Osculating Spaces of Varieties
Linear Network Codes

Johan P. Hansen

Department of Mathematics, Aarhus University, DENMARK
matjph@imf.au.dk
Part of this work was done while visiting
Institut de Mathématiques de Luminy, MARSEILLE, France.

5th International Conference on Algebraic Informatics,
Aix-Marseille University - ERISCS - IML, 2013
Introduction

Idea and construction

Osculating spaces

d-uple embedding and the Veronese variety

The bibliography

Outline

1. Introduction
   - Abstract
   - Linear network coding
   - Notation
2. Idea and construction
   - Terracinis lemma
   - Linear network codes from osculating spaces
3. Osculating spaces
   - Principal Parts.
   - Definition of osculating spaces
4. d-uple embedding and the Veronese variety
   - Definition of the Veronese variety
   - Osculating subspaces of the Veronese variety
   - Network codes from the Veronese variety
5. The bibliography
Abstract

- We present a general theory to obtain linear network codes utilizing the *osculating* nature of algebraic varieties.
- From the osculating spaces of Veronese varieties, we obtain families of vector spaces constituting linear network codes.
- *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 introduced a metric on the set of vector spaces.
- The osculating spaces of Veronese varieties are equidistant in the above metric.
Transmission is obtained by transmitting a number of packets into the network - a packet is 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.

Koetter and Kschischang describe a transmission model in terms of linear subspaces of $\mathbb{F}_q^N$ spanned by the packets and they define a 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 $\mathbb{F}_q^N$ and endowed $G(n, N)(\mathbb{F}_q)$ with the metric

$$\text{dist}(V_1, V_2) := \dim_{\mathbb{F}_q}(V_1 + V_2) - \dim_{\mathbb{F}_q}(V_1 \cap V_2).$$
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.
**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 \( \mathbb{F}_q \).
- \( R_d = \mathbb{F}[X_0, \ldots, X_n]_d \) and \( R_d(\mathbb{F}_q) = \mathbb{F}_q[X_0, \ldots, X_n]_d \) the homogenous polynomials of degree \( d \) with coefficients in \( \mathbb{F} \) and \( \mathbb{F}_q \).
- \( R = \mathbb{F}[X_0, \ldots, X_n] = \bigoplus_d R_d \) and
  \[
  R(\mathbb{F}_q) = \mathbb{F}_q[X_0, \ldots, X_n] = \bigoplus_d R_d(\mathbb{F}_q)
  \]
- \( \text{AffCone}(Y) \subseteq \mathbb{F}^{M+1} \) denotes the affine cone of \( Y \subseteq \mathbb{P}^M \) and \( \text{AffCone}(Y)(\mathbb{F}_q) \) 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.
- \( \mathcal{V} = \sigma_d(\mathbb{P}^n) \subseteq \mathbb{P}^M \) with \( M = \binom{d+n}{n} - 1 \) is the Veronese variety.
Terracinis lemma

- Algebraic varieties have in general an osculating structure. By *Terracini’s lemma* their embedded tangent spaces tend to be in general position. Specifically, the tangent space at a generic point \( P \in Q_1Q_2 \) 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.

- We suggest *osculating spaces* (including *tangent spaces*) of algebraic varieties as a source for constructing linear subspaces in general position of interest for linear network coding.
Codes from osculating spaces

Definition

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 $C_{k,X}$. 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 $X$. Specifically

$$C_{k,X} = \left\{ \text{AffCone}(O_{k,X,P})(\mathbb{F}_q) \mid P \in X(\mathbb{F}_q) \right\}.$$ 

The number of elements in $C_{k,X}$ is the number of $\mathbb{F}_q$-rational points on $X$.

The vector spaces in $C_{k,X}$ have dimension at most $(k+n)$. 

Johan P. Hansen
Osculating Spaces of Varieties and Linear Network Codes
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 $\mathcal{P}^k_X(\mathcal{F})$ are locally free and if $\mathcal{L}$ is of rank 1, then $\mathcal{P}^k_X(\mathcal{L})$ is a locally free sheaf of rank $\binom{k+n}{n}$. There are the fundamental exact sequences

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

where $\Omega_X$ is the sheaf of differentials on $X$ and $S^k\Omega_X$ its $k$th symmetric power.
If $\mathcal{L}$ is of rank 1, then $\mathbb{P}^k_X(\mathcal{L})$ is a locally free sheaf of rank $\binom{k+n}{n}$. If $X$ is affine with coordinate ring $A = K[x_1, \ldots, x_n]$, then

- $X$ and $\mathcal{L}$ can be identified with $A$.
- $S^k\Omega_X$ can be identified with the forms of degree $k$ in $A[dx_1, \ldots, dx_n]$ in the indeterminates $dx_1, \ldots, dx_n$.
- $\mathbb{P}^k_X(\mathcal{L})$ can be identified 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

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

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 $|\alpha| = i_1 + i_2 + \cdots + i_n$. 
Let $X$ be a smooth of dimension $n$ and $f : X \to \mathbb{P}^M$ 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 $k$. There are homomorphisms

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

**Definition**

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

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

*of projective dimension at most $\binom{k+n}{n} - 1$. For $k = 1$ the osculating space is the tangent space.*
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 $X_0, \ldots, X_n$.
- $\mathbb{P}^n = \mathbb{P}(R_1)$, the associated projective $n$-space over $\mathbb{F}$.
- $R_d$ the vector space of forms of degree $d$. A basis consists of the $\binom{n+d}{d}$ monomials $X_0^{d_0} X_1^{d_1} \cdots X_n^{d_n}$ with $d_0 + d_1 + \cdots + d_n = d$.
- $\mathbb{P}^M = \mathbb{P}(R_d)$ the associated projective space of dimension $M = \binom{n+d}{d} - 1$. 
Definition

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

$$\sigma_d : \mathbb{P}^n = \mathbb{P}(R_1) \rightarrow \mathbb{P}^M = \mathbb{P}(R_d)$$

$L \mapsto L^d$

with image the Veronese variety

$$\chi_{n,d} = \sigma_d(\mathbb{P}^n) = \{L^d | L \in \mathbb{P}(R_1)\} \subseteq \mathbb{P}^M.$$
For the Veronese variety $\mathcal{X}_{n,d}$, the $k$-osculating subspaces $(1 \leq k < d)$ at the point $P \in \mathcal{X}_{n,d}$ corresponding to the 1-form $L \in R_1$, can be described explicitly as

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

of projective dimension exactly $\binom{k+n}{n} - 1$.

The osculating spaces constitute a flag of linear subspaces

$$O_1, \mathcal{X}_{n,d}, P \subseteq O_2, \mathcal{X}_{n,d}, P \subseteq \cdots \subseteq O_{d-1}, \mathcal{X}_{n,d}, P.$$
The construction applied to the Veronese variety

Theorem

Let \( n, d \) be positive integers and consider the Veronese variety \( \mathcal{X}_{n,d} \subseteq \mathbb{P}^M \), with \( M = \left( \binom{d+n}{n} - 1 \right) \), defined over the finite field \( \mathbb{F}_q \). Let \( \mathcal{C}_{k,\mathcal{X}_{n,d}} \) be the associated \( k \)-osculating linear network code.

The packet length of the linear network code is \( \left( \binom{d+n}{n} \right) \), 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

\[
|\mathbb{P}^n(\mathbb{F}_q)| = 1 + q + q^2 + \cdots + q^n, \text{ the number of } \mathbb{F}_q\text{-rational points on } \mathbb{P}^n.
\]

The vector spaces \( V \in \mathcal{C}_{k,\mathcal{X}_{n,d}} \) are of dimension \( \left( \binom{k+n}{n} \right) \).
The elements in the code above are equidistant in the metric $\text{dist}(V_1, V_2)$ of Ralf Koetter and Frank R. Kschischang. For vector spaces $V_1, V_2 \in C_{k,x_{n,d}}$ 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

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

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

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

The associated affine cone of the $k$-osculating space is

$$\text{AffCone}(O_k, \mathcal{X}_{n,d}, P)(\mathbb{F}_q) = \{L^{d-k}F \mid F \in R_k\}$$

of dimension $\binom{k+n}{n}$, proving the claim on the dimension of the vector spaces in the linear network code $C_{k, \mathcal{X}_{n,d}}$. As there is one element in $C_{k, \mathcal{X}_{n,d}}$ for each $\mathbb{F}_q$-rational point on $\mathbb{P}^n$, it follows that the number of elements in $C_{k, \mathcal{X}_{n,d}}$ is

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

Finally, let $V_1, V_2 \in C_k, x_{n,d}$ with $V_1 \neq V_2$ and

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

If $2k \geq d$, we have

$$V_1 \cap V_2 = \{ L_1^{d-k} F_1 \mid F_1 \in R_k \} \cap \{ L_2^{d-k} F_2 \mid F_2 \in R_k \}$$

$$= \{ L_1^{d-k} L_2^{d-k} G \mid G \in R_{2k-d} \}.$$ 

Otherwise the intersection is trivial, proving the claims on the dimension of the intersections and the derived distances.
A. Bernardi, M. V. Catalisano, A. Gimigliano, and M. Idà. 
Osculating varieties of Veronese varieties and their higher secant varieties. 

E. Ballico and C. Fontanari. 
On the secant varieties to the osculating variety of a Veronese surface. 

E. Ballico, R. Piene, and H. Tai. 
A characterization of balanced rational normal surface scrolls in terms of their osculating spaces. II. 

M. V. Catalisano, A. V. Geramita, and A. Gimigliano.
On the secant varieties to the tangential varieties of a Veronesean.


**P. A. Chou, Y. Wu and K. Jain.**
Practical network coding.
2003.

**J. P. Hansen.**
Equidistant linear network codes with maximal error-protection from veronese varieties.

**R. Hartshorne.**
*Algebraic geometry.*
Graduate Texts in Mathematics, No. 52.
A random linear network coding approach to multicast.

R. Koetter and F. R. Kschischang.
Coding for errors and erasures in random network coding.

R. Piene.
Numerical characters of a curve in projective $n$-space.

- **R. Piene and H. Tai.**  
  A characterization of balanced rational normal scrolls in terms of their osculating spaces.  

- **B. Segre.**  
  Un’estensione delle varietà di Veronese, ed un principio di dualità per forme algebriche. I.  

- **A. Terracini.**
Sulle $v_k$ per cui la varietà degli $s_h - h + 1$ seganti ha dimensione minore dell’ordinario.


F. L. Zak.

*Tangents and secants of algebraic varieties*, volume 127 of *Translations of Mathematical Monographs*.


Translated from the Russian manuscript by the author.