Osculating Spaces of Varieties, Forms Linear Network Codes

International Conference
on
Algebraic Geometry and Coding Theory
Indian Institute of Technology
Mumbai, India
December 2-6, 2013

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

Outline

Abstract

- We present a *general theory* to obtain linear network codes utilizing the *osculating* nature of algebraic varieties.
- *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.
- By way of example we present *the osculating spaces of Veronese varieties* and obtain families of vector spaces constituting linear network codes
- The osculating spaces of Veronese varieties are equidistant in a certain metric.
- We present linear network codes derived from any set of normalized homogenous polynomials in $\mathbb{F}_q[X_0, \ldots, X_n]_e / \sim$, generalising the above result.

Linear network coding

- Ordinary transmission: Independent data share the same resources and data are merely *forwarded* and stay independent.
- Linear network coding: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.

Network coding - Ahlswede, Cai, Li, Yeung (2000)

$$
\begin{tikzcd}
S_1 : \{x_1\} \arrow[dr, "x_1"] \arrow[ddd, "x_1"'] & & S_2 : \{x_2\} \arrow[dl, "x_2"'] \arrow[ddd, "x_2"] \\
& T_1 : \{x_1, x_2\} \arrow[d, "x_1"] & \\
& T_2 : \{x_1\} \arrow[dl, "x_1"'] \arrow[dr, "x_1"] & \\
R_1 : \{x_1\} & & R_2 : \{x_1, x_2\}
\end{tikzcd}
$$

$$
\begin{tikzcd}
S_1 : \{x_1\} \arrow[dr, "x_1"] \arrow[ddd, "x_1"'] & & S_2 : \{x_2\} \arrow[dl, "x_2"'] \arrow[ddd, "x_2"] \\
& T_1 : \{x_1, x_2\} \arrow[d, "x_1+x_2"] & \\
& T_2 : \{x_1 + x_2\} \arrow[dl, "x_1+x_2"'] \arrow[dr, "x_1+x_2"] & \\
R_1 : \{x_1, x_1 + x_2\} & & R_2 : \{x_1 + x_2, x_2\}
\end{tikzcd}
$$

Figure : Linear network coding allows for *linear combination of information* - both receivers obtain complete information

The problem of linear network code design

How to select which linear combinations to use?

- A simple algorithm is to select the combinations at *random*. However there is a certain probability that linearly dependent combinations are chosen!
- An alternative is to use *deterministic* algorithms to perform the design of linearly independent combinations.

Koetter and Kschischang (2008)

- Described 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

$$\mathrm{dist}(V_1, V_2) := \dim_{\mathbb{F}_q}(V_1 + V_2) - \dim_{\mathbb{F}_q}(V_1 \cap V_2).$$

- 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.
- Obtained Hamming, Gilbert-Varshamov and Singleton coding bounds.

Terracini's lemma - tangent spaces tend to be in general position

- Algebraic varieties are osculating. By *Terracini's lemma* their tangent spaces tend to be in general position. 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 have the expected maximal dimension and therefore the tangent spaces generically span a space of maximal dimension. (F. Zak, R. Lazarsfeld et. al.)
- We suggest *osculating spaces* for constructing linear subspaces in general position for linear network coding.
- *Any netwok code comes from an algebraic curve taking osculating spaces* (E. Ballico, [Bal])

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 $\mathbb{F}_q$.
- $R = \mathbb{F}[X_0, \ldots, X_n] = \oplus_d R_d$ and $R(\mathbb{F}_q) = \mathbb{F}_q[X_0, \ldots, X_n] = \oplus_d R_d(\mathbb{F}_q)$
- $\mathrm{AffCone}(Y) \subseteq \mathbb{F}^{M+1}$ denotes the affine cone of $Y \subseteq \mathbb{P}^M$ 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
- $\mathcal{V} = \sigma_d(\mathbb{P}^n) \subseteq \mathbb{P}^M$ with $M = \binom{d+n}{n} - 1$ is the Veronese variety.

Codes from osculating spaces

Definition

Let $X \subseteq \mathbb{P}^M$ be a smooth projective variety of dimension n defined over $\mathbb{F}_q$.
The elements of the the k-osculating linear network code $\mathcal{C}_{k,X}$ 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.

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

The number of elements in $\mathcal{C}_{k,X}$ is the number of $\mathbb{F}_q$-rational points on X.
The vector spaces in $\mathcal{C}_{k,X}$ have dimension at most $\binom{k+n}{n}$.

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.

Principal parts - local description

If $\mathcal{L}$ is of rank 1, then $\mathcal{P}^k_X(\mathcal{L})$ is a locally free sheaf of rank $\binom{k+n}{n}$.
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 $dx_1, \ldots dx_n$.
- $\mathcal{P}^k_X(\mathcal{L})$ 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.

Canonical morphism

In general, for each k there is a canonical morphism

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

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 $|\alpha| = i_1 + i_2 + \cdots + i_n$.

The osculating subspaces

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 $\mathcal{P}^k_X(\mathcal{L})$ denote the sheaf of principal parts of order k. There are homomorphisms

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

Definition

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

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

of projective dimension at most $\binom{k+n}{n} - 1$. For $k = 1$ the osculating space is the tangent space.

The Veronese variety - an example

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 $X_0^{d_0} X_1^{d_1} \ldots X_n^{d_n}$ with $d_0 + d_1 + \cdots + d_n = d$.
- $\mathbb{P}^M = \mathbb{P}(R_d)$ the associated projective space of dimension $M = \binom{n+d}{d} - 1$.

d-uple embedding and the Veronese variety

Definition

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

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

with image the Veronese variety

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

Osculating subspaces of the Veronese variety

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

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

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 $M = \binom{d+n}{n} - 1$, 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 $\binom{d+n}{n}$, 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 $V \in \mathcal{C}_{k,\mathcal{X}_{n,d}}$ are of dimension $\binom{k+n}{n}$.

Distances in $\mathcal{C}_{k,\mathcal{X}_{n,d}}$

Theorem

The elements in the code above are equidistant in the metric $\mathrm{dist}(V_1, V_2)$ *of Ralf Koetter and Frank R. Kschischang.*
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*

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

Proof.

The associated affine cone of the k-osculating space is

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

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

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

□

Proof.

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. □

Normalized polynomials and linear network codes

Let

$$\mathcal{N}(e) = \mathbb{F}_q[X_0, \ldots, X_n]_e / \sim$$

be the normalized homogenous polynomials over $\mathbb{F}_q$ of degree e, where $F_1 \sim F_2$ iff $F_1 = cF_2$ for some constant $c \in \mathbb{F}_q^*$.
Let $\mathcal{I}(e) \subseteq \mathcal{N}(e)$ be the irreducible normalized homogenous polynomials.
For any subset $\mathcal{B} \subseteq \mathbb{F}_q[X_0, \ldots, X_n]_e / \sim$ of normalized homogenous polynomials of degree e, we define the linear network code $\mathcal{C}_{\mathcal{B}}$ as a collection of $\mathbb{F}_q$-linear subspaces V_G, one for each $G \in \mathcal{B}$, in the vector space of all homogenous forms of degree d .

The linear network codes $\mathcal{C}_{\mathcal{B}}$

Let $G \in \mathbb{F}_q[X_0, \ldots, X_n]_e / \sim$. Assume that $G \neq 0$.
Let $d \geq e$ and consider the $\mathbb{F}_q$-linear injective morphism

$$\begin{array}{rcl} \mathbb{F}_q[X_0, \ldots, X_n]_{d-e} & \to & \mathbb{F}_q[X_0, \ldots, X_n]_d \\ F & \mapsto & G \cdot F \end{array} \tag{1}$$

with image

$$V_G := G \cdot \mathbb{F}_q[X_0, \ldots, X_n]_{d-e} \subseteq \mathbb{F}_q[X_0, \ldots, X_n]_d = \mathbb{F}_q^N \,, \tag{2}$$

which is a $\mathbb{F}_q$-linear subspace of dimension $l = \binom{n+d-e}{n}$ in the ambient vector space of dimension $N = \binom{n+d}{n}$.

The linear netwotk codes $\mathcal{C}_{\mathcal{B}}$

Definition

For any subset $\mathcal{B} \subseteq \mathbb{F}_q[X_0, \ldots, X_n]_e / \sim$ of normalized homogenous polynomials of degree e, the linear network code $\mathcal{C}_{\mathcal{B}} \subseteq G(l, N)(\mathbb{F}_q)$ consists of all the linear subspaces in the vector space $\mathbb{F}_q[X_0, \ldots, X_n]_d$ of homogenous forms of degree d with $d \geq e$, that are realized as images (2) for some $G \in \mathcal{B}$.

$$\mathcal{C}_{\mathcal{B}} = \{V_G = G \cdot \mathbb{F}_q[X_0, \ldots, X_n]_{d-e} |\ G \in \mathcal{B}\} \subseteq G(l, N)(\mathbb{F}_q)\ . \quad (3)$$

Applications of the construction

- In [Han1], we studied the resulting linear network codes $\mathcal{C}_B$, when $\mathcal{B}$ is the set of normalized homogenous polynomials which are *powers of linear terms*.
  This amounted to the study of the osculating spaces of Veronese varieties as presented above.
- In [Han2] we present the resulting linear network codes $\mathcal{C}_B$, when $\mathcal{B}$ is any set of normalized homogenous polynomials in $\mathbb{F}_q[X_0, \ldots, X_n]_e / \sim$, where each pair of unequal polynomials has the constants as their only common divisors generalising the above result.
- In particular we treat the case where $\mathcal{B}$ is the set of all irreducible normalized polynomials.

E. Ballico.
Any network codes comes from an algebraic curve taking osculating spaces.
arxiv.org/abs/1306.0992, June 2013.

J. P. Hansen.
Osculating Spaces of Varieties and Linear Network Codes.
Lecture Notes in Computer Science, 8080, Algebraic Informatics, 2013.

J. P. Hansen.
Forms and Linear Network Codes.
arxiv.org/abs/1303.1626, Marts 2013.

Tracey Ho, Muriel Médard, Ralf Koetter, David R. Karger, Michelle Effros, Jun Shi, and Ben Leong.
A random linear network coding approach to multicast.
IEEE TRANS. INFORM. THEORY, 52(10):4413–4430, 2006.

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