SLOVENSKÝ ČASOPIS PRE GEOMETRIU A GRAFIKU

ročník 14, číslo 27, 2017
ISSN 1336-524X

G
Slovenský časopis pre geometriu a grafiku

Ročník 14 (2017), číslo 27
ISSN 1336-524X

Vydáva:
Slovenská spoločnosť pre Geometriu a Grafiku

SSGG

G je vedecký časopis pre geometriu a grafiku publikujúci originálne vedecké práce, prehľady a informatívne články, krátke referáty, odborné príspevky, analýzy, aktuality a rešerše z rôznych odvetví geometrie (elementárna, deskriptívna, konštrukčná, projektívna, analytická, diferenciálna, algebrická, počítačová, výpočtová, konečná, neeuklidovská) a topológie, geometrického modelovania a počítačovej grafiky, v oblasti základného teoretického výskumu, v oblasti výučby geometrie na všetkých typoch škôl, z histórie a metodológie vývoja geometrie, a z aplikácií geometrie a geometrických metód v rôznych vedeckých, spoločenských a technických disciplínach.

Redakcia: Slovenská spoločnosť pre Geometriu a Grafiku
Ústav matematiky a fyziky, Strojnícka fakulta
Slovenská technická univerzita v Bratislave
Námestie slobody 17
812 31 Bratislava

Objednávky, reklamácie a predplatné vybavuje:
Redakcia G - SSGG
ÚMF SjF STU, Námestie slobody 17, 812 31 Bratislava
ssgg@ssgg.sk

Periodicita: Časopis vychádza dvakrát do roka v náklade 200 kusov.
Ročné predplatné bez poštovného a balného je 20,- Euro.
Evidenčné číslo EV 3228/09

Informácie a pokyny pre autorov na adrese: www.ssgg.sk

Tlačí: ForPress Nitrianske tlačiarne, s. r. o.

Časopis G je citovaný v: Zentralblatt für Mathematik

SLOVENSKÝ ČASOPIS PRE GEOMETRIU A GRAFIKU
SLOVAK JOURNAL FOR GEOMETRY AND GRAPHICS

ročník 14, číslo 27, 2017
volume 14, number 27, 2017

Obsah – Contents

SLOVENSKÁ SPOLOČNOSŤ

SG

PRE GEOMETRIU A GRAFIKU

Nezisková vedecká spoločnosť pre rozvoj geometrie a počítačovej grafiky

zaregistrovaná dňa 13.5.2002 na Ministerstve vnútra SR ponúka
všetkým záujemcom individuálne alebo kolektívne členstvo.
Elektronickú prihlášku nájdete na domovskej stránke spoločnosti.

Cieľom spoločnosti je stimulovať vedecký výskum, aplikácie i pedagogickú prácu a metodiku vyučovania v oblasti geometrie a počítačovej grafiky.

Spoločnosť pôsobí na celom území Slovenskej republiky a jej poslaním je:

a) podporovať rozvoj geometrie a počítačovej grafiky a ich vzájomnej interakcie

b) presadzovať kvalitu geometrického a grafického vzdelania na všetkých typoch škôl v SR

c) spolupracovať s medzinárodnými spoločnosťami a organizáciami rovnakého zamerania

d) podieľať sa na organizácii vedeckých podujatí, konferencií, seminárov a sympózií o geometrii a počítačovej grafike

e) publikovať vedecký časopis s názvom G venovaný geometrii a grafike

f) rozvíjať vlastnú edičnú a publikačnú činnosť

g) získať priazeň a členstvo organizácií aj jednotlivcov.

Vítané sú všetky ďalšie aktivity – diskusné fórum na Internete, softvérový bazár, workshopy, e-learningové kurzy ai., ktoré možno vykonávať pod hlavičkou spoločnosti.

Spoločnosť SSGG
Ústav matematiky a fyziky
Strojnícka fakulta STU v Bratislave
Námestie slobody 17, 812 31 Bratislava, SR
e-mail: ssgg@ssgg.sk, URL: www.ssgg.sk

O ideáloch v pologrupe S_m zvyškových tried (mod m), o minimálnych a maximálnych ideáloch v S_m s ohľadom na jej podmnožiny – lokálna Eulerova-Fermatova veta

Imrich Abrhan

Abstrakt

V prvej časti práce je definovaný pojem maximálneho nezávislého systému hlavných ideálov v pologrupe S_m zvyškových tried (mod m) a pomocou maximálneho nezávislého systému hlavných ideálov sa definujú podmnožiny pologrupy S_m. Dokázané sú tiež tvrdenia o minimálnych a maximálnych ideáloch v S_m a tvrdenia o minimálnych ideáloch v okruhu S_m s ohľadom na tieto podmnožiny v S_m.

V druhej časti práce sa vyšetrujú vlastnosti takých hlavných ideálov v S_m, ktoré obsahujú jednotkový prvok.

V tretej časti práce je dokázaná lokálna Eulerova-Fermatova veta.

Kľúčové slová: pologrupa S_m zvyškových tried (mod m), hlavný ideál v S_m (aj v okruhu S_m), Greenova relácia ekvivalencie na S_m, S_m/ϑ – množina ϑ – tried priradených relácii ekvivalencie ϑ na S_m, čiastočné usporiadanie na S_m/ϑ, (a, b) – najväčší spoločný deliteľ celých čísiel $a \geq 1$, $b \geq 1$, maximálny nezávislý systém hlavných ideálov v S_m, minimálny (maximálny) ideál v S_m (minimálny aj v okruhu S_m) s ohľadom na podmnožinu $B \subseteq S$ $(\emptyset \neq B)$, lokálna Eulerova-Fermatova veta.

Abstract

Concept of maximal independent system of principle ideals in the semigroup S_m residual classes (mod m) is defined in the first part of this paper, and subsets of semigroup S_m are defined by means of this maximal independent system of principle ideals. There are also proved theorems on minimal and maximal ideals in S_m and theorems on minimal ideals in the ring S_m with respect to these subsets of S_m .

Properties of such principle ideals in S_m that contain unit element are studied in the second part of this paper

Local Euler-Fermat theorem is proved in the third part.

Key words: semigroup S_m of reminder classes (mod m), principle ideal in S_m, (also in ring S_m), Green equivalence relation on S_m, S_m/ϑ – set of ϑ – classes related to equivalence relation ϑ on S_m, partial ordering on S_m/ϑ, (a, b) – maximal common divisor of integer numbers $a \geq 1$, $b \geq 1$, maximal independent system of principle ideals in S_m, minimal (maximal) ideal in S_m (minimal also in the ring S_m) with respect to subset $B \subseteq S$ $(\emptyset \neq B)$, local Euler-Fermat theorem.

1 Úvod

V tejto práci a v prácach [8], [14], [17] sa vyšetruje štruktúra multiplikatívnej pologrupy S_m zvyškových tried (mod m) metódami teórie pologrúp. Vyšetrujú vlastnosti ideálov, napr. minimálnych, maximálnych ideálov v S_m s ohľadom na podmnožiny v S_m (pozri [2], [3], [4]) a minimálnych ideálov v okruhu S_m s ohľadom na podmnožiny okruhu S_m. V tretej časti práce je ukázané, že lokálna Eulerova-Fermatova veta je dôsledkom vety 2.9 z práce [8].

Niektoré výsledky o štruktúre špeciálnej pologrupy S_m sa aplikujú napr. v kryptológii.

Predovšetkým uvedieme základné pojmy (ich označenia) a tvrdenia o týchto pojmoch, na ktoré sa budeme v ďalšom odvolávať (nebudeme ich bezprostredne často uvádzať a budeme ich považovať za známe).

Pod číslom (pokiaľ nebude iné poznamenané) budeme v ďalšom rozumieť „celé číslo". V prípade, že číslo a delí číslo b (alebo a je deliteľom čísla b) budeme písať $a \mid b$. V prípade, žečíslo a nedelí číslo b, budeme písať $a \nmid b$. Najväčší spoločný deliteľ čísel a, b budeme označovať (a, b).

V ďalšom budeme pod zápisom

$$m = p_1^{\alpha_1}\ p_2^{\alpha_2} \dots\ p_k^{\alpha_k}$$

rozumieť kanonický rozklad čísla $m > 1$, kde $p_1, p_2, \dots, p_k$ sú navzájom rôzne prvočísla a $\alpha_1, \alpha_2, \dots, \alpha_k$ sú prirodzené čísla.

Veta 1.1 (pozri napr. [9]). Nech $m = p_1^{\alpha_1}\ p_2^{\alpha_2} \dots\ p_k^{\alpha_k}$ je kanonický rozklad celého čísla $m > 1$. Potom číslo d je kladným deliteľom čísla m práve vtedy, ak $d = p_1^{\beta_1}\ p_2^{\beta_2} \dots\ p_k^{\beta_k}$, kde $\beta_1, \beta_2, \dots \beta_k$ sú navzájom rôzne celé čísla a $0 \le \beta_1 \le \alpha_1$, $0 \le \beta_2 \le \alpha_2$, ... , $0 \le \beta_k \le \alpha_k$.

Množinu všetkých navzájom rôznych kladných deliteľov čísla m označme znakom $D(m)$.

Nech je celé číslo $m > 1$ a S_m je množina zvyškových tried (mod m). V ďalšom budeme znakom S_m označovať multiplikatívnu pologrupu (v ďalšom „pologrupu S_m") zvyškových tried (mod m) (s ohľadom na binárnu operáciu násobenia na S_m (mod m)) (pozri napr. [4]). V prípade, že pod S_m budeme rozumieť okruh s ohľadom na binárne operácie sčítania a násobenia na S_m podľa (mod m), budeme vždy písať napr. „v okruhu S_m" (namiesto „v S_m", ak pod S_m rozumieme pologrupu zvyškových tried (mod m)).

1) $[\,\bar{x}\,]$ označujeme hlavný ideál v S_m generovaný prvkom $\bar{x} \in S_m$.

2) $\mathscr{L}$ označujeme Greenovú reláciu ekvivalencie na S_m (definovanú takto: $x, \bar{y} \in S_m$ sú v relácii ϑ na S_m, t. j. $\bar{x}\ \vartheta\ \bar{y}$ práve vtedy, ak $[\,\bar{x}\,] = [\,\bar{y}\,]$.

3) $[\,\bar{x}\,]\mathscr{L}$ označujeme $\mathscr{L}$ – triedu priradenú relácii ekvivalencie $\mathscr{L}$ na S_m obsahujúcu prvok $\bar{x} \in S_m$, t.j. $[\,\bar{x}\,]\mathscr{L} = \{\,\bar{y} \mid \bar{y} \in S_m$ a $\bar{x}\ \mathscr{L}\ \bar{y}\,\}$, teda $[\,\bar{x}\,] = [\,\bar{y}\,]$.

4) $S_m/\mathscr{L}$ označujeme množinu všetkých $\mathscr{L}$–tried priradených k relácii ekvivalencie $\mathscr{L}$ na S_m.

Na množine $S_m/\mathscr{L}$ definujeme čiastočné usporiadanie $\le$ definované takto: $[\,\bar{x}\,]\mathscr{L} \le [\,\bar{y}\,]\mathscr{L}$, $\bar{x}, \bar{y} \in S_m$ práve vtedy, ak $[\,\bar{x}\,] \subseteq [\,\bar{y}\,]$.

Veta 1.2 (pozri napr. [8]). Pre každé dva prvky $\bar{a}, \bar{b} \in S_m$ platí: $[\,\bar{a}\,]\mathscr{L} \le [\,\bar{b}\,]\mathscr{L}$ práve vtedy, ak $(b, m)/(a, m)$.

V ďalšom budeme namiesto „B je podmnožina pologrupy S_m“ stručne písať „$B \subseteq S_m$“ a budeme vždy predpokladať, že $\bar{0} \notin B$, t. j. nulový prvok $\bar{0}$ pologrupy S_m nie je prvkom podmnožiny $B \subseteq S_m$.

Poznámka 1.1. Znakom $A \subset B$ budeme rozumieť, že A je vlastnou podmnožinou B ($A \neq B$). $A \subseteq B$ značí, že buď $A \subset B$, alebo $A = B$.

Ak $B \subseteq S_m$, znakom $\overline{B_m}$ budeme označovať množinu $S_m \backslash B$.

Poznámka 1.2. Nech S_m je pologrupa zvyškových tried (mod m) a $B \subseteq S_m$. Znakom

1) $[B]$ budeme označovať množinu $\cup\{[\bar{b}\,] \mid \bar{b} \in B\}$.

2) $N(B)$ (pozri napr. [2], [3], [4], [5]) množinu všetkých $\bar{x} \in S_m$ takých, že pre každé $\bar{b} \in B$ sa $[\bar{b}\,]\mathscr{L}$ nerovná a nie je menšie ako $[\bar{x}\,]\mathscr{L}$.

Ak $N(B) \neq \emptyset$, potom $N(B)$ je ideál v S_m. Ak $\bar{a} \in S_m$ a $B = \{\bar{a}\}$, potom namiesto „$N(\{a\})$“ budeme písať „$N(\bar{a})$“. Ak $N(\bar{a}) \neq \emptyset$, $\bar{a} \in S_m$, potom $N(\bar{a})$ je ideál v S_m (pozri predchádzajúce tvrdenie o $N(B) \neq \emptyset$ a nazývame ho $\mathscr{L}$ – ideálom pologrupy S_m (generovaný prvkom $\bar{a} \in S_m$ (pozri [5])).

3) Ak $\bar{a} \in S_m$ a $\overline{[\bar{a}]} = ([\bar{a}] \backslash [\bar{a}]\mathscr{L}) \neq \emptyset$, potom $\overline{[\bar{a}]}$ je ideál v S_m.

4) Pre každý ideál N v S_m platí: $N \cap \overline{N(B)_m} \neq \emptyset$ práve vtedy, ak $N \cap B \neq \emptyset$.

Definícia 1.1 (pozri napr. [2], [3], [4]). Nech $B \subseteq S_m$. Ideál N pologrupy S_m nazveme minimálnym ideálom v S s ohľadom na B, ak $N \cap B \neq \emptyset$ a neexistuje taký ideál $N' \subset S_m$, že $N' \subset N$ a $N' \cap B \neq \emptyset$.

Veta 1.3 (pozri napr. [2], [4]). Nech $B \subseteq S_m$.

Potom:

a) Pre každú podmnožinu $N \neq \emptyset$ pologrupy $\overline{S_m}$ platí, že N je minimálny ideál v S_m s ohľadom na B vtedy a len vtedy, ak existuje také $\bar{b} \in B$, že $N = [\bar{b}\,]$ a $[\bar{b}\,]\vartheta$ je minimálny prvok v $\overline{N(B)_m}/\mathscr{L}$.

b) Pre každé $\bar{b} \in B$ platí: $[\bar{b}\,]$ je minimálny ideál v S_m s ohľadom na B vtedy a len vtedy, ak $\overline{N(B)_m} \cap [\bar{b}\,] = [\bar{b}\,]\mathscr{L}$.

Definícia 1.2. Nech $B \subseteq S_m$. Ideál N pologrupy S_m nazveme maximálnym ideálom v S_m s ohľadom na B, ak $\overline{N}_m \cap B \neq \emptyset$ ($\overline{N}_m = S_m \backslash N$) a neexistuje taký ideál N' pologrupy S_m, že $N \subset N'$ a $\overline{N'}_m \cap B \neq \emptyset$.

Veta 1.4 (pozri [6]). Nech $B \subseteq S_m$. Potom:

(a) N je maximány ideál pologrupy S_m s ohľadom na B vtedy a len vtedy, ak existuje taký prvok $\bar{b} \in B$, že $N = N(b)$ a $[\bar{b}\,]\mathscr{L}$ je maximálnym prvkom $[B]/\mathscr{L}$.

(b) Pre každé $b \in B$ platí: $N(b)$ je maximálny ideál v S_m s ohľadom na B vtedy a len vtedy, ak $\overline{N(b)_m} \cap [B] = [\bar{b}]\mathscr{L}$.

2 O minimálnych a maximálnych ideáloch v pologrupe S_m s ohľadom na podmnožiny v S_m

Definícia 2.1 (pozri [4]). Nech $B \subseteq S_m$. Množinu hlavných ideálov $\{[\bar{b}] \mid \bar{b} \in B\}$ pologrupy S_m nazveme nezávislým systémom hlavných ideálov v S, ak buď

α) $[\bar{a}] = [\bar{b}]$ pre každé $\bar{a}, \bar{b} \in B$, alebo

β) existujú také dva prvky $\bar{a}, \bar{b} \in S_m$, že $[\bar{a}] \neq [\bar{b}]$; potom pre každé dva prvky $\bar{u}, \bar{v} \in B$ také, že $[\bar{u}] \neq [\bar{v}]$, je $[\bar{a}] \not\subset [\bar{v}]$ a $[\bar{u}] \not\subset [\bar{v}]$.

Definícia 2.2. Nech $B \subseteq S_m$. Nezávislý systém hlavných ideálov $\{[b] \mid b \in B\}$ nazveme maximálnym nezávislým systémom hlavných ideálov v S_m, ak pre každé $\bar{a} \in S_m$ existuje taký prvok $\bar{b} \in B$, že buď $[\bar{b}]\mathscr{L} \leq [\bar{a}]\mathscr{L}$, alebo $[\bar{a}]\mathscr{L} \leq [\bar{b}]\mathscr{L}$.

Znakom $D(m)$ označme množinu všetkých navzájom rôznych deliteľov celého čísla $m > 1$.

Poznámka 2.1. Na príklade pologrupy S_{360} zvyškových tried (mod m) ukážeme, ako pomocou vety 1.1 a vety 1.2 nájdeme sedem navzájom rôznych maximálnych nezávislých systémov hlavných ideálov v S_{360}.

Nech $m = 2^3 \cdot 3^2 \cdot 5 = 360$. Položme $\alpha = 3 + 2 + 1$, t. j. α je súčet mocnín všetkých prvočísel v kanonickom rozklade čísla 360.

(A) Pomocou vety 1.1 nájdeme všetky prvky množiny $D(360)$. Podľa vety 1.1 platí: Pre každé celé kladné číslo d platí:

$d \in D(360)$ práve vtedy, ak

$$d = 2^{\beta_1} \cdot 3^{\beta_2} \cdot 5^{\beta_3}, \tag{1.1}$$

kde $\beta_1, \beta_2, \beta_3$ sú celé čísla a $0 \leq \beta_1 \leq 3$, $0 \leq \beta_2 \leq 2$, $0 \leq \beta_3 \leq 1$. Potom platí:

0) Ak

$$\beta_1 + \beta_2 + \beta_3 = 0, \tag{1.2}$$

potom s ohľadom na predpoklad má rovnica (1.2) práve jedno riešenie, trojicu (0, 0, 0). Podľa vety 1.1 je číslo 1 deliteľom čísla 360 a nazveme ho deliteľom stupňa 0 čísla 360.
Množina

$$D_0 = \{1\}$$

je množinou všetkých kladných deliteľov stupňa 0 čísla 360.

1) Ak

$$\beta_1 + \beta_2 + \beta_3 = 1, \tag{1.3}$$

potom s ohľadom na predpoklad je množina {(1, 0, 0), (0, 1, 0), (0, 0, 1)} množinou všetkých riešení rovnice (1.2). Z toho podľa vety 1.1 vyplýva, že každé z čísel 2, 3, 5 je deliteľom čísla 360 a každé z nich nazveme deliteľom stupňa 1 čísla 360. Množina

$$D_1 = \{2, 3, 5\} \tag{1.4}$$

je množinou všetkých kladných deliteľov stupňa 1 čísla 360.

2) Ak

$$\beta_1 + \beta_2 + \beta_3 = 2, \ (< \alpha = 6), \tag{1.5}$$

potom s ohľadom na predpoklad je množina {(2, 0, 0), (1, 1, 0), (0, 2, 0), (1, 0, 1), (0, 1, 1), } množinou všetkých riešení rovnice (1.5). Z toho podľa vety 1.1 je každé z čísel 4, 6, 9, 10, 15 deliteľom čísla 360 a každé z nich nazveme deliteľom stupňa 2 čísla 360. Množina

$$D_2 = \{4, 6, 9, 10, 15\}$$

je množinou všetkých kladných deliteľov stupňa 2 čísla 360.

3) Ak

$$\beta_1 + \beta_2 + \beta_3 = 3, \tag{1.6}$$

potom s ohľadom na predpoklad je množina {(3, 0, 0), (2, 1, 0), (2, 0, 1), (1, 2, 0), (0, 2, 1), (1, 1, 1)} množinou všetkých riešení rovnice (1.6). Z toho podľa vety 1.1 je každé z čísel 8, 12, 18, 20, 30, 45 deliteľom čísla 360 a každé z nich nazveme deliteľom stupňa 3 čísla 360. Množina

$$D_3 = \{8, 12, 18, 20, 30, 45\}$$

je množinou všetkých kladných deliteľov stupňa 3 čísla 360.

4) Ak

$$\beta_1 + \beta_2 + \beta_3 = 4, \tag{1.7}$$

potom podobne ako napr. v 3) nájdeme množinu

$$D_4 = \{24, 36, 40, 60, 90\}$$

všetkých kladných deliteľov stupňa 4 čísla 360.

5) Ak

$$\beta_1 + \beta_2 + \beta_3 = 5, \ (5 < \alpha = 6) \tag{1.8}$$

potom množina

$$D_5 = \{72, 120, 180\}$$

je množinou všetkých kladných deliteľov stupňa 5 čísla 360.

6) Ak

$$\beta_1 + \beta_2 + \beta_3 = 6,$$

potom množina

$$D_6 = \{360\}$$

je množinou všetkých kladných deliteľov čísla 360.

Položme $P(0, 6) = \{0, 1, 2, 3, 4, 5, 6\}$. Zrejme platí:

a) $D(360) = \cup\{D_i \mid i \in P(0, 6)\}$.

b) Pre každé $i, j \in P(0, 6)\}$, $i \neq j$ je $D_i \neq D_j$ a $D_i \cap D_j = \emptyset$.

(B) Pomocou tvrdení v (A) nájdeme sedem maximálnych nezávislých systémov hlavných ideálov pologrupy S_{360} zvyškových tried (mod 360).
Ku každému D_i, $i \in P(0, 6)$ priraďme systém hlavných ideálov $\mathscr{H}_i$ takto:

$$D_0 \to \mathscr{H}_0 = \{[\overline{1}]\}$$

$$D_1 \to \mathscr{H}_1 = \{[\overline{2}], [\overline{3}], [\overline{5}]\}$$

$$D_2 \to \mathscr{H}_2 = \{[\overline{4}], [\overline{6}], [\overline{9}], [\overline{10}], [\overline{15}]\}$$

$$D_3 \to \mathscr{H}_3 = \{[\overline{8}], [\overline{12}], [\overline{18}], [\overline{20}], [\overline{30}], [\overline{45}]\}$$

$$D_4 \to \mathscr{H}_4 = \{[\overline{24}], [\overline{36}], [\overline{40}], [\overline{60}], [\overline{90}]\}$$

$$D_5 \to \mathscr{H}_5 = \{[\overline{72}], [\overline{120}], [\overline{180}]\}$$

$$D_6 \to \mathscr{H}_6 = \{[\overline{0}]\}$$

(C) 1) Pomocou vety 1.2 sa ľahko ukáže, že pre každé $i \in P(0, 6)$ takto definované $\mathscr{H}_i$ v (B) je maximálny nezávislý systém hlavných ideálov pologrupy S_{360}.

2) Pre každé $i \in P(0, 6)$ označme H_i množinové zjednotenie všetkých prvkov maximálneho nezávislého systému $\mathscr{H}_i$ ideálov v S_{360}. Pre každé $i, j \in P(0, 6)$ položme $H_{ij} = H_i \cap H_j$. Potom sa dá dokázať, že platí nasledujúce tvrdenie:
α) Ak $H_i \neq H_j$, potom

a) buď $H_i \subset H_j$, alebo $H_j \subset H_i$

b) buď $H_{ij} = H_i$, alebo $H_{ij} = H_j$.

(D) Nech $m = p_1^{\alpha_1}\, p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ je kanonický rozklad celého čísla $m > 1$. Nech S_m je pologrupa zvyškových tried (mod m). Položme $\alpha = \alpha_1 + \alpha_2 + \ldots + \alpha_k$ a $P(0, \alpha) = \{0, 1, 2, \ldots, \alpha\}$.

1) Potom sa dá ukázať, že pologrupa S_m obsahuje $\alpha + 1$ maximálnych nezávislých systémov hlavných ideálov $\mathscr{H}_i$, $i \in P(0, \alpha)$.

2) Podobne ako v (C) 2), ak pre každé $i \in P(0, \alpha)$ je H_i množinovým zjednotením všetkých prvkov maximálneho nezávislého systému $\mathscr{H}_i$ ideálov v S_m a pre každé $i, j \in P(0, 6)$ je $H_{ij} = H_i \cap H_j$, potom platí tvrdenie α) uvedené v (C) 2).

Lema 2.1. Nech S_m je pologrupa zvyškových tried (mod m). Nech $\mathscr{H} = \{[b] \mid b \in B\}$ maximálny nezávislý systém hlavných ľavých ideálov v S_m. Nech $H = \cup\{[\overline{b}] \mid \overline{b} \in B\}$ a $B = \cup\{[\overline{b}]\mathscr{L} \mid \overline{b} \in B\}$. Potom

(a) H je podpologrupa (ideál) pologrupy v S_m.

(b) Pre každé $\overline{a} \in \overline{N(B)}_m$ platí: $[\overline{a}]\mathscr{L}$ je minimálny prvok $\overline{N(B)}_m / \mathscr{L}$ práve vtedy, ak $a \in B$.

(c) Pre každé $a \in H$ platí: $[a]\mathcal{L}$ je maximálny prvok v $H/\mathcal{L}$ práve vtedy, ak $a \in B$.

Dôkaz. Tvrdenie v (a) je zrejmé.

(b) I. Nech $[\bar{a}]\mathcal{L}$, $\bar{a} \in \overline{N(B)_m}$ je minimálny prvok v $\overline{N(B)_m}/\mathcal{L}$. Predpokladajme, že $a \notin B$. Potom $[\bar{a}]\mathcal{L} \cap B = \emptyset$ a podľa predpokladu existuje taký prvok $c \in B$, že platí $[\bar{c}]\mathcal{L} < [\bar{a}]\mathcal{L}$. Z toho vyplýva, že $[\bar{a}]\mathcal{L}$ nie je minimálny prvok $\overline{N(B)_m}/\mathcal{L}$. To je spor s predpokladom. Z predchádzajúceho vyplýva, že $\bar{a} \in B$.

II. Predpokladajme, že $\bar{a} \in B$ a $[\bar{a}]\mathcal{L}$ nie je minimálny prvok v $\overline{N(B)_m}/\mathcal{L}$. Potom podľa predpokladu existuje taký prvok $\bar{x} \in \overline{N(B)_m}$, že $[\bar{x}]\mathcal{L} < [\bar{a}]\mathcal{L}$ a taký prvok $b \in B$, že
$[\bar{b}]\mathcal{L} \leq [\bar{a}]\mathcal{L}$. Potom $[\bar{b}] \subset [\bar{a}]$. To je spor s tým, že podľa predpokladu $\{[\bar{b}] \mid [\bar{b}] \in B\}$ je maximálny nezávislý systém hlavných ideálov ($\bar{a}, \bar{b} \in B$).
Z úvah v I. a II. vyplýva pravdivosť tvrdenia v (b).

(c) I. Nech $\bar{a} \in H$ a $[\bar{a}]\mathcal{L}$ je maximálny prvok v $H/\mathcal{L}$ a $\bar{a} \notin B$. Potom podľa predpokladu existuje taký prvok $\bar{b} \in B$, že $\bar{a} \in [\bar{b}], \bar{b} \in B$. Podľa predpokladu $[\bar{a}]\mathcal{L} = [\bar{b}]\mathcal{L}$. Potom $\bar{a} \in [\bar{a}]\mathcal{L} = [\bar{b}]\mathcal{L} \subseteq B$, čo je v spore s predpokladom. Z toho vyplýva, že $\bar{a} \in [\bar{b}] \setminus [\bar{b}]\mathcal{L}$. Potom $[\bar{a}] \subset [\bar{b}]$ a teda $[\bar{a}]\mathcal{L} < [\bar{b}]\mathcal{L}$, čo je spor s predpokladom. Z predchádzajúceho vyplýva, že $\bar{a} \in B$.

II. Nech $\bar{b} \in B$ a $[\bar{b}]\mathcal{L}$ nie je maximálny prvok $H/\mathcal{L}$. Potom existuje taký prvok $\bar{x} \in H$, že $[\bar{b}]\mathcal{L} < [\bar{x}]\mathcal{L}$. Z toho podľa predpokladu dostaneme, že existuje taký prvok $\bar{d} \in B$, že $[\bar{x}]\mathcal{L} \leq [\bar{d}]\mathcal{L}$. Potom $[\bar{b}]\mathcal{L} < [\bar{d}]\mathcal{L}$ a teda $[\bar{b}] \subset [\bar{d}]$. To je spor s predpokladom. Z toho vyplýva, že pre každé $\bar{b} \in B$ je $[\bar{b}]\mathcal{L}$ maximálny prvok v $H/\mathcal{L}$.
Z úvah v častiach I. a II. vyplýva pravdivosť tvrdenia v (c).

Veta 2.1. Nech sú splnené predpoklady lemy 2.1. Potom:

(a) Pre každú podmnožinu $N \subseteq S_m$ a $N \neq \emptyset$ platí: N je minimálny ideál v S_m s ohľadom na B práve vtedy, ak $N = [\bar{b}]$, $b \in B$.

(b) N je maximálny ideál v S_m s ohľadom na B vtedy a len vtedy, ak $N = N(b)$, $b \in B$.

Dôkaz. Pravdivosť tvrdení v (a), (b) bezprostredne dostaneme pomocou vety 1.1, vety 1.2 a lemy 2.1.

Lema 2.2. Nech S_m, $m > 1$ je okruh zvyškových tried (mod m). Potom pre každé $d \in D(m)$ ($d \neq m$) platí: $[\bar{d}]$ je podokruh okruhu S_m.

Dôkaz. a) Zrejme platí, že $[\bar{d}]$ je multiplikatívna podpologrupa v S_m.

b) Ukážeme, že $[\bar{d}]$ je aditívna pologrupa s ohľadom na binárnu operáciu sčítania v okruhu S_m.

Nech $\bar{u}, \bar{v}$ sú ľubovoľné prvky v $[\bar{d}]$. Potom existujú také dva prvky $\bar{x}, \bar{y} \in S_m$, že $\bar{u} = \bar{d}\,\bar{x}$, $\bar{v} = \bar{d}\,\bar{y}$. Potom $\bar{u} + \bar{v} = \bar{d}\,\bar{x} + \bar{d}\,\bar{y} = \bar{d}(\bar{x} + \bar{y}) \in [\bar{d}]$.

Ďalej ukážeme, že ku každému prvku $\overline{u} \in [\overline{d}\,]$, existuje taký prvok $\overline{u'} \in [\overline{d}\,]$, že $\overline{u}+\overline{u'}=\overline{0}$. Nech $\overline{u} \in [\overline{d}\,]$. Potom existuje taký prvok $\overline{x} \in S_m$, že $\overline{u}=\overline{d}\,\overline{x}$. Je zrejmé, že existuje také číslo m_1, že $m=dm_1$. Potom $\overline{m}-\overline{u}=\overline{dm_1-dx}=\overline{d}\,(\overline{m_1-x}) \in [\overline{d}\,]$. Položme $\overline{u'}=\overline{m-u}$. Potom $\overline{u'}+\overline{u}=\overline{m-u}+\overline{u}=\overline{m}=\overline{0}$. Z predchádzajúcich úvah vyplýva pravdivosť tvrdenia v leme 2.2.

Definícia 2.3 Nech R je okruh a B neprázdna podmnožina okruhu R, $\overline{0} \notin B$, (0 je nulový prvok okruhu R). Ideál N okruhu R nazveme minimálnym ideálom s ohľadom na množinu B, ak $R \cap N = \emptyset$ a neexistuje taký ideál N_1 okruhu R, že $N_1 \cap B \neq \emptyset$ a $N_1 \subset N$.

Veta 2.2. Nech S_m je okruh zvyškových tried (mod m). Nech sú splnené predpoklady lemy 2.1. Potom platí: N je minimálny ideál okruhu S_m s ohľadom na B práve vtedy, ak $N = [\overline{b}\,]$, $\overline{b} \in B$.

Dôkaz. Pravdivosť tvrdenia vo vete 2.2 dostaneme bezprostredne pomocou tvrdení vo vete 2.1 a v leme 2.1.

Definícia 2.4 (pozri [10]). Hovoríme, že ľavý (pravý, obojstranný) ideál $L(R, N)$ pologrupy S je zakrytý ideál v S, ak $L \subset S(S \setminus L)$ ($R \subset (S \setminus R)S$), $N \subseteq S(S \setminus N)S$).

V práci [8] je znakom G_m označená množina všetkých takých prvkov $\overline{a} \in S_m$, pre ktoré je $(a, m) = 1$ a sú dokázané nasledujúce dve tvrdenia (a), (b) uvedené v nasledujúcej leme 2.3.

Lema 2.3 (pozri vetu 3.1 v [8]).

(a) $S_m \setminus G_m$ je maximálny ideál v S_m a pre každý ideál N pologrupy S_m a $N \neq S_m$ je $N \subseteq S_m \setminus G_m(b)$.

(b) Pre každé $d \in D(m)$ je $[\overline{d}\,]\,\mathscr{L} = G_m \overline{d}$.

Lema 2.4 (pozri [9]). Nech $\overline{b} \in S_m$ a $a \in G_m$. Potom rovnica $\overline{b}=\overline{x}\,\overline{a}$ má v S_m práve jedno riešenie.

Veta 2.2. Nech N je ideál pologrupy S_m a $N \neq S_m$. Potom N je zakrytý ideál v S_m.

Dôkaz. Pravdivosť tvrdenia vety 2.2 je bezprostredne dôsledkom tvrdení v leme 2.3 a leme 2.4.

3 Izomorfizmus hlavných ideálov $[\overline{d}\,]$ pologrupy S_m s pologrupami zvyškových tried v pologrupe $S_{\frac{m}{d}}$

Veta 3.1. Nech S_m, $m > 1$ je pologrupa zvyškových tried (mod m). Nech $d \in D(m)$ a nech $S_{\frac{m}{d}}$ je pologrupa zvyškových tried $\left(\operatorname{mod}\dfrac{m}{d}\right)$. Potom:

$$\left|S_{\frac{m}{d}}\right| = \left|[\bar{d}\,]\right|. \tag{3.1}$$

Dôkaz. Nech φ je zobrazenie $S_{\frac{m}{d}}$ do $[\bar{d}\,]$ ($[\bar{d}\,]$ je hlavný ideál v S_m generovaný prvkom $\bar{d} \in S_m$) definovaný takto:

Pre každé $\hat{x} \in S_{\frac{m}{d}}$ položme

$$\phi(\hat{x}) = \bar{x}\,\bar{d}\,. \tag{3.2}$$

a) Nech $x_1 \in \hat{x}$, t. j. $x_1 \equiv x\left(\bmod \dfrac{m}{d}\right)$.

Potom $x_1\,d \equiv x\,d$ (mod m) a teda $\overline{x_1\,d} = \overline{x\,d}$. Z toho dostávame, že zobrazenie φ: $S_{\frac{m}{d}} \to [\bar{d}\,]$ je zobrazenie množiny prvkov $S_{\frac{m}{d}}$ do množiny prvkov $[\bar{d}\,]$.

b) Nech $\hat{x}_1, \hat{x}_2 \in S_{\frac{m}{d}}$ a $\varphi(\hat{x}_1) = \varphi(\hat{x}_2)$. Potom $\overline{x_1\,d} = \overline{x_2\,d}$ a teda $x_1\,d \equiv x_2\,d\left(\bmod \dfrac{m}{d}d\right)$.

Z toho vyplýva, že $x_1 \equiv x_2\left(\bmod \dfrac{m}{d}\right)$, t. j. $\hat{x}_1 = \hat{x}_2$.

c) Nech $\bar{u} \in [\bar{d}\,]$. Potom existuje také $\bar{x} \in S_m$, že $\bar{u} = \bar{x}\,\bar{d}$, t. j. $u \equiv x\,d$ (mod m).

Potom $\dfrac{u}{d}d \equiv x\,d\left(\bmod \dfrac{m}{d}d\right)$ a teda $\dfrac{u}{d} \equiv x\left(\bmod \dfrac{m}{d}\right)$. Potom $\hat{x} = \dfrac{\hat{u}}{d}$

a $\varphi(\hat{x}) = \varphi\left(\dfrac{\hat{u}}{d}\right) = \dfrac{\bar{u}}{d}\cdot\bar{d} = \overline{\dfrac{u}{d}\cdot d} = \bar{u}$.

Z úvah v a), b) a c) vyplýva pravdivosť tvrdenia (3.1).

Veta 3.2. Nech $d \in D(m)$, $d \neq m$ a $[\bar{d}\,]\mathscr{L}$ je podgrupa pologrupy S_m. Potom pologrupa $S_{\frac{m}{d}}$ a hlavný ideál $[\bar{d}\,]$ pologrupy S_m generovaný prvkom $\bar{d} \in S_m$ sú navzájom izomorfné pologrupy.

Dôkaz. Znakom *e* označme jednotku podgrupy $[\bar{d}\,]\mathscr{L}$ pologrupy S_m. Potom podľa lemy 2.3 existuje taký prvok $\bar{a}$ podgrupy G_m (jej jednotkový prvok je 1) pologrupy S_m, že $e = \overline{d\,a}$.

Nech φ je zobrazenie pologrupy $S_{\frac{m}{d}}$ do S_m definované takto: Pre každé $\hat{x} \in S_{\frac{m}{d}}$ položme

$$\varphi(\hat{x}) \in \overline{x\,d\,a}\,. \tag{3.3}$$

a) Nech $\hat{x}$ je ľubovoľný prvok z $S_{\frac{m}{d}}$. Potom podľa (3.3) je

$$\varphi(\hat{x}) \in \overline{x\,d\,a} = \bar{x}\,\bar{d}\,\bar{a} = (\bar{x}\,\bar{a})\bar{d} \in [\bar{d}\,],$$

a teda zobrazenie φ: $S_{\frac{m}{d}}$ do S_m takto definované (3.3) je zobrazenie $S_{\frac{m}{d}}$ do $[\bar{d}]$.

Nech $\hat{x}$ je ľubovoľný prvok $S_{\frac{m}{d}}$ a nech $x_1 \in \hat{x}$. Potom $x_1 \equiv x\left(\bmod \dfrac{m}{d}\right)$, a ďalej platí $x_1\, d \equiv x\, d$ (mod m), $x_1\, d\, a = x\, d\, a$ (mod m), a teda $\overline{x_1\, d\, a} = \overline{x\, d\, a}$. Z toho vyplýva, že zobrazenie definované v (3.3) je zobrazením prvkov množiny S_m do prvkov množiny $[\bar{d}]$.

b) Nech $\hat{x}_1, \hat{x}_2 \in S_{\frac{m}{d}}$ a nech $\varphi(\hat{x}_1) = \varphi(\hat{x}_2)$. Potom $\overline{x_1\, d\, a} \equiv \overline{x_2\, d\, a}$, a ďalej platí $x_1\, d = x_2\, d$ (mod m), a teda $x_1\, d \equiv x_2\, d\left(\bmod \dfrac{m}{d} d\right)$. Potom $x_1 \equiv x_2\left(\bmod \dfrac{m}{d}\right)$ a teda $\hat{x}_1 \equiv \hat{x}_2$.

c) Nech $\bar{u} \in [\bar{d}]$. Ukážeme, že platí: existuje také $\hat{x} \in S_{\frac{m}{d}}$, že

$$\bar{u} = \overline{x\, d\, a}\,. \tag{3.4}$$

Potom $u \equiv x\, d\, a$ (mod m) a $\dfrac{u}{d} d = x\, d\, a \left(\bmod \dfrac{m}{d} d\right)$. Potom $\dfrac{u}{d} = x\, a\left(\bmod \dfrac{m}{d}\right)$, z čoho $\left(\dfrac{\hat{u}}{d}\right) = \hat{x}\,\hat{a}$, a teda $\hat{x} = \left(\dfrac{\hat{u}}{d}\right)\hat{a}^{-1}$.

$$\phi(\hat{x}) = \left(\frac{\bar{u}}{d}\right)\bar{a}^{-1}\bar{d}\,\bar{a} = \left(\frac{\bar{u}}{d}\right)\bar{d}\,\bar{a}^{-1}\,\bar{a} = \overline{\frac{u}{d}\, d}\cdot \bar{1} = \bar{u}\,.$$

d) Nech $\hat{x}_1, \hat{x}_2 \in S_{\frac{m}{d}}$. Potom

$$\varphi(\hat{x}_1)\,\varphi(\hat{x}_2) = (\overline{x_1\, d\, a})(\overline{x_2\, d\, a}) = \overline{x_1\, x_2}(\overline{d\, a}) = \overline{(x_1 x_2)\, d\, a} = \varphi(\widehat{x_1 x_2})$$

(lebo $\bar{d}\,\bar{a} = e$ je jednotkový prvok v $[\bar{d}]$).
Z predchádzajúceho vyplýva pravdivosť tvrdenia vo vete 3.1.

Dôsledok 3.1. Nech $d \in D(m)$, $d \neq m$ a $[\bar{d}]\mathscr{L}$ je podgrupa v S_m. Potom okruh $S_{\frac{m}{d}}$ a podokruh $[\bar{d}]$ okruhu S_m sú navzájom izomorfné.

Dôkaz. V dôkaze vety 3.1 je ukázané, že zobrazenie φ: $S_{\frac{m}{d}}$ do S_m definované v dôkaze vety 3.1 vzťahom (3.3) je izomorfné zobrazenie multiplikatívnej pologrupy okruhu $S_{\frac{m}{d}}$ na multiplikatívnu pologrupu podokruhu $[\bar{d}]$ okruhu S_m (podľa lemy 2.2 je $[\bar{d}]$ podokruh okruhu S_m). Stačí teda dokázať, že takto definované zobrazenie φ: $S_{\frac{m}{d}} \to S_m$ je aj izomorfizmus aditívnej pologrupy okruhu $S_{\frac{m}{d}}$ na aditívnu podpologrupu podokruhu $[\bar{d}]$ okruhu S_m.

Nech $\hat{x}_1, \hat{x}_2 \in S_{\frac{m}{d}}$. Potom:

$$\varphi(\hat{x}+\hat{y}) = \varphi(x\hat{+}y) = \overline{(x+y)\,d\,a} = \overline{x\,d\,a} + \overline{y\,d\,a} = \varphi(\hat{x}) + \varphi(\hat{y})\,.$$

Z predchádzajúcich úvach vyplýva pravdivosť tvrdenia v dôsledku 3.1.

4 Lokálna Eulerova – Fermatova veta

Nakoniec v tejto práci ukážeme, že lokálna Eulerova-Fermatova veta je (bezprostredným) dôsledkom vety 2.9 publikovanej v práci [8].

Pod pojmom pologrupa S budeme v ďalšom rozumieť konečnú pologrupu.

Predovšetkým uvedieme definície pojmov a tvrdenia (známe) o týchto pojmoch, ktoré sú pravdivé pre konečné pologupy a budeme sa na ne v ďalšom odvolávať (pozri napr. [8], [14], [17]).

(A) (a) Znakom $E(S)$ budeme označovať množinu všetkých idempodentov pologrupy S.

(b) Budeme hovoriť, že prvok $x \in S$ patrí prvku $e \in E(S)$, ak existuje také prirodzené číslo ρ, že $x^{\rho} = e$.

(c) Znakom $P(e)$ budeme označovať množinu všetkých prvkov pologrupy S, ktoré patria prvku $e \in E(S)$.

Platia nasledujúce tvrdenia:

(d) Ak S je komutatívna pologrupa, potom pre každý prvok $e \in E(S)$ existuje práve jedna $P(e)$, a každá podgrupa P' pologrupy S taká, že $P' \neq P(e)$, nie je množinou všetkých prvkov patriacich $e \in E(S)$. V tomto prípade podpologrupu $P(e)$ pologrupy S budeme nazývať maximálnou podpologrupou patriacou prvku $e \in E(S)$.

(e) Pre každé $e_1, e_2 \in E(S)$ a $e_1 \neq e_2$ je $P(e_1) \cap P(e_2) = \emptyset$.

(f) $S = \cup\{P(e) \mid e \in E(S)\}$.

(g) Pre každé $a \in S$ platí: $a \in E(S)$ práve vtedy, ak existuje také $d \in D(m)$, že $a \in [\bar{d}]\mathscr{L}$ a $[\bar{d}]\mathscr{L}$ je podgrupa pologrupy S (a je jej jednotkou). Ak $[\bar{d}]\mathscr{L}$, $d \in D(m)$ podgrupa pologrupy S a $e \in E(S)$ je jej jednotkový prvok, potom $[\bar{d}]\mathscr{L}$ budeme označovať $G(e)$, t.j. $[d]\mathscr{L} = G(e)$.

(h) $G(e) \subseteq P(e)$.

(i) $m = p_1^{\alpha_1}\, p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ je kanonický rozklad celého čísla $m > 1$. Znakom $\alpha(m)$ označme $\max\{\alpha_1, \alpha_2, \ldots, \alpha_k\}$.

(j) Pre každý prvok $x \in S$:

α) existuje také $e \in E(S)$, že $x \in P(e)$,
β) $x^{\alpha(m)} \in G(e)$.

(B) V práci [8] je dokázaná veta:

Veta 4.1 (pozri vetu 2.9 v [8]). Nech $d \in D(m)$, $d \neq m$. Nech $[d]\mathscr{L}$ je podgrupa pologrupy S_m a e je jej jednotkový prvok, t. j. $[d]\mathscr{L} = G(e)$. Potom pre každé $a \in [d]\mathscr{L}$ platí:

$$a^{\varphi\left(\frac{m}{d}\right)} = e \,(\mathrm{mod}\ m).$$

Veta 4.2 (lokálna Eulerova-Fermatova veta). Nech $\bar{x} \in S_m$. Potom existuje také $e \in E(S)$ a také $d \in D(m)$, že $\bar{x} \in P(e)$, $[\bar{d}]\mathscr{L}$ je podgrupa pologrupy S_m, e je jej jednotkový prvok a platí:

$$x^{\alpha(m)\varphi\left(\frac{m}{d}\right)+\alpha(m)} = x^{\alpha(m)} \,(\mathrm{mod}\ m).$$

Dôkaz. Nech $\bar{x} \in S$. Potom podľa tvrdení α) a β) v (*j*) existuje také $\bar{e} \in E(S)$, že $x \in P(\bar{e})$ a $x^{\alpha(m)} \in G(\bar{e})$. Potom podľa tvrdenia a (g) existuje také $d \in D(m)$, že $e \in [\bar{d}]$ $\mathscr{L}$, $[\bar{d}]$ je podgrupa a e je jej jednotkový prvok. Z predchádzajúceho podľa vety 4.1 dostaneme, že platí:

$$(x^{\alpha(m)})^{\varphi\left(\frac{m}{d}\right)} = e \,(\mathrm{mod}\ m).$$

Potom

$$(x^{\alpha(m)})^{\varphi\left(\frac{m}{d}\right)} x^{\alpha(m)} = e\, x^{\alpha(m)} \,(\mathrm{mod}\ m)$$

a teda

$$x^{\alpha(m)\varphi\left(\frac{m}{d}\right)+\alpha(m)} = x^{\alpha(m)} \,(\mathrm{mod}\ m),$$

čo bolo treba dokázať.

Záver

V prvej časti práce je definovaný nezávislý (maximálny nezávislý) systém hlavných ideálov pologrupy S_m zvyškových tried (mod m).

Na príklade pologrupy S_{360} zvyškových tried (mod 360) je ukázané ako pomocou množiny všetkých kladných deliteľov čísla 360 nájdeme 6 rôznych maximálnych nezávislých systémov hlavných ideálov v S_{360}.

Pomocou maximálnych nezávislých systémov hlavných ideálov v S_m sú definované podmnožiny (B) v S_m. Dokázané sú nutné a postačujúce podmienky k tomu, aby ideál v pologrupe S_m bol minimálnym (maximálnym) s ohľadom na takto definovanú podmnožinu (B) v S_m (pozri lemu 2.1 a vetu 2.1).

Ďalej je dokázaná nutná a postačujúca podmienka k tomu, aby ideál v N okruhu S_m bol minimálnym s ohľadom na takto definovanú podmnožinu (B) v okruhu S_m (pozri vetu 2.2). Nakoniec je v prvej časti práce je definovaný zakrytý ľavý (pravý, obojstranný) ideál pologrupy S (pozri definíciu 2.4) a je dokázané nasledujúce tvrdenie (pozri vetu 2.3): Každý vlastný ideál v S_m je zakrytý.

V druhej časti práce sú dokázané nasledujúce základné tvrdenia: veta 3.1, veta 3.2 a dôsledok 3.1 vety 3.2.

V tretej časti tejto práce je ukázané, že lokálna Eulerova-Fermatova veta (jej istý tvar – veta 4.2) je bezprostredným dôsledkom (vzhľadom na dokázané tvrdenia uvedené v úvode (A)) vety 2.9 uvedenej v práci [8].

Literatúra

[1] ABRHAN, I. Poznámka k maximálnym (H_1, H_2) ideálom v pologrupách. In *Matematický časopis 21*, 1971, str. 214-218.

[2] ABRHAN, I. On minimal ideals in semigroups with respect to their subsets, I. In *Math. Bohemica*, 122, 1997, No.1, str. 1-12.

[3] ABRHAN, I. On minimal ideals in semigroups with respect to their subsets, II. In *Math. Slovaca*, 44, 1994, No.4, str. 463-478.

[4] ABRHAN, I. O minimálnych ideáloch v pologrupách s ohľadom na ich podmnožiny, III. In *G-slovenský časopis pre geometriu a grafiku č. 17*, *roč.9*, Bratislava: 2012. ISSN 1336-524X, str. 5-26.

[5] ABRHAN, I. O ϑ–подалгебрах в унарных алгебрах, о простых идеалах и ϑ–идеалах в групоидах и подпологрупах. In *Math. Slovaca 28*, 1978, str. 61-80.

[6] ABRHAN, I. O максималных подалгебрах в унарных алгебрах. In *Matematický časopis 24*, 1974, str. 113-128.

[7] ABRHAN, I. O minimálnych a maximálnych podalgebrách v unárnych algebrách s ohľadom na ich podmnožiny. In *G – slovenský časopis pre geometriu a grafiku č. 8, roč.4*, Bratislava: 2007. ISSN 1336-524X, str. 5-20.

[8] ABRHAN, I. O простых идеалах в групоидах и в мултипликативных полугруппах класов вычетов (mod m). In *Math. Slovaca 34*, 1984,No.2, str. 121-133.

[9] БУХШТАБ, А. А. Теория чисел. Гос. ин. – пед. Изд., Москва 1960.

[10] FABRICI, I., MACKO, T. On bases and maximal ideals in semigroups. In *Math. Slovaca 31*, 1981, str. 115-120.

[11] GRILET, P. A. Intersection of maximal ideals in semigroups. In *Amer. Math. Monthly 76*, 1969, str. 503-509.

[12] CLIFFORD, A. H., PRESTON, G. B. *The Algebric Theory of Semigroups*. Vol. I; Vol. II, Amer. Math. Soc. Providence, R. I., 1961.

[13] ЛАПИН, Е. С. Полугруппы. Наука, Москва 1960.

[14] PARIZEK, B., SCHWARZ, Š. O multiplikatívnej pologrupe zvyškových tried (mod *m*). In *Mat.-Fyz. čas. 1958. Str. 136-150.*

[15] PARIZEK, B. Poznámka o štruktúre multiplikatívnej pologrupy zvyškových tried. In *Mat.-Fyz. čas.* Vol. 7 (1957). No.3, str. 183-185.

[16] SCHWARZ, Š. К теории периодических полугрупп. In *Czechoslovak Math. J. 3*, 78, 1953, pp. 7-21.

[17] SCHWARZ, Š. The role of semigroups in the elementary theory of numbers. In *Math. Slovaca*, Vol. 31, 1981, No.4, pp. 369-395.

[18] PARIZEK, B. O rozklade pologrupy zvyškov (mod *m*) na direktný súčin. In *Mat.-Fyz. čas.* 1960, str. 18-29.

[19] CORDES, C. M. Permutations mod *m* in form *X*. In *Amer. Math. Monthly 83,* 1976, pp. 32-33.

[20] HEWITT, E., ZUCKERMAN, H. S. The multiplicative semigroup of integer (mod *m*). In *Pacific J. Math. 10,* 1960, pp. 1291-1308.

[21] LIVINGSTON, A. E., LIVINGSTON, M. L. The congruence (mod *m*). In *Amer. Math. Monthly 85,* 1978, pp. 97-100.

[22] SINGMASTER, D. A maximal generalization of Fermat's theorem. In *Math. Mag. 39*, 1966, pp. 103-107.

[23] SMALL, CH. Powers mod *m*. In *Math. Mag. 50,* 1977, pp. 84-86.

[24] ZANE, B. Uniform distribution (mod *m*) of monomials. In *Amer. Math. Monthly 71,* 1964, pp. 162-164.

[25] MORGANO, J. A property of the Euler φ-function concerning the integers which are regular (mod *m*). In *Portugal. Math.,* 1978, pp. 97-100.

doc. RNDr. Imrich Abrhan, CSc.
Silvánska 11, 841 04 Bratislava, SR

Rational minimal surfaces tangent to E. MÜLLER's surface

Boris Odehnal

Abstrakt
V článku sa zaoberáme novou triedou minimálnych plôch, ktoré sa dotýkajú istej špeciálnej kubickej plochy. Ukážeme, že tieto minimálne plochy možno racionálne parametrizovať, a že sú nositeľkami jednoparametrickej triedy kriviek harmonickej oscilácie vyššieho rádu. Každá z týchto minimálnych plôch definuje svoju vlastnú jednoparametrickú triedu asociovaných minimálnych plôch, ktoré sú všetky algebraickými plochami a dajú sa tiež racionálne parametrizovať.

Kľúčové slová: Minimálna ploha, algebraická plocha, racionálna parametrizácia, polynomická parametrizácia, Björlingov vzorec.

Abstract
We study a new class of minimal surfaces which are in line contact with a special cubic surface. It turns out that these minimal surfaces admit rational parametrizations and carry a one-parameter family of higher order harmonic oscillation curves. Each of these minimal surfaces defines its own one-parameter family of associated minimal surfaces which in turn are all algebraic. Moreover, they also admit rational parametrizations.

Keywords: Minimal surface, algebraic surface, rational parametrization, polynomial parametrization, Björling formula.

MSC 2010: 53A10, 53A99, 53C42, 49Q05, 14J26, 14Mxx

1 Introduction

Algebraic and especially rationally parametrizable minimal surfaces gained less attention in the last years. Though the advantages of rational parametrizations for applications in CAD and CAGD are clearly visible, high degrees and the highly complicated generation of such minimal surfaces may be a reason for the absence of research in this field. Only older literature provides some general results on algebraic minimal surfaces, see [3, 5, 10, 13]. Recently, this topic was picked up in [6] where a rational minimal Möbius strip was studied. In [7], some further new classes of algebraic minimal surfaces were discovered. These surfaces allow rational parametrization, are of relatively low degree, and a huge variety of algebraic properties which were at least known to S. LIE and H.A. SCHWARZ (see [3, 10]) could be verified.

Rational or even polynomial parametrizations of minimal surfaces can be found with help of the various Weierstraß-representations or the Björling formula (also due to WEIERSTRASS), see [1, 2, 5, 8, 13]. In the following, we will use the Björling formula in order to construct rational minimal surfaces on scrolls. The initial (boundary) data shall be taken from a special cubic surface. Until now, useful initial data that yields rational parametrizations of minimal surfaces is found just by chance.

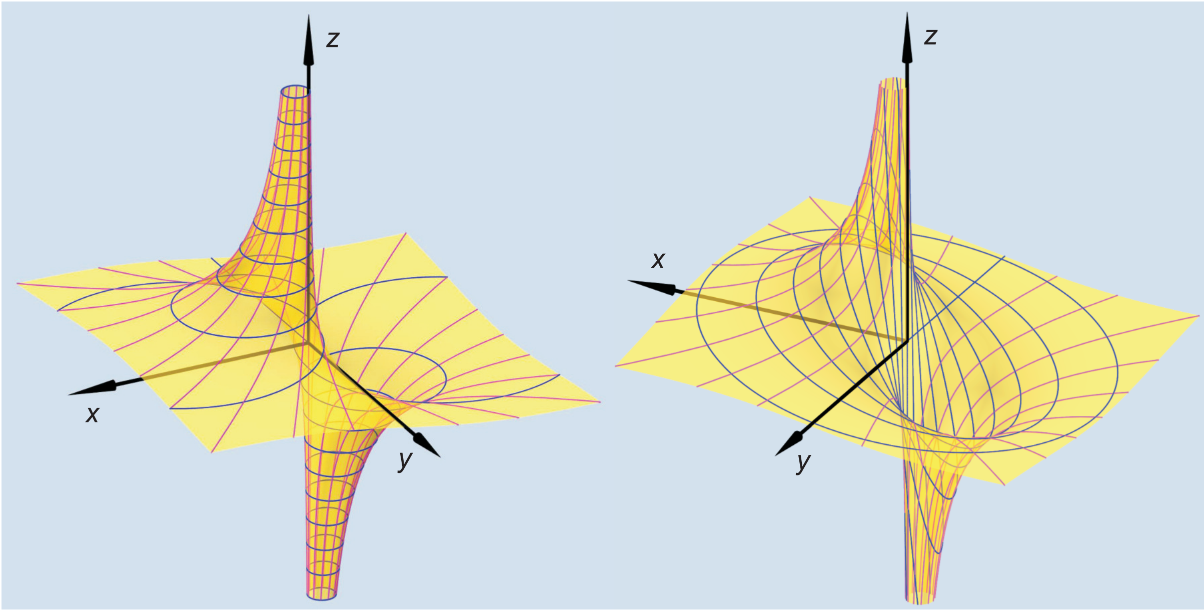


Fig. 1. Left: MÜLLER's surface with its circles and hyperbolae. Right: Ellipses on MÜLLER's surface.

The cubic surfaces that deliver the initial data in the present case are spheres in some sense. Together with the planes in the projectively and complex extended Euclidean three-space they form a set of surfaces that is invariant under a group of transformations generated by special birational cubic transformations, called *axial inversions*. In [4], such inversions transforming points with coordinates (x, y, z) to points with coordinates (x', y', z') were studied in the projective extension of Euclidean three-space. A special version reads

$$x' = \frac{x}{x^2 + y^2}, \quad y' = \frac{y}{x^2 + y^2}, \quad z' = z$$

and maps planes $ax + by + cz + d = 0$ with $a, b, c, d \in \mathbb{R}$ and $a : b : c \neq 0 : 0 : 0$ to a special kind of cubic surfaces with the equations

$$ax + by + (cz + d)(x^2 + y^2) = 0,$$

and *vice versa*. (For the sake of simplicity, we have written x, y, and z instead of x', y', and z'.) These cubics carry three one-parameter families of conics which are the intersections with the planes in the pencils $\lambda(ax + by) + \mu(cz + d) = 0$, $\lambda z + \mu = 0$, and $\lambda x + \mu y = 0$ with $(\lambda, \mu) \in \mathbb{R}^2 \setminus \{(0, 0)\}$.

The contour lines (horizontal curves on the surface) are circles that appear as the members of a parabolic pencil of circles in a top-view, i.e., in an orthogonal projection in the direction of the lead which is henceforth assumed to be parallel to the z-axis of the underlying Cartesian coordinate system.

The curves of steepest ascent (with respect to the vertical lead) are upright cubic circles, i.e., rational cubic curves on right cylinders. The top-views of the curves of steepest ascent constitute the parabolic pencil of circles that is complementary (and thus, orthogonal) to the one previously mentioned.

In the following, we pay our attention to the special surface that we obtain if we let $a = c = 1$ and $b = d = 0$. This particular surface is the image of the plane $x - z = 0$ under the axial inversion and has the equation

$$x - (x^2 + y^2)z = 0 \tag{1}$$

and was first studied in [12].

Obviously, this surface allows two different parametrizations over nearly the same parameter domain $D = \mathbb{R}^\star \times [0, 2\pi[$

$$\left(\frac{r}{2}(1+\cos u), \frac{r}{2}\sin u, \frac{1}{r}\right), \quad (r, u) \in D, \tag{2}$$

or a seemingly simpler version

$$\left(q\cos t, q\sin t, \frac{\cos t}{q}\right), \quad (q, t) \in D. \tag{3}$$

In (2), the parameter curves are the circles in the pencil of planes $z = c$ (with $c \in \mathbb{R}^\star$) and the hyperbolae in the pencil of planes $\lambda x + \mu y = 0$ (with $\lambda : \mu \neq 0 : 0$), see Figure 1 (left). In (3), the parameter curves are the ellipses (different from circles) in the pencil of planes $\lambda x + \mu z = 0$ (with $\lambda : \mu \neq 0 : 0$) and the previously mentioned hyperbolae (see Figure 1, right). The ellipses in the pencil of planes $\lambda x + \mu z = 0$ through the y-axis are given by $q = \mathrm{const.}$ in (3).

MÜLLER's surface (1) has three singular points: the pair of absolute points of Euclidean geometry in the plane $z = 0$ with homogeneous coordinates $(0 : 1 : \pm\mathbf{i} : 0)$ and the ideal point of the z-axis with homogeneous coordinates $(0 : 0 : 0 : 1)$.

This particular cubic surface contains three real lines: the y-axis, the z-axis, and the ideal line of all planes parallel to $z = 0$.

For any fixed $q \in \mathbb{R}^\star$, the ellipses parametrized by (3) carry only regular surface points. Along such an ellipse, the surface normals of the cubic surface (1) are parallel to

$$\nu(t) = \frac{1}{\sqrt{1+q^4}}(\cos 2t, \sin 2t, q^2) \tag{4}$$

and determine a regular and non-torsal algebraic ruled surface of degree six; an example of which is shown in Fig. 2. For any fixed $q \in \mathbb{R}^\star$, the parametrization (3) gives the parametrization

$$\gamma(t) = \left(q\cos t, q\sin t, \frac{\cos t}{q}\right) \tag{5}$$

of an ellipse. The pair (γ, ν) defines a *scroll* as the envelope of the one-parameter family of planes $\langle \mathbf{x} - \gamma, \nu \rangle = 0$.

2 The minimal surfaces

We use the scroll (γ, ν) as the initial (boundary) data for a minimal surface. Following [2, 3, 5, 8, 13], we can use the Björling formula in order to derive a real parametrization of the unique

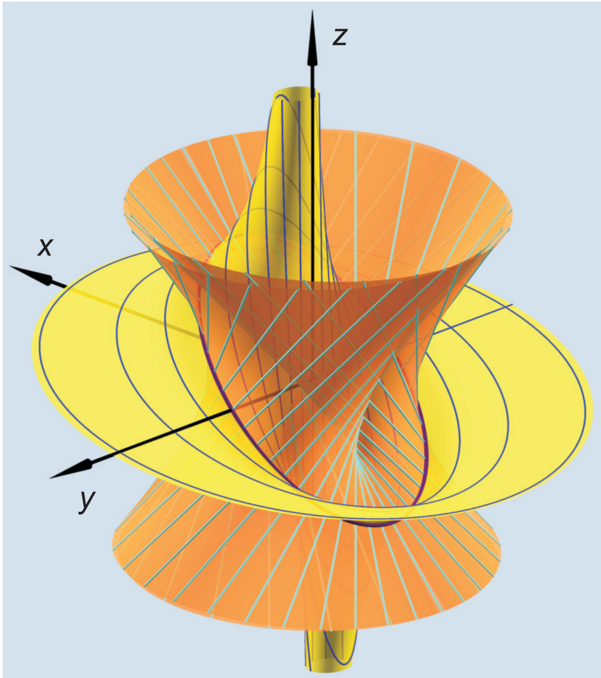


Fig. 2. The sextic ruled surface of normals along an ellipse.

real minimal surface on the scroll (γ,ν), i.e., the uniquely determined real minimal surface through the curve γ with normals parallel to ν along γ. For that we assume that we are given a curve $\gamma:\ I\subset\mathbb{R}\to\mathbb{R}^3$ and a unit vector field $\nu:\ I\to\mathrm{S}^2$ along γ. Both are considered to have complex continuations. Then, the Björling formula

$$\varphi(t)=\gamma(t)-\mathbf{i}\int_{t_0}^{t}\nu\times\mathrm{d}\gamma \tag{6}$$

yields a parametrization of an isotropic curve, i.e., a curve of constant slope $\pm\mathbf{i}$ whose tangents are isotropic lines in Euclidean three-space. The existence of the complex continuation of the curve and the unit normal vector field allows us to set $t=u+\mathbf{i}v$. Then, we extract the real part of the vector function $\varphi(t)$ and obtain a real parametrization

$$\mathbf{f}(u,v)=\mathfrak{Re}\,\varphi(t) \tag{7}$$

of the uniquely defined real minimal surface on the scroll (γ,ν).

With the spine curve γ given in (5) and the unit normal vector field ν described by (4), we can derive the parametrization(s) of the minimal surfaces tangent to MÜLLER's cubic surface. We use shorthand

$$c_x:=\cos x,\quad s_x:=\sin x,\dots,C_x:=\cosh x,\quad S_x:=\sinh x,\dots$$

together with the abbreviation $p:=\sqrt{1+q^4}$ and state:

Theorem 2.1. The one-parameter family of minimal surfaces touching MÜLLER's surface (1) along the ellipses (3) can be parametrized over $\mathbb{R}^2$ by

$$\mathbf{f}(u,v)=\frac{1}{6pq}\begin{pmatrix}6pq^2c_uC_v-3(p^2+q^4)c_uS_v+c_{3u}S_{3v}\\ 6pq^2s_uC_v-3(p^2+q^4)s_uS_v+s_{3u}S_{3v}\\ 6c_u(S_vq^2+pC_v)\end{pmatrix}. \tag{8}$$

Proof. We insert (5) and (4) into (6) and find the parametrization of the isotropic curve $\varphi:\ \mathbb{R}^3\to\mathbb{R}^3$

$$\varphi(t)=\frac{1}{6pq}\begin{pmatrix}6pq^2c_t+3\mathbf{i}(p^2+q^4)s_t-\mathbf{i}s_{3t}\\ 6pq^2s_t-3\mathbf{i}(p^2+q^4)c_t+\mathbf{i}c_{3t}\\ 6(pc_t-\mathbf{i}q^2s_t)\end{pmatrix}\tag{9}$$

depending on the complex parameter t. Then, we replace t by $u+\mathbf{i}v$ and extract the real part and obtain (8). □

Figure 3 shows one particular minimal surface mentioned in Thm. 2.1.

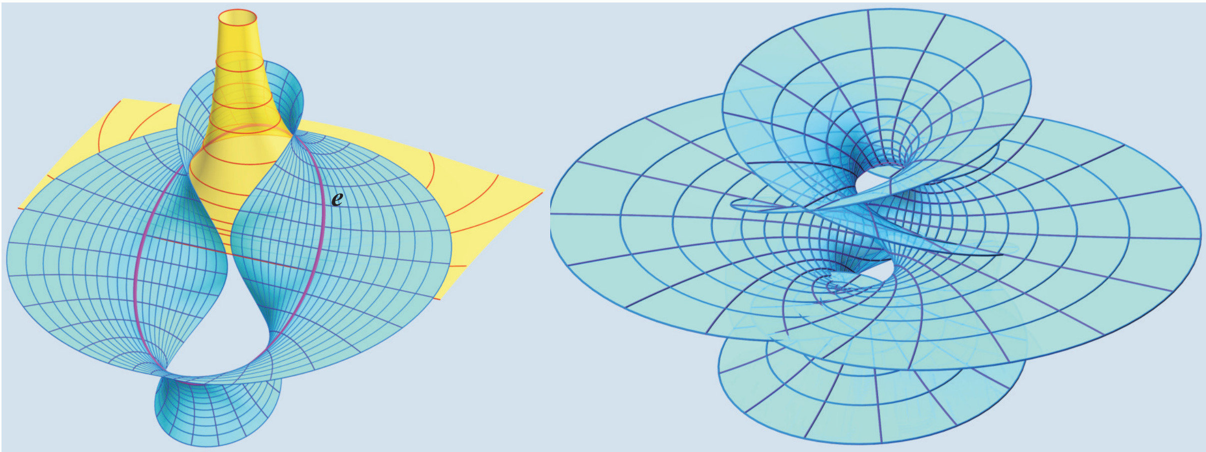


Fig. 3. A minimal surface tangent to MÜLLER's surface along the ellipse e.

The curves $v=$ const. on the minimal surface have a very special shape:

Theorem 2.2. The u-curves (the curves with $v=$ const.) on the minimal surfaces (8) are harmonic oscillation curves and appear as cycloidal curves in the top-view (orthogonal projection onto the $[xy]$-plane).

Proof. We use the first and second coordinate function of $\mathbf{f}=(\mathbf{f}^1,\mathbf{f}^2,\mathbf{f}^3)$ from (8) and build the complex variable $w(t)=\mathbf{f}^1+\mathbf{i}\mathbf{f}^2$ which reads in full length

$$\begin{aligned}w(t)&=qc_uC_v-\tfrac{1}{2pq}(p^2+q^4)c_uS_v+\tfrac{1}{6pq}c_{3u}S_{3v}+\\&\quad+\mathbf{i}\left(qs_uC_v-\tfrac{1}{2pq}(p^2+q^4)s_uS_v+\tfrac{1}{6pq}s_{3u}S_{3v}\right).\end{aligned}$$

With EULER's formula, the latter simplifies to

$$w(t)=\left(qC_v-\frac{p^2+q^2}{2pq}S_v\right)\mathrm{e}^{\mathbf{i}u}+\frac{1}{6pq}S_{3v}\mathrm{e}^{3\mathbf{i}u}$$

which is a parameter representation of family of cycloidal curves according to [14, 15], because $v=$ const., and thus, S_v, C_v, S_{3v}, and C_{3v} are constant. Since $\mathbf{f}^3=c_u\left(\frac{p}{q}S_v+\frac{1}{q}C_v\right)$ is a harmonic function as long as $v=$ const., the u-curves are harmonic oscillation curves as defined in [9]. □

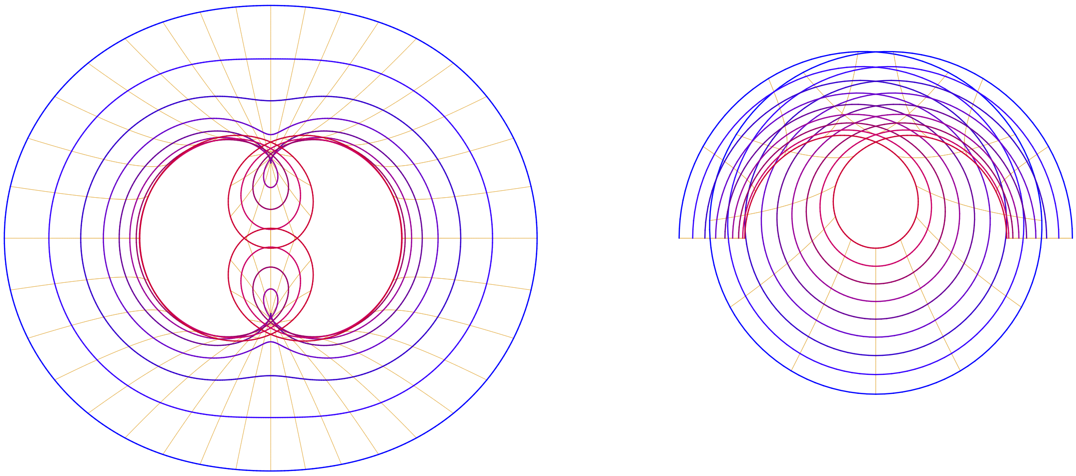


Fig. 4. The top-views of the u-curves on the minimal surfaces are cycloidal curves: $q \in [0.6, 1.2]$ (left), only one half of the curves for $q \in [1.0, 1.4]$ (right).

Figure 4 shows the top-views of some of the harmonic oscillation curves on the minimal surfaces given in (8).

According to WEIERSTRASS, the minimal surface (8) can be generated from two meromorphic functions $A, B: D \subset \mathbb{C} \to \mathbb{C}$ by computing

$$\varphi(t) = \int \begin{pmatrix} A(1-B^2) \\ \mathbf{i}A(1+B^2) \\ 2AB \end{pmatrix} \mathrm{d}t, \tag{10}$$

see, e.g., [1, 2, 3, 5, 8, 13]. Subsequently, we let $t = u + \mathbf{i}v$ and extract the real part $\mathbf{f}(u,v) = \mathfrak{Re}(\varphi)$ in order to obtain a real parametrization of the thus defined real minimal surface. We can state and prove:

Theorem 2.3. The meromorphic functions $A, B: D \subset \mathbb{C} \to \mathbb{C}$ from the representation (10) of the minimal surfaces (8) tangent to Müller's surface read

$$A = \frac{\mathbf{i}}{4pq}((p-q^2)^2 \mathrm{e}^{-\mathbf{i}w} - \mathrm{e}^{-3\mathbf{i}w}), \quad B = \frac{\mathrm{e}^{2\mathbf{i}w}(p-q^2)-(p+q^2)}{(p-q^2)^2 - \mathrm{e}^{-2\mathbf{i}w}}. \tag{11}$$

Proof. Following [1, 2, 3, 5, 8, 13], we compute $\mathbf{F} = (\mathbf{F}^1, \mathbf{F}^2, \mathbf{F}^3) := \partial_u \mathbf{f} - \mathbf{i}\partial_v \mathbf{f}$. Then, $A = \frac{1}{2}(\mathbf{F}^1 - \mathbf{i}\mathbf{F}^2)$ and $B = A/2\mathbf{F}^3$ and we end up with (11). □

The meromorphic functions A and B given in Thm. 2.3 can be replaced by rational functions. This is equivalent to a reparametrization of the isotropic curve φ given in (10). The parametrization of the minimal surface obtained from the reparametrized isotropic curve will in general not be the same, but an equivalent one. We let $\omega = \mathrm{e}^{-\mathbf{i}w}$ and arrive at the following rational equivalents to A and B:

$$\widetilde{A} = \frac{\mathbf{i}}{4pq}\left((p-q^2)^2 - \omega^2\right)\omega, \quad \widetilde{B} = \frac{(p-q^2) - (p+q^2)\omega^2}{\left((p-q^2)^2 - \omega^2\right)\omega^2}.$$

A closer look at the parametrization (8) makes clear that the parameter u appears only as argument of trigonometric functions, whereas v shows up only as argument of hyperbolic functions. Thus, it is obvious that a reparametrization can turn (8) into a rational parametrization. Moreover, we can show:

Theorem 2.4. The minimal surfaces (8) that touch MÜLLER's surface along ellipses admit rational parametrizations and are algebraic minimal surfaces of degree 24 and class 42.

Proof. The existence of a rational parametrization is confirmed by simply substituting the rational equivalents

$$c_u = \frac{1-U^2}{1+U^2},\ s_u = \frac{2U}{1+U^2},\ C_v = \frac{1+V^2}{1-V^2},\ S_v = \frac{2V}{1-V^2}$$

of the trigonometric and hyperbolic functions into (8). This yields a rational parametrization of bi-degree (6,6) in U and V which can be rewritten in terms of rational Bézier functions.

From the rational parametrization, the implicit algebraic equation can be found (more or less) easily by eliminating U and V. This results in a polynomial of degree 24.

The class of these surfaces has to be even, for these algebraic minimal surfaces are orientable, cf. [3]. The algebraic degree of $\varphi(t)$ equals 6 and its rank equals $r = 10$. The absolute conic of Euclidean geometry is a three-fold curve on the tangent developable of φ, i.e., its multiplicity on the developable is $m = 3$. According to [3], the class of the minimal surface swept by φ and its conjugate equals $c = 2m(r-m) = 42$. □

The rational parametrization mentioned in Thm. 2.4 can easily be converted into a rational Bézier representation. Figure 5 shows a part of a minimal surface described in Thm. (2.1) with its control structure.

The following fact is worth to be noted and elementary to verify:

Lemma 2.1. The curves of constant Gaussian curvature on MÜLLER's surface are the ellipses given in (3) with $q \in \mathbb{R}^\star$.

Proof. From (3) we compute the Gaussian curvature function on MÜLLER's surface and arive at

$$K(q,t) = -\frac{4q^2}{(1+q^4)^2}$$

which is obviously independent of t, and thus, constant along each ellipse for the corresponding fixed $q \in \mathbb{R}^\star$. □

As a consequence of Lemma 2.1 and Theorem 2.1, we can formulate

Theorem 2.5. The minimal surfaces (8) touching MÜLLER's surface (1) along the ellipses (3) agree with the minimal surfaces that touch MÜLLER's surface (1) along the curves of constant Gaussian curvature.

A similar result holds true for minimal surfaces tangent to orthogonal hyperbolic paraboloids, see [7]. In this case the curves of constant Gaussian curvature are harmonic oscillation curves and the minimal surfaces are of algebraic degree 30, of class 10, and admit rational parametrizations.

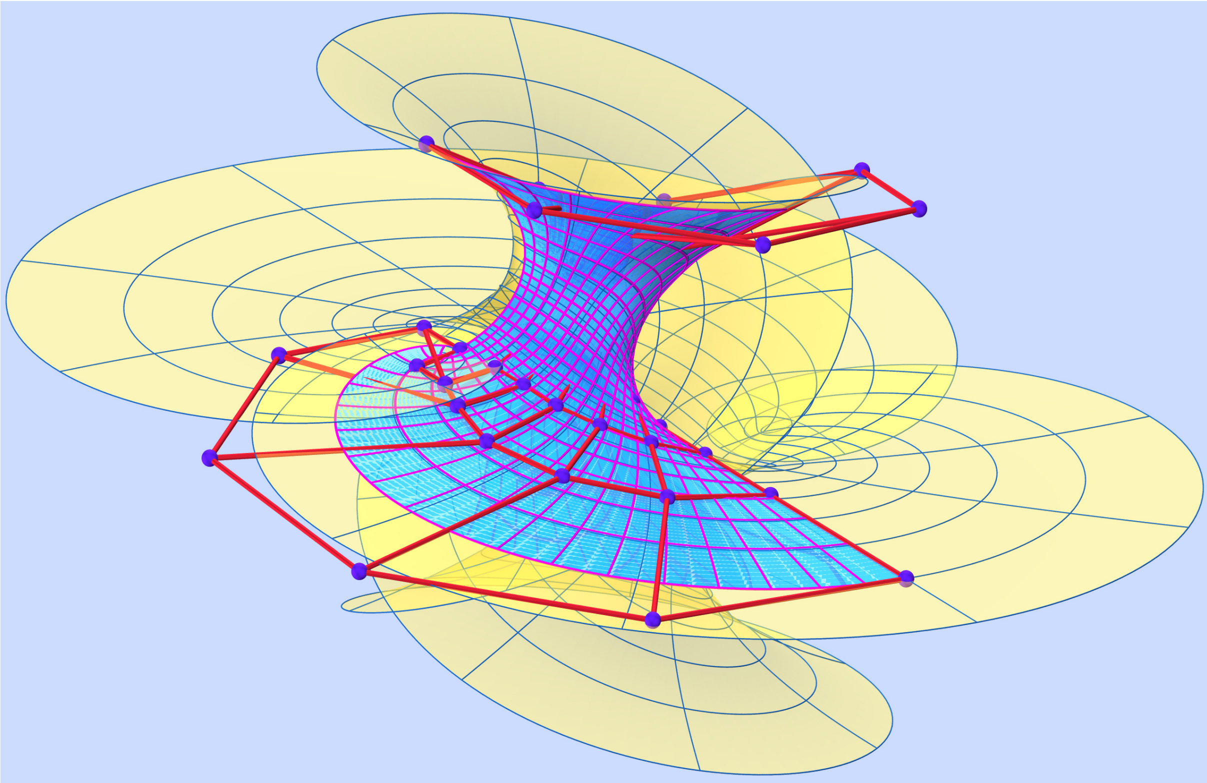


Fig. 5. A part of a minimal surface described in Thm. 2.1 is defined by its control structure.

3 The associate family

The parametrizations (8) of the minimal surfaces tangent to MÜLLER's surface (1) are obtained by extracting the real part of the isotropic curve (9). The imaginary part of $\varphi(t)$ (with $t = u + \mathbf{i}v$) is given by

$$\mathbf{f}^{\perp}(u,v) = \frac{1}{6pq}\begin{pmatrix} -6pq^2 s_u S_v - 3(p^2+q^4)s_u C_v - s_{3u}C_{3v} \\ 6pq^2 c_u S_v - 3(p^2+q^4)c_u C_v + c_{3u}C_{3v} \\ -6s_u(q^2 C_v + pS_v) \end{pmatrix}. \tag{12}$$

An example of a minimal surface $\mathbf{f}^{\perp}(u,v)$ described by (12) is shown in Fig. 6.

Of course, the real algebraic, and indeed rational surfaces parametrized by (12) are minimal surfaces. They are the *adjoint* minimal surfaces to (8). The family of *associate minimal surface* containing (8) and (12) is obtained as the real part of the one-parameter family of isotropic curves

$$\mathbf{f}(u,v,\tau) = \mathfrak{Re}\left(\mathrm{e}^{\mathbf{i}\tau}\varphi(t)\right) = c_\tau \mathbf{f}(u,v) + s_\tau \mathbf{f}^{\perp}(u,v), \quad \tau \in \mathrm{S}^1. \tag{13}$$

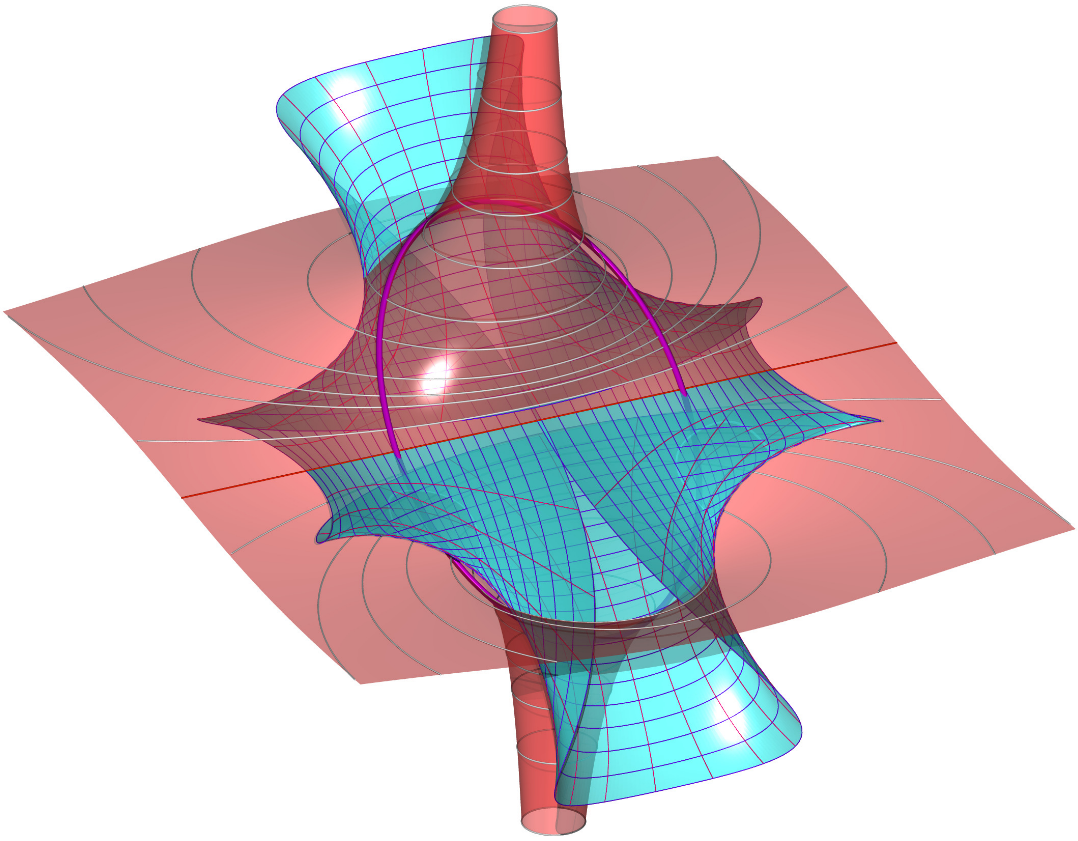


Fig. 6. The minimal surface adjoint to (8) with $q = 1$.

Now, we are able to prove the following:

Theorem 3.1. For any $q \in \mathbb{R}^{\star}$, the one-parameter family of associate minimal surfaces described by (13) consists of rational minimal surfaces of algebraic degree 24 and class 42.

Proof. Independent of the choice of q, we can say: The minimal surfaces parametrized by (12) are rational, since the trigonometric and the hyperbolic functions showing up in the parametrization can be replaced by their rational equivalents. Subsequent to the reparametrization, we can eliminate the parameters and find an algebraic equation of degree 24. The class of the adjoint surfaces is 42 as it is the case with (8), since the isotropic curves corresponding to (12) has the same algebraic properties. From (13) it is clear that the degree and the class of all surfaces in the family of associate minimal surfaces agrees with that of $\mathbf{f}$ and $\mathbf{f}^{\perp}$, because for any $\tau \in \mathrm{S}^1$, (13) is just a linear combination of both. $\square$

Actually, there are two one-parameter families of rational minimal surfaces associated to MÜLLER's surface (1), i.e., a one-parameter family of minimal surfaces related to each ellipse (from the one-parameter family of ellipses) on MÜLLER's surface. It is not worth to mention that this construction of rational minimal surfaces works well for each of the cubic surfaces mentioned in the very beginning of the present paper. So, there is a five-parameter family of rational minimal surfaces sharing the algebraic properties with (8).

4 Some algebraic properties

4.1 Self-intersections

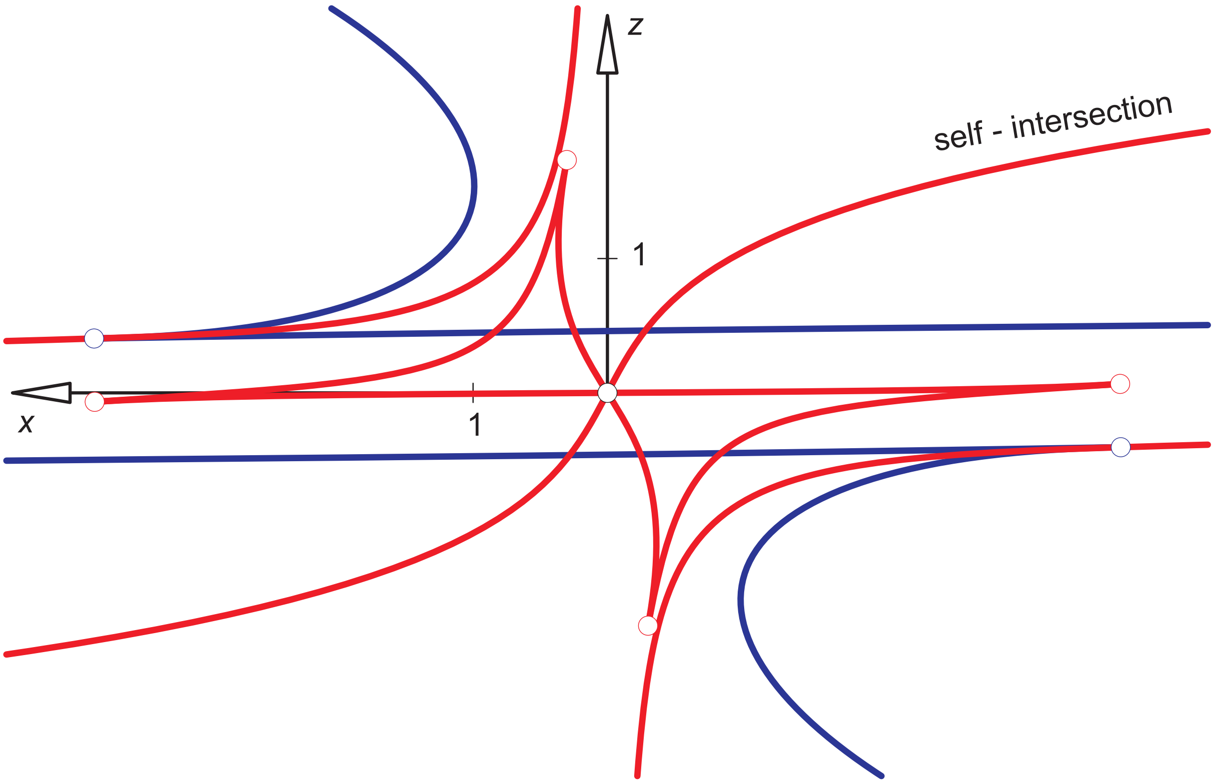


Fig. 7. The self-intersection (red) of the minimal surface (with $q = 4/3$) is a part of the intersection with the plane $y = 0$.

Since the initial data (γ, ν) is symmertic with respect to the plane $y = 0$, the minimal surfaces (8) show the same symmetries. Thus, the plane $y = 0$ carries one part of the self-intersection of the minimal surfaces. Fig. 7 shows the intersection of the minimal surface (8) (with $q = 4/3$) with the plane $y = 0$. This planar cycle is of algebraic degree 24 and consists of a sextic (with multiplicity one, shown in blue) which is not part of the self-intersection. The curve shown in red is of degree nine and has multiplicity two as the planar intersection of (8). Therefore, it is part of the self-intersection of the minimal surface. This nonic has triple-points on the x-axis and the z-axis (at infinity) and a four-fold point at the origin. Further there are four ordinary cusps on the curve, two of which are located on the (non-singular) sextic and are branch points of the minimal surface. Since the nonic is a planar intersection of the minimal surface, it is no surprise that it is a rational curve.

In the plane $x = 0$, we can only find the y-axis as a part of the self-intersection which is also contained in the plane $z = 0$.

4.2 The curve at infinity

The minimal surfaces (8) intersect the ideal plane along the cycle

$$z^{18}(x^2 + y^2)^3 = 0$$

independent of the choice of $q \in \mathbb{R}^\star$. This tells us that the ideal line of all planes parallel to $z = 0$ is of multiplicity 18 and the pair of complex conjugate ideal lines $y = \pm \mathrm{i}x$ through the ideal point of the z-axis is three-fold. The fact that the curve at infinity of these minimal surfaces degenerates completely, i.e., it splits into a finite number of lines, is in accordance with an old result by LIE, see [3].

Because of the high multiplicities of the components in the plane at infinity, these lines also contribute to the self-intersection(s).

4.3 The intersection of MÜLLER's surface

The intersection with MÜLLER's surface (1) with the minimal surfaces (8) along its ellipses contains:

1. the six-fold y-axis (of the underlying Cartesian coordinate system),
2. the two-fold ellipse γ (3) (for any fixed $q \in \mathbb{R}^\star$),
3. the three-fold pair of ideal lines of the complex conjugate pair of planes $x^2 + y^2 = 0$, and
4. the eighteen-fold ideal line of all horizontal planes (parallel to $z = 0$).

References

[1] BLASCHKE, W. *Vorlesungen über Differential Geometrie und geometrische Grundlagen von Einsteins Relativitätstheorie.* Springer, Berlin, 1921.

[2] KARCHER, H. *Construction of minimal surfaces.* In: *Surves in Geometry*, Univ. of Tokyo, 1989, Lecture Notes No. 12, SFB 256, Bonn, 1989.

[3] LIE, S. *Gesammelte Abhandlungen.* Friedrich Engel, Poul Heegaard, eds.,

[4] MÜLLER, E. Die achsiale Inversion. In *Dt. Math.*, Ver. **25**, 1916, pp. 209–251.

[5] NITSCHE, J.C.C. *Vorlesungen über Minimalflächen.* Springer-Verlag, 1975.

[6] ODEHNAL, B. A rational minimal Möbius strip. In *Proc. 17*$^{\text{th}}$ *Internat. Conf. on Geometry and Graphics*, August 4–8, 2016, Beijing, P.R. China, article no. 070.

[7] ODEHNAL, B. On algebraic minimal surfaces. *KoG* **20**, 2016, pp. 61–78.

[8] OSSERMAN, R. *A Survey of Minimal Surfaces.* Dover Publications, New York, 2nd edition, 1986.

[9] POTTMANN, H. Zur Geometrie höherer Planetenumschwungbewegungen. In *Mh. Math.* **97**, 1984, pp. 141–156.

[10] SCHWARZ, H.A. *Gesammelte mathematische Abhandlungen*. Springer, Berlin, 1890.

[11] STRUBECKER, K. *Differentialgeometrie.* Sammlung Göschen, Band 1180/1180a, W. de Gruyter, Berlin, 1969.

[12] THIEME, H. Über eine besondere Fläche dritter Ordnung mit vier Doppelpunkten. In *Z. Math. Phys.* **40**, 1895, pp. 362–369.

[13] WEIERSTRASS, K. *Gesammelte Werke.* 7 Bände, Mayer und Müller, Berlin, 1894–1927 (Nachdruck Olms, Hildesheim, 1967).

[14] WUNDERLICH, W. *Ebene Kinematik*. Bibliograph. Inst. Mannheim, 1970.

[15] WUNDERLICH, W. Höhere Radlinien. In *Österr. Ingen. Archiv* **1**, 1947, pp. 277–296.

Privatdozent Mag. Dr. Boris Odehnal

University of Applied Arts
Oskar-Kokoschka-Platz 2, A-1010 Vienna, Austria
e-mail: boris.odehnal@uni-ak.ac.at

Minkowského súčet a súčin voľne modelovateľných kriviek

Daniela Velichová

Abstrakt
Článok pojednáva o Minkowského množinových operáciách aplikovaných na voľne modelovateľné (aproximačné a interpolačné) krivky, ktoré sú určené riadiacim polygónom a interpolačnými váhovými polynomickými funkciami. Uvedené sú základné vlastnosti plôch modelovaných ako Minkowského súčet, resp. súčin dvoch kriviek, a niektoré ich diferenciálne vlastnosti. Pomocou čiastočného Minkowského súčtu a súčinu sú definované dve triedy špeciálnych kriviek nazvaných stuhy a odvodené sú ich vnútorné geometrické vlastnosti.

Kľúčové slová: Minkowského množinové operácie, čiastočný Minkowského súčet a súčin, voľne modelovateľné krivky.

Abstract
Paper deals with Minkowski point set operations applied to free-form (approximation and interpolation) curves, determined by control polygons and interpolation blending polynomial functions. Basic properties of surfaces modelled as Minkowski sum or product of two curves are presented in addition to some of their differential properties. Two families of special curves called laces are defined by means of partial Minkowski sum and product and their intrinsic geometric properties are derived and sketched.

Key words: Minkowski point set operations, partial Minkowski sum and product, free-form curves.

1 Úvod

V článku pojednávame o aplikácii Minkowského súčtu $\oplus$ a Minkowského súčinu $\otimes$ pri generovaní komplexných bodových množín z voľne modelovateľných kriviek, a uvádzame možnosti ich využitia pri modelovaní geometrických útvarov, ktoré sú diferencovateľnými varietami trojrozmerného euklidovského priestoru. Minkowského súčet a súčin dvoch bodových množín sú množinové operácie definované bodovo, na jednotlivých bodoch príslušných množín, ako súčet a súčin bodov základného priestoru s daným pevným referenčným bodom O. Obe operácie sa vykonávajú ako operácie s polohovými vektormi príslušných bodov vzhľadom na daný referenčný bod. Minkowského súčet dvoch bodových množín je definovaný ako vektorový súčet a Minkowského súčin ako vonkajší súčin polohových vektorov všetkých bodov daných množín, detailné definície pozri v [1].

Uvedené sú tiež obe prípustné formy Minkowského kombinácií dvoch množín - súčtová a súčinová, spolu s určením analytických reprezentácií výsledných dvojparametrických tried listov plôch, alebo dvojparametrických tried oblúkov voľne modelovateľných kriviek v prípade čiastočných Minkowského bodových množinových operácií. Prirodzene je možné odvodiť vnútorné geometrické vlastnosti získaných variet v tvare diferenciálnych charakteristík závislých od vlastností oboch kriviek vystupujúcich ako operandy daných operácií. Detailné opisy a vzorce pre výpočet diferenciálnych vlastností a vnútorných charakteristík výsledných variet sú uvedené napr. v [2], [3].

2 Minkowského súčet a súčtové kombinácie voľne modelovateľných kriviek

Nech sú dané dva oblúky voľne modelovateľných kriviek v $\mathbf{E}^3$ parametricky reprezentované normovanými vektorovými funkciami definovanými na jednotkovom intervale $I = \langle 0,1\rangle \subset \mathbf{R}$

$$\mathbf{r}(u) = \sum_{i=0}^{n} A_i Pl_i(u) = \left(\sum_{i=0}^{n} xa_i Pl_i(u), \sum_{i=0}^{n} ya_i Pl_i(u), \sum_{i=0}^{n} za_i Pl_i(u)\right), u \in I,$$

$$\mathbf{q}(v) = \sum_{i=0}^{n} B_i Pl_i(v) = \left(\sum_{i=0}^{n} xb_i Pl_i(v), \sum_{i=0}^{n} yb_i Pl_i(v), \sum_{i=0}^{n} zb_i Pl_i(v)\right), v \in I,$$

kde $A_i = (xa_i, ya_i, za_i)$, $B_i = (xb_i, yb_i, zb_i)$ sú vrcholy riadiacich polygónov daných kriviek a Pl_i sú interpolačné polynómy v príslušnej forme pre jednotlivé typy voľne modelovateľných kriviek spĺňajúce príslušné kritériá (napr. podmienku uzavretého okraja).

Minkowského súčtová kombinácia daných dvoch kriviek je dvojparametrická trieda translačných plôch definovaná na jednotkovom štvorci $I^2 \subset \mathbf{R}^2$ pre $k, l \in \mathbf{R}$ vektorovou funkciou

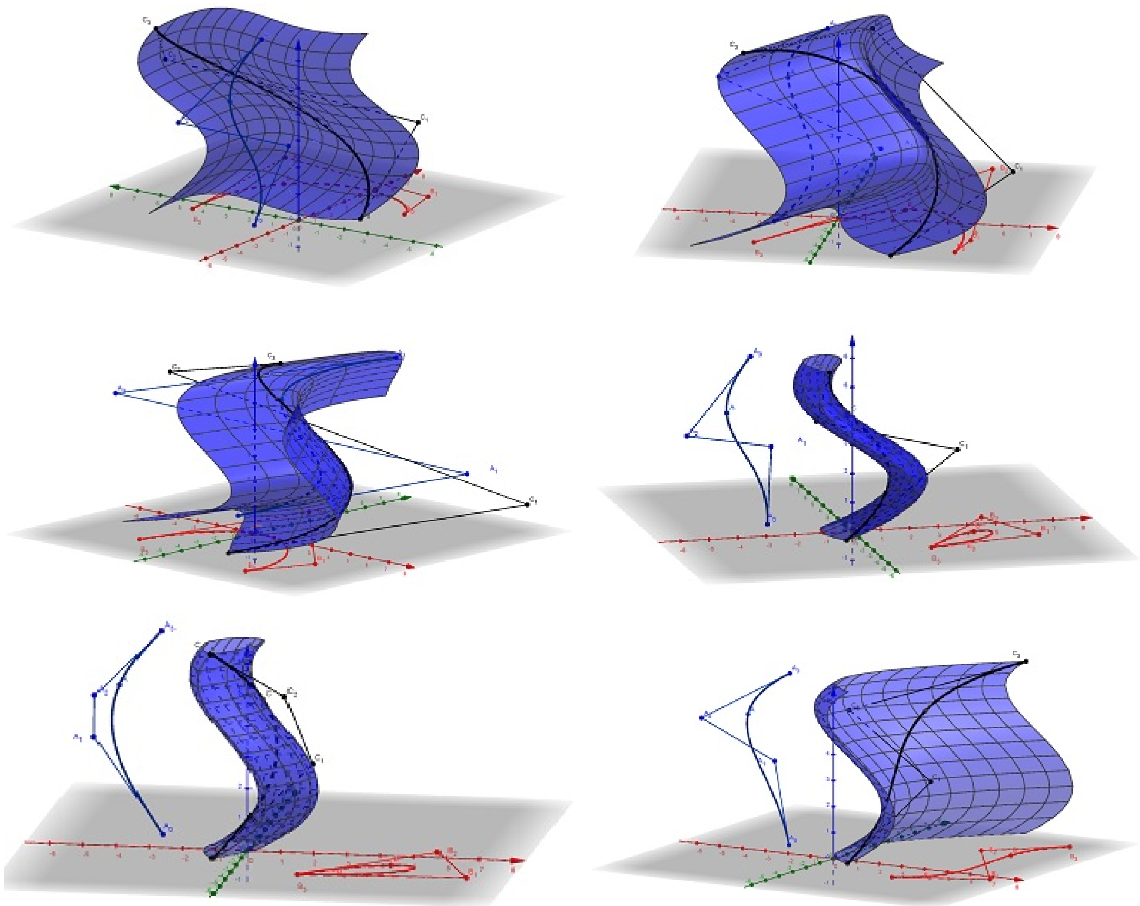
$$\mathbf{s}(u,v) = k\mathbf{r}(u) + l\mathbf{q}(v) = k\sum_{i=0}^{n} A_i Pl_i(u) + l\sum_{i=0}^{n} B_i Pl_i(v) =$$

$$= \sum_{i=0}^{n}(k.A_i Pl_i(u) + l.B_i Pl_i(v)) = (x(u,v), y(u,v), z(u,v))$$

$$x(u,v) = \sum_{i=0}^{n}(k.xa_i Pl_i(u) + l.xb_i Pl_i(v))$$

$$y(u,v) = \sum_{i=0}^{n}(k.ya_i Pl_i(u) + l.yb_i Pl_i(v))$$

$$z(u,v) = \sum_{i=0}^{n}(k.za_i Pl_i(u) + l.zb_i Pl_i(v))$$



Obr. 1. Minkowského súčtové kombinácie Bézierovych oblúkov kriviek.

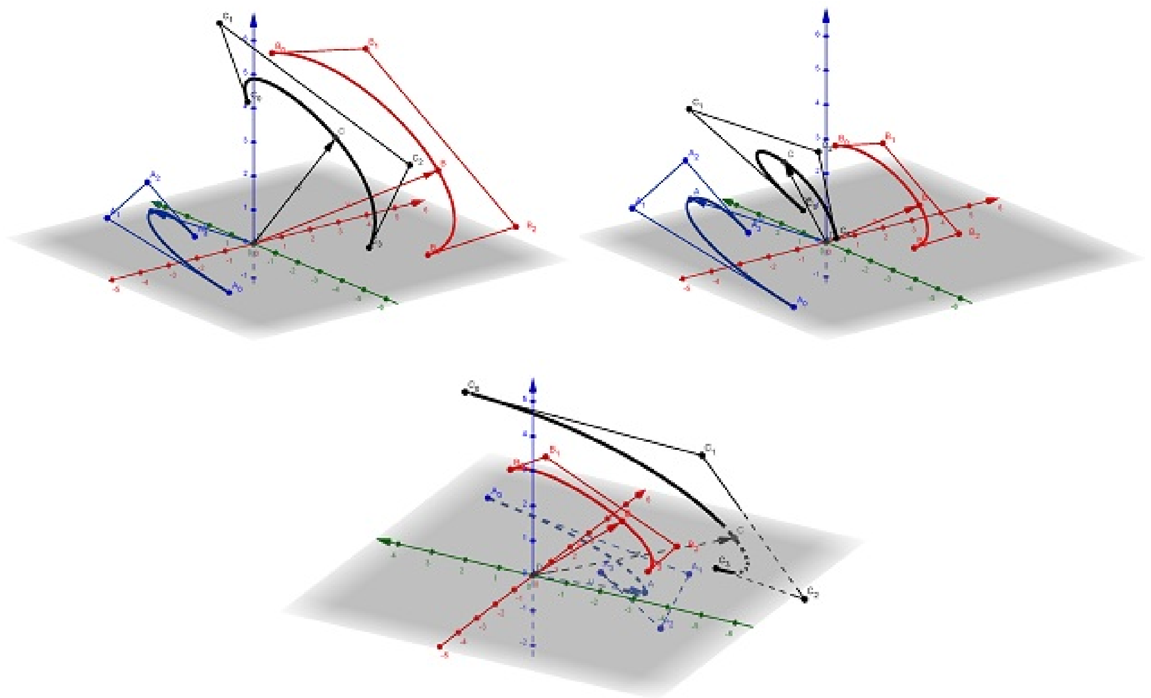
Každá plocha tejto triedy sa dá generovať posúvaním *k*-násobku jednej krivky (obraz prvej krivky v rovnoľahlosti so stredom v referenčnom bode a koeficientom *k*) po *l*-násobku druhej krivky (obraz druhej krivky v rovnoľahlosti so stredom v referenčnom bode a koeficientom *l*). Diferenciálne charakteristiky takýchto plôch možno vyjadriť pomocou derivácií vektorových funkcií definujúcich krivky a v závislosti od konkrétnych hodnôt parametrov $k, l \in \mathbf{R}$.

Ukážky rôznych foriem plôch generovaných ako Minkowského súčtové kombinácie dvoch oblúkov Bézierovych kubických kriviek sú na obr. 1, výsledné plochy sú kubické plochy. Pre hodnoty koeficientov $k = l = 1$ je definovaný Minkowského súčet daných dvoch plôch.

Nech sú dané krivky definované pre ten istý parameter $t \in I = \langle 0, 1\rangle \subset \mathbf{R}$. Minkowského súčtová kombinácia takýchto kriviek

$$\mathbf{s}(t) = k\sum_{i=0}^{n} A_i Pl_i(t) + l\sum_{i=0}^{n} B_i Pl_i(t) = \sum_{i=0}^{n}(k.A_i + l.B_i)Pl_i(t)$$

definuje dvojparametrickú triedu kriviek nazývaných stuhy, pozri v [3], [4]. Každá krivka tejto triedy je opäť aproximačnou krivkou, ktorá je parametricky definovaná vektorovou funkciou $\mathbf{s}(t), t \in \langle 0, 1\rangle$ pre konkrétne hodnoty koeficientov $k, l \in \mathbf{R}$. Riadiace polygóny všetkých



Obr. 2. Minkowského čiastočné súčtové kombinácie Bézierovych oblúkov kriviek.

kriviek triedy sú určené vrcholmi, ktoré sú súčtami príslušných násobkov jednotlivých vrcholov riadiacich polygónov sčítavaných násobkov daných kriviek. Ukážky Minkowského súčtových kombinácií dvoch zhodne parametrizovaných Bézierovych oblúkov kriviek sú na obr. 2.

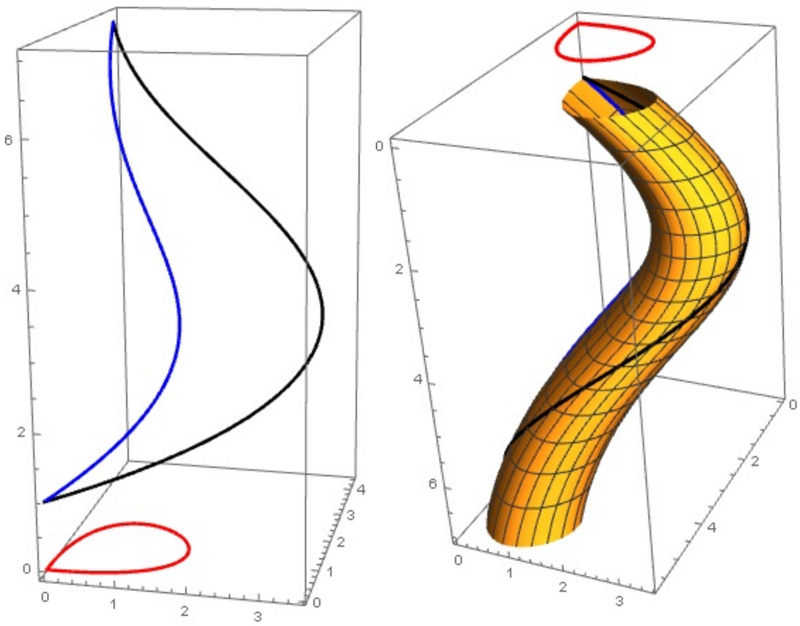
V prípade čiastočného Minkowského súčtu pre hodnoty $k = l = 1$ vznikne ako súčtová kombinácia dvoch kubických Bézierovych oblúkov kriviek opäť Bézierova kubická krivka, viď obr. 3, vľavo. Táto Bézierova krivka stupňa 3 zobrazená čiernou farbou je krivkou kubickej plochy z obr. 3, vpravo, ktorá je Minkowského súčtom Bézierovych oblúkov parametrizovaných rôznymi parametrami. Vrcholy jej riadiaceho polygónu sú súčtami jednotlivých vrcholov riadiacich polygónov sčítancov - pôvodných Bézierovych kubických oblúkov. Krivka je parametricky definovaná vektorovou funkciou

$$\mathbf{s}(t) = \sum_{i=0}^{3} (A_i \oplus B_i) Be_{i3}(t), t \in I = \langle 0, 1 \rangle \subset \mathbf{R},$$

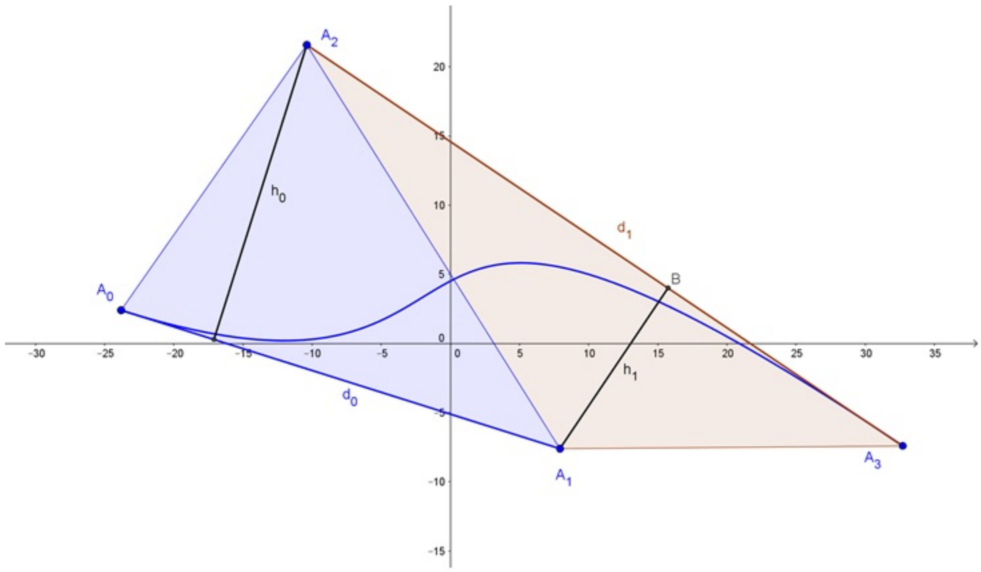
kde $A_i = (xa_i, ya_i, za_i), B_i = (xb_i, yb_i, zb_i)$ sú vrcholy riadiacich polygónov daných Bézierovych kubík a $Be_{i3}(t)$ sú Bernstejnove kubické polynómy.

Vzorec pre výpočet prvej krivosti v začiatočnom (alebo v koncovom) bode oblúka Bézierovej krivky má tvar

$$\kappa(0) = \frac{4P(A_0 A_1 A_2)}{3\|A_1 - A_0\|^3}, \kappa(1) = \frac{4P(A_1 A_2 A_3)}{3\|A_3 - A_2\|^3},$$



Obr. 3. Minkowského čiastočná súčtová kombinácia Bézierovych oblúkov kriviek na súčtovej Bézierovej ploche.



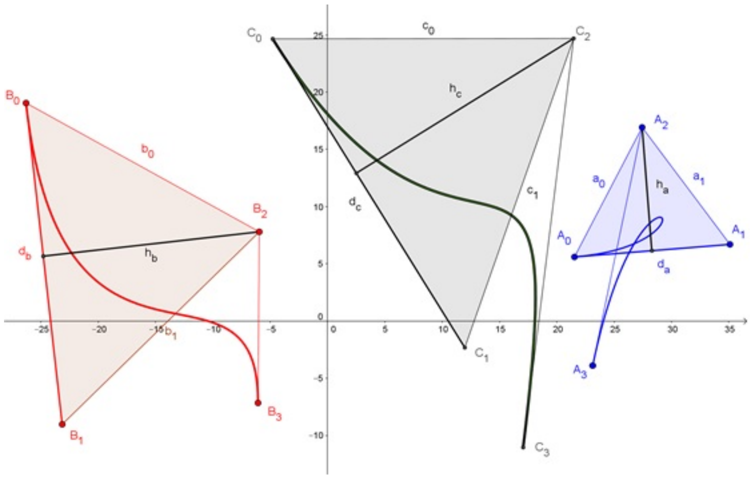
Obr. 4. Trojuholníky určujúce prvú krivosť (flexiu) v začiatočnom a koncovom bode Bézierovej krivky.

kde P je obsah trojuholníka $A_0A_1A_2$ alebo $A_1A_2A_3$, ktorý sa dá prepísať pomocou rozmerov trojuholníkov, teda dĺžky jednej strany $\|A_0A_1\| = d_0$ alebo $\|A_2A_3\| = d_1$, a výšky h_0, alebo h_1, pozri obr. 4, v tvare

$$\kappa(0) = \frac{2h_0}{3d_0^2}, \kappa(1) = \frac{2h_1}{3d_1^2}.$$

Nech je čiastočný Minkowského súčet dvoch Bézierovych kubických oblúkov určených vrcholmi riadiacich polygónov A_0, A_1, A_2, A_3 a B_0, B_1, B_2, B_3 opäť Bézierovym kubickým oblúkom, ktorý je určený vrcholmi riadiaceho polygónu C_0, C_1, C_2, C_3. Pre tieto vrcholy platí

$$C_i = A_i \oplus B_i, i = 0, 1, 2, 3.$$



Obr. 5. Trojuholník určujúci flexiu v začiatočnom bode čiastočného Minkowského súčtu dvoch Bézierovych kubických kriviek.

Prvá krivosť tohto čiastočného Minkowského súčtu v začiatočnom bode (a podobne v koncovom bode) sa dá vyjadriť pomocou dĺžky strany d_c a výšky h_c trojuholníka $C_0C_1C_2$, čo možno prepísať pomocou dĺžok strán a výšok dvoch trojuholníkov tvorených pôvodnými vrcholmi riadiacich polygónov sčítavaných kriviek (pozri obr. 5) v tvare

$$\kappa(0) = \frac{2h_c}{3d_c^2}, d_c^2 = d_a^2 + d_b^2 + 2\Delta xa_{01}\Delta xb_{01} + 2\Delta ya_{01}\Delta yb_{01},$$

$$h_c = \frac{1}{4}\sqrt{4c_0^2d_c^2 - (d_c^2 + c_0^2 - c_1^2)^2},$$

$$c_0^2 = a_0^2 + b_0^2 + 2\Delta xa_{02}\Delta xb_{02} + 2\Delta ya_{02}\Delta yb_{02},$$

$$c_1^2 = a_1^2 + b_1^2 + 2\Delta xa_{12}\Delta xb_{12} + 2\Delta ya_{12}\Delta yb_{12},$$

$$\Delta xa_{ij} = xa_j - xa_i, \Delta xb_{ij} = xb_j - xb_i, \Delta ya_{ij} = ya_j - ya_i, \Delta yb_{ij} = yb_j - yb_i.$$

Prvá krivosť čiastočného Minkowského súčtu dvoch Bézierovych kubických oblúkov v začiatočnom a v koncovom bode sú teda presne určené kombinácie vstupných údajov, ktorými sú rozmery riadiacich polygónov sčítavaných Bézierovych kriviek.

3 Minkowského súčin a súčinová kombinácia voľne modelovateľných kriviek

Minkowského súčinová kombinácia dvoch násobkov oblúkov voľne modelovateľných kriviek stupňa n určených vektorovými fukciami $k.\mathbf{r}(u), l.\mathbf{q}(v), u, v \in I \subset \mathbf{R}, k, l \in \mathbf{R}$ je trieda listov plôch, ktoré sú parametricky reprezentované na jednotkovom štvorci $I^2 \subset \mathbf{R}^2$ funkciou

$$\mathbf{p}(u,v) = k.\mathbf{r}(u) \wedge l.\mathbf{q}(v) = k.l \begin{pmatrix} yr(u)zq(v) - zr(u)yq(v) \\ zr(u)xq(v) - xr(u)zq(v) \\ xr(u)yq(v) - yr(u)xq(v) \end{pmatrix}^T, (u,v) \in I^2,$$

$$xr(u) = \sum_{i=0}^{n} xa_i Pl_i(u), yr(u) = \sum_{i=0}^{n} ya_i Pl_i(u), zr(u) = \sum_{i=0}^{n} za_i Pl_i(u),$$

$$xq(v) = \sum_{i=0}^{n} xb_i Pl_i(v), yq(v) = \sum_{i=0}^{n} yb_i Pl_i(v), zq(v) = \sum_{i=0}^{n} zb_i Pl_i(v).$$

Listy plôch, ktoré vzniknú ako súčinové kombinácie dvoch oblúkov voľne modelovateľných kriviek definované reálnymi koeficientami $k, l \in \mathbf{R}$, sú plochy stupňa $2n$. Obsahujú také body priestoru, ktorých polohové vektory sú $k.l$-násobky vektorových súčinov polohových vektorov bodov daných dvoch kriviek.

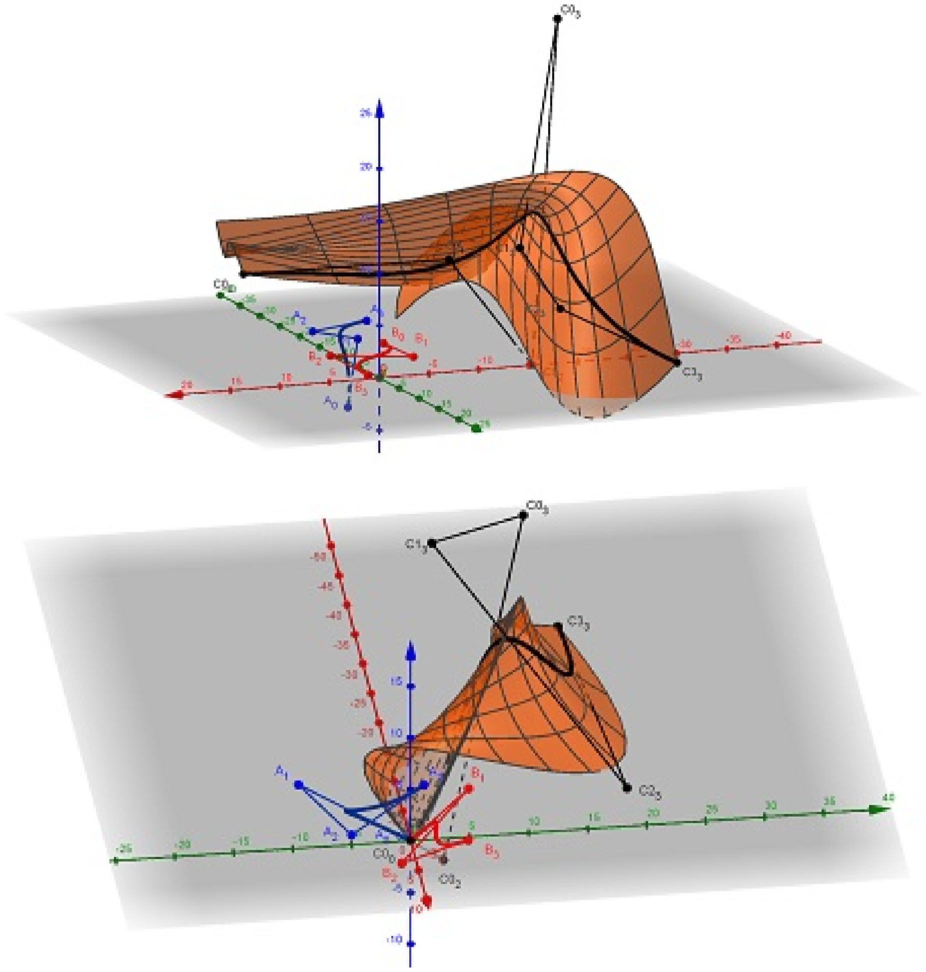
V prípade kubických kriviek pre $k = l = 1$ je Minkowského súčinom list bikubickej Bézierovej plochy šiesteho stupňa. Parametrická reprezentácia takejto plochy má tvar

$$\mathbf{p}(u,v) = \mathbf{r}(u) \wedge \mathbf{q}(v) = \sum_{i=0}^{3} A_i Be_{i3}(u) \otimes \sum_{j=0}^{3} B_j Be_{j3}(v) =$$

$$= (A_0 Be_{03}(u) + A_1 Be_{13}(u) + A_2 Be_{23}(u) + A_3 Be_{33}(u)) \otimes$$

$$\otimes (B_0 Be_{03}(v) + B_1 Be_{13}(v) + B_2 Be_{23}(v) + B_3 Be_{33}(v)) =$$

$$= \sum_{i=0}^{3} \sum_{j=0}^{3} (A_i \otimes B_j) Be_{i3}(u) Be_{j3}(v).$$



Obr. 6. Minkowského súčin Bézierovych oblúkov.

Mapa tejto bikubickej Bézierovej plochy stupňa šesť je matica

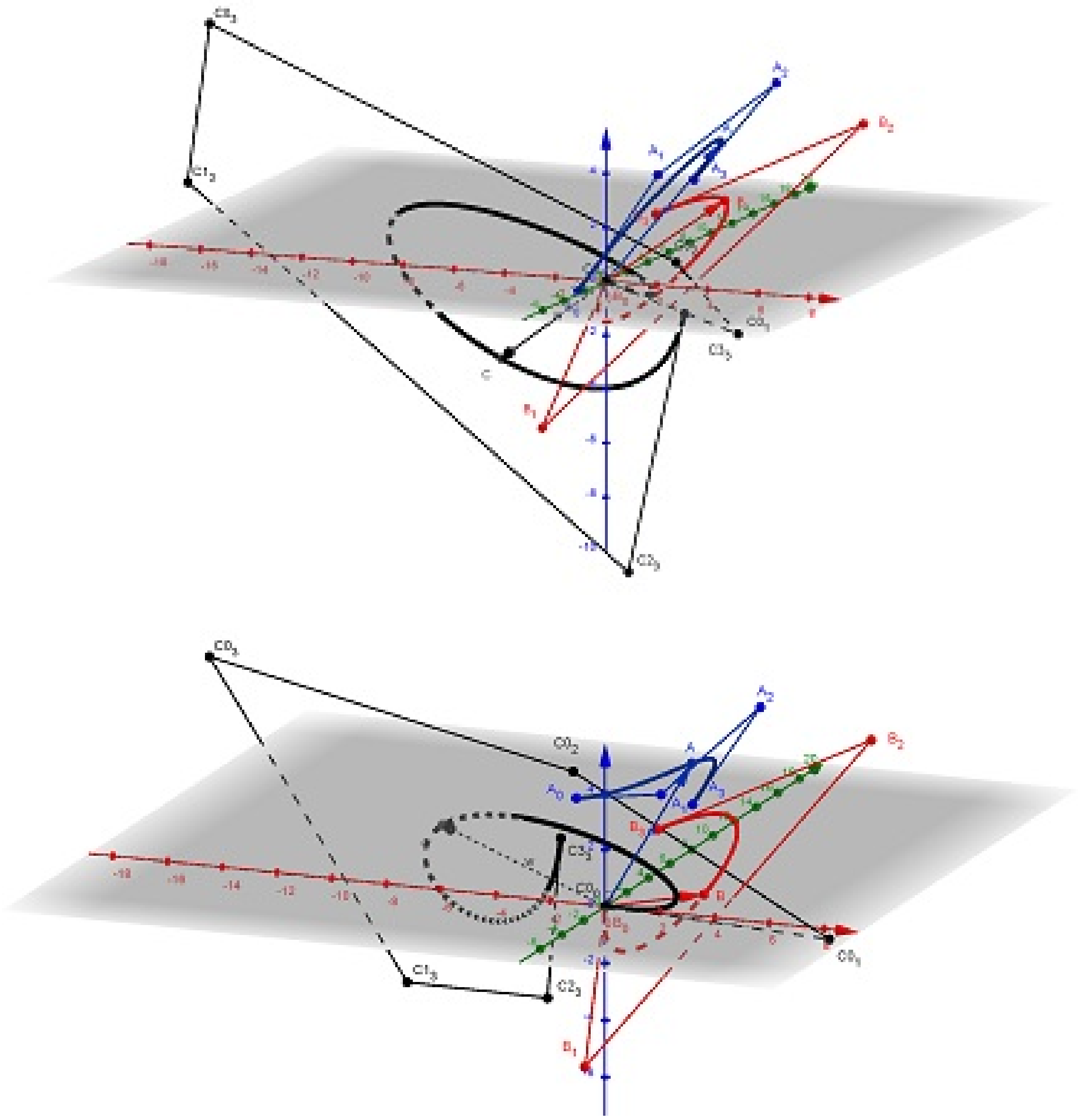
$$\begin{pmatrix} A_0 \otimes B_0, A_0 \otimes B_1, A_0 \otimes B_2, A_0 \otimes B_3 \\ A_1 \otimes B_0, A_1 \otimes B_1, A_1 \otimes B_2, A_1 \otimes B_3 \\ A_2 \otimes B_0, A_2 \otimes B_1, A_2 \otimes B_2, A_2 \otimes B_3 \\ A_3 \otimes B_0, A_3 \otimes B_1, A_3 \otimes B_2, A_3 \otimes B_3 \end{pmatrix}$$

Dve modifikácie plochy sú zobrazené na obr. 6.

Čiastočný Minkowského súčin dvoch oblúkov zhodne parametrizovaných voľne modelovateľných kriviek je generujúcim princípom kriviek, ktoré tvoria triedu stúh homotetických v rovnoľahlosti so stredom v referenčnom bode a koeficientom rovnoľahlosti $k.l$.

Čiastočná Minkowského súčinová kombinácia dvoch voľne modelovateľných oblúkov stupňa n reprezentovaných vektorovými funkciami s rovnakým parametrom z jednotkového intervalu $I \in \mathbf{R}$ je krivka stupňa $2n$ určená nasledujúcou vektorovou funkciou na I

$$\mathbf{p}(t) = k\sum_{i=0}^{n} A_i Pl_i(t) \wedge l\sum_{i=0}^{n} B_i Pl_i(t) = k.l\sum_{i=0}^{n}(A_i \otimes B_i)(Pl_i(t))^2,$$

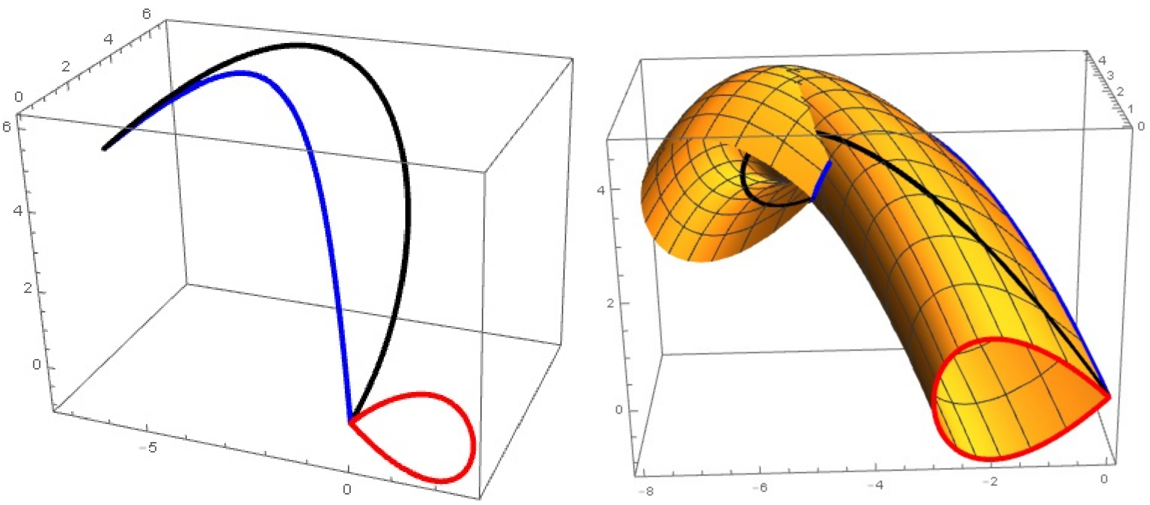


Obr. 7. Minkowského čiastočný súčin dvoch Bézierovych oblúkov.

ktorá je krivkou príslušnej plochy stupňa $2n$ generovanej ako Minkowského súčin pôvodných oblúkov kriviek parametrizovaných rôznymi parametrami.

Stuhy generované ako Minkowského čiastočný súčin dvoch kubických Bézierovych oblúkov sú zobrazené na obr. 7.

Plocha generovaná ako Minkowského súčin dvoch kubických Bézierovych oblúkov, pre $k = l = 1$, z obr. 3 je zobrazená na obr. 8, spolu s čiastočným súčinom daných kriviek, ktorý je zobrazený čiernou farbou. Minkowského čiastočný súčin je krivka šiesteho stupňa ležiaca na ploche Minkowského súčinu daných Bézierovych kubických oblúkov parametrizovaných rôznymi parametrami. Vrcholy jej riadiaceho polygónu sú kombinácie súčinov príslušných vrcholov riadiacich polygónov kriviek vystupujúcich ako prvky Minkowského čiastočného súčinu. Krivka obsahuje všetky tie body plochy, ktorých krivočiare parametre na ploche sú zhodné, $u = v = t \in I$.



Obr. 8. Minkowského súčin a čiastočný súčin dvoch kubických Bézierovych oblúkov.

Parametrická reprezentácia tejto Bézierovej krivky šiesteho stupňa má tvar

$$\mathbf{p}(t) = \mathbf{r}(u) \wedge \mathbf{q}(v) = \sum_{i=0}^{3} A_i Be_{i3}(t) \otimes \sum_{i=0}^{3} B_i Be_{i3}(t) =$$

$$= (A_0 \otimes B_0)(Be_{03}(t))^2 + (A_0 \otimes B_1 + A_1 \otimes B_0) Be_{03}(t) Be_{13}(t) +$$

$$+ [A_0 \otimes B_2 + 3(A_2 \otimes B_2) + A_2 \otimes B_0] Be_{03}(t) Be_{23}(t) +$$

$$+ [A_0 \otimes B_3 + 9(A_1 \otimes B_2) + 9(A_2 \otimes B_1) + A_3 \otimes B_0] Be_{03} Be_{33}(t) +$$

$$+ [A_1 \otimes B_3 + 3(A_2 \otimes B_2) + A_3 \otimes B_1] Be_{13}(t) Be_{33}(t) +$$

$$+ (A_2 \otimes B_3 + A_3 \otimes B_2) Be_{23}(t) Be_{33}(t) + (A_3 \otimes B_3)(Be_{33}(t))^2$$

Mapa krivky je matica

$$\begin{pmatrix} A_0 \otimes B_0 \\ A_0 \otimes B_1 + A_1 \otimes B_0 \\ A_0 \otimes B_2 + 3(A_2 \otimes B_2) + A_2 \otimes B_0 \\ A_0 \otimes B_3 + 9(A_1 \otimes B_2) + 9(A_2 \otimes B_1) + A_3 \otimes B_0 \\ A_2 \otimes B_3 + A_3 \otimes B_2 \\ A_3 \otimes B_3 \end{pmatrix}^T$$

Ak označíme prvky matice $C_i, i = 0, 1, ..., 6$, potom parametrickú reprezentáciu tejto krivky šiesteho stupňa možno zapísať v tvare

$$\mathbf{p}(t) = C_0 Be_{06}(t) + \frac{C_1}{2} Be_{16}(t) + \frac{C_2}{5} Be_{26}(t) +$$

$$+\frac{C_3}{20} Be_{36}(t) + \frac{C_4}{5} Be_{46}(t) + \frac{C_5}{2} Be_{56}(t) + C_6 Be_{66}(t)$$

Vyjadrenie vnútorných geometrických vlastností sextiky, ktorá je čiastočným Minkowského súčinom dvoch Bézierovych kubík, bude zrejme opäť možné pomocou vrcholov riadiacich útvarov určujúcich kubík, a je to predmetom ďalšieho aktuálneho skúmania v tejto oblasti.

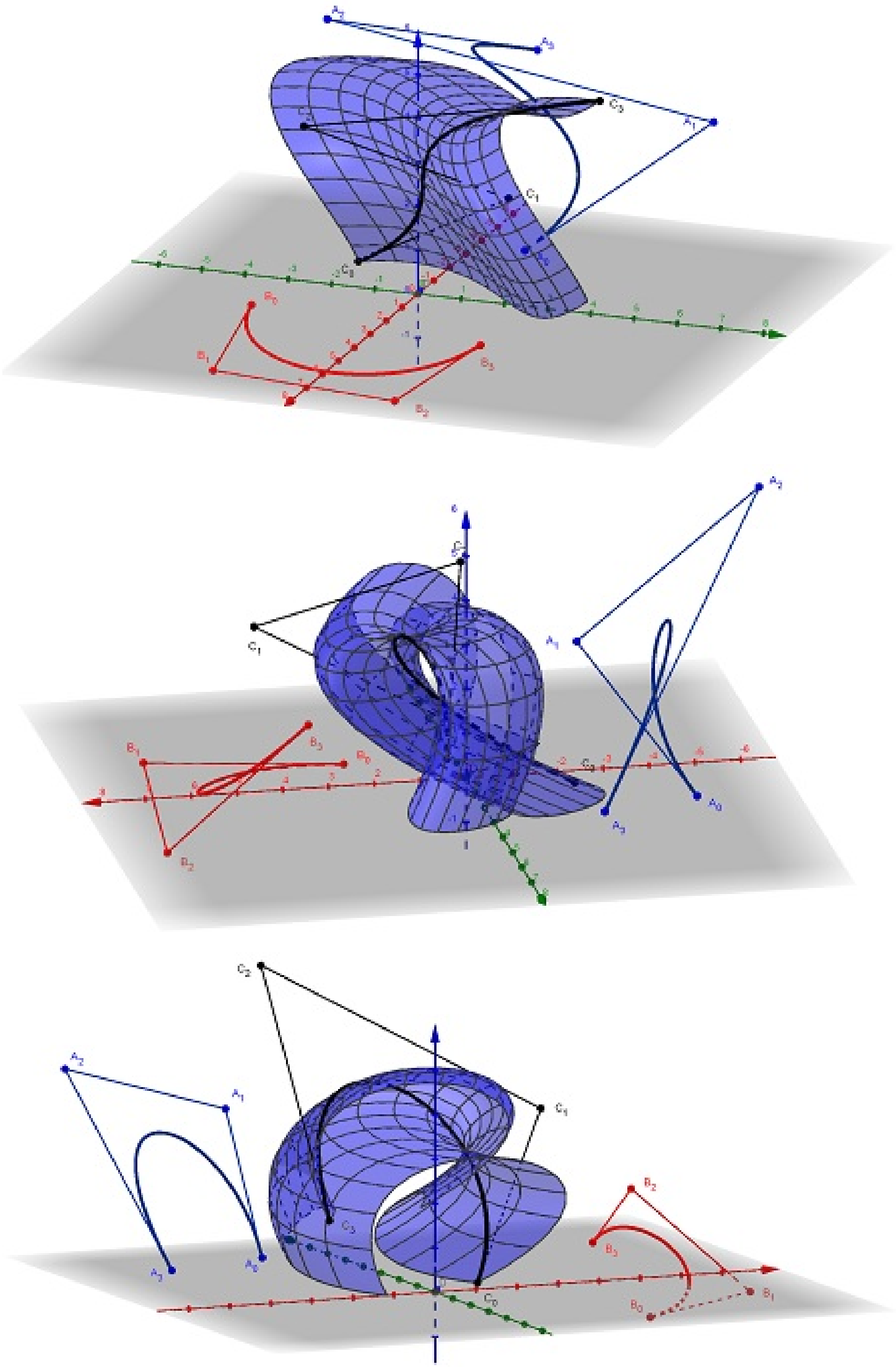
4 Záver

Minkowského množinové kombinácie predstavujú mocný nástroj na modelovanie nových foriem kriviek a plôch, ktorých špecifické vnútorné vlastnosti sú ovplyvniteľné formou dvoch pôvodných kriviek, ktorých kombináciou sú generované. V prípade voľne modelovateľných kriviek sú získané variety opäť voľne modelovateľnými útvarmi, ktorých riadiace útvary sú špecifickými kombináciami riadiacich útvarov pôvodných variet vystupujúcich ako prvky Minkowského kombinácií. V dôsledku tejto skutočnosti sú aj vnútorné geometrické vlastnosti generovaných voľne modelovateľných útvarov determinované vlastnosťami riadiacich útvarov pôvodných kriviek vystupujúcich ako operandy Minowského operácií a možno ich vyjadriť pomocou rozmerov riadiacich útvarov týchto kriviek.

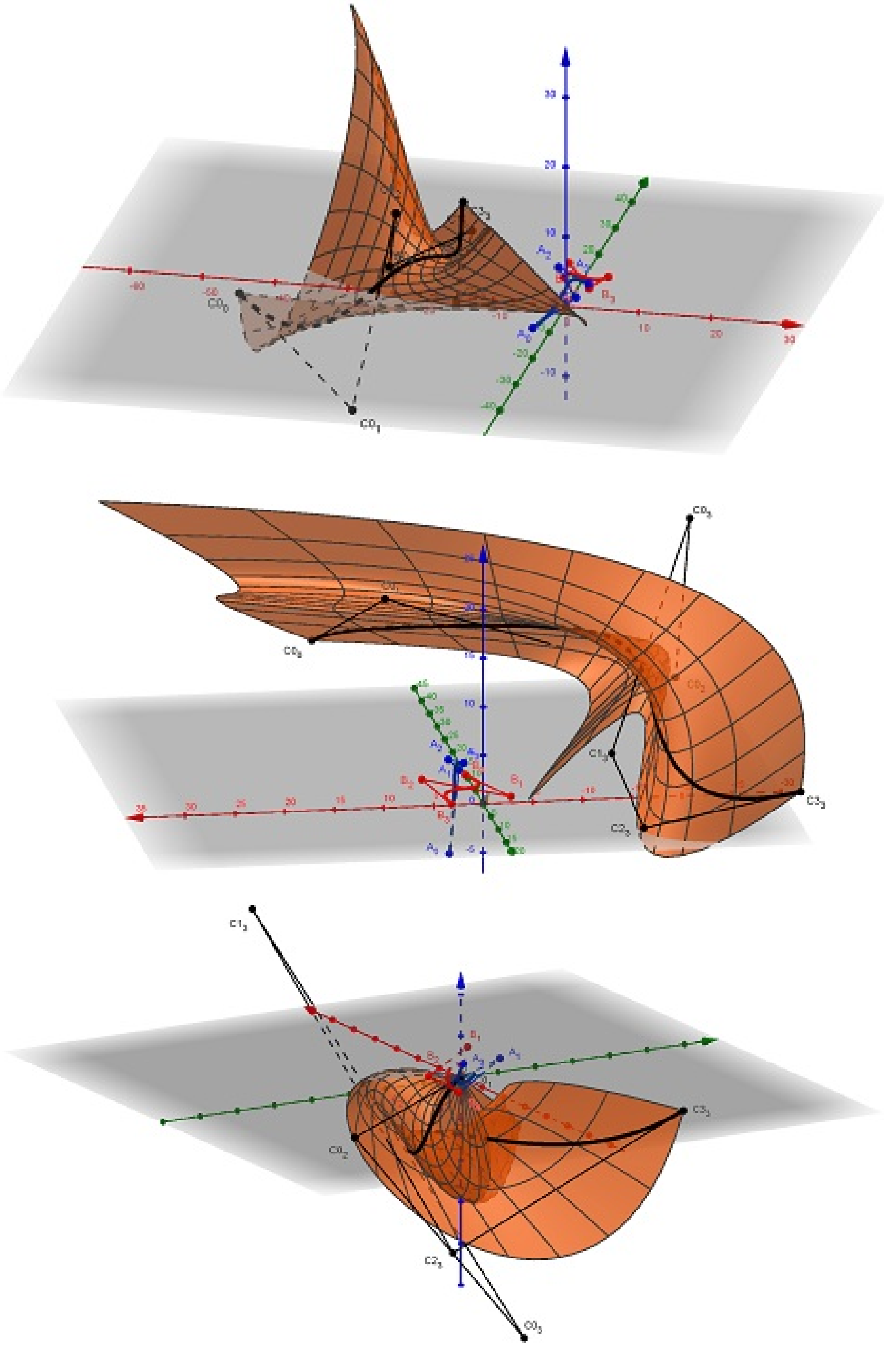
Opísané modelovacie nástroje možno preto považovať za algoritmy deformácií, ktoré obohacujú register a rozsah stratégií voľného modelovania bežne používaných v geometrickom dizajne a modelovaní prostriedkami počítačovej grafiky. Je to nástroj interaktívneho návrhu a manipulatívna technika modelovania tvaru geometrických útvarov, ktorá sa dá jednoducho implementovať a využívať v praktických aplikáciách počítačovej grafiky, v geometrickom modelovaní s podporou počítačov CAGM a CAGD. Tento prirodzený nástroj deformácie môže byť zvlášť užitočným v súvislosti s modelovaním tvaru objektov v umení a architektúre, ako je opísané napr. v [5], [6].

Minkowského množinové operácie definované na podmnožinách trojrozmerného euklidovského priestoru umožňujú formulovať základné princípy Minkowského množinovej algebry. Otvorenými problémami ostávajú otázky ako opísať vlastnosti prípustných algebraických štruktúr s Minkowského množinovými operáciami a identifikácia špeciálnych tried kriviek a plôch, ktoré sa dajú pomocou Minkowského operácií generovať a vymedziť svojimi špecifickými vlastnosťami.

Ilustrácie objektov generovaných pomocou opísaných algoritmov, ktoré by mohli nájsť uplatnenie v umeleckom návrhu,sú uvedené na obr. 9 a obr. 10.



Obr. 9. Minkowského súčtové kombinácie kubických Bézierovych oblúkov kriviek.



Obr. 10. Minkowského súčinové kombinácie kubických Bézierovych oblúkov kriviek.

5 Poďakovanie

Článok vznikol s podporou grantu číslo APVV-0161-12 slovenskej Agentúry na podporu výskumu a vývoja.

Literatúra

[1] VELICHOVÁ, D. Classification of Manifolds Resulting as Minkowski Operation Products of Basic Geometric Point Sets, in *Journal for Geometry and Graphics*, Volume 19 (2015), No. 1, 13-29.

[2] VELICHOVÁ, D. Minkowski Combinations of Free-Form Curves, in *Aplimat proceedings 2016*, STU Bratislava 2016, Slovakia.

[3] VELICHOVÁ, D. Minkowski Combinations of Curves, in *17th International Conference on Geometry and Graphics ICGG 2016*, Beijing 2016, China, 5 str.

[4] VELICHOVÁ, D. Minkowski Laces, in *Proceedings of 23rd Conference Geometry-Graphics-Computer*, Lodž 2016, Poland, 53-54.

[5] VELICHOVÁ, D. The Art of Geometry, in *16th Conference Bridges Enschede*, Proceedings 2013, Tesselations, Phoenix, Arizona, USA, 143-150.

[6] VELICHOVÁ, D. Minkowski Operations in Shape Modelling, in *Mathematics and Art III*, Cassini 2015, France, 127-138.

[7] VELICHOVÁ, D.Minkowského množinové operátory, in *G - Slovenský časopis pre Geometriu a Grafiku*, číslo 17, 2012, ročník 9, Slovenská spoločnosť pre Geometriu a Grafiku, Bratislava 2012, 53-66.

doc. RNDr. Daniela Velichová, CSc.

Ústav matematiky a fyziky, Strojnícka fakulta
Slovenská technická univerzita v Bratislave
Nám. slobody 17, 812 31 Bratislava, Slovenská republika
e-mail: daniela.velichova@stuba.sk

Vrkoče žonglovacích vzorov

Michal Zamboj

Abstrakt
V príspevku ukážeme spôsob grafickej reprezentácie žonglovania za použitia vrkočov. Popíšeme ako vrkoče obohatia matematický popis žonglovania pomocou celočíselných postupností a poukážeme na základné vlastnosti takto vytvorených žonglérskych trikov.

Kľúčové slová: Matematická teória žonglovania, teória vrkočov, celočíselné postupnosti.

Abstract
In the contribution, we will show a method of a graphic representation of juggling using braids. We will describe how braids improve the mathematical notation of juggling by integer sequences and reveal elementary properties of such juggling tricks.

Keywords: Mathematical theory of juggling, braid theory, integer sequences.

1 Úvod

V posledných tridsiatich rokoch upútalo žonglovanie matematikov natoľko, že začali skúmať jeho popis a vlastnosti. Ukázalo sa, že žonglovanie je vhodné pre ďalšie rozvíjanie diskrétnych matematických teórií v kombinatorike, či algebraických štruktúrach s aplikáciami vo fyzike a informatike. Najpoužívanejším zápisom žonglovania je dnes medzi matematikmi aj žonglérmi takzvaný siteswapový zápis pomocou celočíselných postupností. Podrobne je siteswapový zápis popísaný napríklad v [2, 7]. V príspevku sa budeme venovať žonglovaniu z pohľadu grafickej reprezentácie v teórii vrkočov.[1] Článok je doplneným prekladom konferenčného príspevku [10] a autor nadväzuje na svoju diplomovú prácu [9]. Zdrojom inšpirácie boli aj nasledovné práce [3, 4, 8], ktoré prepájajú žonglovanie a teóriu vrkočov, či uzlov.

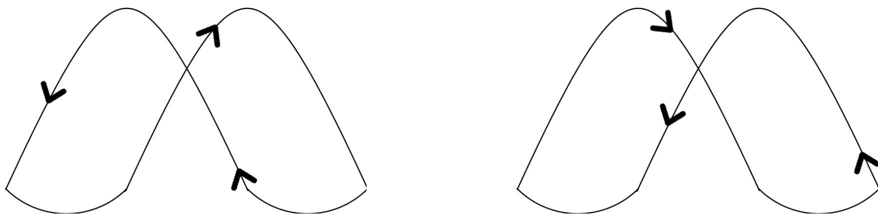
Pre naše účely použijeme nasledovný zjednodušený model žonglovania. Predstavme si metronóm, ktorý vytvára rovnomerné údery v čase. Žonglér:

- vyhadzuje loptičky na dané údery, pričom jeho ruky sa striedajú,
- vždy žongloval a nikdy neskončí,
- vyhodí na každý úder nanajvýš jednu loptičku a ak nejakú loptičku chytí, musí ju vyhodiť (na ten istý úder).

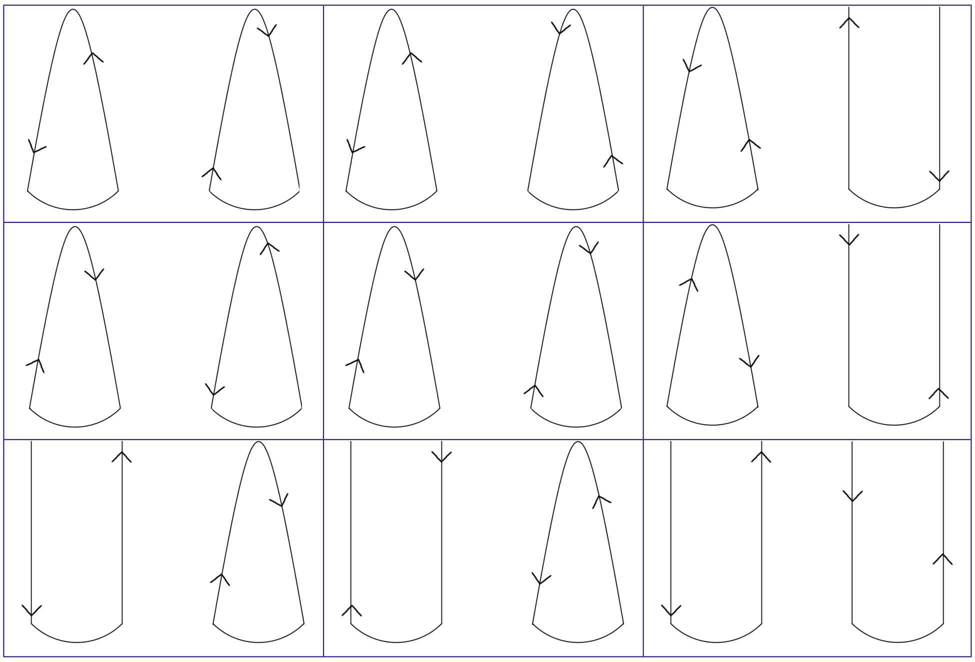
[1] V anglickom preklade tradične „braid theory“.

Počas skúmania sa, bohužiaľ, vyhneme zábavným trikom ako hádzanie za chrbtom, popod nohu a podobne. Žonglér z nášho modelu stojí k žonglovanému vzoru vždy čelom a jeho ruky sú umiestnené v dvoch rôznych pevných bodoch priestoru, až na vnútorné a vonkajšie hody, ktoré hneď popíšeme.

Najjednoduchšie žonglérske vzory s nepárnym počtom loptičiek nazývame *kaskády*, s párnym počtom loptičiek *fontány*. Pri kaskáde vyhodíme postupne každú loptičku do oblúku a chytáme ju do druhej ruky. V reálnej situácii si žonglér môže vybrať, či loptičku vyhadzuje „zvnútra" svojho tela a chytá ju „vonku" - *vnútorný hod* (Obrázok 1 (vľavo)), alebo naopak - *vonkajší hod* (Obrázok 1 (vpravo)). Pri fontáne je každá loptička vyhodená aj chytená do rovnakej ruky. Žonglér si znovu môže zvoliť vnútorné alebo vonkajšie hody (Obrázok 2).[2]



Obr. 1. Kaskáda s tromi loptičkami žonglovaná vnútornými hodmi (vľavo) a vonkajšími hodmi (vpravo).



Obr. 2. Možnosti žonglovania fontány so štyrmi loptičkami.

2 Vrkoče žonglovacích vzorov

Začneme empirickým skúmaním vzťahu vrkočov a žonglovania. Neskôr aplikujeme naše pozorovania na siteswapový zápis.

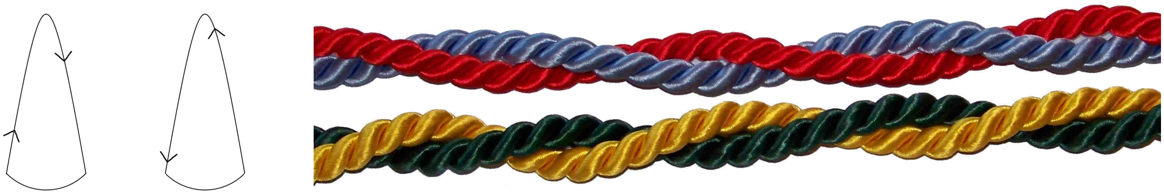
[2]V žonglérskej terminológii nazývame kaskády a fontány žonglované na vonkajšie hody *reverzné*. My sa reverzným žonglovacím vzorom budeme venovať podrobnejšie v súvislosti s vrkočmi.

Obr. 3. Žonglovací vrkoč kaskády s tromi loptičkami.

Predstavme si žongléra žonglujúceho kaskádu s tromi loptičkami na vnútorné hody a kráčajúceho z nášho pohľadu zľava doprava (Obrázok 3). Trajektórie loptičiek vytvoria sústavu priestorových kriviek, ktorú nazývame *žonglovací vrkoč*. Ak budeme zaznamenané trajektórie loptičiek prechádzať zprava doľava (osovo súmerný obraz), všimneme si, že to sú trajektórie loptičiek kaskády žonglovanej vonkajšími hodmi. Žonglovací vrkoč kaskády s piatimi loptičkami a jeho osovo súmerný obraz je na Obrázku 4.

Obr. 4. Žonglovací vrkoč kaskády s piatimi loptičkami žonglovanej vnútornými hodmi a jeho osovo súmerný obraz.

Voľba vnútorných a vonkajších hodov pri fontánach so štyrmi loptičkami nám dáva viacero možností (viď Obrázky 5 — 7).

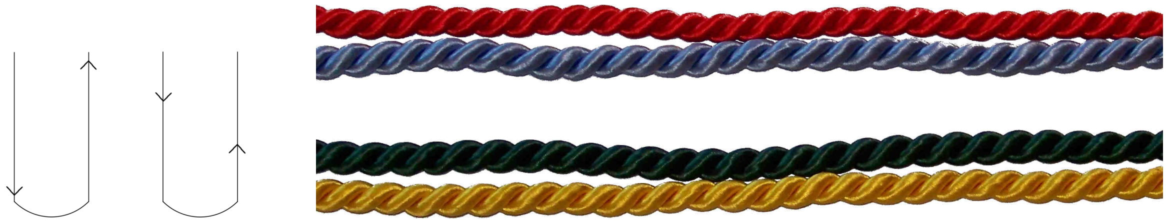


Obr. 5. Žonglovací vrkoč fontány so štyrmi loptičkami žonglovanej vonkajšími hodmi.

Obr. 6. Žonglovací vrkoč fontány so štyrmi loptičkami hádzanými na vnútorné hody v ľavej ruke a na vonkajšie hody v pravej ruke.

2.1 Siteswap

Predstavme si v krátkosti najpoužívanejší zápis žonglovania. Siteswapový zápis je zápis pomocou nezáporných celočíselných postupností. Žonglovanie rozdelíme na jednotlivé hody. *Hod*

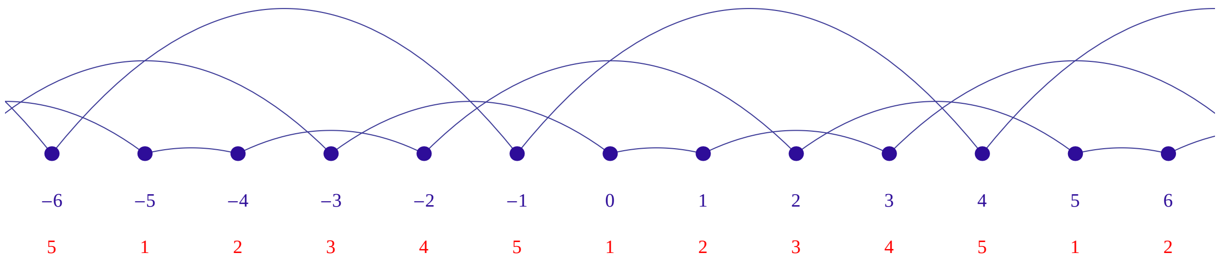


Obr. 7. Žonglovací vrkoč fontány so štyrmi loptičkami hádzanými do stĺpcov (striedanie vnútorných a vonkajších hodov v oboch rukách).

je pohyb loptičky odkedy bola vyhodená, pokým dopadne. *Výška hodu* je počet úderov, ktoré ubehnú počas jej hodu (vrátane dopadu). Napríklad v kaskáde s tromi loptičkami má každý hod výšku 3. Vo fontáne so štyrmi loptičkami má každý hod výšku 4. Je hneď vidieť, že hody o nepárnych výškach vždy dopadnú do druhej ruky a hody o párnych výškach dopadnú do rovnakej ruky. Nás budú zaujímať najmä vzory, v ktorých sú jednotlivé výšky hodov rôzne.

Každému úderu $i \in \mathbb{Z}$ priraďme výšku hodu $h_i \in \mathbb{N}_0$ pomocou *žonglovacej funkcie* ϑ : $\vartheta(i) = h_i$. Aby boli splnené všetky vlastnosti nášho modelu žonglovania, definujme *chytaciu funkciu* γ, ktorá každému úderu, v ktorom loptičku vyhadzujeme, priradí úder, na ktorý bude loptička chytená, $\gamma(i) = h_i + i$. Pretože na každý úder je chytená nanajvýš jedna loptička, hovoríme, že funkcia ϑ je žonglovacia funkcia, ak jej chytacia funkcia γ je permutáciou celých čísel. Žonglovanie obmedzíme na *žonglérske triky* - periodicky sa opakujúce konečné vzory. Príkladom žonglérskeho triku je periodicky sa opakujúca postupnosť ... 12345... (Obrázok 8).

i	...	-3	-2	-1	0	1	2	3	4	5	6	...
$\vartheta(i)$	...	3	4	5	1	2	3	4	5	1	2	...
$\gamma(i)$	...	0	2	4	1	3	5	7	9	6	8	...

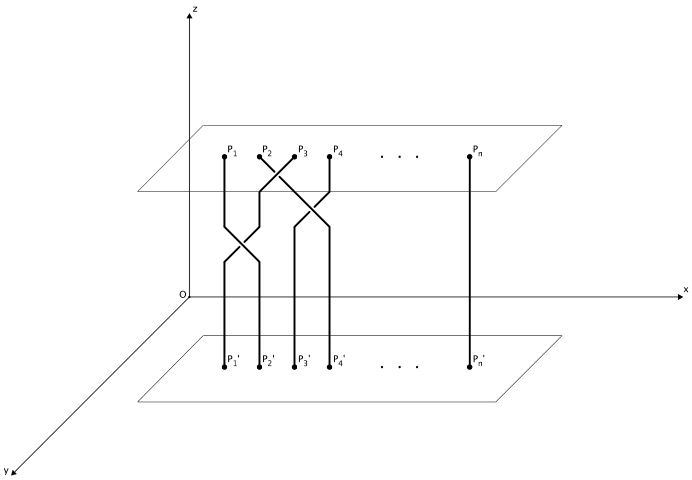


Obr. 8. Žonglovanie hodov o výškach 12345, ktoré sa periodicky opakujú.

Keďže výšky hodov sa opakujú periodicky, stačí nám k popisu žonglérskeho triku len konečná postupnosť. *Žonglovacia postupnosť* alebo *siteswap* je postupnosť výšok hodov $h_0, h_1, \ldots, h_{p-1}$ periodickej žonglovacej funkcie ϑ, kde $h_{k \mod p} = \vartheta(k \mod p), k \in \mathbb{Z}$ a p je dĺžka periódy.

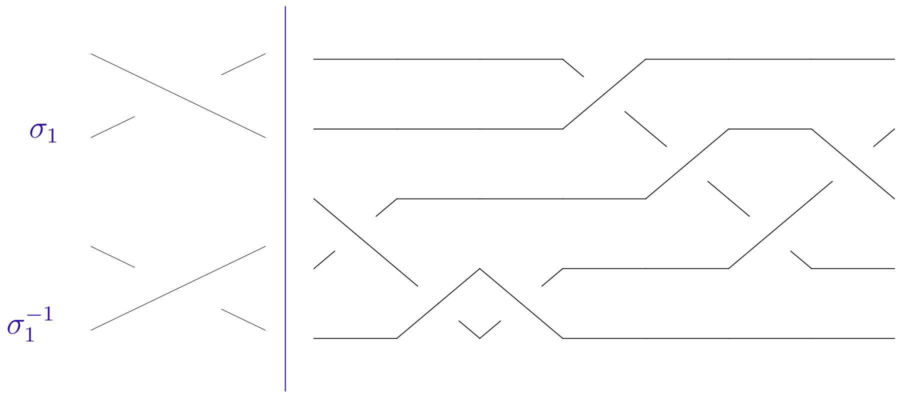
2.2 Vrkoče siteswapov

Keďže vrkoče nepatria do všeobecne známej oblasti matematiky, uvádzame ich definíciu. K matematickému popisu vrkoča vychádzame z trojrozmerného priestoru, v ktorom sa nachádzajú dve rovnobežné roviny (Obrázok 9). Vytýčime vo vrchnej rovine n bodov $P_1, P_2, \ldots, P_n$



Obr. 9. Priestorový model vrkoču.

rovnomerne rozdelených na priamke a premietneme ich kolmo do druhej roviny. Priemetmi sú body $P'_1, P'_2, \ldots, P'_n$. Body $P_1, P_2, \ldots, P_n$ nazývame *začiatočné vrcholy*, body $P'_1, P'_2, \ldots, P'_n$ *koncové vrcholy* vrkoča. Pre každé $i \in \{1, 2, \ldots, n\}$ prepojíme body P_i a $P'_{\pi(i)}$, kde π je permutácia množiny $\{1, 2, \ldots, n\}$, krivkou v páse medzi danými rovinami. Každú krivku nahradíme lomenou čiarou tak, že v každom horizontálnom reze rovinou sa pretnú nanajvýš dve takéto lomené čiary a žiadna čiara nepretína sama seba. Túto lomenú čiaru nazývame *šnúrkou*. Vrkoč vytvorený z n šnúrok nazývame n-*vrkoč*. Kolmý priemet vrkoča do roviny, v ktorej ležia začiatočné a koncové body, nazývame *vrkočový diagram*. V našich obrázkoch prechádzame vrkočový diagram vždy zľava doprava.

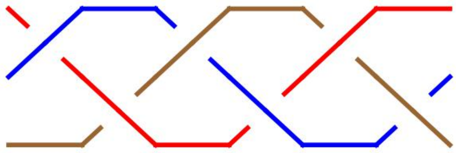
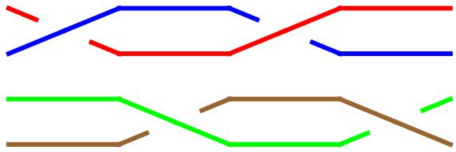
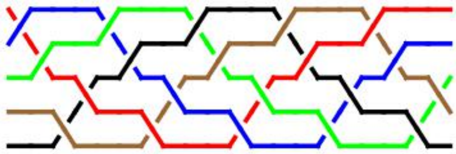
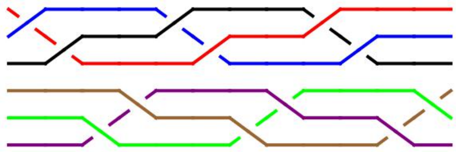
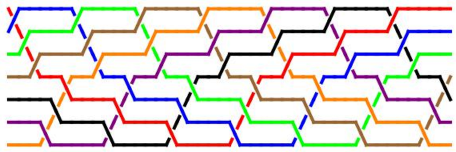


Obr. 10. Vrkočové generátory a vrkočové slovo $\sigma_3\sigma_4^{-1}\sigma_4\sigma_1^{-1}\sigma_2^{-1}\sigma_3^{-1}\sigma_3$.

Stručne zhrnieme vlastnosti vrkočov, ktoré budú pre nás prínosné v skúmaní žonglovania. Vrkoče majú štruktúru neabelovskej grupy. Triviálny vrkoč je vytvorený z n rovných šnúrok. Dva vrkoče sú ekvivalentné ak môžeme jeden previesť na druhý spojitou deformáciou (jednoducho povedané, nemôžeme šnúrky pri deformácii rozstrihnúť). Zloženie dvoch vrkočov si môžeme predstaviť ako prilepenie koncových bodov prvého vrkoča k začiatočným bodom druhého vrkoča. Opačný vrkoč je obraz vrkoča osovo súmerný podľa roviny prechádzajúcej jeho koncovými vrcholmi. Vrkočová grupa je tvorená dvoma generátormi. V oboch generátoroch sa šnúrka na pozícii i a šnúrka na pozícii $i+1$ pretnú. Ak šnúrka na pozícii i prechádza ponad šnúrku na pozícii

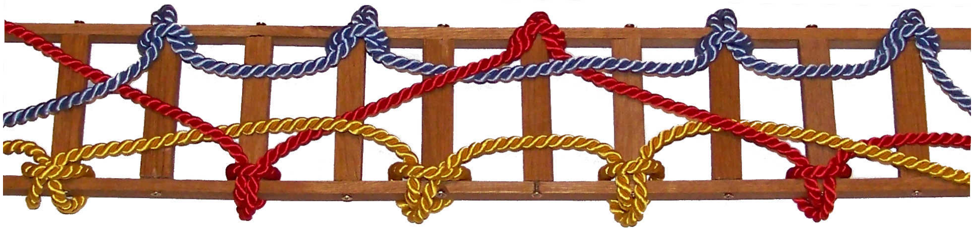
$i+1$, označíme generátor σ_i (Obrázok 10 (vľavo hore)). Ak šnúrka na pozícii i prechádza popod šnúrku na pozícii $i+1$, označíme generátor σ_i^{-1} (Obrázok 10 (vľavo dole)). Skladaním generátorov môžeme vytvoriť ľubovoľný vrkoč. Použitím uvedeného symbolického zápisu môžeme reprezentovať každý vrkoč jeho *vrkočovým slovom*. Príklad vrkoča a vrkočového slova je na Obrázku 10 (vpravo). Nie je našim cieľom ďalšie štúdium vlastností vrkočov. Pre čitateľa so záujmom o túto tému doporučujeme klasické práce o teórii vrkočov [1, 6, 5].

Ak popíšeme žonglovacie vzory pomocou vrkočov, dostaneme na rozdiel od siteswapového zápisu dodatočnú informáciu o tom, či trajektória loptičiek prechádza ponad, respektíve popod ďalšie trajektórie. Zápis kaskád a fontán pomocou vrkočových slov s vrkočovým diagramom uvádzame v Tabuľke 1.

b	vrkočové slovo	vrkočový diagram
3	$\sigma_1^{-1}\sigma_2\sigma_1^{-1}\sigma_2\sigma_1^{-1}\sigma_2$	
4	$\sigma_1^{-1}\sigma_3\sigma_1^{-1}\sigma_3$	
5	$\sigma_1^{-1}\sigma_2^{-1}\sigma_4\sigma_3\ldots\sigma_1^{-1}\sigma_2^{-1}\sigma_4\sigma_3$	
6	$\sigma_1^{-1}\sigma_2^{-1}\sigma_5\sigma_4\ldots\sigma_1^{-1}\sigma_2^{-1}\sigma_5\sigma_4$	
7	$\sigma_1^{-1}\sigma_2^{-1}\sigma_3^{-1}\sigma_6\sigma_5\sigma_4\ldots\sigma_1^{-1}\sigma_2^{-1}\sigma_3^{-1}\sigma_6\sigma_5\sigma_4$	
$\vdots$ $2n$ $2n+1$	 $\sigma_1^{-1}\sigma_2^{-1}\ldots\sigma_{n-1}^{-1}\sigma_{2n-1}\sigma_{2n-2}\ldots\sigma_{n+1}$ n-krát $\sigma_1^{-1}\sigma_2^{-1}\ldots\sigma_n^{-1}\sigma_{2n}\sigma_{2n-1}\ldots\sigma_{n+1}$ $(2n+1)$-krát	

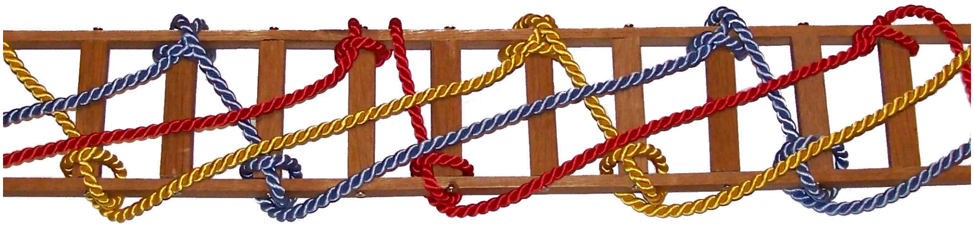
Tab. 1. Vrkočové slová a digramy pre kaskády a fontány s b loptičkami žonglovanými na vnútorné hody.

Ku konštrukcii vrkočov siteswapov môžeme vhodne použiť rebrík. Každý schod na rebríku reprezentuje jeden úder, pričom ruky prechádzajú po bočných stranách rebríka. Na Obrázku 11 môžeme vidieť žonglovací vrkoč siteswapu 423 s tromi loptičkami žonglovanými na vnútorné hody. Žltá loptička hodená do výšky 4 z pravej ruky prechádza popod červenú loptičku dopadajúcu do pravej ruky. Modrá loptička je hodená do výšky 2 z ľavej ruky a nekríži sa so žiadnou inou. Následne červená loptička je hodená do výšky 3 z pravej ruky a prechádza popod žltú loptičku dopadajúcu do pravej ruky. Modrá loptička je hodená z ľavej ruky a prechádza popod červenú loptičku dopadajúcu do ľavej ruky.



Obr. 11. Rebrík siteswapu 423 žonglovaného vnútornými hodmi.

Žonglér si na každý úder môže vybrať, či prevedie vnútorný alebo vonkajší hod. Či sa jednalo o vnútorné alebo vonkajšie hody bolo v kaskádach a fontánach jednoduché spozorovať. Avšak rozlíšiť vnútorné a vonkajšie hody už nebude také jednoduché v siteswapoch s hodmi o rôznych výškach. Napríklad v siteswape 51 s tromi loptičkami (Obrázok 12) je vrkoč rovnaký pre vnútorné aj vonkajšie hody. Pravidlá pohybu loptičky pri použití vnútorných hodov a vonkajších



Obr. 12. Rebrík siteswapu 51.

hodov popíšeme nasledovne:

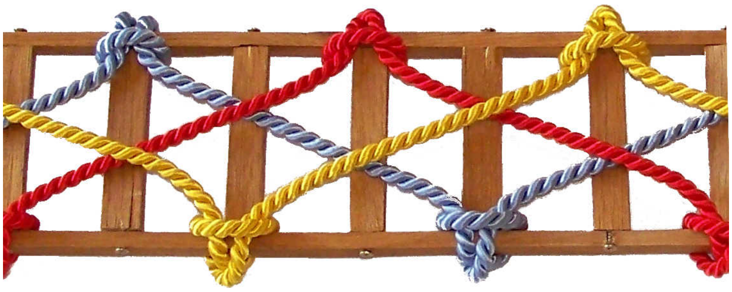
(i) Práve vyhodená loptička vnútorným (vonkajším) hodom prechádza popod (ponad) všetky loptičky, ktoré boli vyhodené skôr a dopadnú skôr ako daná loptička. Pritom uvažované loptičky dopadajú do rovnakej ruky, z ktorej vyhadzujeme.

(ii) Práve vyhodená loptička vnútorným (vonkajším) hodom nepárnej výšky prechádza popod všetky loptičky, ktoré boli vyhodené skôr a dopadnú neskôr ako daná loptička.

(iii) Práve vyhodená loptička vnútorným (vonkajším) hodom párnej výšky prechádza popod všetky loptičky, ktoré boli vyhodené skôr a dopadnú neskôr ako daná loptička. Pritom uvažované loptičky dopadajú do rovnakej ruky, z ktorej vyhadzujeme.

Takto uvedená definícia vnútorných a vonkajších hodov je síce založená na matematickom modeli, no platí aj pre praktické žonglovanie. Pre skúseného žongléra s viacerými objektmi, ktorý dokáže ľubovoľne obmieňať vnútorné a vonkajšie hody, je dokonca prirodzené voliť pohyby rúk tak, aby dráhy loptičiek spĺňali tieto pravidlá. Ako príklad uvedieme klasický žonglérsky trik, ktorý využíva obmeny vnútorných a vonkajších hodov v kaskáde a nazývame ho *tenis* (Obrázok 13).

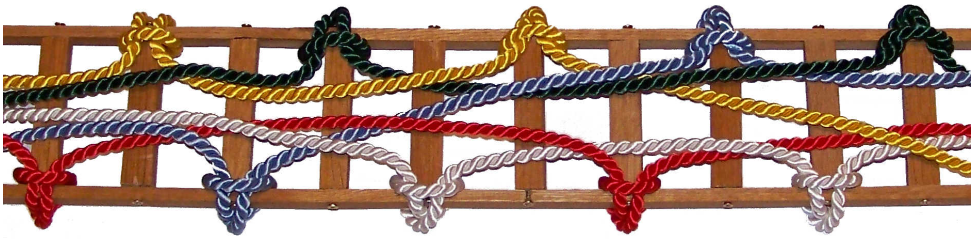
Je zrejmým pozorovaním, že žonglovaním triku tenis počas šiestich úderov dostaneme triviálny vrkoč. Vo všeobecnosti, ak máme siteswapy s rovnakým počtom loptičiek, môžeme ich skladať vhodným použitím vrkočov. Aby pri zložení nedošlo k zámene loptičiek, musíme dodržať



Obr. 13. Rebrík triku tenis s tromi loptičkami - kaskáda žonglovaná opakovaním vnútorného, vnútorného a vonkajšieho hodu. Trajektória žltej loptičky prechádza vždy ponad trajektórie červenej a modrej loptičky.

rozmiestnenie farieb jednotlivých šnúrok. K tomu potrebujeme vedieť počet úderov, za ktorý sa celý vrkoč vráti do svojej začiatočnej pozície.[3] To znamená, že hľadáme počet opakovaní daného siteswapu o perióde p. Nazvime *orbitou loptičky* všetky jej hody v danom žonglovaní. V každom siteswape s viac než jednou loptičkou môže existovať viac zhodných orbít pre rôzne loptičky, alebo môžu mať rôzne loptičky rôzne orbity.

Napríklad v siteswape 645 (Obrázok 14) sú dve loptičky (zelená a červená) so zhodnými orbitami hádzané do výšky 6 a tri loptičky (biela, žltá a modrá) so zhodnými orbitami sú hádzané do výšok 4 a 5.



Obr. 14. Rebrík siteswapu 645 s piatimi loptičkami žonglovanými vnútornými hodmi.

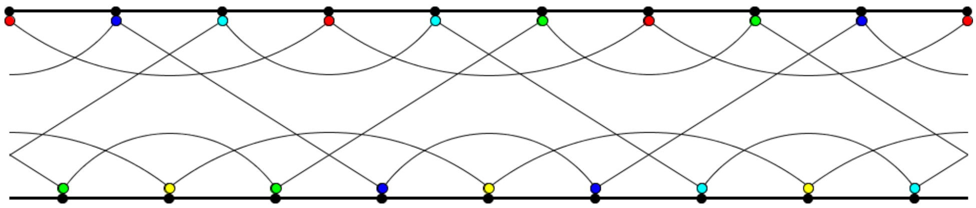
Počet opakovaní spočítame pomocou orbít žonglovacej postupnosti s periódou p nasledovne. Počet periód, ktoré ubehnú za čas, kým jedna loptička prejde svojou orbitou a začne sa opakovať, dostaneme ako súčet výšok všetkých hodov tejto loptičky vydelený periódou p. To je zároveň počet loptičiek, ktoré prechádzajú zhodné orbity $b(O_i)$.[4] V jednom siteswape sa však môže nachádzať viac rôznych orbít, a preto počítame počet ubehnutých periód ako najmenší spoločný násobok počtov loptičiek jednotlivých zhodných orbít $NSN(b(O_1), b(O_2), \ldots, b(O_m))$, pre m menšie alebo rovnajúce sa počtu loptičiek v danom žonglovaní. Pre párne periódy je počet úderov, ktoré ubehnú, kým sa siteswap začne opakovať $p \cdot NSN(b(O_1), b(O_2), \ldots, b(O_m))$. Ak je však perióda siteswapu nepárna, potrebujeme ešte ošetriť, aby vzor začínal z rovnakej ruky. To znamená, že počet ubehnutých úderov musí byť párny a preto hľadáme najmenší spoločný

[3] V terminológii teórie vrkočov potrebujeme vytvoriť takzvaný *rýdzi vrkoč, „pure braid“*.

[4] Dôkaz tohto netriviálneho tvrdenia, nazývaného v matematickej teórii žonglovania veta o aritmetickom priemere, môže čitateľ nájsť napríklad v [7, 9]. Dôsledkom tejto vlastnosti siteswapov je, že na zistenie počtu loptičiek v danom siteswape stačí spočítať jeho aritmetický priemer.

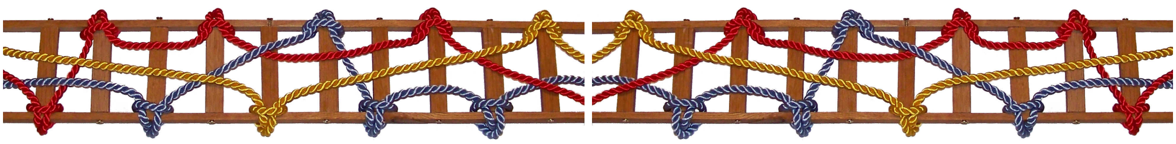
násobok počtu loptičiek jednotlivých zhodných orbít a čísla 2. Celkový počet ubehnutých úderov je potom pre dĺžku periódy p nepárnu $p \cdot NSN(2, b(O_1), b(O_2), \ldots, b(O_m))$.

Napríklad v siteswape 645 je perióda 3. Počty loptičiek v zhodných orbitách sú $b(O_1) = \frac{6}{3} = 2$, $b(O_2) = \frac{4+5}{3} = 3$, ako sme zmienili vyššie. Preto počet úderov, ktoré ubehnú, kým sa vrkoč vráti do pôvodnej pozície, je $3 \cdot NSN(2,3) = 3 \cdot 6 = 18$ (Obrázok 15).



Obr. 15. Rebríkový diagram na osemnástich úderoch siteswapu 645.

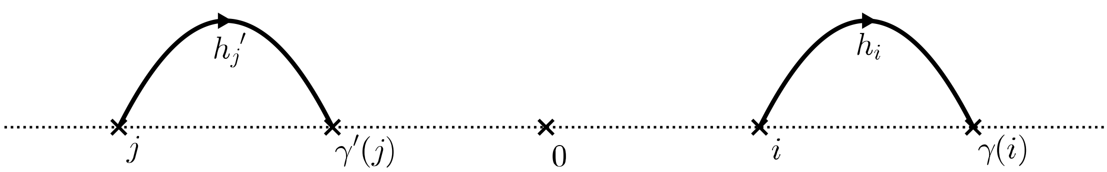
Z vlastností grupy plynie, že zložením vrkoča a opačného vrkoča vzniká triviálny vrkoč. Inak povedané, opačný vrkoč (osovo súmerný obraz) rozuzlí pôvodný vrkoč. Ak použijeme zavedený rebrík, tak schody rebríka reprezentujú čas, pričom opačný vrkoč tento čas otočí. Aby sme ukázali, že opačný žonglovací vrkoč reprezentuje nejaký žonglovací vzor, stačí si nahrať žongléra na video a pustiť toto video pospiatky. Žonglér bude samozrejme žonglovať, výšky hodov budú rovnaké (ich poradie sa však môže zmeniť) a vnútorné hody sa zmenia na vonkajšie a naopak (Obrázok 16).



Obr. 16. Žonglovací vrkoč siteswapu 12345 žonglovaný na vnútorné hody a jeho opačný vrkoč, ktorý reprezentuje siteswap 52413 žonglovaný na vonkajšie hody.

Platí teda nasledovná veta, ktorej jednoduchý dôkaz danú opačnú postupnosť priamo skonštruuje.

Veta 1 (Veta)**.** Nech je daný siteswap $h = \{h_k\}_{k=0}^{p-1}$. Siteswap h^{-1}, ktorý vznikne obrátením časovej osi je siteswap. Siteswap h^{-1} nazývame *reverzný siteswap k siteswapu* h.



Obr. 17. Vytvorenie reverzného siteswapu.

Dôkaz. Použijeme chytaciu funkciu, ktorú dostaneme periodickým opakovaním siteswapu $\gamma(i) = h_i + i$. Údery vyhodenia loptičky i sa pri obrátení času stanú údermi dopadu a naopak. Hody budú prebiehať opačne, avšak ich výšky sa nezmenia. Funkcia γ je permutáciou celých čísel, preto pre každé $j \in \mathbf{Z}$ existuje $i_j \in \mathbf{Z}$ také, že $\gamma(i_j) = -j$. Definujme ďalej $h'_j = h_{i_j}$ a $\gamma'(j) = h'_j + j$.

Platí, že $\gamma'(j) = h'_j + j = h_{i_j} - \gamma(i_j) = -i_j$ a γ' je zrejme permutáciou. Rozdelením periodickej postupnosti hodov $\{h_j\}$ na intervaly dostaneme siteswap (Obrázok 17). $\square$

Majme daný siteswap 12345 žonglovaný vnútornými hodmi.

$$\begin{array}{c|ccccc} i & 0 & 1 & 2 & 3 & 4 \\ h_i & 1 & 2 & 3 & 4 & 5 \\ \gamma(i) \mod 5 & 1 & 3 & 0 & 2 & 4 \end{array}$$

K nemu reverzný siteswap 52413 dostaneme podľa konštrukcie dôkazu predošlej vety.

$$\begin{array}{c|rrrrr} j & -4 & -3 & -2 & -1 & 0 \\ i_j & 4 & 1 & 3 & 0 & 2 \\ h'_j & 5 & 2 & 4 & 1 & 3 \\ \gamma'(j) \mod 5 & 1 & 4 & 2 & 0 & 3 \end{array}$$

Reverzný siteswap sa môže zhodovať s pôvodným siteswapom (u kaskád a fontán je to zrejmé). Pripomeňme si siteswap 423 hádzaný vnútornými hodmi (Obrázok 11)

$$\begin{array}{c|ccc|} i & 0 & 1 & 2 \\ & & & \\ h_i & 4 & 2 & 3 \\ \gamma(i) \mod 3 & 1 & 0 & 2 \end{array}$$

a vytvorme k nemu reverznú postupnosť.

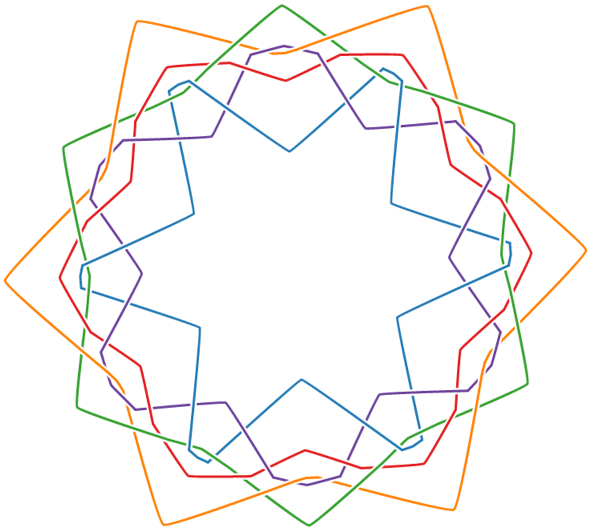
$$\begin{array}{|c|rrr} j & -2 & -1 & 0 \\ i_j & 2 & 0 & 1 \\ h'_j & 3 & 4 & 2 \\ \gamma'(j) \mod 3 & 1 & 0 & 2 \end{array}$$

Reverznou žonglovacou postupnosťou bude rovnaká postupnosť 423, hádzaná však vonkajšími hodmi.

Čitateľovi, ktorý by mal záujem o ďalšie experimenty, odporúčame nedávno spustenú webovú aplikáciu [11], ktorá dokáže vytvoriť vrkoče zadaných siteswapov žonglovaných vnútornými hodmi. Okrem vrkoča v rovine je v nej možné vytvoriť aj vrkoč v anuloide, čo odpovedá modelu trajektórií, keď žonglér kráča po kružnici. Príklady použitia pre 6 periód žonglovania siteswapu 97531 uvádzame v Obrázkoch 18,19.

3 Záver

Empiricky sme preskúmali dráhy loptičiek na mnohých prípadoch žonglovacích vzorov za pomoci elementárnych vlastností teórie vrkočov. Otvára sa nám tak brána k ďalšiemu štúdiu zaujímavých vlastností žonglovania, ako napríklad správanie sa reverzných siteswapov. Autori v článku [3] dokázali zaujímavú vetu, ktorá tvrdí, že každý vrkoč sa dá zažonglovať. Hlavnou myšlienkou je konštrukcia siteswapov vrkočových generátorov a následné zloženie



Obr. 18. Vrkoč v anuloide siteswapu 97531.
Zdroj: https://juggling.graphics/

ľubovoľného vrkoča. Nanešťastie, ponúknutá konštrukcia je prakticky nerealizovateľná. Sme však presvedčení, že za použitia vnútorných a vonkajších hodov tak, ako boli zadefinované, je možné toto tvrdenie dokázať a bude to v našom záujme do budúcnosti. Téma matematiky žonglovania je síce okrajová, no najmä pre matematikov, ktorí majú žonglovanie ako svoje hobby, je veľmi inšpiratívna. Za zmienku stoja veľké osobnosti matematiky ako Claude Shannon, ktorý použil matematický podklad žonglovania ku konštrukcii robotického žongléra, či Ronald Graham - jedna z vedúcich osobností kombinatoriky, ktorý napísal o žonglovaní niekoľko matematických článkov. Na druhú stranu, nakoľko matematický popis žonglovania sa dostal do bežného jazyka žonglérov, núti ich tak precvičovať si svoje matematické schopnosti. Dúfame, že tých, ktorí uvažovali nad zmyslom matematického skúmania žonglovania, sme presvedčili, že žonglovanie je vynikajúca aplikácia niekoľkých abstraktných matematických teórií vhodná pre hľadanie ich vzájomných súvislostí.

Obr. 19. Vrkoč siteswapu 97531.
Zdroj: https://juggling.graphics/

Poďakovanie

Tento výstup vznikol v rámci projektu SVV 2017 č. 260454.

Literatúra

[1] ARTIN, E. Theory of braids. In *Annals of mathematics*, 1947, vol. 48, no. 1, pp. 101-126.

[2] BUHLER, J., EISENBUD, D., GRAHAM, R., WRIGHT, C. Juggling drops and descents. In *American Mathematical Monthly*, 1994, vol. 101, no. 6, p. 507-519.

[3] DEVADOSS, S. L., MUGNO, J. Juggling Braids and Links. In *The Mathematical Intelligencer*, 2007, vol. 29, no. 3, p. 15-22.

[4] MACAULEY, M. *Braids and Juggling Patterns.* Senior thesis, Harvey Mudd College, Claremont, 2003.

[5] MORAN, S. *The Mathematical Theory of Knots and Braids.* Amsterdam: Elsevier Science Publishers B.V., 1983.

[6] MURASUGI, K. *Knot Theory.* Boston: Birkhäuser, 1996.

[7] POLSTER, B. *The Mathematics of Juggling.* New York: Springer - Verlag, 2003.

[8] TAWNEY, J. *Jugglinks.* Master's Thesis, The Ohio State University, 2001.

[9] ZAMBOJ, M. *Matematická teorie žonglování.* Diplomová práca, Univerzita Karlova, Praha, 2014.

[10] ZAMBOJ, M. Braids of Juggling Patterns. In *Proceedings of the Czech-Slovak Conference on Geometry and Graphics 2016*, Rožnov pod Radhoštem, 207-216.

[11] `https://juggling.graphics/`

Mgr. Michal Zamboj

Matematický ústav
Matematicko-fyzikální fakulta
Univerzita Karlova
Sokolovská 83, Praha, ČR
e-mail: zamboj@karlin.mff.cuni.cz

SLOVENSKÁ SPOLOČNOSŤ

SG

PRE GEOMETRIU A GRAFIKU

SLOVAK SOCIETY FOR GEOMETRY AND GRAPHICS

is a non-profit scientific organisation with the objective
to stimulate scientific research and teaching methodology
in the fields of geometry and computer graphics
and to foster international collaboration.

SSGG informs on organisation of different scientific events related to geometry and computer graphics organised in Slovakia.

SSGG provides a platform for donations and sponsorship of scientific workers in the related fields (especially young ones) in order to stimulate scientific development in these disciplines and to enhance the quality of geometry and graphics education of engineers and designers particularly.

Society is publisher of G, the first Slovak scientific journal for geometry and graphics.

All other activities dealing with dissemination of knowledge in the fields of geometry and graphics are welcome, discussion forum on Internet, software market, workshops, Internet courses and chats, etc., and can be provided within the scope of society activities.

Slovak Society for Geometry and Graphics is a collective member of ISGG - International Society for Geometry and Graphics.

SSGG
Institute of Mathematics and Physics
Faculty of Mechanical Engineering
Slovak University of Technology in Bratislava
Námestie slobody 17, 812 31 Bratislava, SR
e-mail: info@ssgg.sk, URL: www.ssgg.sk

Abstracts

I. Abrhan: On ideals in semigroups S_m of residual classes (mod m), on minimal and maximal ideals in S_m with respect to its subsets – local Euler-Fermat theorem

Concept of maximal independent system of principle ideals in the semigroup S_m residual classes (mod m) is defined in the first part of this paper, and subsets of semigroup S_m are defined by means of this maximal independent system of principle ideals. There are also proved theorems on minimal and maximal ideals in S_m and theorems on minimal ideals in the ring S_m with respect to these subsets of S_m .
Properties of such principle ideals in S_m that contain unit element are studied in the second part of this paper Local Euler-Fermat theorem is proved in the third part.

B. Odehnal: Rational minimal surfaces tangent to E. Müller's surface

We study a new class of minimal surfaces which are in line contact with a special cubic surface. It turns out that these minimal surfaces admit rational parametrizations and carry a one-parameter family of higher order harmonic oscillation curves. Each of these minimal surfaces defines its own one-parameter family of associated minimal surfaces which in turn are all algebraic. Moreover, they also admit rational parametrizations.

D. Velichová: Minkowski sum and product of free-form curves

Paper deals with Minkowski point set operations applied to free-form (approximation and interpolation) curves, determined by control polygons and interpolation blending polynomial functions. Basic properties of surfaces modelled as Minkowski sum or product of two curves are presented in addition to some of their differential properties. Two families of special curves called laces are defined by means of partial Minkowski sum and product and their intrinsic geometric properties are derived and

M. Zamboj: Braids of the juggling patterns

In the contribution, we will show a method of a graphic representation of juggling using braids. We will describe how braids improve the mathematical notation of juggling by integer sequences and reveal elementary properties of such juggling tricks.

G
Slovak Journal for Geometry and Graphics

Volume 14 (2017), No. 27
ISSN 1336-524X

Edited by:
Slovak Society for Geometry and Graphics

SSGG

G is a scientific journal covering the fields of geometry and graphics for publication of original scientific papers, review and information articles, brief reports, state-of-the-art reviews, analyses, communications and other contributions from all geometric disciplines (elementary, descriptive, constructive, projective, analytic, coordinate, differential, algebraic, computer, computational, finite, non-Euclidean) and topology, geometric modelling and computer graphics, in the area of the basic theoretical research, education of geometry in all types of schools, from the history and methodology of the development of geometry and on applications of geometry and geometric methods in different scientific, social and technical disciplines.

Editorial office: Slovak Society for Geometry and Graphics
Faculty of Mechanical Engineering
Slovak University of Technology in Bratislava
Námestie slobody 17
812 31 Bratislava, Slovakia

Correspondence concerning subscriptions, claims and distribution:
Redakcia G - SSGG
SjF STU, Námestie slobody 17, 812 31 Bratislava, Slovakia
ssgg@ssgg.sk

Frequency: One volume per year consisting of two issues at a price of EUR 20,- per volume, not including surface mail shipment abroad.
Evidentiary number EV 3228/09

Information and instructions for authors are available at the address: www.ssgg.sk

Printed by: ForPress Nitrianske tlačiarne, s. r. o.

G is cited in: Zentralblatt für Mathematik

www.ssgg.sk