VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA STROJNÍHO INŽENÝRSTVÍ
ÚSTAV MATEMATIKY

FACULTY OF MECHANICAL ENGINEERING
INSTITUTE OF MATHEMATICS

ALGORITMY INTERPOLACE POLYNOMY VÍCE NEURČITÝCH

ALGORITHMS OF THE INTERPOLATION BY MULTIVARIATE POLYNOMIALS

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE ALICE HAVLÍČKOVÁ
AUTHOR

VEDOUCÍ PRÁCE doc. RNDr. MIROSLAV KUREŠ, Ph.D.
SUPERVISOR

BRNO 2011

Vysoké učení technické v Brně, Fakulta strojního inženýrství

Ústav matematiky
Akademický rok: 2010/2011

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

student(ka): Alice Havlíčková

který/která studuje v **bakalářském studijním programu**

obor: **Matematické inženýrství (3901R021)**

Ředitel ústavu Vám v souladu se zákonem č.111/1998 o vysokých školách a se Studijním a zkušebním řádem VUT v Brně určuje následující téma bakalářské práce:

Algoritmy interpolace polynomy více neurčitých

v anglickém jazyce:

Algorithms of the interpolation by multivariate polynomials

Stručná charakteristika problematiky úkolu:

Práce je zaměřena na vícerozměrnou interpolaci nad libovolným polem s výhledem na použití interpolačních polynomů nad binárními poli v kryptografii. Hlavními úkoly jsou objasnění otázky existence a jednoznačnosti interpolačního polynomu a vytvoření programového balíku v prostředí Mathematica.

Cíle bakalářské práce:

- popis interpolačních algoritmů (pro případ více neurčitých)
- diskuse stupně interpolačních polynomů nad konečnými poli
- vytvoření funkčního originálního programového balíku v prostředí Mathematica, který bude obecně řešit vícerozměrnou interpolaci nad libovolným polem

Seznam odborné literatury:

[1] Schuster, D.: Multivariate Interpolationsangriffe auf symmetrische Chiffren, Diploma Thesis, Technische Universität Darmstadt, 2007

[2] Grigoriev, D. Y., Karpinski, M., Singer, M. F.: Fast parallel algorithms for sparse multivariate polynomial interpolation over finite fields, SIAM J. Comp. 19, 1059-1063, 1990

Vedoucí bakalářské práce: doc. RNDr. Miroslav Kureš, Ph.D.

Termín odevzdání bakalářské práce je stanoven časovým plánem akademického roku 2010/2011.

V Brně, dne 25.10.2010

L.S.

prof. RNDr. Josef Šlapal, CSc.	prof. RNDr. Miroslav Doupovec, CSc.
Ředitel ústavu	Děkan fakulty

Abstrakt
Tato bakalářská práce se zabývá algoritmy vícerozměrné interpolace. V první části je studován problém interpolace nad rovinou. Dále je uvedeno zobecnění Lagrangeovy interpolace pro případ více neurčitých. Diskutujeme zde také stupeň polynomu pro libovolné pole. Součástí této práce je i funkční programový balík v prostředí Mathematica, který řeší vícerozměrnou interpolaci nad libovolným polem.

Summary
This bachelor's work concerns to algorithms of the multivariate interpolation. The problem of the interpolation over the plane is studied in the first part of this work. In the next section, the multivariate Lagrange interpolation is described and the polynomial degree is discussed. A Mathematica program package was developed, by this, the multivariate interpolation over an arbitrary field can be solved.

Klíčová slova
Vícerozměrná interpolace, interpolační polynom, konečné pole

Keywords
Multivariable interpolation, interpolation polynomial, finite field

HAVLÍČKOVÁ, A. *Algoritmy interpolace polynomy více neurčitých.* Brno: Vysoké učení technické v Brně, Fakulta strojního inženýrství, 2011. 44 s. Vedoucí doc. RNDr. Miroslav Kureš, Ph.D.

Prohlašuji, že jsem bakalářskou práci „Algoritmy interpolace polynomy více neurčitých" vypracovala samostatně s použitím odborné literatury a pramenů, uvedených na seznamu, jenž je součástí této práce.

Alice Havlíčková

Děkuji panu doc. RNDr. Miroslavu Kurešovi, Ph.D. za rady, věnovaný čas a odborné vedení při tvorbě této bakalářské práce.

Alice Havlíčková

Obsah

1. Úvod

Interpolace se využívá obvykle v numerické matematice. Jejím cílem bývá nalézt přibližné hodnoty funkce v nějakém intervalu, je-li hodnota této funkce známa pouze v některých jiných bodech tohoto intervalu. Motivace pro vícerozměrnou interpolaci ale může být i jiná. Například existují tzv. vícerozměrné kryptografické systémy, které transformují zprávu za pomoci několika polynomů více neurčitých. Nalezení těchto polynomů při známé zprávě pak představuje kryptoanalytickou úlohu. Existuje také velké množství prací, které popisují interpolaci nad konečnými poli [1].

V naší práci se zabýváme popisem algoritmů pro případ polynomů více neurčitých. Diskutujeme také stupeň interpolačního polynomu pro konečná pole. Posledním naším cílem je vytvoření funkčního programového balíku v prostředí Mathematica, který řeší vícerozměrnou interpolaci nad libovolným polem.

Úvodní kapitola práce pojednává o afinní transformaci, kde odvozujeme matici této transformace. V následující kapitole řešíme interpolaci v rovině, kde využíváme matici afinní transformace pro zjednodušení případů. Interpolaci v rovině jsme vyřešili z hlediska náročnosti pro $4, 5$ a 6 bodů a to přímo, řešením soustavy rovnic. Zjišťujeme zvláštní polohu podkladových bodů a následně řešíme počet řešení proložení kvadriky zadanými body. V kapitole o vícerozměrné interpolaci řešíme algoritmy nevyžadující řešení soustavy rovnic. Uvádíme zde dva způsoby, jak lze vícerozměrnou interpolaci řešit Lagrangeovou metodou. V poslední kapitole pak popisujeme notebook řešící vícerozměrnou interpolaci nad libovolným polem.

Cílem naší práce je tedy popsat algoritmy vícerozměrné intepolace nad libovolným polem a vytvořit funkční notebook, který bude tuto interpolaci řešit.

2. Afinní transformace

Budeme se zabývat afinními transformacemi zobrazujícími bod $P = [x, y]$ na bod $Q = [x_1, y_1]$. Tyto transformace zahrnují posunutí, otočení, změně měřítka, zkosení, nebo operaci vzniklé jejich skládáním. Afinní transformace zachovává kolinearitu mezi body a poměry vzdáleností na přímce. Obecně, afinní transformace je složena z lineární transformace a posunutí.

Nyní popíšeme afinní transformaci nad reálnými čísly, která zajistí, aby se libovolné dva různé body o souřadnicích $[p_1, p_2]$, $[q_1, q_2]$ zobrazili do bodů $[0, 0]$ a $[1, 0]$.

1. **Posunutí o vektor (a, b):**

$$\begin{pmatrix} 1 \\ X \\ Y \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ a & 1 & 0 \\ b & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ x \\ y \end{pmatrix}$$

$X = a + x$
$Y = b + y$
Bod $[1, x, y]$ se posune do bodu $[1, X, Y]$.

2. **Otočení o úhel φ:**

$$\begin{pmatrix} 1 \\ X' \\ Y' \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\varphi & -\sin\varphi \\ 0 & \sin\varphi & \cos\varphi \end{pmatrix} \cdot \begin{pmatrix} 1 \\ X \\ Y \end{pmatrix}$$

$X' = X \cdot \cos\varphi - Y \cdot \sin\varphi$
$Y' = X \cdot \sin\varphi + Y \cdot \cos\varphi$

3. **Homotetie:**

$$\begin{pmatrix} 1 \\ X'' \\ Y'' \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & k & 0 \\ 0 & 0 & k \end{pmatrix} \cdot \begin{pmatrix} 1 \\ X' \\ Y' \end{pmatrix}$$

$X'' = k \cdot X'$
$Y'' = k \cdot Y'$
Z toho vyplívá
$X'' = k \cdot a \cdot \cos\varphi + k \cdot x \cdot \cos\varphi - k \cdot b \cdot \sin\varphi - k \cdot y \cdot \sin\varphi$
$Y'' = k \cdot a \cdot \sin\varphi + k \cdot x \cdot \sin\varphi + k \cdot b \cdot \cos\varphi + k \cdot y \cdot \cos\varphi$
A tedy matice celkové transformace je:

$$\begin{pmatrix} 1 \\ X'' \\ Y'' \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ k \cdot a \cdot \cos\varphi - k \cdot b \cdot \sin\varphi & k \cdot cos\varphi & -k \cdot \sin\varphi \\ k \cdot a \cdot \sin\varphi + k \cdot b \cdot \cos\varphi & k \cdot \sin\varphi & k \cdot \cos\varphi \end{pmatrix} \cdot \begin{pmatrix} 1 \\ x \\ y \end{pmatrix}$$

pro zjednodušení označíme výslednou matici maticí A.
Nyní zbývá pouze určit koeficienty a, b, k, φ.
$a = -p_1$
$b = -p_2$
$\varphi = \arctan\left(\frac{p_2 - q_2}{q_1 - p_1}\right)$
$k = \frac{\sqrt{1 + \left(\frac{p_2 - q_2}{q_1 - p_1}\right)^2} \cdot (q_1 - p_1)}{(q_1 - p_1)^2 + (p_2 - q_2)^2}$

Poté můžeme výslednou matici transformace zapsat ve tvaru:

$$\mathbf{A} = \begin{pmatrix} 1 & 0 & 0 \\ \frac{-p_1 \cdot q_1 + p_1^2 - p_2 \cdot q_2 + p_2^2}{(q_1-p_1)^2+(q_2-p_2)^2} & \frac{q_1-p_1}{(q_1-p_1)^2+(q_2-p_2)^2} & \frac{q_2-p_2}{(q_1-p_1)^2+(q_2-p_2)^2} \\ \frac{-p_2 \cdot q_1 + p_1 \cdot q_2}{(q_1-p_1)^2+(q_2-p_2)^2} & \frac{p_2-q_2}{(q_1-p_1)^2+(q_2-p_2)^2} & \frac{q_1-p_1}{(q_1-p_1)^2+(q_2-p_2)^2} \end{pmatrix}$$

A její inverzní matici ve tvaru:

$$\mathbf{A^{-1}} = \begin{pmatrix} 1 & 0 & 0 \\ p_1 & q_1 - p_1 & p_2 - q_2 \\ q_2 & q_2 - p_2 & q_1 - p_1 \end{pmatrix}$$

Nyní si ukážeme použití matice transformace na příkladu. Mějme body $P = [10, 2^{\sqrt{2}}], Q = [\sqrt[3]{7}, 1], R = [-2, \frac{2}{3}], S = [\sqrt{5}, -4]$. Dosazením bodů P, Q do matice transformace dostáváme:

$$\mathbf{A} = \begin{pmatrix} 1 & 0 & 0 \\ \frac{-10 \cdot \sqrt[3]{7} + 10^2 - 2^{\sqrt{2}} \cdot 1 + (2^{\sqrt{2}})^2}{\left(\sqrt[3]{7}-10\right)^2+\left(1-2^{\sqrt{2}}\right)^2} & \frac{\sqrt[3]{7}-10}{\left(\sqrt[3]{7}-10\right)^2+\left(1-2^{\sqrt{2}}\right)^2} & \frac{1-2^{\sqrt{2}}}{\left(\sqrt[3]{7}-10\right)^2+\left(1-2^{\sqrt{2}}\right)^2} \\ \frac{-2^{\sqrt{2}} \cdot \sqrt[3]{7} + 10 \cdot 1}{\left(\sqrt[3]{7}-10\right)^2+\left(1-2^{\sqrt{2}}\right)^2} & \frac{2^{\sqrt{2}}-1}{\left(\sqrt[3]{7}-10\right)^2+\left(1-2^{\sqrt{2}}\right)^2} & \frac{\sqrt[3]{7}-10}{\left(\sqrt[3]{7}-10\right)^2+\left(1-2^{\sqrt{2}}\right)^2} \end{pmatrix}$$

Vynásobením této matice příslušnými body dostaneme ztransformované body o souřadnicích $P_1 = [0, 0], Q_1 = [1, 0], R_1 = [\frac{362 - 5 \cdot 2^{\sqrt{2}} + 3 \cdot 4^{\sqrt{2}} - 36 \cdot \sqrt[3]{7}}{3 \cdot (101 - 2^{1+\sqrt{2}} + 4^{\sqrt{2}} - 20 \cdot \sqrt[3]{7} + (\sqrt[3]{7})^2)}, \frac{16 - 3 \cdot 2^{1+\sqrt{2}} + 2 \cdot \sqrt[3]{7} - 3 \cdot 2^{\sqrt{2}} \cdot \sqrt[3]{7}}{3 \cdot (101 - 2^{1+\sqrt{2}} + 4^{\sqrt{2}} - 20 \cdot \sqrt[3]{7} + (\sqrt[3]{7})^2)}]$, $S_1 = [\frac{96 + 3 \cdot 2^{\sqrt{2}} + 4^{\sqrt{2}} - 10\sqrt{5} - 10 \cdot \sqrt[3]{7} + \sqrt{5} \cdot \sqrt[3]{7}}{101 - 2^{1+\sqrt{2}} + 4^{\sqrt{2}} - 20 \cdot \sqrt[3]{7} + (\sqrt[3]{7})^2}, -\frac{-50 + \sqrt{5} - 2^{\sqrt{2}} \cdot \sqrt{5} + 4 \cdot \sqrt[3]{7} + 2^{\sqrt{2}} \cdot \sqrt[3]{7}}{101 - 2^{1+\sqrt{2}} + 4^{\sqrt{2}} - 20 \cdot \sqrt[3]{7} + (\sqrt[3]{7})^2}]$.

Afinní transformaci lze uvažovat i nad konečnými poli, ovšem s příslušnými modifikacemi: například nemá geometrický smysl uvažovat otočení o úhel φ.

3. Interpolace nad $4, 5$ a 6 body v rovině

3.1. Čtyři body nad rovinou

Vězměme 4 různé body $P = [p_1, p_2, p_3]$, $Q = [q_1, q_2, q_3]$, $R = [r_1, r_2, r_3]$, $S = [s_1, s_2, s_3]$. Označíme $\hat{P} = [p_1, p_2]$, $\hat{Q} = [q_1, q_2]$, $\hat{R} = [r_1, r_2]$, $\hat{S} = [s_1, s_2]$. Bez újmy na obecnosti lze předpokládat, že $\hat{P} = [0, 0]$, $\hat{Q} = [1, 0]$. Toto jsme již ukázali v kapitole o afinní transformaci.

Hledáme kvadriku

$$a + bx + cy + dx^2 + exy + fy^2 = z$$

tzn. řešíme :

$$\begin{pmatrix} 1 & p_1 & p_2 & p_1^2 & p_1p_2 & p_2^2 \\ 1 & q_1 & q_2 & q_1^2 & q_1q_2 & q_2^2 \\ 1 & r_1 & r_2 & r_1^2 & r_1r_2 & r_2^2 \\ 1 & s_1 & s_2 & s_1^2 & s_1s_2 & s_2^2 \end{pmatrix} \cdot \begin{pmatrix} a \\ b \\ c \\ d \\ e \\ f \end{pmatrix} = \begin{pmatrix} p_3 \\ q_3 \\ r_3 \\ s_3 \end{pmatrix}$$

Stručně $(M \cdot \vec{h}) = \vec{v}$

Jde o soustavu lineárních rovnic. Pro rozhodnutí o její řešitelnosti musíme zkoumat hodnost matice M (značíme rank M).

Vezměme naši volbu $\hat{P}$, $\hat{Q}$. Pak

$$M = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & r_1 & r_2 & r_1^2 & r_1r_2 & r_2^2 \\ 1 & s_1 & s_2 & s_1^2 & s_1s_2 & s_2^2 \end{pmatrix}$$

Dále vezměme podmatici N jako první čtyři sloupce z matice M.

Platí: rank $N \leq$ rank $M \leq 4$.

Budeme nyní zkoumat hodnost N:

$$N = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & r_1 & r_2 & r_1^2 \\ 1 & s_1 & s_2 & s_1^2 \end{pmatrix}$$

je zřejmé, že $4 \geq$ rank $N \geq 2$. Poznamenejme dále, že případy $r_1 = r_2 = 0$ a $s_1 = s_2 = 0$ nemohou nastat.

Vezměme další podmatici U (2.-4. řádek N a 2.-4. sloupec N):

$$U = \begin{pmatrix} 1 & 0 & 1 \\ r_1 & r_2 & r_1^2 \\ s_1 & s_2 & s_1^2 \end{pmatrix}$$

Stačí vyšetřit rank U, protože rank $N = 1 +$ rank U.

Nejprve vyšetříme, kdy jsou lineárně závislé 1. a 3. sloupec. evidentně tehdy, když $r_1 = r_1^2$ a současně $s_1 = s_1^2$.

Jsou tedy čtyři možnosti:

α) $r_1 = s_1 = 0$

β) $r_1 = 0$ $s_1 = 1$

γ) $r_1 = 1$ $s_1 = 0$

δ) $r_1 = s_1 = 1$

Tyto možnosti dále analyzujme.

α)

$$U_\alpha = \begin{pmatrix} 1 & 0 & 1 \\ 0 & r_2 & 0 \\ 0 & s_2 & 0 \end{pmatrix}$$

rank $U_\alpha = 2$ (nemůže nastat $r_2 = 0$ ani $s_2 = 0$, protože $\hat{P} \neq \hat{R}$, $\hat{P} \neq \hat{S}$)

β)

$$U_\beta = \begin{pmatrix} 1 & 0 & 1 \\ 0 & r_2 & 0 \\ 1 & s_2 & 1 \end{pmatrix}$$

rank $U_\beta = 2$ (nemůže nastat $r_2 = 0$ ani $s_2 = 0$, protože $\hat{P} \neq \hat{R}$, $\hat{Q} \neq \hat{S}$)

γ)

$$U_\gamma = \begin{pmatrix} 1 & 0 & 1 \\ 1 & r_2 & 1 \\ 0 & s_2 & 0 \end{pmatrix}$$

rank $U_\gamma = 2$ (analogické jako β)

δ)

$$U_\delta = \begin{pmatrix} 1 & 0 & 1 \\ 1 & r_2 & 1 \\ 1 & s_2 & 1 \end{pmatrix}$$

rank $U_\delta = 2$ (podobné zdůvodnění)

Shrnutí: Jsou-li 1. a 3. sloupec v U lineárně závislé, pak je hodnost matice U vždy 2, protože pak už nemůže nastat $r_2 = s_2$, neboť zadané čtyři body jsou různé.

Nyní předpokládejme, že 1. a 3. sloupec v U jsou lineárně nezávislé. Hodnost U může být rovna 2 pouze tehdy, je-li 2.sloupec lineární kombinací 1. a 3. sloupce, tedy v tomto případě, je-li k-násobkem jejich rozdílu.

Tzn. $r_2 = k \cdot (r_1^2 - r_1)$ a $s_2 = k \cdot (s_1^2 - s_1)$

Případ $k = 0$ označíme ϵ: ϵ)

$$U_\epsilon = \begin{pmatrix} 1 & 0 & 1 \\ r_1 & 0 & r_1^2 \\ s_1 & 0 & s_1^2 \end{pmatrix}$$

rank $U_\epsilon = 2$ ($r_1 \neq 1$, $s_1 \neq 1$, $r_1 \neq s_1$)

Případ $k \neq 0$ označme φ: φ)

$$U_\varphi = \begin{pmatrix} 1 & 0 & 1 \\ r_1 & k(r_1^2 - r_1) & r_1^2 \\ s_1 & k(s_1^2 - s_1) & s_1^2 \end{pmatrix}$$

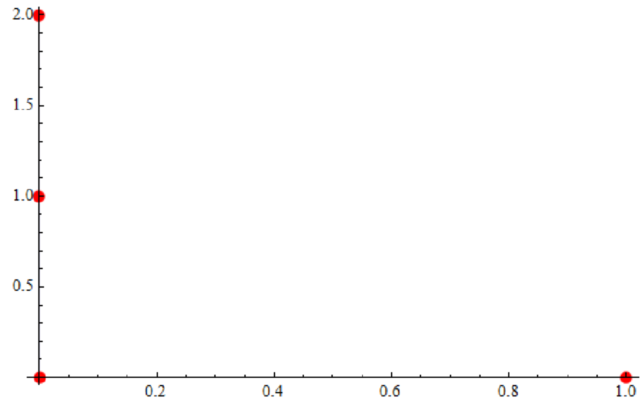
rank $U_\varphi = 2$ ($r_1 \neq 1$, $r_1 \neq 0$)

Ve všech ostatních případech je rank $U = 3$, tzn. že rank $N = 4$, tzn. rank $M = 4$ a také rank $(M|\vec{v}) = 4$ (hodnost rozšířené matice), tedy počáteční soustava má nekonečně mnoho řešení závislých na 2 libovolných parametrech.

Rozeberme nyní znovu případy α) až φ).

$\alpha)\hat{P} = [0, 0]$, $\hat{Q} = [1, 0]$, $\hat{R} = [0, r_2]$, $\hat{S} = [0, s_2]$, tj. $\hat{P}$, $\hat{R}$, $\hat{S}$ leží na přímce $x = 0$.

Obr 3.1 3 body na přímce



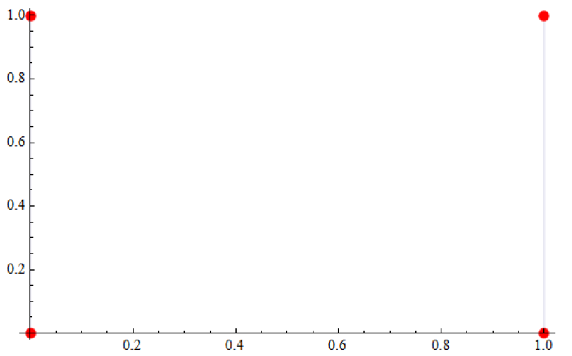
$$M = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & r_2 & 0 & 0 & r_2^2 \\ 1 & 0 & s_2 & 0 & 0 & s_2^2 \end{pmatrix}$$

rank $M = 4$ (protože $r_2 \neq s_2$)

Věta: V případě α existuje nekonečně mnoho řešení závislých na 2 libovolných parametrech.

$\beta)\hat{P} = [0, 0]$, $\hat{Q} = [1, 0]$, $\hat{R} = [0, r_2]$, $\hat{S} = [1, s_2]$. Body leží na dvou rovnoběžných přímkách o rovnicích $x = 0$, $x = 1$.

Obr 3.2 body na dvou rovnoběžkách



$$M = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & r_2 & 0 & 0 & r_2^2 \\ 1 & 1 & s_2 & 1 & s_2 & s_2^2 \end{pmatrix}$$

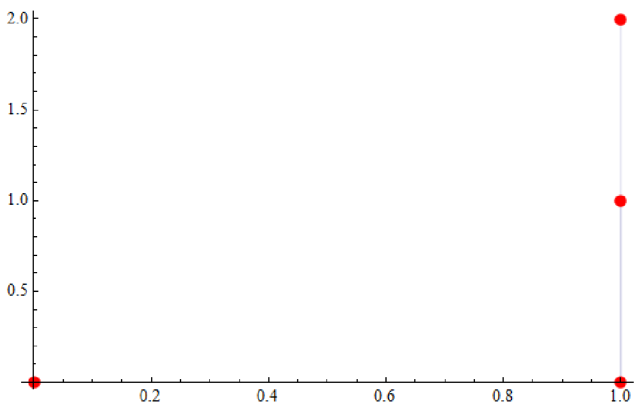
rank $M = 4$ (protože $s_2 \neq 0$)

γ) bude obdobné jako β)

Věta: V případech β, γ existuje nekonečně mnoho řešení závislých na 2 libovolných parametrech.

δ)$\hat{P} = [0, 0]$, $\hat{Q} = [1, 0]$, $\hat{R} = [1, r_2]$, $\hat{S} = [1, s_2]$, tj. $\hat{Q}$, $\hat{R}$, $\hat{S}$ leží na přímce $x = 1$.

Obr 3.3 3 body na přímce



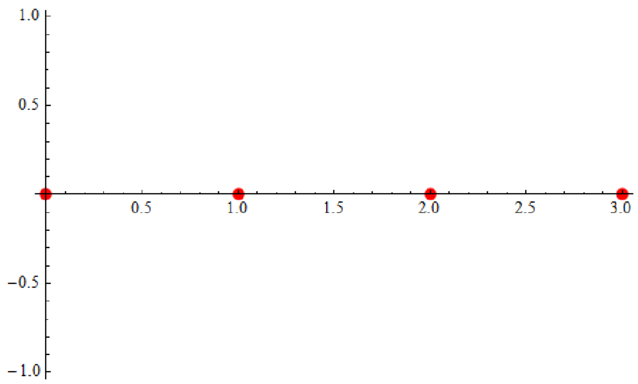
$$M = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & r_2 & 1 & r_2 & r_2^2 \\ 1 & 1 & s_2 & 1 & s_2 & s_2^2 \end{pmatrix}$$

rank $M = 4$ (protože $r_2 \neq s_2$, $r_2 \neq 0$, $s_2 \neq 0$)

Věta: V případě δ existuje nekonečně mnoho řešení závislých na 2 libovolných parametrech.

ϵ)$\hat{P} = [0,0]$, $\hat{Q} = [1,0]$, $\hat{R} = [r_1, 0]$, $\hat{S} = [s_1, 0]$, tj. všechny 4 body leží na přímce $y = 0$.

Obr 3.4 4 body na přímce



$$M = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & r_1 & 0 & r_1^2 & 0 & 0 \\ 1 & s_1 & 0 & s_1^2 & 0 & 0 \end{pmatrix}$$

rank $M = 3$ (protože $r_1 \neq 1$, $s_1 \neq 1$)

$$\mathrm{rank}(M|\vec{v}) = \mathrm{rank} \left(\begin{array}{ccc|c} 1 & 0 & 0 & p_3 \\ 1 & 1 & 1 & q_3 \\ 1 & r_1 & r_1^2 & r_3 \\ 1 & s_1 & s_1^2 & s_3 \end{array}\right)$$

Tato hodnost může být jak 3 (nekonečně mnoho řešení závislých na 3 libovolných parametrech), tak 4 (řešení neexistuje).

Zbývá určit, kdy nastane která možnost (podmínky pro p_3, q_3, r_3, s_3). Hodnost rozšířené matice je 3 pro případy:

$p_3 = q_3 = r_3 = s_3 = a$

$p_3 = 0 \qquad q_3 = b \qquad r_3 = b \cdot r_1 \qquad s_3 = b \cdot s_1$

$p_3 = 0 \qquad q_3 = c \qquad r_3 = c \cdot r_1^2 \qquad s_3 = c \cdot s_1^2$

$a, b, c \in \mathbb{R}$

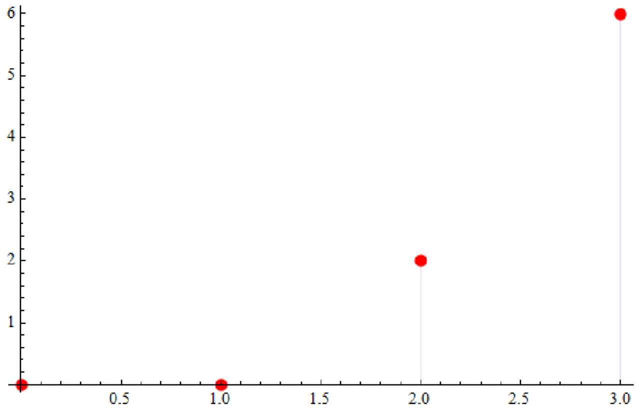
a jejich lineární kombinace. V ostatních případech kvadrika neexistuje. Na závěr můžeme vyslovit shrnutí:

Věta: Leží-li body $\hat{P}$, $\hat{Q}$, $\hat{R}$, $\hat{S}$ na přímce o rovnici $y = 0$ a souřadnice p_3, q_3, r_3, s_3 neleží na žádné křivce o rovnici $z = a \cdot x^2 + b \cdot x + c$, kde $(a, b, c) \in \mathbb{F}$, kde

$z \in \{p_3, q_3, r_3, s_3\}$**, $x \in \{p_1, q_1, r_1, s_1\}$, pak řešení neexistuje a pro případ $\hat{P}$, $\hat{Q}$, $\hat{R}$, $\hat{S}$ ležících na přímce o rovnici $y = 0$ a splňující rovnici $z = a \cdot x^2 + b \cdot x + c$, kde $(a, b, c) \in \mathbb{F}$, kde $z \in \{p_3, q_3, r_3, s_3\}$, $x \in \{p_1, q_1, r_1, s_1\}$ existuje nekonečně mnoho řešení závislých na 3 libovolných parametrech.**

$\varphi)\hat{P} = [0, 0]$, $\hat{Q} = [1, 0]$, $\hat{R} = [r_1, k \cdot (r_1^2 - r_1)]$, $\hat{S} = [s_1, k \cdot (s_1^2 - s_1)]$, tj. $\hat{P}$, $\hat{Q}$, $\hat{R}$, $\hat{S}$ leží na parabole o rovnici $y = k \cdot (x^2 - x)$.

Obr 3.5 4 body na parabole



$$M = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & r_1 & k \cdot (r_1^2 - r_1) & r_1^2 & r_1 \cdot k \cdot (r_1^2 - r_1) & k^2 \cdot (r_1^2 - r_1)^2 \\ 1 & s_1 & k \cdot (s_1^2 - s_1) & s_1^2 & s_1 \cdot k \cdot (s_1^2 - s_1) & k^2 \cdot (s_1^2 - s_1)^2 \end{pmatrix}$$

rank $M = 4$ (protože $r_2 \neq s_2$, $r_2 \neq 0$, $s_2 \neq 0$)

Věta: V případě φ existuje nekonečně mnoho řešení závislých na 2 libovolných parametrech.

Věta: V ostatních případech existuje nekonečně mnoho řešení závislých na 2 libovolných parametrech.

3.2. Pět bodů nad rovinou

Vezměme pět různých bodů $P = [p_1, p_2, p_3]$, $Q = [q_1, q_2, q_3]$, $R = [r_1, r_2, r_3]$, $S = [s_1, s_2, s_3]$, $T = [t_1, t_2, t_3]$.Označíme $\hat{P} = [p_1, p_2]$, $\hat{Q} = [q_1, q_2]$, $\hat{R} = [r_1, r_2]$, $\hat{S} = [s_1, s_2]$, $\hat{T} = [t_1, t_2]$. Lze předpokládat, že $\hat{P} = [0, 0]$, $\hat{Q} = [1, 0]$. Toto jsme již ukázali v kapitole o afinní transformaci.

Hledáme kvadriku

$$a + bx + cy + dx^2 + exy + fy^2 = z$$

Řešíme soustavu:

$$\begin{pmatrix} 1 & p_1 & p_2 & p_1^2 & p_1p_2 & p_2^2 \\ 1 & q_1 & q_2 & q_1^2 & q_1q_2 & q_2^2 \\ 1 & r_1 & r_2 & r_1^2 & r_1r_2 & r_2^2 \\ 1 & s_1 & s_2 & s_1^2 & s_1s_2 & s_2^2 \\ 1 & t_1 & t_2 & t_1^2 & t_1t_2 & t_2^2 \end{pmatrix} \cdot \begin{pmatrix} a \\ b \\ c \\ d \\ e \\ f \end{pmatrix} = \begin{pmatrix} p_3 \\ q_3 \\ r_3 \\ s_3 \\ t_3 \end{pmatrix}$$

Jde o soustavu lineárních rovnic, pro rozhodnutí o její řešitelnosti musíme zkoumat hodnost matice M (značíme rank M).

Vezměme naši volbu $\hat{P}$, $\hat{Q}$. Pak

$$M = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & r_1 & r_2 & r_1^2 & r_1r_2 & r_2^2 \\ 1 & s_1 & s_2 & s_1^2 & s_1s_2 & s_2^2 \\ 1 & t_1 & t_2 & t_1^2 & t_1t_2 & t_2^2 \end{pmatrix}$$

Dále vezměme podmatici N jako prvních 5 sloupců z matice M.
Platí: rank $N \leq$ rank $M \leq 5$.
Budeme nyní zkoumat hodnost N:

$$N = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 1 & r_1 & r_2 & r_1^2 & r_1r_2 \\ 1 & s_1 & s_2 & s_1^2 & s_1s_2 \\ 1 & t_1 & t_2 & t_1^2 & t_1t_2 \end{pmatrix}$$

je zřejmé, že $5 \geq$ rank $N \geq 3$ (případy $r_1 = r_2 = 0$, $s_1 = s_2 = 0$ a $t_1 = t_2 = 0$ nemohou nastat).

Vezměme další podmatici U (2.-5. řádek a 2.-5. sloupec):

$$U = \begin{pmatrix} 1 & 0 & 1 & 0 \\ r_1 & r_2 & r_1^2 & r_1r_2 \\ s_1 & s_2 & s_1^2 & s_1s_2 \\ t_1 & t_2 & t_1^2 & t_1t_2 \end{pmatrix}$$

Stačí vyšetřit rank U, protože rank $N = 1 +$ rank U.

Nejprve vyšetříme, kdy je 1. a 3. či 2. a 4. sloupec lineárně závislý. Vyjde nám 21 možností :

α) $r_1 = s_1 = t_1 = 0$
β) $r_1 = 0$ $s_1 = 0$ $t_1 = 1$
γ) $r_1 = 0$ $s_1 = 1$ $t_1 = 0$
δ) $r_1 = 1$ $s_1 = 0$ $t_1 = 0$
ϵ) $r_1 = 0$ $s_1 = 1$ $t_1 = 1$
ζ) $r_1 = 1$ $s_1 = 0$ $t_1 = 1$
η) $r_1 = 1$ $s_1 = 1$ $t_1 = 0$
ϑ) $r_1 = 1$ $s_1 = 1$ $t_1 = 1$
ι) $r_2 = 0$ $s_2 = 0$ $t_2 = 0$

κ) $r_2 = 0$ $s_2 = 0$ $t_2 = 1$
λ) $r_2 = 0$ $s_2 = 1$ $t_2 = 0$
μ) $r_2 = 1$ $s_2 = 0$ $t_2 = 0$
ν) $r_2 = 0$ $s_1 = k$ $t_2 = 0$
ξ) $r_1 = k$ $s_2 = 0$ $t_2 = 0$
o) $r_2 = 0$ $s_2 = 0$ $t_2 = k$
π) $r_1 = k$ $s_2 = 0$ $t_1 = k$
ρ) $r_2 = 0$ $s_1 = k$ $t_1 = k$
σ) $r_1 = k$ $s_1 = k$ $t_2 = 0$
τ) $r_1 = k$ $s_1 = k$ $t_1 = k$
υ) $r_2 = k \cdot (1 - r_1)$ $s_2 = k \cdot (1 - s_1)$ $t_2 = k \cdot (1 - t_1)$
φ) $r_2 = k \cdot (r_1 - r_1^2)$ $s_2 = k \cdot (s_1 - s_1^2)$ $t_2 = k \cdot (t_1 - t_1^2)$
Tyto možnosti dále analyzujme.
α)

$$U_\alpha = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & r_2 & 0 & 0 \\ 0 & s_2 & 0 & 0 \\ 0 & t_2 & 0 & 0 \end{pmatrix}$$

$$\text{rank } U_\alpha = 2$$

(nemůže nastat $r_2 = 0$ ani $s_2 = 0$ ani $t_2 = 0$)
β)

$$U_\beta = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & r_2 & 0 & 0 \\ 0 & s_2 & 0 & 0 \\ 1 & t_2 & 1 & t_2 \end{pmatrix}$$

$$\text{rank } U_\beta = 3$$

(nemůže nastat $r_2 = 0$ ani $s_2 = 0$ ani $t_2 = 0$).
Obdobně γ a δ
ϵ)

$$U_\epsilon = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & r_2 & 0 & 0 \\ 1 & s_2 & 1 & s_2 \\ 1 & t_2 & 1 & t_2 \end{pmatrix}$$

$$\text{rank } U_\epsilon = 3$$

(nemůže nastat $r_2 = 0$ ani $s_2 = 0$ ani $t_2 = 0$).
Obdobně ζ a η
ϑ)

$$U_\vartheta = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & r_2 & 1 & r_2 \\ 1 & s_2 & 1 & s_2 \\ 1 & t_2 & 1 & t_2 \end{pmatrix}$$

$$\text{rank } U_\vartheta = 2$$

(nemůže nastat $r_2 = 0$ ani $s_2 = 0$ ani $t_2 = 0$)

ι)

$$U_\iota = \begin{pmatrix} 1 & 0 & 1 & 0 \\ r_1 & 0 & r_1^2 & 0 \\ s_1 & 0 & s_1^2 & 0 \\ t_1 & 0 & t_1^2 & 0 \end{pmatrix}$$

$$\operatorname{rank} U_\iota = 2$$

(nemůže nastat $r_1 = 0$ ani $r_1 = 1$)

μ)

$$U_\mu = \begin{pmatrix} 1 & 0 & 1 & 0 \\ r_1 & 1 & r_1^2 & r_1 \\ s_1 & 0 & s_1^2 & 0 \\ t_1 & 0 & t_1^2 & 0 \end{pmatrix}$$

$$\operatorname{rank} U_\mu = 3$$

(nemůže nastat $s_1 = 1$ ani $s_1 = 0$ ani $t_1 = 1$ ani $t_1 = 0$).
Obdobně κ a λ

ν)

$$U_\nu = \begin{pmatrix} 1 & 0 & 1 & 0 \\ r_1 & 0 & r_1^2 & 0 \\ s_1 & 0 & s_1^2 & 0 \\ k & t_2 & k^2 & k \cdot t_2 \end{pmatrix}$$

$$\operatorname{rank} U_\nu = 3$$

(nemůže nastat $r_1 = 0$ ani $r_1 = 1$ ani $s_1 = 0$ ani $s_1 = 1$).
Obdobně ξ a o

ρ)

$$U_\rho = \begin{pmatrix} 1 & 0 & 1 & 0 \\ r_1 & 0 & r_1^2 & 0 \\ k & s_2 & k^2 & k \cdot s_2 \\ k & t_2 & k^2 & k \cdot t_2 \end{pmatrix}$$

$$\operatorname{rank} U_\rho = 3$$

(nemůže nastat $r_1 = 0$ ani $r_1 = 1$).
Obdobně π a σ

τ)

$$U_\tau = \begin{pmatrix} 1 & 0 & 1 & 0 \\ k & r_2 & k^2 & k \cdot r_2 \\ k & s_2 & k^2 & k \cdot s_2 \\ k & t_2 & k^2 & k \cdot t_2 \end{pmatrix}$$

$$\operatorname{rank} U_\tau = 3$$

(případy $k = 0$ ani $k = 1$ jsme již zkoumali).

υ)

$$U_\upsilon = \begin{pmatrix} 1 & 0 & 1 & 0 \\ r_1 & k\cdot(1-r_1) & r_1^2 & k\cdot r_1\cdot(1-r_1) \\ s_1 & k\cdot(1-s_1) & s_1^2 & k\cdot s_1\cdot(1-s_1) \\ t_1 & k\cdot(1-t_1) & t_1^2 & k\cdot t_1\cdot(1-t_1) \end{pmatrix}$$

$$\text{rank } U_\upsilon = 3$$

(nemůže nastat $r_1 = 1$)

φ)

$$U_\varphi = \begin{pmatrix} 1 & 0 & 1 & 0 \\ r_1 & k\cdot(r_1-r_1^2) & r_1^2 & k\cdot r_1\cdot(r_1-r_1^2) \\ s_1 & k\cdot(s_1-s_1^2) & s_1^2 & k\cdot s_1\cdot(s_1-s_1^2) \\ t_1 & k\cdot(t_1-t_1^2) & t_1^2 & k\cdot t_1\cdot(t_1-t_1^2) \end{pmatrix}$$

$$\text{rank } U_\varphi = 3$$

(nemůže nastat $r_1 = 1$ ani $r_1 = 0$)

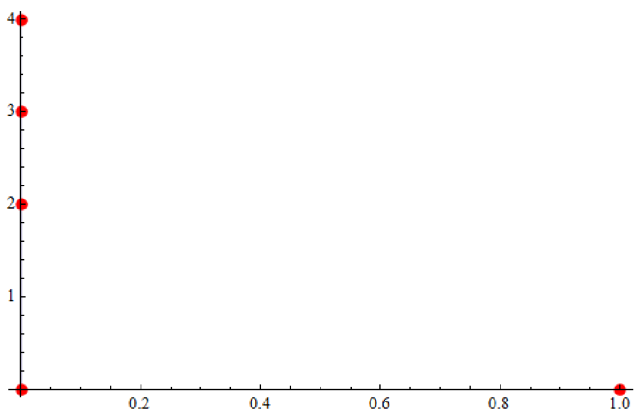
Shrnutí: V ostatních případech, je-li jeden sloupec lineární kombinací zbývajících 3, pak je $rank\ U = 3$.

Jinak je rank $U = 4$, tzn. rank $N = 5 \Rightarrow$ rank $M = 5$, tedy nastává nekonečně mnoho řešení závislých na 1 libovolném parametru.

Rozeberme nyní znovu případy α) až τ).

α)$\hat{P} = [0,0]$, $\hat{Q} = [1,0]$, $\hat{R} = [0,r_2]$, $\hat{S} = [0,s_2]$, $\hat{T} = [0,t_2]$, tj. $\hat{P}$, $\hat{R}$, $\hat{S}$, $\hat{T}$ leží na přímce o rovnici $x = 0$.

Obr 3.6 4 body na přímce



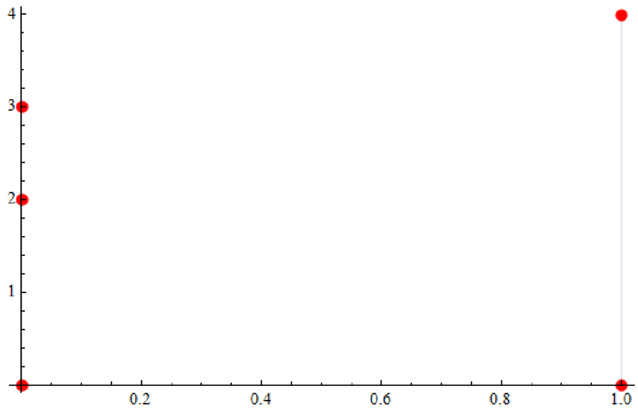
$$M = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & r_2 & 0 & 0 & r_2^2 \\ 1 & 0 & s_2 & 0 & 0 & s_2^2 \\ 1 & 0 & t_2 & 0 & 0 & t_2^2 \end{pmatrix}$$

$$\text{rank } M = 4$$

Splňují-li body P, Q, R, S, T rovnici $z = a \cdot y^2 + b \cdot y + c$, kde $(a, b, c) \in \mathbb{F}$, kde $z \in \{p_3, q_3, r_3, s_3, t_3\}$, $y \in \{p_2, q_2, r_2, s_2, t_2\}$, pak je hodnost rozšířené matice rovna 4 a existuje nekonečně mnoho řešení závislých na 2 libovolných parametrech. Pokud body P, Q, R, S, T tuto rovnici nesplňují, je hodnost rozšířené matice rovna 5 a řešení neexistuje.

$\beta)\hat{P} = [0, 0]$, $\hat{Q} = [1, 0]$, $\hat{R} = [0, r_2]$, $\hat{S} = [0, s_2]$, $\hat{T} = [1, t_2]$,tj. 3 body leží na přímce o rovnici $x = 0$ a 2 body leží na přímce o rovnici $x = 1$.

Obr 3.7 body na dvou rovnoběžkách



$$M = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & r_2 & 0 & 0 & r_2^2 \\ 1 & 0 & s_2 & 0 & 0 & s_2^2 \\ 1 & 1 & t_2 & 1 & t_2 & t_2^2 \end{pmatrix}$$

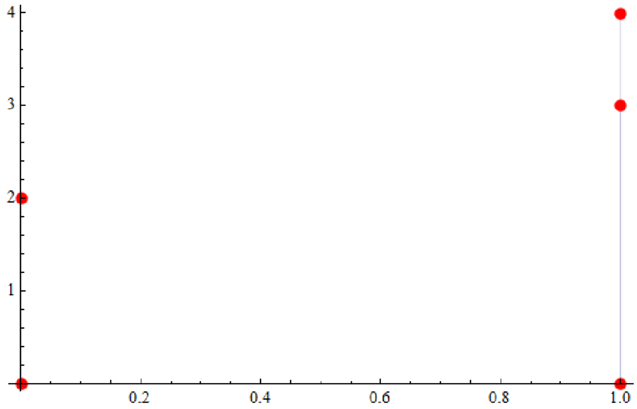
$$\text{rank } M = 5$$

Obdobně γ, δ.

V případech β, γ, δ existuje nekonečně mnoho řešení závislých na 1 libovolném parametru.

$\epsilon)\hat{P} = [0, 0]$, $\hat{Q} = [1, 0]$, $\hat{R} = [0, r_2]$, $\hat{S} = [1, s_2]$, $\hat{T} = [1, t_2]$, tj. 3 body leží na přímce o rovnici $x = 1$ a 2 body leží na přímce o rovnici $x = 0$.

Obr 3.8 body na dvou rovnoběžkách



$$M = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & r_2 & 0 & 0 & r_2^2 \\ 1 & 1 & s_2 & 1 & s_2 & s_2^2 \\ 1 & 1 & t_2 & 1 & t_2 & t_2^2 \end{pmatrix}$$

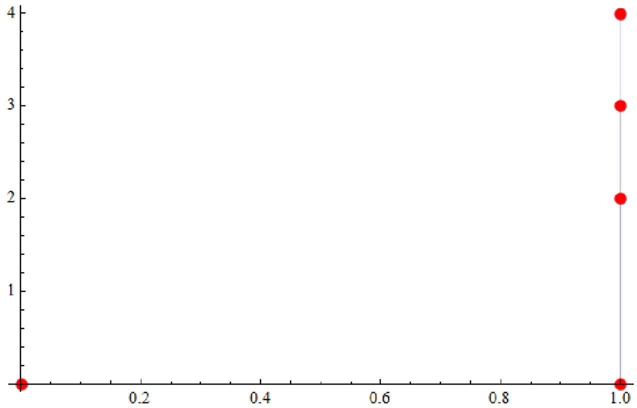
$$\operatorname{rank} M = 5$$

Obdobně ζ, η.

V případech ϵ, ζ, η existuje nekonečně mnoho řešení závislých na 1 libovolném parametru.

$\vartheta)\hat{P} = [0,0]$, $\hat{Q} = [1,0]$, $\hat{R} = [1,r_2]$, $\hat{S} = [1,s_2]$, $\hat{T} = [1,t_2]$, tj. 4 body na přímce o rovnici $x = 1$.

Obr 3.9 4 body na přímce



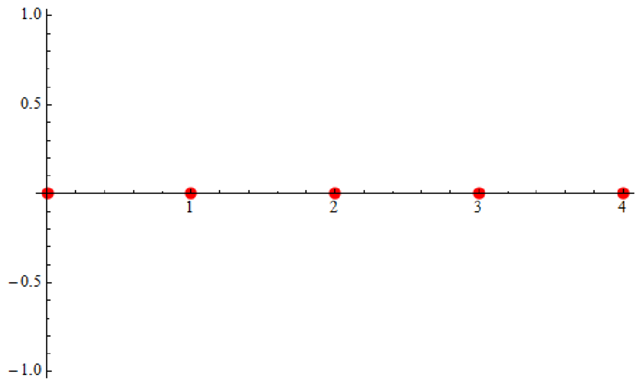
$$M = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & r_2 & 1 & r_2 & r_2^2 \\ 1 & 1 & s_2 & 1 & s_2 & s_2^2 \\ 1 & 1 & t_2 & 1 & t_2 & t_2^2 \end{pmatrix}$$

$$\text{rank } M = 4$$

Splňují-li body P, Q, R, S, T rovnici $z = a \cdot y^2 + b \cdot y + c$, kde $(a, b, c) \in \mathbb{F}$, kde $z \in \{p_3, q_3, r_3, s_3, t_3\}$, $y \in \{p_2, q_2, r_2, s_2, t_2\}$, pak je hodnost rozšířené matice rovna 4 a existuje nekonečně mnoho řešení závislých na 2 libovolných parametrech. Pokud body P, Q, R, S, T tuto rovnici nesplňují, je hodnost rozšířené matice rovna 5 a řešení neexistuje.

$\iota)\hat{P} = [0, 0]$, $\hat{Q} = [1, 0]$, $\hat{R} = [r_1, 0]$, $\hat{S} = [s_1, 0]$, $\hat{T} = [t_1, 0]$, tj. 5 bodů na přímce o rovnici $y = 0$.

Obr 3.10 5 bodů na přímce



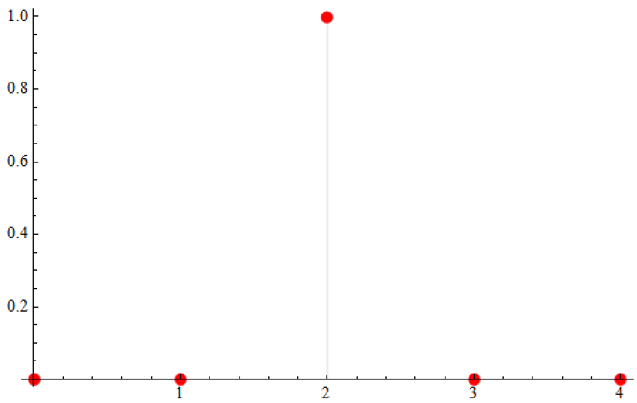
$$M = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & r_1 & 0 & r_1^2 & 0 & 0 \\ 1 & s_1 & 0 & s_1^2 & 0 & 0 \\ 1 & t_1 & 0 & t_1^2 & 0 & 0 \end{pmatrix}$$

$$\text{rank } M = 3$$

Splňují-li body P, Q, R, S, T rovnici $z = a \cdot x^2 + b \cdot x + c$, kde $(a, b, c) \in \mathbb{F}$, kde $z \in \{p_3, q_3, r_3, s_3, t_3\}$, $x \in \{p_1, q_1, r_1, s_1, t_1\}$, pak je hodnost rozšířené matice rovna 3 a existuje nekonečně mnoho řešení závislých na 3 libovolných parametrech. Pokud body P, Q, R, S, T tuto rovnici nesplňují, je hodnost rozšířené matice rovna 4 a řešení neexistuje.

$\mu)\hat{P} = [0, 0]$, $\hat{Q} = [1, 0]$, $\hat{R} = [r_1, 1]$, $\hat{S} = [s_1, 0]$, $\hat{T} = [t_1, 0]$, tj. 4 body na přímce o rovnici $y = 0$.

Obr 3.11 4 body na přímce



$$M = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & r_1 & 1 & r_1^2 & r_1 & 1 \\ 1 & s_1 & 0 & s_1^2 & 0 & 0 \\ 1 & t_1 & 0 & t_1^2 & 0 & 0 \end{pmatrix}$$

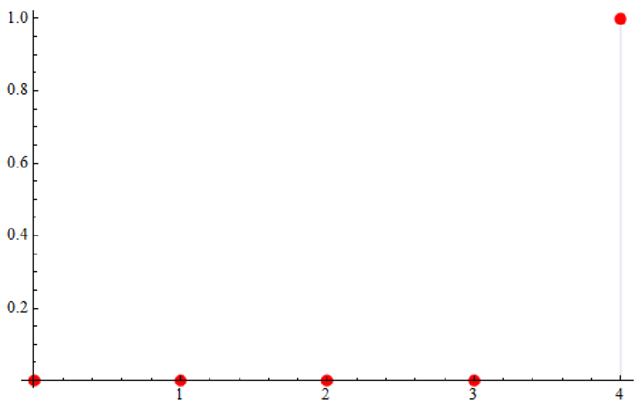
$$\text{rank } M = 4$$

Obdodně κ, λ.

Splňují-li body P, Q, R, S, T **rovnici** $z = a \cdot x^2 + b \cdot x + c$**, kde** $(a, b, c) \in \mathbb{F}$**, kde** $z \in \{p_3, q_3, r_3, s_3, t_3\}$**,** $x \in \{p_1, q_1, r_1, s_1, t_1\}$**, pak je hodnost rozšířené matice rovna 4 a existuje nekonečně mnoho řešení závislých na 2 libovolných parametrech. Pokud body** P, Q, R, S, T **tuto rovnici nesplňují, je hodnost rozšířené matice rovna 5 a řešení neexistuje.**

$\nu)\hat{P} = [0, 0]$, $\hat{Q} = [1, 0]$, $\hat{R} = [r_1, 0]$, $\hat{S} = [s_1, 0]$, $\hat{T} = [k, t_2]$, tj. 4 body na přímce o rovnici $y = 0$.

Obr 3.12 4 body na přímce



$$M = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & r_1 & 0 & r_1^2 & 0 & 0 \\ 1 & s_1 & 0 & s_1^2 & 0 & 0 \\ 1 & k & t_2 & k^2 & k \cdot t_2 & t_2^2 \end{pmatrix}$$

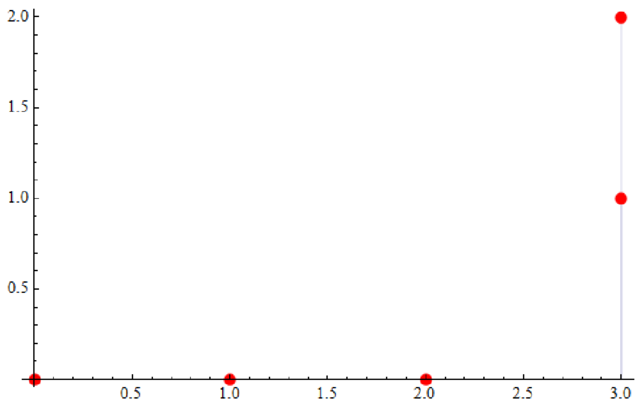
$$\text{rank } M = 4$$

Pozn.($t_2 = 1, t_2 = 0$ jsme zkoumali již dříve)

V případě ν existuje nekonečně mnoho řešení závislých na 1 libovolném parametru.

$\rho)\hat{P} = [0,0]$, $\hat{Q} = [1,0]$, $\hat{R} = [r_1, 0]$, $\hat{S} = [k, s_2]$, $\hat{T} = [k, t_2]$, tj. 3 body leží na přímce o rovnici $y = 0$ a 2 body leží na přímce o rovnici $x = k$.

Obr 3.13 body na kolmicích



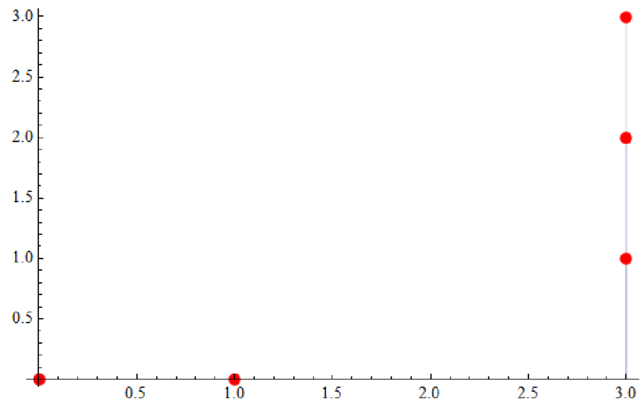
$$M = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & r_1 & 0 & r_1^2 & 0 & 0 \\ 1 & k & s_2 & k^2 & k \cdot s_2 & s_2^2 \\ 1 & k & t_2 & k^2 & k \cdot t_2 & t_2^2 \end{pmatrix}$$

$$\text{rank } M = 5$$

V případě ρ existuje nekonečně mnoho řešení závislých na 1 libovolném parametru.

$\tau)\hat{P} = [0,0]$, $\hat{Q} = [1,0]$, $\hat{R} = [k, r_2]$, $\hat{S} = [k, s_2]$, $\hat{T} = [k, t_2]$, tj. 2 body leží na přímce o rovnici $y = 0$ a 3 body leží na přímce o rovnici $x = k$.

Obr 3.14 body na kolmicích



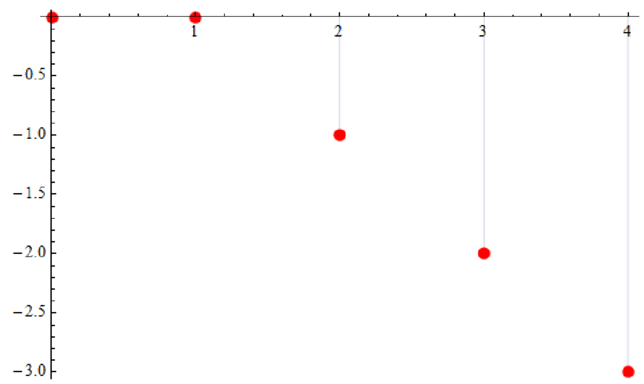
$$M = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & k & r_2 & k^2 & k \cdot r_2 & r_2^2 \\ 1 & k & s_2 & k^2 & k \cdot s_2 & s_2^2 \\ 1 & k & t_2 & k^2 & k \cdot t_2 & t_2^2 \end{pmatrix}$$

$$\text{rank } M = 5$$

V případě τ existuje nekonečně mnoho řešení závislých na 1 libovolném parametru.

$\upsilon)\hat{P} = [0,0]$, $\hat{Q} = [1,0]$, $\hat{R} = [r_1, k \cdot (1 - r_1)]$, $\hat{S} = [s_1, k \cdot (1 - s_1)]$, $\hat{T} = [t_1, k \cdot (1 - t_1)]$, tj. 4 body leží na přímce o rovnici $y = k \cdot (1 - x)$.

Obr 3.15 4 body na přímce



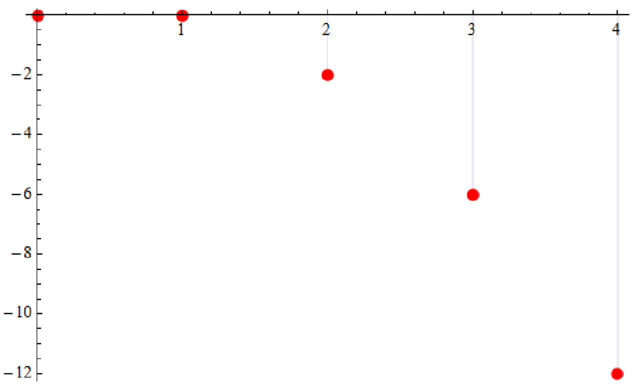
$$M = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & r_1 & k \cdot (1 - r_1) & r_1^2 & k \cdot r_1 \cdot (1 - r_1) & k^2 \cdot (1 - r_1)^2 \\ 1 & s_1 & k \cdot (1 - s_1) & s_1^2 & k \cdot s_1 \cdot (1 - s_1) & k^2 \cdot (1 - s_1)^2 \\ 1 & t_1 & k \cdot (1 - t_1) & t_1^2 & k \cdot t_1 \cdot (1 - t_1) & k^2 \cdot (1 - t_1)^2 \end{pmatrix}$$

$$\text{rank } M = 4$$

Splňují-li body P, Q, R, S, T rovnici $z = a \cdot x^2 + b \cdot x + c$, kde $(a, b, c) \in \mathbb{F}$, kde $z \in \{p_3, q_3, r_3, s_3, t_3\}$, $x \in \{p_1, q_1, r_1, s_1, t_1\}$, pak je hodnost rozšířené matice rovna 4 a existuje nekonečně mnoho řešení závislých na 2 libovolných parametrech. Pokud body P, Q, R, S, T tuto rovnici nesplňují, je hodnost rozšířené matice rovna 5 a řešení neexistuje.

$\varphi)\hat{P} = [0, 0]$, $\hat{Q} = [1, 0]$, $\hat{R} = [r_1, k \cdot (r_1 - r_1^2)]$, $\hat{S} = [s_1, k \cdot (s_1 - s_1^2)]$, $\hat{T} = [t_1, k \cdot (t_1 - t_1^2)]$, tj. 5 bodů leží na parabole o rovnici $y = k \cdot (x - x^2)$.

Obr 3.16 5 bodů na parabole



$$M = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & r_1 & k \cdot (r_1 - r_1^2) & r_1^2 & k \cdot r_1 \cdot (r_1 - r_1^2) & k^2 \cdot (r_1 - r_1^2)^2 \\ 1 & s_1 & k \cdot (s_1 - s_1^2) & s_1^2 & k \cdot s_1 \cdot (s_1 - s_1^2) & k^2 \cdot (s_1 - s_1^2)^2 \\ 1 & t_1 & k \cdot (t_1 - t_1^2) & t_1^2 & k \cdot t_1 \cdot (t_1 - t_1^2) & k^2 \cdot (t_1 - t_1^2)^2 \end{pmatrix}$$

$$\text{rank } M = 5$$

V případě φ existuje nekonečně mnoho řešení závislých na 1 libovolném parametru.

V ostatních případech existuje nekonečně mnoho řešení závislých na 1 libovolném parametru.

3.3. Šest bodů nad rovinou

Vezměme 6 různých bodů $P = [p_1, p_2, p_3]$, $Q = [q_1, q_2, q_3]$, $R = [r_1, r_2, r_3]$, $S = [s_1, s_2, s_3]$, $T = [t_1, t_2, t_3]$, $U = [u_1, u_2, u_3]$. Označíme $\hat{P} = [p_1, p_2]$, $\hat{Q} = [q_1, q_2]$, $\hat{R} = [r_1, r_2]$, $\hat{S} = [s_1, s_2]$, $\hat{T} = [t_1, t_2]$, $\hat{U} = [u_1, u_2]$. Lze předpokládat, že $\hat{P} = [0, 0]$, $\hat{Q} = [1, 0]$. Toto jsme již ukázali v kapitole o afinní transformaci.

Hledáme kvadriku

$$a + bx + cy + dx^2 + exy + fy^2 = z$$

Řešíme soustavu:

$$\begin{pmatrix} 1 & p_1 & p_2 & p_1^2 & p_1p_2 & p_2^2 \\ 1 & q_1 & q_2 & q_1^2 & q_1q_2 & q_2^2 \\ 1 & r_1 & r_2 & r_1^2 & r_1r_2 & r_2^2 \\ 1 & s_1 & s_2 & s_1^2 & s_1s_2 & s_2^2 \\ 1 & t_1 & t_2 & t_1^2 & t_1t_2 & t_2^2 \\ 1 & u_1 & u_2 & u_1^2 & u_1u_2 & u_2^2 \end{pmatrix} \cdot \begin{pmatrix} a \\ b \\ c \\ d \\ e \\ f \end{pmatrix} = \begin{pmatrix} p_3 \\ q_3 \\ r_3 \\ s_3 \\ t_3 \\ u_3 \end{pmatrix}$$

Jde o soustavu lineárních rovnic, musíme zkoumat hodnost matice M (značíme rank M). Vezměme naši volbu $\hat{P}$, $\hat{Q}$. Pak

$$M = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & r_1 & r_2 & r_1^2 & r_1r_2 & r_2^2 \\ 1 & s_1 & s_2 & s_1^2 & s_1s_2 & s_2^2 \\ 1 & t_1 & t_2 & t_1^2 & t_1t_2 & t_2^2 \\ 1 & u_1 & u_2 & u_1^2 & u_1u_2 & u_2^2 \end{pmatrix}$$

Vezměme podmatici U (2.-6. řádek a 2.-6. sloupec):

$$U = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ r_1 & r_2 & r_1^2 & r_1r_2 & r_2^2 \\ s_1 & s_2 & s_1^2 & s_1s_2 & s_2^2 \\ t_1 & t_2 & t_1^2 & t_1t_2 & t_2^2 \\ u_1 & u_2 & u_1^2 & u_1u_2 & u_2^2 \end{pmatrix}$$

Stačí vyšetřit rank U, protože rank $M = 1 + \operatorname{rank} U$. Pro lepší názornost budeme zkoumat zvlášť matici V, která vznikne z 2.,4. a 5. sloupce matice U. Je zřejmé, že rank $U = \operatorname{rank} V + 2$.

Nejprve vyšetříme, kdy je 1. a 3. či 2.,4. a 5. sloupec lineárně závislý. Vyjde nám 26 možností :

α) $r_1 = s_1 = t_1 = u_1 = 0$
β) $r_1 = 0$ $s_1 = 0$ $t_1 = 0$ $u_1 = 1$
γ) $r_1 = 0$ $s_1 = 0$ $t_1 = 1$ $u_1 = 0$
δ) $r_1 = 0$ $s_1 = 1$ $t_1 = 0$ $u_1 = 0$
ϵ) $r_1 = 1$ $s_1 = 0$ $t_1 = 0$ $u_1 = 0$
ζ) $r_1 = 0$ $s_1 = 0$ $t_1 = 1$ $u_1 = 1$
η) $r_1 = 0$ $s_1 = 1$ $t_1 = 1$ $u_1 = 0$
ϑ) $r_1 = 1$ $s_1 = 1$ $t_1 = 0$ $u_1 = 0$
ι) $r_1 = 1$ $s_1 = 0$ $t_1 = 1$ $u_1 = 0$
κ) $r_1 = 1$ $s_1 = 0$ $t_1 = 0$ $u_1 = 1$
λ) $r_1 = 0$ $s_1 = 1$ $t_1 = 0$ $u_1 = 1$
μ) $r_1 = 1$ $s_1 = 1$ $t_1 = 1$ $u_1 = 0$
ν) $r_1 = 1$ $s_1 = 1$ $t_1 = 0$ $u_1 = 1$
ξ) $r_1 = 1$ $s_1 = 0$ $t_1 = 1$ $u_1 = 1$
o) $r_1 = 0$ $s_1 = 1$ $t_1 = 1$ $u_1 = 1$
π) $r_1 = 1$ $s_1 = 1$ $t_1 = 1$ $u_1 = 1$
ρ) $r_2 = 0$ $s_2 = 0$ $t_2 = 0$ $u_2 = 0$

$\sigma)$ $r_1 = k \cdot (1 + r_2)$, $s_1 = k \cdot (1 + s_2)$, $t_1 = k \cdot (1 + t_2)$, $u_1 = k \cdot (1 + u_2)$
$\tau)$ $r_2 = 1$ $s_2 = 1$ $t_2 = 1$ $u_2 = 1$
$\upsilon)$ $r_2 = r_1$ $s_2 = s_1$ $t_2 = t_1$ $u_2 = u_1$
$\varphi)$ $r_2 = 0$ $s_2 = 0$ $t_2 = 0$ $u_2 lib.$
$\chi)$ $r_1 = l$ $s_1 = l$ $t_1 = l$ $u_1 = l$
$\psi)$ $r_1 = k \cdot r_2$ $s_1 = k \cdot s_2$ $t_1 = k \cdot t_2$ $u_1 = k \cdot u_2$
$\omega)$ $r_2 = l$ $s_2 = l$ $t_2 = l$ $u_2 = l$
$\alpha\alpha)$ $r_2 = k \cdot (r_1^2 - r_1)$ $s_2 = k \cdot (s_1^2 - s_1)$ $t_2 = k \cdot (t_1^2 - t_1)$ $u_2 = k \cdot (u_1^2 - u_1)$
$\alpha\beta)$ $r_2^2 = k \cdot (r_1^2 - r_1)$ $s_2^2 = k \cdot (s_1^2 - s_1)$ $t_2^2 = k \cdot (t_1^2 - t_1)$ $u_2^2 = k \cdot (u_1^2 - u_1)$
Tyto možnosti dále analyzujme.
$\alpha)$

$$U_\alpha = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & r_2 & 0 & 0 & r_2^2 \\ 0 & s_2 & 0 & 0 & s_2^2 \\ 0 & t_2 & 0 & 0 & t_2^2 \\ 0 & u_2 & 0 & 0 & u_2^2 \end{pmatrix}$$

$$\text{rank } U_\alpha = 3$$

(nemůže nastat $r_2 = 0$ ani $s_2 = 0$ ani $t_2 = 0$ ani $s_2 = 0$)
$\beta)$

$$U_\beta = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & r_2 & 0 & 0 & r_2^2 \\ 0 & s_2 & 0 & 0 & s_2^2 \\ 0 & t_2 & 0 & 0 & t_2^2 \\ 1 & u_2 & 1 & u_2 & u_2^2 \end{pmatrix}$$

$$\text{rank } U_\beta = 4$$

(nemůže nastat $r_2 = 0$ ani $s_2 = 0$ ani $t_2 = 0$ ani $u_2 = 0$)
Obdobně γ a δ a ϵ
$\zeta)$

$$U_\zeta = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & r_2 & 0 & 0 & r_2^2 \\ 0 & s_2 & 0 & 0 & s_2^2 \\ 1 & t_2 & 1 & t_2 & t_2^2 \\ 1 & u_2 & 1 & u_2 & u_2^2 \end{pmatrix}$$

$$\text{rank } U_\zeta = 4$$

(nemůže nastat $r_2 = 0$ ani $s_2 = 0$ ani $t_2 = 0$ ani $u_2 = 0$)
Obdobně η a ϑ a ι a κ a λ
$\mu)$

$$U_\mu = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & r_2 & 1 & r_2 & r_2^2 \\ 1 & s_2 & 1 & s_2 & s_2^2 \\ 1 & t_2 & 1 & t_2 & t_2^2 \\ 0 & u_2 & 0 & 0 & u_2^2 \end{pmatrix}$$

$$\text{rank } U_\mu = 4$$

(nemůže nastat $r_2 = 0$ ani $r_2 = 1$) Obdobně ν a ξ a o

π)

$$U_\pi = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & r_2 & 1 & r_2 & r_2^2 \\ 1 & s_2 & 1 & s_2 & s_2^2 \\ 1 & t_2 & 1 & t_2 & t_2^2 \\ 1 & u_2 & 1 & u_2 & u_2^2 \end{pmatrix}$$

$$\text{rank } U_\pi = 3$$

(nemůže nastat $r_2 = 0$ ani $r_2 = 1$)

ρ)

$$U_\rho = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ r_1 & 0 & r_1^2 & 0 & 0 \\ s_1 & 0 & s_1^2 & 0 & 0 \\ t_1 & 0 & t_1^2 & 0 & 0 \\ u_1 & 0 & u_1^2 & 0 & 0 \end{pmatrix}$$

$$\text{rank } U_\rho = 2$$

(nemůže nastat $r_1 = 0$ ani $r_1 = 1$)

σ)

$$U_\sigma = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ k\cdot(1+r_2) & r_2 & (k\cdot(1+r_2))^2 & r_2\cdot(k\cdot(1+r_2)) & r_2^2 \\ k\cdot(1+s_2) & s_2 & (k\cdot(1+s_2))^2 & s_2\cdot(k\cdot(1+s_2)) & s_2^2 \\ k\cdot(1+t_2) & r_2 & (k\cdot(1+t_2))^2 & t_2\cdot(k\cdot(1+t_2)) & t_2^2 \\ k\cdot(1+u_2) & u_2 & (k\cdot(1+u_2))^2 & u_2\cdot(k\cdot(1+u_2)) & u_2^2 \end{pmatrix}$$

$$\text{rank } U_\sigma = 4$$

(nemůže nastat $r_2 = 0$ ani $r_2 = 1$)

τ)

$$U_\tau = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ r_1 & 1 & r_1^2 & r_1 & 1 \\ s_1 & 1 & s_1^2 & s_1 & 1 \\ t_1 & 1 & t_1^2 & t_1 & 1 \\ u_1 & 1 & u_1^2 & u_1 & 1 \end{pmatrix}$$

$$\text{rank } U_\tau = 4$$

(nemůže nastat $r_1 = 0$ ani $r_1 = 1$)

υ)

$$U_\upsilon = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ r_1 & r_1 & r_1^2 & r_1^2 & r_1^2 \\ s_1 & s_1 & s_1^2 & s_1^2 & s_1^2 \\ t_1 & t_1 & t_1^2 & t_1^2 & t_1^2 \\ u_1 & u_1 & u_1^2 & u_1^2 & u_1^2 \end{pmatrix}$$

$$\text{rank } U_\upsilon = 4$$

(nemůže nastat $r_1 = 0$ ani $r_1 = 1$)

φ)

$$V_\varphi = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ u_2 & u_2 \cdot u_1 & u_2^2 \end{pmatrix}$$

$$\text{rank } V_\varphi = 1 \Rightarrow \text{rank } U_\varphi = 3$$

(nemůže nastat $u_2 = 0$)

χ)

$$V_\chi = \begin{pmatrix} 0 & 0 & 0 \\ r_2 & l \cdot r_2 & r_2^2 \\ s_2 & l \cdot s_2 & s_2^2 \\ t_2 & l \cdot t_2 & t_2^2 \\ u_2 & l \cdot u_2 & u_2^2 \end{pmatrix}$$

$$\text{rank } V_\chi = 2 \Rightarrow \text{rank } U_\chi = 4$$

(nemůže nastat $r_2 = 0$ ani $r_2 = 1$)

ψ)

$$V_\psi = \begin{pmatrix} 0 & 0 & 0 \\ r_2 & k \cdot r_2^2 & r_2^2 \\ s_2 & k \cdot s_2^2 & s_2^2 \\ t_2 & k \cdot t_2^2 & t_2^2 \\ u_2 & k \cdot u_2^2 & u_2^2 \end{pmatrix}$$

$$\text{rank } V_\psi = 2 \Rightarrow \text{rank } U_\psi = 4$$

(nemůže nastat $r_2 = 0$ ani $r_2 = 1$)

ω)

$$V_\omega = \begin{pmatrix} 0 & 0 & 0 \\ l & l \cdot r_1 & l^2 \\ l & l \cdot s_1 & l^2 \\ l & l \cdot t_1 & l^2 \\ l & l \cdot u_1 & l^2 \end{pmatrix}$$

$$\text{rank } V_\omega = 2 \Rightarrow \text{rank } U_\omega = 4$$

(nemůže nastat $r_1 = 0$ ani $r_1 = 1$)

$\alpha\alpha$)

$$U_{\alpha\alpha} = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ r_1 & k \cdot (r_1^2 - r_1) & r_1^2 & k \cdot r_1 \cdot (r_1^2 - r_1) & k^2 \cdot (r_1^2 - r_1)^2 \\ s_1 & k \cdot (s_1^2 - s_1) & s_1^2 & k \cdot s_1 \cdot (s_1^2 - s_1) & k^2 \cdot (s_1^2 - s_1)^2 \\ t_1 & k \cdot (t_1^2 - t_1) & t_1^2 & k \cdot t_1 \cdot (t_1^2 - t_1) & k^2 \cdot (t_1^2 - t_1)^2 \\ u_1 & k \cdot (u_1^2 - u_1) & u_1^2 & k \cdot u_1 \cdot (u_1^2 - u_1) & k^2 \cdot (u_1^2 - u_1)^2 \end{pmatrix}$$

$$\text{rank } U_{\alpha\alpha} = 4$$

(nemůže nastat $r_1 = 0$ ani $r_1 = 1$)

$\alpha\beta$)

$$U_{\alpha\beta} = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ r_1 & \sqrt{k\cdot(r_1^2-r_1)} & r_1^2 & r_1\cdot\sqrt{k\cdot r_1\cdot(r_1^2-r_1)} & k\cdot(r_1^2-r_1) \\ s_1 & \sqrt{k\cdot(s_1^2-s_1)} & s_1^2 & s_1\cdot\sqrt{k\cdot s_1\cdot(s_1^2-s_1)} & k\cdot(s_1^2-s_1) \\ t_1 & \sqrt{k\cdot(t_1^2-t_1)} & t_1^2 & t_1\cdot\sqrt{k\cdot t_1\cdot(t_1^2-t_1)} & k\cdot(t_1^2-t_1) \\ u_1 & \sqrt{k\cdot(u_1^2-u_1)} & u_1^2 & u_1\cdot\sqrt{k\cdot u_1\cdot(u_1^2-u_1)} & k\cdot(u_1^2-u_1) \end{pmatrix}$$

$$\text{rank } U_{\alpha\beta} = 4$$

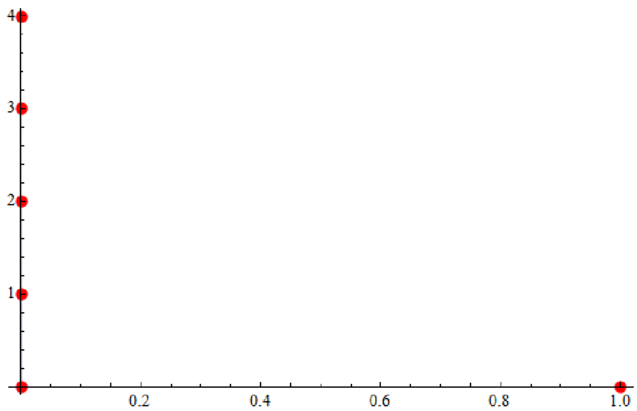
(Pro názornost bereme pouze kladnou odmocninu). (nemůže nastat $r_1 = 0$ ani $r_1 = 1$)

Jindy je rank $U = 5$, tzn. rank $M = 6$.

Rozeberme nyní znovu případy α) až υ).

$\alpha)\hat{P} = [0,0]$, $\hat{Q} = [1,0]$, $\hat{R} = [0,r_2]$, $\hat{S} = [0,s_2]$, $\hat{T} = [0,t_2]$,$\hat{U} = [0,u_2]$, tj. $\hat{P}$, $\hat{R}$, $\hat{S}$, $\hat{T}$ $\hat{U}$ leží na přímce o rovnici $x = 0$.

Obr 3.17 5 bodů na přímce



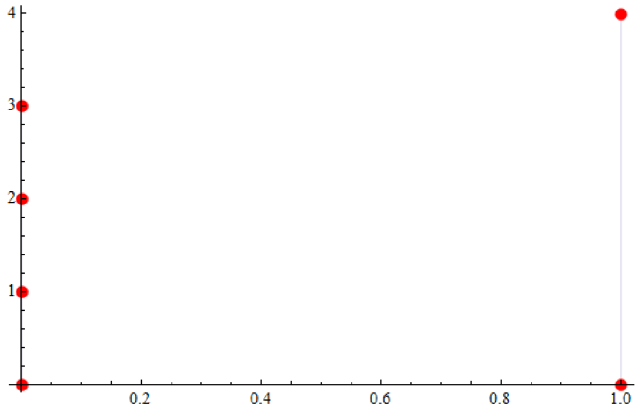
$$M = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & r_2 & 0 & 0 & r_2^2 \\ 1 & 0 & s_2 & 0 & 0 & s_2^2 \\ 1 & 0 & t_2 & 0 & 0 & t_2^2 \\ 1 & 0 & u_2 & 0 & 0 & u_2^2 \end{pmatrix}$$

$$\text{rank } M = 4$$

Splňují-li body P, Q, R, S, T, U rovnici $z = a\cdot y^2 + b\cdot y + c$, kde $(a,b,c) \in \mathbb{F}$, kde $z \in \{p_3, q_3, r_3, s_3, t_3, u_3\}$, $y \in \{p_2, q_2, r_2, s_2, t_2, u_2\}$, pak je hodnost rozšířené matice rovna 4 a existuje nekonečně mnoho řešení závislých na 2 libovolných parametrech. Pokud body P, Q, R, S, T, U tuto rovnici nesplňují, je hodnost rozšířené matice rovna 5 a řešení neexistuje.

$\beta)\hat{P} = [0,0]$, $\hat{Q} = [1,0]$, $\hat{R} = [0,r_2]$, $\hat{S} = [0,s_2]$, $\hat{T} = [0,t_2]$, $\hat{U} = [1,u_2]$, tj. 4 body na přímce o rovnici $x = 0$ a 2 body na přímce o rovnici $x = 1$.

Obr 3.18 body na dvou rovnoběžkách



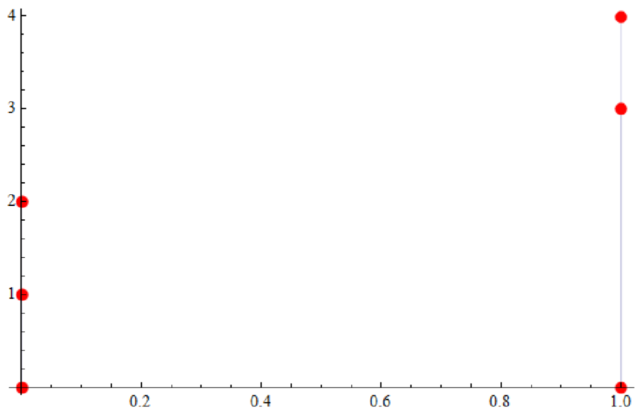
$$M = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & r_2 & 0 & 0 & r_2^2 \\ 1 & 0 & s_2 & 0 & 0 & s_2^2 \\ 1 & 0 & t_2 & 0 & 0 & t_2^2 \\ 1 & 1 & u_2 & 1 & u_2 & u_2^2 \end{pmatrix}$$

$$\text{rank } M = 5$$

Obdobně γ a δ a ϵ. **Splňují-li body P, Q, R, S, T, U rovnici $z = a \cdot y^2 + b \cdot y + c$, kde $(a, b, c) \in \mathbb{F}$, kde $z \in \{p_3, q_3, r_3, s_3, t_3, u_3\}$, $y \in \{p_2, q_2, r_2, s_2, t_2, u_2\}$, pak je hodnost rozšířené matice rovna 5 a existuje nekonečně mnoho řešení závislých na 1 libovolném parametru. Pokud body P, Q, R, S, T, U tuto rovnici nesplňují, je hodnost rozšířené matice rovna 6 a řešení neexistuje.**

$\zeta)\hat{P} = [0, 0]$, $\hat{Q} = [1, 0]$, $\hat{R} = [0, r_2]$, $\hat{S} = [0, s_2]$, $\hat{T} = [1, t_2]$, $\hat{U} = [1, u_2]$, tj. 3 body na přímce o rovnici $x = 0$ a 3 body na přímce o rovnici $x = 1$.

Obr 3.19 body na dvou rovnoběžkách



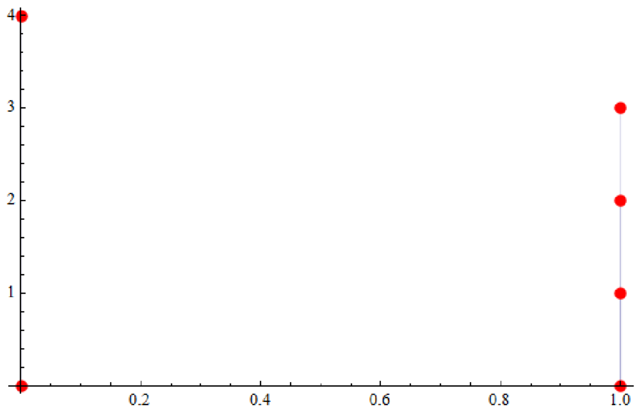
$$M = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & r_2 & 0 & 0 & r_2^2 \\ 1 & 0 & s_2 & 0 & 0 & s_2^2 \\ 1 & 1 & t_2 & 1 & t_2 & t_2^2 \\ 1 & 1 & u_2 & 1 & u_2 & u_2^2 \end{pmatrix}$$

$$\operatorname{rank} M = 5$$

Obdobně η, ϑ, ι, κ, λ. **Splňují-li body** P, Q, R, S, T, U **rovnici** $z = a \cdot y^2 + b \cdot y + c$**, kde** $(a, b, c) \in \mathbb{F}$**, kde** $z \in \{p_3, q_3, r_3, s_3, t_3, u_3\}$, $y \in \{p_2, q_2, r_2, s_2, t_2, u_2\}$**, pak je hodnost rozšířené matice rovna 5 a existuje nekonečně mnoho řešení závislých na 1 libovolném parametru. Pokud body** P, Q, R, S, T, U **tuto rovnici nesplňují, je hodnost rozšířené matice rovna 6 a řešení neexistuje.**

$\mu)\hat{P} = [0, 0]$, $\hat{Q} = [1, 0]$, $\hat{R} = [1, r_2]$, $\hat{S} = [1, s_2]$, $\hat{T} = [1, t_2]$, $\hat{U} = [0, u_2]$, tj. 4 body na přímce o rovnici $x = 1$ a 2 body na přímce o rovnici $x = 0$.

Obr 3.20 body na dvou rovnoběžkách



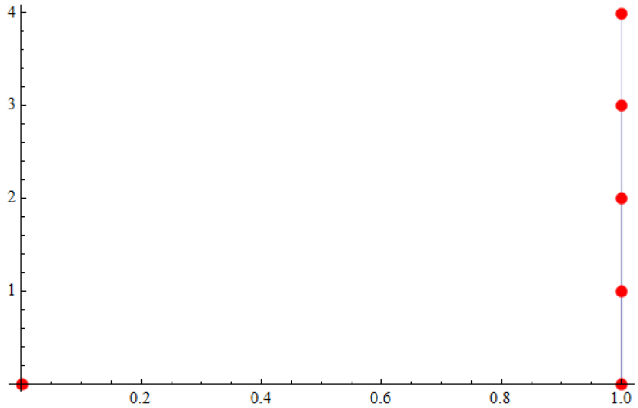
$$M = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & r_2 & 1 & r_2 & r_2^2 \\ 1 & 1 & s_2 & 1 & s_2 & s_2^2 \\ 1 & 1 & t_2 & 1 & t_2 & t_2^2 \\ 1 & 0 & u_2 & 0 & 0 & u_2^2 \end{pmatrix}$$

$$\operatorname{rank} M = 5$$

Obdobně ν, ξ, o. **Splňují-li body** P, Q, R, S, T, U **rovnici** $z = a \cdot y^2 + b \cdot y + c$**, kde** $(a, b, c) \in \mathbb{F}$**, kde** $z \in \{p_3, q_3, r_3, s_3, t_3, u_3\}$, $y \in \{p_2, q_2, r_2, s_2, t_2, u_2\}$**, pak je hodnost rozšířené matice rovna 5 a existuje nekonečně mnoho řešení závislých na 1 libovolném parametru. Pokud body** P, Q, R, S, T, U **tuto rovnici nesplňují, je hodnost rozšířené matice rovna 6 a řešení neexistuje.**

$\pi)\hat{P} = [0,0]$, $\hat{Q} = [1,0]$, $\hat{R} = [1, r_2]$, $\hat{S} = [1, s_2]$, $\hat{T} = [1, t_2]$, $\hat{U} = [1, u_2]$, tj. 5 bodů na přímce o rovnici $x = 1$.

Obr 3.21 5 bodů na přímce



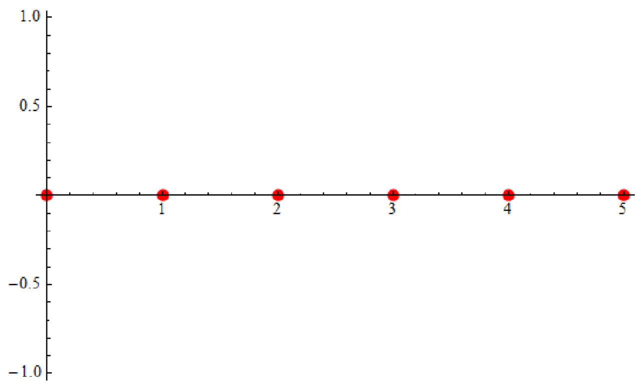
$$M = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & r_2 & 1 & r_2 & r_2^2 \\ 1 & 1 & s_2 & 1 & s_2 & s_2^2 \\ 1 & 1 & t_2 & 1 & t_2 & t_2^2 \\ 1 & 1 & u_2 & 1 & u_2 & u_2^2 \end{pmatrix}$$

$$\text{rank } M = 4$$

Splňují-li body P, Q, R, S, T, U rovnici $z = a \cdot y^2 + b \cdot y + c$, kde $(a, b, c) \in \mathbb{F}$, kde $z \in \{p_3, q_3, r_3, s_3, t_3, u_3\}$, $y \in \{p_2, q_2, r_2, s_2, t_2, u_2\}$, pak je hodnost rozšířené matice rovna 4 a existuje nekonečně mnoho řešení závislých na 2 libovolných parametrech. Pokud body P, Q, R, S, T, U tuto rovnici nesplňují, je hodnost rozšířené matice rovna 5 a řešení neexistuje.

$\rho)\hat{P} = [0,0]$, $\hat{Q} = [1,0]$, $\hat{R} = [r_1, 0]$, $\hat{S} = [s_1, 0]$, $\hat{T} = [t_1, 0]$, $\hat{U} = [u_1, 0]$, tj. 6 bodů na přímce o rovnici $y = 0$.

Obr 3.22 6 bodů na přímce



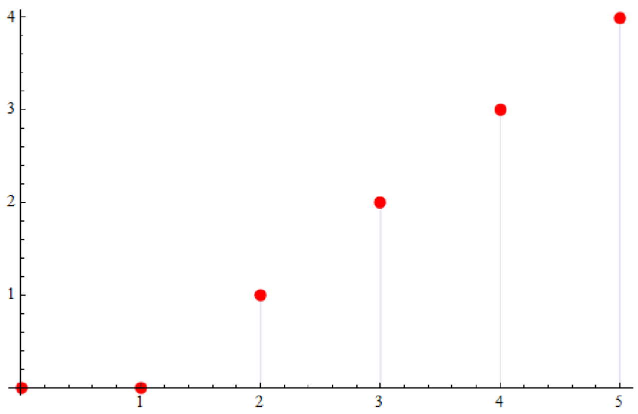
$$M = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & r_1 & 0 & r_1^2 & 0 & 0 \\ 1 & s_1 & 0 & s_1^2 & 0 & 0 \\ 1 & t_1 & 0 & t_1^2 & 0 & 0 \\ 1 & u_1 & 0 & u_1^2 & 0 & 0 \end{pmatrix}$$

$$\text{rank } M = 3$$

Splňují-li body P, Q, R, S, T, U rovnici $z = a \cdot x^2 + b \cdot x + c$, kde $(a, b, c) \in \mathbb{F}$, kde $z \in \{p_3, q_3, r_3, s_3, t_3, u_3\}$, $x \in \{p_1, q_1, r_1, s_1, t_1, u_1\}$, pak je hodnost rozšířené matice rovna 3 a existuje nekonečně mnoho řešení závislých na 3 libovolných parametrech. Pokud body P, Q, R, S, T, U tuto rovnici nesplňují, je hodnost rozšířené matice rovna 4 a řešení neexistuje.

$\sigma)\hat{P} = [0, 0]$, $\hat{Q} = [1, 0]$, $\hat{R} = [k \cdot (1 + r_2), r_2]$, $\hat{S} = [k \cdot (1 + s_2), s_2]$, $\hat{T} = [k \cdot (1 + t_2), t_2]$, $\hat{U} = [k \cdot (1 + u_2), u_2]$, tj. 2 body na přímce o rovnici $y = 0$ a 4 body na přímce o rovnici $x = k \cdot (1 + y)$.

Obr 3.23 4 body na přímce



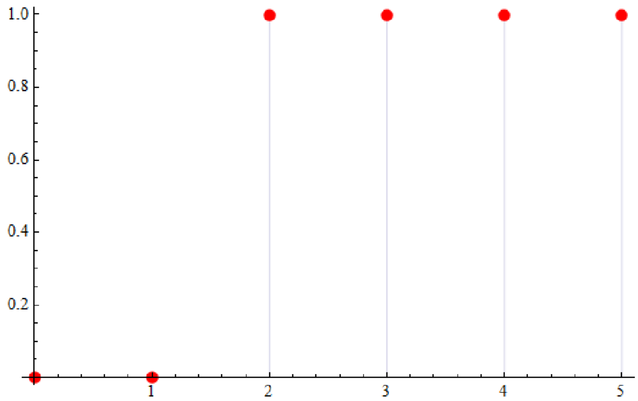
$$M = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & k \cdot (1 + r_2) & r_2 & (k \cdot (1 + r_2))^2 & r_2 \cdot k \cdot (1 + r_2) & r_2^2 \\ 1 & k \cdot (1 + s_2) & s_2 & (k \cdot (1 + s_2))^2 & s_2 \cdot k \cdot (1 + s_2) & s_2^2 \\ 1 & k \cdot (1 + t_2) & t_2 & (k \cdot (1 + t_2))^2 & t_2 \cdot k \cdot (1 + t_2) & t_2^2 \\ 1 & k \cdot (1 + u_2) & u_2 & (k \cdot (1 + u_2))^2 & u_2 \cdot k \cdot (1 + u_2) & u_2^2 \end{pmatrix}$$

$$\text{rank } M = 4$$

Splňují-li body P, Q, R, S, T, U rovnici $z = a \cdot y^2 + b \cdot y + c$, kde $(a, b, c) \in \mathbb{F}$, kde $z \in \{p_3, q_3, r_3, s_3, t_3, u_3\}$, $y \in \{p_2, q_2, r_2, s_2, t_2, u_2\}$, pak je hodnost rozšířené matice rovna 4 a existuje nekonečně mnoho řešení závislých na 2 libovolných parametrech. Pokud body P, Q, R, S, T, U tuto rovnici nesplňují, je hodnost rozšířené matice rovna 5 a řešení neexistuje.

$\tau)\hat{P} = [0,0]$, $\hat{Q} = [1,0]$, $\hat{R} = [r_1, 1]$, $\hat{S} = [s_1, 1]$, $\hat{T} = [t_1, 1]$, $\hat{U} = [u_1, 1]$, tj. 4 body na přímce o rovnici $y = 1$ a 2 body na přímce o rovnici $y = 0$.

Obr 3.24 body na dvou rovnoběžkách



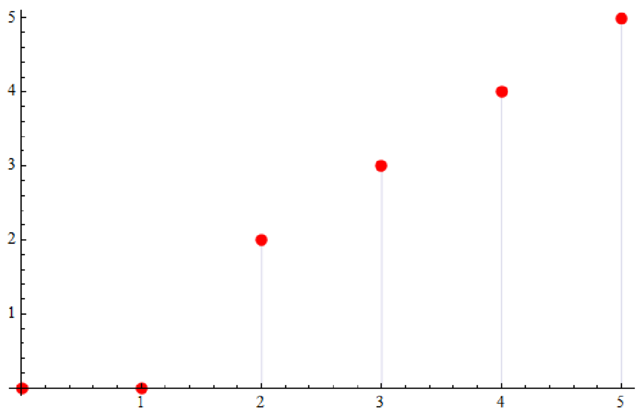
$$M = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & r_1 & 1 & r_1^2 & r_1 & 1 \\ 1 & s_1 & 1 & s_1^2 & s_1 & 1 \\ 1 & t_1 & 1 & t_1^2 & t_1 & 1 \\ 1 & u_1 & 1 & u_1^2 & u_1 & 1 \end{pmatrix}$$

$$\text{rank } M = 5$$

Splňují-li body P, Q, R, S, T, U rovnici $z = a \cdot x^2 + b \cdot x + c$, kde $(a, b, c) \in \mathbb{F}$, kde $z \in \{p_3, q_3, r_3, s_3, t_3, u_3\}$, $x \in \{p_1, q_1, r_1, s_1, t_1, u_1\}$, pak je hodnost rozšířené matice rovna 5 a existuje nekonečně mnoho řešení závislých na 1 libovolném parametru. Pokud body P, Q, R, S, T, U tuto rovnici nesplňují, je hodnost rozšířené matice rovna 6 a řešení neexistuje.

$\upsilon)\hat{P} = [0,0]$, $\hat{Q} = [1,0]$, $\hat{R} = [r_1, r_1]$, $\hat{S} = [s_1, s_1]$, $\hat{T} = [t_1, t_1]$, $\hat{U} = [u_1, u_1]$, tj. 5 bodů na přímce o rovnici $x = y$.

Obr 3.25 5 bodů na přímce



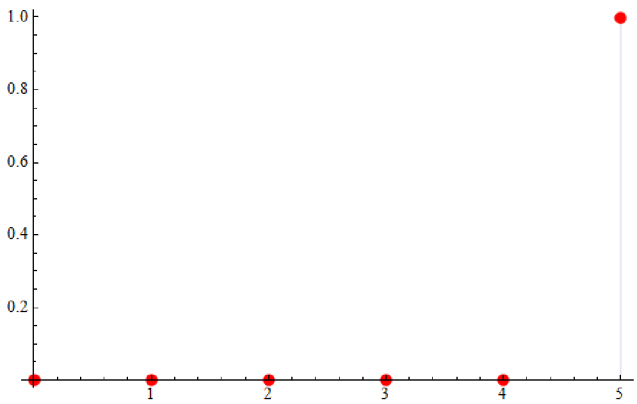
$$M = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & r_1 & r_1 & r_1^2 & r_1^2 & r_1^2 \\ 1 & s_1 & s_1 & s_1^2 & s_1^2 & s_1^2 \\ 1 & t_1 & t_1 & t_1^2 & t_1^2 & t_1^2 \\ 1 & u_1 & u_1 & u_1^2 & u_1^2 & u_1^2 \end{pmatrix}$$

$$\text{rank } M = 4$$

Splňují-li body P, Q, R, S, T, U **rovnici** $z = a \cdot x^2 + b \cdot x + c$**, kde** $(a, b, c) \in \mathbb{F}$**, kde** $z \in \{p_3, q_3, r_3, s_3, t_3, u_3\}$, $x \in \{p_1, q_1, r_1, s_1, t_1, u_1\}$**, pak je hodnost rozšířené matice rovna 4 a existuje nekonečně mnoho řešení závislých na 2 libovolných parametrech. Pokud body** P, Q, R, S, T, U **tuto rovnici nesplňují, je hodnost rozšířené matice rovna 5 a řešení neexistuje.**

$\varphi)\hat{P} = [0, 0]$, $\hat{Q} = [1, 0]$, $\hat{R} = [r_1, 0]$, $\hat{S} = [s_1, 0]$, $\hat{T} = [t_1, 0]$, $\hat{U} = [u_1, u_2]$,tj. 5 bodů na přímce o rovnici $y = 0$.

Obr 3.26 5 bodů na přímce



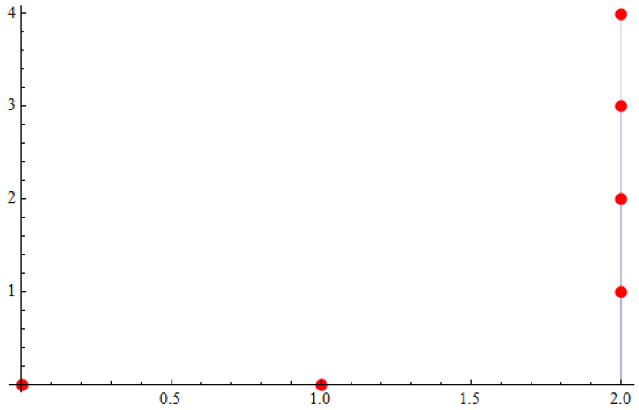
$$M = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & r_1 & 0 & r_1^2 & 0 & 0 \\ 1 & s_1 & 0 & s_1^2 & 0 & 0 \\ 1 & t_1 & 0 & t_1^2 & 0 & 0 \\ 1 & u_1 & u_2 & u_1^2 & u_1 \cdot u_2 & u_2^2 \end{pmatrix}$$

$$\text{rank } M = 4$$

Splňují-li body P, Q, R, S, T, U **rovnici** $z = a \cdot x^2 + b \cdot x + c$**, kde** $(a, b, c) \in \mathbb{F}$**, kde** $z \in \{p_3, q_3, r_3, s_3, t_3, u_3\}$, $x \in \{p_1, q_1, r_1, s_1, t_1, u_1\}$**, pak je hodnost rozšířené matice rovna 4 a existuje nekonečně mnoho řešení závislých na 2 libovolných parametrech. Pokud body** P, Q, R, S, T, U **tuto rovnici nesplňují, je hodnost rozšířené matice rovna 5 a řešení neexistuje.**

$\chi)\hat{P} = [0, 0]$, $\hat{Q} = [1, 0]$, $\hat{R} = [l, r_2]$, $\hat{S} = [l, s_2]$, $\hat{T} = [l, t_2]$, $\hat{U} = [l, u_2]$,tj. 4 body na přímce o rovnici $x = l$ a 2 body na přímce o rovnici $y = 0$.

Obr 3.27 body na kolmicích



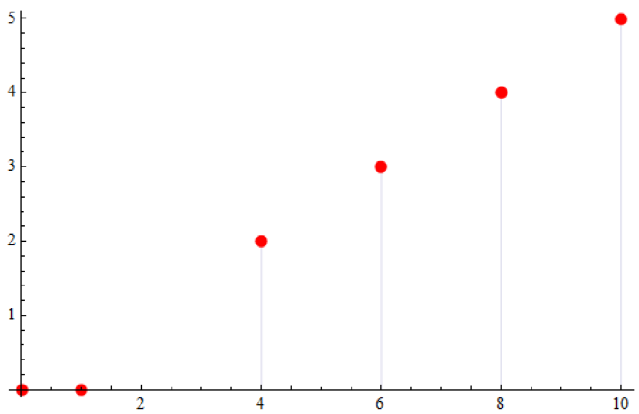
$$M = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & r_1 & r_2 & r_1^2 & l \cdot r_2 & r_2^2 \\ 1 & s_1 & s_2 & s_1^2 & l \cdot s_2 & s_2^2 \\ 1 & t_1 & t_2 & t_1^2 & l \cdot t_2 & t_2^2 \\ 1 & u_1 & u_2 & u_1^2 & l \cdot u_2 & u_2^2 \end{pmatrix}$$

$$\text{rank } M = 5$$

Splňují-li body P, Q, R, S, T, U rovnici $z = a \cdot x^2 + b \cdot x + c \cdot y^2 + d \cdot y + e$, (rovnice eliptického paraboloidu) kde $(a, b, c, d, e) \in \mathbb{F}$, kde $z \in \{p_3, q_3, r_3, s_3, t_3, u_3\}$, $x \in \{p_1, q_1, r_1, s_1, t_1, u_1\}$, $y \in \{p_2, q_2, r_2, s_2, t_2, u_2\}$, pak je hodnost rozšířené matice rovna 5 a existuje nekonečně mnoho řešení závislých na 1 libovolném parametru. Pokud body P, Q, R, S, T, U tuto rovnici nesplňují, je hodnost rozšířené matice rovna 6 a řešení neexistuje.

$\psi)\hat{P} = [0, 0]$, $\hat{Q} = [1, 0]$, $\hat{R} = [k \cdot r_2, r_2]$, $\hat{S} = [k \cdot s_2, s_2]$, $\hat{T} = [k \cdot t_2, t_2]$, $\hat{U} = [k \cdot u_2, u_2]$,tj. 5 bodů na přímce o rovnici $x = k \cdot y$.

Obr 3.28 5 bodů na přímce



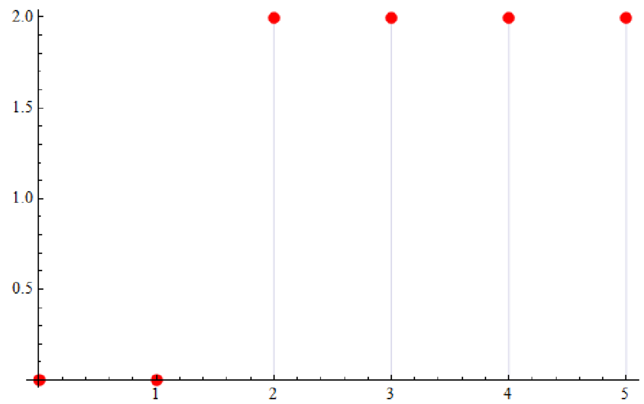
$$M = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & k \cdot r_2 & r_2 & k^2 \cdot r_2^2 & k \cdot r_2^2 & r_2^2 \\ 1 & k \cdot s_2 & s_2 & k^2 \cdot s_2^2 & k \cdot s_2^2 & s_2^2 \\ 1 & k \cdot t_2 & t_2 & k^2 \cdot t_2^2 & k \cdot t_2^2 & t_2^2 \\ 1 & k \cdot u_2 & u_2 & k^2 \cdot u_2^2 & k \cdot u_2^2 & u_2^2 \end{pmatrix}$$

$$\text{rank } M = 5$$

Splňují-li body P, Q, R, S, T, U rovnici $z = a \cdot y^2 + b \cdot y + c$, kde $(a, b, c) \in \mathbb{F}$, kde $z \in \{p_3, q_3, r_3, s_3, t_3, u_3\}$, $y \in \{p_2, q_2, r_2, s_2, t_2, u_2\}$, pak je hodnost rozšířené matice rovna 5 a existuje nekonečně mnoho řešení závislých na 1 libovolném parametru. Pokud body P, Q, R, S, T, U tuto rovnici nesplňují, je hodnost rozšířené matice rovna 6 a řešení neexistuje.

$\omega)\hat{P} = [0, 0]$, $\hat{Q} = [1, 0]$, $\hat{R} = [r_1, l]$, $\hat{S} = [s_1, l]$, $\hat{T} = [t_1, l]$, $\hat{U} = [u_1, l]$,tj. 4 body na přímce o rovnici $y = l$ a 2 body na přímce o rovnici $y = 0$.

Obr 3.29 body na dvou rovnoběžkách



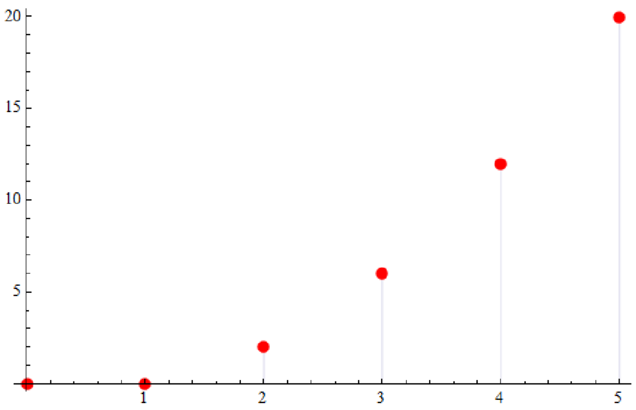
$$M = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & r_1 & l & r_1^2 & l \cdot r_1 & l^2 \\ 1 & s_1 & l & s_1^2 & l \cdot s_1 & l^2 \\ 1 & t_1 & l & t_1^2 & l \cdot t_1 & l^2 \\ 1 & u_1 & l & u_1^2 & l \cdot u_1 & l^2 \end{pmatrix}$$

$$\text{rank } M = 5$$

Splňují-li body P, Q, R, S, T, U rovnici $z = a \cdot x^2 + b \cdot x + c$, kde $(a, b, c) \in \mathbb{F}$, kde $z \in \{p_3, q_3, r_3, s_3, t_3, u_3\}$, $x \in \{p_1, q_1, r_1, s_1, t_1, u_1\}$, pak je hodnost rozšířené matice rovna 5 a existuje nekonečně mnoho řešení závislých na 1 libovolném parametru. Pokud body P, Q, R, S, T, U tuto rovnici nesplňují, je hodnost rozšířené matice rovna 6 a řešení neexistuje.

$\alpha\alpha)\hat{P} = [0, 0]$, $\hat{Q} = [1, 0]$, $\hat{R} = [r_1, k \cdot (r_1^2 - r_1)]$, $\hat{S} = [s_1, k \cdot (s_1^2 - s_1)]$, $\hat{T} = [t_1, k \cdot (t_1^2 - t_1)]$, $\hat{U} = [u_1, k \cdot (u_1^2 - u_1)]$,tj. 6 bodů na parabole o rovnici $y = k \cdot (x^2 - x)$.

Obr 3.30 6 bodů na parabole



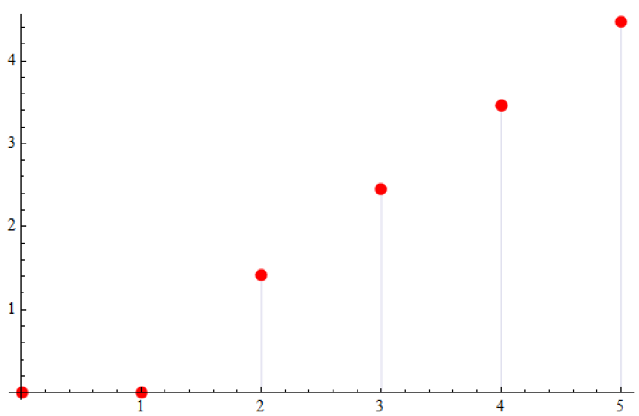
$$M = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & r_1 & k\cdot(r_1^2 - r_1) & r_1^2 & k\cdot r_1\cdot(r_1^2-r_1) & k^2\cdot(r_1^2-r_1)^2 \\ 1 & s_1 & k\cdot(s_1^2 - s_1) & s_1^2 & k\cdot s_1\cdot(s_1^2-s_1) & k^2\cdot(s_1^2-s_1)^2 \\ 1 & t_1 & k\cdot(t_1^2 - t_1) & t_1^2 & k\cdot t_1\cdot(t_1^2-t_1) & k^2\cdot(t_1^2-t_1)^2 \\ 1 & u_1 & k\cdot(u_1^2 - u_1) & u_1^2 & k\cdot u_1\cdot(u_1^2-u_1) & k^2\cdot(u_1^2-u_1)^2 \end{pmatrix}$$

$$\text{rank } M = 5$$

Splňují-li body P, Q, R, S, T, U rovnici $z = a\cdot x^4 + b\cdot x^3 + c\cdot x^2 + d\cdot x + e$, kde $(a,b,c,d,e) \in \mathbb{F}$, kde $z \in \{p_3, q_3, r_3, s_3, t_3, u_3\}$, $x \in \{p_1, q_1, r_1, s_1, t_1, u_1\}$, pak je hodnost rozšířené matice rovna 5 a existuje nekonečně mnoho řešení závislých na 1 libovolném parametru. Pokud body P, Q, R, S, T, U tuto rovnici nesplňují, je hodnost rozšířené matice rovna 6 a řešení neexistuje.

$\alpha\beta)\hat{P} = [0,0]$, $\hat{Q} = [1,0]$, $\hat{R} = \left[r_1, \sqrt{k\cdot(r_1^2 - r_1)}\right]$, $\hat{S} = \left[s_1, \sqrt{k\cdot(s_1^2 - s_1)}\right]$, $\hat{T} = \left[t_1, \sqrt{k\cdot(t_1^2 - t_1)}\right]$, $\hat{U} = \left[u_1, \sqrt{k\cdot(u_1^2 - u_1)}\right]$,tj. 6 bodů na hyperbole o rovnici $y^2 = k\cdot(x^2 - x)$.

Obr 3.31 6 bodů na hyperbole



$$M = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & r_1 & \sqrt{k \cdot (r_1^2 - r_1)} & r_1^2 & r_1 \cdot \sqrt{k \cdot (r_1^2 - r_1)} & k \cdot (r_1^2 - r_1) \\ 1 & s_1 & \sqrt{k \cdot (s_1^2 - s_1)} & s_1^2 & s_1 \cdot \sqrt{k \cdot (s_1^2 - s_1)} & k \cdot (s_1^2 - s_1) \\ 1 & t_1 & \sqrt{k \cdot (t_1^2 - t_1)} & t_1^2 & t_1 \cdot \sqrt{k \cdot (t_1^2 - t_1)} & k \cdot (t_1^2 - t_1) \\ 1 & u_1 & \sqrt{k \cdot (u_1^2 - u_1)} & u_1^2 & u_1 \cdot \sqrt{k \cdot (u_1^2 - u_1)} & k \cdot (u_1^2 - u_1) \end{pmatrix}$$

$$\text{rank } M = 5$$

Splňují-li body P, Q, R, S, T, U rovnici $z^2 = a \cdot x^4 + b \cdot x^3 + c \cdot x^2 + d \cdot x + e$, (rovnice hyperbolického paraboloidu) kde $(a, b, c, d, e) \in \mathbb{F}$, kde $z \in \{p_3, q_3, r_3, s_3, t_3, u_3\}$, $x \in \{p_1, q_1, r_1, s_1, t_1, u_1\}$, pak je hodnost rozšířené matice rovna 5 a existuje nekonečně mnoho řešení závislých na 1 libovolném parametru. Pokud body P, Q, R, S, T, U tuto rovnici nesplňují, je hodnost rozšířené matice rovna 6 a řešení neexistuje.

V Ostatních případech je $\text{rank} M = 6$, tedy soustava má právě jedno řešení.

4. Algoritmy vícerozměrné interpolace

4.1. Jednorozměrná Lagrangeova interpolace

Lagrangeův interpolační polynom pro zadané body $[x_1, y_1], \ldots, [x_n, y_n]$ definujeme jako

$$L := \sum_{j=1}^{n} y_j \prod_{\substack{i=1 \\ i \neq j}}^{n} \frac{X - x_i}{x_j - x_i},$$

Označíme-li stupeň interpolačního polynomu s, pak můžeme psát:

$$s \leq n - 1.$$

Rovnost nastává pouze v případě, kdy:

$$\sum_{i=1}^{n} y_i \prod_{\substack{j=1 \\ j \neq i}}^{n} \frac{1}{x_j - x_i} \neq 0.$$

Lagrangeovu jednorozměrnou interpolaci zobecníme pro případ více neurčitých. Ukážeme zde dva způsoby.

4.2. Lagrangeova vícerozměrná interpolace použitím souhrnného vzorce

Pro výpočet vícerozměrné Lagrangeovy interpolace můžeme použít souhrnný vzorec [3]

$$L := \sum_{j=0}^{n} y_j \prod_{k=1}^{m} \prod_{\substack{i=0 \\ i \neq j}}^{n} \frac{X_k - x_{ki}}{x_{kj} - x_{ki}},$$

kde m označuje dimenzi a n značí počet bodů. Označíme-li stupeň interpolačního polynomu s, pak můžeme psát:

$$s \leq m \cdot (n - 1).$$

Rovnost nastává pouze v případě, kdy:

$$\sum_{\sigma \in A_3} y_{\sigma_1} \prod_{i=1}^{m-1} (x_{i\sigma_2} - x_{i\sigma_3}) \neq 0,$$

kde $\sigma = (\sigma_1, \sigma_2, \sigma_3)$ a A_3 je alternující podgrupa, což je podgrupa sudých permutací na konečné množině. Postup výpočtu si zde ukážeme na příkladu:

Mějme body: $[3, 5, 8], [2, 1, 3], [-2, 4, 7]$.Pak

$$L := 8 \cdot (\frac{x-2}{3-2} \cdot \frac{x+2}{3+2} \cdot \frac{y-1}{5-1} \cdot \frac{y-4}{5-4}) + 3 \cdot (\frac{x-3}{2-3} \cdot \frac{x+2}{2+2} \cdot \frac{y-5}{1-5} \cdot \frac{y-4}{1-4}) +$$

$$+7 \cdot (\frac{x-3}{-2-3} \cdot \frac{x-2}{-2-2} \cdot \frac{y-5}{4-5} \cdot \frac{y-1}{4-1}).$$

Vyřešením poté získáme hledaný interpolační polynom

$$L := \frac{53}{240}x^2y^2 - \frac{59}{80}x^2y - \frac{7}{30}x^2 + \frac{31}{48}xy^2 - 4\frac{1}{16}xy + 4\frac{1}{6}x - 1\frac{37}{40}y^2 + 8\frac{33}{40}y - 2\frac{2}{5}$$

Tento vzorec však lze použít jen v případě, že bod nemá žádnou souřadnici shodnou s jiným bodem. V opačném případě bychom dostali dělení nulou a tento vzorec bychom použít nemohli. Pro tyto případy použijeme druhého způsobu.

4.3. Lagrangeova vícerozměrná interpolace pomocí determinantů

Tato kapitola je založena na článku [2].

Nechť $f = f(X_1, ..., X_m)$ je polynom stupně s o m proměnných. Protože f má $\binom{s+m}{s} = n$ členů, nutnou podmínkou je, že máme n různých bodů $(x_{1i}, ..., x_{mi}, y_i) \in \mathbb{R}^{s+1}$, $1 \leq i \leq n$, $y_i = f(x_{1i}, ..., x_{mi})$ proto, aby byla f jednoznačně definována. Jinými slovy $f(X_1, ..., X_m) = \sum_{\mathbf{e}_i \cdot \mathbf{1} \leq s} \alpha_{\mathbf{e}_i} \mathbf{X}^{\mathbf{e}_i}$, kde α_{e_i} jsou koeficienty f, $\mathbf{X} = (X_1, ..., X_m)$ je m-tice nezávisle proměnných f, $\mathbf{e}_i = (e_{1i}, ..., e_{mi})$ je multiindex, jehož položky jsou celá nezáporná čísla tvořící uspořádaný rozklad čísla mezi 0 a s včetně a $\mathbf{1} = (1, ..., 1)$. $\mathbf{e}_i \cdot \mathbf{1} := \sum_{j=1}^{m} e_{ji}$ je obvyklý vnitřní součin a $\mathbf{X}^{\mathbf{e}_i} := \prod_{j=1}^{m} X_j^{e_{ji}}$. Podle známého Lagrangeova postupu budeme f psát ve formě $\sum_{i=1}^{\rho} f_i l_i(\mathbf{X})$, kde $l_i(\mathbf{X})$ je polynom nezávislých proměnných $X_1, ..., X_m$ s vlastností, že když $\mathbf{X}$ je rovno i-té hodnotě, nebo $\mathbf{X} = \mathbf{x}_i((x_1, ..., x_m) = (x_{1i}, ..., x_{mi}))$, pak $l_i(\mathbf{x}_i) = 1$ a $l_j(\mathbf{x}_i) = 0 (j \neq i)$. Abychom toho dosáhli, uvažujme soustavu lineárních rovnic $f_i = \sum_{\mathbf{e}_j \cdot \mathbf{1} \leq s} \alpha_{\mathbf{e}_j} \mathbf{x}_i^{\mathbf{e}_j}$, kde $1 \leq i \leq n$. Z této soustavy zkonstruujeme matici $M = [\mathbf{x}_i^{\mathbf{e}_j}]$:

$$M = \begin{pmatrix} x_1^{e_1} & \cdots & x_1^{e_\rho} \\ \vdots & & \vdots \\ x_i^{e_1} & \cdots & x_i^{e_\rho} \\ \vdots & & \vdots \\ x_\rho^{e_1} & \cdots & x_\rho^{e_\rho} \end{pmatrix}$$

Předpokládáme, že $\det(M) \neq 0$. Ačkoliv bychom mohli řešit koeficienty α_i v f invertováním M (která, jak víme, je čtvercová, protože počet rovnic výše uvedeného lineárního systému je stejný jako počet koeficientů), toto není náš cíl. Užitečnost Lagrangeovy interpolace je o tom, že můžeme určit f bez explicitního řešení pro koeficienty.

Pozn.: Je-li M singulární, pak koeficienty f nejsou jednoznačně určeny a f je nejednoznačný polynom. Proto f je jednoznačná tehdy a pouze tehdy, když M je regulární. V opačném případě je popis geometrické konfigurace ρ bodů, pro něž je $\det(M) = 0$, složitý problém (řešili jsme ve třetí kapitole pro $4, 5$ a 6 bodů nad rovinou).

Nechť $\Delta = \det(M)$. Nyní uděláme substituci $x_j = X$ v M, dostáváme následující matici $M_j(X)$:

$$M_j(X) = \begin{pmatrix} x_1^{e_1} & \cdots & x_1^{e_\rho} \\ \vdots & & \vdots \\ X^{e_1} & \cdots & X^{e_\rho} \\ \vdots & & \vdots \\ x_\rho^{e_1} & \cdots & x_\rho^{e_\rho} \end{pmatrix}$$

Nechť $\Delta_j(X) = \det(M_j(X))$. Dále uděláme substituci $X = x_i$ v $M_j(X)(i \neq j)$, to dává následující matici $(M_j)_i$:

$$(M_j)_i = \begin{pmatrix} x_1^{e_1} & \cdots & x_1^{e_\rho} \\ \vdots & & \vdots \\ x_i^{e_1} & \cdots & x_i^{e_\rho} \\ \vdots & & \vdots \\ x_i^{e_1} & \cdots & x_i^{e_\rho} \\ \vdots & & \vdots \\ x_\rho^{e_1} & \cdots & x_\rho^{e_\rho} \end{pmatrix}$$

Poznamenejme, že i-tý řádek se v $(M_j)_i$ objevuje dvakrát. To znamená, že $\det(M_j)_i = 0$. Jinými slovy, když $X = x_i$, pak $\Delta_j(x_i) = 0 (i \neq j)$. Navíc konstrukcí $X = x_i \Rightarrow \Delta_i(X) = \Delta$. Z toho důvodu

$$l_i(X) = \frac{\Delta_i(X)}{\Delta}$$

a dále

$$f = \sum_{i=1}^{\rho} f_i \frac{\Delta_i(X)}{\Delta}.$$

Mějme interpolaci nad $\mathbb{R}^m$, pro n bodů. Vezměme kombinační čísla $\binom{m}{0}$, $\binom{m+1}{1}$, $\binom{m+2}{2}$, …, obecně $\binom{m+s}{s}$. Z těchto čísel vybereme to, pro které platí $\binom{m+s}{s} \geq n$. Pak s je stupeň interpolačního polynomu.

Postup si ukážeme na příkladu. Mějme body: $[3, 5, 8]$, $[2, 1, 3]$, $[-2, 4, 7]$. Řešení hledáme ve tvaru: $z = \alpha_1 x_i + \alpha_2 y_i + \alpha_3$. Dostáváme tedy soustavu rovnic:

$$\begin{aligned} 8 &= 3\alpha_1 + 5\alpha_2 + \alpha_3 \\ 3 &= 2\alpha_1 + \alpha_2 + \alpha_3 \\ 7 &= -2\alpha_1 + 4\alpha_2 + \alpha_3 \end{aligned}$$

Dostáváme následující matice:

$$M = \begin{pmatrix} 3 & 5 & 1 \\ 2 & 1 & 1 \\ -2 & 4 & 1 \end{pmatrix}$$

$$M_1 = \begin{pmatrix} x & y & 1 \\ 2 & 1 & 1 \\ -2 & 4 & 1 \end{pmatrix}$$

$$M_2 = \begin{pmatrix} 3 & 5 & 1 \\ x & y & 1 \\ -2 & 4 & 1 \end{pmatrix}$$

$$M_3 = \begin{pmatrix} 3 & 5 & 1 \\ 2 & 1 & 1 \\ x & y & 1 \end{pmatrix}$$

$$\det M = -19, \det M_1 = -3x - 4y + 10, \det M_2 = -x + 5y - 22, \det M_3 = 4x - y - 7.$$

Dosazením dostáváme:

$$z = 8\frac{(-3x - 4y + 10)}{-19} + 3\frac{(-x + 5y - 22)}{-19} + 7\frac{(4x - y - 7)}{-19} = \frac{-x + 24y + 35}{19}.$$

Ihned vidíme, že stupeň polynomu je v tomto případě nižší, než při použití souhrnného vzorce.

4.4. Vícerozměrná interpolace nad konečnými poli

Mějme pole $\mathbb{F}_{p^k}$. Platí

$$x^{p^k} = x.$$

Věta: Uvažujme zobrazení $\varphi : \mathbb{F}_{p^k} \longrightarrow \mathbb{F}_{p^k}$ definované $\varphi(x) = x^p$. Pak φ je bijekce a platí

$$\varphi^k = \underbrace{\varphi \circ \ldots \circ \varphi}_{k} : \varphi^k(x) = x^{p^k} = x$$

Důsledek: Malá Fermatova věta
Pro každé prvočíslo p a každé celé číslo a takové, že p nedělí a (a není násobkem p), platí

$$a^p \equiv a \pmod{p}.$$

Důsledek: Polynom x^{p^k} indukuje totéž zobrazení jako x.

Nyní pro redukci stupně monomu použijeme $x^l \longmapsto x^{l \bmod p^k - 1}$, jelikož platí

$$\begin{aligned} x^{p^k} &= x \\ x^{p^k-1} &= 1 \\ x^l \cdot x^{p^k-1} &= x^l \\ x^{l+p^k-1} &= x^l \end{aligned}$$

Označme s stupeň polynomu. Pak platí

$$s \leq p^k - 2.$$

Nyní tento vztah porovnejme se vztahem pro stupeň polynomu vícerozměrné interpolace použitím souhrnného vzorce. Řešme, jaká volba m, n nevyvolá nutnost redukce polynomu.

Vezměme si například pole $\mathbb{F}_4$. Podle vzorce pro stupeň polynomu platí $s \leq 2$, tzn. že maximální stupeň polynomu bude 2. Nyní vezměme vzorec pro stupeň polynomu Lagrangeovy vícerozměrné interpolace a zkoumejme, kdy už je nutná redukce stupně polynomu. Zjistíme, že pokud je $m = 3$, $n = 2$ či $m = 2$ a $n = 3$, je redukce polynomu již nutná. Pro pole $\mathbb{F}_8$ nebo $\mathbb{F}_9$ dochází k redukci polynomu při $m = 2$, $n = 5$ či $m = 3$ a $n = 4$.

5. Manuál k notebooku v prostředí Mathematica

Interpolaci nad rovinou pro $4, 5$ a 6 bodů jsem řešila v programu Mathematica. Vytvořila jsem dva notebooky. První z nich řeší interpolaci nad reálnými čísly a druhý notebook interpolaci nad konečnými poli. Pro správné fungování obou notebooků je nutné vytvořit složku $C:\backslash ProgramFiles\backslash WolframResearch\backslash Mathematica\backslash 8.0\backslash AddOns\backslash Packages$ $\backslash MultivariateInterpolation$ a zkopírovat do ní soubor `I456.m`. Teď již přejděme k jednotlivým notebookům.

5.1. Notebook Test I456Points.nb

Nejprve musíme načíst soubor `I456.m` pomocí příkazu

$$\ll MultivariateInterpolation`I456Points`$$

Nyní již můžeme zadávat body. Tento notebook řeší interpolaci pro $4, 5$ nebo 6 bodů nad rovinou. Každý bod tudíž musí mít 3 souřadnice, které jsou oddělené čárkou. Takže například 4 body zadáme následovně:

$$Body = \{\{5,0,2\},\{1,0,1\},\{2,2,0\},\{3,6,1\}\}.$$

Nyní si popíšeme všechny procedury:

`I456Info`$[Body]$ kontroluje, zda jsou body zadány správně. Je zde ošetřeno, aby každý bod měl 3 souřadnice a podkladové body v rovině byly různé. Výstupem nám v našem případě bude:

`Vícerozměrná interpolace nad rovinnými body` $\{\{5,0\},\{1,0\},\{2,2\},\{3,6\}\}$

`I456ResSoust`$[Body, a, b, c, d, e, f]$ řeší soustavu rovnic, pro neznámé a, b, c, d, e, f. Tím máme určenou kvadriku a ihned vidíme, kolik existuje řešení, existuje-li vůbec nějaké. Náš výstup bude ve tvaru

$$\left\{\left\{b \to \frac{23}{20} - \frac{6a}{5},\ d \to \frac{1}{20}\cdot(-3+4a),\ e \to \frac{1}{90}\cdot(-71+23a-60c),\ f \to \frac{1}{360}\cdot(131-38a+60c)\right\}\right\}$$

`I456LinTransf`$[Body]$ provede lineární transformaci zadaných bodů. První bod převede do bodu $\{0,0\}$ a druhý do bodu $\{1,0\}$. Pro naše body je výstupem:

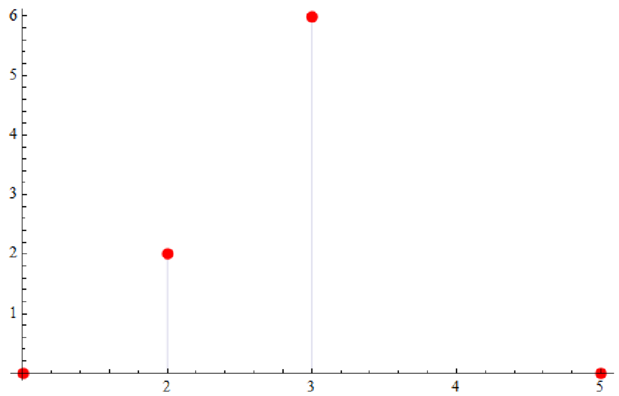
$$\left\{\{0,0\},\{1,0\},\left\{\frac{3}{4},-\frac{1}{2}\right\},\left\{\frac{1}{2},-\frac{3}{2}\right\}\right\}$$

Nejdůležitější procedurou celého notebooku je
`I456PolohaPodBodu`$[Body]$, jejímž výstupem je počet řešení a případná zvláštní poloha podkladových bodů. Pro vzorové zadání je výstupem

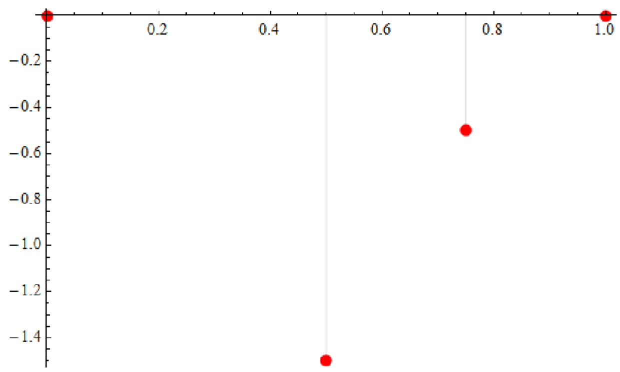
`nekonečně mnoho řešení závislých na 2 libovolných parametrech`

Poslední dvě procedury
`I456KPobraz`[*Body*] ,resp. `I456KPobrazt`[*Body*] nám vykreslí zadané, resp. ztransformované podkladové body do kartézské soustavy souřadnic.

Obr 5.1 zadané body



Obr 5.2 ztransformované body



5.2. Notebook Test I456PointsFiniteField.nb

Tento notebook funguje obdobně jako notebook `Test I456Points.nb`. Můžeme ho použít pro zjištění interpolace nad konečnými poli pro 4 body. Čtyři body zadáme následovně:

$$Body = \{\{k[0], k[0], k[3]\}, \{k[1], k[0], k[0]\}, \{k[1], k[5], k[0]\}, \{k[0], k[3], k[0]\}\}.$$

V tomto notebooku je jediná nová procedura s názvem
`I456KPole`[*Body*]. Výstupem je počet řešení a zvláštní poloha podkladových bodů. V našem případě je výstup tvaru:

```
body leží na dvou rovnoběžkách-nekonečně mnoho řešení závislých na 2
                    libovolných parametrech.
```

6. Závěr

V bakalářské práci jsme řešili vícerozměrnou interpolaci a diskutovali jsme stupeň interpolačního polynomu. Také jsme se zabývali vytvořením notebooku, který tuto interpolaci bude řešit.

V úvodní kapitole jsme zkonstruovali matici afinní transformace, kterou využijeme ve třetí kapitole. V té jsme řešili interpolaci $4, 5$ a 6 bodů nad rovinou. Při řešení interpolace jsme postupovali přímo, a to řešením soustavy rovnic. Ve čtvrté kapitole jsme se poté zaměřili na vícerozměrnou interpolaci nad libovolným polem. Tu jsme vyřešili nepřímo, algoritmy nevyžadujícími řešení soustavy rovnic. Pro vytvoření interpolačního polynomu jsme použili Lagrangeovu metodu. V poslední kapitole jsme popsali notebook v prostředí Mathematica, který řeší vícerozměrnou interpolaci nad libovolným polem.

V kapitole o interpolaci nad rovinou jsme prodiskutovali všechny možnosti, jak lze proložit zadanými body kvadriku. Vypsali jsme všechny zvláštní polohy podkladových bodů a k nim příslušná řešení. V následující kapitole jsme se zabývali vícerozměrnou interpolací. Tu jsme řešili dvěma způsoby, nejdříve souhrnným vzorcem a poté pomocí determinantů. V obou případech je zde uveden vzorec pro stupeň interpolačního polynomu a názorný příklad. Dále jsme se zabývali stupněm interpolačního polynomu nad konečnými poli. V poslední kapitole jsme pak popsali jednotlivé procedury funkčního notebooku v prostředí Mathematica, který řeší vícerozměrnou interpolaci nad libovolným polem.

Literatura

[1] GRIGORIJEV, D. Y., KARPINSKI, M., SINGER, M. F. *Fast parallel algorithms for sparse multivariate polynomial interpolation over finite fields*. SIAM J. Comp. 19, 1059-1063, 1990.

[2] SANIEE K. *A simple expression for multivariate Lagrange interpolation*. New Providence High School, New Providence, NJ 07974, 2007.

[3] SCHUSTER, D. *Multivariate Interpolationsangriffe auf symmetrische Chiffren*. Diploma Thesis, Technische Universität Darmstadt, 2007.