International Journal of Pure and Applied Mathematics

Volume 21 No. 3 2005, 299-305

MULTIDIMENSIONAL HERMITE AND BIRKHOFF INTERPOLATION OVER A FINITE FIELD

E. Ballico

Department of Mathematics
University of Trento
380 50 Povo (Trento) - Via Sommarive, 14, ITALY
e-mail: ballico@science.unitn.it

Abstract: Here we study multivariant Birkhoff and Hermite interpolation over a finite field using projective geometry and elementary cohomological techniques from algebraic geometry.

AMS Subject Classification: 13M10, 14N05, 41A05, 65D05
Key Words: Hermite interpolation, Birkhoff interpolation, multidimensional interpolation, finite field

1. Introduction

Fix a prime p. For any p-power q let $GF(q)$ denote the finite field with q elements. For any integer $n > 0$ let $\mathbb{A}^n(q)$ denote the affine n-dimensional space over $GF(q)$ with a prescribed system of coordinates $x_1, \dots, x_n$. See $\mathbb{A}^n(q)$ as a subset of the n-dimensional projective space $PG(n, q)$ with a prescribed system of homogeneous coordinates $z_0, \dots, z_n$ such that $x_i = z_i/z_0$ for $1 \leq i \leq n$. Hence $PG(n, q) \backslash \mathbb{A}^n(q)$ is the hyperplane $\{z_0 = 0\}$. Set $\partial_i := \partial/\partial x_i$. Similarly, for any multi-index $\alpha = (a_1, \dots, a_n)$ let ∂_α denote the corresponding differential

Received: March 21, 2005

operator of order $|\alpha| := a_1 + \cdots + a_n$, where if $a_i \geq p$ for some i we use the Hasse derivatives (see [5], §3, for their elementary properties), not the usual high order partial derivatives. For any integer $d \geq 0$, let $V_{n,d}$ denote the $GF(q)$-vector space of all polynomials of degree at most d in the variables $x_1, \dots, x_n$ and $W_{n,d}$ the $GF(q)$-vector space of all homogeneous polynomials of degree d in the variables $z_0, \dots, z_n$. Hence $\dim(V_{n,d}) = \dim(W_{n,d}) = \binom{n+d}{n}$. For any $S \subseteq \mathbb{A}^n(q)$ and any $M \subseteq PG(n,q)$, set $V_{n,d}(-S) := \{f \in V_{n,d} : f(P) = 0 \text{ for every } P \in S\}$ and $W_{n,d}(-M) := \{f \in W_{n,d} : f(P) = 0 \text{ for every } P \in M\}$. Hence $\dim(V_{n,d}(-S)) \geq \binom{n+d}{n} - \operatorname{card}(S)$ and $\dim(W_{n,d}(-S)) \geq \binom{n+d}{n} - \operatorname{card}(M)$. Fix $P = (x_1^0, \dots, x_n^0) \in \mathbb{A}^n(q)$. Let $H_i(P)$ denote the affine hyperplane $\{x_i = x_i^0\}$ and $D_i(P)$ the affine line $\cap_{j \neq i} H_j(P)$. Hence $D_i(P)$ is the affine line passing through P and parallel to the x_i-axis. Set $\overline{H_i}(P) := \{z_i = x_i^0 z_0\}$. Hence $\overline{H_i}(P)$ is the hyperplane of the projective space which is the completion of $H_i(P)$. Set $\overline{D_i} := \cap_{j \neq i} \overline{H_j(P)}$, the projective line passing through P which is the natural completion of $D_i(P)$. Write P_i for the point P when we see it as a point on the line $D_i(P)$ or the line $\overline{D_i}(P)$. Fix integers $m_i > 0$, $1 \leq i \leq n$. Let $m_i P_i$ denote the effective degree m_i divisor of $D_i(P)$ or $\overline{D_i}(P)$ supported by P_i and with multiplicity m_i. Hence on $D_i(P)$ (resp. $\overline{D_i}(P)$) $m_i P_i$ has equation $(x_i - x_i^0)^m$ (resp. $(z_i - x_i^0 z_0)^m$). We see $m_i P_i$ as a zero-dimensional scheme with length m_i and we write $(m_1, \dots, m_n)P$ for the products of the n schemes $m_i P_i$. Hence $(m_1, \dots, m_n)P$ is a zero-dimensional scheme defined over $GF(q)$ with length $m_1 \cdot m_2 \cdots m_n$ and with P as its support. Let $\mathbb{K}$ denote an algebraically closed field; usually, $\mathbb{K}$ will be the algebraic closure of the field we are interested in or, at least, it will contain it. We will call $(m_1, \dots, m_n)P$ a cubical fat point with multiplicity (or of type) $(m_1, \dots, m_n)$. For any polynomial $f \in \mathbb{K}[x_1, \dots, x_n]$ its restriction to $(m_1, \dots, m_n)P$ represents the part of its Taylor expansion with respect to the variables $x_i - x_i^0$ associated to the evaluation at P of all Hasse derivatives ∂_α, $\alpha = (\alpha_1, \dots, \alpha_n)$, such that $\alpha_i < m_i$ for all i. The usual fat point mP with multiplicity m supported by P would corresponds to the part of the Taylor series associated to the Hasse derivatives ∂_α, $\alpha = (\alpha_1, \dots, \alpha_n)$, such that $\alpha_1 + \cdots + \alpha_n < m$. Cubical fat points are much better behaved and easier to handle than the usual fat points because they are complete intersections (both in the affine or the projective space) of hypersurfaces, respectively the affine hypersurfaces $H_i(P)^{m_i}$ and the projective hypersurfaces $\overline{H_i}(P)^{m_i}$, $1 \leq i \leq n$. All these hypersurfaces are just hyperplanes with a certain multiplicity. However, the definition of cubical fat point depends on the choice of a fixed coordinate system. For any $S \subseteq \mathbb{A}^n(q)$ and all $m_i > 0$, $1 \leq i \leq n$, set $(m_1, \dots, m_s)S := \cup_{P \in S}(m_1, \dots, m_s)P$. For any field K let ${\mathbb{A}^n}_K$ (resp. ${\mathbf{P}^n}_K$) denote the n-dimensional affine (resp. projective) space.

Remark 1. For all $y \in GF(q)$ and every integer i such that $1 \leq i \leq n$, let $H_{i,y}$ be the affine hyperplane $\{x_i = y\}$ of $\mathbb{A}^n_{\mathbb{K}}$ and $\overline{H_{i,y}}$ the hyperplane $\{z_i = z_0 y\}$ of $\mathbf{P}^n_{\mathbb{K}}$. Set $A_i := \cup_{y \in GF(q)}$ and $\overline{A_i} := \cup_{y \in GF(q)} \overline{H_{i,y}}$. Hence A_i (resp. $\overline{A_i}$) is an affine (resp. projective) degree q hypersurface. Notice that $\mathbb{A}^n(q) = \cap_{i=1}^n A_i = \cap_{i=1}^n \overline{A_i}$ (even scheme-theoretically).

Remark 2. Fix $S \subseteq \mathbb{A}^n(q)$ and integers $m_i > 0$, $1 \leq i \leq n$. Assume the existence of $E_i \subseteq GF(q)$ such that, setting $B_i := \cup_{y \in E_i} \overline{H_{i,y}}$, we have $S = \cap_{i=1}^n B_i$. Then $(m_1, \ldots, m_s)S$ is the complete intersection in $\mathbf{P}^n_{\mathbb{K}}$ of n hypersurfaces of degree $m_1 \mathrm{card}(S_1), \ldots, m_n \mathrm{card}(S_n)$.

We will use the previous observations that $\mathbb{A}^n(q)$ are complete intersections in a projective space over $\mathbb{K}$ in order to apply to $\mathbb{A}^n(q)$ several cohomological computations (see Section 2).

Remark 3. For all integer d such that $0 \leq d < q$ we have $V_{n,d}(-\mathbb{A}^n(q)) = \{0\}$ and $W_{n,d}(-PG(n,q)) = \{0\}$. Notice that this is false for $d \geq q$ (e.g use $x_1^{d-q}(x_1^q - x_1)$). Hence there are $S \subset \mathbb{A}^n(q)$ and $M \subset PG(n,q)$ such that $\mathrm{card}(S) = \mathrm{card}(M) = \binom{n+d}{n}$ and $V_{n,d}(-S) = W_{n,d}(-M) = \{0\}$. Hence S (resp. M) imposes independent conditions to $V_{n,d}$ (resp. $W_{n,d}$). Hence for all $A \subseteq S$, all $B \subseteq M$, all $S \subseteq E \subseteq \mathbb{A}^n(q)$ and all $M \subseteq F \subseteq PG(n,q)$ we have $\dim(V_{n,d}(-A)) = \binom{n+d}{n} - \mathrm{card}(A)$, $\dim(W_{n,d}(-B)) = \binom{n+d}{n} - \mathrm{card}(B)$, $V_{n,d}(-E) = \{0\}$ and $W_{n,d}(-F) = \{0\}$.

This research was inspired by the reading of [7], in which Birkhoff interpolation appears as a tool in secret sharing theory; for other related applications of polynomial interpolation over a finite field (in particular, to security on ad-hoc networks), see [2]. For Birkhoff interpolation in characteristic zero, see [6], [1] and [3].

2. The Main Results

For any algebraic scheme X over a field and any closed subscheme Y of X, let $\mathcal{I}_{Y,X}$ (or just $\mathcal{I}_Y$ if X is either a projective space or an affine space and there is no danger of misunderstandings) denote the ideal sheaf of Y in X.

Remark 4. Let X be an algebraic scheme defined over $GF(q)$ and $\mathcal{F}$ an algebraic coherent sheaf on X defined over $GF(q)$. Let $X_{\mathbb{K}}$ (resp. $\mathcal{F}_{\mathbb{K}}$) be the algebraic $\mathbb{K}$-scheme (resp. coherent sheaf on $X_{\mathbb{K}}$) obtained from X (resp. $\mathcal{F}$) using the field extension $GF(q) \subset \mathbb{K}$. Since any extension of fields is flat, we may apply a theorem on the invariance of cohomology groups for flat extensions

([4], Proposition III.9.3) and obtain $H^i(X,\mathcal{F}) \otimes_{GF(q)} \mathbb{K} \cong H^i(X_{\mathbb{K}},\mathcal{F}_{\mathbb{K}})$ for all $i \geq 0$ (as $\mathbb{K}$-vector spaces). Hence to compute cohomology groups of objects defined over $GF(q)$ we may use all the results available for schemes over $\mathbb{K}$.

We stress that in the next three lemmas we do not assume that the hypersurfaces X_i have no multiple component.

Lemma 1. *Let X_i, $1 \leq i \leq n-1$, be hypersurfaces of $\mathbf{P}^n_{\mathbb{K}}$ such that $\dim(X_1 \cap \cdots \cap X_{n-1}) = 1$. Set $d_i := \deg(X_i)$. For any integer i such that $1 \leq i \leq n-1$ set $Y_i := \cap_{j=1}^{i} X_j$ (scheme-theoretic intersection). Then $\dim(Y_i) = n-i$ and $h^j(Y_i,\mathcal{O}_{Y_i}(t)) = 0$ for all $1 \leq i \leq n-1$, all $j \geq n-i+1$ and all $t \in \mathbb{Z}$ and $H^{n-i}(Y_i,\mathcal{O}_{Y_i}(x)) = 0$ for all i and all $x \geq d_1 + \cdots + d_i - n$. We have $h^{n-i}(Y_i,\mathcal{O}_{Y_i}(d_1 + \cdots + d_i - n - 1)) = 1$. We have $h^j(\mathbf{P}^n_{\mathbb{K}},\mathcal{I}_{Y_i}(z)) = 0$ for all $j > 0$, $z \in \mathbb{Z}$ and $1 \leq i \leq n-1$.*

Proof. Notice that $\mathcal{O}_{\mathbf{P}^n_{\mathbb{K}}}(-d_j)$ is isomorphic to the ideal sheaf of X_j in $\mathbf{P}^n_{\mathbb{K}}$ and that if $j \geq 2$ its restriction to Y_{j-1} is isomorphic to the ideal sheaf of Y_j in Y_{j-1}. Then use the cohomology of $\mathbf{P}^n_{\mathbb{K}}$ ([4], Chapter III, §5), the cohomology exact sequences of the exact sequence of sheaves

$$0 \to \mathcal{O}_{Y_i}(y - d_i) \to \mathcal{O}_{Y_i}(y) \to \mathcal{O}_{Y_{i+1}}(y) \to 0 \tag{1}$$

and induction on the integer i. □

In the same way we obtain the following well-known result.

Lemma 2. *Let X_i, $1 \leq i \leq n$, be hypersurfaces of $\mathbf{P}^n_{\mathbb{K}}$ such that $\dim(X_1 \cap \cdots \cap X_n) = 0$. Set $d_i := \deg(X_i)$ and $T := X_1 \cap \cdots \cap X_n$ (scheme-theoretically). Then $h^1(\mathbf{P}^n_{\mathbb{K}},\mathcal{I}_T(t)) = 0$ for every $t \geq d_1 + \cdots + d_n - n$ and $h^1(\mathbf{P}^n_{\mathbb{K}},\mathcal{I}_T(d_1 + \cdots + d_n - n - 1)) = 1$.*

Lemma 3. *Let X_i, $1 \leq i \leq n$, be hypersurfaces of $\mathbf{P}^n_{\mathbb{K}}$ such that $\dim(X_1 \cap \cdots \cap X_n = 0$. Set $d_i := \deg(X_i)$ and $T := X_1 \cap \cdots \cap X_n$ (scheme-theoretically). Set $\delta := \min\{d_i\}_{1 \leq i \leq n}$ and let τ be the number of indices i such that $d_i = \delta$. For all integers t let $\rho_{T,t} : H^0(\mathbf{P}^n_{\mathbb{K}},\mathcal{O}_{\mathbf{P}^n_{\mathbb{K}}}(t)) \to H^0(T,\mathcal{O}_T(t))$ denote the restriction map. We have $\operatorname{Ker}(\rho_{T,t}) \cong H^0(\mathbf{P}^n_{\mathbb{K}},\mathcal{I}_T(t)$ and $\operatorname{Coker}(\rho_{T,t}) \cong H^1(\mathbf{P}^n_{\mathbb{K}},\mathcal{O}_T(t)$. The linear map $\rho_{T,t}$ is surjective if and only if $t \geq d_1 + \cdots + d_n - n$. We have $\dim(\operatorname{Coker}(\rho_{T,d_1+\cdots+d_n-n-1})) = 1$. The map $\rho_{T,t}$ is injective if and only if $t < \delta$. We have $\dim(\operatorname{Ker}(\rho_{T,\delta})) = \binom{n+\delta}{n} - \tau$.*

Proof. The first assertion follows from the cohomology exact sequence of the exact sequence 1 as in the proof of Lemma 1. The same proof together with the last assertion of Lemma 2 give all results on $\operatorname{Coker}(\rho_{T,t})$. Looking at

the beginning parts of the cohomology exact sequences of the exact sequence 1 instead of the last parts we get all the results on $\mathrm{Ker}(\rho_{T,t})$. □

Notation 1. For all integers t, $n > 0$ and $m_i > 0$ and $E_i \subseteq GF(q)$, $1 \le i \le n$ let $\rho_{n,q,t} : H^0(\mathbf{P}^n_{\mathbb{K}}, \mathcal{O}_{\mathbf{P}^n_{\mathbb{K}}}(t)) \to H^0(\mathbb{A}^n(q), \mathcal{O}_{\mathbb{A}^n(q)}(t))$, $\rho_{n,q,t;m_1,\dots,m_n} : H^0(\mathbf{P}^n_{\mathbb{K}}, \mathcal{O}_{\mathbf{P}^n_{\mathbb{K}}}(t)) \to H^0((m_1,\dots,m_n)\mathbb{A}^n(q), \mathcal{O}_{(m_1,\dots,m_n)\mathbb{A}^n(q)}(t))$ and

$$\rho_{n,q,t;m_1,\dots,m_n,E_1,\dots,E_n} : H^0(\mathbf{P}^n_{\mathbb{K}}, \mathcal{O}_{\mathbf{P}^n_{\mathbb{K}}}(t)) \to H^0((m_1,\dots,m_n)S, \mathcal{O}_{(m_1,\dots,m_n)S}(t))$$

(where S is as described in Remark 2) denote the restriction maps.

From Lemma 3 and Remark 1 and Remark 2 we obtain the following result.

Theorem 1. *Fix integers t, $n > 0$ and $m_i > 0$ and $E_i \subseteq GF(q)$, $1 \le i \le n$. Set $e_i := \mathrm{card}(E_i)$. Then $\rho_{n,q,t;m_1,\dots,m_n,E_1,\dots,E_n}$ is surjective if and only if $t \ge m_1e_1 + \cdots + m_ne_n - n$ and it is injective if and only if $t < \min\{m_ie_i\}_{1\le i\le n}$.*

Taking $m_i = 1$ and $E_i = GF(q)$ for all i in the statement of Theorem 1 we obtain the following result.

Corollary 1. *The map $\rho_{n,q,t}$ is surjective if and only if $t \ge nq - n$ and it is injective if and only if $t < q$.*

Remark 5. Fix integers t, $n > 0$ and $m_i > 0$ and $E_i \subseteq GF(q)$, $1 \le i \le n$. Set $e_i := \mathrm{card}(E_i)$. If $\min\{m_ie_i\}_{1\le i\le n} \le t \le m_1e_1 + \cdots + m_ne_n - n - 1$, then the map $\rho_{n,q,t;m_1,\dots,m_n,E_1,\dots,E_n}$ is neither injective nor surjective (Theorem 1), i.e. the associated interpolation problem has not maximal rank.

Up to now we have considered multivariant Hermite interpolation. Now we are going to consider multivariant Birkhoff interpolation, i.e. we prescribe only the vanishing of some of the Hasse derivatives in a cubical box. Fix integers $n > 0$ and $m_i > 0$ and $E_i \subseteq GF(q)$, $1 \le i \le n$. Set $e_i := \mathrm{card}(E_i)$. Let $S \subseteq \mathbb{A}^n(q)$ the complete intersection of the n hypersurfaces of degree $e_1,\dots,e_n$ unions of the affine hyperplanes associated to the pairs (i, E_i), $1 \le i \le S$ and $Z := (m_1,\dots,m_n)S$ the cubical scheme associated to these hypersurfaces counted with multiplicities $m_1,\dots,m_n$. Hence $\mathrm{card}(S) = \prod_{i=1}^n e_i$ and $\mathrm{length}(Z) = \prod_{i=1}^n m_ie_i$. By Theorem 1 for any integer t such that $t \ge m_1e_1 + \cdots + m_ne_n - n$, Z imposes $\prod_{i=1}^n m_ie_i$ independent conditions to the vector space of all polynomial over $GF(q)$ in n variables with degree at most t. Now assume also $t < q$. In particular we require $\prod_{i=1}^n m_ie_i < q$ and hence we require that q is large. However, we stress that we do not require that p is large. Under these assumptions Theorem 1 says that the set Σ of all Hasse derivatives associated to Z gives $\prod_{i=1}^n m_ie_i$ independent conditions to the set $V_{n,t}$. Hence

any $\Gamma \subset \Sigma$ gives independent condition to $V_{n,t}$. This is a partial Birkhoff type interpolation problem (we have existence, but not uniqueness). Now we use the assumption $t < q$. Set $\gamma := \text{card}(\Gamma)$. By Remark 3 there is $A \subset \mathbb{A}^n(q)$ such that $\text{card}(A) = \binom{n+t}{n} - \gamma$ such that the union of the interpolation data associated to γ and the order zero conditions associated to A has only the trivial solution and hence this union gives $\binom{n+t}{n}$ independent conditions to $V_{n,t}$. In summary, we have just proved the following result.

Theorem 2. *Fix integers t, γ, $n > 0$ and $m_i > 0$ and $E_i \subseteq GF(q)$, $1 \le i \le n$. Set $e_i := \text{card}(E_i)$. Assume $m_1e_1 + \cdots + m_ne_n - n \le t < q$ and $\gamma \le \binom{n+t}{n}$. Let Σ be the set of all Hasse derivatives associated to the sets E_i and the integers m_i. Fix any $\Gamma \subseteq \Sigma$ such that $\text{card}(\Gamma) = \gamma$. Then there exists $A \subset \mathbb{A}^n(q)$ such that $\text{card}(A) = \binom{n+t}{n} - \gamma$ and the interpolation problem associated to $\Gamma \cup A$ is perfect, i.e. the associated homogeneous interpolation problem has zero as the only solution and the non-homogeneous one satisfies the existence and the uniqueness of the solution.*

Acknowledgements

The author was partially supported by MIUR and GNSAGA of INdAM (Italy).

References

[1] K. Atkinson, A. Sharma, A partial characterization of Hermite-Birkhoff interpolation problems, *J. Numer. Anal.*, **6**, No. 2 (1969), 230-235.

[2] E. Ballico, G. Boato, C. Fontanari, F. Granelli, Multipath secret sharing in ad hoc networks: a hierarchical approach via Birkhoff interpolation, *Preprint*.

[3] R.A. DeVore, G.G. Lorentz, *Constructive Approximation, Grundlehren der Mathematischen Wissenschaften*, **303**, Springer-Verlag, Berlin (1993).

[4] R. Hartshorne, *Algebraic Geometry*, Springer, Berlin-Heidelberg-New York (1977).

[5] A. Hefez, Nonreflexive curves, *Compositio Math.*, **69**, No. 1 (1989), 3-35.

[6] I.J. Schoenberg, On Hermite-Birkhoff interpolation, *J. Math. Anal. Appl.*, **16** (1966), 583-543.

[7] T. Tassa, Hierarchical threshold secret sharing, In: *The Proceedings of the First Theory of Cryptography Conference*, TCC 2004, MIT, Cambridge (February 2004), 473-490.