Pascal–Dreieck und rationale Normkurven bei Charakteristik $p > 0$

Johannes Gmainer und Hans Havlicek
Abteilung für Lineare Algebra und Geometrie
Technische Universität Wien

FWF Projekt P–12353–MAT

PG(n, K) sei der n–dimensionale projektive Raum über K^{n+1}, mit $n \geq 2$ und K kommutativ.

Jede *rationale Normkurve* in PG(n, K) ist der rationalen Normkurve

$$\Gamma := \{K(1, t, \ldots, t^n) \mid t \in K \cup \{\infty\}\}$$

projektiv äquivalent.

Hasse–Ableitung in $K[t]$:

$$\begin{array}{rcccl} D_t^{(r)} & : & K[t] & \longrightarrow & K[t] \qquad \text{linear} \\ & & t^m & \longmapsto & \binom{m}{r} t^{m-r} \end{array}$$

Zusammenhang mit der formalen Ableitung in $K[t]$:

$$\frac{d^r}{dt^r} = r!\, D_t^{(r)}$$

$D_t^{(r)} \circ D_t^{(s)} \neq D_t^{(r+s)}$, d.h. die Hasse–Ableitung ist nicht iterativ.

Die Spaltenvektoren $c_t,\ c_t',\ldots,\ c_t^{(n-1)},\ c_t^{(n)}$ der Matrix

$$C_t := \begin{pmatrix} \binom{0}{0} & 0 & 0 & \ldots & 0 \\ \binom{1}{0}t & \binom{1}{1} & 0 & \ldots & 0 \\ \binom{2}{0}t^2 & \binom{2}{1}t & \binom{2}{2} & \ldots & 0 \\ \vdots & & & \ddots & \vdots \\ \binom{n}{0}t^n & \binom{n}{1}t^{n-1} & \binom{n}{2}t^{n-2} & \ldots & \binom{n}{n} \end{pmatrix}$$

bestimmen für $t \in K$ die Kurven– bzw. Ableitungspunkte von Γ.

Es gilt $C_t^{-1} = C_{-t}$.

Außerdem sei $c_\infty^{(k)} := (\delta_{0,n-k},\ldots,\delta_{n,n-k})$.

Beispiel: Normkurve in 4–Raum bei Charakteristik $p = 2$

$$C_t = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ t & 1 & 0 & 0 & 0 \\ t^2 & 0 & 1 & 0 & 0 \\ t^3 & t^2 & t & 1 & 0 \\ t^4 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Der k–Schmiegraum $\mathcal{S}_t^{(k)}\Gamma$ $(-1 \leq k \leq n-1\})$ von Γ im Punkt Kc_t ist die projektive Hülle über die Punkte $Kc_t, Kc_t', \ldots, Kc_t^{(k)}$.

DEFINITION 1 Der k–*Knoten* $\mathcal{N}^{(k)}\Gamma$ einer rationalen Normkurve Γ in $\mathrm{PG}(n, K)$ sei der Durchschnitt all ihrer k–Schmiegräume.

Beispiel: Kegelschnitt bei $\operatorname{char} K = 2$:

$$C_t = \begin{pmatrix} \binom{0}{0} & 0 & 0 \\ \binom{1}{0}t & \binom{1}{1} & 0 \\ \binom{2}{0}t^2 & \binom{2}{1}t & \binom{2}{2} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ t & 1 & 0 \\ t^2 & 0 & 1 \end{pmatrix}$$

$$\Rightarrow \dim \mathcal{N}^{(-1)}\Gamma = \dim \mathcal{N}^{(0)}\Gamma = -1$$

$$\Rightarrow \dim \mathcal{N}^{(1)}\Gamma = \dim \mathcal{N}^{(n-1)}\Gamma = 0$$

k–Schmiegraum $\mathcal{S}_t^{(k)}$ ist Lösung des linearen Systems

$$\begin{array}{lcl}
\binom{k+1}{0}(-t)^{k+1}x_0+\ldots+\binom{k+1}{k+1}x_{k+1} & = & 0\\
\binom{k+2}{0}(-t)^{k+2}x_0+\ldots\quad+\binom{k+2}{k+2}x_{k+2} & = & 0\\
\vdots\qquad\qquad\qquad\ddots & & \vdots\\
\binom{n}{0}(-t)^{n}x_0+\ldots\qquad\qquad+\binom{n}{n}x_{n} & = & 0
\end{array}$$

da $C_t = C_{-t}$.

THEOREM 1 *Sei* $\#K \geq k+1$ *und* $\operatorname{char} K = p \geq 0$. *Dann wird der Knoten* $\mathcal{N}^{(k)}\Gamma$ *durch jene Basispunkte* P_j *des Bezugssystems aufgespannt, deren Index* $j \in \{0, 1, \ldots, n\}$ *die Bedingung*

$$\binom{k+1}{j} \equiv \binom{k+2}{j} \equiv \ldots \equiv \binom{n}{j} \equiv 0 \pmod{p}$$

erfüllt.

p ... fest gewählte Primzahl

p–adische Zifferndarstellung:

$$n = \sum_{\lambda=0}^{\infty} n_\lambda p^\lambda =: \langle n_\lambda \rangle =: \langle n_r, n_{r-1}, \ldots, n_0 \rangle$$

mit $0 \le n_\lambda \le p - 1$.

Satz von Lucas:

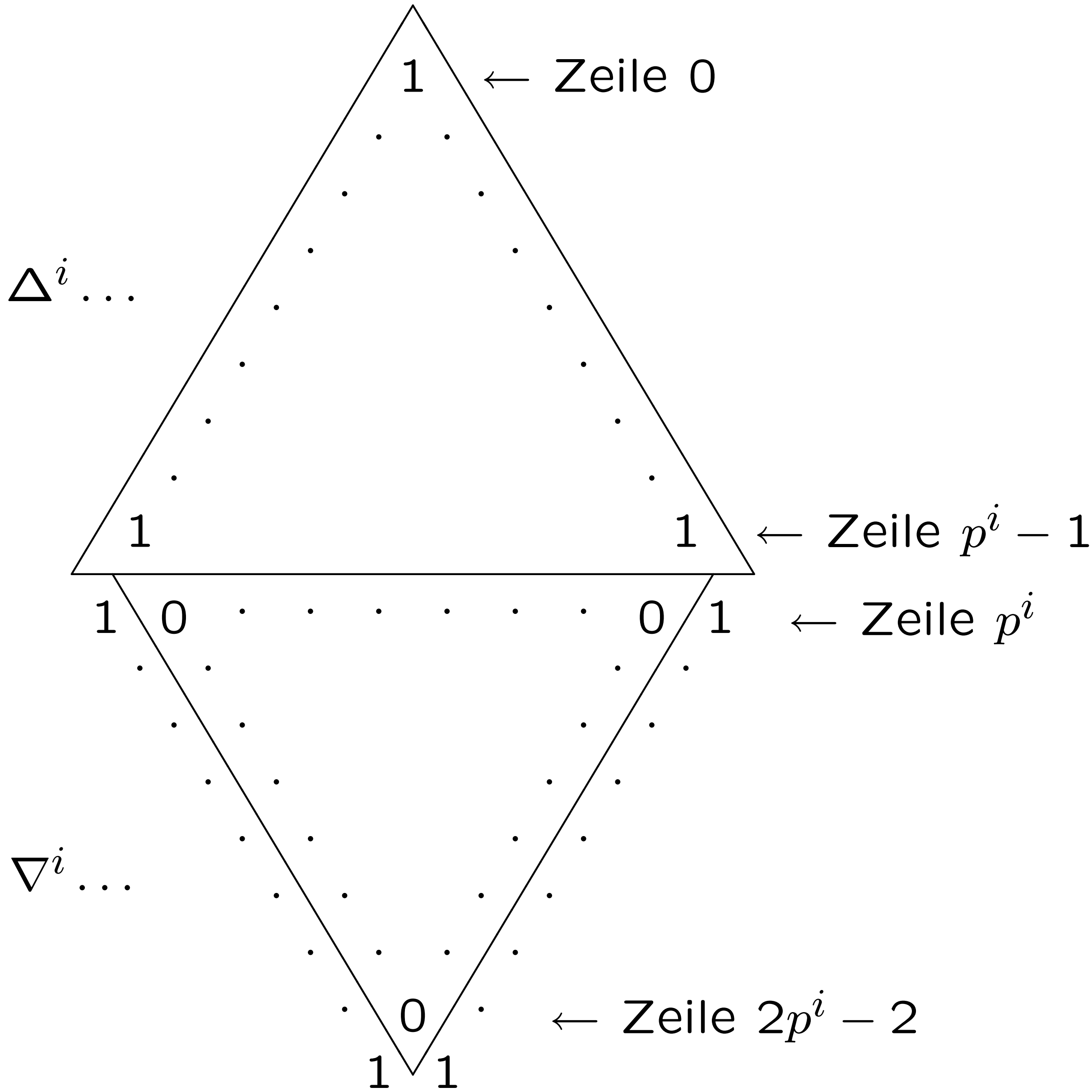
$$\binom{n}{j} \equiv \prod_{\lambda=0}^{\infty} \binom{n_\lambda}{j_\lambda} \pmod{p}.$$

Folgerung:

$$\binom{n}{j} \equiv 0 \pmod{p} \Leftrightarrow \exists \lambda \text{ mit } n_\lambda < j_\lambda.$$

$\Delta(p)$ ... **Pascal**–Dreieck modulo p

Teildreiecke:



Klasseneinteilung der 0–Einträge von $\Delta(p)$:

$\bar{i}$ . . . Union aller ∇^i, $i \in \mathbb{N}^+$

Beispiel:

$p = 3$, $\binom{147}{43} \equiv 0 \pmod 3$, liegt in $\bar{i} = \bar{3}$

$$\begin{array}{rcccccl} n = \langle & 1, & 2, & 1, & 1, & 0 & \rangle = 147 \\ j = \langle & 0, & 1, & 1, & 2, & 1 & \rangle = 43 \\ & & \uparrow & & \uparrow & & \\ & & i & & L & & \end{array}$$

$$L := \max\{\lambda \in \mathbb{N} \mid j_\lambda > n_\lambda\} \in \mathbb{N}$$

$$i := \min\{\lambda \mid \lambda > L,\ j_\lambda < n_\lambda\} \in \mathbb{N}^+$$

Anzahl der Nullen der Klasse $\bar{i}$ in der Zeile n:

$$\Phi(i,n) := \Big(p^i - 1 - \sum_{\mu=0}^{i-1} n_\mu p^\mu\Big) \cdot n_i \cdot \prod_{\lambda=i+1}^{\infty} (n_\lambda + 1).$$

$$\Phi(i,n) = 0 \Leftrightarrow \begin{cases} n_i = 0 \\ \text{oder} \\ n_{i-1} = \ldots = n_1 = n_0 = p-1 \end{cases}$$

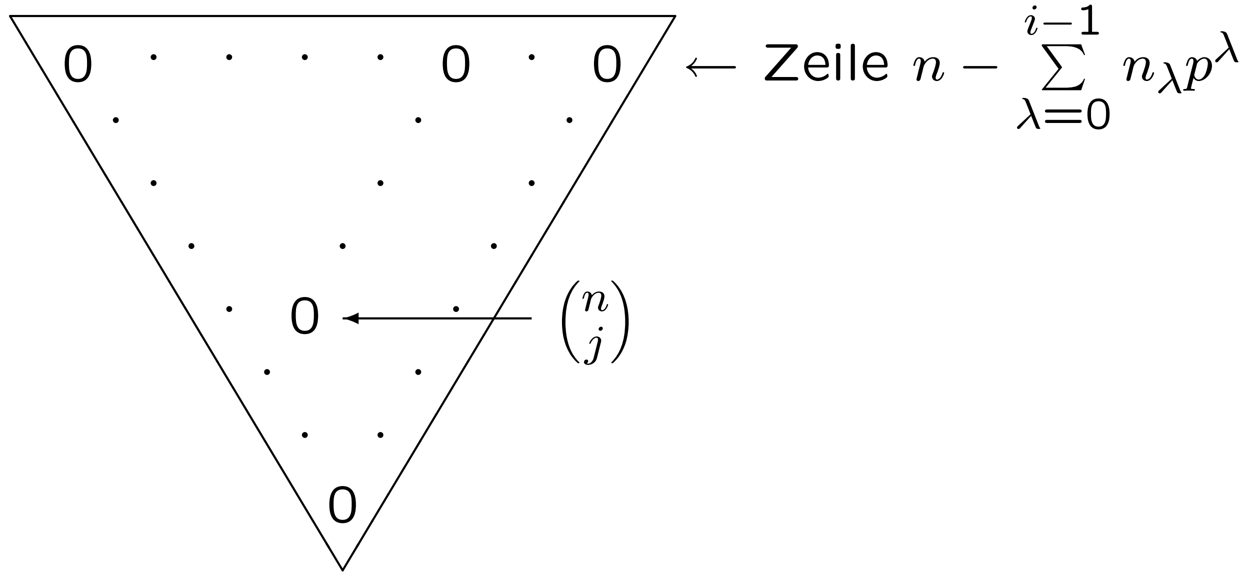
Übergang von n zu $b := n+1$:

$$\begin{aligned} n &= \langle \ldots, n_{M+1}, n_M, p-1, \ldots, p-1 \rangle \\ &\qquad \text{mit } n_M < p-1 \\ b &= \langle \ldots, b_{M+1}, b_M, 0, \ldots, 0 \rangle \\ &= \langle \ldots, n_{M+1}, n_M + 1, 0, \ldots, 0 \rangle \end{aligned}$$

$$\Phi(i,n) = 0 \Leftrightarrow \begin{cases} b_{i-1} = 0 \text{ für } i \leq M, \\ b_i = 0 \text{ für } i > M. \end{cases}$$

Vertikale Verteilung der Nullen in $\Delta(p)$:

$\binom{n}{j}$ liege in ∇^i



$$T(i,b) := n - \sum_{\lambda=0}^{i-1} n_\lambda p^\lambda = b - \sum_{\lambda=0}^{i-1} b_\lambda p^\lambda$$

Beispiel: $p = 2$, $n = 14$:

$$\begin{aligned} n &= \langle 1,1,1,0 \rangle \\ b &= \langle 1,1,1,1 \rangle \end{aligned}$$

$$\begin{array}{rl}
 & 1 \\
 & 1\ 1 \\
 & 1\ 0\ 1 \\
 & 1\ 1\ 1\ 1 \\
 & 1\ 0\ 0\ 0\ 1 \\
 & 1\ 1\ 0\ 0\ 1\ 1 \\
 & 1\ 0\ 1\ 0\ 1\ 0\ 1 \\
 & 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1 \\
\langle 1,0,0,0 \rangle \rightarrow & 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1 \\
 & 1\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 1 \\
 & 1\ 0\ 1\ 0\ 0\ 0\ 0\ 0\ 1\ 0\ 1 \\
 & 1\ 1\ 1\ 1\ 0\ 0\ 0\ 0\ 1\ 1\ 1\ 1 \\
\langle 1,1,0,0 \rangle \rightarrow & 1\ 0\ 0\ 0\ 1\ 0\ 0\ 0\ 1\ 0\ 0\ 0\ 1 \\
 & 1\ 1\ 0\ 0\ 1\ 1\ 0\ 0\ 1\ 1\ 0\ 0\ 1\ 1 \\
\langle 1,1,1,0 \rangle \rightarrow & 1\ 0\ 1\ 0\ 1\ 0\ 1\ 0\ 1\ 0\ 1\ 0\ 1\ 0\ 1 \\
\langle 1,1,1,1 \rangle \rightarrow &
\end{array}$$

Beispiel: $p = 3$, $n = 584$

$$\begin{aligned} n &= \langle 2,1,0,1,2,2 \rangle \\ b &= \langle 2,1,0,2,0,0 \rangle \end{aligned}$$

$$\begin{aligned} T(1,b) &= \langle 2,1,0,2,0,0 \rangle = 585 > 584 \\ T(2,b) &= \langle 2,1,0,2,0,0 \rangle = 585 > 584 \\ T(3,b) &= \langle 2,1,0,0,0,0 \rangle = 567 \\ T(4,b) &= \langle 2,1,0,0,0,0 \rangle = 567 \\ T(5,b) &= \langle 2,0,0,0,0,0 \rangle = 486 \end{aligned}$$

$$\begin{aligned} \Phi(1,n) &= 0 \\ \Phi(2,n) &= 0 \\ \Phi(3,n) &= 0 \\ \Phi(4,n) &= 189 \\ \Phi(5,n) &= 288 \end{aligned}$$

Eine Summenfunktion:

$$\begin{aligned}\Sigma(R,n) &= \sum_{\eta=R}^{\infty} \Phi(\eta,n)\\ &= n+1-\Big(1+\sum_{\mu=0}^{R-1} n_\mu p^\mu\Big)\prod_{\lambda=R}^{\infty}(n_\lambda+1)\end{aligned}$$

THEOREM 2 *Sei* Γ *eine rationale Normkurve in* $\mathrm{PG}(n,K)$ *mit* $\#K \geq k+1$. *Erfüllt die natürliche Zahl* k *die Ungleichung*

$$T(R,b) \leq k+1 < T(Q,b),$$

($b_\lambda \neq 0$ *für genau ein* $\lambda \in \{Q, Q+1, \ldots, R-1\}$*), dann hat der* k*–Knoten von* Γ *die Dimension*

$$\dim \mathcal{N}^{(k)}\Gamma = \Sigma(R,n) - 1.$$

Beispiel: $p = 3$, $n = 584$

$$
\begin{aligned}
n &= \langle 2, 1, 0, 1, 2, 2 \rangle \\
b &= \langle 2, 1, 0, 2, 0, 0 \rangle
\end{aligned}
$$

$$
\begin{aligned}
0 = T(6,b) \ &\leq k+1 < \ T(5,b) = 486 \\
&\Rightarrow \quad \dim \mathcal{N}^{(k)}\Gamma = -1 \\
486 = T(5,b) \ &\leq k+1 < \ T(3,b) = 567 \\
&\Rightarrow \quad \dim \mathcal{N}^{(k)}\Gamma = 288 - 1 \\
567 = T(3,b) \ &\leq k+1 < \ T(1,b) = 585 \\
&\Rightarrow \quad \dim \mathcal{N}^{(k)}\Gamma = 477 - 1
\end{aligned}
$$

THEOREM 3 *Es sei Γ eine rationale Normkurve in* $\mathrm{PG}(n, K)$ *und K habe mindestens n Elemente. Dann entspricht die Anzahl der von Null verschiedenen Ziffern in der Darstellung von $b = n + 1$ in der Basis p genau der Anzahl der verschiedenen Knoten von Γ.*