VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA STROJNÍHO INŽENÝRSTVÍ
ÚSTAV MATEMATIKY

FACULTY OF MECHANICAL ENGINEERING
INSTITUTE OF MATHEMATICS

KVADRATICKÉ POLYNOMY NAD BINÁRNÍMI POLI

QUADRATIC POLYNOMIALS OVER BINARY FIELDS

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — BARBORA NAVRÁTILOVÁ
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): Barbora Navrátilová

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:

Kvadratické polynomy nad binárními poli

v anglickém jazyce:

Quadratic polynomials over binary fields

Stručná charakteristika problematiky úkolu:

Práce se zaměří na studium kvadratických polynomů nad konečnými poli charakteristiky 2. Mezi těmito polynomy pak na ty, které indukují bijekci nad polem a na popis třídy takových bijekcí. Dále bude vyšetřeno zobecnění pro n kvadratických polynomů n neurčitých.

Cíle bakalářské práce:

- studium polynomů na binárních polích, možnosti jejich grafického znázornění
- popis kvadratických polynomů indukující bijekci na binárních polích o 2^n prvcích (alespoň pro malá n)
- diskuse vlastnosti těchto bijekcí (typ permutace)
- uvedení souvislostí s Maubachovou hypotézou o neexistenci k-tice polynomů indukujících lichou permutaci

Seznam odborné literatury:

[1] Lidl, R., Niederreiter, H.: Finite Fields, Cambridge University Press, 1997
[2] Maubach, S., A problem on polynomial maps over finite fields, arXiv:0802.0630v1

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

Abstrakt
Tato bakalářská práce se zabývá kvadratickými polynomy nad binárními poli, které indukují bijekci. Stanovíme podmínky bijekce na konktrétním binárním poli s výhledem dalšího zkoumání polynomiálních automorfismů indukujících bijekci.

Summary
This bachelor's work concerns to quadratic polynomials over binary fields which induce bijection. We specify conditions for the bijection on the particular binary field with a view to further examine the polynomial automorphisms inducing a bijection.

Klíčová slova
Polynomiální automorfismus, kvadratický polynom, binární pole

Keywords
Polynomial automorphisms, quadratic polynomial, binary field

NAVRÁTILOVÁ, B. *Kvadratické polynomy nad binárními poli*. Brno: Vysoké učení technické v Brně, Fakulta strojního inženýrství, 2011. 39 s. Vedoucí doc. RNDr. Miroslav Kureš, Ph.D.

Prohlašuji, že jsem bakalářskou práci „Kvadratické polynomy nad binárními poli“ vypracovala samostatně s použitím odborné literatury a pramenů, uvedených na seznamu, jenž je součástí této práce.

Barbora Navrátilová

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

Barbora Navrátilová

Obsah

1. Úvod

Předložená bakalářská práce je zaměřena na kvadratické polynomy nad binárními poli, které indukují bijekci. V úvodu této práce zavádíme polynomy obecně pro okruh, kde následně závádíme i veškeré operace, pojmy polynomiálního zobrazení, substitučního principu a kompozice. Nezavádíme binární aritmetiku viz [1]. V další kapitole se zabýváme polynomiálními automorfismy na konečných polích, závádíme pojem krotkého automorfismu, který zmiňujeme především v souvislosti s Maubachovou hypotézou, jež pojednává o neexistenci liché permutace polynomiálního zobrazení $\mathbb{F}_{2^m}^n \to \mathbb{F}_{2^m}^n$, $n \geq 2$, $m > 1$.
Další kapitola je věnována vlastní analýze konkrétních binárních polí. Zabýváme se polynomy jedné neurčité, dvojicí polynomů dvou neurčitých. Pro tuto část byl vytvořen program v systému Mathematica. Na základě jeho výstupu byla formulována a následně dokazována tvrzení o vlastnostech dvojice polynomů nad konečným polem $\mathbb{F}_{2^2}$. Uvádíme podmínky nutné i postačující pro bijekci, přičemž platnost nutných podmínek můžeme uvažovat obecně. Zároveň postačující podmínky nám mohou sloužit i jako návod ke konstrukci bijektivní dvojice.
Následující kapitola je věnována grafické interpretaci těchto dvojic kvadratických polynomů na toru, kde je mimo jiné i srovnání jejich specifických vlastností s polem $\mathbb{F}_{2^3}$, tedy vyloučení obecné platnosti pro libovolné binární pole.
Poslední kapitola je věnována menší diskusi získaných výsledků v souvislosti s Maubachovou hypotézou vzhledem k počtu bijekcí indukovaných krotkými automorfismy. Uvádíme přehled počtu bijekcí pro pole $\mathbb{F}_{2^2}$ pro kombinace dvojic polynomů nejvýše kvadratických.

2. Polynomy n neurčitých nad okruhem

Tuto kapitolu rozdělíme na dvě části. V první části si uvedeme speciální případ polynomů n neurčitých - polynomy jedné neurčité. Uvedeme zde základní definice, zavedeme základní aritmetiku polynomů a některé vlastnosti, které budeme dále potřebovat. Druhá část zobecní poznatky z první části pro polynomy n neurčitých a také pro n-tice takových polynomů. Důkazy v obou částech mají obdobnou konstrukci, proto ve většině případů jsou pro názornost uvedeny pouze v první části.

2.1. Polynomy jedné neurčité nad okruhem

Definice 2.1. Nechť $R = (R, +, \cdot)$ je neprázdná množina se dvěma binárními operacemi $+$ a $\cdot$. R se nazývá *okruh*, jestliže platí:

$(R1)$ $(R, +)$ je komutativní grupa.

$(R2)$ $(R, \cdot)$ je pologrupa s jedničkou.

$(R3)$ platí tzv. *distributivní zákony*: pro $a, b, c \in R$

$$a \cdot (b + c) = a \cdot b + a \cdot c \ ,$$

$$(b + c) \cdot a = b \cdot a + c \cdot a \ .$$

Neutrální prvek grupy $(R, +)$ se nazývá *neutrální prvek okruhu* R vzhledem k operaci $+$ a označíme jej 0_R.
Neutrální prvek pologrupy $(R, \cdot)$ se nazývá *neutrální prvek okruhu* R vzhledem k operaci $\cdot$ a označíme jej 1_R.

Poznámka 2.1. Obvykle předpokládáme $1_R \neq 0_R$, v případě rovnosti by se jednalo o triviální okruh.

Definice 2.2. Nechť R je okruh. Jestliže pologrupa $(R, \cdot)$ je komutativní, nazývá se R *komutativní okruh.*

Definice 2.3. Nechť $(R, +, \cdot)$ a $(\underline{R}, \underline{+}, \underline{\cdot})$ jsou dva okruhy. Zobrazení $\varphi : R \to \underline{R}$ nazveme *homomorfismus* jestliže pro $a, b \in R$

$$\begin{aligned} \varphi(a + b) &= \varphi(a) \underline{+} \varphi(b), \\ \varphi(a \cdot b) &= \varphi(a) \underline{\cdot} \varphi(b), \\ \varphi(1_R) &= 1_{\underline{R}}. \end{aligned}$$

Definice 2.4. Polynom jedné neurčité nad okruhem R definujeme jako zobrazení $a : \mathbb{N}_0 \to R$ s konečným nosičem.

Označení 2.1. Polynom $a : \mathbb{N}_0 \to R$, $a(0) = r_0$, $a(1) = r_1$, $a(2) = r_2, \ldots$, označíme jako $r_0X^0 + r_1X^1 + r_2X^2 + \ldots$ (pouze konečný počet r_i je nenulových) s následující konvencí:

(α) místo $0_R X^0 + 0_R X^1 + 0_R X^2 + \ldots$ (všechna r_i nulová) píšeme 0.

(β) místo $r_0 X^0$ budeme psát $r_0 I$

(γ) místo $1_R X^i$ budeme psát X^i

Polynom a můžeme tedy zapsat jako $a \equiv r_0 I + r_1 X^1 + r_2 X^2 + \ldots$ zkráceně $a \equiv \sum_i r_i X^i$.

Nadcházející definice 2.5, 2.6 ,2.8 a věta 2.2 společně s jejím důkazem inspirovány [3]. Důkaz věty 2.1 inspirován [2].

Definice 2.5. (Sčítání a násobení polynomů):

Mějme dva polynomy a, b, kde $a \equiv \sum_i r_i X^i$, $b \equiv \sum_i s_i X^i$, pak

$a + b \equiv \sum_i t_i X^i$, kde $t_i = r_i + s_i$, tedy $a + b \equiv \sum_i (r_i + s_i) X^i$

$a \cdot b \equiv \sum_i t_i X^i$, kde $t_i = \sum_{\substack{k,l \in \mathbb{N}_0 \\ i=k+l}} r_k \cdot s_l$.

pro $a \equiv r_0 I$ budeme psát $a \cdot b = \sum_i r_0 s_i X^i$, pro $\underbrace{b \cdot b \cdot b \cdot \ldots \cdot b}_{i-\text{krát}}$ užijeme označení b^i.

Věta 2.1. Polynomy s operacemi + a $\cdot$ tvoří komutativní okruh. Okruh polynomů v neurčité X nad okruhem R označíme $R[X]$.

Důkaz: v důkazu budeme uvažovat $n = \max\{\deg f,\ \deg g,\ \deg h\}$
$(R, +)$ *je komutativní grupa:*

$$\begin{aligned}
\text{Komutativita: } f + g &= \textstyle\sum_{i=0}^n a_i X^i + \sum_{i=0}^n b_i X^i = \sum_{i=0}^n (a_i + b_i) X^i = \sum_{i=0}^n (a_i + b_i) \\
&= \textstyle\sum_{i=0}^n b_i X^i + \sum_{i=0}^n a_i X^i = g + f.
\end{aligned}$$

$$\begin{aligned}
\text{Asociativita: } f + (g + h) &= \textstyle\sum_{i=0}^n a_i X^i + (\sum_{i=0}^n b_i X^i + \sum_{i=0}^n c_i X^i) \\
&= \textstyle\sum_{i=0}^n a_i X^i + \sum_{i=0}^n (b_i + c_i) X^i = \sum_{i=0}^n (a_i + (b_i + c_i)) X^i \\
&= \textstyle\sum_{i=0}^n ((a_i + b_i) + c_i) X^i = \sum_{i=0}^n (a_i + b_i) X^i + \sum_{i=0}^n c_i X^i \\
&= \textstyle(\sum_{i=0}^n a_i X^i + \sum_{i=0}^n b_i X^i) + \sum_{i=0}^n c_i X^i = (f + g) + h.
\end{aligned}$$

$$\begin{aligned}\text{Neutrální prvek: } f+0 &= \textstyle\sum_{i=0}^{n} a_iX^i + \sum_{i=0}^{n} 0X^i = \sum_{i=0}^{n}(a_i+0)X^i \\ &= \textstyle\sum_{i=0}^{n} a_iX^i = f.\end{aligned}$$

$$\begin{aligned}\text{Inverzní prvek: } f+(-f) &= \textstyle\sum_{i=0}^{n} a_iX^i + \sum_{i=0}^{n}(-a_i)X^i = \sum_{i=0}^{n}(a_i+(-a_i))X^i \\ &= \textstyle\sum_{i=0}^{n} 0_RX^i = 0.\end{aligned}$$

$(R,\cdot)$ je pologrupa s jedničkou:

$$\begin{aligned}\text{Komutativita: } f\cdot g &= (\textstyle\sum_{i=0}^{n} a_iX^i)\cdot(\sum_{j=0}^{n} b_jX^j) = \sum_{l=0}^{2n}(\sum_{i+j=l} a_ib_j)X^l \\ &= \textstyle\sum_{l=0}^{2n}(\sum_{i+j=l} b_ja_i)X^l = g\cdot f.\end{aligned}$$

$$\begin{aligned}\text{Asociativita: } f\cdot(g\cdot h) &= (\textstyle\sum_{i=0}^{n} a_iX^i)\cdot((\sum_{j=0}^{n} b_jX^j)\cdot(\sum_{k=0}^{n} c_kX^k)) \\ &= (\textstyle\sum_{i=0}^{n} a_iX^i)\cdot(\sum_{l=0}^{2n}(\sum_{j+k=l}(b_jc_k))X^l) \\ &= \textstyle\sum_{m=0}^{3n}(\sum_{i+j+k=m} a_i(b_jc_k))X^m \\ &= \textstyle\sum_{m=0}^{3n}(\sum_{i+j+k=m}(a_ib_j)c_k)X^m \\ &= (\textstyle\sum_{q=0}^{2n}(\sum_{q=i+j=m-k}(a_ib_j))X^q)\cdot\sum_{k=0}^{n} c_kX \\ &= ((\textstyle\sum_{i=0}^{n} a_iX^i)\cdot(\sum_{j=0}^{n} b_jX^j))\cdot(\sum_{k=0}^{n} c_kX)\end{aligned}$$

$$\text{Jednička: } f\cdot 1_R = (\textstyle\sum_{i=0}^{n} a_iX^i)\cdot 1_R = \sum_{i=0}^{n} a_iX^i = f.$$

Distributivní zákony:

$$\begin{aligned}f\cdot(g+h) &= (\textstyle\sum_{i=0}^{n} a_iX^i)\cdot(\sum_{j=0}^{n} b_jX^j + \sum_{j=0}^{n} c_jX^j) \\ &= (\textstyle\sum_{i=0}^{n} a_iX^i)\cdot(\sum_{j=0}^{n}(b_j+c_j)X^j) = \sum_{l=0}^{2n}(\sum_{i+j=l} a_i(b_j+c_j))X^l \\ &= \textstyle\sum_{l=0}^{2n}(\sum_{i+j=l}(a_ib_j+a_ic_j))X^l \\ &= \textstyle\sum_{l=0}^{2n}(\sum_{i+j=l} a_ib_j)X^l + \sum_{l=0}^{2n}(\sum_{i+j=l} a_ic_j)X^l \\ &= f\cdot g + f\cdot h.\end{aligned}$$

Obdobně dokážeme pravý distributivní zákon.

□

Věta 2.2. (Substituční princip): Nechť $\varphi : R \to \underline{R}$ je homomorfismus a $\underline{r} \in \underline{R}$. Pak existuje jediný homomorfismus $\Phi_{\underline{r}} : R[X] \to \underline{R}$ takový, že :

(i) $\Phi_{\underline{r}}(X) = \underline{r}$

(ii) $\Phi_{\underline{r}}(rI) = \varphi(r)$ pro všechna $r \in R$

Důkaz: Nechť $a \in R[X]$, $a \equiv \sum_i r_i X^i$. Nejprve ukážeme, že $\Phi_{\underline{r}}$ je jediné. Vezmeme-li $\Phi_{\underline{r}} \equiv \sum_i \varphi(r_i)\underline{r}^i$, pak z $(i), (ii)$ plyne jednoznačnost Φ. Nyní ukážeme, že Φ existuje jako homorfismus.
Mějme

$$\Phi_{\underline{r}}(I) = \Phi_{\underline{r}}(1_R I) = \varphi(1_R)1_{\underline{R}};$$

pro $a \equiv \sum_i r_i X^i, b \equiv \sum_i s_i X^i$ máme

$$\begin{aligned}
\Phi_{\underline{r}}(a+b) &= \Phi_{\underline{r}}\left(\sum_i (r_i+s_i)X^i\right) = \sum_i \varphi(r_i+s_i)\underline{r}^i = \\
&\sum_i \varphi(r_i)\underline{r}^i + \sum_i \varphi(s_i)\underline{r}^i = \Phi_{\underline{r}}\left(\sum_i r_i X^i\right) + \Phi_{\underline{r}}\left(\sum_i s_i X^i\right) = \\
&\Phi_{\underline{r}}(a) + \Phi_{\underline{r}}(b) \\
\Phi_{\underline{r}}(a\cdot b) &= \Phi_{\underline{r}}\left(\sum_{k,l}(r_k+s_l)X^{k+l}\right) = \sum_{k,l}\varphi(r_k\times s_l)\underline{r}^{k+l} = \\
&\sum_{k,l}\varphi(r_k)\underline{r}^k\cdot\varphi(s_l)\underline{r}^l = \sum_k \varphi(r_k)\underline{r}^k \cdot \sum_l \varphi(s_l)\underline{r}^l = \\
&\Phi_{\underline{r}}\left(\sum_k r_k X^k\right)\cdot\Phi_{\underline{r}}\left(\sum_l s_l X^l\right) = \Phi_{\underline{r}}(a)\cdot\Phi_{\underline{r}}(b).
\end{aligned}$$

□

Definice 2.6. Nechť $\underline{R} = Map(R)$ je množina všech zobrazení z R do R s operacemi $+, \cdot$ (snadno ověříme, že jde o okruh), nechť $r = id_R$ je identické zobrazení a nechť φ zobrazí $r \in R$ na příslušné konstantní zobrazení ($f(x) = r$ pro všechna $x \in R$).

Pak $\Phi_{\underline{r}}$ zobrazí polynom na zobrazení, které nazveme *polynomiální*: pro daný polynom $a \in R[X]$, $a = \sum_i r_i X^i$ obdržíme zobrazení: $f_a : R \to R$, kde $f_a(x) = \sum_i r_i x^i$. Polynomiální zobrazení na R (definované pro každý prvek z R) tvoří podokruh $Map(R)$, označme ji $PolMap(R)$.

Zobrazení $ev : R[X] \to PolMap(R)$ definujeme jako $ev(a) = f_a$ a nazveme ho *evaluace* polynomu a.

Označení 2.2. Zobrazení $s : R \to R$ může být bijekcí. Bijekce tvoří grupu vzhledem ke skládání, ale ne okruh vzhledem k operacím $+$ a $\cdot$. (Jednoduchý protipříklad: Mějmě dvě bijektivní zobrazení s_1, s_2 daná předpisem:

$$\begin{array}{ll} s_1 : 0 \mapsto 0 & s_2 : \ 0 \mapsto 1 \\ \quad 1 \mapsto 1 & \quad\ \ 1 \mapsto 0 \end{array}$$

je zřejmé, že jejich součet $s_1 + s_2$ již bijekcí není.) Bijekce z R do RoOznačme $Bij(R)$.

Věta 2.3. Pro $card\ R < \infty$ je $Map(R) = PolMap(R)$.

Důkaz: Mějme konečný okruh R o p prvcích, pak každý předpis zobrazení, lze obdržet proložením interpolačním polynomem řádu nejvýše $p-1$.

□

Poznámka 2.2. Pro *card* $R < \infty$ každá bijekce je permutace.

Definice 2.7. Polynom $a \in R[X]$ takový, že $ev(a)$ je bijekce, nazveme *polynom indukující bijekci*, označíme $a \in \widehat{R[X]}$.

Poznámka 2.3. $\widehat{R[X]}$ značí pouze polynomy indukující bijekci, netvoří okruh. Jednoduchý protipříklad, sečteme-li dva polynomy indukující bijekci lišící se jen o konstantu nebo přímo totožné, obdržíme konstantní zobrazení. $x^2 + x^2 = 0$, pro všechna $x \in R$, kde $R = \mathbb{F}_{2^m}$.

Poznámka 2.4. Nad polem existuje polynom indukující bijekci vždy. Obecně nad okruhem existovat nemusí.

Definice 2.8. (Skládání polynomů): Nechť $\underline{R} = R[X]$ a nechť a, b jsou polynomy jedné neurčité, $\underline{r} = a$ a $\varphi : R \to R[X]$, kde $\underline{r} \to rI$.
Pak definujeme

$$b \circ a = \Phi_a(b),$$

operaci $\circ$ nazýváme *skládání polynomů* a čteme "b po a".

Věta 2.4. Nechť a, b jsou polynomy z okruhu R takové, že $a \in \widehat{R[X]}$ a $b \in \widehat{R[X]}$, pak

$$a \circ b \in \widehat{R[X]}$$

Důkaz: Je zřejmé, že permutace permutace je opět permutací.

□

2.2. Polynomy n neurčitých nad okruhem

Předchozí část nyní zobecníme pro polynom n neurčitých a pro n-tice polynomů n neurčitých. Na úvod si uvedeme další definici speciálního případu okruhu. Kapitola je inspirována [3]

Definice 2.9. Komutativní okruh $(R, +, \cdot)$ s další binární operací označenou $\circ$ nazveme *kompoziční okruh*, pokud splňuje

$$\begin{aligned} (F + G) \circ H &= (F \circ H) + (G \circ H) \\ (F \cdot G) \circ H &= (F \circ H) \cdot (G \circ H) \\ (F \circ G) \circ H &= F \circ (G \circ H) \end{aligned}$$

pro všechna $F, G, H \in R$.

Definice 2.10. Polynom n neurčitých nad okruhem R definujeme jako zobrazení $a : \mathbb{N}_0^n \to R$ s konečným nosičem.

Věta 2.5. Polynomy n neurčitých s operacemi + a $\cdot$ tvoří okruh. Okruh polynomů v neurčité $X_1, \ldots, X_n = \mathbf{X}$ označíme $R[\mathbf{X}]$.

Důkaz: Obdobný jako v případě jedné neurčité.

Sčítání a násobení polynomů n neurčitých zavedeme obdobně jako v případě jedné neurčité.

Definice 2.11. n-tici polynomů n neurčitých nad okruhem R definujeme jako zobrazení $a : \mathbb{N}_0^n \to R^n$ s konečným nosičem.

Věta 2.6. n-tice polynomů n neurčitých s operacemi + a $\cdot$ tvoří okruh. Okruh těchto $n-$tic $(R[\mathbf{X}])^n$ označíme $\mathbf{R}[\mathbf{X}]$. Okruh $R[X] = R[X_1]$ polynomů jedné neurčité je speciální případ $\mathbf{R}[\mathbf{X}]$.

Důkaz: Obdobný jako v případě jedné neurčité.

Označení 2.3. Polynom $a : \mathbb{N}_0^n \to R$, $a(0, \ldots, 0) = r_{0,\ldots,0}$, $a(1, 0, \ldots, 0) = r_{1,0,\ldots,0}$, $\ldots$, $a(0, \ldots, 0, 1) = r_{0,\ldots,0,1}$, $a(2, 0, \ldots, 0) = r_{2,0,\ldots,0}$, $a(1, 1, 0, \ldots, 0) r_{1,1,0,\ldots,0}$, $\ldots$, označíme jako $r_{0,\ldots,0} I + r_{1,0\ldots,0} X_1 + \ldots + r_{0,\ldots,0,1} X_n + r_{2,0,\ldots,0} X_1^2 + r_{1,1,0,\ldots,0} X_1 X_2 + \ldots$ (pouze konečný počet r_α je nenulových) s konvencí obdobnou jako u polynomů jedné neurčité.
Polynom a můžeme tedy zapsat jako $a \equiv r_{0,\ldots,0} I + r_{1,0\ldots,0} X_1 + \ldots + r_{0\ldots,0,1} X_n + r_{2,0\ldots,0} X_1^2 + r_{1,1,0\ldots,0} X_1 X_2 + \ldots$ zkráceně $a \equiv \sum_\alpha r_\alpha X^\alpha$, kde $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}_0^n$.
n-tici polynomů zapíšeme $\boldsymbol{a} = (a_1, \ldots, a_n)$.

Věta 2.7. (Substituční princip): Nechť $\varphi : R \to \underline{R}$ je homomorfismus a $\underline{r}_1, \ldots \underline{r}_n \in \underline{R}$. Pak existuje jediný homomorfismus $\Phi_{\underline{r}_1,\ldots \underline{r}_n} : R[\mathbf{X}] \to \underline{R}$ takový, že :

(i) $\Phi_{\underline{r}_1,\ldots \underline{r}_n}(X_i) = \underline{r}_i$

(ii) $\Phi_{\underline{r}_1,\ldots \underline{r}_n}(rI) = \varphi(r)$ pro všechna $r \in R$

Důkaz: Obdobný jako v případě jedné neurčité.

Definice 2.12. Nechť $\underline{R} = Map(R^n)$ je okruh všech zobrazení z R^n do R^n, $r_i, i = 1, .., n$ je projekcí na i-tou složku a nechť φ zobrazí $r \in R^n$ na příslušné zobrazení ($f(x_1, ..., x_n) = r$ pro všechna $x \in R^n$).
Pak $\Phi_{\underline{r}_{1_\alpha},\ldots \underline{r}_{n_\alpha}}$ zobrazí $n-$tici polynomů na zobrazení, které nazveme *polynomiální zobrazení*: pro danou n-tici polynomů $\boldsymbol{a} = (a_1, ..., a_n) \in \mathbf{R}[\mathbf{X}]$, obdržíme zobrazení

$f_{\boldsymbol{a}} : R^n \to R^n$. Jako v případě jedné neurčité, polynomiální zobrazení tvoří podokruh $Map(R^n)$, budeme jej značit $PolMap(R^n)$.
Zobrazení $ev : \mathbf{R}[\mathbf{X}] \to Map(R^n)$ definujeme jako $ev(\boldsymbol{a}) = f_{\boldsymbol{a}}$ a nazveme jej *evaluace* n-tice polynomů $\boldsymbol{a}$.
Je-li G podgrupa vzhledem ke skládání $\mathbf{R}[\mathbf{X}]$, pak $ev(G)$ značí podgrupu vzhledem ke skládání v $PolMap(R^n)$.

Označení 2.4. $Bij(R^n) \subset Map(R^n)$ je grupa vzhledem ke skládání všech bijekcí $R^n \to R^n$.

Definice 2.13. Nechť $F = (a_1, \ldots, a_n), G = (b_1, \ldots, b_n), a_i, b_i \in R[\mathbf{X}], r_i = a_i, i = 1, \ldots, n$ a $\varphi : R \to R[\mathbf{X}]$, kde $r \to rI$. Pak definujeme

$$G \circ F = (\Phi_{a_1,\ldots,a_n}(b_1), \ldots, \Phi_{a_1,\ldots,a_n}(b_n)),$$

binární operaci $\circ$ nazýváme *skládání n-tic polynomů o n neurčitých*.

Věta 2.8. Okruh $\mathbf{R}[\mathbf{X}]$ je kompoziční okruh.

Důkaz: Ověříme, zda $\mathbf{R}[\mathbf{X}]$ splňuje předpoklady kompozičního okruhu

$$\begin{array}{rcl} \text{Nechť } F & = & (a_1, \cdots, a_n) \equiv (\sum_\alpha r_{1_\alpha}\mathbf{X}^\alpha, \cdots, \sum_\alpha r_{n_\alpha}\mathbf{X}^\alpha), \\ G & = & (b_1, \cdots, b_n) \equiv (\sum_\alpha s_{1_\alpha}\mathbf{X}^\alpha, \cdots, \sum_\alpha s_{n_\alpha}\mathbf{X}^\alpha), \\ H & = & (c_1, \cdots, c_n) \equiv (\sum_\alpha t_{1_\alpha}\mathbf{X}^\alpha, \cdots, \sum_\alpha t_{n_\alpha}\mathbf{X}^\alpha) \end{array}$$

$$\begin{array}{rcl} (F+G)\circ H & = & (a_1+b_1, \cdots, a_n+b_n)\circ H \\ & & = (\sum_\alpha (r_{1_\alpha}+s_{1_\alpha})H^\alpha, \ldots, \sum_\alpha (r_{n_\alpha}+s_{n_\alpha})H^\alpha) \\ & & = (\sum_\alpha r_{1_\alpha}H^\alpha, \ldots, \sum_\alpha r_{n_\alpha}H^\alpha) + (\sum_\alpha s_{1_\alpha}H^\alpha, \ldots, \sum_\alpha s_{n_\alpha}H^\alpha) \\ & & = (F\circ H) + (G\circ H) \end{array}$$

$$\begin{array}{rcl} (F\cdot G)\circ H & = & (\sum_{\beta,\gamma} (r_{1_\beta}\cdots{}_{1_\gamma})H^{\beta+\gamma}, \ldots, \sum_{\beta,\gamma}(r_{n_\beta}\cdots{}_{n_\gamma})H^{\beta+\gamma}) \\ & = & (\sum_\beta r_{1_\beta}H^\beta \cdot \sum_\gamma s_{1_\gamma}H^\gamma, \ldots, \sum_\beta r_{n_\beta}H^\beta \cdot \sum_\gamma s_{n_\gamma}H^\gamma) \\ & = & (F\circ H)\cdot(G\circ H) \end{array}$$

Jak $(F \circ G) \circ H$ tak i výraz $(F \circ G) \circ H$ je roven

$$\left(\sum_\gamma r_{1_\gamma}\left(\sum_\beta s_{1_\beta}\left(\sum_\alpha t_{1_\alpha}\mathbf{X}^\alpha, \ldots, \sum_\alpha t_{n_\alpha}\mathbf{X}^\alpha\right)^\beta, \ldots, \sum_\beta s_{n_\beta}\left(\sum_\alpha t_{1_\alpha}\mathbf{X}^\alpha, \cdots, \sum_\alpha t_{n_\alpha}\mathbf{X}^\alpha\right)^\beta\right)^\gamma,\right.$$
$$\ldots,$$
$$\left.\sum_\gamma r_{n_\gamma}\left(\sum_\beta s_{1_\beta}\left(\sum_\alpha t_{1_\alpha}\mathbf{X}^\alpha, \cdots, \sum_\alpha t_{n_\alpha}\mathbf{X}^\alpha\right)^\beta, \ldots, \sum_\beta s_{n_\beta}\left(\sum_\alpha t_{1_\alpha}\mathbf{X}^\alpha, \ldots, \sum_\alpha t_{n_\alpha}\mathbf{X}^\alpha\right)^\beta\right)^\gamma\right.$$

důkaz asociativity pro technickou náročnost neuvádíme celý.

□

3. Polynomiální automorfismy na konečných polích

V této kapitole si zavedeme polynomiální automorfismy na konečných polích a budeme se zabývat Maubachovou hypotézou, podle které polynomiální bijektivní zobrazení $\mathbb{F}_{2^m}^n \to \mathbb{F}_{2^m}^n$, $n \geq 2$, $m > 1$, představují poze sudé permutace. Veškeré uvedené definice a věty se vztahují pouze ke konečným polím. Definice 3.3 a 3.4 zavedeny dle [4], věta 3.4 a definice 3.5 dle [5].

Definice 3.1. Grupu sudých permutací množiny S nazveme *alternující grupa* a budeme ji značit $Alt(S)$. (Grupa všech permutací se značí $Sym(S)$.)

Definice 3.2. Prostý surjektivní homomorfismus okruhu R do $\underline{R}$ nazveme *izomorfismus*. Homomorfismus okruhu do sebe nazveme *endomorfismus*.
Izomorfní a zároveň endomorfní zobrazení nazýváme *automorfismus* na okruhu R.

Označení 3.1. Označme $\mathrm{Aut}_R R[X]$ množinu automorfismů na $R[X]$.

Věta 3.1. $\mathrm{Aut}_R R[X]$ s operací skládání tvoří grupu.

Důkaz: Asociativitu bychom ověřili přímým výpočtem. Jedničku grupy zde představuje identické zobrazení. Inverzním prvkem je zde inverzní zobrazení.

□

Poznámka 3.1. Automorfismus $\varphi \in \mathrm{Aut}_R R[\mathbf{X}]$ přiřadí každému polynomu n neurčitých jiný polynom n neurčitých. Takový automorfismus je plně popsán následujícím předpisem, kam se zobrazí $1, X_1, X_2, \ldots, X_n$:

$$\begin{aligned} 1 &\longmapsto 1 \\ X_1 &\longmapsto F_1(X_1, \ldots, X_n) \\ &\vdots \\ X_n &\longmapsto F_n(X_1, \ldots, X_n) \end{aligned}$$

Definice 3.3. *Afinní automorfismus* $F \in \mathrm{Aut}_R R[X]$ je automorfismus ve tvaru

$$\begin{aligned} 1 &\longmapsto 1 \\ X_1 &\longmapsto F_1(X_1, \ldots, X_n) \\ X_2 &\longmapsto F_2(X_1, \ldots, X_n) \\ &\vdots \\ X_n &\longmapsto F_n(X_1, \ldots, X_n) \end{aligned}$$

kde $deg F_i = 1$, pro všechna $i = 1, 2 \ldots n$.

Věta 3.2. Afinní automorfismy tvoří grupu vzhledem ke skládání. Označíme ji $\mathrm{Aff}(R, n) \subseteq \mathrm{Aut}_R R[\mathbf{X}]$

Důkaz: Je zřejmé, že skládáním polynomů prvního stupně dostaneme opět polynom prvního stupně. Identický automorfismus je prvkem $\mathrm{Aff}(R,n)$, složky inverzního automorfismu jsou opět polynomy prvního stupně.

□

Definice 3.4. *De Jonquièrův automorfismus* $F \subseteq \mathrm{Aut}_R R[\mathbf{X}]$ je automorfismus tvaru

$$\begin{array}{rcl} 1 & \longmapsto & 1 \\ X_1 & \longmapsto & a_1X_1 + f_1(X_2,\ldots,X_n) \\ X_2 & \longmapsto & a_2X_2 + f_2(X_3,\ldots,X_n) \\ & \vdots & \\ X_n & \longmapsto & a_nX_n + f_n \end{array}$$

kde $a_i \in R$ je jednotka (tedy i $a^{-1} \in R$), $f_i \in R[X_{i+1},...,X_n]$ pro všechna $1 \leq i \leq n-1$ a $f_n \in R$.

Věta 3.3. De Jonquièrův automorfismus tvoří grupu vzhledem ke skládání. Budeme značit $\mathrm{J}(R,n) \subseteq \mathrm{Aut}_R R[X]$.

Důkaz: Je zřejmé, že ani v tomto případě operace skladání vlastnosti grupy nenaruší. Identické zobrazení je opět prvkem $\mathrm{J}(R,n)$, inverzní zobrazení obdržíme téhož tvaru. Postup skládání v tomto případě můžeme prezentovat podobností s Gaussovou eliminační metodou. Jde o eliminaci tvaru De Jonquièrova automorfismu, kde vhodnou úpravou lze vyjádřit jednotlivé elementy pravé strany. Po této úpravě dostane opět tvar De Jonquièrova automorfismu.

□

Definice 3.5. *Grupa krotkých automorfismů* $\mathrm{T}(R,n) \subseteq \mathrm{Aut}_R R[X]$ je generována $\mathrm{J}(R,n)$ a $\mathrm{Aff}(R,n)$, tzn.

$$\mathrm{T}(R,n) = \langle \mathrm{Aff}(R,n), \mathrm{J}(R,n) \rangle$$

tzn. každý krotký automorfismus získáme složením afinních a de Jonquièrových automorfismů.

Definice 3.6. Automorfismus, který není krotký, nazýváme *divoký automorfismus.*

Věta 3.4. Nechť $\mathbb{F}_{p^m}$ je konečné pole. Pak

(*i*) $card\ ev(\mathrm{T}(\mathbb{F}_{p^m},1)) = card\ Bij(\mathbb{F}_{p^m})/(p^m-2)!$,

pro $\mathbb{F}_2$,$\mathbb{F}_3$ máme $ev(\mathrm{T}(\mathbb{F}_{p^m},1)) = Bij(\mathbb{F}_{p^m})$

(*ii*) $ev(\mathrm{T}(\mathbb{F}_{p^m},n)) = Bij(\mathbb{F}_{p^m}^n)$

pro $n \geq 2$,kde $p \neq 2$ nebo $p = 2$, $m = 1$

(*iii*) $card\ ev(\mathrm{T}(\mathbb{F}_{p^m}, n)) = card\ Bij(\mathbb{F}_{p^m}^n)/2$

pro $n \geq 2$,kde $p = 2$, $m \geq 2$

zejména $ev(\mathrm{T}(\mathbb{F}_{p^m}, n)) = Alt(\mathbb{F}_{p^m}^n)$.

Hypotéza: Nechť $\mathbb{F}_{p^m}$ je konečné pole a n je kladné celé číslo, pak platí

$$ev(\mathrm{Aut}_{\mathbb{F}_{p^m}}\mathbb{F}_{p^m}[\mathbf{X}]) = ev(T(\mathbb{F}_{p^m}, n)).$$

Tedy neexistuje polynomiální automorfismus, který indukuje lichou bijekci. [5]

Poznámka 3.2. Pokud by existoval, musí být nutně divoký.

4. Experimentální analýza kvadratických polynomů na binárních polích

Tato kapitola obsahuje závěry v podobě vět, získaných na základě výstupů z programů v systému Mathematica na ověření bijekce kvadratických polynomů a n-tic kvadratických polynomů nad konečným polem $\mathbb{F}_{2^m}$. Rozebíráme zde hlavně bijekci $\mathbb{F}_{2^m}^n \to \mathbb{F}_{2^m}^n$ a za jakých podmínek nastane. Zejména nás zajímají podmínky nutné a postačující.
Řešíme pro $1 \leq n \leq 3$ a pro malá m, vyjímaje případ $n = 1$, zde řešíme obecně pro všechna m.

Označení 4.1. Množinu dvojic kvadratických polynomů dvou neurčitých nad binárním polem $\mathbb{F}_{2^m}$ označíme $(\overset{2}{\mathbb{F}}_{2^m}[X, Y])^2$

4.1. Kvadratické polynomy jedné neurčité nad konečným polem $\mathbb{F}_{2^m}$

Tedy řešíme situaci pro $n = 1$. Analyzovali jsme pole pro $1 \leq m \leq 5$. Kvadratický polynom má tvar $ax^2 + bx + c$, kde $a \neq 0$.

Pro vypsání bijektivních polynomů jedné neurčité nad polem $\mathbb{F}_{2^m}$ jsme použili následujícího jednoduchého programu. Pole K zadáváme pomocí jeho redukčního polynomu, v našem případě pro pole $\mathbb{F}_{2^5}[X]$ zadané $K = GF[2, 1, 0, 0, 1, 0, 1]$ je redukční polynom tvaru $x^5 + x^2 + 1$, číslo 2 znamená použití binarní aritmetiky. Symbol $k[\ ]$ označuje prvky pole. Nejprve si vygenerujeme všechny možné kombinace tvaru kvadratického polynomu. Do daných rovnic dosadíme prvky pole K a hodnotu zobrazení si necháme vypsat v množinovém tvaru, u kterého určíme jeho délku. Pokud se délka shoduje s celkovým počtem prvků pole, necháme jej vypsat.

Obr 4.1 ukázka programu na vygenerování bijektivních polynomů nad polem $\mathbb{F}_{2^5}$

Wolfram Mathematica | FOR STUDENTS Demonstrations | MathWorld | Student Forum

```
<< FiniteFields`FiniteFields`
K = GF[2, {1, 0, 0, 1, 0, 1}]
SetFieldFormat[K, FormatType → FunctionOfCode[k]]


n = 32;(* pocet prvku pole K*)


aa = Table[k[a] * x^2 + k[b] * x + k[c], {a, 1, n - 1},
  {b, 0, n - 1}, {c, 0, n - 1}];
(*zadani obecneho predpisu pro kvadraticky polynom*)
(*generovani vsech kvadratickych polynomu*)
For[i = 1, i < n, i++,
     For[j = 1, j < n + 1, j++,
        For[l = 1, l < n + 1, l++,
               B = aa[[i]][[j]][[l]];

          (*dosazeni prvku pole K do predpisu polynomu*)
                bb = B /. x → Table[k[l], {l, 0, n - 1}];

          (*vypsani hodnot zobrazeni mnozinove*)
                bbb = Union [bb];

    If[Length[bbb] == n, Print [B]]
    (*porovnani poctu pvrku hodnot zobrazeni s poctem
     prvku pole K*)
  ]
 ]
]
```

Obr 4.2 ukázka výstupu polynomů indukujících bijekci nad polem $\mathbb{F}_{2^5}$

```
x^2 k[1]
k[1] + x^2 k[1]
k[2] + x^2 k[1]
x^2 k[1] + k[3]
k[4] + x^2 k[1]
x^2 k[1] + k[5]
k[6] + x^2 k[1]
x^2 k[1] + k[7]
k[8] + x^2 k[1]
x^2 k[1] + k[9]
k[10] + x^2 k[1]
x^2 k[1] + k[11]
...
```

Na základě výstupů jsme zformulovali větu:

Věta 4.1. Nechť $P \in \mathbb{F}_{2^m}[X]$, $P = ax^2 + bx + c$, kde $a, b, c \in \mathbb{F}_{2^m}$, $a \neq 0$.
Pak $P \in \widehat{\mathbb{F}_{2^m}[X]} \Leftrightarrow b = 0$.

Důkaz:
" $\Leftarrow$ " Předpokládejme $b = 0$, tedy $P = ax^2 + c$. Koeficient c představuje posunutí zobrazení, tedy bez újmy na obecnosti položme $c = 0$. Nechť $D, Q \in \mathbb{F}_{2^m}$, $D = x_1^2$, $Q = x_2^2$, $P = Q \circ D$. Tedy stačí dokázat, že $x^2 \in \widehat{\mathbb{F}_{2^m}[X]}$.

Předpokládejme, že $x^2 = (x + d)^2$. Pak

$$\begin{aligned} x^2 &= x^2 + d^2 \\ 0 &= d^2 \\ 0 &= d \end{aligned}$$

$\Rightarrow$ P indukuje bijekci.

" $\Rightarrow$ " Dokážeme nepřímo. Předpokládejme, že $b \neq 0$ bez újmy na obecnosti uvažujme $P = x^2 + bx$, pak $\exists d$ takové, že $(x + c)(x + c + b) = x(x + b)$, pak pro $\forall b\ \exists c$ takové, že $c^2 + cb = 0$. Pro $b = c$ je rovnost splněna $\Rightarrow$ P neindukuje bijekci.

□

4.2. Dvojice kvadratických polynomů dvou neurčitých nad konečným polem $\mathbb{F}_{2^m}$

Tedy řešíme případ $n = 2$ pro $1 \leq m \leq 2$. Kvadratický polynom má tvar $ax^2 + bxy + cy^2 + dx + ey + f$, kde $a \neq 0$ nebo $b \neq 0$ nebo $c \neq 0$ a kde $a, b, c, d, e, f \in \mathbb{F}_{2^m}$.

V tomto případě je konstrukce programu náročnější a celková doba výpočtu výrazně delší než v předchozím případě. Pole K zadefinujeme obvyklým způsobem. Opět generujeme množinu všech možných polynomů, které je možné sestrojit daným předpisem. V dalším kroku ověřujeme, zda daný polynom je kvadratický, pokud ano, dosadíme do předpisu prvky pole K. Aby polynom mohl tvořit s jiným polynomem „bijektivní pár“, musí mít počet všech prvků zobrazení stejný a taktéž musí obsahovat všechny možné prvky. K tomu nám slouží porovnávací prvek - *Ress*, s kterým je každý polynom, tedy jeho hodnoty zobrazení, porovnávány. *Ress* je generován zvlášť, mimo hlavní program. Pokud polynom vyhovuje této podmínce, je přiřazen do předchystaného pole, čímž každý polynom dostává i své pořadové číslo. V dalším kroku polynomy „párujeme“ a následně jako v případě jedné neurčité, dosazujeme prvky pole K do vytvořených dvojic. Výsledky necháváme vypsat množinově a porovnáváme s potřebnou délkou pro bijekci n^2. Dvojice polynomů, které vyhovují této podmínce, necháváme vypsat.

Obr 4.3 ukázka programu na vygenerování dvojic polynomů nad polem $\mathbb{F}_{2^2}$

Wolfram Mathematica | FOR STUDENTS — Demonstrations | MathWorld | Student Forum

```
<< FiniteFields`FiniteFields`
K = GF[2, {1, 1, 1}];
SetFieldFormat[K, FormatType → FunctionOfCode[k]]
n = 4;   (*pocet prvku pole K*)
Timing[
 (*vytvoreni sesti-indexoveho pole polynomu,
 indexovano po koeficientech*)
 pp = Table[k[a] * x^2 + k[b] * y^2 + x * y * k[c] + k[d] * x + k[e] * y + k[f],
   {a, 0, n - 1}, {b, 0, n - 1}, {c, 0, n - 1}, {d, 0, n - 1}, {e, 0, n - 1},
   {f, 0, n - 1}];

 (*kontrolni prvek*)
 Ress = {0, 0, 0, 0, k[2], k[2], k[2], k[2], k[1], k[1], k[1], k[1],
   k[3], k[3], k[3], k[3]};
 (*prevedeni pp na 1-indexove pole polynomu, indexovano po polynomech*)
 Ast = Flatten[pp, 6];

 P = {};  (*predchystane pole*)
 pocet = 0;
 (*prochazeni polynomu*)
 For[i = 1, i < Length[Ast] + 1, i++,

   (*vylouceni nekvadratickych polynomu*)
   If[Not[Exponent[Ast[[i]], x] == 2 || Exponent[Ast[[i]], y] == 2 ||
      Exponent[Ast[i], x * y] == 1], Continue[]];

   (*dosazeni prvku pole K do predpisu kvadratickeho polynomu*)
   L = {Ast[[i]]} /. Table[Table[{x → k[s], y → k[t]}, {s, 0, n - 1}],
      {t, 0, n - 1}];

   (*kontrola predpokladu k bijekci - porovnani s kontrolnim prvkem*)
   If[Sort[Flatten[L]] == Ress, AppendTo[P, Ast[[i]]];]
  ]
  Print[Length[P]]; (*pocet polynomu podobne kontrolnimu prvku*)

 (*vytvoreni pole dvojic polynomu*)
 For[i = 1, i < Length[P] + 1, i++,|
    For[j = 1, j < Length[P] + 1, j++,
     (*dosazeni prvku pole K do dvou-indexoveho pole =
      do dvojice polynomu, indexovano po polynomech*)
     A = {P[[i]], P[[j]]} /. Table[Table[{x → k[s], y → k[t]}, {s, 0, n - 1}],
        {t, 0, n - 1}];
     Seskupeni = Flatten[A, 1]; (*prevedeni na jedno-indexove pole,
     idexovano po jednotlivych polynomech*)
     Mnozinove = Union[Seskupeni];
     (*hodnoty zobrazeni budou brany mnozinove*)

     (*porovnani delky zobrazeni s delkou bijektivniho zobrazeni*)
     If[Length[Mnozinove] == n^2, pocet++;
      Print[{P[[i]], P[[j]], {i, j}}]] ;
    ]
   ]
   Print[pocet](*celkovy pocet dvojic*)
]
```

Výstup z programu dostaneme ve formě vypsání dvojice polynomů a jejich číselnou pořadovou reprezentaci. Tento výstup si upravíme a následně přenesem do textového souboru. Výstup obdržíme ve formě: pořadové číslo polynomu, daný polynom, ke kterému jsou vypsána pouze pořadové čísla polynomů - zkráceně ve formě intervalů, s kterými

tvoří dohromady „bijektivní pár“. V textovém souboru provádíme i následnou celkovou analýzu.

Obr 4.4 ukázka části výstupu v textovém souboru, první sloupec je pořadové číslo polynomů, další sloupec je vypsané dané polynomy, dále intervaly polynomů vhodných k „ párování“ nad polem $\mathbb{F}_{2^2}$

```
1       'y^2*k[1]'      :5-52,57-104,109-172,209-224,261-276,313-328,365-380,417-432,469-.......
2       'k[1]+y^2*k[1]' :5-52,57-104,109-172,209-224,261-276,313-328,365-380,417-432,469-.......
3       'k[2]+y^2*k[1]' :5-52,57-104,109-172,209-224,261-276,313-328,365-380,417-432,469-.......
4       'y^2*k[1]+k[3]' :5-52,57-104,109-172,209-224,261-276,313-328,365-380,417-432,469-.......
5       'x*k[1]+y^2*k[1]'       :1-4,9-24,37-40,53-60,77-92,105-112,125-128,145-160,165-........
6       'k[1]+x*k[1]+y^2*k[1]'  :1-4,9-24,37-40,53-60,77-92,105-112,125-128,145-160,165-........
7       'k[2]+x*k[1]+y^2*k[1]'  :1-4,9-24,37-40,53-60,77-92,105-112,125-128,145-160,165-........
8       'x*k[1]+y^2*k[1]+k[3]'  :1-4,9-24,37-40,53-60,77-92,105-112,125-128,145-160,165-........
9       'x*k[1]+y*k[1]+y^2*k[1]'        :1-8,13-20,29-32,49-56,61-64,73-80,85-88,101-108,113-...
10      'k[1]+x*k[1]+y*k[1]+y^2*k[1]'   :1-8,13-20,29-32,49-56,61-64,73-80,85-88,101-108,113-...
11      'k[2]+x*k[1]+y*k[1]+y^2*k[1]'   :1-8,13-20,29-32,49-56,61-64,73-80,85-88,101-108,113-...
12      'x*k[1]+y*k[1]+y^2*k[1]+k[3]'   :1-8,13-20,29-32,49-56,61-64,73-80,85-88,101-108,113-...
13      'y*k[2]+x*k[1]+y^2*k[1]'        :1-12,17-20,33-36,41-44,53-56,65-68,73-84,93-96,105-....
14      'y*k[2]+k[1]+x*k[1]+y^2*k[1]'   :1-12,17-20,33-36,41-44,53-56,65-68,73-84,93-96,105-....
15      'k[2]+y*k[2]+x*k[1]+y^2*k[1]'   :1-12,17-20,33-36,41-44,53-56,65-68,73-84,93-96,105-....
16      'y*k[2]+x*k[1]+y^2*k[1]+k[3]'   :1-12,17-20,33-36,41-44,53-56,65-68,73-84,93-96,105-....
17      'x*k[1]+y^2*k[1]+y*k[3]'        :1-16,25-28,45-48,53-56,69-76,81-88,97-100,105-108,121-.
18      'k[1]+x*k[1]+y^2*k[1]+y*k[3]'   :1-16,25-28,45-48,53-56,69-76,81-88,97-100,105-108,121-.
19      'k[2]+x*k[1]+y^2*k[1]+y*k[3]'   :1-16,25-28,45-48,53-56,69-76,81-88,97-100,105-108,121-.
20      'x*k[1]+y^2*k[1]+k[3]+y*k[3]'   :1-16,25-28,45-48,53-56,69-76,81-88,97-100,105-108,121-.
21      'x*k[2]+y^2*k[1]'       :1-8,25-40,53-60,73-76,93-108,113-128,141-144,157-164,169-......
22      'x*k[2]+k[1]+y^2*k[1]'  :1-8,25-40,53-60,73-76,93-108,113-128,141-144,157-164,169-......
23      'k[2]+x*k[2]+y^2*k[1]'  :1-8,25-40,53-60,73-76,93-108,113-128,141-144,157-164,169-......
24      'x*k[2]+y^2*k[1]+k[3]'  :1-8,25-40,53-60,73-76,93-108,113-128,141-144,157-164,169-......
25      'x*k[2]+y*k[1]+y^2*k[1]'        :1-4,17-24,29-36,45-48,53-56,69-72,77-80,89-96,101-.....
26      'x*k[2]+k[1]+y*k[1]+y^2*k[1]'   :1-4,17-24,29-36,45-48,53-56,69-72,77-80,89-96,101-.....
27      'k[2]+x*k[2]+y*k[1]+y^2*k[1]'   :1-4,17-24,29-36,45-48,53-56,69-72,77-80,89-96,101-.....
28      'x*k[2]+y*k[1]+y^2*k[1]+k[3]'   :1-4,17-24,29-36,45-48,53-56,69-72,77-80,89-96,101-.....
29      'x*k[2]+y*k[2]+y^2*k[1]'        :1-4,9-12,21-28,33-36,49-56,61-64,81-84,89-100,105-.....
30      'x*k[2]+y*k[2]+k[1]+y^2*k[1]'   :1-4,9-12,21-28,33-36,49-56,61-64,81-84,89-100,105-.....
31      'k[2]+x*k[2]+y*k[2]+y^2*k[1]'   :1-4,9-12,21-28,33-36,49-56,61-64,81-84,89-100,105-.....
32      'x*k[2]+y*k[2]+y^2*k[1]+k[3]'   :1-4,9-12,21-28,33-36,49-56,61-64,81-84,89-100,105-.....
33      'x*k[2]+y^2*k[1]+y*k[3]'        :1-4,13-16,21-32,41-44,53-56,65-68,85-92,97-116,121-....
34      'x*k[2]+k[1]+y^2*k[1]+y*k[3]'   :1-4,13-16,21-32,41-44,53-56,65-68,85-92,97-116,121-....
35      'k[2]+x*k[2]+y^2*k[1]+y*k[3]'   :1-4,13-16,21-32,41-44,53-56,65-68,85-92,97-116,121-....
36      'x*k[2]+y^2*k[1]+k[3]+y*k[3]'   :1-4,13-16,21-32,41-44,53-56,65-68,85-92,97-116,121-....
```

Na základě výstupů jsme pro $m = 2$ zformulovali věty:

Věta 4.2. (První nutná podmínka pro jednotlivé polynomy dvojice)

Nechť $(P, Q) \in (\overset{2}{\mathbb{F}}_{2^m}[X, Y])^2$. Pak nutnou podmínkou $(P, Q) \in (\overset{2}{\mathbb{F}}_{2^m}[X, Y])^2$, pro polynom $P = ax^2 + bxy + cy^2 + dx + ey + f$ je $b = 0$. (Analogicky platí pro Q).

Důkaz: Uvažujme všechny součiny $x \cdot y$ prvků $x, y \in \mathbb{F}_{2^m}$. Jako hodnoty zobrazení obdržíme $2m - 1$ nul, $m - 1$ prvků označených 1, $m - 1$ prvků označených 2,... Je zřejmé, že počet nul je odlišný od zbytku prvků zobrazení, přičtením tedy nedostaneme bijekci.

□

Věta 4.3. (Druhá nutná podmínka pro jednotlivé polynomy dvojice)

Nechť $(P, Q) \in (\overset{2}{\mathbb{F}}_{2^m}[X, Y])^2$. Pak nutnou podmínkou $(P, Q) \in (\overset{2}{\mathbb{F}}_{2^m}[X, Y])^2$, pro polynom $P = ax^2 + cy^2 + dx + ey + f$ je:

$$\text{jestliže } c = 0,\ e = 0 \text{ pak } d = 0,$$

podobně:

$$\text{jestliže } a = 0,\ d = 0 \text{ pak } e = 0.$$

(Analogicky platí pro Q).

Důkaz: Bez újmy na obecnosti můžeme vzít $f = 0$. Stačí tedy dokázat, že $ax^2 + dx$ nebo $cy^2 + ey$ nemá předpoklady k bijekci. Zde můžeme použít modifikaci důkazu věty 3.1.

□

Věta 4.4. (Třetí nutná podmínka pro jednotlivé polynomy dvojice)

Nechť $(P, Q) \in (\overset{2}{\mathbb{F}}_{2^m}[X, Y])^2$. Pak nutnou podmínkou $(P, Q) \in \widehat{(\overset{2}{\mathbb{F}}_{2^m}[X, Y])^2}$, pro polynom $P = ax^2 + cy^2 + dx + ey + f$, kde $a \neq 0$, $c \neq 0$, $d \neq 0$, $e \neq 0$, je:

$$\text{jestliže } a = c \text{ pak } d \neq e.$$

(Analogicky platí pro Q).

Důkaz: Vezměme $P = P_1 + P_2$, kde $P_1 = ax^2 + bx$, $P_2 = ay^2 + by$. Hodnoty zobrazení obou polynomů P_1, P_2 jsou množinově je stejné dvojice čísel. Je zřejmé, že po jejich sečtení nedostaneme bijekci.

□

Věta 4.5. (První nutná podmínka pro dvojici polynomů)

Nechť $(P, Q) \in \widehat{(\overset{2}{\mathbb{F}}_{2^m}[X, Y])^2}$. Pak nutnou podmínkou pro dvojici polynomů, aby $(P, Q) \in (\overset{2}{\mathbb{F}}_{2^m}[X, Y])^2$ je $P \neq Q + k$, kde $k \in \mathbb{F}_{2^m}^2$.

Důkaz: Pro konkrétní (x, y) mějme $P(x, y) = u$, pak $Q(x, y) = k + u = v$. Dvojice (u, v) tedy leží v obrazu zobrazení (P, Q), ale dvojice (u, w), kde $w \neq v$ tam již ležet nemůže. Nejde tedy o surjekci.

□

Věta 4.6. (Druhá nutná podmínka pro dvojici polynomů)

Nechť $(P, Q) \in \widehat{(\overset{2}{\mathbb{F}}_{2^m}[X, Y])^2}$. Pak nutnou podmínkou pro dvojici polynomů, aby $(P, Q) \in (\overset{2}{\mathbb{F}}_{2^m}[X, Y])^2$ je $P \neq Q \cdot k$, kde $k \in \mathbb{F}_{2^m}^2$.

Důkaz: Mějme pro konkrétní (x, y) $P(x, y) = u$, pak $Q(x, y) = k \cdot u = v$. Dvojice (u, v) tedy leží v obrazu zobrazení (P, Q), ale dvojice (u, w), kde $w \neq v$ tam již ležet nemůže. Nejde tedy o surjekci.

□

Věta 4.7. (Zachování bijekce při přičtení konstanty)

Nechť $(P, Q) \in (\overset{2}{\mathbb{F}}_{2^m}[X, Y])^2$. Pokud $(P, Q) \in \widehat{(\overset{2}{\mathbb{F}}_{2^m}[X, Y])^2}$ pak i $(k_1 + P, k_2 + Q) \in \widehat{(\mathbb{F}_{2^m}[X, Y])^2}$, kde $k_1, k_1 \in \mathbb{F}_{2^m}^2$.

Důkaz: Mějme hodnoty zobrazení dvojice (P, Q). Uspořádejme tyto hodnoty dle první souřadnice, dostaneme tedy pro každou první souřadnici množinu všech možných prvků. Názorně ukažme na dvojici polynomů $(P, Q) \in (\overset{2}{\mathbb{F}}_{2^2}\ [X, Y])^2$.

$$\begin{array}{cccc} 0 \mapsto 0 & 1 \mapsto 0 & 2 \mapsto 0 & 3 \mapsto 0 \\ 0 \mapsto 1 & 1 \mapsto 1 & 2 \mapsto 1 & 3 \mapsto 1 \\ 0 \mapsto 2 & 1 \mapsto 2 & 2 \mapsto 2 & 3 \mapsto 2 \\ 0 \mapsto 3 & 1 \mapsto 3 & 2 \mapsto 3 & 3 \mapsto 3 \end{array}$$

Následně přičteme-li k hodnotám dané konstanty, dojde pouze k permutaci původních hodnot. Zvolme pro názornost $k_1 = 1$, $k_2 = 2$, kde 2 je prvek pole označovám symbolem 2, podobně 1 je prvek pole označován symbolem 1.

$$\begin{array}{cccc} 1 \mapsto 2 & 0 \mapsto 2 & 3 \mapsto 2 & 2 \mapsto 2 \\ 1 \mapsto 3 & 0 \mapsto 3 & 3 \mapsto 3 & 2 \mapsto 3 \\ 1 \mapsto 0 & 0 \mapsto 0 & 3 \mapsto 0 & 2 \mapsto 0 \\ 1 \mapsto 1 & 0 \mapsto 1 & 3 \mapsto 1 & 2 \mapsto 1 \end{array}$$

Bijekce je tedy zachována.

□

Věta 4.8. (Zachování bijekce při vynásobení konstantou)
Nechť $(P, Q) \in (\mathbb{F}_{2^m}[X, Y])^2$. Pokud $(P, Q) \in (\overset{2}{\mathbb{F}}_{2^m}\ [X, Y])^2$
pak i $(k_1 \cdot P, k_2 \cdot Q) \in (\overset{2}{\mathbb{F}}_{2^m}\ [X, Y])^2$, kde $k_1, k_2 \neq 0$, $k_1, k_1 \in \mathbb{F}_{2^m}^2$.

Důkaz: Obdobný jako pro pravidla přičítání konstanty. Mějme hodnoty zobrazení (P, Q). Uspořádejme tyto hodnoty dle první souřadnice, dostaneme tedy pro každou první souřadnici množinu všech možných prvků. Následně vynásobíme danými konstantami, dostaneme pro každou skupinku hodnot permutaci puvodnich hodnot. Bijekce je tedy zachována.

□

Podrobnou analýzu jsme provedli pro pole $\mathbb{F}_{2^2}$, kde jsme pro jeho velikost mohli uvést všechny předpoklady pro tvorbu „bijektivního páru“. Pro toto pole uvedeme jeho specifické vlastnosti, které již pro vyšší stupeň $m < 2$ obecně neplatí, pro prvkový rozsah se nám nepodaří jej plně uplatnit pro stupeň nižší, tedy $m = 1$. K nadcházejícím větám nebudou uvedeny důkazy, jejich provedení je přímým výpočtem.

Věta 4.9. (Pravidla symetrie)
Nechť $(P(X, Y), Q) \in (\overset{2}{\mathbb{F}}_{2^2}\ [X, Y])^2$, kde $P(X, Y) = ax^2 + cy^2 + dx + \overbrace{ey + f}$, kde $a \neq 0$, $c \neq 0$, $d \neq 0$, $\overbrace{e \neq 0}$, $a \neq c \wedge d \neq e$. Pokud $(P(X, Y), Q) \in (\overset{2}{\mathbb{F}}_{2^m}\ [X, Y])^2$ pak i $(P(Y, X), Q) \in (\overset{2}{\mathbb{F}}_{2^m}\ [X, Y])^2$, kde $P(Y, X) = ay^2 + cx^2 + dy + ex + f$.

Poznámka 4.1. Jedná se skládání a speciální volbu náhrady v jednom polynomu z dvojice. Mějmě dvojici kvadratických polynomů (P, Q) indukující bijekci a dvojici polynomů (S, T) indukující bijekci. Pro volbu $S = Y$, $T = X$ obdržíme složením $(P(S, T), Q)$ jinou formulaci předcházející věty o symetrii. Obecně tato věta neplatí. Za předpokladu platnosti podmíněnosti polynomu je dále rozhodující volba polynomů S a T - musejí zachovávat kvadratičnost a nenarušit bijekci.
Obecně můžeme předpokládat pro volbu $S = X + k_1$, $T = Y + k_2$, kde k je prvkem pole, nenarušení ani jednoho z předpokladů. Tímto složením získáme jinak modifikovanou větu: Zachování bijekce při přičtení konstanty.
Otázkou zůstává jaká jiná volba dvojice S a T by byla vhodná.

Věta 4.10. Nechť $(P, Q) \in (\overset{2}{\mathbb{F}}_{2^m}[X, Y])^2$, kde $P = a_1x^2+d_1x+e_1y$ a $Q = a_2x^2+\overbrace{d_2x+e_2y}$, $a \neq 0$, pak za předpokladu platnosti všech nutných podmínek $(P, Q) \in (\overset{2}{\mathbb{F}}_{2^m}[X, Y])^2$, jestliže

(i) $d_1 = e_1 = 0 \wedge e_2 \neq 0$
př: $(P, Q) = (x^2, x^2 + 2x + 2y)$

(ii) $d_1 = d_2 = 0 \wedge a_1 = k \cdot a_2 \wedge e_1 \neq k \cdot e_2$
př: $(P, Q) = (x^2 + 3y, x^2 + 2y)$

(iii) $d_1 = e_1 \wedge d_2 = e_2$
př: $(P, Q) = (x^2 + x + y, x^2 + 2y + 2x)$

(iv) $a_1 = k \cdot a_2 \wedge e_1 = k \cdot e_2 \wedge d_1 \neq k \cdot d_2$, kde $e_1 \neq 0$
př: $(P, Q) = (x^2 + 2y + 2x, x^2 + 2y + 3x)$

(v) $a_1 = k \cdot a_2 \wedge e_1 = k \cdot d_2 \wedge d_1 \neq k \cdot d_2 \neq e_1$
př: $(P, Q) = (x^2 + 2y + x, x^2 + 3y + 2x)$

(Analogicky pro $P = a_1y^2 + d_1y + e_1x$ a $Q = a_2y^2 + d_2y + e_2x$)

Věta 4.11. Nechť $(P, Q) \in (\overset{2}{\mathbb{F}}_{2^m}[X, Y])^2$, kde $P = ax^2+d_1x+e_1y$ a $Q = cy^2+d_2x+e_2y$, kde $a \neq 0$, $\overbrace{c \neq 0}$, $a = k \cdot c$, pak za předpokladu platnosti všech nutných podmínek $(P, Q) \in (\overset{2}{\mathbb{F}}_{2^m}[X, Y])^2$, jestliže

(i) $(d_1 = e_1 = e_2 = 0 \vee d_2 = e_2 = d_1 = 0$
př: $(P, Q) = (x^2, y^2 + x)$

(ii) $d_1 = e_2 = 0 \wedge e_1 \neq k \cdot d_2$
př: $(P, Q) = (x^2 + 3y, y^2 + 2x)$

(iii) $e_2 = 0 \wedge e_1 = k \cdot d_2$
př: $(P, Q) = (x^2 + x + 2y, y^2 + 2x)$

(iv) pro $a = k \cdot c$, $e_1 \neq 0 \wedge e_2 \neq 0 \wedge d_1 \neq 0 \wedge d_2 \neq 0$ platí:

- (α) $d_1 = e_1 = k \cdot d_2 = k \cdot e_2$
  př: $(P, Q) = (x^2 + 2x + 2y, y^2 + 2x + 2y)$

(β) $d_1 = e_1 \neq k \cdot d_2 \wedge e_2 \neq d_2$
přː $(P, Q) = (x^2 + x + y, y^2 + 3x + 2y)$

(γ) $d_1 \neq e_1 \wedge d_2 = e_2 \wedge e_1 \neq k \cdot e_2$
přː $(P, Q) = (x^2 + x + 2y, y^2 + x + y)$

(δ) $e_1 = k \cdot e_2 \wedge d_1 \neq k \cdot d_2 \wedge d_2 \neq e_2$
přː $(P, Q) = (x^2 + 3x + y, y^2 + 2x + y)$

(ϵ) $d_1 = k \cdot d_2 \wedge e_1 \neq k \cdot e_2 \wedge d_1 \neq e_1$
přː $(P, Q) = (x^2 + 2x + 3y, y^2 + 2x + y)$

(ζ) $e_1 = k \cdot d_2 \wedge (d_1 \neq k \cdot e_2 \wedge e_2 \neq d_2$ nebo $d_1 = k \cdot e_2 \wedge d_2 = e_2)$
přː $(P, Q) = (x^2 + 3x + y, y^2 + x + 2y)$

(Analogicky pro $P = ay^2 + d_1y + e_1x$ a $Q = cx^2 + d_2y + e_2x$)

Věta 4.12. Nechť $(P, Q) \in (\overset{2}{\mathbb{F}}_{2^m}[X, Y])^2$, kde $P = a_1x^2 + e_1y$ a $Q = a_2x^2 + cy^2 + d_2x + e_2y$,kde $a_1 \neq 0$, $a_2 \neq 0$, $a_1 = k \cdot a_2$, $c \neq 0$, $d_2 \neq 0 \vee e_2 \neq 0$ pak za předpokladu platnosti všech nutných podmínek $(P, Q) \in (\overset{2}{\mathbb{F}}_{2^m}[X, Y])^2$, jestliže

(i) $e_1 = 0 \wedge e_2 = 0$
přː $(P, Q) = (x^2, x^2 + 2y^2 + x)$

(ii) $e_1 \neq 0 \wedge a_2 = c \wedge e_1 = k \cdot d_2$
přː $(P, Q) = (2x^2 + 2y, x^2 + y^2 + x)$

(iii) $e_1 \neq 0 \wedge e_1 = k \cdot e_2$
přː $(P, Q) = (x^2 + 3y, x^2 + y^2 + 2x + 3y)$

(iv) $e_1 \neq 0 \wedge d_2 \neq 0 \wedge e_1 = k \cdot c \wedge a_1 \neq e_1 \wedge d_2 \neq a_2 \wedge e_1 \neq k \cdot d_2$
přː $(P, Q) = (x^2 + 2y, x^2 + 2y^2 + 3x)$

(v) $e_1 \neq 0 \wedge k \cdot a_2 = e_1 \wedge e_1 \neq k \cdot e_2 \wedge d_2 = c$
přː $(P, Q) = (x^2 + y, x^2 + 3y^2 + 3x)$

(vi) $e_1 \neq 0 \wedge a_2 = d_2 \wedge e_1 \neq a_1 \wedge a_2 \neq c \wedge e_1 \neq c$
přː $(P, Q) = (x^2 + 3y, x^2 + 2y^2 + x + 2y)$

(Analogicky pro $P = a_1y^2 + e_1x$ a $Q = a_2y^2 + cx^2 + d_2y + e_2x$)

Věta 4.13. Nechť $(P, Q) \in (\overset{2}{\mathbb{F}}_{2^m}[X, Y])^2$, kde $P = a_1x^2 + d_1x + e_1y$ a $Q = a_2x^2 + cy^2 + d_2x + e_2y$, kde $a_1 \neq 0$, $a_2 \neq 0$, $d_1 \neq 0$, $e_1 \neq 0$, $c \neq 0$, $a_1 = k \cdot a_2$, pak za předpokladu platnosti všech nutných podmínek $(P, Q) \in (\overset{2}{\mathbb{F}}_{2^m}[X, Y])^2$, jestliže

(i) jestliže $d_2 = e_2 = 0$ pak:

(α) $d_1 = k \cdot c \wedge a_1 = e_1$
přː $(P, Q) = (x^2 + 2x + y, x^2 + 2y^2)$

(β) $a_1 = d_1 \neq k \cdot c \wedge e_1 \neq k \cdot c \wedge e_1 \neq a_1$
př: $(P, Q) = (x^2 + x + 3y, x^2 + 2y^2)$

(γ) $e_1 = k \cdot c \wedge a_1 \neq e_1 \wedge d_1 \neq e_1 \wedge d_1 \neq a_1$
př: $(P, Q) = (x^2 + 3x + 2y, x^2 + 2y^2)$

(δ) $e_1 = d_1 \wedge a_2 = c$
př: $(P, Q) = (x^2 + 3x + 3y, 2x^2 + 2y^2)$

(ii) jestliže $d_2 \neq 0$ nebo $e_2 \neq 0$, pak:

(α) $d_2 = 0 \wedge a_1 = k \cdot c = d_1 \wedge e_1 \neq a_1$
př: $(P, Q) = (x^2 + x + 2y, x^2 + y^2 + y)$

(β) $d_2 = 0 \wedge a_1 = d_1 = e_1 = k \cdot a_2 \wedge e_1 \neq k \cdot e_2 \wedge d_1 \neq k \cdot c$
př: $(P, Q) = (x^2 + x + y, x^2 + 3y^2 + 3y)$

(γ) $d_2 = 0 \wedge d_1 = e_1 \wedge c = e_2 \wedge d_1 \neq k \cdot c \wedge a_2 \neq c$
př: $(P, Q) = (x^2 + 2x + 2y, x^2 + 3y^2 + 3y)$

(δ) $e_2 = 0 \wedge d_1 = e_1 = a_1 \wedge (c = d_2$ nebo $d_2 = a_2$ pro $c \neq d_2)$
př: $(P, Q) = (x^2 + x + y, x^2 + 3y^2 + 3x)$

(ϵ) $d_2 = 0 \wedge c = e_1 = k \cdot e_2 \wedge (d_1 \neq a_1 \vee c \neq a_2)$
př: $(P, Q) = (x^2 + 2x + 3y, x^2 + 3y^2 + 3y)$

(ζ) $d_2 = 0 \wedge d_1 = k \cdot c \wedge e_1 = k \cdot e_2 \wedge e_1 = a_1$
př: $(P, Q) = (x^2 + 2x + y, x^2 + 2y^2 + y)$

(η) $d_2 = 0 \wedge k \cdot c = d_1 = e_1 \wedge c \neq e_2$
př: $(P, Q) = (x^2 + 2x + 2y, x^2 + 2y^2 + y)$

(θ) $d_2 = 0 \wedge d_1 = k \cdot e_2 \wedge e_1 = k \cdot c \wedge e_1 \neq d_1 \wedge (a_1 = d_1$ nebo $a_2 = c)$
př: $(P, Q) = (x^2 + 2x + y, x^2 + y^2 + 2y)$

(ι) $d_2 = 0 \wedge d_1 = e_1 = k \cdot e_2 \wedge a_1 \neq d_1 \wedge a_2 = c$
př: $(P, Q) = (x^2 + 2x + 2y, x^2 + y^2 + 2y)$

(κ) $d_2 = 0 \wedge d_1 = k \cdot e_2 = k \cdot c \wedge a_1 \neq e_1 \wedge e_1 \neq d_1$
př: $(P, Q) = (x^2 + 3x + 2y, x^2 + 3y^2 + 3y)$

(λ) $d_2 = 0 \wedge e_1 = k \cdot e_2 \wedge d_1 = a_1 \wedge e_2 \neq c$
př: $(P, Q) = (x^2 + x + 3y, x^2 + 2y^2 + 3y)$

(μ) $d_2 = 0 \wedge a_1 = e_1 \neq d_1 \wedge c = e_2 \neq a_2 \wedge d_1 \neq k \cdot e_2$
př: $(P, Q) = (x^2 + 3x + y, x^2 + 2y^2 + 2y)$

(ν) $d_2 = 0 \wedge a_2 = e_2 \wedge d_1 = e_1 \neq k \cdot c \wedge a_2 \neq c$
př: $(P, Q) = (x^2 + 3x + 3y, x^2 + 2y^2 + y)$

(ξ) $d_2 = 0 \wedge d_1 = k \cdot c \wedge d_1 \neq e_1 \wedge c \neq e_2 \wedge e_2 = a_2$
př: $(P, Q) = (x^2 + 3x + 2y, x^2 + 3y^2 + y)$

(o) $d_2 = 0 \wedge d_1 = k \cdot e_2 \wedge d_1 \neq e_1 \wedge e_1 \neq k \cdot c \wedge c \neq e_2 \wedge (e_1 = a_1$ nebo $c = a_2)$
př: $(P, Q) = (x^2 + 2x + y, x^2 + 3y^2 + 2y)$

(π) $d_2 = 0 \wedge e_1 = k \cdot c \wedge e_1 \neq k \cdot e_2 \wedge e_1 \neq d_1 \wedge e_2 \neq a_2 \wedge k \cdot e_2 \neq d_1$
př: $(P, Q) = (x^2 + 2x + y, x^2 + y^2 + 3y)$

(ρ) $d_2 = 0 \wedge a_2 = e_2 = c \wedge e_1 \neq k \cdot e_2$
př: $(P, Q) = (x^2 + 2x + 3y, x^2 + y^2 + y)$

(iii) jestliže $d_2 \neq 0$, $e_2 \neq 0$, $d_1 \neq k \cdot d_2$ pak :

(α) $d_1 = a_1 = k \cdot c \wedge (d_1 = e_1 \wedge e_1 \neq k \cdot e_2$ nebo $d_1 \neq e_1 \wedge e_1 = k \cdot e_2)$
př: $(P, Q) = (x^2 + x + 3y, x^2 + y^2 + 3x + y)$

(β) $a_1 = e_1 = k \cdot e_2 = k \cdot c \wedge d_1 \neq a_1 \wedge a_2 \neq d_2$
př: $(P, Q) = (x^2 + 3x + y, x^2 + y^2 + 2x + y)$

(γ) $d_1 = k \cdot e_2 \wedge e_1 = k \cdot d_2 \wedge d_1 \neq e_1$
př: $(P, Q) = (x^2 + 3x + 2y, x^2 + y^2 + 2x + 3y)$

(δ) $d_1 = k \cdot e_2 \wedge e_1 \neq k \cdot d_2 \wedge (a_1 = k \cdot c \wedge d_1 \neq e_1$ nebo $a_2 \neq c \wedge e_1 = d_1)$
př: $(P, Q) = (x^2 + x + 2y, x^2 + y^2 + 3x + y)$

(ϵ) $e_1 \neq k \cdot d_2 \wedge d_1 = k \cdot e_2 \wedge (a_2 \neq c \wedge d_1 \neq e_1)$
př: $(P, Q) = (x^2 + x + y, x^2 + 3y^2 + 2x + y)$

(ζ) $a_1 = k \cdot e_2 \wedge a_1 \neq d_1 \wedge d_1 = e_1 = k \cdot c$
př: $(P, Q) = (x^2 + 2x + 2y, x^2 + 2y^2 + 3x + y)$

(η) $d_1 \neq k \cdot e_2 \wedge a_1 \neq d_1 \wedge a_2 = c = d_2 \wedge d_1 \neq e_1 \wedge (e_1 = k \cdot e_2$ nebo $d_1 = e_1)$
př: $(P, Q) = (x^2 + 3x + 2y, x^2 + y^2 + x + 2y)$

(θ) $e_1 \neq k \cdot e_2 \wedge d_1 \neq k \cdot c \wedge a_1 = e_1 = d_1 \wedge (c = d_2 \neq e_2$ nebo $d_2 = c \wedge e_1 = d_1)$
př: $(P, Q) = (x^2 + x + y, x^2 + 2y^2 + 2x + 2y)$

(Analogicky pro $P = a_1y^2 + d_1y + e_1x$ a $Q = a_2y^2 + cx^2 + d_2y + e_2x$)

Věta 4.14. Nechť $(P, Q) \in (\overset{2}{\mathbb{F}}_{2^m}[X, Y])^2$, kde $P = a_1x^2 + c_1y^2 + d_1x + e_1y$ a $Q = a_2x^2 + c_2y^2 + d_2x + e_2y$,kde $a_1 \neq 0$, $a_2 \neq 0$, $c_1 \neq 0$, $c_2 \neq 0$, $a_1 = k \cdot a_2$ pak za předpokladu platnosti všech nutných podmínek $(P, Q) \in (\overset{2}{\mathbb{F}}_{2^m}[X, Y])^2$, jestliže

(i) jestliže $d_1 = e_1 = d_2 = e_2 = 0 \wedge c_1 \neq c_2$
př: $(P, Q) = (x^2 + y^2, x^2 + 2y^2)$

(ii) jestliže $e_1 = d_1 = 0 \wedge e_2 \neq 0 \vee d_2 \neq 0$ pak:

(α) $c_1 = k \cdot c_2$
př: $(P, Q) = (x^2 + 2y^2, x^2 + 2y^2 + 3x + y)$

(β) $c_1 \neq k \cdot c_2 \wedge c_1 = k \cdot d_2 \wedge a_2 = e_2$
př: $(P, Q) = (x^2 + 2y^2 + y, x^2 + y^2 + 2x + y)$

(γ) $c_1 \neq k \cdot c_2 \wedge c_1 = k \cdot e_2 \wedge a_2 \neq d_2 \wedge (c_2 = d_2 \neq a_2$ nebo $a_2 = c_2 \neq d_2)$
př: $(P, Q) = (x^2 + 3y^2, x^2 + y^2 + 2x + 3y)$

(δ) $c_1 \neq k \cdot c_2 \wedge c_1 \neq k \cdot e_2 \wedge a_2 = c_2 = d_2 \neq e_2$
př: $(P, Q) = (x^2 + 2y^2, x^2 + y^2 + x + 3y)$

(ϵ) $c_1 \neq k \cdot c_2 \wedge c_2 = e_2 \neq a_2 \wedge c_1 \neq k \cdot d_2 \wedge a_1 \neq c_1$
př: $(P, Q) = (x^2 + 3y^2, x^2 + 2y^2 + x + 2y)$

(ζ) $c_1 \neq k \cdot c_2 \wedge c_1 = k \cdot d_2 \wedge a_2 = e_2$
př: $(P, Q) = (x^2 + 3y^2, x^2 + 2y^2 + 3x + y)$

(*iii*) jestliže $a_1 = k \cdot a_2 \wedge e_1 \neq 0 \wedge e_2 \neq 0 \wedge d_1 = 0 \wedge d_2 = 0$ pak:

(α) $c_1 = k \cdot c_2 \wedge e_1 \neq k \cdot e_2$ nebo $e_1 = k \cdot e_2 \wedge c_1 \neq k \cdot c_2$
př: $(P, Q) = (x^2 + 2y^2 + y, x^2 + y^2 + y)$

(*iv*) jestliže $a_1 = k \cdot a_2 \wedge d_1 = 0 \wedge d_2 \neq 0, e_1 \neq 0, e_2 \neq 0$ pak:

(α) $a_1 = k \cdot a_2 \wedge c_1 = k \cdot c_2 \wedge e_1 \neq k \cdot e_2$
př: $(P, Q) = (x^2 + y^2 + y, x^2 + y^2 + 3x + 2y)$

(β) $c_1 = k \cdot c_2 \wedge e_1 = k \cdot d_2 \wedge a_1 \neq c_1$
př: $(P, Q) = (x^2 + 2y^2 + 3y, x^2 + 2y^2 + 3x + y)$

(γ) $a_1 = k \cdot c_2 = k \cdot d_2 \wedge a_1 \neq c_1$ pak $(e_1 = k \cdot d_2 \wedge c_1 = k \cdot e_2)$ nebo $(e_1 \neq k \cdot d_2 \wedge c_1 = e_1)$
př: $(P, Q) = (x^2 + 2y^2 + y, x^2 + y^2 + x + 2y)$

(δ) $c_1 = k \cdot d_2 \wedge e_1 = k \cdot e_2 \wedge a_1 \neq e_1$
př: $(P, Q) = (x^2 + 3y^2 + 2y, x^2 + y^2 + 3x + 2y)$

(ϵ) $c_2 = d_2 \wedge e_1 \neq k \cdot d_2 \wedge a_1 = c_1$
př: $(P, Q) = (x^2 + y^2 + 3y, x^2 + 2y^2 + 2x + 3y)$

(ζ) $c_1 = k \cdot e_2 \wedge e_1 = k \cdot c_2 \wedge c_1 \neq k \cdot c_2 \wedge e_1 \neq k \cdot d_2$
př: $(P, Q) = (x^2 + y^2 + 2y, x^2 + 2y^2 + 3x + y)$

(η) $c_2 = e_2 \wedge c_1 = k \cdot d_2 \wedge e_1 \neq k \cdot d_2$
př: $(P, Q) = (x^2 + 2y^2 + 3y, x^2 + y^2 + 2x + y)$

(θ) $a_2 \neq c_2 \wedge c_1 = k \cdot c_2 \wedge c_1 = k \cdot d_1 \wedge e_1 = k \cdot d_2$
př: $(P, Q) = (x^2 + 2y^2 + 2y, x^2 + 2y^2 + 2x + 3y)$

(ι) $c_1 = e_1 = k \cdot d_2 \wedge a_1 = k \cdot c_2 \wedge e_2 \neq a_2$
př: $(P, Q) = (x^2 + 2y^2 + 2y, x^2 + y^2 + 2x + 3y)$

(κ) $a_1 = k \cdot e_2 \wedge e_1 = k \cdot d_2 \wedge c_1 \neq k \cdot c_2 \wedge (c_1 = e_1 \wedge c_2 \neq e_2)$ nebo $(c_2 = e_2 \wedge c_1 \neq e_1)$
př: $(P, Q) = (x^2 + 3y^2 + 3y, x^2 + 2y^2 + 3x + y)$

(λ) $a_1 = e_1 = k \cdot c_2 = k \cdot e_2 \wedge k \cdot d_2 \neq c_1 \wedge c_1 \neq e_1$
př: $(P, Q) = (x^2 + 3y^2 + y, x^2 + y^2 + 2x + y)$

(μ) $c_2 = e_2 \wedge e_1 = k \cdot d_2 \wedge c_1 \neq k \cdot e_2$
př: $(P, Q) = (x^2 + 3y^2 + y, x^2 + 2y^2 + x + 2y)$

(*v*) jestliže $d_1 \neq k \cdot d_2 \wedge e_1 \neq 0$, $e_2 \neq 0$, $d_1 \neq 0$, $d_2 \neq 0$ pak:

(α) $c_1 = k \cdot c_2$ nebo $e_1 = k \cdot e_2$
př: $(P, Q) = (x^2 + 2y^2 + x + 2y, x^2 + y^2 + 3x + 2y)$

(β) $d_1 = k \cdot e_2 \wedge e_1 = k \cdot d_2 \wedge c_1 = k \cdot c_2 \wedge c_1 = a_1$
př: $(P, Q) = (x^2 + y^2 + x + 3y, x^2 + y^2 + 3x + y)$

(γ) $a_1 = k \cdot c_2 \wedge k \cdot d_2 = e_1 \wedge d_1 \neq e_2 \wedge d_2 \neq e_2$
př: $(P, Q) = (x^2 + y^2 + 3x + y, x^2 + y^2 + 2x + 3y)$

(Analogicky pro $P = a_1y^2 + c_1x^2 + d_1y + e_1x$ a $Q = a_2y^2 + c_2x^2 + d_2y + e_2x$

Poznámka 4.2. Pro stanovení postačujících podmínek pro tvorbu „bijektivních párů“ jsme využili další specifické vlastnosti polynomů pole $\mathbb{F}_{2^2}$ a to stejný obor hodnot pro evaluace různých polynomů. V tomto případě nemáme na mysli polynomy lišící se o konstantu nebo o násobnost, zde je shoda zřejmá.
Na tomto základě stačilo uvést pouze jednu podmínku pro daný polynom, splňuje-li podmínku jeden, po prohození bude indukovat bijekci i druhý.
Jedná se o tyto polynomy včetně jejich násobností a rozšíření o konstantu:

$x^2 + y + 2x$	$x^2 + 3y + x$	$x^2 + y + 3x$
$x^2 + 2y^2 + 2x$	$x^2 + y^2 + x$	$x^2 + 3y^2 + 3x$
$x^2 + 3y^2 + 3y$	$x^2 + y^2 + 2y$	$x^2 + y^2 + y$
$y^2 + 3x + y$	$y^2 + 2y + 2x$	$y^2 + y + x$
$x^2 + 3y^2 + 2y$	$y^2 + 2x + y$	$y^2 + 3y + x$
$y^2 + 3y + 2x$	$2y^2 + x^2 + 2y$	$2y^2 + x^2 + y$
$x^2 + 2y + x$	$x^2 + x + y$	$x^2 + 3y + 3x$
$x^2 + 3y^2 + x$	$y^2 + x^2 + x$	$x^2 + y^2 + 3x$
$x^2 + y$	$x^2 + 2y$	$x^2 + 3y$
$y^2 + x$	$y^2 + 2x$	$x^2 + 3x$

$x^2+2y+2x$	x^2+2y^2+3y	y^2+x^2+3y
x^2+y^2+2x	$y^2+3x+2y$	$y^2+3y+3x$
y^2+x+2y	$x^2+3y+2x$	$x^2+2y+3x$
$3y^2+x^2+y$	x^2+3y^2+2x	x^2+2y^2+3x
x^2+y^2+2x+y	x^2+y^2+x+3y	x^2+y^2+3x+y
$x^2+2y^2+2x+2y$	x^2+2y^2+y+x	$x^2+3y^2+3x+3y$
x^2+y^2+x+2y	$x^2+y^2+3x+2y$	$x^2+y^2+2x+3y$
x^2+3y^2+x+y	$x^2+2y^2+3y+3x$	$x^2+3y^2+2x+2y$

Vraťme se k případu $p=2$, $m=1$, $n=2$, tedy kvadratické polynomy dvou neurčitých nad polem $\mathbb{F}_2$. V tomto případě nám $x^2=x$, tedy pro pole $\mathbb{F}_2$ nemá smysl kvadratické polynomy uvažovat.

4.3. Trojice kvadratických polynomů tří neurčitých nad konečným polem $\mathbb{F}_{2^m}$

Tedy řešíme případ $n=3$ pro $m=1$.
Kvadratický polynom má tvar $ax^2+by^2+cz^2+dxy+eyz+fxz+gx+hy+kz+l$, kde $a\neq 0$ nebo $b\neq 0$ nebo $c\neq 0$ nebo $d\neq 0$ nebo $e\neq 0$ nebo $f\neq 0$ a kde $a,b,c,d,e,f\in\mathbb{F}_{2^m}$.

V tomto případě stačilo pouze pozměnit program předcházející. Změnili jsme předpis polynomu, podmínky pro kvadratický polynom, drobné změny jako odstranění přebytečných závorek apod. a závěrem jsme netvořili dvojice, ale trojice polynomů. Vypsané polynomy jsme dále nezpracovávali.

Obr 4.5 ukázka výstupu programu na vygenerování trojic polynomů nad polem $\mathbb{F}_2$

```
{x + y*z, x + z + y*z, x + y + y*z, {1, 3, 5}}
{x + y*z, x + z + y*z, k[1] + x + y +  y*z, {1, 3, 6}}
{x + y*z, x + z + y*z, x + y + z +  y*z, {1, 3, 7}}
{x + y*z, x + z + y*z, k[1] + x + y +  z + y*z, {1, 3, 8}}
{x + y*z, x + z + y*z, x + y + x*z, {1, 3, 13}}
{x + y*z, x + z + y*z, k[1] + x + y +  x*z, {1, 3, 14}}
{x + y*z, x + z + y*z, x + y + z +  x*z, {1, 3, 15}}
{x + y*z, x + z + y*z, k[1] + x + y +  z + x*z, {1, 3, 16}}
{x + y*z, x + z + y*z, y + x*z + y*z, {1, 3, 17}}
{x + y*z, x + z + y*z, k[1] + y + x*z +  y*z, {1, 3, 18}}
{x + y*z, x + z + y*z, y + z + x*z +  y*z, {1, 3, 19}}
{x + y*z, x + z + y*z, k[1] + y + z +  x*z + y*z, {1, 3, 20}}
{x + y*z, x + z + y*z, y + z^2, {1, 3, 51}}
{x + y*z, x + z + y*z, k[1] + y + z^2, {1, 3, 52}}
{x + y*z, x + z + y*z, y + z + z^2, {1, 3, 53}}
{x + y*z, x + z + y*z, k[1] + y + z +  z^2, {1, 3, 54}}
{x + y*z, x + z + y*z, x + y + y*z +  z^2, {1, 3, 67}}
{x + y*z, x + z + y*z, k[1] + x + y +  y*z + z^2, {1, 3, 68}}
{x + y*z, x + z + y*z, x + y + z +  y*z + z^2, {1, 3, 69}}
{x + y*z, x + z + y*z, k[1] + x + y +  z + y*z + z^2, {1, 3, 70}}
{x + y*z, x + z + y*z, x + y + x*z +  z^2, {1, 3, 75}}
{x + y*z, x + z + y*z, k[1] + x + y +  x*z + z^2, {1, 3, 76}}
{x + y*z, x + z + y*z, x + y + z +  x*z + z^2, {1, 3, 77}}
{x + y*z, x + z + y*z, k[1] + x + y +  z + x*z + z^2, {1, 3, 78}}
{x + y*z, x + z + y*z, y + x*z + y*z +  z^2, {1, 3, 79}}
{x + y*z, x + z + y*z, k[1] + y + x*z +  y*z + z^2, {1, 3, 80}}
{x + y*z, x + z + y*z, y + z + x*z +  y*z + z^2, {1, 3, 81}}
{x + y*z, x + z + y*z, k[1] + y + z +  x*z + y*z + z^2, {1, 3, 82}}
{x + y*z, x + z + y*z, y^2, {1, 3, 119}}
{x + y*z, x + z + y*z, k[1] + y^2, {1, 3, 120}}
{x + y*z, x + z + y*z, y^2 + z, {1, 3, 121}}
{x + y*z, x + z + y*z, k[1] + y^2 + z, {1, 3, 122}}
{x + y*z, x + z + y*z, x + y^2 + y*z, {1, 3, 133}}
{x + y*z, x + z + y*z, k[1] + x + y^2 +  y*z, {1, 3, 134}}
{x + y*z, x + z + y*z, x + y^2 + z +  y*z, {1, 3, 135}}
{x + y*z, x + z + y*z, k[1] + x + y^2 +  z + y*z, {1, 3, 136}}
{x + y*z, x + z + y*z, x + y^2 + x*z, {1, 3, 145}}
{x + y*z, x + z + y*z, k[1] + x + y^2 +  x*z, {1, 3, 146}}
{x + y*z, x + z + y*z, x + y^2 + z +  x*z, {1, 3, 147}}
{x + y*z, x + z + y*z, k[1] + x + y^2 +  z + x*z, {1, 3, 148}}
{x + y*z, x + z + y*z, y^2 + x*z + y*z, {1, 3, 149}}
{x + y*z, x + z + y*z, k[1] + y^2 + x*z +  y*z, {1, 3, 150}}
{x + y*z, x + z + y*z, y^2 + z + x*z +  y*z, {1, 3, 151}}
{x + y*z, x + z + y*z, k[1] + y^2 + z +  x*z + y*z, {1, 3, 152}}
{x + y*z, x + z + y*z, y^2 + z^2, {1, 3, 189}}
{x + y*z, x + z + y*z, k[1] + y^2 + z^2, {1, 3, 190}}
{x + y*z, x + z + y*z, y^2 + z + z^2, {1, 3, 191}}
{x + y*z, x + z + y*z, k[1] + y^2 + z +  z^2, {1, 3, 192}}
{x + y*z, x + z + y*z, x + y^2 + y*z +  z^2, {1, 3, 203}}
{x + y*z, x + z + y*z, k[1] + x + y^2 +  y*z + z^2, {1, 3, 204}}
{x + y*z, x + z + y*z, x + y^2 + z +  y*z + z^2, {1, 3, 205}}
{x + y*z, x + z + y*z, k[1] + x + y^2 +  z + y*z + z^2, {1, 3, 206}}
{x + y*z, x + z + y*z, x + y^2 + x*z +  z^2, {1, 3, 215}}
{x + y*z, x + z + y*z, k[1] + x + y^2 +  x*z + z^2, {1, 3, 216}}
{x + y*z, x + z + y*z, x + y^2 + z +  x*z + z^2, {1, 3, 217}}
{x + y*z, x + z + y*z, k[1] + x + y^2 +  z + x*z + z^2, {1, 3, 218}}
{x + y*z, x + z + y*z, y^2 + x*z + y*z +  z^2, {1, 3, 219}}
{x + y*z, x + z + y*z, k[1] + y^2 + x*z +  y*z + z^2, {1, 3, 220}}
{x + y*z, x + z + y*z, y^2 + z + x*z +  y*z + z^2, {1, 3, 221}}
{x + y*z, x + z + y*z, k[1] + y^2 + z +  x*z + y*z + z^2, {1, 3, 222}}
```

Obr 4.6 ukázka programu na vygenerování trojic polynomů nad polem $\mathbb{F}_2$

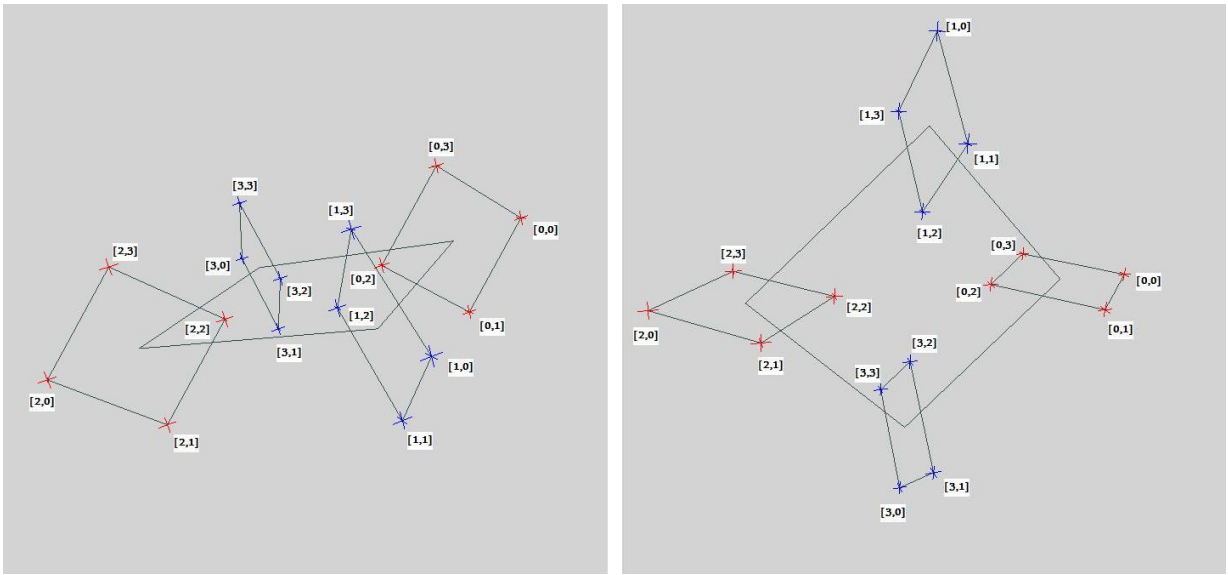
Wolfram Mathematica | FOR STUDENTS — Demonstrations | MathWorld | Student Forum

```
<< FiniteFields`FiniteFields`
K = GF[2];
SetFieldFormat[K, FormatType → FunctionOfCode[k]]
n = 2;

Timing[
 (*vytvoreni deseti-indexoveho pole polynomu,
 indexovano po koeficientech*)
 pp = Table[k[a] * x^2 + k[b] * y^2 + k[c] * z^2 + k[d] * x * y + k[e] * x * z +
    k[f] * z * y + k[g] * x + k[h] * y + k[aa] * z + k[bb], {a, 0, n - 1}, {b, 0, n - 1},
   {c, 0, n - 1}, {d, 0, n - 1}, {e, 0, n - 1}, {f, 0, n - 1}, {g, 0, n - 1},
   {h, 0, n - 1}, {aa, 0, n - 1}, {bb, 0, n - 1}];

 Ress = {0, 0, 0, 0, k[1], k[1], k[1], k[1]}; (*kontrolni prvek*)

 (*prevedeni pp na jedno-indexove pole polynomu,
 indexovano po polynomech*)
 Ast = Flatten[pp, 9];

 P = {};       (*predchystane pole*)

 pocet = 0;

 (*prochazeni polynomu*)
 For[i = 1, i < Length[Ast] + 1, i++,

    (*vylouceni nekvadratickych polynomu*)
   If[Not[Exponent[Ast[[i]], x] == 2 || Exponent[Ast[[i]], y] == 2 ||
     Exponent[Ast[[i]], z] == 2 || Exponent[Ast[[i]], x * z] == 1 ||
     Exponent[Ast[[i]], z * y] == 1 || Exponent[Ast[i], x * y] == 1], Continue[]]

   (*dosazeni prvku pole K do predpisu kvadratickeho polynomu*)
   L = {Ast[[i]]} /. Table[Table[{x → k[s], y → k[t], z → k[st]}, {s, 0, n - 1}],
     {t, 0, n - 1}, {st, 0, n - 1}];

   (*kontrola predpokladu k bijekci - porovnani s kontrolnim prvkem*)
   If[Sort[Flatten[L]] == Ress, AppendTo[P, Ast[[i]]];]
  ]

  Print[Length[P]]; (*pocet polynomu podobne kontrolnimu prvku*)

 (*vytvoreni pole trojic polynomu*)
 For[i = 1, i < Length[P] + 1, i++,
    For[j = 1, j < Length[P] + 1, j++,
     For[ji = 1, ji < Length[P] + 1, ji++,
      (*dosazeni prvku pole K do tri-indexoveho pole = do trojice polynomu,
      indexovano po polynomech**)
      A = {P[[i]], P[[j]], P[[ji]]} /.
       Table[Table[{x → k[s], y → k[t], z → k[st]}, {s, 0, n - 1}],
        {t, 0, n - 1}, {st, 0, n - 1}];

      (*prevedeni na jedno-indexove pole,
      idexovano po jednotlivych polynomech*)
      Seskupeni = Flatten[A, 2];

      (*hodnoty zobrazeni budou brany mnozinove*)
      Mnozinove = Union[Seskupeni];

      (*porovnani delky zobrazeni s delkou bijektivniho zobrazeni*)
      If[Length[Mnozinove] == n^3, pocet++;
       Print [{P[[i]], P[[j]], P[[ji]], {i, j, ji}}]] ;
     ]
    ]
   ]
   Print[pocet]        (*celkovy pocet trojic*)
]
```

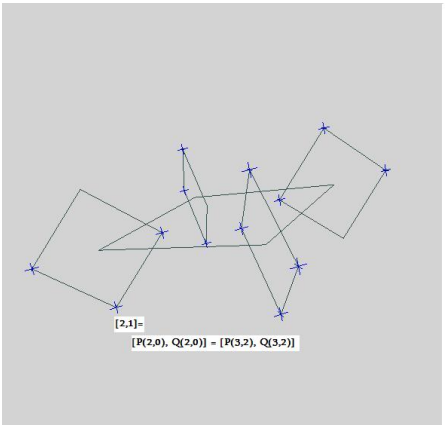
5. Grafické znázornění dvojic kvadratických polynomů na toru

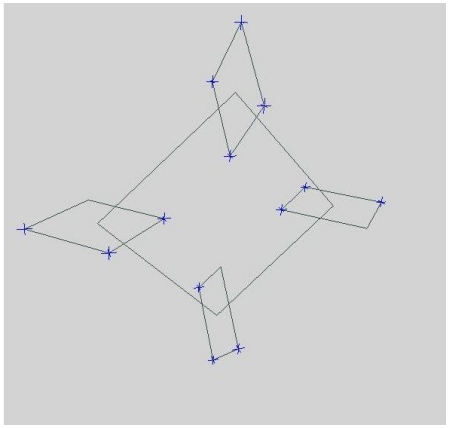
V této kapitole uvedeme zobrazení dvojic kvadratických polynomů na konečném poli a to na toru. Pro znázornění konečného pole využíváme kružnici, která nám zachovává aritmetiku pole. Této vlastnosti využijeme ke znázornění dvojice polynomů. Jelikož potřebujeme zobrazit dvojici polynomů, použijeme „kružnici krát kružnici“ tedy torus. První polynom určuje první souřadnici - tedy umístění na řídící kružnici a druhý polynom určuje umístění na vedlejší kružnici, která je na řídící kružnici kolmá.
Torus nám v našem případě představuje n-úhelník - řídící, kde kolem každého vrcholu je kolmo veden podobný n-úhelník - vedlejší. Pro naše případy pole $\mathbb{F}_{2^m}^2$ je $n = 2^m$. Takto zkonstruovaný torus, nám opět zachovává operace na konečném poli.
Ukážeme si znázornění bijektivních i nebijektivních dvojic. Úvodním obrázkem si ukážeme orientaci na toru pomocí souřadnic, které dále pro přehlednost neuvádíme, ale zachováváme natočení toru. Použitý program pro grafickou interpetaci viz [6].

Obr 5.1 popis toru: každý vrchol řídícího n-úhelníku, tvoří první souřadnici, druhá souřadnice je dána vedlejšími n-úhelníky



Obr 5.2 $(P,Q) \in (\widehat{\mathbb{F}_{2^2}^2[X,Y]})^2$, $P = x^2 + xy + 1$, $Q = x^2 + xy + x$ - dvojici tvoří polynomy, které nesplňují ani nutnou podmínku pro bijekci

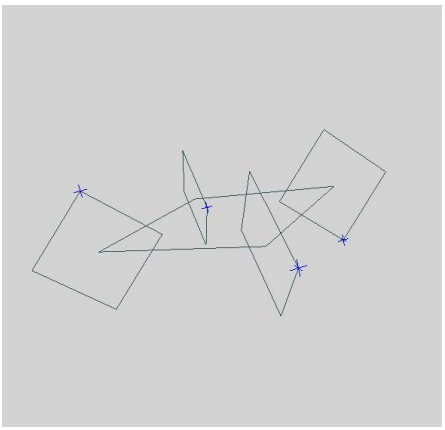


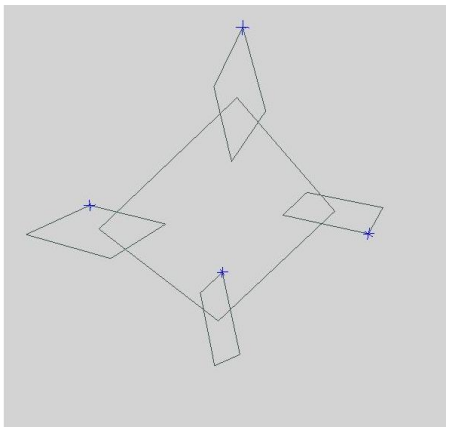


Jak lze z obrázku 5.2 vidět, člen xy nám narušuje bijekci „nesymetricky“, tedy ani vhodným přidáním dalšího členu, bychom bijekce nedosáhli. Jak bude patrné z nadcházejí-

cích obrázku, jsou-li splněny nutné podmínky, obdržíme jako hodnoty zobrazení buď všechny možné hodnoty, polovinu nebo čtvrtinu možných hodnot. Rozložení lze považovat za „symetrické“ ve smyslu rozložení vzhledem k řídícímu n-úhelníku, tedy na všech vedlejších n-úhelnících je stejný počet bodů.

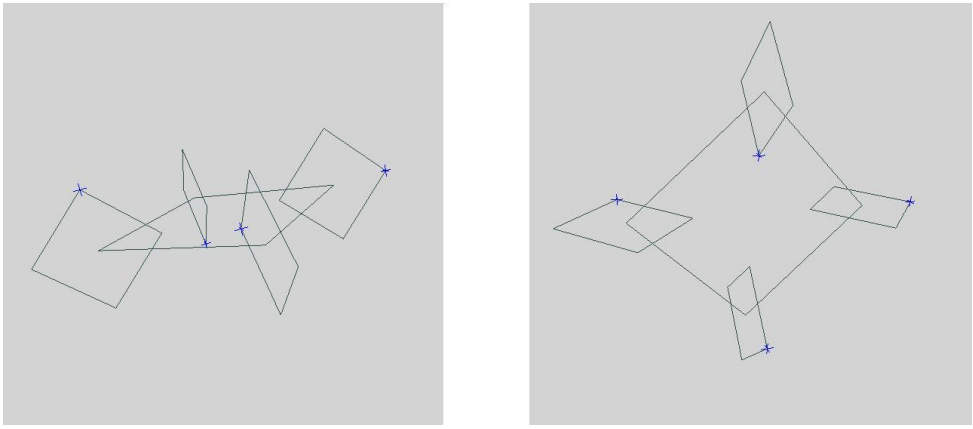
Obr 5.3 $(P,Q) \in (\widehat{\mathbb{F}_{2^2}^2[X,Y]})^2$, $P = y^2$, $Q = y^2 + 1$ - dvojici tvoří polynomy, které se liší o konstantu



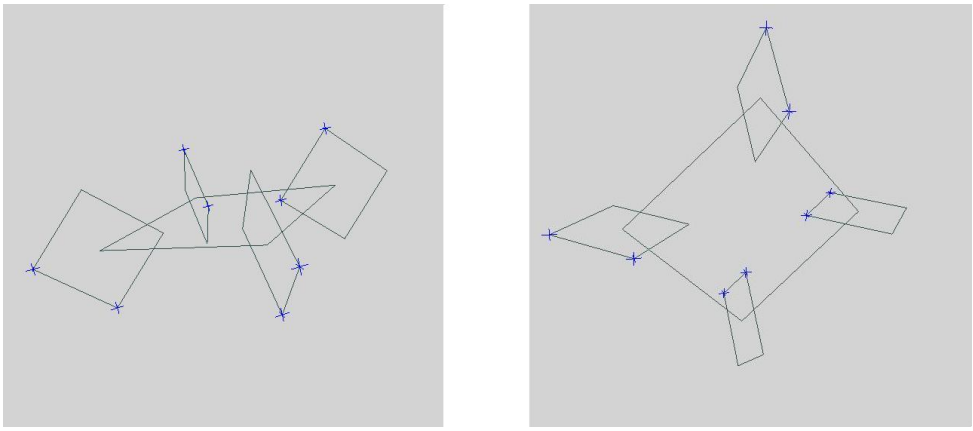


Jak lze na obrázku 5.3 vidět, máme-li dvojici polynomů, jenž se liší o konstantu, dostaneme vždy čtyřprvkovou množinu řešení. Oproti totožnému zobrazení, jsou souřadnice pouze posunuty na vedlejším n-úhelníku. Podobné řešení obdržíme v podání dvojice polynomů lišící se k-násobkem 5.4. I v tomto případě je řešení posunuto oproti totožnému, avšak samozřejmě jiným způsobem, než je tomu v případě konstanty.

Obr 5.4 $(P,Q) \in (\widehat{\mathbb{F}_{2^2}^2[X,Y]})^2$, $P = y^2 + x + 2y + 1$, $Q = y^2 + 2x + 3y + 2$ - dvojici tvoří polynomy, které se liší o k-násobek

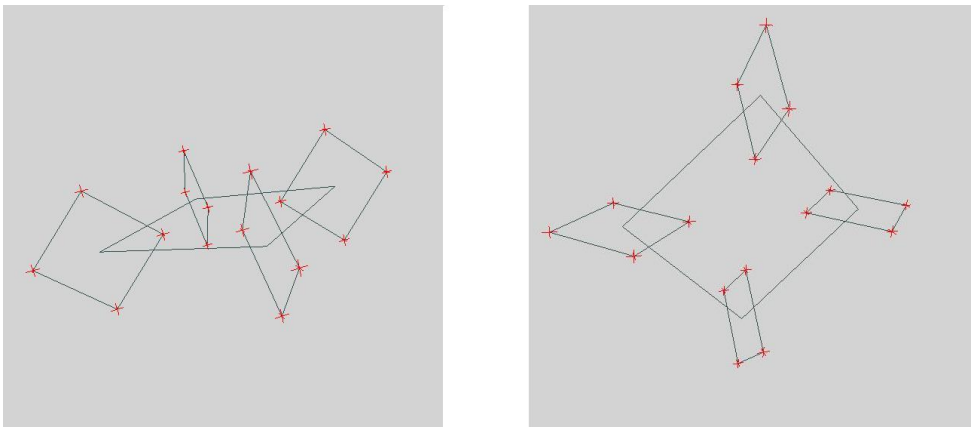


Obr 5.5 $(P,Q) \in (\widehat{\mathbb{F}_{2^2}^2[X,Y]})^2$, $P = x^2 + x + 3y + 1$, $Q = y^2 + x$ - dvojici tvoří polynomy, které nesplňují postačující podmínku

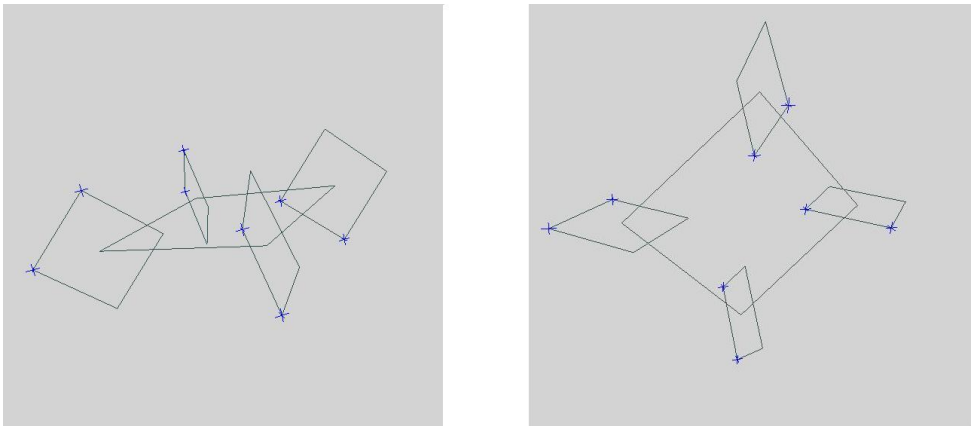


Na obrázku 5.5 a 5.6 lze vidět jak vhodnou úpravou lze z nebijektivního „páru“ obdržet bijektivní zobrazení. V tomto případě stačilo pouze modifikovat koeficient členu x v polynomu Q.

Obr 5.6 $(P,Q) \in (\widehat{\mathbb{F}_{2^2}^2[X,Y]})^2$, $P = x^2 + x + 3y + 1$, $Q = y^2 + 3x$ - dvojici tvoří polynomy indukující bijekci

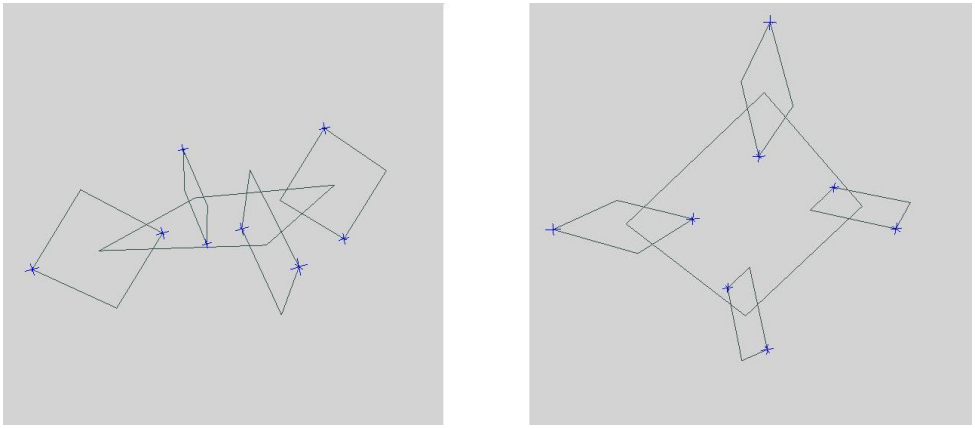


Obr 5.7 $(P,Q) \in (\widehat{\mathbb{F}_{2^2}^2[X,Y]})^2$, $P = x^2 + x + y$, $Q = x^2 + 2x + 3y + 2$ - dvojici tvoří polynomy, které splňují nutnou podmínku, nikoliv postačující



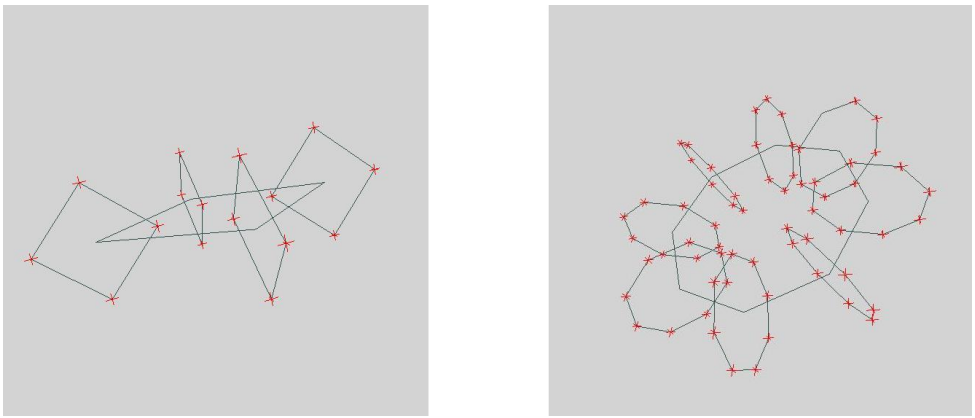
V případě dvojice polynomů 5.7 by pro bijekci stačilo pouze upravit člen y polynomu Q. Pokud bychom nahradili stávající koeficient u y číslem 2 byla by splněna jedna z postačujících podmínek a zobrazením bychom obdrželi bijekci. Podobně v případě dvojice 5.8 lze bijekce dosáhnout například odstraněním členu $2x$ z polynomu P.

Obr 5.8 $(P,Q) \in (\overset{2}{\widehat{\mathbb{F}_{2^2}}}[X,Y])^2$, $P = x^2+2x+y+3$, $Q = y^2+3$ - dvojici tvoří polynomy, které nesplňují postačující podmínku



V předchozí kapitole jsem zmiňovali specifické vlastnosti polynomů pro pole $\mathbb{F}_{2^2}$, které dále obecně pro jiná pole nepředpokládáme. Dále tedy pro názornost porovnáme některá specifika pole $\mathbb{F}_{2^2}$ s dalším binárním polem $\mathbb{F}_{2^3}$. Popis toru pro znázornění binárního pole $\mathbb{F}_{2^3}$ neuvádíme, jde nám pouze názornost a porovnání vlastností. Zejména porovnání platnosti věty o symetrii a nesjednocení odpovídajících si polynomů - tímto nevyvracíme existenci odpovídajících si polynomů pro $\mathbb{F}_{2^3}$ pouze poukazujeme na skutečnost, že vlastnosti jednoho pole nelze automaticky přenést na pole jiné.

Obr 5.9 $(P,Q) \in (\overset{2}{\widehat{\mathbb{F}_{2^2}}}[X,Y])^2$ oproti $(P,Q) \in (\overset{2}{\widehat{\mathbb{F}_{2^3}}}[X,Y])^2$, $P = x^2+2y$, $Q = x^2+3y^2+x+3y$ - zachování symetrie

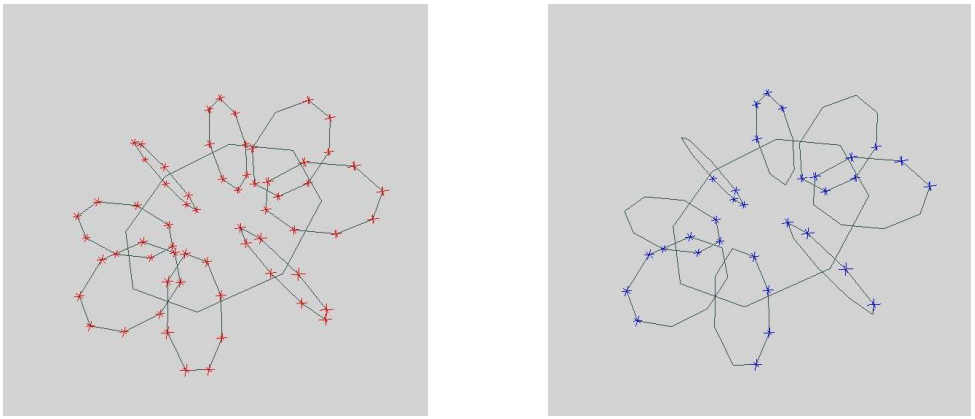


Pro dvojici polynomů $(P,Q) \in (\overset{2}{\widehat{\mathbb{F}_{2^2}}}[X,Y])^2$ jsme zavedli symetrii pomocí 4.9. Věta poukazuje na skutečnost, že v případě, kdy má polynom odpovídající tvar a splňuje nutné předpoklady k bijekci, je možné neurčitou x a y zaměnit, aniž by byla narušena bijekce „páru“. Pro volbu dvojice polynomů z 5.9 by se zdálo, že věta bude v platnosti i zde, neb i po „symetrii“ obdržíme totožná zobrazení jako jsou uvedena.

Vezmeme-li ovšem dvojici polynomů $(P,Q) \in (\overset{2}{\widehat{\mathbb{F}_{2^3}}}[X,Y])^2$ jako na 5.10, pak pak polynom P na předpoklady pro „symetrii“ a s polynomem Q bijekci tvoří. Provedeme-li

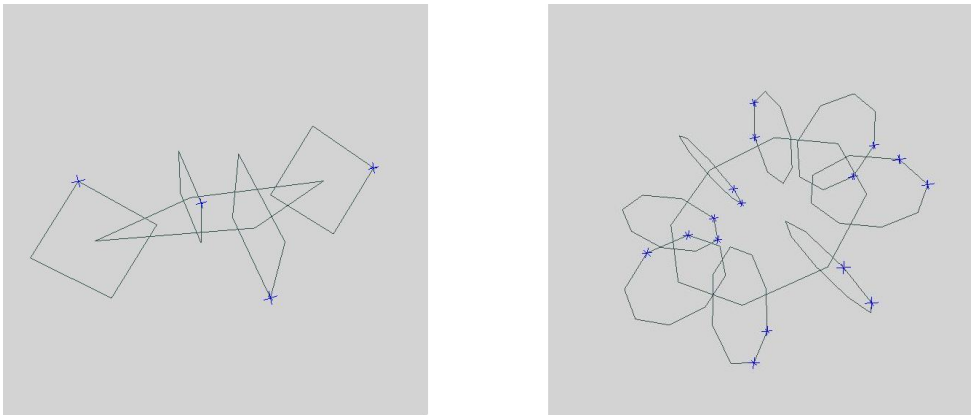
ji ovšem, obdržíme tak nebijektivní zobrazení, jak lze vidět na 5.10 vpravo. Věta tedy obecně nemůže být brána pro libovolná pole.

Obr 5.10 $(P,Q) \in (\overset{2}{\widehat{\mathbb{F}_{2^2}}}[X,Y])^2$ oproti $(P,Q) \in (\overset{2}{\widehat{\mathbb{F}_{2^3}}}[X,Y])^2$, $P = x^2 + 3y^2 + 3x + y$, $Q = x^2 + y^2 + x + y$ - narušení symtrie



Dále jsme měli dvojice polynomů, jenž se lišila předpisem, ale hodnoty zobrazení byly pro oba polynomy stejné, tedy tvořila „bijektivní pár“ se stejnou množinou polynomů. Vezmeme-li jednu takovou dvojici, jejich společné zobrazení nám dá početně stejnou množinu jako zobrazení dvou totožných polynomů. Jak lze vidět na 5.11 obecně nemůžeme přepokládat stejné vlastnosti polynomů pro různá pole.

Obr 5.11 $(P,Q) \in (\overset{2}{\widehat{\mathbb{F}_{2^3}}}[X,Y])^2$, $P = 3x^2 + y^2 + x + 3y$, $Q = x^2 + y^2 + 2x + 3y$



6. Diskuse výsledků o polynomech indukující bijekci v souvislosti s Maubachovou hypotézou

V této kapitole si aplikujeme 3.4 na předcházející kapitolu. Věta pojednává o celkovém počtu bijekcí vzhledem k charakteru binarního pole a srovnání celkového počtu bijekcí s počtem bijekcí indukovaných krotkými automorfismy. Vyhodnotíme pro případ podkapitoly 3.1 a pro případ uveden v podkapitole 3.2. Pro pomocné výpočty opět užíváme systému Mathematica, ve kterém jsme tvořili „bijektivní páry“ kombinace: dvou lineárních polynomů, dvojici kvadratický polynom-lineární polynom. Zdrojové kódy neuvádíme, jedná se o modifikaci kódů v práci uvedených a využíváme zde pro naše účely pouze číselného počtu takto vytvořených dvojic.

Případ 3.1 se týká věty 3.4 části $(i), (ii)$, kterou jsme řešili obecně.
Uvažujme celkový počet bijekcí nad $\mathbb{F}_{2^m}$ tedy $(2^m)!$

Máme-li kvadratický polynom indukující bijekci, tedy ax^2+c, celkový počet takto získaných bijekcí je $2^m \cdot (2^m - 1)$.
Podobně uvažujme lineární polynomy indukující bijekci, tedy $ax + b$, kde i zde obdržíme počet bijekcí $2^m \cdot (2^m - 1)$.
Využijeme-li vztahu z věty 3.4 $(i), (ii)$ obdržíme

$$\frac{(2^m)!}{(2^m - 2)!} = 2^m \cdot (2^m - 1)!.$$

Dle věty 3.4 by měl tento počet odpovídat počtu krotkých automorfismů, ty nám pro tento případ představují pouze polynomy lineární. Srovnáním obou čísel dojdeme k rovnosti.

Vezmeme-li jednoduchý příklad dvojice polynomů nad polem $\mathbb{F}_2$,tedy případ $m = 1$, $p = 2$, $n = 2$, celkový počet možných bijekcí je 4!.
Polynomy máme ve tvaru $P = cx + dy + e$, $Q = fx + gy + h$. Abychom obdrželi bijekci, musí být matice koeficientů regulární tj.

$$\begin{pmatrix} c & d \\ f & g \end{pmatrix} \neq 0$$

V našem případě to znamená tyto možnosti:

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \qquad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \qquad \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \qquad \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Máme tedy šest možných kombinací. Vezmeme-li v úvahu možnosti, které nám poskytují konstanty e, h dostaneme se na číslo $6 \cdot 2 \cdot 2 = 24$. Počet bijekcí získaných lineárními polynomy je shodný s celkovým počtem bijekci.

Případ 3.2 se týká věty 3.4 části (iii), kterou jsme řešili pro pole $\mathbb{F}_4$.
Každou bijekci je možné indukovat n-ticí polynomů, kde stupeň polynomů je menší než $p^m - 1$ viz [7]. Vezměme nyní naši situaci $p = 2$, $m = 2$, $n = 2$. Tedy v tomto případě nám vstupují do hry navíc polynomy třetího stupně.
Celkový počet bijekcí $(2^m)!$ je v našem případě roven 16!.

Uvažujme dvojici polynomů (P, Q), pro polynom stupně nejvýše tři mohou nastat tyto možnosti:

A	$degP = 1,$	$degQ = 1$	2880
B	$degP = 1,$	$degQ = 2$	20160
C	$degP = 1,$	$degQ = 3$	
D	$degP = 2,$	$degQ = 1$	20160
E	$degP = 2,$	$degQ = 2$	279360$*$
F	$degP = 2,$	$degQ = 3$	
G	$degP = 3,$	$degQ = 1$	
H	$degP = 3,$	$degQ = 2$	
I	$degP = 3,$	$degQ = 3$	

Poslední sloupec nám představuje počet bijekcí indukovaných kombinací polynomů příslušného řádu. $*$ - tento výsledek je v práci plně popsán, ostatní výsledky jsou jen na základě programových výstupů. Je patrné, že číselně srovnáme-li počet bijekcí, které známe, je to pouze nepatrné číslo oproti hodnotě 16!. V případě A nám celou množinu řešení představují afinní automorfismy. De Jonquièrův automorfismy můžeme očekávat v případě A, D, G kde ovšem nepokrývají veškeré možné bijekce. Vyvstává otázka polynomů třetího stupně a jejich chování v páru.

Máme tedy připraven program i metodu pro klasifikaci polynomů indukujících bijekci a jsme schopni odvodit počty n-tic indukujících bijekci. Rovněž víme, mezi dvojicemi kterých stupňů lze hledat afinní a de Jonquièrovy automorfismy, tato analýza nám tedy může dát i údaj o jejich počtu a ve srovnání s počtem možných bijekcí i napomoci zodpovězení otázky, zda divoký automorfismus indukuje bijekci. Tento případ je ale potřeba řešit pro případ $n \geq 3$, kdy nad polem divoké automorfismy existují viz. [8]
Námi zpracovaný program ale pro výpočetní náročnost neumožňuje zatím efektivně provádět analýzu pro $n \geq 3$, doba výpočtu přesahuje 240 hodin při běžném výkonu počítače. Je tedy třeba zefektivnit algoritmus. Máme za to, že metoda analýzy n-tic polynomů daných stupňů indukujících bijekci může k očekávanému potvrzení Maubachovy hypotézy přispět.

Obr 6.1 Masayoshi Nagata „konstruktér“ prvního divokého automorfismu, 1972

Nagatův divoký automorfismus:

$$\begin{aligned}\sigma(X) &= X - 2(XZ + Y^2)Y - (XZ + Y^2)^2 Z,\\ \sigma(Y) &= Y + (XZ + Y^2)Z,\\ \sigma(Z) &= Z.\end{aligned}$$

7. Závěr

V bakalářské práci jsme si po zavedení základních pojmů představili kvadratické polynomy indukující bijekci na konkrétním binárním poli. Na základě analýzy výstupu programů v systému Mathematica jsme formulovali věty 4.1 až 4.8, které jsme dokázali. Věty pojednávají o podmínkách nutných pro tvorbu „bijektivního páru “. V případě věty 4.1 se jedná o podmínku nutnou a zároveň i postačující. Dále přecházíme z obecných předpokladů na specifické vlastnosti kvadratických polynomů nad polem $\mathbb{F}_4$. Po celkové analýze těchto polynomů jsme formulovali věty 4.9 až 4.14, pomocí nichž lze i snadno sestrojit „bijektivní pár“ nebo upravit jinak nebijektivní dvojici. V závěru kapitoly jsme také uvedli dvojice kvadratických polynomů, které si navzájem odpovídají a díky kterým jsme mohli počet podmínek částečně zredukovat. V nasledující části jsme interpretovali vlastnosti z vět 4.9 až 4.14 grafickým znázorněním na toru. Uvedli jsme nebijektivní zobrazení a následně i možnosti jeho nápravy na bijektivní zobrazení. Skutečnost, že uvedené vlastnosti jsou specifické jen pro dané pole, jsme ukázali na protipříkladu vedeném pro pole $\mathbb{F}_8$. Poslední kapitola aplikuje větu 3.4 o srovnání celkového počtu bijekcí s počtem bijekcí indukovaných krotkými automorfismy na námi získané výsledky z programů. Pro případ 3.2 jsme modifikovali zde uvedené programy a provedli alespoň číselnou analýzu všech možných kombinací dvojic lineárních a kvadratických polynomů indukujících bijekci.

Literatura

[1] COHEN H., FREY G., *Handbook of Elliptic and Hyperelliptic curve cryptography.* Chapman and Hall/CRC,2005

[2] KARÁSEK, J., SKULA, L., *Lineární algebra.* Akademicke nakladatelství CERM, 1999

[3] KUREŠ, M., *The composition of polynomials by the substitution principle.* Journal of Discrete Mathematical Sciences and Cryptography, Vol.13, No.6, pp.543-552, 2010

[4] VAN DEN ESSEN, A., *Polynomial Automorphisms and the Jacobian Conjecture* . Birkhuser Verlag, 2000

[5] MAUBACH, S., *Polynomial automrphisms over finite fields.* Serdica Mathematical journal, 343-350, 2001

[6] BAJKO, J., *Transfer eliptických křivek na torus.* Brno: Vysoké učení technické v Brně, Fakulta strojního inženýrství, 2011

[7] HAVLÍČKOVÁ, A., *Algoritmy interpolace polynomy více neurčitých.* Brno: Vysoké učení technické v Brně, Fakulta strojního inženýrství, 2011

[8] SHESTAKOV, I.P., UMIRBAEV, U.U., *The Nagata automorphism is wild.* Proc. Natl.Acad. Sci. USA 100,No. 22, 12561-12563, 2003