliže $3|X_0$, pak $9|Y_0$.*
(iv) *Jestliže $3|Y_0$, pak $3|X_0$, $9|Y_0$.*

Kombinací vlastností (i) a (ii) obdržíme, že $X_0 \equiv 0 \pmod 2 \iff Y_0 \equiv 0 \pmod 2$. Je tedy přirozené zavést, podobně jako v případě kubických polynomů, následující definice:

Řešení $[X_0, Y_0] \in M_Q(D)$ se nazývá sudé, když X_0 a Y_0 jsou sudá čísla.
Řešení $[X_0, Y_0] \in M_Q(D)$ se nazývá liché, když X_0 a Y_0 jsou lichá čísla.

Dále, pro každé $0 \neq D \in \mathbb{Z}$ položme

$$\mathcal{E}(D) = \{[X_0, Y_0] \in M_Q(D) : X_0 \equiv Y_0 \equiv 0 \pmod 2\},$$
$$\mathcal{O}(D) = \{[X_0, Y_0] \in M_Q(D) : X_0 \equiv Y_0 \equiv 1 \pmod 2\}.$$

Pak $\mathcal{E}(D) \cap \mathcal{O}(D) = \emptyset$ a $\mathcal{E}(D) \cup \mathcal{O}(D) = M(D)$. Konečně pro každé přirozené číslo n definujme

$$\varepsilon(n) = \sum_{D=1}^{n} \#\mathcal{E}(D), \quad \varepsilon(-n) = \sum_{D=-1}^{-n} \#\mathcal{E}(D),$$
$$o(n) = \sum_{D=1}^{n} \#\mathcal{O}(D), \quad o(-n) = \sum_{D=-1}^{-n} \#\mathcal{O}(D).$$

Výpočet hodnot čísel $\varepsilon(n)$, $\varepsilon(-n)$, $o(n)$ a $o(-n)$ prezentovaný v článku [22, str. 46] odhalil následující významný rozdíl mezi počtem sudých a lichých řešení:

$$\varepsilon(-1000) = 1572, \quad \varepsilon(1000) = 1090, \quad o(-1000) = 100, \quad o(1000) = 44.$$

Z uvedených hodnot plyne, že existuje přibližně 95% sudých a pouze 5% lichých řešení Mordellovy rovnice $Y^2 = X^3 - 2^{16}3^3D$ pro $0 \neq |D| \leq 1000$. Tato překvapující skutečnost se stala inspirací k podrobnějšímu studiu sudých řešení. Hlavním dosaženým výsledkem je tvrzení, že pro každé sudé řešení Mordellovy rovnice může být odpovídající eliptická rovnice (3.6) nahrazena eliptickou rovnicí (3.13), jejíž celočíselné koeficienty jsou v absolutní hodnotě podstatně menší, než koeficienty v rovnici (3.6) .

Věta 3.17. *Nechť $0 \neq D \in \mathbb{Z}$ a nechť $[X_0, Y_0] \in \mathcal{E}(D)$.*

(i) *Jestliže kongruence $3\alpha X_0 + Y_0 - 4\alpha^3 \equiv 0 \pmod{27}$ neplatí pro žádné $\alpha \in \{0, 1, 2\}$, pak soustava diofantických rovnic*

$$R^2 + 3T = X_0, \quad R^3 - 9RT + 108S^2 = Y_0 \tag{3.12}$$

není řešitelná v oboru celých čísel.

(ii) *Jestliže kongruence $3\alpha X_0 + Y_0 - 4\alpha^3 \equiv 0 \pmod{27}$ platí pro nějaké $\alpha \in \{0, 1, 2\}$, pak α je jednoznačně určeno, $X_0 - 4\alpha^2 \equiv 0 \pmod{12}$, $3\alpha X_0 + Y_0 - 4\alpha^3 \equiv 0 \pmod{108}$ a množina K všech celočíselných řešení soustavy (3.12) může být získána z množiny L všech celočíselných řešení eliptické rovnice*

$$\eta^2 = \xi^3 - \alpha\xi^2 - \frac{X_0 - 4\alpha^2}{12}\,\xi + \frac{3\alpha X_0 + Y_0 - 4\alpha^3}{108}\,. \tag{3.13}$$

Navíc mezi množinami L a K existuje vzájemně jednoznačné zobrazení $\varphi : L \to K$ definované vztahem

$$\varphi(\xi_0, \eta_0) = \left[-3\xi_0 + \alpha, \eta_0, 2\alpha\xi_0 - 3\xi_0^2 + \frac{X_0 - \alpha^2}{3}\right] = [R_0, S_0, T_0] \in K. \tag{3.14}$$

(iii) *Nechť $[R_0, S_0, T_0] \in K$ a nechť*

$$g(x) = x^4 + \frac{R_0}{8}\,x^2 + \frac{S_0}{8}\,x + \frac{T_0}{256} \in \mathbb{Q}[x].$$

Dále nechť $e \in \{0, 1, 2, 3\}$ a $g_e(x) = g(x + e/4) \in \mathbb{Q}[x]$. Pak $D(g) = D(g_e) = D$ a

$$g_e(x) \in R_Q(D) \Longleftrightarrow g_e(x) \in \mathbb{Z}[x]. \tag{3.15}$$

Postup nalezení množiny $R_Q(D)$ v případě sudých řešení Mordellovy rovnice budeme demonstrovat na následujícím příkladu.

Příklad 3.18. Nechť $D = -87$. Pak $[X_0, Y_0] = [-320, 11008] \in \mathcal{E}(-87)$ a pro $\alpha = 1$ platí $3\alpha X_0 + Y_0 - 4\alpha^3 = 10044 \equiv 0 \pmod{27}$. Podle Věty 3.17 můžeme množinu K všech celočíselných řešení systému diofantických rovnic

$$R^2 + 3T = -320, \quad R^3 - 9RT + 108S^2 = 11008$$

získat pomocí množiny L všech celočíselných řešení eliptické rovnice

$$\eta^2 = \xi^3 - \xi^2 + 27\xi + 93.$$

Protože

$$L = \{[-1, \pm 8], [7, \pm 24], [11, \pm 40], [239, \pm 3688]\},$$

aplikací zobrazení (3.14) obdržíme, že

$$K = \{[4, \pm 8, -112], [-20, \pm 24, -240], [-32, \pm 40, -448], [-716, \pm 3688, -170992]\}.$$

Dále aplikací vztahu (3.15) zjistíme, že pouze dva prvky ležící v množině K vedou k polynomům s celočíselnými koeficienty. Z trojice $[-20, -24, -240]$ obdržíme pro $e = 2$ polynom $[2, -1, -5, -3] \in R_Q(-87)$ a trojice $[-20, 24, -240]$ vede pro $e = 2$ k polynomu $[2, -1, 1, 0] \in R_Q(-87)$. Všechny prvky množiny $R_Q(-87)$ získáme analogickým postupem, který aplikujeme na zbývající řešení $[X_0, Y_0] \in \mathcal{E}(-87) = M_Q(-87)$. Viz Příklad 3.15.

Na závěr poznamenejme, že množina K může být určena také pomocí množiny

$$H = \{[-80, \pm 1216], [-48, \pm 1728], [240, \pm 5184], [384, \pm 8640], [8592, \pm 796608]\}$$

všech celočíselných řešení eliptické rovnice (3.6), tj. rovnice

$$\eta^2 = \xi^3 + 34560\xi + 4755456.$$

Množinu K nalezneme tak, že každému prvku $[\xi_0, \eta_0] \in H$ přiřadíme trojici

$$\left[-\frac{\xi_0}{12}, \frac{\eta_0}{216}, \frac{144X_0 - \xi_0^2}{432}\right]$$

a ze všech získaných trojic vybereme pouze ty, které mají všechny souřadnice celočíselné.

3.7. Nové hypotézy týkající se Mordellovy rovnice

Nechť $0 \neq D \in \mathbb{Z}$ a nechť

$$\mu(D) = \begin{cases} 0, & \text{když } M_Q(D) = \emptyset, \\ 1, & \text{když } M_Q(D) \neq \emptyset. \end{cases}$$

Dále pro každé přirozené číslo n položme

$$\sigma(n) = \sum_{D=1}^{n} \mu(D) \quad \text{a} \quad \sigma(-n) = \sum_{D=-1}^{-n} \mu(D).$$

Výpočtem hodnot $\sigma(n)$ a $\sigma(-n)$ pro $n \leq 1000$ bylo v [22, str. 48] zjištěno, že

$$\frac{\sigma(1000)}{1000} = \frac{280}{1000} = 0{,}280, \quad \frac{\sigma(-1000)}{1000} = \frac{426}{1000} = 0{,}426, \quad \frac{\sigma(1000)}{\sigma(-1000)} = \frac{280}{426} \approx 0{,}657.$$

Uvedené výsledky mohou vést k následujícím hypotézám:

$$\begin{gathered} \lim_{n\to\infty} \frac{\sigma(n)}{n} = \frac{2}{7} \approx 0{,}286, \quad \lim_{n\to\infty} \frac{\sigma(-n)}{n} = \frac{3}{7} \approx 0{,}429, \\ \lim_{n\to\infty} \frac{\sigma(n)}{\sigma(-n)} = \frac{2}{3} \approx 0{,}667. \end{gathered} \tag{3.16}$$

Domněnky prezentované v (3.16) vedou k další zajímavé otázce, totiž zda podobné hypotézy mohou být formulovány také pro případ obecné Mordellovy rovnice. Je zřejmé, že ke stanovení takových hypotéz bude zapotřebí mnoha výpočtů na počítači. Díky výpočtům, které provedli Michael A. Bennett a Amir Ghadermarzi v článku [1], jsou známa všechna celočíselná řešení Mordellovy rovnice

$Y^2 = X^3 + k$ pro každé $k \in \mathbb{Z}$, kde $0 \neq |k| \leq 10^7$. Na základě výsledků těchto autorů mohou být formulovány nové hypotézy.

Pro každé $0 \neq k \in \mathbb{Z}$ nechť $\mathbb{M}(k)$ označuje množinu všech celočíselných řešení Mordellovy rovnice $Y^2 = X^3 + k$ a nechť

$$\nu(k) = \begin{cases} 0, & \text{když } \mathbb{M}(k) = \emptyset, \\ 1, & \text{když } \mathbb{M}(k) \neq \emptyset. \end{cases}$$

Dále, pro každé přirozené číslo n položme

$$s(n) = \sum_{k=1}^{n} \nu(k) \quad \text{a} \quad s(-n) = \sum_{k=-1}^{n} \nu(-k).$$

Z Tabulky 1 a Tabulky 2, které jsou prezentovány v článku [1, str. 642–643] obdržíme, že

$$\frac{s(10^7)}{10^7} = \frac{1332934}{10^7} \approx 0{,}133, \quad \frac{s(-10^7)}{10^7} = \frac{834604}{10^7} \approx 0{,}083,$$
$$\frac{s(-10^7)}{s(10^7)} = \frac{834604}{1332934} \approx 0{,}626.$$

Uvedené výsledky mohou vést k následujícím hypotézám:

$$\lim_{n\to\infty} \frac{s(n)}{n} = \frac{2}{15} = 0{,}1\bar{3}, \quad \lim_{n\to\infty} \frac{s(-n)}{n} = \frac{1}{12} = 0{,}08\bar{3},$$
$$\lim_{n\to\infty} \frac{s(-n)}{s(n)} = \frac{5}{8} = 0{,}625. \tag{3.17}$$

Domněnky (3.16) a (3.17) byly předloženy v článku [22, str. 49] ve formě problému: Dokažte nebo vyvraťte hypotézy (3.16) a (3.17).

4. Perspektivy dalšího výzkumu

Předně tabulky uvedené v publikacích [21] a [23] mohou poskytnout důležitá vodítka pro další výzkum obtížné problematiky týkající se zákona zachování rozkladu kubických polynomů nad konečnými tělesy $\mathbb{F}_p$, kde p je prvočíslo. Odkazy na literaturu týkající se tohoto problému může čtenář nalézt například v [21, str. 46]. Rovněž tabulky prezentované v [24] mohou sehrát důležitou roli při studiu analogického problému pro kvartické polynomy.

Dále je možné soustředit pozornost na nalezení důkazů hypotéz uvedených v článku [22, str. 48–49]. Tyto hypotézy se týkají asymptotického poměru počtu řešitelných a neřešitelných Mordellových rovnic. Volným pokračováním této studie by mohlo být určení asymptotického poměru počtu lichých a sudých řešení Mordellovy rovnice $Y^2 = X^3 + k$, kde $k = -432D$ a $k = -1769472D$. Některé dílčí výsledky týkající se tohoto problému byly publikovány v článcích [20, str. 112] a [22, str. 46].

Jiný možný směr výzkumu může souviset s revizí výsledků, které se týkají struktury množiny $Q(D)/\sim$. Revize by měla vést k přesnější a ucelenější představě o

počtu tříd množiny $Q(D)/\sim$ a k podrobnějšímu popisu vztahů mezi reprezentanty těchto tříd.

Konečně je možné zaměřit pozornost na popis podobností a odlišností struktur množin $C(D)/\sim$ a $Q(D)/\sim$. Lze očekávat, že důležitou roli v této otázce budou hrát Mordellovy rovnice $Y^2 = X^3 - 432D$ a $Y^2 = X^3 - 1769472D$.

Vyřešení uvedených problémů by mohlo být další částí pokračujícího příběhu kubických a kvartických rovnic.

Reference

[1] M. A. Bennett, A. Ghadermarzi: *Mordell's equation: a classical approach*, LMS Journal of Computation and Mathematics **18.1** (2015), 633–646.

[2] B. N. Delone: *Über die Darstellung der Zahlen durch die binären kubischen Formen von negativer Diskriminante*, Mathematische Zeitschrift **31** (1930), 1–26.

[3] B. N. Delone, D. K. Faddeev: *Těorija irracionalnostěj tretěj stěpeni*, Trudy Matematičeskogo Instituta imeni V. A. Steklova XI, Moskva–Leningrad, 1940.

[4] B. N. Delone, D. K. Faddeev: *The Theory of Irrationalities of the Third Degree*, Translations of Mathematical Monographs 10, AMS providence, 1964.

[5] L. E. Dickson: *History of the Theory of Numbers – Diophantine Analysis*, Volume II, Chelsea, New York, (1952).

[6] W. J. Ellison, F. Ellison, J. Pesek, C. E. Stahl, D. S. Stall: *The diophantine equation* $y^2+k = x^3$, Journal of Number Theory **4** (1972), 107–117.

[7] J.-H. Evertse: *On the representation of integers by binary cubic forms of positive discriminant*, Inventiones mathematicae, **73** (1983), 117–138.

[8] J.-H. Evertse, K. Győry: *Discriminant Equations in Diophantine Number Theory*, New Mathematical Monographs 32, Cambridge University Press, 2016.

[9] J.-H. Evertse, K. Győry: *Unit Equations in Diophantine Number Theory*, Cambridge Studies in Advanced Mathematics **146**, Cambridge University Press, 2016.

[10] J.-H. Evertse, K. Győry: *Effective Results and Methods for Diophantine Equations over Finitely Generated Domains*, London Mathematical Society Lecture Note Series **475**, 2022.

[11] S. Gauthier, F. Lê: *On the youthful writings of Louis J. Mordell on the Diophantine equation* $y^2 - k = x^3$, Archive for History of Exact Sciences **73** (2019), 427–468.

[12] J. Gebel, A. Pethö, G. H. Zimmer: *On Mordell's equation*, Compositio Mathematica **110** (1998), 335–367.

[13] K. Győry: *Sur les polynômes à coefficients entiérs et de discriminant donné*, Acta Arithmetica **23** (1973), 419–426.

[14] K. Győry: *Sur les polynômes à coefficients entiérs et de discriminant donné* II, Publicationes Mathematicae Debrecen **21** (1974), 125–144.

[15] K. Győry: *Sur les polynômes à coefficients entiérs et de discriminant donné* III, Publicationes Mathematicae Debrecen **23** (1976), 141–165.

[16] K. Győry: *Sur les polynômes à coefficients entiérs et de discriminant donné* IV, Publicationes Mathematicae Debrecen **25** (1978), 155–167.

[17] K. Győry: *On polynomials with integer coefficients and given discriminant* V, p-adic generalizations, Acta Mathematica Academiae Scientiarum Hungaricae **32** (1978), 175–190.

[18] K. Győry: *Polynomials and binary forms with given discriminant*, Publicationes Mathematicae Debrecen **69.4** (2006), 473–499.

[19] O. Hemer: *On the Diophantine Equation* $y^2 - k = x^3$, Uppsala (1952).

[20] J. Klaška: *On cubic polynomials with a given discriminant*, Mathematics for Applications **10** (2021), 103–113.

[21] J. Klaška: *Tabulky reprezentantů kubických polynomů s daným diskriminantem*, Akademické nakladatelství CERM, Brno, 2022.

[22] J. Klaška: *Quartic polynomials with a given discriminant*, Mathematica Slovaca **72.1** (2022), 35–50.
[23] J. Klaška: *The Full Systems of Canonical Representatives of Cubic Polynomials with a Given Discriminant*, Akademické nakladatelství CERM, Brno, 2023.
[24] J. Klaška: *Tabulky reprezentantů kvartických polynomů s daným diskriminantem*, Akademické nakladatelství CERM, Brno, 2024.
[25] J. London, M. Finkelstein: *On Mordell's Equation* $y^2-k=x^3$, Bowling Green, Ohio Bowling Green State University, 1973.
[26] L. J. Mordell: *The diophantine equation* $y^2-k=x^3$, Proceedings of the London Mathematical Society **13** (1913), 60–80.
[27] L. J. Mordell: *A statement by Fermat*, Proceedings of the London Mathematical Society, 2nd ser. **18** (1920), pp. v–vi.
[28] L. J. Mordell: *Diophantine Equations*, Pure and Applied Mathematics **30**, Academic Press, London–New York, 1969.
[29] C. L. Siegel: *Über einige Anwendungen diophantischer Approximationen*, Abhandlungen der Preußischer Akademie der Wissenschaften. Physikalisch–mathematische Klasse, 1–41, 1929.
[30] N. P. Smart: *The Algorithmic Resolution of Diophantine Equations*, Cambridge University Press, 1998.

Jiří Klaška, Ústav matematiky, Fakulta strojního inženýrství, Vysoké učení technické v Brně, Technická 2, 61669 Brno, Česká republika,
e-mail: klaska@fme.vutbr.cz

KONSTRUKCE KUŽELOSEČEK POMOCÍ VNĚJŠÍHO SOUČINU GEOMETRICKÉ ALGEBRY PRO KUŽELOSEČKY

PAVEL LOUČKA

Abstrakt. Článek se věnuje konstrukcím kuželoseček ze skupin bodů a konstrukcím založeným na průniku dvou kuželoseček; konstrukce jsou pak realizovány pomocí vnějšího součinu, který se vyskytuje v geometrické algebře pro kuželosečky. Popsané postupy jsou umožněny i díky využití projektivní teorie kuželoseček, například zahrnutím reprezentace bodů v nekonečnu. Zvláštní ohled se bere na konstrukci kuželoseček procházejících pěti body a na hledání speciálních kuželoseček ve svazcích kuželoseček.

1. Úvod

Kuželosečky – křivky známé již starým Řekům – našly od antiky různé využití v architektuře, matematice, inženýrství a v mnoha dalších odvětvích, [6, 8]. Byl to zvláště rapidní rozvoj počítačových technologií během 20. století, který během posledních desetiletí podnítil další využití kuželoseček, nejčastěji v problémech spojených s počítačovým viděním a grafikou, [4, 14, 22, 26].

V tomto článku se ale namísto popsání konkrétního aplikačního potenciálu těchto křivek pokusíme spíše prozkoumat jejich geometrickou krásu, a to za pomocí spojení dvou matematických nástrojů: 1) projektivní geometrie kuželoseček a 2) geometrických algeber.

V sekci 2 článku definujeme základy geometrické algebry pro kuželosečky, popíšeme, jak se v ní dají kromě vlastních bodů reálné roviny reprezentovat i body v nekonečnu, a nakonec stručně shrneme i klasifikaci různých typů kuželoseček.

V sekci 3 se potom zaměříme na použití teoretického základu při konstrukci vybraných kuželoseček z daných prvků. Kromě již známých poznatků z projektivní teorie kuželoseček sekce prezentuje také nová zjištění (ta se zvláště týkají tzv. zobecněných parabol) a nabízí alternativní, geometricky orientované způsoby konstrukcí kuželoseček.

Pro větší stručnost článku bylo nutné zahrnout jen nejdůležitější teoretický aparát a demonstrovat jen vybranou část možných případů. Detailnější popis problematiky, důkazy vět a větší množství příkladů lze najít v disertační práci [17].

2020 *MSC.* Primární 15A66; Sekundární 15A75, 15A18, 14N05.

Klíčová slova. Kuželosečka, svazek kuželoseček, singulární kuželosečka, geometrická algebra, Cliffordova algebra, reálná projektivní rovina, vnější součin.

Článek vznikl na základě disertační práce autora v oboru Aplikovaná matematika na FSI VUT v Brně, školitelem byl Petr Vašík z Ústavu matematiky.

2. Geometrická algebra pro kuželosečky (GAC)

2.1. Stručný úvod do geometrických algeber

Pro větší porozumění struktuře geometrické algebry pro kuželosečky popišme nejdříve vybrané koncepty týkající se geometrických algeber. Kvůli větší stručnosti vybíráme jen pojmy, které jsou skutečně důležité pro pochopení dalšího textu. Pro detailní popis vlastností geometrických algeber můžeme doporučit knihu C. Perwasse [25] a knihu P. Lounesta [20], které sloužily jako zdroje informací pro tuto podsekci.

Začněme pojmem *kvadratický prostor*, který je klíčový pro výstavbu geometrických algeber (pro naše potřeby se omezíme pouze na reálné kvadratické prostory).

Definice 2.1. *Kvadratickým prostorem* $\mathbb{R}^{p,q,r}$ se myslí reálný vektorový prostor dimenze $n = p + q + r$ opatřený komutativním pseudoskalárním součinem[1] $*\colon \mathbb{R}^{p,q,r} \times \mathbb{R}^{p,q,r} \to \mathbb{R}$ a *kanonickou vektorovou bází*

$$\overline{\mathbb{R}}^{p,q,r} := \{e_1, \ldots, e_p, e_{p+1}, \ldots, e_{p+q}, e_{p+q+1}, \ldots, e_{p+q+r}\},$$

pro které platí

$$e_i * e_j = \begin{cases} +1, & \text{pro } i = j, \quad i,j \in \langle 1, p\rangle, \\ -1, & \text{pro } i = j, \quad i,j \in \langle p+1, p+q\rangle, \\ 0, & \text{pro } i = j, \quad i,j \in \langle p+q+1, p+q+r\rangle, \\ 0, & \text{pro } i \neq j. \end{cases} \tag{2.1}$$

Jinými slovy, kvadratický prostor $\mathbb{R}^{p,q,r}$ obsahuje p bázových vektorů, jejichž druhá mocnina vůči součinu $*$ je $+1$, q bázových vektorů, jejichž druhá mocnina je -1, a r bázových vektorů, jejichž druhá mocnina je 0; jakákoliv dvojice různých bázových vektorů je pak na sebe ortogonální, tedy $e_i * e_j = 0$ pro $i \neq j$. Poznamenejme ještě, že bázovým vektorům, jejichž druhá mocnina je 0, se říká *vektory nulové velikosti* (angl. *null vectors*).

Ekvivalentně se dá také říct, že kvadratický prostor $\mathbb{R}^{p,q,r}$ je $(p + q + r)$-dimenzionální reálný vektorový prostor opatřený kvadratickou formou, která je indukovaná bilineární formou $*$ s vlastností (2.1). Tato kvadratická forma (stejně jako bilineární forma, která ji indukuje) se dá reprezentovat diagonální maticí B, která má na hlavní diagonále postupně p jedniček, q mínus jedniček a r nul. Kdybychom např. uvažovali prostor $\mathbb{R}^{2,3,1}$, jeho kvadratická forma by byla reprezentovaná maticí

[1] Běžný skalární součin je symetrická, pozitivně definitní, bilineární forma; použitý součin $*$ nazýváme jako „pseudoskalární“ v tom smyslu, že jeho násobením nějakého nenulového vektoru sama se sebou můžeme získat i 0 nebo dokonce záporné číslo, viz další text. Použitý součin je symetrická bilineární forma, obecně ale není pozitivně definitní. O běžný skalární součin se jedná pouze v případě, že $q = r = 0$.

$$B = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Matici B také můžeme vnímat jako přehled všech možností pseudoskalárního součinu mezi bázovými vektory podle (2.1), např. $e_1 * e_1 = 1, e_3 * e_3 = -1, e_6 * e_6 = 0$ a pro rozdílné bázové vektory platí $e_i * e_j = 0$. Pokud bychom dále chtěli spočítat v tomto prostoru pseudoskalární součin dvou obecných vektorů u a v, lze to udělat pomocí distributivity nebo – ekvivalentně – pomocí běžného maticového násobení s využitím matice B. Uvažujme např.

$$u = 3e_1 - 2e_2 + 5e_3 - 4e_4 + e_5 - e_6,$$
$$v = 2e_1 + e_2 - 4e_3 - e_4 + 3e_5 + 7e_6,$$

které lze dále reprezentovat jako vektory koeficientů v bázi $\{e_1, \ldots, e_6, \}$, tedy

$$u = (3, -2, 5, -4, 1, -1)^T,$$
$$v = (2, 1, -4, -1, 3, 7)^T.$$

Potom $u * v = u^T B v$ neboli

$$u * v = (3, -2, 5, -4, 1, -1) \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 2 \\ 1 \\ -4 \\ -1 \\ 3 \\ 7 \end{pmatrix} =$$
$$= 3{\cdot}1{\cdot}2 + (-2){\cdot}1{\cdot}1 + 5{\cdot}(-1){\cdot}(-4) + (-4){\cdot}(-1){\cdot}(-1) + 1{\cdot}(-1){\cdot}3 + (-1){\cdot}0{\cdot}7 =$$
$$= 6 - 2 + 20 - 4 - 3 + 0 = 17.$$

Zmiňme také, že trojici (p, q, r) se říká *signatura* a kromě počtů bázových vektorů, které se po řadě umocňují na $+1, -1$ a 0, značí tato trojice také *signaturu matice* příslušné kvadratické formy, tedy počty kladných, záporných a nulových vlastních čísel matice.

Na kvadratickém prostoru lze pak pomocí následující definice vystavět geometrickou algebru.

Definice 2.2. Nechť je $\mathbb{R}^{p,q,r}$ kvadratický prostor s pseudoskalárním součinem $*$ a kanonickou vektorovou bází $\overline{\mathbb{R}}^{p,q,r}$. Dále uvažujme volnou, unitární a asociativní algebru $\mathbb{A}(\mathbb{R}^{p,q,r})$ nad kvadratickým prostorem $\mathbb{R}^{p,q,r}$, jejíž součin značíme $\circ$. Potom $\mathbb{A}(\mathbb{R}^{p,q,r})$ se nazývá *geometrická algebra*, jestliže pro libovolný vektor $a \in \mathbb{R}^{p,q,r} \subset \mathbb{A}(\mathbb{R}^{p,q,r})$ platí

$$a \circ a = a * a. \tag{2.2}$$

Geometrická algebra nad $\mathbb{R}^{p,q,r}$ se pak značí $\mathbb{G}\left(\mathbb{R}^{p,q,r}\right)$ nebo jednodušeji $\mathbb{G}_{p,q,r}$ a jejímu součinu $\circ$ se pak říká *Cliffordův* nebo *geometrický součin*. Ačkoli v definici výše se tento součin značí jako $\circ$, obvykle se jeho značka zcela vypouští; pro geometrický součin dvou objektů se tedy používá prostá juxtapozice.

Poznámka 2.3. Často se lze setkat s kvadratickými prostory, které nemají žádné bázové vektory nulové velikosti; v takových případech se prostor obvykle značí pouze jako $\mathbb{R}^{p,q}$ a přidružená geometrická algebra jako $\mathbb{G}_{p,q}$. Podobně lze také geometrické algebry budovat nad kvadratickými prostory $\mathbb{R}^n$ s n-ticí běžných euklidovských bázových vektorů, jejichž druhá mocnina je $+1$; takové geometrické algebry se potom značí jednoduše jako $\mathbb{G}_n$.

Následně, pokud není v kvadratickém prostoru či příslušné geometrické algebře přítomna trojice horních (resp. dolních) indexů, ale například jen dvojice či pouze jedno číslo, i této dvojici či jednomu číslu se někdy říká signatura.

Abychom lépe mohli vysvětlit některé přívlastky popisující geometrické algebry zavedené v Definici 2.2, řekněme nejprve něco víc o prvcích geometrických algeber.

Kromě vektorů z $\mathbb{R}^{p,q,r}$ (tedy vektorů v běžném slova smyslu) obsahuje $\mathbb{G}_{p,q,r}$ i jiné prvky, jak uvidíme níže (prvkům geometrických algeber se pak obecně říká *multivektory*). Ke konstrukci složitějších multivektorů se váže několik dalších pojmů, které můžeme snadno demonstrovat pomocí geometrické algebry $\mathbb{G}_3$ s kanonickou vektorovou bází $\{e_1, e_2, e_3\}$.

Geometrickému součinu více různých bázových vektorů se říká *bázový blade*. Příkladem bázového bladu v této geometrické algebře může být např. $e_2e_3e_1$; takové blady se pak někdy zapisují jednodušeji pomocí jednoho písmene, s následným zřetězením spodních indexů, tudíž $e_2e_3e_1 = e_{231}$.

Stupeň nebo *grade* bázového bladu je potom počet různých generujících bázových vektorů v bladu a značí se gr. Platí tedy $\mathrm{gr}(e_2e_3e_1) = 3$.

Důležité je také, že na pořadí bázových vektorů v bázovém bladu *záleží*, dá se totiž ukázat, že geometrický součin dvou bázových vektorů je antikomutativní, tj.

$$e_ie_j = -e_je_i, \tag{2.3}$$

z čehož mimo jiné plyne, že geometrický součin bázového vektoru se sebou samým je nula, tj.

$$e_ie_i = 0.$$

Pomocí vlastnosti (2.3) lze jakýkoliv bázový blade přeskládat tak, aby byly indexy tvořicích bázových vektorů ve vzestupném pořadí, například

$$e_2e_3e_1 = -e_2e_1e_3 = e_1e_2e_3.$$

Množina všech různých bázových bladů se vzestupným pořadím indexů tvořicích bázových vektorů, ve které jsou navíc blady seřazeny vzestupně podle stupně, se pak nazývá *kanonická algebraická báze* geometrické algebry. Pro $\mathbb{G}_3$ je to báze

$$\overline{\mathbb{G}}_3 = \{1, e_1, e_2, e_3, e_1e_2, e_1e_3, e_2e_3, e_1e_2e_3\}.$$

Obecně platí, že geometrická algebra $\mathbb{G}_{p,q,r}$ má vždy bázové blady stupňů 0 až $n = p + q + r$ a její kanonická algebraická báze obsahuje dohromady 2^n různých bázových bladů. Zde také poznamenejme, že bázový blade nulového stupně je 1 a že bázovému bladu s nejvyšším možným stupněm se říká *pseudoskalár* a značívá se jako I. Navíc, pokud i-tý bázový blade z kanonické algebraické báze označíme jako E_i, pak se dá jakýkoli multivektor $A \in \mathbb{G}_{p,q,r}$ zapsat jako

$$A = \sum_{i=1}^{2^n} a^i E_i, \quad a^i \in \mathbb{R}$$

nebo pomocí Einsteinovy sumační konvence jednoduše jako $A = a^i E_i$. Takový multivektor v $\mathbb{G}_3$ může mít např. formu

$$A = 5 - 3e_2 + 7e_1e_3.$$

Zmiňme také, že multivektor, který se skládá jen z bladů k-tého stupně, se nazývá *k-vektor*. Některé k-vektory se vyskytují tak často, že mají i zaběhlý jednoslovný název; např. 1-vektorům se někdy pro zjednodušení říká *vektory*, 2-vektorům *bivektory* a 3-vektorům *trivektory*.

Nyní, po přiblížení pojmu multivektoru, můžeme algebraické vlastnosti geometrických algeber snadněji vyložit:

1. To, že geometrická algebra je *volná algebra*, znamená, že její prvky lze volně konstruovat řetězením pomocí součinu algebry – tady konkrétně pomocí geometrického součinu, jak jsme viděli na příkladech výše.
2. To, že geometrická algebra je *unitární algebra*, znamená, že vůči jejímu součinu existuje neutrální prvek – neutrálním prvkem vůči geometrickému součinu je 1.
3. To, že geometrická algebra je *asociativní algebra*, se dá shrnout ve dvou bodech:
   (a) Multivektory společně s operací sčítání multivektorů a s operací násobení skalárem tvoří vektorový prostor nad $\mathbb{R}$.
   (b) Geometrický součin multivektorů je vůči algebře uzavřený, je asociativní a distributivní a navíc platí, že geometrický součin skaláru α a multivektoru A je shodný se skalárním násobkem multivektoru, tedy

$$\alpha \circ A = A \circ \alpha = \alpha A.$$

Zásadní rozdíl mezi geometrickou algebrou a jinými asociativními algebrami je rovnost (2.2), které se říká *definující rovnost* (angl. *defining equation*). Tato rovnost říká, že geometrickým součinem 1-vektoru sama se sebou je skalár.

Ještě popišme dvě zásadní operace mezi multivektory – *vnitřní* a *vnější součin*. Obě operace lze zavést pomocí tzv. *stupňové projekce* (angl. *grade projection*). Tu nejprve zavedeme mezi bázovými blady a pak ji rozšíříme na multivektory.

Definice 2.4. Nechť E_i je i-tý bázový blade geometrické algebry. Potom *stupňová projekce* bladu E_i na stupeň k se značí jako $\langle E_i \rangle_k$ a je definována jako

$$\langle E_i \rangle_k := \begin{cases} E_i, & \text{pro } \operatorname{gr}(E_i) = k, \\ 0, & \text{pro } \operatorname{gr}(E_i) \neq k. \end{cases}$$

Definice 2.5. Nechť E_i a E_j je i-tý, resp. j-tý bázový blade a jejich stupně jsou po řadě k a l. Potom *vnitřní součin* bladů E_i a E_j je definován jako

$$E_i \cdot E_j := \begin{cases} \langle E_i E_j \rangle_{|k-l|}, & \text{pro } i, j > 0, \\ 0, & \text{pro } i = 0 \text{ nebo } j = 0. \end{cases}$$

Definice 2.6. Nechť E_i a E_j je i-tý, resp. j-tý bázový blade a jejich stupně jsou po řadě k a l. Potom *vnější součin* bladů E_i a E_j je definován jako

$$E_i \wedge E_j := \langle E_i E_j \rangle_{k+l}.$$

Pro názornost uveďme jednoduchý příklad vnitřního a vnějšího součinu dvou bázových bladů:

$$\begin{aligned} (e_1 e_2) \cdot e_2 &= \langle e_1 e_2 e_2 \rangle_{|2-1|} = \langle e_1 \rangle_1 = e_1, \\ (e_1 e_2) \wedge e_3 &= \langle e_1 e_2 e_3 \rangle_{2+1} = \langle e_1 e_2 e_3 \rangle_3 = e_1 e_2 e_3. \end{aligned}$$

Protože stupňová projekce je distributivní, pro multivektor $A = a^i E_i$ platí

$$\langle A \rangle_k = a^i \langle E_i \rangle_k,$$

a předchozí definice vnitřního a vnějšího součinu se tedy dají přirozeně rozšířit na jakékoliv multivektory.

Nakonec také zmiňme, že lze ukázat, jak elegantně v sobě geometrický součin 1-vektorů spojuje vnitřní a vnější součin. Jsou-li a a b 1-vektory, pak platí

$$ab = a \cdot b + a \wedge b.$$

Geometrický součin dvou 1-vektorů je tedy formálním součtem jejich vnitřního a vnějšího součinu. Zdůrazněme ovšem, že pro obecné multivektory tato rovnost neplatí. Je také vhodné upozornit na to, že pro dva různé 1-vektory a a b (a obecně jakékoli dva blady stejného stupně) vnitřní součin splývá se součinem pseudoskalárním, tj.

$$a \cdot b = a * b,$$

matici bilineární formy lze tedy vnímat i jako matici realizující vnitřní součin 1-vektorů.

2.2. Základy GAC

Geometrická algebra pro kuželosečky (zkráceně GAC, z angl. *Geometric Algebra for Conics*), původně navržená C. Perwassem v knize [25] a později rozvinutá trojicí Hrdina, Návrat a Vašík v článku [12], rozšiřuje koncept dvoudimenzionální konformní geometrické algebry $\mathbb{G}_{3,1}$ (2D CGA) tak, aby byla nová algebra schopna

reprezentovat kuželosečky. Přesněji řečeno, GAC je geometrická algebra $\mathbb{G}_{5,3}$ s vnořením $C : \mathbb{R}^2 \to \mathbb{R}^{5,3}$ bodu $p = xe_1 + ye_2$ z roviny $\mathbb{R}^2$ do 6-dimenzionálního podprostoru 1-vektorů ve tvaru

$$C(x,y) = \bar{n}_+ + xe_1 + ye_2 + \frac{1}{2}(x^2+y^2)n_+ + \frac{1}{2}(x^2-y^2)n_- + xyn_\times, \tag{2.4}$$

kde

$$\{\bar{n}_\times, \bar{n}_-, \bar{n}_+, e_1, e_2, n_+, n_-, n_\times\} \tag{2.5}$$

je báze $\mathbb{G}_{5,3}$, společně s bilineární formou danou maticí

$$B = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Význam bázových vektorů je pak následující: vektory $\bar{n}$ označují tři vzájemně ortogonální vektory, kterým se říká „počátky“, vektory e_1 a e_2 jsou bázové vektory euklidovské roviny $\mathbb{R}^2$ a nakonec vektory n představují trojici vzájemně ortogonálních „nekonečen“.

Poznamenejme, že GAC jakožto geometrická algebra se signaturou $(5,3)$ by měla ve své výchozí definici obsahovat 5 bázových vektorů s druhou mocninou $+1$ a 3 bázové vektory s druhou mocninou -1; to ale, podle matice bilineární formy, zdá se, neplatí. Příčinou je, že zde nepoužíváme výchozí bázi, ale bázi transformovanou, pro kterou platí, že vektory e_1 a e_2 mají druhou mocninu $+1$ a počátky i nekonečna se umocňují na 0, jsou to tedy vektory nulové velikosti. Navíc, vnitřní součin každého počátku se sobě odpovídajícím nekonečnem dává -1, [12, 13].

Zdůrazněme také, že ani změnou původní báze se nezměnila *signatura kvadratické formy* matice B, jež je shodná se signaturou geometrické algebry, tedy $(5,3)$.

Dále připomeňme základní typy reprezentací objektů v GAC:

Definice 2.7. Řekneme, že prvek $A_I \in \mathbb{G}_{5,3}$ je *reprezentací geometrického objektu* $A \subset \mathbb{R}^2$ *vnitřním součinem* právě tehdy, když

$$A = \left\{p \in \mathbb{R}^2 : C(p) \cdot A_I = 0\right\},$$

kde „$\cdot$“ značí vnitřní součin v GAC. Této reprezentaci se také říká *IPNS reprezentace* (z angl. *Inner Product Null Space Representation*), [12].

IPNS reprezentace kuželosečky Q v GAC j pak dána 1-vektorem

$$Q_I = \bar{v}^\times \bar{n}_\times + \bar{v}^- \bar{n}_- + \bar{v}^+ \bar{n}_+ + v^1 e_1 + v^2 e_2 + v^+ n_+ \tag{2.6}$$

a IPNS reprezentace bodu $p = xe_1 + ye_2$, $p \in \mathbb{R}^2$, je dána vnořením (2.4), tedy jako 1-vektor

$$P_I = \bar{n}_+ + xe_1 + ye_2 + \frac{1}{2}(x^2 + y^2)n_+ + \frac{1}{2}(x^2 - y^2)n_- + xyn_\times.$$

Je tedy vidět, že jak bod, tak kuželosečka, jsou vnořeny do 6-dimenzionálních podprostorů $\mathbb{R}^{5,3}$.

Objekty GAC můžeme reprezentovat také pomocí vnějšího součinu, kterému se v geometrických algebrách říká *wedge* a který se značí „$\wedge$“. Díky dualitě (značené hvězdičkou) mezi reprezentacemi vnitřním a vnějším součinem platí

$$\left\{p \in \mathbb{R}^2 : C(p) \cdot A_I = 0\right\} = \left\{p \in \mathbb{R}^2 : C(p) \wedge A_I^* = 0\right\}.$$

Je to právě A_I^*, které je v geometrických algebrách obvykle považováno za reprezentaci objektu A pomocí vnějšího součinu, v GAC je tomu ovšem trochu jinak. A_I^* je vždy multivektor ve formě $A_O \wedge \bar{n}_- \wedge \bar{n}_\times$, kde A_O je 5-vektor, který obsahuje pouze bázové vektory zastoupené v 6-dimenzionálním podprostoru kuželoseček (2.6). Vzhledem k tomu je vhodné jako reprezentaci objektu A vnějším součinem v GAC zvolit právě A_O:

Definice 2.8. Řekneme, že prvek $A_O \in \mathbb{G}_{5,3}$ je *reprezentací geometrického objektu* $A \subset \mathbb{R}^2$ *vnějším součinem* právě tehdy, když

$$A = \left\{p \in \mathbb{R}^2 : C(p) \wedge A_O \wedge \bar{n}_- \wedge \bar{n}_\times = 0\right\}.$$

Této reprezentaci se také říká *OPNS reprezentace* (z angl. *Outer Product Null Space Representation*),[12].

Dualita mezi IPNS a OPNS reprezentacemi potom vypadá následovně:

$$A_O = (A_I \wedge n_- \wedge n_\times)^*,$$
$$A_I = (A_O \wedge \bar{n}_- \wedge \bar{n}_\times)^*.$$

Přechod od jedné reprezentace ke druhé se pak dá realizovat pomocí nepravých pseudoskalárů

$$\begin{aligned} I_{OI} &= \bar{n}_+\bar{n}_-\bar{n}_\times e_1e_2n_+, \\ I_{IO} &= \bar{n}_+e_1e_2n_+n_-n_\times, \end{aligned} \tag{2.7}$$

a vnitřního součinu jako

$$\begin{aligned} A_O &= A_I \cdot I_{IO}, \\ A_I &= A_O \cdot I_{OI}. \end{aligned} \tag{2.8}$$

Jak bude podrobněji popsáno v sekci 3, vnější součin se dá využít ke konstrukci některých kuželoseček – např. OPNS reprezentace kuželosečky Q, která prochází pěti různými body $p_1, \ldots, p_5$, se dá zkonstruovat jako

$$Q_O = P_1 \wedge P_2 \wedge P_3 \wedge P_4 \wedge P_5,$$

kde $P_1, \ldots, P_5$ jsou body $p_1, \ldots, p_5$ vnořené do GAC podle (2.4). Pomocí wedge se dá také získat IPNS reprezentace průniku dvou kuželoseček, konkrétně jako wedge jejich IPNS reprezentací, tedy

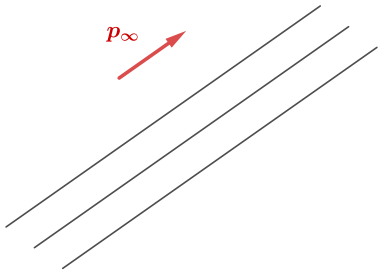
$$\left(Q^1 \cap Q^2\right)_I = Q_I^1 \wedge Q_I^2. \tag{2.9}$$

Takto získaný průnik dvou kuželoseček se potom nazývá *čtyřbod* (angl. *four-point*), [12].

Poznámka 2.9. Je třeba zdůraznit, že reprezentace objektů v GAC jsou homogenní – nenulový násobek reprezentace tedy představuje stejný objekt, jako reprezentace původní, [12].

2.3. Projektivizace GAC

Kromě bodů reálné roviny $\mathbb{R}^2$ lze také uvažovat *body v nekonečnu* – každý z těchto bodů si lze představit jako společný bod všech rovnoběžek se stejným směrem, takový bod se pak značí šipkou v příslušném směru a lze ho reprezentovat jako vektor tohoto směru, viz Obrázek 1. Množina všech bodů v nekonečnu (pro všechny možné směry rovnoběžek) potom tvoří *přímku v nekonečnu* l_∞. Když reálnou rovinu dále obohatíme o prvky v nekonečnu,vznikne projektivní reálná rovina $\mathbb{RP}^2$, tedy $\mathbb{RP}^2 = \mathbb{R}^2 \cup l_\infty$. Pro snadné odlišení se pak bodům z $\mathbb{R}^2$ říká *vlastní body*, bodům v nekonečnu *nevlastní body*, a přímce v nekonečnu *nevlastní přímka*[2], [27, 15].



Obrázek 1. Nevlastní bod p_∞ jako směr rovnoběžných přímek

Poznámka 2.10. Poznamenejme také, že slovem *směr* se zde myslí spíše *sklon* přímky, takže nenulový násobek nevlastního bodu reprezentuje stále stejný nevlastní bod. Šipka na Obrázku 1 by tedy klidně mohla být obousměrná.

Ačkoli nevlastní body jsou pro teorii kuželoseček zásadní, GAC původně uvažovala jen vlastní body, [12]. Jak vlastní, tak nevlastní body projektivní roviny $\mathbb{RP}^2$ se mimo rámec GAC dají snadno reprezentovat pomocí tzv. *homogenních souřadnic*, [11]:

[2]V anglicky psané literatuře se obvykle nevlastní bod nazývá *point at infinity*, *ideal point* nebo *figurative point*, nevlastní přímka pak *line at infinity*. Aby se daly vlastní a nevlastní body snadno odlišit, používal autor článku v disertaci [17] pojmenování podobná češtině: *vlastní–proper* a *nevlastní–improper*. I takto rozlišené názvy lze v anglicky psané literatuře někdy potkat.

Definice 2.11. Nechť $p = (x, y)$, $p \in \mathbb{RP}^2$, je vlastní bod, potom jeho *homogenní souřadnice* v $\mathbb{RP}^2$ jsou

$$p = k(x, y, 1), \qquad k \in \mathbb{R} \setminus \{0\},$$

zatímco *homogenní souřadnice* nevlastního bodu $p_\infty = (s, t)$, $(s, t) \neq (0, 0)$, $p_\infty \in \mathbb{RP}^2$, jsou

$$p_\infty = k(s, t, 0), \qquad k \in \mathbb{R} \setminus \{0\}.$$

Právě díky konceptu homogenních souřadnic se v GAC dají reprezentovat jak vlastní, tak nevlastní body, a to rozšířením definičního oboru vnoření (2.4) z $\mathbb{R}^2$ na $\mathbb{RP}^2$ podle následující definice, [17, 18, 19]:

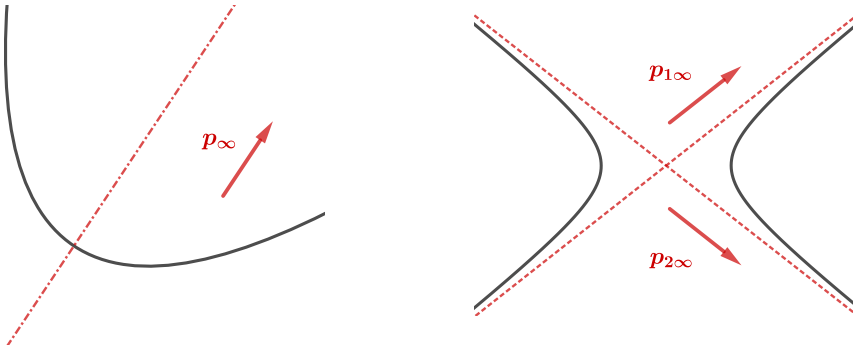
Definice 2.12. Úpravou vnoření $C : \mathbb{R}^2 \to \mathbb{R}^{5,3}$ ve formě (2.4) definujeme *rozšířené vnoření* $C\mathbb{P} : \mathbb{RP}^2 \to \mathbb{R}^{5,3}$ bodu $p = (a, b, c)$, $(a, b, c) \neq (0, 0, 0)$, reálné projektivní roviny $\mathbb{RP}^2$ jako

$$C\mathbb{P}(a, b, c) = c^2\bar{n}_+ + ace_1 + bce_2 + \frac{1}{2}(a^2 + b^2)n_+ + \frac{1}{2}(a^2 - b^2)n_- + abn_\times.$$

Poznámka 2.13. Kdybychom místo bodu $(a, b, c) \in \mathbb{RP}^2$ chtěli do GAC vnořit jeho nenulový násobek (tedy geometricky identický bod), dostaneme po úpravě

$$C\mathbb{P}(k(a, b, c)) = k^2\left(c^2\bar{n}_+ + ace_1 + bce_2 + \frac{1}{2}(a^2 + b^2)n_+ + \frac{1}{2}(a^2 - b^2)n_- + abn_\times\right),$$

což je opět jen nenulový násobek původního vnoření. Rozšířené vnoření je tedy konzistentní s Poznámkou 2.9, protože nenulový násobek jakéhokoliv geometrického objektu v GAC musí reprezentovat stejnou geometrickou množinu.



Obrázek 2. Nevlastní body paraboly a hyperboly: Parabola má jeden nevlastní bod ve směru své osy, hyperbola má dva ve směrech svých asymptot.

Důsledek 2.14. *Protože vlastní bod* $p = (x, y)$ *lze pomocí homogenních souřadnic zapsat jako* $(x, y, 1)$*, rozšířené vnoření* $C\mathbb{P}$ *i původní vnoření* C *vnořují vlastní body do GAC stejným předpisem:*

$$C\mathbb{P}(x, y, 1) \equiv C(x, y) = \bar{n}_+ + xe_1 + ye_2 + \frac{1}{2}(x^2 + y^2)n_+ + \frac{1}{2}(x^2 - y^2)n_- + xyn_\times.$$

Na druhou stranu, nevlastní bod $p_\infty = (s,t)$ s homogenními souřadnicemi $(s,t,0)$ je do GAC vnořen ve formě

$$C\mathbb{P}(s,t,0) = \frac{1}{2}(s^2+t^2)n_+ + \frac{1}{2}(s^2-t^2)n_- + stn_\times.$$

Poznamenejme také, že – na rozdíl do vlastního bodu – vnoření nevlastního bodu obsahuje pouze „nekonečna“ vektorové báze (2.5).

2.4. Klasifikace kuželoseček

Připomeňme také, že kuželosečky se dají reprezentovat pomocí symetrické matice typu 3×3, kterou lze získat z koeficientů IPNS kuželosečky (2.6) jako

$$M = \begin{pmatrix} -\frac{1}{2}(\bar v^+ + \bar v^-) & -\frac{1}{2}\bar v^\times & \frac{1}{2}v^1 \\ -\frac{1}{2}\bar v^\times & -\frac{1}{2}(\bar v^+ - \bar v^-) & \frac{1}{2}v^2 \\ \frac{1}{2}v^1 & \frac{1}{2}v^2 & -v^+ \end{pmatrix} = \begin{pmatrix} q_{11} & q_{12} & q_{13} \\ q_{12} & q_{22} & q_{23} \\ q_{13} & q_{23} & q_{33} \end{pmatrix}. \tag{2.10}$$

Pomocí této matice pak lze kuželosečku plně klasifikovat, tj. určit její typ a další vlastnosti, [16]. Její koeficienty také definují obvyklé rovnice kuželosečky v $\mathbb{R}^2$, resp. v $\mathbb{RP}^2$, [16, 8]:

$$Q_{\mathbb{R}^2}: q_{11}x^2 + 2q_{12}xy + q_{22}y^2 + 2q_{13}x \ + 2q_{23}y \ + q_{33} \ = 0, \tag{2.11}$$

$$Q_{\mathbb{RP}^2}: q_{11}x^2 + 2q_{12}xy + q_{22}y^2 + 2q_{13}xz + 2q_{23}yz + q_{33}z^2 = 0. \tag{2.12}$$

Pro naše účely bude později důležitá i hlavní podmatice typu 2×2

$$\bar M = M_{33} = \begin{pmatrix} -\frac{1}{2}(\bar v^+ + \bar v^-) & -\frac{1}{2}\bar v^\times \\ -\frac{1}{2}\bar v^\times & -\frac{1}{2}(\bar v^+ - \bar v^-) \end{pmatrix} = \begin{pmatrix} q_{11} & q_{12} \\ q_{12} & q_{22} \end{pmatrix} \tag{2.13}$$

a další dvě podmatice typu 2×2

$$M_{11} = \begin{pmatrix} -\frac{1}{2}(\bar v^+ - \bar v^-) & \frac{1}{2}v^2 \\ \frac{1}{2}v^2 & -v^+ \end{pmatrix} = \begin{pmatrix} q_{22} & q_{23} \\ q_{23} & q_{33} \end{pmatrix}, \tag{2.14}$$

$$M_{22} = \begin{pmatrix} -\frac{1}{2}(\bar v^+ + \bar v^-) & \frac{1}{2}v^1 \\ \frac{1}{2}v^1 & -v^+ \end{pmatrix} = \begin{pmatrix} q_{11} & q_{13} \\ q_{13} & q_{33} \end{pmatrix}. \tag{2.15}$$

Následně definujme ještě pomocné veličiny

$$\begin{aligned} \Delta &= \det(M), \\ \delta &= \det(\bar M), \\ J &= \operatorname{tr}(\bar M) = q_{11} + q_{22}, \\ \Delta' &= \det(M_{11}) + \det(M_{22}) \end{aligned} \tag{2.16}$$

a popišme základní rozdělení kuželoseček na základě výše definovaných matic a veličin:

Definice 2.15. Nechť je Q kuželosečka reprezentovaná maticí M ve formě (2.10), podmaticemi (2.13)–(2.15) a pomocnými veličinami definovanými v (2.16).

Jestliže $\Delta \neq 0$, pak nazýváme Q *regulární kuželosečkou*, v opačném případě se jedná o kuželosečku *singulární* (ve starší literatuře se jí též říká *zvrhlá*). Ekvivalentně se dá říct, že matice M regulární kuželosečky má plnou hodnost, tedy $\mathrm{h}(M) = 3$, a matice singulární kuželosečky nemá plnou hodnost, tj. $\mathrm{h}(M) < 3$.

Jestliže $\delta \neq 0$, pak nazýváme Q *středovou kuželosečkou*, v opačném případě se jedná o kuželosečku *nestředovou*. Ekvivalentně se dá říct, že podmatice $\bar{M}$ středové kuželosečky má plnou hodnost, tedy $\mathrm{h}(\bar{M}) = 2$, a podmatice nestředové kuželosečky nemá plnou hodnost, tj. $\mathrm{h}(\bar{M}) < 2$, [15].

Detailní klasifikaci kuželoseček v $\mathbb{RP}^2$ na základě výše definovaných matic a veličin lze najít v Tabulce 1.

Úmluva 2.16. *Kuželosečka reprezentovaná nulovou maticí by ve skutečnosti představovala všechny body v $\mathbb{RP}^2$ a taková množina obvykle není za kuželosečku považována. Pokud tedy budeme mluvit o kuželosečce v $\mathbb{RP}^2$, uvažujme vždy, že její matice je nenulová.*

Úmluva 2.17. *V textu uvažujme jen kuželosečky s reálnými koeficienty. Druhým dechem dodejme, že i kuželosečky popsané rovnicemi s výlučně reálnými koeficienty můžou představovat množinu v $\mathbb{C}^2$ (resp. $\mathbb{CP}^2$), která je geometricky smysluplná, jak lze vidět v Tabulce 1.*

Poznámka 2.18. Singulární kuželosečky lze vždy algebraicky rozložit na dvojici přímek, a to včetně případů dvou splývajících přímek či dvou imaginárních přímek, [8]. Jeden z algoritmů schopných takové dekompozice lze najít např. v knize [27].

Dodejme také, že v $\mathbb{RP}^2$ může být alespoň jednou z dvojice přímek i *přímka v nekonečnu* (*nevlastní přímka*), proto se v klasifikaci dané Tabulkou 1 označují přímky, které nejsou přímkami v nekonečnu, jako přímky *vlastní*. Nakonec poznamenejme, že kuželosečky obsahující nevlastní přímku existují v $\mathbb{RP}^2$, ale nikoli v $\mathbb{R}^2$, takže je lze vyjádřit pouze rovnicí ve tvaru (2.12), ale rovnicí (2.11) už ne.

3. Konstrukce kuželoseček pomocí vnějšího součinu (wedge)

3.1. Pět různých bodů

Jak bylo již zmíněno, OPNS reprezentaci kuželosečky Q lze obecně získat jako wedge pěti různých bodů $p_1, \ldots, p_5$ vnořených do GAC, tedy:

$$Q_O = P_1 \wedge P_2 \wedge P_3 \wedge P_4 \wedge P_5.$$

Takto získaná kuželosečka poté prochází všemi pěti body, nebo – v některých případech – nemůže být geometricky jednoznačně určena; v takových případech platí

$$P_1 \wedge P_2 \wedge P_3 \wedge P_4 \wedge P_5 = 0.$$

Existenci, jednoznačnost a regularitu kuželosečky dané pomocí pěti bodů lze posoudit na základě největšího počtu kolineárních bodů v dané pětici, [24], jak je shrnuto v Tabulce 2.

Tabulka 1. Klasifikace kuželoseček v $\mathbb{RP}^2$ podle hodnosti jejich matic a pomocných veličin, [16, 7]

h(M)	h($\bar{M}$)	Další specifikace		**Typ kuželosečky**
3	2	$\delta > 0$	$\frac{\Delta}{J} < 0$	**reálná elipsa** (reálná kružnice, pokud $q_{11} = q_{22}$ a $q_{12} = 0$)
			$\frac{\Delta}{J} > 0$	**žádná reálná množina** (imaginární elipsa)
		$\delta < 0$		**hyperbola**
	1			**parabola**
2	2	$\delta < 0$		**dvě vlastní reálné různoběžky**
		$\delta > 0$		**vlastní reálný bod** (dvě vlastní imaginární různoběžky)
	1	$\Delta' < 0$		**dvě vlastní reálné rovnoběžky**
		$\Delta' > 0$		**nevlastní reálný bod** (dvě vlastní imaginární rovnoběžky)
	0			**vlastní přímka a nevlastní přímka**
1	1			**dvojnásobná vlastní reálná přímka**
	0			**dvojnásobná nevlastní přímka**

Prozkoumejme nyní několik příkladů konstrukce kuželosečky procházející 5 body pomocí GAC wedge[3].

Příklad 3.1. Regulární kuželosečku danou 5 body v obecné lineární poloze (tj. žádné tři body nejsou kolineární) lze vidět na Obrázku 3 (a). Zvolené body mají souřadnice $(-1,-4), (3,-2), (3,3), (-2,3)$ a $(-4,0)$, jejich GAC reprezentanti jsou tedy

$$P_1 = C(-1,-4) = \bar{n}_+ - e_1 - 4e_2 + \frac{17}{2}n_+ - \frac{15}{2}n_- + 4n_\times,$$
$$P_2 = C(3,-2) = \bar{n}_+ + 3e_1 - 2e_2 + \frac{13}{2}n_+ + \frac{5}{2}n_- - 6n_\times,$$
$$P_3 = C(3,3) = \bar{n}_+ + 3e_1 + 3e_2 + 9n_+ + 9n_\times,$$
$$P_4 = C(-2,3) = \bar{n}_+ - 2e_1 + 3e_2 + \frac{13}{2}n_+ - \frac{5}{2}n_- - 6n_\times,$$

[3]Příklady uvedené v článku byly napočítány v softwaru MAPLE s pomocí balíčku „Clifford“, [1], který umožňuje výpočty v prostředí Cliffordových algeber.

Tabulka 2. Klasifikace kuželoseček daných pěti body

Největší počet kolineárních bodů	Vytvořená kuželosečka		
	existence	**regularita**	**možné typy**
2	jednoznačná	regulární	elipsa, hyperbola, parabola
3	jednoznačná	singulární	dvě různoběžky nebo rovnoběžky
4	nejednoznačná	singulární	dvě různoběžky nebo rovnoběžky
5	nejednoznačná	singulární	dvě různoběžky nebo rovnoběžky, dvojnásobná přímka

$$P_5 = C(-4,0) = \bar{n}_+ - 4e_1 + 8n_+ + 8n_-,$$

a OPNS kuželosečka, která jimi prochází, má tvar 5-vektoru

$$\begin{aligned} Q_O = P_1 \wedge P_2 \wedge P_3 \wedge P_4 \wedge P_5 = &-86\bar{n}_+e_1e_2n_+n_- + 7\bar{n}_+e_1e_2n_+n_\times \\ &+ 469\bar{n}_+e_1e_2n_-n_\times - 20\bar{n}_+e_1n_+n_-n_\times + 27\bar{n}_+e_2n_+n_-n_\times + 3588e_1e_2n_+n_-n_\times. \end{aligned}$$

Konverze do IPNS reprezentace pomocí rovnic (2.7), (2.8) pak dává 1-vektor

$$Q_I = (Q_O)^* = -86\bar{n}_\times - 7\bar{n}_- + 469n_+ - 27e_1 - 20e_2 - 3588n_+$$

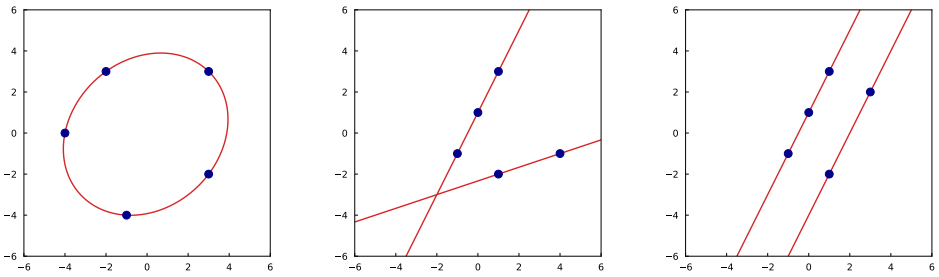
a po převodu do běžné rovnice dostáváme elipsu

$$Q : -231x^2 + 86xy - 238y^2 - 27x - 20y + 3588 = 0.$$

Pro větší stručnost uvádíme další ukázky této konstrukce kuželosečky z pěti bodů bez detailnějšího popisu výpočtu.

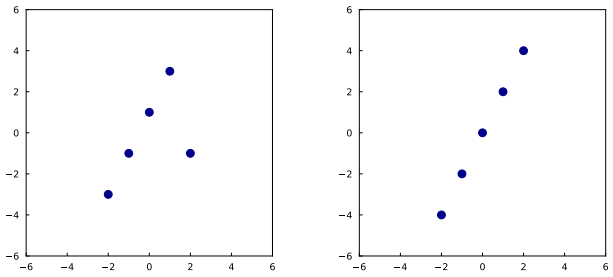
Případy, kdy jsou 3 body z 5 kolineární, jsou v témže Obrázku, v částech (b) a (c) – v obou případech jsme zkonstruovali kuželosečku, která je jednoznačně určená, ale je singulární; konkrétně dvojici přímek (jedna přímka z dvojice je určená třemi kolineárními body a druhá přímka zbylými dvěma body).

Pro úplnost uveďme také Obrázek 4, kde uvažujeme pětici bodů se 4, resp. s 5, kolineárními body – v obou případech by kuželosečka procházející všemi body musela být singulární (tedy dvojice přímek), ani v jednom z případů ale není určena jednoznačně, takže $P_1 \wedge P_2 \wedge P_3 \wedge P_4 \wedge P_5 = 0$. Důvod je tento: V podobrázku (a) jedna z přímek musí procházet 4 kolineárním body a druhá zbylým posledním bodem – směr tento přímky však může být jakýkoli. Podobný úsudek si lze vytvořit o podobrázku (b) – 5 kolineárními body musí jedna ze dvou přímek projít, druhá však může mít jakoukoli polohu i směr.



(a) 5 bodů v obecné lineární poloze **(b)** 3 kolineární body **(c)** 3 kolineární body

Obrázek 3. Kuželosečky procházející 5 vlastními body



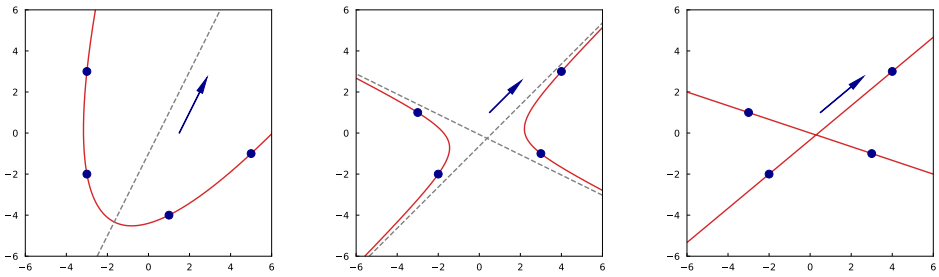
(a) 4 kolineární body **(b)** 5 kolineárních bodů

Obrázek 4. Pětice vlastních bodů se 4 a 5 kolineárními body. Kuželosečka procházející takovými množinami nemůže být určena jednoznačně.

Díky inkluzi nevlastních bodů do GAC navíc nemusíme jako body konstruované kuželosečky uvažovat jen vlastní body; vždyť některé kuželosečky, jako např. . parabola, hyperbola nebo dvojice přímek, obsahují jeden či více nevlastních bodů.

Příklad 3.2. Příklad takto nalezené paraboly je na Obrázku 5 (a) – parabola prochází 4 vlastními body a 1 nevlastním bodem, který představuje směr její osy. Zde také poznamenejme, že wedge 4 vlastních a 1 nevlastního bodu vytvoří parabolu pouze za zvláštních podmínek, [17]. To, že wedge 4 vlastních a 1 nevlastního bodu může snadno vytvořit i jiné kuželosečky, je evidentní na podobrázcích (b) a (c) – v prvním případě dostáváme hyperbolu, jejíž jedna asymptota vede použitým nevlastním bodem; v druhém případě vzniká dvojice přímek, z nichž má jedna směr nevlastního bodu a spojuje 2 ze 4 vlastních bodů (druhá přímka pak nutně spojuje poslední 2 zbývající body).

Ukázky wedge 2 a více nevlastních bodů s vlastními body lze najít v disertační práci [17].



(a) parabola **(b)** hyperbola **(c)** různoběžky

Obrázek 5. Kuželosečky procházející 4 vlastními a 1 nevlastním bodem

3.2. Čtyřbod a další bod

Připomeňme, že pomocí GAC se dá průnik dvou kuželoseček reprezentovat jako takzvaný *čtyřbod* ve tvaru (2.9). Protože čtyřbod je algebraicky ekvivalentní vnějšímu součinu čtyř individuálních bodů, lze ho také využít ke konstrukci kuželosečky procházející čtyřbodem a dalším bodem, který na průniku kuželoseček neleží. Velkou výhodou této reprezentace a konstrukce je, že takovou kuželosečku můžeme zkonstruovat, aniž bychom museli počítat polohu individuálních bodů průniku, a to podle následující věty, [17]:

Věta 3.3. *Nechť Q_I^1 a Q_I^2 jsou IPNS reprezentace dvou různých kuželoseček $Q^1, Q^2 \subset \mathbb{RP}^2$, a P_I je IPNS reprezentace bodu $p \in \mathbb{RP}^2$, který neleží na $Q^1 \cap Q^2$. Potom OPNS reprezentaci kuželosečky Q procházející průnikem $Q^1 \cap Q^2$ a bodem p lze vyjádřit jako*

$$Q_O = \left(Q_I^1 \wedge Q_I^2\right)^* \wedge P_I. \tag{3.1}$$

Příklad 3.4. Uvažujme dvě různé kuželosečky, konkrétně elipsu Q^1 a hyperbolu Q^2 s rovnicemi

$$Q^1\colon\ 9x^2 + 25y^2 - 225 = 0,$$
$$Q^2\colon\ 44x^2 - 64xy - 4y^2 - 112x + 136y - 31 = 0,$$

IPNS reprezentacemi

$$Q_I^1 = -34\bar{n}_+ + 16\bar{n}_- + 225n_+,$$
$$Q_I^2 = 64\bar{n}_\times - 48\bar{n}_- - 40\bar{n}_+ - 112e_1 + 136e_2 + 31n_+,$$

a dále uvažujme body $p_1 = (-2, -6)$ a $p_2 = (6, 2)$ s IPNS reprezentacemi

$$P_I^1 = C(p_1) = \bar{n}_+ - 2e_1 - 6e_2 + 20n_+ - 16n_- + 12n_\times,$$
$$P_I^2 = C(p_2) = \bar{n}_+ + 6e_1 + 2e_2 + 20n_+ + 16n_- + 12n_\times.$$

Následně můžeme udělat wedge čtyřbodu $Q_I^1 \wedge Q_I^2$ s body P_I^1, P_I^2 podle (3.1), čímž získáme OPNS kuželosečky C^1, C^2 jako

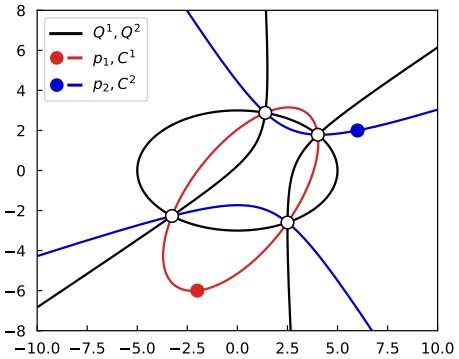
$$C_O^1 = \left(Q_I^1 \wedge Q_I^2\right)^* \wedge P_I^1$$

$$C_O^2 = \left(Q_I^1 \wedge Q_I^2\right)^* \wedge P_I^2.$$

Po konverzi do IPNS reprezentací dostáváme

$$C_I^1 = \left(C_O^1\right)^* = 2528\bar{n}_\times - 688\bar{n}_- - 4147\bar{n}_+ - 4424e_1 + 5372e_2 + 18212n_+,$$
$$C_I^2 = \left(C_O^2\right)^* = 6368\bar{n}_\times - 7728\bar{n}_- + 2293\bar{n}_+ - 11144e_1 + 13532e_2 - 38428n_+.$$

Výchozí situace a zkonstruované kuželosečky jsou k vidění na Obrázku 6.



Obrázek 6. Čtyřbod získaný jako průnik Q^1, Q^2 z Příkladu 3.4. Kuželosečky C^1a C^2 byly vytvořeny jako wedge čtyřbodu s bodem p_1, resp. p_2.

Předtím, než použijeme tento způsob konstrukce k získání speciálních kuželoseček, zmiňme pojem úzce spojený se čtyřbodem a průnikem kuželoseček – *svazek kuželoseček*, [27, 8].

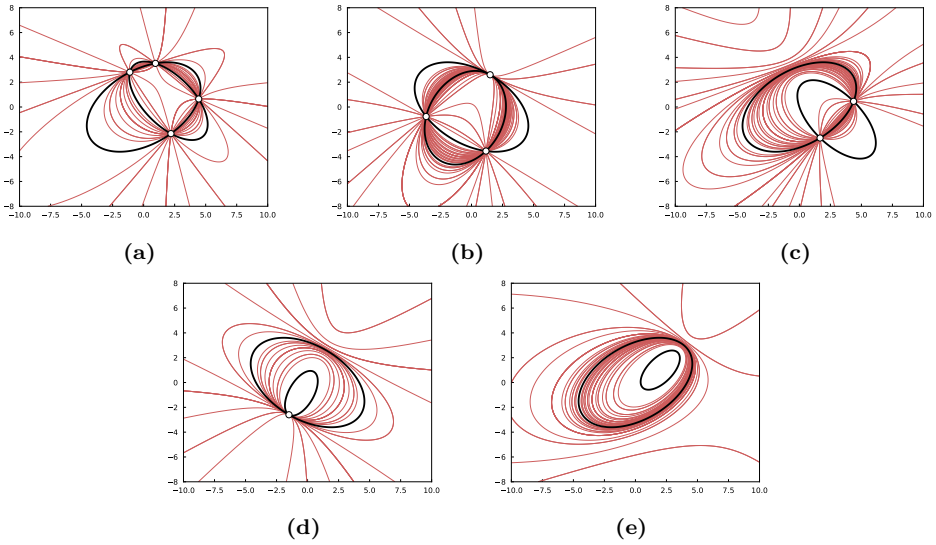
Definice 3.5. *Svazek kuželoseček* generovaný kuželosečkami Q^1 a Q^2 je množina všech kuželoseček procházejících skrz jejich společný průnik. Ekvivalentně se dá říct, že pokud jsou Q^1 a Q^2 reprezentovány rovnicemi $E_1 = 0$ a $E_2 = 0$, pak se dá svazek charakterizovat pomocí všech netriviálních lineárních kombinací rovnic $E_1 = 0$ a $E_2 = 0$, tedy

$$\{Q : \lambda E_1 + \mu E_2 = 0, \quad \lambda, \mu \in \mathbb{R}, (\lambda, \mu) \neq (0, 0)\}.$$

$E_1 = 0$ a $E_2 = 0$ jsou rovnice ve tvaru (2.11) nebo (2.12), a to podle toho, zda uvažujeme kuželosečky v $\mathbb{R}^2$ nebo v $\mathbb{RP}^2$.

Průsečíkům obou generujících kuželoseček se pak říká *základní body* (volný překlad anglického *„base points“*), [24, 27, 3].

Poznámka 3.6. Z algebraického pohledu mají dvě kuželosečky vždy čtyři průsečíky, ačkoli některé z nich mohou být algebraicky vícenásobné a ne všechny musí být reálné. Je důležité si uvědomit, že všechny kuželosečky svazku, který je generován kuželosečkami Q^1 a Q^2, procházejí všemi společnými průsečíky, a to i v případech, kdy nejsou všechny čtyři průsečíky reálné, zahrnujeme tedy i případy imaginárních průsečíků a navíc i průsečíky nevlastní. Příklad několika svazků kuželoseček s různým počtem reálných průsečíků lze vidět na Obrázku 7.



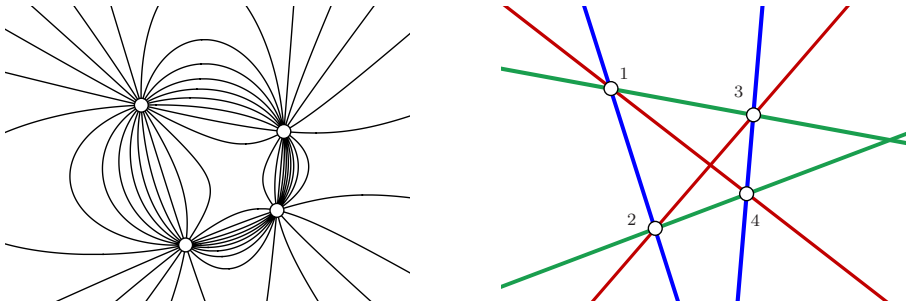
Obrázek 7. Svazky kuželoseček generované dvěma kuželosečkami. Případy 4 až 0 reálných průsečíků.

Se znalostí konceptu čtyřbodu a svazku kuželoseček můžeme tedy konstrukci kuželosečky pomocí vnějšího součinu čtyřbodu a dalšího bodu vnímat jako výběr jedné konkrétní kuželosečky ze svazku, která prochází jak čtyřbodem, tak zvoleným dalším bodem. V následujícím textu toho můžeme využít k nalezení geometricky významných kuželoseček, které se ve svazcích vyskytují.

3.2.1. Dvojice přímek ve svazku kuželoseček. Jednou z důležitých skupin kuželoseček vyskytujících se ve svazcích, je množina *singulárních kuželoseček*, která se skládá (až na speciální případy) z nejvýše tří *dvojic přímek*, jež procházejí všemi základními body svazku. Bod, kde se přímky z dané dvojice protínají, se pak nazývá *dvojitý bod* nebo *diagonální bod* (angl. *double point*, resp. *diagonal point*). Svazky tedy obvykle obsahují až tři dvojice přímek a odpovídající dvojité body. Vyobrazení svazku a jeho dvojic přímek lze vidět na Obrázku 8. Zdůrazněme ještě, že základní body, dvojité body a dvojice přímek svazku mohou být i imaginární, [27, 29, 8].

Jsou to právě dvojice přímek ve svazku, které se často používají k nalezení průsečíků dvou kuželoseček, [27, 2, 3]. Nejobvyklejším způsobem nalezení dvojic přímek ve svazku je využití faktu, že singulární kuželosečky jsou reprezentovány singulární maticí. Protože každá kuželosečka Q ze svazku generovaného kuželosečkami Q^1 a Q^2 může být vyjádřena jako lineární kombinace těchto kuželoseček, totéž platí i pro jejich maticové reprezentace. Jestliže tedy označíme matice kuželoseček Q^1 a Q^2 jako M_1 a M_2, pak maticí kuželosečky Q je $M = \lambda M_1 + \mu M_2$. Z toho plyne, že aby Q byla singulární, musí platit

$$\det(M) \equiv \det(\lambda M_1 + \mu M_2) = 0,$$



Obrázek 8. Svazek kuželoseček procházející čtyřmi základními body a jeho tři singulární kuželosečky, tj. dvojice přímek ([27])

což představuje kubickou rovnici v proměnných λ a μ. Jeden z algoritmů na řešení této rovnice je detailně popsaný v knize [27].

Nyní ale popišme i jiný – geometricky motivovaný – způsob nalezení dvojic přímek ve svazku: Protože každá dvojice přímek ve svazku prochází základními body svazku (reprezentovanými čtyřbodem) *a zároveň* svým dvojitým bodem, můžeme každou dvojici přímek zkonstruovat jako vnější součin čtyřbodu svazku a dvojitého bodu dané dvojice přímek.

I když je myšlenka takové konstrukce poměrně jednoduchá, nalezení dvojitých bodů svazku není zdaleka tak zřejmé. Naštěstí bylo ukázáno, že dvojité body svazku lze vypočítat pomocí tzv. *polarity* kuželoseček, [9].

Definice 3.7. Nechť Q je kuželosečka v $\mathbb{RP}^2$ reprezentovaná maticí M a $p = (x_p, y_p, z_p)^T$ je homogenní bod v $\mathbb{RP}^2$. Dále (zneužitím značení) ztotožněme homogenní přímku $l : ax + by + cz = 0$ s vektorem jejích koeficientů, tj. $l = (a, b, c)^T$. Potom se homogenní přímka $l = Mp$ nazývá *polára* bodu p vůči kuželosečce Q a bod p se nazývá *pól*, [27].

Definice 3.8. Nechť Q je kuželosečka a p_1, p_2, p_3 jsou tři homogenní body v $\mathbb{RP}^2$. Jestliže polára každého z těchto bodů prochází zbývajícím dvěma body, pak se trojúhelníku $\triangle p_1 p_2 p_3$ říká *autopolární trojúhelník*[4] kuželosečky Q, [9].

Dále, nechť Q^1 a Q^2 jsou dvě kuželosečky a p_1, p_2, p_3 jsou tři homogenní body v $\mathbb{RP}^2$. Jestliže body p_1, p_2, p_3 tvoří autopolární trojúhelník obou kuželoseček současně, trojúhelník se pak nazývá *společný autopolární trojúhelník* kuželoseček Q^1 a Q^2.

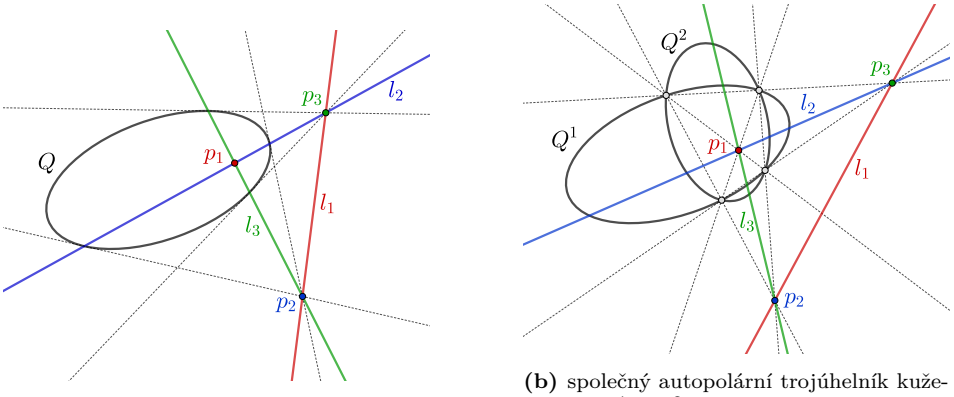
Věta 3.9. *Dvojité body svazku kuželoseček tvoří vrcholy společného autopolárního trojúhelníka generujících kuželoseček Q^1 a Q^2,* [28].

Díky autopolaritě dvojitých bodů svazku můžeme jejich výpočtu dosáhnout za pomocí následující věty:

[4]Anglický název pojmu je „*self-polar triangle*“; český ekvivalent se nepodařilo najít, proto volně překládáme „self-polar“ jako „autopolární“.

Věta 3.10. *Nechť Q^1 a Q^2 jsou generující kuželosečky svazku kuželoseček a M_1 a M_2 jsou jejich matice. Potom platí, že pokud společný autopolární trojúhelník kuželoseček Q^1 a Q^2 existuje, tak jeho vrcholy se dají vypočítat jako vlastní vektory p zobecněné úlohy vlastních čísel a vlastních vektorů*

$$M_1 p = \lambda M_2 p. \tag{3.2}$$



(a) autopolární trojúhelník kuželosečky Q

(b) společný autopolární trojúhelník kuželoseček Q^1 a Q^2

Obrázek 9. Autopolární trojúhelníky. (a) Přerušované přímky jsou tečny vedené z pólů ke kuželosečce (poláry protínají kuželosečku právě v bodech dotyku). (b) Přerušované čáry značí dvojice přímek ve svazku generovaném dvěma kuželosečkami.

Abychom nyní zkonstruovali dvojice přímek ve svazku generovaném kuželosečkami Q^1 a Q^2, vypočteme dvojité body svazku jako vlastní vektory úlohy (3.2) a vytvoříme vnější součin jejich GAC reprezentantů se čtyřbodem $Q^1 \wedge Q^2$ jako v rovnici (3.1). Jinými slovy, OPNS reprezentaci i-té dvojice přímek svazku najdeme jako

$$LP_O^i = \left(Q_I^1 \wedge Q_I^2\right)^* \wedge C\mathbb{P}(p_i).$$

Příklad 3.11. Uvažujme dvě elipsy E^1, E^2 s rovnicemi

$$E^1\colon 9x^2 + 25y^2 - 225 = 0,$$
$$E^2\colon 4x^2 + y^2 - 16x - 2y + 1 = 0,$$

s IPNS reprezentacemi

$$E_I^1 = 16\bar{n}_- - 34\bar{n}_+ + 225n_+,$$
$$E_I^2 = -3\bar{n}_- - 5\bar{n}_+ - 16e_1 - 2e_2 - n_+,$$

a maticemi

$$M_1 = \begin{pmatrix} 9 & 0 & 0 \\ 0 & 25 & 0 \\ 0 & 0 & -225 \end{pmatrix}, \quad M_2 = \begin{pmatrix} 4 & 0 & -8 \\ 0 & 1 & -1 \\ -8 & -1 & 1 \end{pmatrix}.$$

Řešením zobecněného problému vlastních čísel a vlastních vektorů (3.2) pak dostáváme

$$\begin{pmatrix}\lambda_1\\ \lambda_2\\ \lambda_3\end{pmatrix} \approx \begin{pmatrix}13.0501\\ 21.6502\\ 2.7997\end{pmatrix}, \quad \begin{pmatrix}p_1 & p_2 & p_3\end{pmatrix} \approx \begin{pmatrix}2.4167 & 2.2320 & 10.1865\\ -1.0921 & -6.4631 & -0.1261\\ 1 & 1 & 1\end{pmatrix}$$

a IPNS reprezentace dvojitých bodů P_1, P_2, P_3 hledaných dvojic přímek spočítáme vnořením získaných vlastních vektorů do GAC, tedy

$$P_i = C\mathbb{P}(p_i), \qquad i = 1, 2, 3.$$

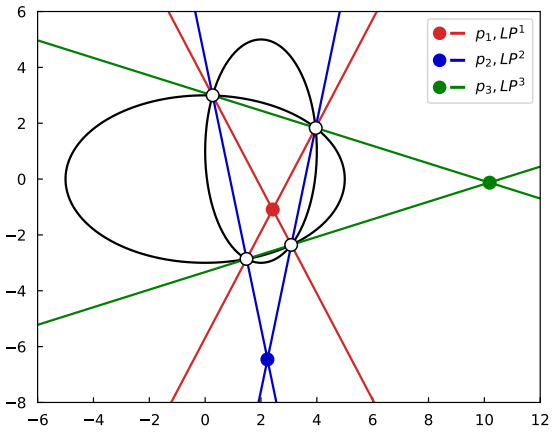
Nakonec získáváme každou dvojici přímek ve svazku podle konstrukce (3.1):

$$LP_O^i = \left(E_I^1 \wedge E_I^2\right)^* \wedge P_i, \qquad i = 1, 2, 3.$$

Po konverzi do IPNS reprezentací dostáváme dvojice přímek:

$$LP_I^1 \approx -6181.408\bar{n}_- + 5067.328\bar{n}_+ - 11348.626e_1 - 1418.578e_2 - 57712.203n_+,$$
$$LP_I^2 \approx 602.728\bar{n}_- + 341.532\bar{n}_+ + 2281.956e_1 + 285.245e_2 + 2601.605n_+,$$
$$LP_I^3 \approx -3231.034\bar{n}_- - 2963.629\bar{n}_+ - 13826.218e_1 - 1728.277e_2 - 9844.710n_+.$$

Obě generující kuželosečky svazku, jeho čtyřbod a nalezené dvojice přímek jsou k vidění na Obrázku 10.



Obrázek 10. Čtyřbod získaný jako průnik kuželoseček z Příkladu 3.11. Každá ze tří dvojic přímek byla získána jako vnější součin čtyřbodu a příslušného dvojitého bodu.

V některých úlohách může být pak hledání dvojic přímek obzvláště jednoduché, např. pokud jsou dvě generující kuželosečky soustředné, jak můžeme vidět v následujícím příkladu.

Příklad 3.12. Uvažujme dvě soustředné elipsy E^1, E^2 z Obrázku 11 (a). Protože obě jsou soustředné, je zřejmé, že jejich průsečíky (reprezentované čtyřbodem) jsou souměrné vůči společnému středu; jedna z hledaných dvojic přímek tedy musí procházet jak čtyřbodem, tak středem, který je v tomto případě bod $(0, 0, 1)$. Díky soustřednosti také platí, že zbývající dvojice přímek se skládají z rovnoběžek, a jejich dvojité body jsou tedy nevlastní. Ve zvoleném případě mají navíc obě generující elipsy osy rovnoběžné se souřadnými osami, tudíž i rovnoběžky dvojic přímek povedou rovnoběžně se souřadnými osami – nevlastní bod osy x lze zapsat jako $(1, 0, 0)$ a nevlastní bod osy y jako $(0, 1, 0)$. Díky takovému rozložení lze v tomto případě najít dvojice přímek generovaného svazku bez nutnosti počítat jakékoli vlastní vektory – konstrukce pomocí vnějšího součinu pak vypadá následovně:

$$\begin{aligned} LP_O^1 &= \left(E_I^1 \wedge E_I^2\right)^* \wedge C\mathbb{P}(0, 0, 1), \\ LP_O^2 &= \left(E_I^1 \wedge E_I^2\right)^* \wedge C\mathbb{P}(0, 1, 0), \\ LP_O^3 &= \left(E_I^1 \wedge E_I^2\right)^* \wedge C\mathbb{P}(1, 0, 0). \end{aligned}$$

Elipsy E^1, E^2 na Obrázku 11 (b) mají také společný střed $(0, 0, 1)$, jedna z elips je ale natočená o $30°$. Situace je skoro stejná jako předtím: Jedna z dvojic přímek půjde společným středem, a zbývající dvě dvojice budou tvořit rovnoběžky; tyto rovnoběžky už ale nepůjdou ve směrech souřadných os, ale jejich nevlastní body musí být spočítány pomocí úlohy (3.2). Výsledné vlastní vektory pak vycházejí jako

$$\begin{pmatrix} p_1 & p_2 & p_3 \end{pmatrix} \approx \begin{pmatrix} 0 & -0.2525 & 2.2281 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \end{pmatrix},$$

a konstrukce dvojic přímek je pak dána vztahy

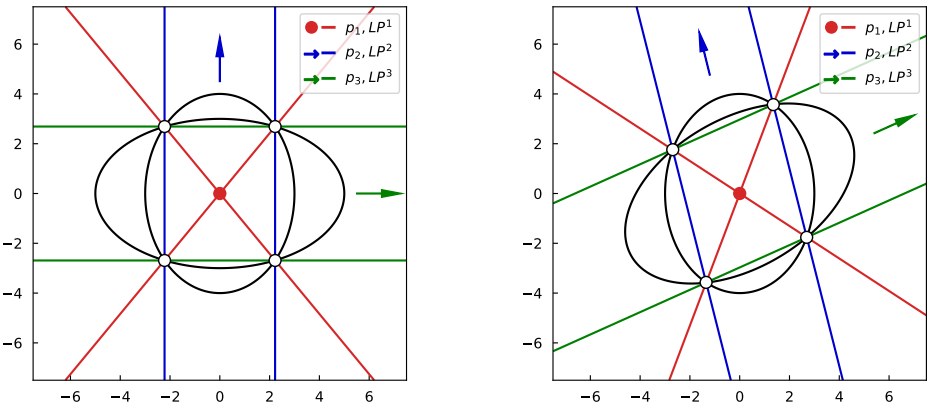
$$\begin{aligned} LP_O^1 &= \left(E_I^1 \wedge E_I^2\right)^* \wedge C\mathbb{P}(p_1), \\ LP_O^2 &= \left(E_I^1 \wedge E_I^2\right)^* \wedge C\mathbb{P}(p_2), \\ LP_O^3 &= \left(E_I^1 \wedge E_I^2\right)^* \wedge C\mathbb{P}(p_3). \end{aligned}$$

Poznámka 3.13. Na závěr podpodsekce poznamenejme, že konstrukce dvojic přímek demonstrovaným způsobem není možná pro některé ze svazků, jejíž generující kuželosečky jsou vůči sobě ve speciálních polohách; pro detaily viz [17].

3.2.2. Zobecněné paraboly ve svazcích kuželoseček. Další význačnou skupinou kuželoseček ve svazcích jsou tzv. *zobecněné paraboly*. Jak bude detailněji popsáno dále v textu, svazek kuželoseček může obsahovat právě žádnou, jednu, dvě, nebo (ve velice speciálních případech) nekonečné množství zobecněných parabol; nejobvyklejším případem ale budou dvě zobecněné paraboly, [17].

Připomeňme, že parabola je regulární, nestředová kuželosečka. Pokud je tedy reprezentována maticí M a hlavní podmaticí $\bar{M}$, platí

$$\det(M) \neq 0, \quad \det(\bar{M}) = 0.$$



Obrázek 11. Čtyřbod jako průsečík dvou soustředných kuželoseček z Příkladu 3.12. Jedna z vyobrazených dvojic přímek vznikla jako wedge čtyřbodu a společného středu kuželoseček, další dvojice pak jako wedge čtyřbodu s příslušným nevlastním bodem.

Na druhou stranu, stejně jako hyperbola jakožto regulární kuželosečka může „zdegenerovat“ v dvojici různoběžek (tedy kuželosečku singulární), tak může „zdegenerovat“ parabola, jmenovitě do dvojice rovnoběžek či jedné dvojnásobné přímky (tato dvojnásobná přímka navíc může být nevlastní). Když budeme tedy hledat paraboly ve svazcích kuželoseček, nebudeme se omezovat jen na paraboly v obvyklém smyslu slova, ale zahrneme všechny nestředové kuželosečky, a to jak regulární, tak singulární. Zobecněné paraboly jsou tedy všechny kuželosečky vyhovující vztahům

$$M \neq 0, \tag{3.3}$$

$$\det(\bar{M}) = 0. \tag{3.4}$$

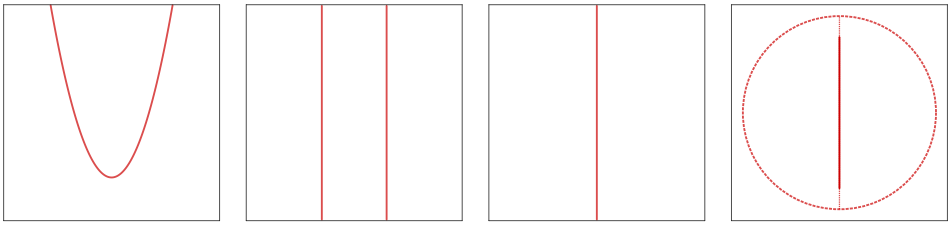
Kromě zmíněných zobecněných parabol navíc můžeme uvažovat i dvojici přímek, z nichž je jedna vlastní a druhá nevlastní, neboť taková dvojice také splňuje rovnosti (3.3) a (3.4).

Přehled všech typů zobecněných parabol lze vidět na Obrázku 12 (nevlastní přímka je v podobrázku (d) znázorněna jako přerušovaná kružnice, protože ji můžeme vnímat jako nekonečně velkou kružnici obepínající reálnou rovinu $\mathbb{R}^2$).

Jak bylo ukázáno v disertační práci [17], počet zobecněných parabol ve svazku generovaném kuželosečkami Q^1 a Q^2 lze jednoznačně určit na základě jejich matic a podmatic, a to podle následující věty.

Věta 3.14. *Uvažujme kuželosečky Q^1 a Q^2 reprezentované maticemi M_1 a M_2 tvaru* (2.10) *a hlavními podmaticemi $\bar{M}_1$ a $\bar{M}_2$ tvaru* (2.13). *Dále definujme matici*

$$N = \begin{pmatrix} \delta_1 & \gamma_{12} \\ \gamma_{12} & \delta_2 \end{pmatrix},$$



(a) parabola **(b)** dvě rovnoběžky **(c)** dvojnásobná přímka **(d)** sjednocení vlastní a nevlastní přímky

Obrázek 12. Typy zobecněných parabol

kde

$$\delta_1 = \det(\bar{M}_1),$$
$$\gamma_{12} = \frac{1}{2}\operatorname{tr}\left(\operatorname{adj}\left(\bar{M}_1\right)\bar{M}_2\right),$$
$$\delta_2 = \det(\bar{M}_2).$$

Potom počet zobecněných parabol ve svazku generovaném kuželosečkami Q^1 a Q^2 může být určen na základě matic M_1, M_2 a N podle přehledu v Tabulce 3.

Tabulka 3. Počet zobecněných parabol ve svazku generovaném kuželosečkami Q^1 a Q^2 s maticemi M_1 a M_2 podle jejich vztahu a vůči matici N. Označení případů zvýrazněno tučně. Případy se značkou „–“ nejsou algebraicky možné.

	$M_2 \neq kM_1$, $k \neq 0$	$M_2 = kM_1$, $k \neq 0$
$\det(N) < 0$	**A1** 2 reálné paraboly	**B1** –
$\det(N) = 0$, $N \neq 0$	**A2** 1 reálná parabola	**B2** žádná parabola
$\det(N) > 0$	**A3** žádná reálná parabola (2 imaginární paraboly)	**B3** –
$N = 0$	**A4** nekonečné množství různých reálných parabol	**B4** identické reálné paraboly Q^1 a Q^2

Díky klasifikaci možných případů můžeme nyní více diskutovat různé situace, které mohou při konstrukci zobecněných parabol ve svazcích nastat. Podobně jako v předchozím oddíle, i zde budeme křivky hledat jako wedge čtyřbodu $Q_I^1 \wedge Q_I^2$ a dalšího bodu. Každá zobecněná parabola (kromě těch, které obsahují nevlastní

přímku) prochází právě jedním nevlastním bodem, který je asociovaný se směrem osy zobecněné paraboly – z tohoto důvodu je přirozené konstruovat vnější součin čtyřbodu a právě tohoto nevlastního bodu. Jak bude zanedlouho ukázáno, způsob výpočtu nevlastních bodů zobecněných parabol má podobnou strukturu jako výpočet dvojitých bodů dvojic přímek. Tyto nevlastní body můžeme nalézt pomocí tzv. *sdružených průměrů* a *sdružených směrů*.

Definice 3.15. Přímce d se říká *průměr* kuželosečky Q, jestliže je polárou nějakého nevlastního bodu vůči kuželosečce Q. Ekvivalentně se dá říct, že průměr je jakákoliv přímka procházející středem kuželosečky.

Dvěma průměrům d_1 a d_2 kuželosečky Q se říká *sdružené*, jestliže oba průměry jsou polárou nevlastního bodu druhého průměru vůči Q.

Pokud jsou navíc průměry d_1 a d_2 sdružené vůči kuželosečkám Q^1 a Q^2 současně, říká se jim *společné sdružené průměry* kuželoseček Q^1 a Q^2, [10, 15].

Definice 3.16. Uvažujme kuželosečku Q a dva směry $\bar{p}_{\infty 1} = (x_{p_{\infty 1}}, y_{p_{\infty 1}})^T$ a $\bar{p}_{\infty 2} = (x_{p_{\infty 2}}, y_{p_{\infty 2}})^T$. Potom $\bar{p}_{\infty 1}$ a $\bar{p}_{\infty 2}$ se nazývají *sdružené směry* kuželosečky Q, jestliže jsou směry jejích sdružených průměrů.

Pokud jsou navíc směry $\bar{p}_{\infty 1}$ a $\bar{p}_{\infty 2}$ sdružené vůči kuželosečkám Q^1 a Q^2 současně, říká se jim *společné sdružené směry* kuželoseček Q^1 a Q^2, [17].

Lze ukázat, že svazek má (obvykle dva) sdružené směry společné *všem* kuželosečkám ve svazku, takže i generujícím kuželosečkám Q^1 a Q^2. Tyto směry jsou zároveň směry nevlastních bodů zobecněných parabol. Lze je – stejně jako dvojité body předtím – najít pomocí zobecněného problému vlastních čísel a vlastních vektorů podle následující věty, [17].

Věta 3.17. *Nechť Q^1 a Q^2 jsou generující kuželosečky svazku kuželoseček a $\bar{M}_1$ a $\bar{M}_2$ jsou jejich hlavní podmatice. Potom platí, že pokud společné sdružené směry kuželoseček Q^1 a Q^2 existují, tak se dají vypočítat jako vlastní vektory $\bar{p}_\infty$ zobecněné úlohy vlastních čísel a vlastních vektorů*

$$\bar{M}_1 \bar{p}_\infty = \lambda \bar{M}_2 \bar{p}_\infty. \tag{3.5}$$

Abychom nyní mohli zkonstruovat zobecněné paraboly ve svazku generovaném kuželosečkami Q^1 a Q^2, musíme nejdříve najít společné sdružené směry $\bar{p}_{\infty j}$ podle (3.5), přidáním nulové třetí souřadnice z nich vytvořit nevlastní body $p_{\infty j}$ a nakonec jejich GAC reprezentanty „vywedgovat“ se čtyřbodem $Q^1 \wedge Q^2$ jako v (3.1). Řečeno matematičtěji, OPNS reprezentaci j-té zobecněné paraboly P^j svazku můžeme najít jako

$$P_O^j = \left(Q_I^1 \wedge Q_I^2\right)^* \wedge C\mathbb{P}(p_{\infty j}). \tag{3.6}$$

Nyní demonstrujme konstrukci zobecněných parabol na konkrétních příkladech. Kvůli stručnosti textu uvádíme konstrukci detailně pouze u jednoho příkladu; konstrukce u dalších příkladů by byly analogické a jejich výsledek je v textu doprovozen obrázkem a alespoň stručným komentářem. Pro zevrubnější diskuzi příkladů viz [17].

Příklad 3.18. (1) Uvažujme E^1, E^2 s rovnicemi

$$E^1\colon\ -13x^2+8xy\sqrt{3}-21y^2+225=0,$$
$$E^2\colon\ -20x^2-24xy-20y^2+92x+68y+19=0,$$

s IPNS reprezentacemi

$$E^1_I=-8\sqrt{3}\bar{n}_\times-8\bar{n}_-+34\bar{n}_+-225n_+,$$
$$E^2_I=24\bar{n}_\times+40\bar{n}_++92e_1+68e_2-19n_+,$$

a hlavními podmaticemi

$$\bar{M}_1=\begin{pmatrix}-13 & 4\sqrt{3}\\ 4\sqrt{3} & -21\end{pmatrix},\quad \bar{M}_2=\begin{pmatrix}-20 & -12\\ -12 & -20\end{pmatrix}.$$

Řešení zobecněného problému vlastních čísel a vlastních vektorů (3.5) dává

$$\begin{pmatrix}\lambda_1\\ \lambda_2\end{pmatrix}\approx\begin{pmatrix}0.2916\\ 3.0142\end{pmatrix},\quad \begin{pmatrix}\bar{p}_{\infty 1} & \bar{p}_{\infty 2}\end{pmatrix}\approx\begin{pmatrix}1.4547 & -0.9115\\ 1 & 1\end{pmatrix},$$

IPNS reprezentace nevlastních bodů $p_{\infty 1}$ a $p_{\infty 2}$ asociovaných se směry $\bar{p}_{\infty 1}$ a $\bar{a}_{\infty 2}$ os hledaných zobecněných parabol je jejich vnořením do GAC, tedy

$$P_{\infty j}=C\mathbb{P}(p_{\infty j}),\qquad j=1,2.$$

Zobecněné paraboly P^j jsou nakonec zkonstruovány pomocí wedge podle (3.1) jako

$$P^j_O=\left(E^1_I\wedge E^2_I\right)^*\wedge P_{\infty j},\qquad j=1,2.$$

Po konverzi do IPNS reprezentace dostáváme zobecněné paraboly ve tvarech

$$P^1_I\approx-20.2775\bar{n}_\times-7.7786\bar{n}_-+21.7183\bar{n}_+-26.0840e_1-19.2795e_2-213.3868n_+,$$
$$P^2_I\approx-12.7058\bar{n}_\times-1.1792\bar{n}_--12.7604\bar{n}_+-40.8760e_1-30.2127e_2-24.7243n_+.$$

Obě elipsy, čtyřbod a nalezené zobecněné paraboly se svými osovými směry lze vidět na Obrázku 13 (a).

Mimoto ještě poznamenejme, že tento příklad skutečně představuje případ A1 z klasifikace podle Tabulky 3, tj. dvě různé reálné paraboly ve svazku generovaném kuželosečkami Q^1 a Q^2. To se dá ukázat i algebraicky, protože elipsy E^1 a E^2 jsou zřejmě různé (takže jejich matice nejsou nenulovým násobkem té druhé) a matice N formy (3.14) je

$$N=\begin{pmatrix}225 & 340+48\sqrt{3}\\ 340+48\sqrt{3} & 256\end{pmatrix},$$

takže $\det(N)<0$. Kromě toho uveďme stručně i příklady případů A2, A3 a A4.

(2) Uvažujme dvě hyperboly H^1, H^2 z Obrázku 13 (b). Tyto hyperboly se vyznačují tím, že mají obě jeden společný nevlastní bod, který je zároveň nevlastním bodem $p_{\infty 1}$ jediné paraboly ze svazku, který tyto hyperboly generují. V tomto svazku se tedy nachází pouze jedna reálná parabola, která ale nemůže být výše

popsaným způsobem zkonstruovaná, protože obě hyperboly se protínají ve společném nevlastním bodě, který splývá s bodem $p_{\infty 1}$; platí tedy $\left(H_I^1 \wedge H_I^2\right)^* \wedge P_{\infty 1} = 0$. Další výpočet by potvrdil, že se jedná o případ A2.

(3) Uvažujme dvě hyperboly H^1, H^2 z Obrázku 13 (c). Tyto kuželosečky se protínají ve čtyřech reálných bodech, které ale dohromady tvoří nekonvexní čtyřúhelník, a snadno tedy nahlédneme, že skrze tyto čtyři body nelze proložit žádnou reálnou parabolu. Výpočet by v této konfiguraci vyústil ve dvě imaginární paraboly, tedy případ A3.

(4) Nakonec prozkoumejme ještě svazek generovaný parabolami Q^1, Q^2 na Obrázku 13 (d), které mají rovnoběžné osy – v takovém případě svazek obsahuje nekonečné množství zobecněných parabol. Zajímavé také je, že zobecněnému problému (3.5) může odpovídat jakýkoliv nenulový vlastní vektor. Pokusíme-li se o konstrukci zobecněné paraboly pomocí nevlastního bodu $p_{\infty 1}$, který je asociovaný se směrem osy y, pak konstrukce selže, protože je to zároveň nevlastní průsečík obou parabol, takže $\left(Q_I^1 \wedge Q_I^2\right)^* \wedge P_{\infty 1} = 0$. Na druhou stranu, pokud utvoříme vnější součin čtyřbodu s jakýmkoli jiným nevlastním bodem, dostaneme zobecněnou parabolu, která se skládá z jedné vlastní přímky (spojující vlastní průsečíky obou parabol) a nevlastní přímky. Lze ukázat, že jde o případ A4.

Aby příklady k možným případům z Tabulky 3 byly kompletní, ukažme ještě B2 a B4.

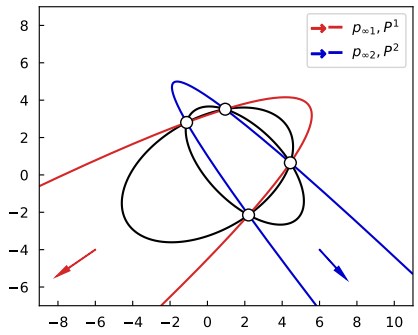
Příklad 3.19. (1) Uvažujme dvě hyperboly H^1, H^2 z Obrázku 14 (a), jejichž rovnice se liší pouze v násobku, takže představují obě stejnou hyperbolu. V této speciální situaci se svazek skládá jen z hyperboly samotné, takže svazek neobsahuje žádnou zobecněnou parabolu a jedná se o případ B2.

(2) Nechť P^1, P^2 jsou geometricky shodné paraboly z Obrázku 14 (b), jejichž rovnice se taktéž liší jen násobkem. V tomto případě se svazek skládá jen z paraboly samotné, která je jedinou zobecněnou parabolou svazku, a není tedy potřeba žádnou parabolu konstruovat (případ B4).

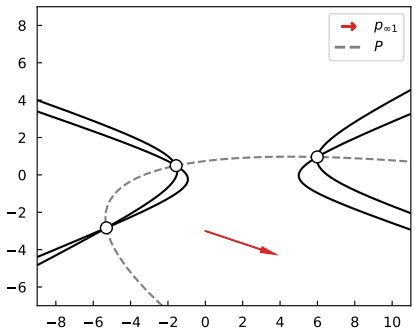
Protože konstrukce zobecněných parabol se ukazuje jako zvláště užitečná a elegantní v případech A1 (tedy, když jsou ve svazku právě dvě různé reálné paraboly), uveďme na závěr pár dalších příkladů této kategorie.

Příklad 3.20. (1) Ukažme si dva příklady, ve kterých oba páry kuželoseček mají čtyři různé průsečíky (Obrázek 15 (a,b)). V prvním se kuželosečky protínají ve dvou reálných a imaginárních bodech, i tak se ale pomocí našeho postupu podařilo spočítat osové směry i příslušné paraboly generovaného svazku. Druhý případ je překvapivější – kuželosečky nemají žádné reálné průsečíky (všechny čtyři jsou imaginární), i tak se ale povedlo zkonstruovat dvě paraboly generovaného svazku.

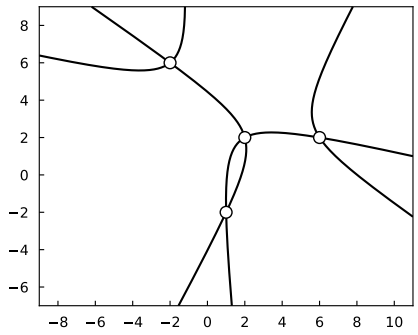
(2) Uvažujme ještě čtyři další příklady, ve kterých jsou generující kuželosečky vůči sobě ve speciálních polohách (Obrázek 15 (c)–(f)). Ve všech případech je alespoň jeden z průsečíků vícenásobným bodem dotyku, konstrukce parabol svazku



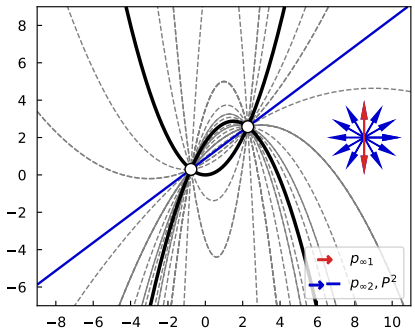
(a) A1 – dvě různé reálné paraboly



(b) A2 – jedna reálná parabola



(c) A3 – žádná reálná parabola (dvě různé imaginární paraboly)



(d) A4 – nekonečné množství reálných parabol (svazek obsahuje jen zobecněné paraboly)

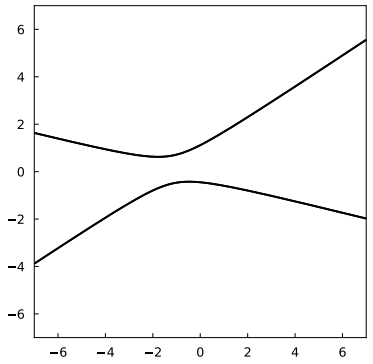
Obrázek 13. Kuželosečky z Příkladu 3.18, jejich průsečíky a paraboly generovaného svazku. Přerušované paraboly nelze námi popsanou konstrukcí (3.6) sestrojit.

byla ale všude úspěšná. Jak je vidět na obrázcích, kromě běžných parabol se v takových situacích můžeme setkat i s parabolami v obecnějším smyslu, jako jsou rovnoběžky nebo dvojnásobná přímka.

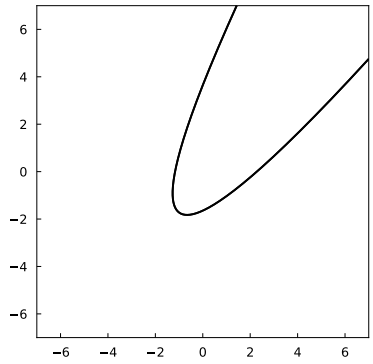
Výpočet matice N by potvrdil, že všechny tyto příklady skutečně spadají do kategorie A1, tedy dvě různé reálné paraboly ve svazku.

Poznámka 3.21. Jestliže byly nějaké konstrukce parabol uvažovány v příbuzné literatuře, obvykle se zabývaly konstrukcí paraboly skrz čtyři vlastní body. Pravděpodobně prvním, kdo se takovou konstrukcí zabýval, byl Isaac Newton v díle *Arithmetica Universalis*, [23], kde představil geometrický způsob nalezení směrů os parabol, které skrz čtyři vlastní body vedou.

Tento problém byl pak znovu diskutován v [5], kde kromě zopakování Newtonova přístupu bylo také ukázáno, že tyto paraboly jsou až na výjimky právě dvě.



(a) B2 – žádné paraboly ve svazku



(b) B4 – Q^1 a Q^2 jsou vzájemně identické a jsou jedinou parabolou ve svazku

Obrázek 14. Kuželosečky z Příkladu 3.19 a jimi generované svazky. Vyobrazené kuželosečky Q^1 a Q^2 jsou geometricky identické, takže generují pouze samy sebe a jsou jedinou kuželosečkou ve svazku.

Explicitní výpočet rovnic parabol skrz čtyři body byl pak uveden v [21], kde se problém studoval s ohledem na konvexitu čtyřúhelníku tvořeného těmito body.

Všechny zmíněné zdroje mají však společné to, že ke konstrukci parabol používaly známé body a nijak nezkoumaly (zobecněné) paraboly, které se vyskytují ve svazcích kuželoseček a které přirozeně se čtyřbodem souvisí. Snad jediný zdroj, který se tématu lehce dotkl, je kniha [8], ve které byl nějaký příklad parabol ve svazku prezentován. Jedním z cílů článku bylo tedy také seznámit čtenáře se zobecněnými parabolami jako s něčím, čemu se doposud nedostalo náležité pozornosti.

Reference

[1] R. Abłamowicz, R. Fauser: *Mathematics of Clifford - a Maple package for Clifford and Graßmann algebras,* Advances in Applied Clifford Algebras **15.2** (2005), 157–181.

[2] R. Byrtus, A. Derevianko, P. Vašík, D. Hildenbrand, C. Steinmetz: *On specific Conic intersections in GAC and symbolic calculations in GAALOPWeb*, Advances in Applied Clifford Algebras **32.2** (2022).

[3] C. Chomicki, S. Breuils, V. Biri, V. Nozick: *Intersection of Conic Sections Using Geometric Algebra*, Advances in Computer Graphics (2024), 175–187.

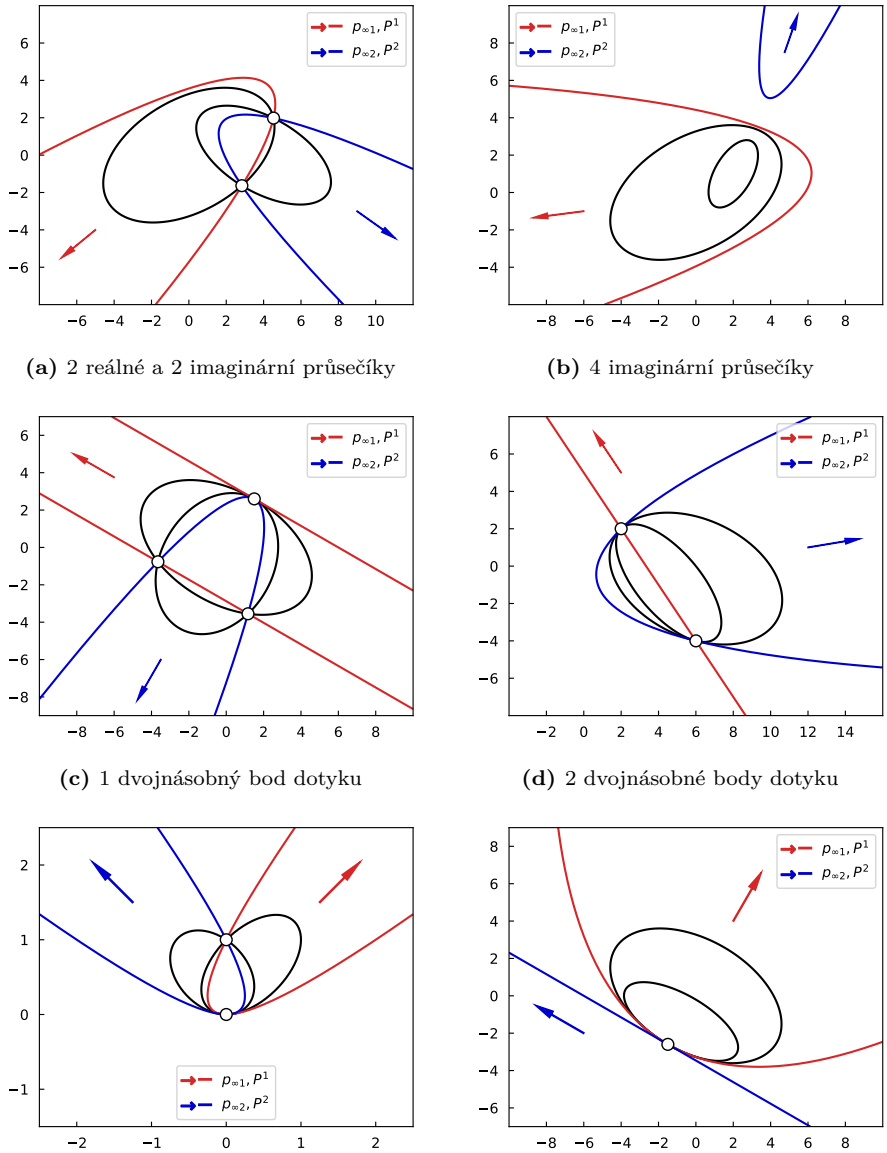
[4] C. Doignon, M. De Mathelin: *A Degenerate Conic-Based Method for a Direct Fitting and 3-D Pose of Cylinders with a Single Perspective View,* Proceedings 2007 IEEE International Conference on Robotics and Automation (2007), 4220-4225.

[5] H. Dorrie: *100 Great Problems of Elementary Mathematics*, Mineola, 1965.

[6] J. W. Downs: *Practical conic sections: the geometric properties of ellipses, parabolas and hyperbolas,* Mineola, 2003.

[7] C. G. Gibson: *Elementary Geometry of Algebraic Curves: An Undergraduate Introduction*, Cambridge 1999.

[8] G. Glaeser, H. Stachel, B. Odehnal: *The Universe of Conics: From the ancient Greeks to 21st century developments*, Heidelberg, 2024.



(a) 2 reálné a 2 imaginární průsečíky

(b) 4 imaginární průsečíky

(c) 1 dvojnásobný bod dotyku

(d) 2 dvojnásobné body dotyku

(e) 1 trojnásobný bod dotyku

(f) 1 čtyřnásobný bod dotyku

Obrázek 15. Kuželosečky z Příkladu 3.20 v různých vzájemných polohách. Zobecněné paraboly generovaných svazků.

[9] Y. Guo: *Homography Estimation from Ellipse Correspondences Based on the Common Self-polar Triangle,* Journal of Mathematical Imaging and Vision **62** (2020), 169-188.
[10] G. B. Halsted: *Synthetic Projective Geometry*, Hoboken, 1906.
[11] R. Hartley, A. Zisserman: *Multiple view geometry in computer vision*, Cambridge, 2000.
[12] J. Hrdina, A. Návrat, P. Vašík: *Geometric algebra for Conics*, Advances in Applied Clifford Algebras **28.66** (2018).
[13] J. Hrdina, A. Návrat, P. Vašík: *Conic fitting in geometric algebra setting*, Advances in Applied Clifford Algebras **29.72** (2019).
[14] H. Huang: *The common self-polar triangle of conics and its applications to computer vision*, disertační práce, 2017.
[15] J. Janyška, A. Sekaninová: *Analytická teorie kuželoseček a kvadrik*, Brno, 2001
[16] G. A. Korn: *Mathematical handbook for scientists and engineers*, Mineola, 1961.
[17] P. Loučka: *Algorithms for Conics in Geometric Algebras*, disertační práce, 2024.
[18] P. Loučka: *On Proper and Improper Points in Geometric Algebra for Conics and Conic Fitting Through Given Waypoints*, Lecture Notes in Computer Science (2023), 67–79.
[19] P. Loučka, P. Vašík: *Algorithms for Conic Fitting Through Given Proper and Improper Waypoints in Geometric Algebra for Conics*, Advances in Applied Clifford Algebras **34** (2024).
[20] P. Lounesto: *Clifford Algebras and Spinors*, Cambridge, 1997.
[21] K. R. McLean: *Conics and convexity*, The Mathematical Gazette **98.542** (2014), 266–272.
[22] X. Meng, Z. Hu: *A new easy camera calibration technique based on circular points*, Pattern Recognition **36.5** (2003), 1155–1164.
[23] I. Newton: *Arithmetica universalis: sive de compositione et resolutione arithmetica liber*, 1707.
[24] P. Pamfilos: *A Gallery of Conics by Five Elements*, Forum Geometricorum **14** (2014), 295–348.
[25] C. Perwass: *Geometric Algebra with Applications in Engineering*, Heidelberg, 2008.
[26] M. Rahayem, N. Werghi, J. Kjellander: *Best ellipse and cylinder parameters estimation from laser profile scan sections*, Optics and Lasers in Engineering **50.9** (2012), 1242–1259.
[27] J. Richter-Gebert: *Perspectives on Projective Geometry: A guided tour through real and complex geometry*, Heidelberg, 2011.
[28] J. Semple, G. Kneebone: *Algebraic Projective Geometry*, Oxford, 1952.
[29] A. Thomas: *Geometric Characterizations of the Cross Ratio in a Pencil of Conics* (preprint) (2020).

Pavel Loučka, Ústav matematiky, Fakulta strojního inženýrství, Vysoké učení technické v Brně, Technická 2, 61669 Brno, Česká republika,
e-mail: Pavel.Loucka@vutbr.cz

INVERZE MATIC NAD NEKOMUTATIVNÍMI OKRUHY POMOCÍ SCHUROVÝCH DOPLŇKŮ

ALŽBĚTA KOČENDOVÁ A MIROSLAV KUREŠ

Abstrakt. Je vysvětleno užití Schurových doplňků pro výpočet inverzní matice a uveden ilustrativní příklad pro matice nad okruhem racionálních kvaternionů s lichými jmenovateli.

1. Úvod

Článek lze chápat jako rozšiřující text pro kurs lineární algebry. Zabývá se metodou výpočtu inverzní matice, kterou lze použít pro nekomutativní tělesa, ale i nekomutativní okruhy. Lze ji samozřejmě použít i pro struktury komutativní. Jak je obvyklé, inverzní maticí pro čtvercovou matici A řádu n rozumíme matici A^{-1} splňující $AA^{-1} = A^{-1}A = I_n$.

Hlavní uplatnění vidíme pro inverzi kvaternionových matic nebo duálně kvaternionových matic, které mají aplikace v kinematice a v dalších oborech.

2. Nejběžnější metody výpočtu inverzní matice

2.1. Výpočet užitím adjungované matice

Začněme nejužívanější metodou uvedenou prakticky v každém učebním textu z lineární algebry či z algebry (viz například [4]). *Algebraickým doplňkem* A_{ij} prvku a_{ij} čtvercové matice A rozumíme determinant matice vzniklé z A vypuštěním i-tého řádku a j-tého sloupce násobený $(-1)^{i+j}$. Transponovaná matice z algebraických doplňků se nazývá *adjungovaná matice*, označíme ji $\operatorname{adj} A$ a máme tedy

$$\operatorname{adj} A = \begin{pmatrix} A_{11} & \dots & A_{n1} \\ \dots & \dots & \dots \\ A_{1n} & \dots & A_{nn} \end{pmatrix}.$$

Je-li A invertovatelná s deteminantem d, lze inverzní matici A^{-1} spočíst jako $\frac{1}{d}$-násobek $\operatorname{adj} A$.

Důkaz tohoto tvrzení není těžký, počítejme $A \cdot \operatorname{adj} A$. Diagonální prvky součinu jsou tvaru $\sum_{k=1}^{n} a_{ik}A_{ik}$, což není nic jiného než Laplaceův rozvoj podle i-tého řádku, a tedy diagonální prvky jsou rovny d. Nediagonální prvky součinu jsou

2020 *MSC.* Primární 15A09, 15B33.
Klíčová slova. Schurův doplněk, inverzní matice, nekomutativní okruh.
Práce byla podpořena projektem FSI-S-23-8161.

tvaru $\sum_{k=1}^{n} a_{jk}A_{ik}$, $j \neq i$, což lze opět chápat jako Laplaceův rozvoj podle i-tého řádku, kde hodnoty i-tého řádku byly nahrazeny hodnotami j-tého řádku, tedy j-tý řádek je v takové matici dvakrát a ta je tudíž singulární. Proto jsou nediagonální prvky rovny 0 a protože jsme zjistili, že $A \cdot \operatorname{adj} A = dI_n$, důkaz je tím hotov.

Pro nekomutativní okruhy je ale tento postup problematický, neboť je problematická už samotná definice determinantu. Už pro matici druhého řádu $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ nám nekomutativita násobení umožňuje čtyři zobecnění obvyklé definice determinantu, a sice $ad-bc$, $ad-cb$, $da-bc$ a $da-cb$. Pokud akceptujeme první možnost, $ad-bc$, můžeme si všimnout jevu, nad nímž se pozastavil už slavný Arthur Cayley (1821–1895): Matice se dvěma stejnými sloupci, tedy $\begin{pmatrix} a & a \\ b & b \end{pmatrix}$, bude mít determinant $ab - ab = 0$, zatímco matice se dvěma stejnými řádky $\begin{pmatrix} a & b \\ a & b \end{pmatrix}$ bude mít determinant $ab - ba$, což je při nekomutativním násobení obecně nenulové číslo.

2.2. Výpočet užitím Gaussovy-Jordanovy eliminace

Kvůli výše uvedeným potížím s deteminantem obraťme naši pozornost k další metodě. Inverzní matici lze najít tak, že provádíme řádkové úpravy matice $\left(A \mid I_n\right)$ typu $n \times 2n$ vzniklé tak, že k matici A zprava „přilepíme“ identickou matici I_n. Tyto řádkové úpravy provádíme takové, abychom v levé polovině obdélníkové matice obdrželi matici I_n, v pravé polovině pak bude A^{-1}, schematicky

$$\left(A \mid I_n\right) \sim \cdots \sim \left(I_n \mid A^{-1}\right).$$

Korektnost postupu je jasná: každá řádková úprava matice A představuje násobení matice A vhodnou regulární maticí zleva; pro posloupnost řádkových úprav A pak máme násobení matice A součinem takových regulárních matic, který označme P. V levé polovině $\left(A \mid I_n\right)$ tedy máme

$$PA = I_n,$$

v pravé polovině násobení maticí P dává

$$PI_n = A^{-1}.$$

Také tento postup nelze použít pro libovolný okruh. Existují totiž okruhy, kde invertovatelnou matici A nelze obdržet řádkovými ani sloupcovými úpravami z jednotkové matice (a pochopitelně ani I_n pak nelze obdržet úpravami z A). Příkladem je okruh $R = \mathbb{Z}[\theta] = \{x + y\theta; x, y \in \mathbb{Z}\}$ pro $\theta = \frac{1+\sqrt{-19}}{2}$ a matice

$$A = \begin{pmatrix} 3-\theta & 2+\theta \\ -3-2\theta & 5-2\theta \end{pmatrix}.$$

Tato matice má inverzi, kterou je $A^{-1} = \begin{pmatrix} 5-2\theta & -2-\theta \\ 3+2\theta & 3-\theta \end{pmatrix}$, ale neexistují řádkové ani sloupcové úpravy převádějící I_n na A nebo A na I_n. Uvedeným příkladem se jako první zabýval Paul Moritz Cohn (1924–2006), který jej zmiňuje ve svém

již zhruba šedesát let starém článku [1]. Důkaz neexistence řádkových či sloupcových úprav není triviální, vyžaduje jistou průpravu, ta je ovšem v článku popsána. Existují i jednodušší okruhy, nad kterými matice tohoto druhu existují: další podrobnosti k jejich existenci, zejména pro případ řádů imaginárních kvadratických polí, lze nalézt v [3].

3. Výpočet užitím Schurových doplňků

3.1. Popis metody

Budeme počítat inverzi ke čtvercové matici M. Tu si rozdělme na bloky takto:

$$M = \begin{pmatrix} A & B \\ C & D \end{pmatrix},$$

kde A je typu $m \times m$, B typu $m \times n$, C typu $n \times m$ a D typu $n \times n$. Je-li A invertovatelná, nazveme matici

$$A_s = D - CA^{-1}B \tag{3.1}$$

Schurův doplněk matice A v M.

Nyní můžeme M vyjádřit jako součin tří matic. Přesvědčme se násobením, že pro invertovatelné A je

$$M = \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} I_m & O \\ CA^{-1} & I_n \end{pmatrix} \begin{pmatrix} A & O \\ O & A_s \end{pmatrix} \begin{pmatrix} I_m & A^{-1}B \\ O & I_n \end{pmatrix}.$$

Přínosem tohoto vyjádření je, že teď můžeme invertovat postupně tři matice v součinu, a to v obráceném pořadí, tedy aplikujeme $(UVW)^{-1} = W^{-1}V^{-1}U^{-1}$. Je zřejmé, že první a třetí matice invertovatelné jsou a druhá je invertovatelná právě tehdy, když je invertovatelná matice A_s. V takovém případě tudíž dostaneme

$$M^{-1} = \begin{pmatrix} I_m & -A^{-1}B \\ O & I_n \end{pmatrix} \begin{pmatrix} A^{-1} & O \\ O & A_s^{-1} \end{pmatrix} \begin{pmatrix} I_m & O \\ -CA^{-1} & I_n \end{pmatrix}. \tag{3.2}$$

Uvědomme si, že postup nevykazuje nejednoznačnosti ani pro případ, že matice jsou nad nekomutativní strukturou, například nad kvaterniony. Pro komutativní případ pak snadno odvodíme další tvrzení, a sice

$$\det M = \det A \det A_s. \tag{3.3}$$

Ano, první a třetí matice mají přece determinant rovný 1, takže determinant M je součinem determinantů bloků prostřední matice, tedy $\det A$ a $\det A_s$. Pro nekomutativní případ ale takto zavedený determinant zůstává jen jednou z možností (stejně tak se nabízí součin $\det A_s \det A$), takže determinantu zavedenému vztahem (3.3) budeme říkat *Schurův determinant*. (V poněkud jiné situaci je tímto způsobem počítán determinant v článku [5].)

Vraťme se k inverzi matice. Algoritmus výpočtu bude prostý. Matici A budeme brát typu 1×1, pak půjde o jeden prvek v levém horním rohu (říkáme mu *pivot*), je-li jednotkou, existuje k němu prvek inverzní. Pokud jednotkou není, provedeme řádkové a/nebo sloupcové permutace tak, aby tento prvek jednotkou byl.

Nyní se otázka invertovatelnosti matice M převede na invertovatelnost matice A_s, jejíž řád je o jedničku nižší. Pro matici A_s proto postup zopakujeme a toto iterujeme tak dlouho, až se problém zredukuje na invertovatelnost matice prvního řádu, což už je triviální.

Pokud jsme přehodili řádky či sloupce proto, aby pivot byl jednotkou, vynásobili jsme matici jistými regulárními (tzv. *permutačními)* maticemi zleva nebo zprava. Tak jsme obdrželi novou matici

$$N = PMQ,$$

kde P a Q jsou permutační matice. Najdeme-li ovšem inverzi N^{-1}, pak $N^{-1} = (PMQ)^{-1} = Q^{-1}M^{-1}P^{-1}$ a odtud

$$M^{-1} = QN^{-1}P.$$

3.2. Okruh racionálních kvaternionů s lichými jmenovateli

Budeme uvažovat nekomutativní okruh racionálních kvaternionů s lichými jmenovateli [1], tj.

$$R = \{a + bi + cj + dk;\ a, b, c, d \text{ jsou racionální čísla s lichými jmenovateli,}$$
$$i^2 = j^2 = k^2 = -1, ij = -ji = k\}.$$

Vezměme libovolný prvek okruhu $q = a+bi+cj+dk$. Podívejme se, jaké podmínky musí splňovat čísla a, b, c, d, aby byl prvek q jednotkou okruhu R. To, že q je jednotkou znamená, že existuje prvek $q^{-1} = e + fi + gj + hk$ takový, že platí

$$qq^{-1} = q^{-1}q = 1.$$

Musí tedy platit

$$(a + bi + cj + dk)\,(e + fi + gj + hk) = 1.$$

Roznásobením dostáváme

$$\begin{aligned} ae + afi + agj + ahk + bei - bf + bgk - bhj \\ + cej - cfk - cg + chi + dek + dfj - dgi - dh = 1, \end{aligned}$$

což lze zapsat jako soustavu 4 rovnic pro 4 neznámé e, f, g, h.

$$\begin{aligned} ae - bf - cg - dh &= 1, \\ af + be + ch - dg &= 0, \\ ag - bh + ce + df &= 0, \\ ah + bg - cf + de &= 0. \end{aligned}$$

[1] volba tohoto okruhu pro ilustrační příklad má své dobré důvody: z pohledu aplikací je za nekomutativní okruh vhodné vzít kvaterniony, ale existence multiplikativní inverze pro všechny nenulové prvky, kterou mají kvaterniony nad $\mathbb{R}$ nebo nad $\mathbb{Q}$, mnohé usnadňuje: proto jsme vzali nekomutativní okruh, v němž multiplikativní inverze pro nenulové prvky obecně nemusí existovat; důležité je i to, že náš okruh R má jediný maximální (oboustranný) ideál

Řešení této soustavy je tvaru

$$\begin{aligned} e &= \frac{a}{a^2+b^2+c^2+d^2}, \quad f = \frac{-b}{a^2+b^2+c^2+d^2}, \\ g &= \frac{-c}{a^2+b^2+c^2+d^2}, \quad h = \frac{-d}{a^2+b^2+c^2+d^2}. \end{aligned} \tag{3.4}$$

a, b, c, d jsou racionální čísla tvaru $\frac{x}{y}$, kde y je liché číslo. Můžeme snadno ověřit, že také $q^{-1}q = 1$. [2]

Potřebujeme zjistit, za jakých podmínek budou čísla e, f, g, h stejného tvaru. Vyjádřeme jednotlivé koeficienty ve tvaru základních zlomků jako $a = \frac{x_1}{y_1}$, $b = \frac{x_2}{y_2}$, $c = \frac{x_3}{y_3}$, $d = \frac{x_4}{y_4}$ a dosaďme do (3.4). Dostáváme

$$\begin{aligned} e &= \frac{\frac{x_1}{y_1}}{\frac{x_1^2}{y_1^2}+\frac{x_2^2}{y_2^2}+\frac{x_3^2}{y_3^2}+\frac{x_4^2}{y_4^2}}, \quad f = \frac{-\frac{x_2}{y_2}}{\frac{x_1^2}{y_1^2}+\frac{x_2^2}{y_2^2}+\frac{x_3^2}{y_3^2}+\frac{x_4^2}{y_4^2}}, \\ g &= \frac{-\frac{x_3}{y_3}}{\frac{x_1^2}{y_1^2}+\frac{x_2^2}{y_2^2}+\frac{x_3^2}{y_3^2}+\frac{x_4^2}{y_4^2}}, \quad h = \frac{-\frac{x_4}{y_4}}{\frac{x_1^2}{y_1^2}+\frac{x_2^2}{y_2^2}+\frac{x_3^2}{y_3^2}+\frac{x_4^2}{y_4^2}}. \end{aligned}$$

Zjednodušme vyjádření e následovně:

$$\begin{aligned} e &= \frac{x_1}{y_1} \cdot \frac{y_1^2y_2^2y_3^2y_4^2}{x_1^2y_2^2y_3^2y_4^2+x_2^2y_1^2y_3^2y_4^2+x_3^2y_1^2y_2^2y_4^2+x_4^2y_1^2y_2^2y_3^2}, \\ e &= \frac{y_1^2y_2^2y_3^2y_4^2}{y_1} \cdot \frac{x_1}{x_1^2y_2^2y_3^2y_4^2+x_2^2y_1^2y_3^2y_4^2+x_3^2y_1^2y_2^2y_4^2+x_4^2y_1^2y_2^2y_3^2}. \end{aligned}$$

Z předpokladů víme, že hodnoty y_i, kde $i = 1, \ldots, 4$, jsou liché. Je tedy zřejmé, že čitatel i jmenovatel prvního zlomku jsou také liché. Parita čitatele i jmenovatele druhého zlomku závisí pouze na hodnotách x_i, kde $i = 1, \ldots, 4$. Jmenovatel je lichý právě tehdy, když je lichý počet jednotlivých x_i lichých. Ekvivalentně lze tuto podmínku formulovat tak, že jmenovatel je lichý právě tehdy, když je číslo $x_1 + x_2 + x_3 + x_4$ liché. Pokud je tento součet lichý, tak nezáleží na hodnotě čitatele druhého zlomku, tedy hodnotě x_1 a e bude ve tvaru $\frac{x}{y}$, kde y je liché číslo. Analogicky lze ukázat, že pokud je součet $x_1 + x_2 + x_3 + x_4$ lichý, tak také f, g, h budou ve tvaru $\frac{x}{y}$, kde y je liché číslo, tedy $q^{-1} \in R$. Jinými slovy pokud je součet $x_1 + x_2 + x_3 + x_4$ lichý, tak prvek q je jednotkou okruhu R. Pokud by byl součet $x_1 + x_2 + x_3 + x_4$ sudý a všechna x_i, kde $i = 1, \ldots, 4$, sudá mohl by nastat případ, kdy lze ve vyjádření e, f, g, h krátit a dosáhnout tak také lichého jmenovatele. Tento případ ale vyloučíme následujícími úvahami. Nejdříve vyloučíme případ, kdy je $q = 0$. Takový prvek zřejmě jednotkou není. Dále předpokládejme q nenulové. Nechť n je největší sudé číslo, které dělí všechna x_i, kde $i = 1, \ldots, 4$, pak každé x_i lze zapsat jako $x_i = nz_i$. Pak musí nutně být alespoň jedno z_i liché. Nechť je liché například z_1. Potom pro e platí

$$e = \frac{y_1^2y_2^2y_3^2y_4^2}{y_1} \cdot \frac{nz_1}{n^2\left(z_1^2y_2^2y_3^2y_4^2+z_2^2y_1^2y_3^2y_4^2+z_3^2y_1^2y_2^2y_4^2+z_4^2y_1^2y_2^2y_3^2\right)},$$

[2] tento výsledek je dobře známý: inverzní kvaternion lze spočíst pomocí konjugovaného kvaternionu; ve jmenovateli vidíme právě normu kvaternionu

$$e = \frac{y_1^2y_2^2y_3^2y_4^2z_1}{y_1} \cdot \frac{1}{n\,(z_1^2y_2^2y_3^2y_4^2 + z_2^2y_1^2y_3^2y_4^2 + z_3^2y_1^2y_2^2y_4^2 + z_4^2y_1^2y_2^2y_3^2)}.$$

Vidíme, že v čitateli jsou pouze lichá čísla, takže n ve jmenovateli nelze krátit a jmenovatel je tím pádem sudý. Tedy q^{-1} není prvek okruhu R, neboli q není jednotkou okruhu R. Analogicky to lze ukázat i pro liché z_2, z_3 nebo z_4. Celkově jsme odvodili:
Jednotky okruhu R jsou právě ty prvky $q = \frac{x_1}{y_1} + \frac{x_2}{y_2}i + \frac{x_3}{y_3}j + \frac{x_4}{y_4}k$, pro které platí, že součet $x_1 + x_2 + x_3 + x_4$ je lichý.

3.3. Ukázkový příklad

Mějme okruh $R = \{a + bi + cj + dk$; a, b, c, d jsou racionální čísla s lichými jmenovateli, $i^2 = j^2 = k^2 = -1$, $ij = -ji = k\}$. Dále mějme zadanou matici M_0. Vypočítejte inverzní matici k M_0, jestliže

$$M_0 = \begin{pmatrix} \frac{2}{3}k & 0 & 2i & 1 \\ \frac{1}{3} + \frac{2}{3}i + \frac{1}{3}j + k & 0 & 0 & 3j \\ \frac{1}{3}j & 0 & 1 & j \\ \frac{4}{5}i + \frac{1}{5}k & \frac{3}{5} & 2i & \frac{2}{3}j + k \end{pmatrix}.$$

Pro použití algoritmu potřebujeme mít jako pivota jednotku. $\frac{2}{3}k$ není jednotka. V prvním řádku ve čtvrtém sloupci je prvek, který ovšem jednotkou je. Provedeme tedy takovou permutaci, ve které prohodíme první a čtvrtý sloupec. Tím získáme matici která má pivota jednotku. Vezměme permutační matice

$$P_1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad Q_1 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

Potom dostáváme

$$M_1 = P_1M_0Q_1 = \begin{pmatrix} 1 & 0 & 2i & \frac{2}{3}k \\ 3j & 0 & 0 & \frac{1}{3} + \frac{2}{3}i + \frac{1}{3}j + k \\ j & 0 & 1 & \frac{1}{3}j \\ \frac{2}{3}j + k & \frac{3}{5} & 2i & \frac{4}{5}i + \frac{1}{5}k \end{pmatrix}.$$

Na matici M_1 lze použít algoritmus a vypočítat příslušný Schurův doplněk A_{s1}. K tomu je potřeba rozdělit matici do bloků následujícím způsobem

$$M_1 = \left(\begin{array}{c|ccc} 1 & 0 & 2i & \frac{2}{3}k \\ \hline 3j & 0 & 0 & \frac{1}{3} + \frac{2}{3}i + \frac{1}{3}j + k \\ j & 0 & 1 & \frac{1}{3}j \\ \frac{2}{3}j + k & \frac{3}{5} & 2i & \frac{4}{5}i + \frac{1}{5}k \end{array}\right).$$

Dostáváme tedy submatice

$$A_1 = \begin{pmatrix} 1 \end{pmatrix}, \qquad B_1 = \begin{pmatrix} 0 & 2i & \frac{2}{3}k \end{pmatrix}, \qquad C_1 = \begin{pmatrix} 3j \\ j \\ \frac{2}{3}j + k \end{pmatrix},$$

$$D_1 = \begin{pmatrix} 0 & 0 & \frac{1}{3} + \frac{2}{3}i + \frac{1}{3}j + k \\ 0 & 1 & \frac{1}{3}j \\ \frac{3}{5} & 2i & \frac{4}{5}i + \frac{1}{5}k \end{pmatrix}.$$

Díky provedenému blokovému rozdělení matice M_1 lze snadno spočítat inverzní matici k jednoprvkové matici A_1. Tedy

$$A_1^{-1} = \begin{pmatrix} 1 \end{pmatrix}.$$

Následně lze dosadit do vztahu (3.1) pro výpočet Schurova doplňku,

$$A_{s1} = D_1 - C_1 A_1^{-1} B_1 = \begin{pmatrix} 0 & 6k & \frac{1}{3} - \frac{4}{3}i + \frac{1}{3}j + k \\ 0 & 1 + 2k & -\frac{2}{3}i + \frac{1}{3}j \\ \frac{3}{5} & 2i - 2j + \frac{4}{3}k & \frac{2}{3} + \frac{16}{45}i + \frac{1}{5}k \end{pmatrix}.$$

Pro výpočet M_1^{-1} pomocí vztahu (3.2) je nutné znát A_{s1}^{-1}. Pro výpočet této inverzní matice použijeme stejný postup jako pro výpočet M_1^{-1}. V matici A_{s1} vidíme jednotku v prvním řádku ve třetím sloupci. Vezmeme tedy permutační matice

$$P_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad Q_2 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}.$$

Pak dostáváme

$$M_2 = P_2 A_{s1} Q_2 = \begin{pmatrix} \frac{1}{3} - \frac{4}{3}i + \frac{1}{3}j + k & 6k & 0 \\ -\frac{2}{3}i + \frac{1}{3}j & 1 + 2k & 0 \\ \frac{2}{3} + \frac{16}{45}i + \frac{1}{5}k & 2i - 2j + \frac{4}{3}k & \frac{3}{5} \end{pmatrix}.$$

Matici opět rozdělíme do bloků tak, aby byl pivot v jednoprvkové matici, tedy

$$M_2 = \left(\begin{array}{c|cc} \frac{1}{3} - \frac{4}{3}i + \frac{1}{3}j + k & 6k & 0 \\ \hline -\frac{2}{3}i + \frac{1}{3}j & 1 + 2k & 0 \\ \frac{2}{3} + \frac{16}{45}i + \frac{1}{5}k & 2i - 2j + \frac{4}{3}k & \frac{3}{5} \end{array}\right).$$

Dostáváme submatice

$$A_2 = \begin{pmatrix} \frac{1}{3} - \frac{4}{3}i + \frac{1}{3}j + k \end{pmatrix}, \qquad B_2 = \begin{pmatrix} 6k & 0 \end{pmatrix}, \qquad C_2 = \begin{pmatrix} -\frac{2}{3}i + \frac{1}{3}j \\ \frac{2}{3} + \frac{16}{45}i + \frac{1}{5}k \end{pmatrix},$$

$$D_2 = \begin{pmatrix} 1 + 2k & 0 \\ 2i - 2j + \frac{4}{3}k & \frac{3}{5}. \end{pmatrix}.$$

Pro matici A_2^{-1} platí

$$A_2^{-1} = \left(\tfrac{1}{9} + \tfrac{4}{9}i - \tfrac{1}{9}j, -\tfrac{1}{3}k\right).$$

Spočítejme Schurův doplněk k matici M_2.

$$A_{s2} = D_2 - C_2 A_2^{-1} B_2 = \begin{pmatrix} \frac{5}{9} + \frac{10}{9}i - \frac{10}{9}j & 0 \\ -\frac{194}{135} + \frac{6}{5}i + \frac{4}{27}j + \frac{194}{135}k & \frac{3}{5} \end{pmatrix}.$$

Pro výpočet M_2^{-1} je potřeba znát A_{s2}^{-1}. K výpočtu A_{s2}^{-1} opět použijeme stejný postup. V matici A_{s2} je pivotem jednotka, takže není potřeba provádět permutace, tedy

$$M_3 = A_{s2}.$$

Matici M_3 rozdělíme do bloků

$$M_3 = \left(\begin{array}{c|c} \frac{5}{9} + \frac{10}{9}i - \frac{10}{9}j & 0 \\ \hline -\frac{194}{135} + \frac{6}{5}i + \frac{4}{27}j + \frac{194}{135}k & \frac{3}{5} \end{array}\right).$$

Dostáváme submatice

$$A_3 = \left(\tfrac{5}{9} + \tfrac{10}{9}i - \tfrac{10}{9}j\right), \qquad B_3 = \left(0\right), \qquad C_3 = \left(-\tfrac{194}{135} + \tfrac{6}{5}i + \tfrac{4}{27}j + \tfrac{194}{135}k\right),$$
$$D_3 = \left(\tfrac{3}{5}\right).$$

Inverzní matice k matici A_3 je

$$A_3^{-1} = \left(\tfrac{1}{5} - \tfrac{2}{5}i + \tfrac{2}{5}j\right).$$

Schurův doplněk k matici M_3 je

$$A_{s3} = D_3 - C_3 A_3^{-1} B_3 = \left(\tfrac{3}{5}\right).$$

K jednoprvkové matici A_{s3} vypočítáme inverzní matici snadno jako

$$A_{s3}^{-1} = \left(\tfrac{5}{3}\right).$$

Hodnotu A_{s3}^{-1} lze dosadit do vztahu (3.2) a tím získáme hodnotu M_3^{-1}.

$$M_3^{-1} = \begin{pmatrix} I_1 & -A_3^{-1}B_3 \\ 0 & I_1 \end{pmatrix} \begin{pmatrix} A_3^{-1} & 0 \\ 0 & A_{s3}^{-1} \end{pmatrix} \begin{pmatrix} I_1 & 0 \\ -C_3 A_3^{-1} & I_1 \end{pmatrix}$$
$$= \begin{pmatrix} \frac{1}{5} - \frac{2}{5}i + \frac{2}{5}j & 0 \\ -\frac{2}{9} - \frac{2}{5}i + \frac{28}{15}j - \frac{62}{45}k & \frac{5}{3} \end{pmatrix}.$$

Jelikož $A_{s2} = M_3$, platí také $A_{s2}^{-1} = M_3^{-1}$. Opět využijeme vztah (3.2) a vypočítáme

$$M_2^{-1} = \begin{pmatrix} I_1 & -A_2^{-1}B_2 \\ 0 & I_2 \end{pmatrix} \begin{pmatrix} A_2^{-1} & 0 \\ 0 & A_{s2}^{-1} \end{pmatrix} \begin{pmatrix} I_1 & 0 \\ -C_2 A_2^{-1} & I_2 \end{pmatrix},$$

odkud

$$M_2^{-1} = \begin{pmatrix} \frac{1}{5} - \frac{2}{5}i - \frac{1}{5}j - \frac{3}{5}k & -\frac{6}{5} + \frac{6}{5}i + \frac{6}{5}k & 0 \\ -\frac{1}{15} + \frac{1}{5}i - \frac{1}{15}j - \frac{2}{15}k & \frac{1}{5} - \frac{2}{5}i + \frac{2}{5}j & 0 \\ -\frac{1}{15} - \frac{1}{9}i - \frac{10}{9}j + \frac{19}{45}k & -\frac{2}{9} - \frac{2}{5}i + \frac{28}{15}j - \frac{62}{45}k & \frac{5}{3} \end{pmatrix}.$$

Následujícími úpravami získáme vztah pro hodnotu A_{s1}^{-1}:

$$\begin{aligned} M_2 &= P_2 A_{s1} Q_2, \\ M_2^{-1} &= (P_2 A_{s1} Q_2)^{-1}, \\ M_2^{-1} &= Q_2^{-1} A_{s1}^{-1} P_2^{-1}, \\ A_{s1}^{-1} &= Q_2 M_2^{-1} P_2. \end{aligned}$$

Dosazením dostáváme

$$A_{s1}^{-1} = \begin{pmatrix} -\frac{1}{15} - \frac{1}{9}i - \frac{10}{9}j + \frac{19}{45}k & -\frac{2}{9} - \frac{2}{5}i + \frac{28}{15}j - \frac{62}{45}k & \frac{5}{3} \\ -\frac{1}{15} + \frac{1}{5}i - \frac{1}{15}j - \frac{2}{15}k & \frac{1}{5} - \frac{2}{5}i + \frac{2}{5}j & 0 \\ \frac{1}{5} - \frac{2}{5}i - \frac{1}{5}j - \frac{3}{5}k & -\frac{6}{5} + \frac{6}{5}i + \frac{6}{5}k & 0 \end{pmatrix}.$$

Nyní využijeme vztah (3.2) pro výpočet hodnoty M_1^{-1}:

$$M_1^{-1} = \begin{pmatrix} I_1 & -A_1^{-1}B_1 \\ 0 & I_3 \end{pmatrix} \begin{pmatrix} A_1^{-1} & 0 \\ 0 & A_{s1}^{-1} \end{pmatrix} \begin{pmatrix} I_1 & 0 \\ -C_1 A_1^{-1} & I_3 \end{pmatrix}$$

$$= \begin{pmatrix} \frac{1}{5} + \frac{2}{5}k & 0 & -\frac{2}{5}i - \frac{4}{5}j & 0 \\ -\frac{22}{15} - \frac{1}{9}i - \frac{31}{45}j - \frac{14}{15}k & -\frac{1}{15} - \frac{1}{9}i - \frac{10}{9}j + \frac{19}{45}k & -\frac{2}{9} - \frac{2}{5}i + \frac{28}{15}j - \frac{62}{45}k & \frac{5}{3} \\ \frac{1}{5} - \frac{2}{5}i - \frac{1}{5}k & -\frac{1}{15} + \frac{1}{5}i - \frac{1}{15}j - \frac{2}{15}k & \frac{1}{5} - \frac{2}{5}i + \frac{2}{5}j & 0 \\ -\frac{3}{5} - \frac{3}{5}i + \frac{3}{5}j & \frac{1}{5} - \frac{2}{5}i - \frac{1}{5}j - \frac{3}{5}k & -\frac{6}{5} + \frac{6}{5}i + \frac{6}{5}k & 0 \end{pmatrix}.$$

Opět lze odvodit, že

$$M_0^{-1} = Q_1 M_1^{-1} P_1.$$

Dosazením dostáváme

$$M_0^{-1} = \begin{pmatrix} -\frac{3}{5} - \frac{3}{5}i + \frac{3}{5}j & \frac{1}{5} - \frac{2}{5}i - \frac{1}{5}j - \frac{3}{5}k & -\frac{6}{5} + \frac{6}{5}i + \frac{6}{5}k & 0 \\ -\frac{22}{15} - \frac{1}{9}i - \frac{31}{45}j - \frac{14}{15}k & -\frac{1}{15} - \frac{1}{9}i - \frac{10}{9}j + \frac{19}{45}k & -\frac{2}{9} - \frac{2}{5}i + \frac{28}{15}j - \frac{62}{45}k & \frac{5}{3} \\ \frac{1}{5} - \frac{2}{5}i - \frac{1}{5}k & -\frac{1}{15} + \frac{1}{5}i - \frac{1}{15}j - \frac{2}{15}k & \frac{1}{5} - \frac{2}{5}i + \frac{2}{5}j & 0 \\ \frac{1}{5} + \frac{2}{5}k & 0 & -\frac{2}{5}i - \frac{4}{5}j & 0 \end{pmatrix}.$$

Reference

[1] P. M. Cohn: *On the structure of the GL_2 of a ring*, Publications Mathématiques de l'IHÉS **30** (1966), 5–53.

[2] N. Cohen, S. de Leo: *Quaternionic matrices: inversion and determinant*, preprint, `https://www.ime.unicamp.br/sites/default/files/pesquisa/relatorios/rp-1999-45.pdf`

[3] M. Kureš, L. Skula: *Reduction of matrices over orders of imaginary quadratic fields*, Linear Algebra and Its Applications **435.8** (2011), 1903–1919.

[4] A. G. Kuroš: *Kurs vyššej algebry*, 7. vydání, GITTL, Moskva, 1962, rusky.

[5] B. Maya, M. Kureš: *Some tridiagonal matrices and determinants of Schur-Cohn criterion for trinomials*, University Politehnica of Bucharest Scientific Bulletin, Series A, Applied Mathematics and Physics **84.4** (2022), 67–80.

Alžběta Kočendová, Ústav matematiky, Fakulta strojního inženýrství, Vysoké učení technické v Brně, Technická 2, 616 69 Brno, Česká republika,
e-mail: 226835@vutbr.cz

Miroslav Kureš, Ústav matematiky, Fakulta strojního inženýrství, Vysoké učení technické v Brně, Technická 2, 616 69 Brno, Česká republika,
e-mail: kures@fme.vutbr.cz

VYBRANÉ PRÍKLADY Z INTERNETOVEJ MATEMATICKEJ SÚŤAŽE MATHING

VIERA ŠTOUDKOVÁ RŮŽIČKOVÁ

Abstrakt. Článok obsahuje dva vybrané príklady z internetovej matematickej súťaže MATHING. V prvom príklade sa dokazuje implikácia, ktorá obsahuje nerovnice, a sú tu diskutované často sa vyskytujúce chybné postupy pri riešení tohto typu úloh. Druhý príklad je takisto dôkazový, na tému sudoku, a okrem diskusie k jeho riešeniu je tu zmienená aj motivácia k jeho zaradeniu do súťaže. V tomto prípade sa riešenie dalo nájsť aj na internete, čo je v súlade s pravidlami súťaže.

Ústav matematiky na FSI VUT v Brne každoročne organizuje matematickú súťaž MATHING pre študentov stredných škôl v Česku a na Slovensku, s pôvodným názvom Internetová matematická olympiáda. V novembri v roku 2023 prebehol už jej šestnásty ročník. Na príprave príkladov a ich vyhodnotení sa nemalou mierou podieľajú študenti oboru Matematické inženýrství a oboru Aplikovaná matematika. Na stránkach `mathing.fme.vutbr.cz` je možné nájsť zadania aj riešenia príkladov zo všetkých ročníkov.

Tento príspevok je šiesty v poradí na túto tému. Pozrieme sa v ňom bližšie na dva príklady, ktoré boli v súťaži v minulosti zaradené.

1. Príklad Nerovnosti

V roku 2022 bol príklad číslo 4 venovaný nerovnostiam. Uvádzam tu jeho zadanie.

Príklad 1. *Dokažte, že pokud reálná čísla a, b splňují nerovnosti*

$$|a+b| < ab+1 < 2, \tag{1}$$

potom

$$|a| < 1,\ |b| < 1. \tag{2}$$

Príklad skúste vyriešiť sami. Dve možné riešenia príkladu nájdete aj na stránkach súťaže.

Mojim cieľom teraz nie je prediskutovať ďalšie možné správne riešenia tohto príkladu, ale ukázať, čo všetko sa pri riešení dalo pokaziť. Teda na čo všetko si treba dať pozor, keď dokazujeme takéto tvrdenie. Uvediem niekoľko možných nesprávnych postupov. Všetky tieto chybné postupy sa v riešeniach doručených od našich súťažiacich skutočne vyskytovali, prvé tri opakovane, štvrtý je perlička na pobavenie.

Pre zaujímavosť: Dokazované tvrdenie je v skutočnosti trochu inak zapísaná podmienka stability diferenčných rovníc druhého rádu.

Ak čísla a, b sú korene kvadratickej rovnice $x^2 + \alpha x + \beta = 0$, potom koeficienty tejto rovnice α, β sú dané vzťahom $\alpha = -(a + b), \beta = ab$.

Tvrdenie z príkladu 1 teda hovorí, že ak sú korene rovnice $x^2 + \alpha x + \beta = 0$ reálne čísla a $|\alpha| < \beta + 1 < 2$, potom sú oba korene rovnice v absolútnej hodnote menšie ako jedna, čo znamená stabilitu.

Takže nemusíme túto rovnicu riešiť, stačí overiť, či platí $|\alpha| < \beta + 1 < 2$.

1.1. Prvý chybný postup

Skúšam nájsť také dve reálne čísla a, b, že platí (1), t.j. $|a + b| < ab + 1 < 2$.

Napríklad to platí pre $a = 0$ a $b = 0{,}5$: $|0 + 0{,}5| < 0 \cdot 0{,}5 + 1 < 2$.
Alebo aj pre $a = 0{,}5$ a $b = 0{,}5$: $|0{,}5 + 0{,}5| < 0{,}5 \cdot 0{,}5 + 1 < 2$.
Alebo aj pre $a = 0{,}9$ a $b = 0{,}7$: $|0{,}9 + 0{,}7| < 0{,}9 \cdot 0{,}7 + 1 < 2$.
Ale ak skúsim vziať $a = 1, 2, 3 \ldots$, nedarí sa mi nájsť také b, aby to platilo.

Takže vo všetkých prípadoch, ktoré som našla, platí $|a| < 1, |b| < 1$. Záver teda je, že tvrdenie platí.

Kde je chyba: Overila som to len pre vybrané dvojice. Nemám istotu, že pre nejakú inú dvojicu a, b, ktorú som vôbec neskúšala, sa stane, že bude platiť (1), ale budú to pritom také veľké čísla, že nebude platiť $|a| < 1, |b| < 1$. Čo keby to pre nejakú kombináciu veľkých (kladných alebo záporných) čísel predsa len platilo?

Ako som uviedla vyššie, je to akýsi test stability. Čo ak by sa tým testovala stabilita nejakého životne dôležitého systému? A ja by som si povedala: nepodarilo sa mi nájsť takú rovnicu, ktorá splňuje podmienky a pritom je systém nestabilný, budem teda veriť tomu, že tie podmienky mi zaručia stabilitu. Riskli by ste to?

◇ Toto bol nesprávny postup typu: „Skúšam rôzne možnosti a pre všetky z nich to platí, takže to platí vždy.“

1.2. Druhý chybný postup

Všimnem si, že podmienka (2) vyzerá jednoduchšie než podmienka (1), začnem teda s ňou: Vezmem také a, b, že platí $|a| < 1, |b| < 1$. Potom aj $|ab| < 1$, a z toho aj $ab < 1$. To už je vlastne druhá z nerovností (1), lebo potom $ab + 1 < 2$.

Zostáva ešte tá prvá nerovnosť, $|a + b| < ab + 1$. Umocním ju a upravím:

$$\begin{aligned}
(|a + b|)^2 &< (ab + 1)^2, \\
a^2 + 2ab + b^2 &< a^2b^2 + 2ab + 1, \qquad / - 2ab - a^2b^2 - b^2 \\
a^2 - a^2b^2 &< 1 - b^2, \\
a^2(1 - b^2) &< 1 - b^2, \\
0 &< (1 - a^2)(1 - b^2).
\end{aligned}$$

Pretože viem, že $|a| < 1, |b| < 1$, potom určite aj $a^2 < 1, b^2 < 1$ a súčin vpravo je kladný. Nerovnosť $0 < (1-a^2)(1-b^2)$ teda platí a platí aj pôvodná nerovnosť, lebo úpravy boli ekvivalentné a pôvodná nerovnica pred umocnením mala obe strany kladné.

Platia teda obe nerovnosti z podmienky (1) a tvrdenie je dokázané.

Kde je chyba: Naše dokazované tvrdenie je implikácia. Hovorí:

Ak pre reálne čísla a, b platí (1)*, potom platí aj* (2)*.*

Ale ja som namiesto toho dokázala, že

Ak pre reálne čísla a, b platí (2)*, potom platí aj* (1)*.*

A to nie je to isté. Neoverovala som také reálne čísla a, b, pre ktoré neplatí (2). O takých som v mojom dôkaze vôbec neuvažovala. Nezistila som, či by aj pre také čísla mohli platiť nerovnosti (1). Ak áno, tak to by znamenalo, že naše dokazované tvrdenie je nepravdivé.

Platnosť opačnej implikácie nehovorí nič o tom, či platí aj pôvodná implikácia!

◇◇ Toto bol nesprávny postup typu: „Dokazujem opačnú implikáciu“.

Poznámka: V skutočnosti teda sú podmienky (1) a (2) ekvivalentné.

1.3. Tretí chybný postup

Výpočty v predchádzajúcom príklade nie sú úplne nanič, mohli by sa použiť aj pri dokazovaní tej správnej implikácie. Napríklad, začnem s prvou nerovnicou z (1). Predpokladám, že platí a umocním ju na druhú:

$$\begin{aligned} (|a+b|)^2 &< (ab+1)^2, \\ a^2+2ab+b^2 &< a^2b^2+2ab+1, \qquad / -2ab-a^2b^2-b^2 \\ a^2-a^2b^2 &< 1-b^2, \\ a^2(1-b^2) &< 1-b^2. \end{aligned}$$

Teraz celú nerovnicu vydelím výrazom $(1-b^2)$ a dostanem $a^2 < 1$, z toho $|a| < 1$. Alebo, ak prehodím a, b, z toho istého dostanem

$$\begin{aligned} a^2+2ab+b^2 &< a^2b^2+2ab+1, \qquad / -2ab-a^2b^2-a^2 \\ -a^2b^2+b^2 &< 1-a^2, \\ b^2(1-a^2) &< 1-a^2. \end{aligned}$$

Túto nerovnicu vydelím výrazom $(1-a^2)$ a dostanem $b^2 < 1$, z toho $|b| < 1$. Dôkaz je hotový.

Kde je chyba: Mohlo by mi byť podozrivé, že som v dôkaze vôbec nevyužila druhú nerovnosť z predpokladu, to je, že $ab+1 < 2$. Ale nie je to ešte samo o sebe chyba, občas sa stane, že nejaká časť predpokladu je zbytočná.

K chybe došlo pri delení nerovnice výrazom $(1-b^2)$ a potom podobne výrazom $(1-a^2)$. O týchto výrazoch neviem, či sú kladné, záporné, alebo dokonca by mohli byť aj nulové. Nemôžem nimi teda len tak deliť. Musím to rozdeliť na tieto tri

prípady a každý vyšetriť zvlášť. Pri delení záporným výrazom sa zmení znamienko nerovnice!

Na dokončenie dôkazu je potrebná tá zatiaľ nevyužitá nerovnica $ab + 1 < 2$. Už to tu nebudem dokončovať, podobný postup je použitý v riešení uvedenom na stránkach súťaže.

◇◇◇ Toto bol nesprávny postup typu: „Nedávam si pozor pri úpravách nerovníc.“

1.4. Štvrtý chybný postup

Na záver jedna perlička: v jednom riešení autorom z nejakého dôvodu vadilo, že čísla a, b majú byť z otvoreného intervalu $(-1, 1)$, oni tam chceli mať uzavretý interval. Vyriešili to veľmi originálne. Našli číslo $c < 1$, ktoré je „tesne vedľa“ čísla 1 a otvorený interval $(-1, 1)$ mohli potom zapísať ako uzavretý interval $\langle -c, c\rangle$.

Boli si pritom vedomí toho, že toto číslo c nemôže byť $0{,}\overline{9}$, aj keď to tak na prvý pohľad vyzerá, pretože v skutočnosti $0{,}\overline{9} = 1$. Dokonca k tomu napísali aj správny výpočet pomocou vzorca pre súčet geometrického radu:

$$0{,}\overline{9} = 0{,}9 + 0{,}09 + 0{,}009 + \cdots = 0{,}9\left(1 + 0{,}1 + 0{,}1^2 + 0{,}1^3 + \cdots\right) = 0{,}9\frac{1}{1 - 0{,}1} = 1.$$

Ale nevzdali to. Tesne vedľa čísla, ktoré má za desatinnou čiarkou nekonečne veľa deviatok, logicky bude číslo, ktoré tam má samé deviatky a nejakú osmičku. To je (podľa nich) číslo $0{,}9\overline{89}$.

Keby sa zamysleli, asi by ich napadlo, že napríklad číslo $0{,}9\overline{98}$ je určite väčšie. Otázka je, či neexistuje ešte väčšie číslo. Podozrivé je napríklad $0{,}\overline{998}$. Alebo, možno by sa mohla tá osmička dať ešte ďalej od desatinnej čiarky...

Nechávam to čitateľom na premyslenie. Ak by sa vám podarilo toto číslo nájsť a dokázať, že medzi ním a jednotkou už žiadne iné reálne číslo nie je, bol by to prevratný objav.

2. Príklad Sudoku

Občas riešim sudoku. Je to celkom dobré cvičenie na logiku, postreh a na sústredenie. S logikou problém nemám, ale vedieť dobre riešiť sudoku znamená aj mať schopnosť rýchle a neomylne nájsť v tabuľke to voľné políčko, ktoré sa práve dá logicky doplniť. Často je tam také jediné. Mne to obvykle trvá dlho, než si také miesto všimnem, a občas niečo prehliadnem a doplním nesprávne číslo. Uvedomujem si, ako to robím nedokonale, a že lepšie by si s tým poradil počítačový algoritmus... Vždy ale pri týchto úvahách nakoniec dôjdem k záveru, že použiť na to počítač by nebolo ono, a radšej sa s tým trápim sama.

Raz ma pri riešení sudoku napadlo, že by na túto tému mohol byť aj príklad v našej súťaži. A aby to nebolo až také zložité, namiesto klasického sudoku 9×9 by sa použila jeho zmenšená verzia, 4×4, nazývaná shidoku.

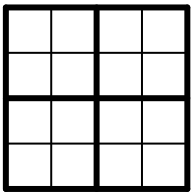
Úlohou by bolo ukázať, že najmenší možný počet dopredu vyplnených políčok, aby toto sudoku malo jednoznačné riešenie, je 4.

Toto tvrdenie je známe, a pretože naša súťaž dovoľuje používať všetky možné zdroje, dalo sa predpokladať, že niektorí súťažiaci si ten dôkaz skúsia dohľadať.

Skúsila som to aj ja. Prekvapilo ma, že sa mi to vôbec nedarilo. O sudoku sa toho samozrejme na internete dá nájsť veľa, dá sa ľahko zistiť aj potrebný minimálny počet zadaných čísiel pre klasické sudoku, je to 17. Ako to ale býva, väčšina textov uvádza len tvrdenia bez dôkazu, často dokonca aj bez odkazu na zdroj. Ukážkou takéhoto textu je napríklad príspevok „Matematika za sudoku“, [1]. A pretože takéto „jednoduchšie“ texty sú populárnejšie, vyhľadávač ich uprednostní pred tými „serióznejšími“. Takže skutočnosť, že o sudoku sa na internete píše veľa, nám vyhľadávanie nášho dôkazu paradoxne skôr skomplikuje.

Zhodnotila som, že nájdenie toho dôkazu je tak náročné, že môžeme príklad bez obáv zaradiť. Stalo sa tak v roku 2021 a v súťaži mal číslo 8. Príklad bol rozdelený na dve časti, aby sme trochu pomohli slabším riešiteľom. Od tých sa očakávalo, že zvládnu len prvú časť.

Príklad 2. *Máme sudoku* 4×4*, do kterého doplňujeme čísla od* 1 *do* 4 *tak, že v každém řádku jsou 4 různá čísla, v každém sloupci jsou 4 různá čísla, a v každém ze čtyř tlustě vyznačených čtverců* 2×2 *jsou 4 různá čísla, viz obrázek 1.*



Obrázek 1. Obrázek k zadání příkladu 2..

Je známo, že k tomu, aby mohlo mít toto sudoku jediné řešení, je potřeba mít zadaná 4 čísla.

a) Nalezněte takové zadání sudoku 4×4*, že budou dopředu vyplněna právě 4 čísla a poloha zbývajících čísel už pak bude určena jednoznačně. Naznačte i postup řešení takto vámi zadaného sudoku.*

b) Dokažte, že neexistuje takové zadání sudoku 4×4*, kde budou dopředu vyplněna jenom 3 čísla a poloha ostatních už bude určena jednoznačně.*

Poznámka: O sudoku je spousta informací na internetu a v literatuře. Pokud váš důkaz obsahuje něco, co jste sami nevymysleli, jenom převzali, je v něm potřeba uvést i odkaz na zdroj s důkazem vámi použitého tvrzení.

Tento príklad bol teda výnimočný tým, že riešitelia mali na výber dva možné prístupy - buď dôkaz vymyslia sami, alebo sa ho pokúsia niekde dohľadať. To bolo dovolené, ale v takom prípade by museli buď celý dôkaz prepísať do svojho riešenia, alebo uviesť odkaz na zdroj – článok – v ktorom je tento dôkaz uvedený.

Dopadlo to tak, že len asi tri tímy uviedli odkazy na články, kde toto tvrdenie bolo uvedené, a ani jeden z odkazovaných článkov neobsahoval jeho dôkaz.

Tí riešitelia, ktorí poslali nejaký vlastný dôkaz, postupovali tak, že systematicky prechádzali možné rozmiestnenia troch dopredu vyplnených čísiel a pre každú možnosť ukázali, že nedáva jednoznačné riešenie. Tých možností je však toľko, že skoro všetci nejaké vynechali a ich dôkazy neboli úplné.

Moje nádeje, že behom dvoch hodín, ktoré mali riešitelia k dispozícii, niekto objaví elegantný dôkaz, či už vlastný, alebo prevzatý z internetu, sa teda nesplnili.

Naopak, bolo sklamaním, koľkí z nich za dôkaz považovali to, že uviedli len jedno konkrétne zadanie s dopredu vyplnenými tromi číslami a ukázali, že nemá jednoznačné riešenie.

Ďalej, niektorí sa pokúsili o rôzne pomocné tvrdenia, konkrétne sa vyskytli tieto tri:

Tvrdenie 1. *Aby existovalo jednoznačné riešenie, musia byť vyplnené tri rôzne čísla.*

Tvrdenie 2. *Aby existovalo jednoznačné riešenie, musí byť v každom štvorci vyplnené aspoň jedno číslo.*

Tvrdenie 3. *Aby existovalo jednoznačné riešenie, v každom riadku alebo v každom stĺpci musí byť vyplnené aspoň jedno číslo.*

Tvrdenie 1 je pravdivé, a dá sa ľahko dokázať napríklad úvahou: Ak by neboli vyplnené tri rôzne čísla, aspoň dve sa v zadaní vôbec neobjavia. Určite teda ku každému riešeniu existuje aj druhé riešenie také, kde sú tieto dve čísla vymenené.

Tvrdenie 2 a Tvrdenie 3 by nám síce hneď implikovalo hľadaný dôkaz, obe tieto tvrdenia sú však nepravdivé a dajú sa vyvrátiť protipríkladom. Nájdenie týchto protipríkladov nie je zložité a nechávam ho čitateľom na pobavenie.

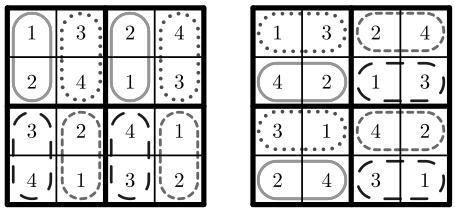
Pri príprave tohto článku som konečne natrafila aj na text, uvádzajúci dôkaz neexistencie jednoznačného zadania len s tromi číslami pre sudoku 4×4, [2]. Autorom je indický fyzik Sourendu Gupta. Má tam nejakú teóriu, ale aj on nakoniec v dôkaze postupne overuje rôzne možnosti.

Na záver uvádzam svoj dôkaz, uvedený na stránkach našej súťaže ako časť riešenia príkladu 8 (14. ročník). Obvykle do týchto článkov nekopírujem autorské riešenia príkladov, pretože sa dajú jednoducho dohľadať na stránkach súťaže, ale v tomto prípade urobím výnimku, vzhľadom na to, že je to jediný mne známy dôkaz tohto tvrdenia nevyužívajúci postupné prechádzanie možností ani žiadnu teóriu.

Riešenie príkladu 2 b): (Prevzaté z `https://mathing.fme.vutbr.cz`)

Důkaz. Ukážeme, že políčka v každém vyplněném sudoku lze rozdělit do 4 skupin tak, že v každé skupině se mohou čísla navzájem prohodit. Pokud jsou dopředu vyplněna pouze 3 čísla, pak v alespoň jedné ze skupin není vyplněno nic a úloha má tak více řešení.

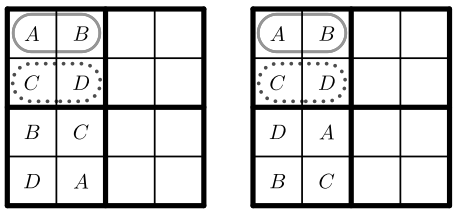
Příklady takového dělení u dvou různě vyplněných sudoku jsou na obrázku 2. (Pozn.: pro případ černobílého zobrazení jsou skupiny vyznačeny i různým typem



Obrázek 2. Obrázek k řešení příkladu 2..

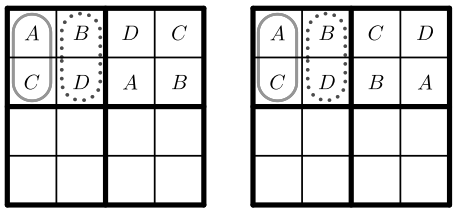
čáry. Zelená skupina je vyznačena plnou čárou a červená skupina je vyznačena tečkovanou čárou)

V obou případech stačí, aby existovalo rozdělení na červenou a zelenou skupinu, a pak už lze i zbývajících 8 políček určitě rozdělit na dvě další skupiny vyznačeným způsobem. Předpokládejme, že existuje vyplněné sudoku, které nelze rozdělit tímto způsobem. Označme čísla v levém horním čtverci v prvním řádku A a B a ve druhém řádku C a D. Pak z předpokladu plyne, že v levém dolním čtverci jsou čísla A a B v různých řádcích a stejně tak jsou v různých řádcích i čísla C a D. Dostáváme tedy pouze dvě možnosti jejich umístění, viz obrázek 3.



Obrázek 3. Obrázek k řešení příkladu 2..

Podobně z předpokladu dostaneme, že v pravém horním čtverci jsou čísla A a C v různých sloupcích a stejně tak i čísla B a D. Dostáváme tedy opět pouze dvě možnosti jejich umístění, viz obrázek 4.



Obrázek 4. Obrázek k řešení příkladu 2..

Vidíme, že v levém dolním čtverci je určitě řádek obsahující dvojici čísel B a C a v pravém horním čtverci je určitě sloupec obsahující dvojici čísel A a D.

Políčko v tomto řádku a v tomto sloupci v pravém dolním čtverci už tedy nemůže obsahovat žádné z čísel A, B, C, D. To je ve sporu s předpokladem, že je sudoku vyplněno. □

Na záver niečo na zamyslenie: Nedal by sa podobne urobiť aj dôkaz toho, že potrebný minimálny počet zadaných čísiel pre klasické sudoku je 17? Ten, ktorý je verejne známy, publikovaný v článku [3], totiž tiež využíva prechádzanie možností a dá sa realizovať jedine na počítači.

Reference

[1] *Matematika za sudoku*, https://sciencemag.cz/matematika-za-sudoku/
[2] Sourendu Gupta. *Some results on Su Doku*, 2006, https://theory.tifr.res.in/~sgupta/sudoku/theorems.pdf
[3] Gary McGuire and Bastian Tugemann and Gilles Civario. *There is no 16-Clue Sudoku: Solving the Sudoku Minimum Number of Clues Problem*, 2013, https://doi.org/10.48550/arXiv.1201.0749

Viera Štoudková Růžičková, Ústav matematiky, Fakulta strojního inženýrství, Vysoké učení technické v Brně, Technická 2, 616 69 Brno, Česká republika,
e-mail: ruzickova@fme.vutbr.cz