International Journal of Pure and Applied Mathematics

Volume 39 No. 2 2007, 147-149

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: Fix integers $n \geq m-1 \geq 0$, a Birkhoff interpolation problem $\mathcal{B}$ (interpolation of a polynomial and certain of its derivatives of order $\leq n$ at m points of a field) induced by a matrix $E = [e_{i,k}]$, $1 \leq i \leq m$, $0 \leq k \leq n$, $e_{i,k} \in \{0,1\}$, a prime $p > n$ and a p-power q. Here we prove the regularity of $\mathcal{B}$ at $(t_1, \dots, t_m) \in \mathbb{F}_q^m$ if it is regular at $(t_1^{q/p}, \dots, t_1^{q/p}) \in \mathbb{F}_p^m$. The regularity over $\mathbb{F}_p$ was recently studied by T. Tassa to solve a cryptographic model (hierarchical thresold secret sharing).

AMS Subject Classification: 14N05
Key Words: Hermite interpolation, Birkhoff interpolation, finite field

*

Fix integers $n \geq m-1 \geq 0$. An interpolation matrix for a Birkhoff problem with parameters (n,m) is a matrix $E = [e_{i,k}]$, $1 \leq i \leq m$, $0 \leq k \leq n$, such that $e_{i,k} \in \{0,1\}$ for all i,k and E has exactly $n+1$ non-zero entries (see [1], Chapter IV, Section 9, 10, or [4]). Fix a field K such that either $\mathrm{char}(K) = 0$ or $\mathrm{char}(K) > n$. For the case $0 < \mathrm{char}(K) \leq n$, see Remark 1. The matrix E is the abstract datum for the following classical interpolation problem due to Birkhoff. Fix $t_1, \dots, t_m \in K$ such that $t_i \neq t_j$ for all $i \neq j$. Let $V_K[E; t_1, \dots, t_m]$ denote the K-vector space of all polynomials f in one variable over K such that $f^{(k)}(t_i) = 0$ for all i,k such that $0 \leq i \leq n$, $1 \leq k \leq m$ and $e_{i,k} = 1$; here $f^{(k)}$ denotes the order k derivative of f. The Birkhoff problem associated to E is regular at $t_1, \dots, t_m$ if $V[E; t_1, \dots, t_m] = \{0\}$. The Birkhoff problem associated

Received: March 19, 2007

to E is called regular if it is regular at all m-ples of distinct elements of K. The condition that E has exactly $n+1$ non-zero entries is equivalent to the hope of existence and uniqueness of the solutions. In the homogeneous case, the good behaviour of the interpolation problem means that the zero-solution is the only solution. The notion of regularity strongly depend from the choice of K (for an $\mathbb{R}$-regular, but not $\mathbb{C}$-regular problem, see [1], Example (c) at p. 125). Indeed, very few Birkhoff matrices are regular in this sense over an algebraically closed field. Our interest is the case K finite and we want to study existence of good m-ples for as much Birkhoff matrices as possible. Our interest comes from cryptography and it was aroused from [5]. T. Tassa used a very particular Birkhoff matrix E to make a model for the problem of threshold secret sharing. Fix $n \geq m-1 \geq 0$ and a Birhkoff matrix E with parameters (n,m) and assume $p > n$. He assumed $p \gg 0$ but we want to use also lower p. Take a p-power q, say $q = p^e$ with $e \geq 1$. He used in [5] only the case $q = p$, but we want to be allowed to increase arbitrarily the size of the field, just increasing the integer e.

Theorem 1. *Fix a Birkhoff matrix E of type (n,m), a prime $p > n$, a p-power $q = p^e$, $e \geq 2$, and $t_1, \dots, t_m \in \mathbb{F}_q$ such that $t_i^{q/p} \neq t_j^{q/p}$ for all $i \neq j$ and that E is regular at the m-ple $(t_1^{q/p}, \dots, t_m^{q/p}) \in \mathbb{F}_p^m$ (as a Birkhoff problem over $\mathbb{F}_p$). Then E is regular at $(t_1, \dots, t_m)$ (as a Birkhoff problem over $\mathbb{F}_q$).*

Obviously, Theorem 1 has the following corollary.

Corollary 1. *Fix integers $n \geq m-1$, a prime $p > n$, a p-power q and $t_1, \dots, t_m \in \mathbb{F}_q$ such that $t_i^{q/p} \neq t_j^{q/p}$ for all $i \neq j$. Let E be a Birkhoff matrix of type (n,m) which is regular for $\mathbb{F}_p$. Then E is regular at $(t_1, \dots, t_m)$ for the field $\mathbb{F}_q$.*

Notice that the assumption on the m-ple $(t_1, \dots t_m) \in \mathbb{F}_q^m$ does not depend from the choice of E, but only from its regularity over $\mathbb{F}_p$. Hence we may fix $(t_1, \dots t_m)$ before knowing E and for many different matrices E.

Proof of Theorem 1. Fix $f = \sum_{j=0}^{n} a_j x^k \in V_{\mathbb{F}_q}[E; t_1, \dots, t_m]$. Hence the $n+1$ coefficients $a_j \in \mathbb{F}_q$ satisfy the following $n+1$ linear equations:

$$\sum_{j \geq k} (j!/k!) a_j t_i^{j-k} = 0, \qquad e_{i,k} = 1\,. \tag{1}$$

Now we raise to the q/p power the left hand side of each of the equations (1), obtaining the following linear system:

$$\sum_{j \geq k} (j!/k!)^{q/p} a_j^{q/p} (t_i^{q/p})^{j-k} = 0, \qquad e_{i,k} = 1\,. \tag{2}$$

Notice that $(j!/k!)^{q/p} \equiv j!/k! \pmod p$ and hence $(j!/k!)^{q/p} = j!/k!$ as elements of $\mathbb{F}_p$. Since $a_j^{q/p} \in \mathbb{F}_p$ for all j and $V_{\mathbb{F}_p}[E; t_1^{q/p}, \ldots, t_m^{q/p}] = \{0\}$, we obtain $a_j^{q/p} = 0$ for all j, i.e. $a_j = 0$ for all j, concluding the proof. $\square$

Remark 1. Assume $p := \mathrm{char}(K) > 0$. The order p derivatives of the polynomial t^p is identically zero. Hence if $p \leq n$, we must modify the set-up of the problem. We use the Hasse derivatives instead of the ordinary derivatives (see [2], §3, for their definition and main properties). With the use of Hasse derivatives the geometry of a rational normal curve of $\mathbf{P}^n$ and the approach of [3] show that any Hermite problem (i.e. any Birkhoff problem with a matrix E such that $e_{i,k} = 1$ implies $e_{i,h} = 1$ for all $0 \leq h \leq k$) is regular over any field K without any restriction on $\mathrm{char}(K)$. However, it seems very likely to us that if $p \leq n$ too many interesting Birkhoff problems are not regular.

Acknowledgements

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

References

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

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

[3] D. Laksov, Wronskians and Plücker formulas for linear systems on curves, *Ann. Scient. École Norm. Sup.*, **17** (1984), 565-579.

[4] G.G. Lorentz, K. Jetter, S.D. Riemenschneider, Birkhoff interpolation, *Encyclopedia of Mathematics and its Applications*, Volume 19, Addison-Wesley, Reading (1983).

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