Any network code comes from an algebraic curve taking osculating spaces

Edoardo Ballico

Received: 21 January 2013 / Accepted: 31 May 2013 / Published online: 15 June 2013
© Springer Science+Business Media New York 2013

Abstract  In this note we prove that every network code over \( \mathbb{F}_q \) may be realized taking some of the osculating spaces of a smooth projective curve.

Keywords  Linear network coding · Algebraic curve · Osculating space

Mathematics Subject Classification  14H50 · 14N05 · 94B27

1 Introduction

In linear network coding informations go from one or more sources to one of more targets in terms of a basis of a possible altered vector space ([2, 6, 7, 9, 13] and references therein). It is well-known that every linear code may be seen as a Goppa code over a high genus curve [10]. In this paper we prove that the same is true for network codes. We may also fix the curve \( C \) with the only condition that \( \sharp(C(\mathbb{F}_q)) \) is at least the number of subspaces of our network code. We need to say what is the equivalent of a Goppa code in the set-up of network coding. We use the osculating codes introduced by Hansen in [3] and [4]. We do not need to restrict to constant dimension network coding.

Warning: in this paper we prove an existence theorem. We do not claim that it may be useful for the construction of network codes with good parameters.

Fix a finite field \( \mathbb{F}_q \) and an integer \( n > 0 \). Let \( \mathcal{P}(\mathbb{F}_q^n) \) denote the set of all linear subspaces of the \( \mathbb{F}_q \)-vector space \( \mathbb{F}_q^n \). A network code is just a non-empty subset \( S \subseteq \mathcal{P}(\mathbb{F}_q^n) \).

For any vector space \( W \) let \( \mathbb{P}(W) \) denote the projective space of all lines of \( W \) through 0. In this note we prove the following result.
Theorem 1 Let $S \subseteq \mathbb{P}(\mathbb{F}^n_q) \setminus \{0\}$, $n \geq 3$, be any network code. Let $C$ be a smooth and geometrically connected curve defined over $\mathbb{F}_q$ and such that $\mathfrak{z}(C(\mathbb{F}_q)) \geq \mathfrak{z}(S)$. Fix $A \subseteq C(\mathbb{F}_q)$ such that $\mathfrak{z}(A) = \mathfrak{z}(S)$ and fix a bijection $u : A \rightarrow S$. For every $W \in S$ fix $Q_W \in \mathbb{P}(W) \subseteq \mathbb{P}(\mathbb{F}_q^r)$. Then there exists a morphism $f : C \rightarrow \mathbb{P}^{n-1}$ defined over $\mathbb{F}_q$ such that $f(P) = Q_{u(P)}$ for every $P \in A$. $f$ has invertible differential at each point of $A$ and $u(P)$ is the vector space where associated projective space is the osculating space of dimension $\dim(u(P)) - 1$ to $(C, u)$ at $Q_{u(P)}$.

See Sect. 2 for the definition of osculating spaces to a curve. We also gives another property of the map $f$, which is related to the definition of osculating space (see Remark 2).

Remark 1 The map $u|A$ is injective if and only if $Q_a \neq Q_b$ for all $a \neq b$. By Hall’s marriage theorem [1, p. 6] we may find a set $\{Q_s\}_{s \in S}$, with $Q_s \in U_s$ for all $s$ and $Q_a \neq Q_b$ for all $a \neq b$ if and only if for all $S' \subseteq S$ we have $\mathfrak{z}(\cup_{s \in S'}U_s(\mathbb{F}_q)) \geq \mathfrak{z}(S')$. This condition is satisfied for any $S$ which may be interesting for network coding.

We do not know if (in the case $n \geq 4$ and when the condition of Remark 1 is satisfied) we may take as $f$ an embedding. Another promising tool would be to use Poonen’s Bertini’s theorem over a finite field [11,12]. However, we certainly cannot prescribe the curve $C$ using Bertini’s theorem. As far as we know no statement in the literature would give that $S$ comes from an embedding of a smooth curve. Two statements in [11], i.e. [11], Theorem 1.2 and Corollary 3.4, are very interesting, but not enough (as far as we see) to prove that any network code for which the condition of Remark 1 is satisfied arises as osculating spaces of a smooth curve.

2 The proof

For any subset $E$ of a projective space, let $(E)$ denote its linear span.

Let $C$ be a smooth and connected curve defined over an algebraically closed field $\mathbb{K}$. We recall the notion of osculating spaces to a curve in the algebraic set-up ([5,8], Chap. 7). Fix a morphism $u : C \rightarrow \mathbb{P}^r$ defined over $\mathbb{K}$, an integer $x > 0$ and $P \in C(\mathbb{K})$. Assume $a := \dim((C(\mathbb{K}))) > x$. The completion $\hat{O}_{C,P}$ of the local ring $O_{C,P}$ is the ring $\mathbb{K}[[t]]$ of power series in one variable over $\mathbb{K}$. We fix a homogenous system of coordinates $x_0, \ldots, x_r$ on $\mathbb{P}^r$ such that $u(P) = (1 : 0 : \cdots : 0)$ and $\langle C(\mathbb{K}) \rangle = \{x_i = 0 \text{ for all } i > a\}$. Hence $u$ induces $r$ power series $f_1(t), \ldots, f_r(t)$ with $f_i(0) = 0$ for all $i$, $f_i \neq 0$ for all $i \leq a$ and $f_i \equiv 0$ for all $i > a$. We may find a linear change of coordinates such that $f_1(t), \ldots, f_a(t)$ are power series with increasing order of zero. In this new coordinate system (call it $w_0, \ldots, w_r$, but notice that it depends from $P$) the $x$-dimensional osculating space to $(C, u)$ at $P$ is the $x$-dimensional linear subspace $\{w_{x+1} = \cdots = w_r = 0\}$. Write $f_s(t) = ct^{e_s} + g(t)$ with $c \neq 0$ and each term in the power series $g(t)$ of order $\geq e + 1$. The definition of osculating space implies $e \geq x + 1$. We say that $(C, u)$ has an ordinary $x$-osculation at $P$ if $e = x + 1$.

In our construction we may often obtain ordinary $(d_p - 1)$-osculation at each $P \in A$ (see Remark 2).

Lemma 1 Fix linear subspaces $A_i \subseteq \mathbb{P}^r$, $B_i \subseteq \mathbb{P}^r$, $1 \leq i \leq e$, such that $\dim(A_i) = \dim(B_i)$ for all $i$ and $\dim(A_1 + \cdots + A_e) = \dim(B_1 + \cdots + B_e) = \dim(A_1) + \cdots + \dim(A_e) + e - 1$. Fix $O_i \in A_i$ and $O'_i \in B_i$. Then there is an automorphism $h : \mathbb{P}^r \rightarrow \mathbb{P}^r$ such that $h(A_i) = B_i$ and $h(O_i) = O'_i$ for all $i$. If all $A_i$, $B_i$, $O_i$ and $O'_i$ are defined over $\mathbb{F}_q$, then we may find $h$ defined over $\mathbb{F}_q$. 
Proof The condition “\(\dim(A_1 + \cdots + A_e) = \dim(A_1) + \cdots + \dim(A_e) + e - 1\)” says that \(A_i \neq A_j\) for all \(i \neq j\) and that all these subspaces are linearly independent. The same condition holds for the linear subspaces \(B_i\), \(1 \leq i \leq e\). Hence the existence of \(h\) such that \(h(A_i) = B_i\) just says that any linear independent subset of a finite-dimensional vector space \(V\) may be completed to a basis and that any two basis of \(V\) differ by a linear automorphism of \(V\). To get also the condition \(h(O_i) = O'_i\) for all \(i\) it is sufficient to take \(O_i\) (resp. \(O'_i\)) as one of the elements of a minimal subset of \(A_i\) (resp. \(B_i\)) spanning \(A_i\) (resp. \(B_i\)).

For any linear subspace \(W \subseteq \mathbb{P}^r\) let \(\ell_W : \mathbb{P}^r \setminus A \to \mathbb{P}^{r-\dim(W)-1}\) denote the linear projection from \(W\).

Lemma 2 Let \(U_i \subseteq \mathbb{P}^{n-1}\), \(1 \leq i \leq e\), be finitely many non-empty linear subspaces (we allow the case in which \(U_i \subseteq U_j\) or \(U_i = U_j\) for some \(i \neq j\)). Let \(U \subseteq \mathbb{P}^{n-1}\) be the linear span of \(\bigcup_{i=1}^e U_i\). Set \(k := \dim(U)\), \(N := \sum_{i=1}^e \dim(U_i) + e - 1\) and take any integer \(r \geq \max\{N, k\}\). Fix \(Q_i \in U_i\), \(1 \leq i \leq e\). Let \(A_i \subseteq \mathbb{P}^r\), \(1 \leq i \leq e\), be linear subspaces such that \(\dim(A_i) = \dim(A_i)\) for all \(i\) and \(\dim(A_1 + \cdots + A_e) = N\). Fix \(O_i \in A_i\). Then there is a linear subspace \(W \subseteq U\) such that \(W \cap A_i = \emptyset\) for all \(i\), \(\dim(W) = r - k - 1\), \(\ell_W(A_i) = U_i\) and \(\ell_W(O_i) = Q_i\) for all \(i\). If all \(U_i\), \(A_i\), \(Q_i\) and \(O_i\) are defined over \(\mathbb{F}_q\), then \(W\) is defined over \(\mathbb{F}_q\).

Proof Let \(E := V_1 \cup \cdots \cup V_e\) be the algebraic scheme with \(e\) connected components \(V_1, \ldots, V_e\) with \(V_i = U_i\) as an abstract scheme. The inclusion \(\cup U_i \subseteq \mathbb{P}^{r-1}\) induces a morphism \(v : E \to U\) with \(v(V_i) = U_i\) for all \(i\) and \(v|V_i : V_i \to U_i\) an isomorphism. Fix \(Q'_i \in V_i\) to be the only point such that \(v(Q'_i) = Q_i\). Let \(L := v^*(O_U(1))\). Since each \(U_i\) is a linear subspace of \(U\) and \(V_i \cap V_j = \emptyset\) for all \(i \neq j\), \(L\) is a very ample line bundle on \(E\) and \(h^0(E, L) = N + 1\). Let \(w : E \hookrightarrow \mathbb{P}^n\) be the embedding of \(E\) induced by the complete linear system \(|L|\). Up to an automorphism of \(\mathbb{P}^r\) we may assume that \(A_i = w(V_i)\) and \(O_i = w(Q'_i)\) for all \(i\) (Lemma 1). Since \(v\) is induced by a subspace of \(|L|\), there is a linear subspace \(W \subseteq \mathbb{P}^r\) such that \(\dim(W) = r - k - 1\) and \(v = \ell_A \circ w\), i.e. \(U_i = \ell_A(A_i)\) for all \(i\). Since \(\dim(U_i) = \dim(V_i)\), we have \(W \cap U_i = \emptyset\) for all \(i\). Since \(w(Q_i') = O_i\) and \(w(Q'_i) = Q_i\), we have \(\ell_W(O_i) = Q_i\). If all linear spaces \(U_i\) and \(A_i\) are defined over a field \(K\), \(Q_i \in U_i(K)\) and \(O_i \in A_i(K)\), then the construction works over \(K\) and hence \(W\) is defined over \(K\).

Lemma 3 Let \(g \geq 0\) be the genus of \(C\). For any \(P \in A\) set \(d_P := \dim(w(P)) + 1\). Set \(\delta := \sum_{P \in A} d_P\). Fix any line bundle \(L\) on \(C\) defined over \(\mathbb{F}_q\) and such that \(\deg(L) \geq \max\{2g + 1, 2g - 1 + \delta\}\). Let \(w : C \hookrightarrow \mathbb{P}^r\), \(r := \deg(L) - 1\), be the embedding induced by the complete linear system \(|L|\). Each degree \(d\) divisor \(d_P w(P) \subseteq w(C)\) spans a linear subspace \(A_P\) defined over \(\mathbb{F}_q\), \(\dim(A_P) = d_P - 1\) for all \(P\) and \(\cup_{P \in A} A_P\) is a linear subspace of dimension \(\delta\).

Proof \(L\) is very ample, because \(\deg(L) \geq 2g + 1\). Fix an effective divisor \(D\) on \(C\) such that \(\deg(D) \leq \delta\). Since \(\deg(L(-D)) \geq 2g - 1\), we have \(h^1(C, L(-D)) = 0\). Riemann–Roch gives \(h^0(C, L(-D)) = h^0(C, L) - \deg(D), i.e. \dim(w(D)) = \deg(D) - 1\). Apply this observation first to each divisor \(d_P P\) and then to the divisor \(\sum_{P \in A} d_P P\).

Proof of Theorem 1 For each \(P \in A\) set \(\eta_P := \max\{d_P, 2\}\). Set \(\eta := \sum_{P \in A} \eta_P\). Let \(L\) be a line bundle of degree \(\geq \max\{2g + 1, 2g - 1 + \eta\}\) defined over \(\mathbb{F}_q\). Let \(w : C \to \mathbb{P}^r\), \(r := \deg(L) - g\), denote the map associated to the complete linear system \(|L|\). Lemma 2 gives that \(w\) is an embedding, that each linear space \(A_P := \langle d_P w(P) \rangle\) has dimension \(d_P - 1\).
and that the suspaces $A_p$, $P \in A$, are linearly independent. Lemma 1 gives the existence of a linear subspace $W \subset \mathbb{P}^r$ such that $\dim(W) = r - k - 1$, $W \cap A_p = \emptyset$ for all $P$ and $u(P) = \ell_W(A_p)$ for all $P$. Since $\dim(A_p) = d_p - 1$, $A_p$ is the osculating space of dimension $d_p - 1$ to $w(C)$ at $w(P)$. Take $s = u(P) \in S$ such that $\dim(U_s) > 0$. Since $A_p$ contains the tangent line to $w(C)$ at $w(P)$ and $W \cap A_p = \emptyset$, $\ell_W$ induces an embedding of $w(C)$ into $\mathbb{P}^{n-1}$ in a neighborhood of $w(P)$, i.e. we are computing the osculating space with respect to a smooth branch of $u(C)$. This is not necessarily true at the points $s = u(P)$ such that $\dim(U_s) = 0$. We do not need any smoothness to compute $u(P)$, but in the statement of Theorem 1 we claimed that we may find $u$ which is unramified at each point of $A$, i.e. that the differential of $u$ is invertible at each point of $A$. Set $S' := \{s \in S : \dim(U_s) > 0\}$. For each $s \in S \setminus S'$ choose any line $\tilde{U}_s \subset \mathbb{P}^{n-1}$ defined over $\mathbb{F}_q$ and containing the point $U_s$. Set $S' := S' \cup \bigcup_{S \in S', \ell} \tilde{U}_s$ in which each line $\tilde{U}_s$ has the point $U_s$ as its prescribed $u(P) = Q_s$ (i.e. we use $\eta P$ instead of $dP$ and $\eta$ instead of $\delta$). If $\tilde{U}_s = U_a$ for some $s \in S \setminus S'$ and some $a \in S'$ or if $\tilde{U}_a = \tilde{U}_b$ for some $a \neq b$, then we count twice or more the linear space $\tilde{U}_a$ (indeed, in Lemma 2 we allowed that some of the subspaces coincide). We chose $Q_s$ as the point of $\tilde{U}_a$. With this convention the new map $u$ is unramified at each point of $A$. □

Remark 2 Assume $\dim(U_s) \leq n - 3$ for all $s \in S$. For each $s \in S$ take a linear subspace $\tilde{U}_s \subset \mathbb{P}^n_q$ such that $\tilde{U}_s \supset U_s$ and $\dim(\tilde{U}_s) = \dim(U_s) + 1$. Write $\tilde{S} := \delta + \tilde{z}(S)$, i.e. write $\tilde{S} := \sum_{s \in S}(\dim(\tilde{U}_s) + 1)$. Take $\tilde{Q}_s$ as the prescribed point of $\tilde{U}_s$. Let $\tilde{S}$ be the family of linear subspaces of $\mathbb{P}^n_q$ counting them several times if we take $\tilde{U}_a = \tilde{U}_b$ for some $a \neq b$. Do the construction used to prove Theorem 1 using the family $\tilde{S}$ with the points $\{Q_s\}_{s \in S}$. If $s = u(P)$, then $U_s$ is associated to the divisor $dP$, while $\tilde{U}_s$ is associated to the divisor $(dP + 1)P$. Since $\tilde{U}_s \subset \tilde{U}_s$, we get that $(C, u)$ has an ordinary $(dP - 1)$-ramification at each $P \in A$.

Acknowledgments Partially supported by MIUR and GNSAGA (Indam).

References

1. Bollobas B.: Combinatorics. Cambridge University Press, Cambridge (1986).
2. Chou P.A., Wu Y., Jain K.: Practical network coding. In: Allerton Conference on Communication, Control, and Computing (2003).
3. Hansen J.P.: Euclidean Linear Network Codes with Maximal Error-Projection from Veronese Varieties. Lect. Notes in Computer Science. Springer (2013, to appear). arXiv:1207.2083.
4. Hansen J.P.: Osculating Spaces of Varieties and Linear Network Codes. arXiv:1210.7961v1 (2012).
5. Hirschfeld J W.P., Korchmáros G., Torres, F.: Algebraic curves over a finite field. Princeton Series in Applied Mathematics. Princeton University Press, Princeton (2008).
6. Ho T., Médard M., Koetter R., Karger D.R., Effros M., Shi J., Leong B.: A random linear network coding approach to multicast. IEEE Trans. Inform. Theory 52(10), 4413–4430 (2006).
7. Koetter R., Kschischang F.R.: Coding for errors and erasures in network coding. IEEE Trans. Inform. Theory 54(8), 3579–3591 (2008).
8. Laksov D.: Wronskians and Plücker formulas for linear systems on curves. Ann. Scient. École Norm. Sup. 17, 565–579 (1984).
9. Li S.-Y.R., Yeung R.W., Chai N.: Linear network coding. IEEE Trans. Inform. Theory 49(2), 371–381 (2003).
10. Pellikann R., Shen B.-Z., van Wee G.J.M.: Which linear codes are algebraic–geometric? IEEE Trans. Inform. Theory 37(3), 583–602 (1991).
11. Poonen B.J.: Bertini theorems over finite fields. Ann. Math. 160(3), 1099–1127 (2004).
12. Poonen B.J.: Smooth hypersurface sections containing a given subscheme over a finite field. Math. Res. Lett. 15(2), 265–271 (2008).
13. Trautmann A.-L., Manganiello F., Rosenthal J.: Orbit codes—a new concept in the area of network coding. In: Theory, Information Workshop (ITW), 2010 IEEE, Dublin, Ireland, pp. 1–4 (2010).