Osculating Spaces of Varieties and Linear Network Codes

Johan P. Hansen

Department of Mathematics, Aarhus University[*], matjph@imf.au.dk

Abstract. We present a general theory to obtain good linear network codes utilizing the osculating nature of algebraic varieties. In particular, we obtain from the osculating spaces of Veronese varieties explicit families of equidimensional vector spaces, in which any pair of distinct vector spaces intersect in the same dimension.
Linear network coding transmits information in terms of a basis of a vector space and the information is received as a basis of a possible altered vector space. Ralf Koetter and Frank R. Kschischang [KK08] introduced a metric on the set of vector spaces and showed that a minimal distance decoder for this metric achieves correct decoding if the dimension of the intersection of the transmitted and received vector space is sufficiently large.
The proposed osculating spaces of Veronese varieties are equidistant in the above metric. The parameters of the resulting linear network codes are determined.

Notation

- $\mathbb{F}_q$ is the finite field with q elements of characteristic p.
- $\mathbb{F} = \overline{\mathbb{F}_q}$ is an algebraic closure of $\mathbb{F}_q$.
- $R_d = \mathbb{F}[X_0, \dots, X_n]_d$ and $R_d(\mathbb{F}_q) = \mathbb{F}_q[X_0, \dots, X_n]_d$ the homogenous polynomials of degree d with coefficients in $\mathbb{F}$ and $\mathbb{F}_q$.
- $R = \mathbb{F}[X_0, \dots, X_n] = \oplus_d R_d$ and $R(\mathbb{F}_q) = \mathbb{F}_q[X_0, \dots, X_n] = \oplus_d R_d(\mathbb{F}_q)$
- $\mathrm{AffCone}(Y) \subseteq \mathbb{F}^{M+1}$ denotes the affine cone of the subvariety $Y \subseteq \mathbb{P}^M$ and $\mathrm{AffCone}(Y)(\mathbb{F}_q)$ its $\mathbb{F}_q$-rational points.
- $O_{k,X,P} \subseteq \mathbb{P}^M$ is the embedded k-osculating space of a variety $X \subseteq \mathbb{P}^M$ at the point $P \in X$ and $O_{k,X,P}(\mathbb{F}_q)$ its $\mathbb{F}_q$-rational points, see 2.
- $\mathcal{V} = \sigma_d(\mathbb{P}^n) \subseteq \mathbb{P}^M$ with $M = \binom{d+n}{n} - 1$ is the Veronese variety, see 1.1.

For generalities on algebraic geometry we refer to [Har77].

---

[*] Part of this work was done while visiting Institut de Mathématiques de Luminy, MARSEILLE, France.

1 Introduction

Algebraic varieties have in general an osculating structure. By Terracini's lemma [Ter11], their embedded tangent spaces tend to be in general position. Specifically, the tangent space at a generic point $P \in \overline{Q_1 Q_2}$ on the secant variety of points on some secant is spanned by the tangent spaces at Q_1 and Q_2. In general, the secant variety of points on some secant have the expected maximal dimension and therefore the tangent spaces generically span a space of maximal dimension, see [Zak93].

This paper suggests k-osculating spaces including tangent spaces of algebraic varieties as a source for constructing linear subspaces in general position of interest for linear network coding. The k-osculating spaces are presented in 1.1.

In particular, we will present the k-osculating subspaces of Veronese varieties and apply them to obtain linear network codes generalizing the results in [Han12]. The Veronese varieties are presented in 2.

Definition 1 *Let $X \subseteq \mathbb{P}^M$ be a smooth projective variety of dimension n defined over the finite field $\mathbb{F}_q$ with q elements. For each positive integer k we define the k-osculating linear network code $\mathcal{C}_{k,X}$. The elements of the code are the linear subspaces in $\mathbb{F}_q^{M+1}$ which are the affine cones of the k-osculating subspaces $O_{k,X,P}(\mathbb{F}_q)$ at $\mathbb{F}_q$-rational points P on X, as defined in 1.1.*

Specifically

$$\mathcal{C}_{k,X} = \{\mathrm{AffCone}(O_{k,X,P})(\mathbb{F}_q) \mid P \in X(\mathbb{F}_q)\} .$$

The number of elements in $\mathcal{C}_{k,X}$ is by construction $|X(\mathbb{F}_q)|$, the number of $\mathbb{F}_q$-rational points on X.

One should remark that the elements in $\mathcal{C}_{k,X}$ are not necessarily equidimensional as linear vector spaces, however, their dimension is at most $\binom{k+n}{n}$.

Applying the construction to the Veronese variety $\mathcal{X}_{n,d}$ presented in 2, we obtain a linear network code $\mathcal{C}_{k,\mathcal{X}_{n,d}}$ and the following result, which is proved in section 2.1.

Theorem 2 *Let n, d be positive integers and consider the Veronese variety $\mathcal{X}_{n,d} \subseteq \mathbb{P}^M$, with $M = \binom{d+n}{n} - 1$, defined over the finite field $\mathbb{F}_q$ as in 2.*

Let $\mathcal{C}_{k,\mathcal{X}_{n,d}}$ be the associated k-osculating linear network code, as defined in Definition 1.

The packet length of the linear network code is $\binom{d+n}{n}$, the dimension of the ambient vector space. The number of vector spaces in the linear network code $\mathcal{C}_{k,\mathcal{X}_{n,d}}$ is $|\mathbb{P}^n(\mathbb{F}_q)| = 1 + q + q^2 + \cdots + q^n$, the number of $\mathbb{F}_q$-rational points on $\mathbb{P}^n$.

The vector spaces $V \in \mathcal{C}_{k,\mathcal{X}_{n,d}}$ in the linear network code are equidimensional of dimension $\binom{k+n}{n}$ as linear subspaces of the ambient $\binom{d+n}{n}$-dimensional $\mathbb{F}_q$-vector space.

The elements in the code are equidistant in the metric $\mathrm{dist}(V_1, V_2)$ of (5) of Section 3. Specifically, we have the following results.

For vector spaces $V_1, V_2 \in \mathcal{C}_{k,\mathcal{X}_{n,d}}$ with $V_1 \neq V_2$

i) if $2k \geq d$, then $\dim_{\mathbb{F}_q}(V_1 \cap V_2) = \binom{2k-d+n}{n}$ and

$$\mathrm{dist}(V_1, V_2) = 2 \left(\binom{k+n}{n} - \binom{2k-d+n}{n} \right).$$

ii) if $2k \leq d$, then $\dim_{\mathbb{F}_q}(V_1 \cap V_2) = 0$ and

$$\mathrm{dist}(V_1, V_2) = 2 \binom{k+n}{n}.$$

1.1   Osculating spaces

Principal Parts. Let X be a smooth variety of dimension n defined over the field K and let $\mathcal{F}$ be a locally free $\mathcal{O}_X$-module. The sheaves of k-principal parts $\mathcal{P}_X^k(\mathcal{F})$ are locally free and if $\mathcal{L}$ is of rank 1, then $\mathcal{P}_X^k(\mathcal{L})$ is a locally free sheaf of rank $\binom{k+n}{n}$.

There are the fundamental exact sequences

$$0 \to S^k \Omega_X \otimes_{\mathcal{O}_X} \mathcal{F} \to \mathcal{P}_X^k(\mathcal{F}) \to \mathcal{P}_X^{k-1}(\mathcal{F}) \to 0 \ ,$$

where Ω_X is the sheaf of differentials on X and $S^k \Omega_X$ its kth symmetric power. These sequences can be used to give a local description of the sheaf principal parts. Specifically, if $\mathcal{L}$ is of rank 1, then $\mathcal{P}_X^k(\mathcal{L})$

is a locally free sheaf of rank $\binom{k+n}{n}$. Assume furthermore that X is affine with coordinate ring $A = K[x_1, \ldots, x_n]$, then X and $\mathcal{L}$ can be identified with A. Also $S^k \Omega_X$ can be identified with the forms of degree k in $A[dx_1, \ldots, dx_n]$ in the indeterminates $dx_1, \ldots dx_n$ and $\mathcal{P}_X^k(\mathcal{L})$ with the polynomials of total degree $\leq k$ in the indeterminates $dx_1, \ldots dx_n$. For arbitrary X, the local picture is similar, taking local coordinates $x_1, \ldots, x_n$ at the point in question replacing A by the completion of the local ring at that point.

In general, for each k there is a canonical morphism

$$d_k : \mathcal{F} \to \mathcal{P}_X^k(\mathcal{F}) \ .$$

For $\mathcal{L}$ of rank 1, using local coordinates as above, d_k maps an element in A to its truncated Taylor series

$$f = f(x_1, \ldots, x_n) \mapsto \sum_{|\alpha| \leq k} \frac{1}{|\alpha|!} \frac{\partial^{|\alpha|} f}{\partial x^\alpha} \ ,$$

where $\alpha = i_1 i_2 \ldots i_n$ and $|\alpha| = i_1 + i_2 + \cdots + i_n$.

Osculating Spaces. Let X be a smooth variety of dimension n and let $f : X \to \mathbb{P}^M$ be an immersion. For $\mathcal{L} = f^* \mathcal{O}_{\mathbb{P}^n}(1)$ let $\mathcal{P}_X^k(\mathcal{L})$ denote the sheaf of principal parts of order k. Then $\mathcal{P}_X^k(\mathcal{L})$ is a locally free sheaf of rank $\binom{k+n}{n}$ and there are homomorphisms

$$a^k : \mathcal{O}_X^{M+1} \to \mathcal{P}_X^k(\mathcal{L}) \ .$$

For $P \in X$ the morphism $a^k(P)$ defines the k-osculating space $O_{k,X,P}$ to X at P as

$$O_{k,X,P} := \mathbb{P}(\mathrm{Im}(a^k(P))) \subseteq \mathbb{P}^M \qquad (1)$$

of projective dimension at most $\binom{k+n}{n} - 1$, see [Pie77], [BPT92] and [PT90]. For $k = 1$ the osculating space is the tangent space to X at P.

2 The Veronese variety

Let $R_1 = \mathbb{F}[X_0, \ldots, X_n]_1$ be the $n+1$ dimensional vector space of linear forms in $X_0, \ldots, X_n$ and let $\mathbb{P}^n = \mathbb{P}(R_1)$ be the associated projective n-space over $\mathbb{F}$.

For each integer $d \geq 1$, consider R_d the vector space of forms of degree d. A basis consists of the $\binom{n+d}{d}$ monomials $X_0^{d_0} X_1^{d_1} \ldots X_n^{d_n}$ with $d_0 + d_1 + \cdots + d_n = d$. Let $\mathbb{P}^M = \mathbb{P}(R_d)$ be the associated projective space of dimension $M = \binom{n+d}{d} - 1$.

The d-uple morphism of $\mathbb{P}^n = \mathbb{P}(R_1)$ to $\mathbb{P}^M = \mathbb{P}(R_d)$ is the morphism

$$\sigma_d : \mathbb{P}^n = \mathbb{P}(R_1) \to \mathbb{P}^M = \mathbb{P}(R_d)$$
$$L \mapsto L^d$$

with image the Veronese variety

$$\mathcal{X}_{n,d} = \sigma_d(\mathbb{P}^n) = \{L^d | \ L \in \mathbb{P}(R_1)\} \subseteq \mathbb{P}^M. \tag{2}$$

2.1 Osculating subspaces of the Veronese variety

For the Veronese variety $\mathcal{X}_{n,d}$ of (2), the k-osculating subspaces of (1) with $1 \leq k < d$, at the point $P \in \mathcal{X}_{n,d}$ corresponding to the 1-form $L \in R_1$, can be described explicitly as

$$O_{k,\mathcal{X}_{n,d},P} = \mathbb{P}(\{L^{d-k}F | \ F \in R_k\}) = \mathbb{P}(R_k) \subseteq \mathbb{P}^M \tag{3}$$

of projective dimension exactly $\binom{k+n}{n} - 1$, see [Seg46], [CGG02], [BCGI07] and [BF03]. The osculating spaces constitute a flag of linear subspaces

$$O_{1,\mathcal{X}_{n,d},P} \subseteq O_{2,\mathcal{X}_{n,d},P} \subseteq \cdots \subseteq O_{d-1,\mathcal{X}_{n,d},P} \ .$$

This explicit description of the k-osculating spaces allows us to establish the claims in Theorem 2.

The associated affine cone of the k-osculating space in (3) is

$$\mathrm{AffCone}(O_{k,\mathcal{X}_{n,d},P})(\mathbb{F}_q) = \{L^{d-k}F | \ F \in R_k\} \tag{4}$$

of dimension $\binom{k+n}{n}$, proving the claim on the dimension of the vector spaces in the linear network code $\mathcal{C}_{k,\mathcal{X}_{n,d}}$.

As there is one element in $\mathcal{C}_{k,\mathcal{X}_{n,d}}$ for each $\mathbb{F}_q$-rational point on $\mathbb{P}^n$, it follows that the number of elements in $\mathcal{C}_{k,\mathcal{X}_{n,d}}$ is

$$|\mathcal{C}_{k,\mathcal{X}_{n,d}}| = |\mathbb{P}^n(\mathbb{F}_q)| = 1 + q + q^2 + \cdots + q^n \ .$$

Finally, let $V_1, V_2 \in \mathcal{C}_{k, \mathcal{X}_{n,d}}$ with $V_1 \neq V_2$ and

$$V_i = \{L_i^{d-k} F_i | \ F_i \in R_k\}$$

If $2k \geq d$, we have

$$
\begin{aligned}
V_1 \cap V_2 &= \{L_1^{d-k} F_1 | \ F_1 \in R_k\} \cap \{L_2^{d-k} F_2 | \ F_2 \in R_k\} \\
&= \{L_1^{d-k} L_2^{d-k} G | \ G \in R_{2k-d}\} \ .
\end{aligned}
$$

Otherwise the intersection is trivial, proving the claims on the dimension of the intersections and the derived distances.

3 Linear network coding

In linear network, coding transmission is obtained by transmitting a number of packets into the network and each packet is regarded as a vector of length N over a finite field $\mathbb{F}_q$. The packets travel the network through intermediate nodes, each forwarding $\mathbb{F}_q$-linear combinations of the packets it has available. Eventually the receiver tries to infer the originally transmitted packages from the packets that are received, see [CWJJ03] and [HMK$^+$06].

All packets are vectors in $\mathbb{F}_q^N$; however, Ralf Koetter and Frank R. Kschischang [KK08] describe a transmission model in terms of linear subspaces of $\mathbb{F}_q^N$ spanned by the packets and they define a fixed dimension *code* as a nonempty subset $\mathcal{C} \subseteq G(n, N)(\mathbb{F}_q)$ of the Grassmannian of n-dimensional $\mathbb{F}_q$-linear subspaces of $\mathbb{F}_q^N$. They endowed the Grassmannian $G(n, N)(\mathbb{F}_q)$ with the metric

$$\text{dist}(V_1, V_2) := \dim_{\mathbb{F}_q}(V_1 + V_2) - \dim_{\mathbb{F}_q}(V_1 \cap V_2), \qquad (5)$$

where $V_1, V_2 \in G(n, N)(\mathbb{F}_q)$.

The size of the code $\mathcal{C} \subseteq G(n, N)(\mathbb{F}_q)$ is denoted by $|\mathcal{C}|$, the minimal distance by

$$D(\mathcal{C}) := \min_{V_1, V_2 \in \mathcal{C}, V_1 \neq V_2} \text{dist}(V_1, V_2) \qquad (6)$$

and $\mathcal{C}$ is said to be of type $[N, n, \log_q |\mathcal{C}|, D(\mathcal{C})]$. Its normalized weight is $\lambda = \frac{n}{N}$, its rate is $R = \frac{\log_q(|\mathcal{C}|)}{Nn}$ and its normalized minimal distance is $\delta = \frac{D(\mathcal{C})}{2n}$.

They showed that a minimal distance decoder for this metric achieves correct decoding if the dimension of the intersection of the transmitted and received vector-space is sufficiently large. Also they obtained Hamming, Gilbert-Varshamov and Singleton coding bounds.

References

[BCGI07] A. Bernardi, M. V. Catalisano, A. Gimigliano, and M. Idà. Osculating varieties of Veronese varieties and their higher secant varieties. *Canad. J. Math.*, 59(3):488–502, 2007.

[BF03] E. Ballico and C. Fontanari. On the secant varieties to the osculating variety of a Veronese surface. *Cent. Eur. J. Math.*, 1(3):315–326, 2003.

[BPT92] E. Ballico, R. Piene, and H. Tai. A characterization of balanced rational normal surface scrolls in terms of their osculating spaces. II. *Math. Scand.*, 70(2):204–206, 1992.

[CGG02] M. V. Catalisano, A. V. Geramita, and A. Gimigliano. On the secant varieties to the tangential varieties of a Veronesean. *Proc. Amer. Math. Soc.*, 130(4):975–985, 2002.

[CWJJ03] P. A. Chou, Y. Wu and K. Jain. Practical network coding. 2003.

[Han12] J. P. Hansen. Equidistant linear network codes with maximal error-protection from veronese varieties. *http://arxiv.org*, abs/1207.2083, 2012.

[Har77] R. Hartshorne. *Algebraic geometry*. Springer-Verlag, New York, 1977. Graduate Texts in Mathematics, No. 52.

[HMK^{+}06] T. Ho, M. Médard, R. Koetter, D. R. Karger, M. Effros, J. Shi, and B. Leong. A random linear network coding approach to multicast. *IEEE TRANS. INFORM. THEORY*, 52(10):4413–4430, 2006.

[KK08] R. Koetter and F. R. Kschischang. Coding for errors and erasures in random network coding. *IEEE Transactions on Information Theory*, 54(8):3579–3591, 2008.

[Pie77] R. Piene. Numerical characters of a curve in projective n-space. In *Real and complex singularities (Proc. Ninth Nordic Summer School/NAVF Sympos. Math., Oslo, 1976)*, pages 475–495. Sijthoff and Noordhoff, Alphen aan den Rijn, 1977.

[PT90] R. Piene and H. Tai. A characterization of balanced rational normal scrolls in terms of their osculating spaces. In *Enumerative geometry (Sitges, 1987)*, volume 1436 of *Lecture Notes in Math.*, pages 215–224. Springer, Berlin, 1990.

[Seg46] B. Segre. Un'estensione delle varietà di Veronese, ed un principio di dualità per forme algebriche. I. *Atti Accad. Naz. Lincei. Rend. Cl. Sci. Fis. Mat. Nat. (8)*, 1:313–318, 1946.

[Ter11] A. Terracini. Sulle v_k per cui la variet'a degli $s_h - h + 1$ seganti ha dimensione minore dell'ordinario. *Rend. Circ. Mat. Palermo*, 31:392–396, 1911.

[Zak93] F. L. Zak. *Tangents and secants of algebraic varieties*, volume 127 of *Translations of Mathematical Monographs*. American Mathematical Society, Providence, RI, 1993. Translated from the Russian manuscript by the author.