Veronese Varieties over Fields with non-zero Characteristic: A Survey

Hans Havlicek

1 Introduction

Non-zero characteristic of the (commutative) ground field F heavily influences the geometric properties of Veronese varieties and, in particular, normal rational curves. Best known is probably the fact that, in case of characteristic two, all tangents of a conic are concurrent. This has lead to the concept of a *nucleus*. However, it seems that there are essentially distinct definitions. Some authors, like J.A. Thas [38], use this term to denote a point which extends a normal rational curve to an $(q+2)$-arc (F a finite field of even order q), others, like A. Herzer [23], use the same term for the intersection of all osculating hyperplanes of a Veronese variety. In order to overcome this difference of terminology we introduce the term (r,k)*-nucleus*. The two types of nuclei mentioned above are just particular examples fitting into this general concept.

Each nucleus is an *invariant subspace*, i.e. a subspace in the ambient space of a Veronese variety which is fixed (as a set of points) under the group of automorphic collineations of the variety. However, an invariant subspace needs not be a nucleus.

In the present survey we collect some recent results on nuclei of Veronese varieties and invariant subspaces of normal rational curves. We must assume, however, that the ground field is not "too small", since otherwise a Veronese variety is like dust: "few points" in some "high-dimensional" space.

Nuclei and invariant subspaces do not appear in classical textbooks on Veronese varieties ($F = \mathbb{R}, \mathbb{C}$), since for characteristic zero all invariant subspaces are trivial. If the ground field has characteristic $p > 0$, then geometric properties of invariant subspaces are closely related to *multinomial coefficients* that vanish modulo p and to the representations of certain integers in base p. In order to illustrate this connection some results on binomial and multinomial coefficients are gathered in Chapters 2 and 4.

2 Pascal's triangle modulo a prime p

2.1 A partition of zero entries

Throughout this section let p be a fixed prime. The representation of a non–negative integer $n \in \mathbb{N} := \{0, 1, 2, \ldots\}$ in base p has the form

$$n = \sum_{\sigma=0}^{\infty} n_\sigma p^\sigma =: \langle n_\sigma \rangle \tag{1}$$

with only finitely many digits $n_\sigma \in \{0, 1, \ldots, p-1\}$ different from 0.

Let $\langle n_\sigma \rangle$ and $\langle j_\sigma \rangle$ be the representations of non–negative integers n and j in base p. By a Theorem of Lucas [4, 364],

$$\binom{n}{j} \equiv \prod_{\sigma=0}^{\infty} \binom{n_\sigma}{j_\sigma} \pmod{p}. \tag{2}$$

Pascal's triangle modulo p will be denoted by Δ. The numbering of its rows starts with the index 0. Also, let Δ^i ($i \in \mathbb{N}$) be the subtriangle of Δ that is formed by the rows $0, 1, \ldots, p^i - 1$. From (2) each triangle Δ^{i+1} ($i \geq 0$) has the following form, with products taken modulo p:

$$\begin{array}{c}
\binom{0}{0}\Delta^i \\
\binom{1}{0}\Delta^i \quad \nabla^i \quad \binom{1}{1}\Delta^i \\
\binom{2}{0}\Delta^i \quad \nabla^i \quad \binom{2}{1}\Delta^i \quad \nabla^i \quad \binom{2}{2}\Delta^i \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
\binom{p-1}{0}\Delta^i \quad \nabla^i \qquad\qquad \cdots \qquad\qquad \nabla^i \quad \binom{p-1}{p-1}\Delta^i
\end{array}$$

Here the ∇^i's are triangles with all entries equal to zero. Observe that the baseline of Δ^i has p^i entries, whereas the top line of ∇^i is formed by $p^i - 1$ zero entries. So ∇^0 is empty. The binomial coefficients on the left hand side of the Δ^i's are exactly the entries of Δ^1. None of them vanishes modulo p. If $i \geq 2$, then each subtriangle $\binom{n}{j}\Delta^i$ from above can be decomposed into subtriangles proportional to Δ^{i-1} and subtriangles ∇^{i-1}, and so on. Cf., among others, [24, 91–92], [33, Theorem 1], [44].

The zero entries of Pascal's triangle modulo p fall into (disjoint) maximal subtriangles ∇^i ($i \in \mathbb{N}^+$). We get a partition of all zero entries of Δ by gluing together all triangles ∇^i of same size to one class, say $\bar{\imath}$. A formal definition of this partition, which is the backbone of many further considerations, is as follows:

Definition 1 [12] A pair $(n, j) = (\langle n_\sigma \rangle, \langle j_\sigma \rangle)$ of non–negative integers with $j \leq n$, $\binom{n}{j} \equiv 0 \pmod{p}$, and $L := \max\{\sigma \in \mathbb{N} \mid j_\sigma > n_\sigma\}$, is in *class* $\bar{\imath}$, if

$$i = \min\{\sigma \mid \sigma > L,\ j_\sigma < n_\sigma\} \in \mathbb{N}^+. \tag{3}$$

2.2 Counting zero entries

The following is taken from [12]. Let $n = \langle n_\sigma \rangle \in \mathbb{N}$ and $i \in \mathbb{N}^+$. Then the number of entries in row n of Δ belonging to class $\bar{i}$ equals

$$\Phi(i,n) := \#\overline{i(n)} = \Big(p^i - 1 - \sum_{\mu=0}^{i-1} n_\mu p^\mu\Big) \cdot n_i \cdot \prod_{\sigma=i+1}^{\infty} (n_\sigma + 1). \tag{4}$$

The number of entries in row n of Δ belonging to classes $\bar{i}$, $\overline{(i+1)}$, ... is

$$\Sigma(i,n) := \sum_{\eta=i}^{\infty} \Phi(\eta,n) = n + 1 - \Big(1 + \sum_{\mu=0}^{i-1} n_\mu p^\mu\Big) \prod_{\sigma=i}^{\infty} (n_\sigma + 1). \tag{5}$$

For $i = 1$ this is due to N.J. Fine [7].

When exhibiting "vertical" properties of Δ the following *top line function* turns out useful: Given $b \in \mathbb{N}^+$ and $R \in \mathbb{N}$ then let

$$T(R,b) := \sum_{\sigma=R}^{\infty} b_\sigma p^\sigma. \tag{6}$$

This function has the following property: If $(n,j) \in \bar{i}$ and $b := n+1$ then $T(i,b)$ gives the "top line" of the triangle ∇^i containing the (n,j)-entry of Δ, i.e.

$$0 \equiv \binom{n}{j} \equiv \binom{n-1}{j} \equiv \ldots \equiv \binom{T(i,b)}{j} \not\equiv \binom{T(i,b)-1}{j} \pmod{p}. \tag{7}$$

We refer to [14], [31], [36] for further properties of Δ.

3 Normal rational curves

3.1 Definition of k-nuclei

Let $\{\mathbf{b}_0, \mathbf{b}_1\}$ be a basis of a 2-dimensional vector space $\mathbf{X}$ over a commutative field F (the parameter space) and let $\mathbf{Y}$ be an $(n+1)$-dimensional vector space over F with a basis $\{\mathbf{c}_0, \mathbf{c}_1, \ldots, \mathbf{c}_n\}$, where $n \geq 2$. The *Veronese mapping*

$$F(x_0\mathbf{b}_0 + x_1\mathbf{b}_1) \mapsto F\Big(\sum_{e=0}^{n} x_0^{n-e} x_1^e \mathbf{c}_e\Big) \quad (x_i \in F) \tag{8}$$

maps the point set of the projective line $\mathcal{P}(\mathbf{X})$ into the point set of $\mathcal{P}(\mathbf{Y})$, i.e. the projective space on $\mathbf{Y}$. Its image is a *normal rational curve* $\mathcal{V}_1^n$ (sometimes abbreviated as NRC) with ambient space $\mathcal{P}(\mathbf{Y})$ [1], [2], [3], [5], [26, Chapter 21]. In terms of coordinates and an inhomogeneous parameter $x := x_1/x_0$ we obtain

$$\mathcal{V}_1^n := \{F(1, x, \ldots, x^n) \mid x \in F \cup \{\infty\}\}. \tag{9}$$

Recall the *non-iterative derivation* due to H. Hasse, F.K. Schmidt, and O. Teichmüller [15], [27, 1.3]. The k-th derivative $D^{(k)} : F[X] \to F[X]$ is a linear mapping such that $D^{(k)}(X^r) = \binom{r}{k}X^{r-k}$ for $k \le r$ and $D^{(k)}(X^r) = 0$ otherwise $(r, k \in \mathbb{N})$.

If we fix one $u \in F$ then columns of the regular matrix

$$\begin{pmatrix} \binom{0}{0} & 0 & 0 & \ldots & 0 \\ \binom{1}{0}u & \binom{1}{1} & 0 & \ldots & 0 \\ \binom{2}{0}u^2 & \binom{2}{1}u & \binom{2}{2} & \ldots & 0 \\ \vdots & & & \ddots & \vdots \\ \binom{n}{0}u^n & \binom{n}{1}u^{n-1} & \binom{n}{2}u^{n-2} & \ldots & \binom{n}{n} \end{pmatrix} \tag{10}$$

give, respectively, a point of the NRC (9) and its *derivative points*. The *k-osculating subspace* $(k \in \{-1, 0, \ldots, n-1\})$ of $\mathcal{V}_1^n$ at the given point is the k-dimensional projective subspace spanned by the first $k+1$ columns of the matrix (10). The derivative points at $F\mathbf{c}_n$ $(u = \infty)$ are $F\mathbf{c}_{n-1}, F\mathbf{c}_{n-2} \ldots, F\mathbf{c}_0$.

Formal derivation in $F[X]$ is in general not an adequate tool to describe osculating subspaces [35].

The (empty) (-1)-osculating subspace is introduced for formal reasons only. However, we refrain from calling the entire space an n-osculating subspace. As usual, a 1-osculating subspace is also called a *tangent*.

Definition 2 [12] The *k-nucleus* $\mathcal{N}^{(k)}\mathcal{V}_1^n$ $(k \in \{-1, 0, \ldots, n-1\})$ of a normal rational curve $\mathcal{V}_1^n$ is the intersection of all its k-osculating subspaces.

Remark 1 Instead of a parametric representation one could also use a *generating map* [16], [19], *Segre varieties* [5], [32], [46], [47] or tools from multilinear algebra [11], [23] in order to define osculating subspaces.

The NRC (9) has exactly $\#F + 1$ points. Every subset with $s \le n+1$ points is linearly independent. If $\#F \ge n+2$ then the NRC is a set with at least $n+3$ points of which every $n+1$ are linearly independent.

Suppose now that $q := \#F$ is finite. From above, for $q \ge n+2$ the NRC is a non-trivial example of a $(q+1)$-arc in the n-dimensional projective space $\mathcal{P}(\mathbf{Y})$. If $q = n+1$ then the NRC is a frame. Furthermore, $u^n = u^{q-1} = 1$ for all non-zero elements u of F. This illustrates that here the hyperplane with equation $x_0 = x_n$ contains all points of the NRC other than $F\mathbf{c}_0$ and $F\mathbf{c}_n$. Finally, if $q \le n$ then the NRC is just a basis of a q-dimensional projective subspace.

If $\#F \geq n+2$ or $n=2$, then each automorphic collineation of the NRC (9) preserves osculating subspaces. Otherwise, there are automorphic collineations of the NRC that do not preserve all osculating subspaces, whence the concept of osculating subspaces depends on the parametric representation of the NRC rather than on the points of the NRC [17], [19, 2.4].

3.2 Number and dimensions of nuclei

The following theorem links nuclei of a NRC with Pascal's triangle:

Theorem 1 [12] *If $\#F \geq k+1$, then the k-nucleus $\mathcal{N}^{(k)}\mathcal{V}_1^n$ of the normal rational curve (9) equals the subspace spanned by those base points $F\mathbf{c}_j$, where $j \in \{0,1,\ldots,n\}$ is subject to*

$$\binom{k+1}{j} \equiv \binom{k+2}{j} \equiv \ldots \equiv \binom{n}{j} \equiv 0 \pmod{\operatorname{char} F}. \tag{11}$$

By Theorem 1, $\operatorname{char} F = 0$ implies that all nuclei of a NRC are empty. Thus we assume in the remaining part of this section that

$$\operatorname{char} F =: p > 0;\ n =: \langle n_\sigma \rangle,\ n+1 =: b =: \langle b_\sigma \rangle \text{ (in base } p). \tag{12}$$

We are now in a position to describe the (projective) dimension of a k-nucleus:

Theorem 2 [12] *If $\#F \geq k+1$ and*

$$T(R,b) = \sum_{\mu=R}^{\infty} b_\mu p^\mu \leq k+1 < \sum_{\sigma=Q}^{\infty} b_\sigma p^\sigma = T(Q,b) \tag{13}$$

with at most one $b_\sigma \neq 0$ for $\sigma \in \{Q, Q+1, \ldots, R-1\}$, then the k-nucleus of $\mathcal{V}_1^n$ has dimension

$$n - \Big(1 + \sum_{\mu=0}^{R-1} n_\mu p^\mu\Big) \prod_{\sigma=R}^{\infty} (n_\sigma + 1) = \Sigma(R,n) - 1. \tag{14}$$

The condition on the digits b_σ guarantees that the top line function T does not assume a value that is properly between $T(R,b)$ and $T(Q,b)$.

If $k = n-1$, then (14) turns into Timmermann's formula [41, 4.15]

$$\dim \mathcal{N}^{(n-1)}\mathcal{V}_1^n = n - \prod_{\sigma=0}^{\infty} (n_\sigma + 1) = \Sigma(1,n) - 1; \tag{15}$$

cf. also [40].

Remark 2 If the ground field F does not meet the richness condition of Theorem 2, then (14) is a lower bound for the dimension of the k-nucleus, but it seems to be an open problem to explicitly determine the dimension of the k-nucleus in terms of k, n, and $\#F$. See also [18] and Example 3.

Next we state a formula for the number of distinct nuclei:

Theorem 3 [12] *If $\#F \geq n$, then there are as many distinct nuclei of $\mathcal{V}_1^n$ as non-zero digits in the representation of $b = n + 1$ in base p.*

Example 1 Let $p = 2$ and $n = 50$: The representation of $50 + 1$ in base 2 is $\langle 110011 \rangle$; there are four non-zero digits. So there are four distinct nuclei, including one empty nucleus. From

$$\begin{gathered} T(0,51) = \langle 110011 \rangle = 51, \quad T(1,51) = \langle 110010 \rangle = 50, \\ T(2,51) = T(3,51) = T(4,51) = \langle 110000 \rangle = 48, \\ T(5,51) = \langle 100000 \rangle = 32, \quad T(6,51) = \langle 0 \rangle = 0, \end{gathered}$$

we obtain the following values:

k	$-1, 0, \ldots, 30$	$31, 32, \ldots, 46$	$47, 48$	49
$\dim \mathcal{N}^{(k)} \mathcal{V}_1^n$	-1	12	38	42

Remark 3 Let $\#F \geq n$. Then

$$n = 2p^i - 2 \geq 2 \text{ (for some } i \in \mathbb{N}) \tag{16}$$

is necessary and sufficient for the smallest non-empty nucleus to be a single point. In fact, this point is $F\mathbf{c}_{p^i - 1}$. In particular, if F is a finite field of even order q then this point together with $\mathcal{V}_1^n$ is a $(q+2)$-arc provided that $n = 2$ or provided that $n = q - 2 \geq 2$ [38]. Cf. also [8], [37]. In general, however, the geometric meaning of this point seems to be unknown.

From Theorem 3 all nuclei are empty exactly if

$$n = \langle n_J, p-1, \ldots, p-1 \rangle = n_J p^J - 1 \geq 2 \tag{17}$$

with $1 \leq n_J < p$ and $J \in \mathbb{N}$. See also [23], [32].

Further properties of nuclei can be found in [9], [12].

3.3 Invariant subspaces

Each NRC $\mathcal{V}_1^n$ admits a group of collineations that is similar - via (8) - to $\mathrm{P\Gamma L}(2, F)$ acting on the projective line $\mathcal{P}(\mathbf{X})$. If $\#F \geq n + 2$ or $n = 2$ then this group is the full collineation group of the curve [17].

Each nucleus is an *invariant subspace* i.e. it remains fixed (as a point set) under the full collineation group of the NRC. In many low-dimensional examples there are no invariant subspaces other than nuclei. Clearly, all invariant subspaces form a lattice with the operations of "join" and "meet".

In order to find all invariant subspaces, we follow J. Gmainer [10]: Suppose that the dimension n is fixed. For $j \in \mathbb{N}$ let

$$\Omega(j) := \{m \in \mathbb{N} \mid 0 \leq m \leq n, \tbinom{m}{j} \not\equiv 0 \pmod{\operatorname{char} F}\}. \tag{18}$$

Given a subset $J \subset \{0, 1, \dots, n\}$ then put

$$\Omega(J) := \bigcup_{j \in J} \Omega(j), \quad \Psi(J) := \bigcup_{j \in J} \{j, n-j\}. \tag{19}$$

Both Ω and Ψ are closure operators on $\{0, 1, \dots, n\}$. The idea behind these definitions is as follows: For each $a \in F \setminus \{0\}$ the mapping

$$F(x_0, x_1, \dots, x_n) \mapsto F(a^0 x_0, a^1 x_1, \dots, a^n x_n) \tag{20}$$

describes (in terms of coordinates) an automorphic projective collineation of the NRC (9). If the ground field is sufficiently large then every subspace, which is invariant under all collineations (20), is spanned by base points $F\mathbf{c}_\lambda$. Here λ runs in a subset Λ of $\{0, 1, \dots, n\}$. So it is enough to look for appropriate subsets Λ. Likewise, the projective collineation

$$F(x_0, x_1, \dots, x_n) \mapsto F(x_n, x_{n-1}, \dots, x_0) \tag{21}$$

leaves the NRC invariant, whence Λ has to be closed with respect to Ψ. A similar argument yields the operator Ω.

Now we are able to formulate the main theorem for invariant subspaces.

Theorem 4 [10] *Let $\#F \geq n+2$ or $n = 2$. A subspace $\mathcal{U}$ is invariant under the collineation group of the normal rational curve (9) if, and only if, $\mathcal{U}$ is spanned by base points $F\mathbf{c}_\lambda$ with $\lambda \in \Lambda \subset \{0, 1, \dots, n\}$ such that $\Psi(\Lambda) \subset \Lambda$ and $\Omega(\Lambda) \subset \Lambda$.*

In case of $\operatorname{char} F = 0$ there are only trivial invariant subspaces. Thus we may restrict ourselves to the case

$$\operatorname{char} F = p > 0. \tag{22}$$

By Theorem 4 it suffices to find all Ψ-closed index sets $\Omega(J) \subset \{0, 1, \dots, n\}$. To this end we proceed in four steps:

Firstly, let $\langle b_\sigma \rangle$ be the expansion of $b = n + 1$ in base p. We define

$$V(i, b) := \sum_{\sigma=0}^{i-1} b_\sigma p^\sigma \text{ for all } i \in \mathbb{N}. \tag{23}$$

Secondly, we fix one number $i \in \mathbb{N}$. Suppose that I_α, where $\alpha \in \{1, 2, \dots, L\}$, is a family of sets such that the following conditions on the sets I_α and the digits b_σ of b hold true:

1. Each non-empty set I_α has the form $I_\alpha = \{j \in \mathbb{N} \mid H_\alpha > j \geq h_\alpha\}$ with $i-1 \geq H_\alpha > h_\alpha \geq 0$.
2. If $\alpha > \beta$ and $I_\alpha, I_\beta \neq \emptyset$, then $h_\alpha > H_\beta$.
3. $b_{H_\alpha} < p-1$ and $b_{h_\alpha} > 0$ for each non-empty set I_α.

For empty subsets I_α no numbers H_α, h_α will be defined. Thus

$$V(i,b) = \langle \ldots, b_{H_\alpha}, \underbrace{b_{H_\alpha - 1}, \ldots, b_{h_\alpha}}_{I_\alpha \neq \emptyset}, \ldots \rangle \tag{24}$$

and blocks of digits belonging to different non-empty sets $I_\alpha \cup \{H_\alpha\}$ do not overlap. So we are in a position to define a number by simultaneously changing the digits of $V(i,b)$ for all non-empty sets I_α as follows:

$$V(I_1, \ldots, I_L; i, b) := \langle \ldots, b_{H_\alpha} + 1, \underbrace{0, \ldots, 0}_{I_\alpha \neq \emptyset}, \ldots \rangle \tag{25}$$

Thirdly, we assign to each $(I_1, I_2, \ldots, I_L, i, b)$, such that $V(I_1, I_2, \ldots, I_L; i, b)$ is defined, the set

$$\mathcal{T}(I_1 \times I_2 \times \cdots \times I_L) \tag{26}$$

of all $(T_1, T_2, \ldots, T_L)$ satisfying the following conditions:

1. If $T_\alpha \neq \emptyset$ then $T_\alpha \subset I_\alpha$ and $h_\alpha = \min T_\alpha$.
2. $V(T_1, T_2, \ldots, T_L; i, b)$ is defined.

Finally, whenever $V(I_1, I_2, \ldots, I_L; i, b)$ is defined, put

$$\Lambda(I_1, \ldots, I_L; i, b) := \bigcup \Big(\Omega(V(T_1, \ldots, T_L; i, b)) \Big), \tag{27}$$

by taking the union over all $(T_1, T_2, \ldots, T_L) \in \mathcal{T}(I_1 \times I_2 \times \cdots \times I_L)$.

Let us say that an invariant subspace is *irreducible* if it is not spanned by the invariant subspaces properly contained in it. Then, with all the assumptions made so far, we obtain the following result:

Theorem 5 [10] *Let $\#F \geq n+2$ or $n = 2$. An invariant subspace $\mathcal{U}$ of the normal rational curve (9) is irreducible if, and only if, it can be written as*

$$\mathcal{U} := \operatorname{span}\{F\mathbf{c}_\lambda \mid \lambda \in \Lambda(I_1, \ldots, I_L; i, b)\}. \tag{28}$$

As the lattice of invariant subspaces has only finitely many elements, each invariant subspace is a join of irreducible ones.

Example 2 Let $n = 31$, $p = 3$ and $\#F \geq 33$. From $b = 32 = \langle 1012 \rangle$ we get

$$\begin{array}{rcl rcl}
V(0,32) & = & \langle 0 \rangle, & V(1,32) & = & \langle 2 \rangle, \\
V(3,32) & = & \langle 012 \rangle, & V(\{0\};3,32) & = & \langle 020 \rangle, \\
V(\{1\};3,32) & = & \langle 102 \rangle, & V(\{0,1\};3,32) & = & \langle 100 \rangle, \\
V(4,32) & = & \langle 1012 \rangle. & & &
\end{array}$$

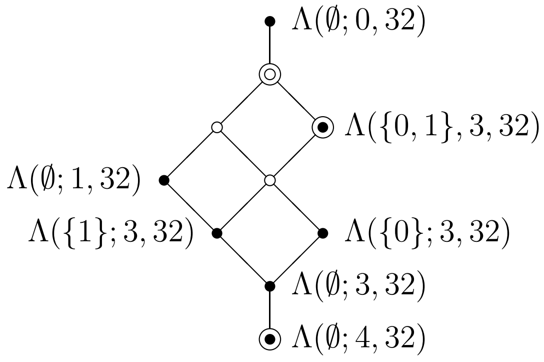
Note that, for example, $V(0,32) = V(\emptyset;0,32)$. Further $V(2,32) = V(3,32)$, $V(\{0\};2,32) = V(\{0\};3,32)$, and $V(I_1, I_2, \ldots, I_L; 4, 32) \geq 32$. So

$$\begin{aligned}
\Omega(\langle 0 \rangle) &= \{\langle 0 \rangle, \langle 1 \rangle, \ldots, \langle 1011 \rangle\}, \\
\Omega(\langle 2 \rangle) &= \{\langle 2 \rangle, \langle 12 \rangle, \langle 22 \rangle, \langle 102 \rangle, \langle 112 \rangle, \langle 122 \rangle, \langle 202 \rangle, \langle 212 \rangle, \langle 222 \rangle, \langle 1002 \rangle\}, \\
\Omega(\langle 12 \rangle) &= \{\langle 12 \rangle, \langle 22 \rangle, \langle 112 \rangle, \langle 122 \rangle, \langle 212 \rangle, \langle 222 \rangle\}, \\
\Omega(\langle 20 \rangle) &= \{\langle 20 \rangle, \langle 21 \rangle, \langle 22 \rangle, \langle 120 \rangle, \langle 121 \rangle, \langle 122 \rangle, \langle 220 \rangle, \langle 221 \rangle, \langle 222 \rangle\}, \\
\Omega(\langle 102 \rangle) &= \{\langle 102 \rangle, \langle 112 \rangle, \langle 122 \rangle, \langle 202 \rangle, \langle 212 \rangle, \langle 222 \rangle\}, \\
\Omega(\langle 100 \rangle) &= \{\langle 100 \rangle, \langle 101 \rangle, \ldots, \langle 222 \rangle\}, \\
\Omega(\langle 1012 \rangle) &= \emptyset,
\end{aligned}$$

are the relevant index sets and

$$\begin{array}{rcl}
\Lambda(\emptyset;0,32) & = & \Omega(\langle 0 \rangle), \\
\Lambda(\emptyset;1,32) & = & \Omega(\langle 2 \rangle), \\
\Lambda(\emptyset;3,32) & = & \Omega(\langle 12 \rangle), \\
\Lambda(\{0\};3,32) & = & \Omega(\langle 12 \rangle) \cup \Omega(\langle 20 \rangle) \\
\Lambda(\{1\};3,32) & = & \Omega(\langle 12 \rangle) \cup \Omega(\langle 102 \rangle) \\
\Lambda(\{0,1\};3,32) & = & \Omega(\langle 12 \rangle) \cup \Omega(\langle 20 \rangle) \cup \Omega(\langle 102 \rangle) \cup \Omega(\langle 100 \rangle) \\
\Lambda(\emptyset;4,32) & = & \emptyset.
\end{array}$$

The Hasse diagram of the lattice of invariant subspaces is given in the figure. Filled circles represent irreducible subspaces and double circles mark nuclei.


$\Lambda(\emptyset;0,32)$
$\Lambda(\{0,1\},3,32)$
$\Lambda(\emptyset;1,32)$
$\Lambda(\{1\};3,32)$
$\Lambda(\{0\};3,32)$
$\Lambda(\emptyset;3,32)$
$\Lambda(\emptyset;4,32)$

In many low-dimensional examples the invariant subspaces form a chain. In general, however, the following holds:

Theorem 6 [10] *Let the positions of the non-zero digits of $b := n+1$ in base p be denoted by $N_1, N_2, \ldots, N_d$. Then the lattice of invariant subspaces is totally ordered if, and only if, one of the following cases occurs:*

1. $d \in \{1, 2\}$.
2. $d \geq 3$, $N_d - N_1 = d - 1$, *and* $N_2 = \ldots = N_{d-1} = p - 1$.

Thus all invariant subspaces can be found, provided that the ground field is sufficiently large. Also, in specific cases the structure of the lattice of invariant subspaces is known.

Remark 4 If we project a NRC from one of its invariant subspaces other than $\mathcal{P}(\mathbf{Y})$, then a rational curve is obtained; this curve admits a collineation group isomorphic to $\mathrm{P\Gamma L}(2, F)$. Via (8) and the projection, the group actions on the curve and the projective line $\mathcal{P}(\mathbf{X})$ are similar.

4 Pascal's simplex modulo a prime

Throughout this section let p be a fixed prime. Given $m, t \in \mathbb{N}$ then put

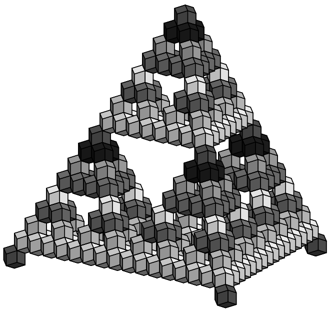
$$E_m^t := \{(e_0, e_1, \ldots, e_m) \in \mathbb{N}^{m+1} \mid e_0 + e_1 + \ldots + e_m = t\}. \tag{29}$$

The array of multinomial coefficients $\binom{t}{e_0, e_1, \ldots, e_m}$ with $(e_0, e_1, \ldots, e_m) \in E_m^t$ is frequently called *Pascal's simplex.*

The theorem of Lucas (2) can be generalized to multinomial coefficients as follows [4, 364]: If $t, e_0, e_1, \ldots, e_m \in \mathbb{N}$ have representations $t = \sum_\sigma t_\sigma p^\sigma$ and $e_i = \sum_\sigma e_{i,\sigma} p^\sigma$ in base p then

$$\binom{t}{e_0, e_1, \ldots, e_m} \equiv \prod_{\sigma \in \mathbb{N}} \binom{t_\sigma}{e_{0,\sigma}, e_{1,\sigma}, \ldots, e_{m,\sigma}} \pmod{p}. \tag{30}$$

For trinomial coefficients ($m = 3$) it is possible to illustrate Pascal's simplex in the form of a pyramid:



The picture above shows a part of Pascal's pyramid modulo 2. It is based upon a tiling of the space by rhombic dodecahedra. If an entry of the pyramid vanishes, then the corresponding dodecahedron is omitted. Entries at the same "horizontal" level (t constant) are equally shaded. Cf. [25].

The following has been established independently by F.T. Howard [30, Theorem 3.1] and N.A. Volodin [42, Theorem 2]; see also [43]:

The number of $(m+1)$–tuples $(e_0, e_1, \dots, e_m) \in E^t_m$ such that the multinomial coefficient $\binom{t}{e_0, e_1, \dots, e_m}$ is divisible by the prime p equals

$$\binom{m+t}{t} - \prod_{\sigma \in \mathbb{N}} \binom{m+t_\sigma}{t_\sigma}. \tag{31}$$

5 Veronese varieties

5.1 Definition of (r,k)-nuclei

Let $\{\mathbf{b}_0, \mathbf{b}_1, \dots, \mathbf{b}_m\}$ be a basis of an $(m+1)$-dimensional vector space $\mathbf{X}$ over F (the parameter space) and let $\mathbf{Y}$ be an $\binom{m+t}{t}$-dimensional vector space over F with a basis $\{\mathbf{c}_{e_0, e_1, \dots, e_m} \mid (e_0, e_1, \dots, e_m) \in E^t_m\}$; cf. (29). We shall always assume that $m \geq 1$ and $t \geq 2$ in order to avoid trivialities.

Generalizing (8), the *Veronese mapping* is given by

$$F\Big(\sum_{i=0}^{m} x_i \mathbf{b}_i\Big) \mapsto F\Big(\sum_{E^t_m} x_0^{e_0} x_1^{e_1} \dots x_m^{e_m} \mathbf{c}_{e_0, e_1, \dots, e_m}\Big) \;\; (x_i \in F). \tag{32}$$

Its image is a *Veronese variety* $\mathcal{V}^t_m$ with ambient space $\mathcal{P}(\mathbf{Y})$, i.e. the projective space on $\mathbf{Y}$. (By putting $m := 1$ and $n := t$ a NRC $\mathcal{V}^n_1$ is obtained.)

The Veronese image of each r-dimensional subspace of $\mathcal{P}(\mathbf{X})$ $(0 \leq r < m)$ is a sub-Veronesean $\mathcal{V}^t_r$ of $\mathcal{V}^t_m$. (For $r = 0$ we get just one point, for $r = 1$ a normal rational curve, etc. Cf. also [6].) For each $k \in \{-1, 0, \dots, t-1\}$ there exists a *k-osculating subspace of $\mathcal{V}^t_m$ along $\mathcal{V}^t_r$*. We call it an *(r,k)-osculating subspace* of $\mathcal{V}^t_m$. Its dimension equals

$$\sum_{i=t-k}^{t} \binom{r+i}{i} \binom{m+t-r-i-1}{t-i} - 1; \tag{33}$$

cf. [23] and the papers cited in Remark 1. We are thus led to the following definition:

Definition 3 The (r,k)-*nucleus* of a Veronese variety $\mathcal{V}^t_m$ is the intersection of all its (r,k)-osculating subspaces.

The k-nuclei of a normal rational curve are the $(0,k)$-nuclei according to the present definition.

Remark 5 A geometric characterization of quadratic Veronese mappings ($t = 2$) can be found in [22]. Combinatorial characterizations of the Veronese surface ($m = t = 2$) over a finite field and further references on this particular subject are given in [29]. Applications of Veronese varieties over finite fields in coding theory and authentication systems can be found in [13], [20], [21], [28], [37], [39], [45]. Partial linear spaces derived from Veronese varieties are discussed in [34].

5.2 Intersection of osculating hyperplanes

From (33), each $(t-1, m-1)$-osculating subspace of a Veronese variety $\mathcal{V}_m^t$ is a hyperplane of $\mathcal{P}(\mathbf{Y})$ which is called an *osculating hyperplane* (or *contact hyperplane*) of the Veronese variety $\mathcal{V}_m^t$. Thus to each hyperplane of the parameter space there corresponds an osculating hyperplane of the Veronesean. In terms of dual bases this *dual Veronese mapping* is given by

$$F\Big(\sum_{i=0}^{m} a_i \mathbf{b}_i^*\Big) \mapsto F\Big(\sum_{E_m^t} \tbinom{t}{e_0, e_1, \ldots, e_m} a_0^{e_0} a_1^{e_1} \ldots a_m^{e_m} \mathbf{c}^*_{e_0, e_1 \ldots, e_m}\Big) \ \ (a_i \in F). \tag{34}$$

See also [5, pp. 160–163]. The intersection of all osculating hyperplanes of a $\mathcal{V}_m^t$ is its $(m-1, t-1)$-nucleus. Both A. Herzer [23] and H. Karzel [32] determined all Veronese varieties where this specific nucleus is empty.

Theorem 7 [11] *The $(m-1, t-1)$-nucleus of a Veronese variety $\mathcal{V}_m^t$ contains exactly those base points $F\mathbf{c}_{e_0, e_1, \ldots, e_m}$ satisfying*

$$\binom{t}{e_0, e_1, \ldots, e_m} \equiv 0 \pmod{\operatorname{char} F}. \tag{35}$$

If $\#F \geq t$, then this nucleus is spanned by those base points.

From this and (31) follows

Theorem 8 [11] *Let $\sum_{\sigma \in \mathbb{N}} t_\sigma p^\sigma$ be the representation of t in base $p = \operatorname{char} F > 0$. If $\#F \geq t$, then the $(m-1, t-1)$-nucleus of a Veronese variety $\mathcal{V}_m^t$ has dimension*

$$\binom{m+t}{t} - \prod_{\sigma \in \mathbb{N}} \binom{m + t_\sigma}{t_\sigma} - 1. \tag{36}$$

Example 3 Let $\operatorname{char} F = 2$.

The $(1,1)$-nucleus of the Veronese surface $\mathcal{V}_2^2$ is a plane; cf. [29, Chapter 25].

From Theorem 8 the $(1,2)$-nucleus of the Veronese surface $\mathcal{V}_2^3$ is a single point provided that $\#F \neq 2$. On the other hand, if $\#F = 2$ then, by solving a system of seven linear equations, the $(1,2)$-nucleus of $\mathcal{V}_2^3$ is easily seen to be three-dimensional. In either case $\mathcal{V}_2^3$ carries a family of twisted cubics that arise as Veronese images of the lines in the parameter plane. For $\#F \neq 2$ the 2-nucleus of a twisted cubic is empty, but for $\#F = 2$ this nucleus is a single point.

References

[1] E. Bertini. *Introduzione alla geometria proiettiva degli iperspazi.* E. Spoerri, Pisa, 1907.

[2] E. Bertini. *Einführung in die projektive Geometrie mehrdimensionaler Räume.* Seidel u. Sohn, Wien, 1924.

[3] H. Brauner. *Geometrie projektiver Räume II.* BI-Wissenschaftsverlag, Mannheim Wien Zürich, 1976.

[4] A.E. Brouwer and H.A. Wilbrink. Block designs. In F. Buekenhout, editor, *Handbook of incidence geometry*, chapter 8, pages 349–382. Elsevier, Amsterdam, 1995.

[5] W. Burau. *Mehrdimensionale projektive und höhere Geometrie.* Dt. Verlag d. Wissenschaften, Berlin, 1961.

[6] W. Burau. Über ausgezeichnete Aufspaltungen des Raumes einer Veroneseschen V_n^t und ihre Anwendung auf die Berechnung der Hilbertfunktion der rationalen Normregelmannigfaltigkeiten. *Veröff. Univ. Innsbruck*, 91:17–28, 1974.

[7] N.J. Fine. Binomial coefficients modulo a prime. *Am. Math. Mon.*, 54:589–592, 1947.

[8] D.G. Glynn. The non-classical 10-arc of $\mathrm{PG}(4, 9)$. *Discrete Math.*, 59:43–51, 1986.

[9] J. Gmainer. *Rationale Normkurven in Räumen mit positiver Charakteristik.* Thesis, Vienna University of Technology, 1999.

[10] J. Gmainer. Pascal's triangle, normal rational curves, and their invariant subspaces. *Eur. J. Comb.*, 22:37–49, 2001.

[11] J. Gmainer and H. Havlicek. A dimension formula for the nucleus of a Veronese variety. *Lin. Algebra Appl.*, 305:191–201, 2000.

[12] J. Gmainer and H. Havlicek. Nuclei of normal rational curves. *J. Geometry*, 69:117–130, 2000.

[13] V.D. Goppa. *Geometry and codes.* Kluwer, Dordrecht Boston London, 1988.

[14] H. Harborth. Über die Teilbarkeit im Pascal-Dreieck. *Math.-phys. Semesterber.*, 22:13–21, 1975.

[15] H. Hasse. Noch eine Begründung der Theorie der höheren Differentialquotienten in einem algebraischen Funktionenkörper einer Unbestimmten. *J. Reine Angew. Math.*, 177:215–237, 1937.

[16] H. Havlicek. Normisomorphismen und Normkurven endlichdimensionaler projektiver Desargues-Räume. *Monatsh. Math.*, 95:203–218, 1983.

[17] H. Havlicek. Die automorphen Kollineationen nicht entarteter Normkurven. *Geom. Dedicata*, 16:85–91, 1984.

[18] H. Havlicek. Erzeugnisse projektiver Bündelisomorphismen. *Ber. Math.-Stat. Sekt. Forschungszent. Graz*, 215, 1984.

[19] H. Havlicek. Applications of results on generalized polynomial identities in desarguesian projective spaces. In R. Kaya, P. Plaumann, and K. Strambach, editors, *Rings and geometry*, pages 39–77. D. Reidel, Dordrecht, 1985.

[20] H. Havlicek. The Veronese surface in $\mathrm{PG}(5, 3)$ and Witt's 5-$(12, 6, 1)$–design. *J. Comb. Theory, Ser. A*, 84(1):87–94, 1998.

[21] H. Havlicek. Giuseppe Veronese and Ernst Witt – neighbours in PG(5,3). *Aequationes Math.*, 58:85–92, 1999.

[22] H. Havlicek and C. Zanella. Quadratic embeddings. *Beitr. Algebra Geom.*, 38:289–298, 1997.

[23] A. Herzer. Die Schmieghyperebenen an die Veronese-Mannigfaltigkeit bei beliebiger Charakteristik. *J. Geom.*, 18:140–154, 1982.

[24] E. Hexel and H. Sachs. Counting residues modulo a prime in Pascal's triangle. *Indian J. Math.*, 20:91–105, 1978.

[25] P. Hilton and J. Pedersen. Relating geometry and algebra in the pascal triangle, hexagon, tetrahedron, and cuboctahedron Part 1: Binomial coefficients, extended binomial coefficients and preparation for further work. *College Mathematics Journal*, 30(3):170–186, 1999.

[26] J.W.P. Hirschfeld. *Finite projective spaces of three dimensions.* Oxford University Press, Oxford, 1985.

[27] J.W.P. Hirschfeld. *Projective geometries over finite fields.* Clarendon Press, Oxford, second edition, 1998.

[28] J.W.P. Hirschfeld and L. Storme. The packing problem in statistics, coding theory, and finite projective spaces. *J. Stat. Plann. Inference*, 72(1–2):355–380, 1998.

[29] J.W.P. Hirschfeld and J.A. Thas. *General Galois geometries.* Oxford University Press, Oxford, 1991.

[30] F.T. Howard. The number of multinomial coefficients divisible by a fixed power of a prime. *Pac. J. Math.*, 50:99–108, 1974.

[31] V.V. Karachik. p-latin matrices and Pascal's triangle modulo a prime. *Fibonacci Q.*, 34(4):362–372, 1996.

[32] H. Karzel. Über einen Fundamentalsatz der synthetischen algebraischen Geometrie von W. Burau und H. Timmermann. *J. Geom.*, 28:86–101, 1987.

[33] C.T. Long. Pascal's triangle modulo p. *Fibonacci Q.*, 19:458–463, 1981.

[34] N. Melone. Veronese spaces. *J. Geom.*, 20:169–180, 1983.

[35] R. Riesinger. Normkurven in endlichdimensionalen Desarguesräumen. *Geom. Dedicata*, 10:427–449, 1981.

[36] J.B. Roberts. On binomial coefficient residues. *Canadian J. Math.*, 9:363–370, 1957.

[37] L. Storme and J.A. Thas. k-arcs and dual k-arcs. *Discrete Math.*, 125, No.1–3:357–370, 1994.

[38] J.A. Thas. Normal rational curves and $(q+2)$–arcs in a Galois space $S_{q-2,q}$ $(q = 2^h)$. *Atti Accad. Naz. Lincei, VIII. Ser., Rend., Cl. Sci. Fis. Mat. Nat.*, 47:249–252, 1969.

[39] J.A. Thas. M.D.S. codes and arcs in projective spaces: A survey. *Le Matematiche*, 47(2):315–328, 1992.

[40] H. Timmermann. Descrizioni geometriche sintetiche di geometrie proiettive con caratteristica $p > 0$. *Ann. Mat. Pura Appl. IV. Ser.*, 114:121–139, 1977.

[41] H. Timmermann. *Zur Geometrie der Veronesemannigfaltigkeit bei endlicher Charakteristik.* Habilitationsschrift, Univ. Hamburg, 1978.

[42] N.A. Volodin. Distribution of polynomial coefficients congruent modulo p^N. *Math. Notes*, 45:195–199, 1989.

[43] N.A. Volodin. Number of multinomial coefficients not divisible by a prime. *Fibonacci Q.*, 32(5):402–406, 1994.

[44] S. Wolfram. Geometry of binomial coefficients. *Am. Math. Mon.*, 91:566–571, 1984.

[45] C. Zanella. Linear sections of the finite Veronese varieties and authentication systems defined using geometry. *Des. Codes Cryptography*, 13(2):199–212, 1998.

[46] J. Zeuge. Eine geometrische Kennzeichnung der Mannigfaltigkeiten von Segre und Veronese und eine damit zusammenhängende ausgezeichnete Transformation zwischen gewissen projektiven Räumen. *Atti Accad. naz. Lincei, VIII. Ser., Rend., Cl. Sci. fis. Mat. natur.*, 53:531–540, 1972.

[47] J. Zeuge. Die Schmiegräume an die Veronesemannigfaltigkeit. *Mitt. Math. Ges. Hamburg*, 10(5):391–393, 1977.

Hans Havlicek, Abteilung für Lineare Geometrie, Technische Universität, Wiedner Hauptstraße 8–10, A-1040 Wien, Austria.
Email: havlicek@geometrie.tuwien.ac.at
Web site: http://www.geometrie.tuwien.ac.at/havlicek