NMMB538 - DÚ7

Jan Oupický

1

Z definice [2] víme, že $\forall \alpha \in D : [2](\alpha) = \alpha \oplus \alpha$. Vyjádříme tedy vzorec pro výpočet bodu $\alpha \oplus \alpha \in D$ křivky V_w.

Nejprve vyjádříme racionální funkci. Použijeme vzorec pro součet bodů a to, že pro body $(\alpha_1, \alpha_2) \in D$ platí $\alpha_2^2 = \alpha_1^3 + a\alpha_1^2 + b\alpha$. γ bude značit reprezentanta rac. zobrazení $\gamma(\alpha) = [2](\alpha), \gamma = (\gamma_1, \gamma_2), \gamma_i \in K(x_1, x_2)$.

Vyjádříme nejprve $\gamma_1(x_1, x_2)$. Ze vzorců pro součet stejného bodu vyjde, že:

$$\gamma_1(x_1, x_2) = \frac{-8x_1x_2^2 - 4ax_2^2 + 9x_1^4 + 12ax_1^3 + 6bx_1^2 + 4a^2x_1^2 + 4abx_1 + b^2}{4x_2^2}$$

zasubstituujeme za x_2^2 v čitateli a vyjde:

$$\gamma_1(x_1, x_2) = \frac{x_1^4 - 2bx_1^2 + b^2}{4x_2^2} = \left(\frac{x_1^2 - b}{2x_2}\right)^2$$

Nyní spočteme $\gamma_2(x_1, x_2)$:

$$\gamma_2(x_1, x_2) = \frac{3x_1^3 + 2ax_1^2 + bx_1}{2x_2} - \frac{3x_1^3 + 2ax_1 + b}{2x_2} \cdot \frac{x_1^4 - 2bx_1^2 + b^2}{4x_2^2} - x_2$$

Převedení na společného jmenovatele a použití substituce za x_2^2 v čitateli:

$$\gamma_2(x_1, x_2) = \frac{x_1^6 + 2ax_1^5 + 5bx_1^4 - 5b^2x_1^2 - 2ab^2x_1 - b^3}{8x_2^3}$$

Máme tedy reprezentanty $K-$racionálního zobrazení $[2] : D \to D$, kde
$[2] = (\gamma_1 + (w), \gamma_2 + (w))$. Sestrojíme nyní projektivní reprezentaci zobrazení [2] jako v předchozím úkolu pomocí lemma M.3.

$$\gamma_i = \frac{a_i}{b_i}, a_i, b_i \in K[x_1, x_2], b_i \neq 0$$
$$A_1' = \widehat{a_1}X_3^2 = (X_1^4 - 2bX_1^2X_3^2 + b^2X_3^4)X_3^2$$
$$A_2' = \widehat{a_2}X_3^3 = (X_1^6 + 2aX_1^5X_3 + 5bX_1^4X_3^2 - 5b^2X_1^2X_3^4 - 2ab^2X_1X_3^5 - b^3X_3^6)X_3^3$$
$$B_1' = 4X_2^2X_3^4$$
$$B_2' = 8X_2^3X_3^6$$
$$\Longrightarrow$$
$$(A_1 : A_2 : A_3) = (A_1'B_2' : A_2'B_1' : B_1'B_2')$$

dosazení a zkrácení:

$$(A_1 : A_2 : A_3) = (2(X_1^4 - 2bX_1^2X_3^2 + b^2X_3^4)X_2X_3 : \widehat{a_2} : 4X_2^3X_3^3)$$

2

Pro reprezentaci $[2] = (A_1 : A_2 : A_3)$ výše platí $\deg_{X_2}(A_1) = 1, \deg_{X_2}(A_2) = 0$. V posledním členu A_3 nahradíme $X_2^2X_3$ za $X_1^3 + aX_1^2X_3 + bX_1X_3^2$. Máme tedy novou reprezentaci, která splňuje podmínky:

$$(A_1' : A_2' : A_3') = (2(X_1^4 - 2bX_1^2X_3^2 + b^2X_3^4)X_2X_3 : \widehat{a_2} : 4X_2X_3^2(X_1^3 + aX_1^2X_3 + bX_1X_3^2))$$

Pro reprezentaci [2] $= (B_1 : B_2 : B_3), \deg_{X_1}(B_i) \leq 2$ využijeme substituci $X_1^3 = X_2^2X_3 - aX_1^2X_3 - bX_1X_3^2$. Každá substituce sníží stupeň (v X_1) polynomu o 1. Zřejmě se dostaneme do tvaru, kde $\deg_{X_1}(B_i) \leq 2$. Substituce do 1. členu:

$$B_1 = 2X_2X_3^2((a^2 - 3b)X_1^2X_3 + X_1X_2^2 + abX_1X_3^2 - aX_2^2X_3 + b^2X_3^3)$$

B_2 získáme opakovanou substitucí za X_1^3. Polynom je tvaru:

$$B_2 = -X_3^2(-X_2^4 + X_2^2X_3f_1(X_1, X_2, X_3) + X_3^2f_2(X_1, X_2, X_3)), \deg_{X_1}(f_i) = i$$

3

Bod $\infty = (0 : 1 : 0) \in D$. Zřejmě $A_1', A_3'(\infty) = 0$ (násobky X_3) a $A_2'(\infty) = 0$ (jsou tam jen monočleny $X_1^iX_3^j$). Obdobně $B_i(\infty) = 0$ (všechno to jsou násobky X_3).

Pokud ale definujeme $B_i' = \frac{B_i}{X_3^2}$. Poté $B_2'(\infty) = 1$.

4