International Journal of Pure and Applied Mathematics

Volume 17 No. 2 2004, 165-167

ORDER REGULARITY FOR BIRKHOFF INTERPOLATION PROBLEMS OVER $GF(p)$

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 $n > 0$, $m > 0$ and $M > 0$ such that $m \leq 2M + 1$ and a prime $p > (M/2)^{n+1}(n+2)^{(n+2)/2}$. Let E be a Birkhoff matrix of type (n, m) whose associated Birkhoff problem is order regular. Here we prove that for all m-ples x_i, $1 \leq i \leq m$, of integers such that $-M \leq x_1 < \cdots < x_m \leq M$ the Birkhoff problem associated to E for the field $GF(p)$ is regular at the m-ple $(P_1, \ldots, P_m)$, where $P_i \in GF(p)$ is the reduction modulo p of x_i.

AMS Subject Classification: 41A05, 12E20
Key Words: Birkhoff interpolation problem, order regularity of a Birkhoff interpolation problem

1. Order Regularity for Birkhoff Interpolation Problems over $GF(p)$

There is a huge literature concerning Birkhoff interpolation for real or complex polynomials (see [3]), but, after [4] it seems useful to collect many crietria of regularity over a finite field. Fix integers $n \geq m - 1 \geq 0$. An interpolation matrix for a Birkhoff problem 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 exactly $n+1$ non-zero entries. Let K be any field. For any ordered m-ple $(P_1, \ldots, P_m)$ of distinct points of K let $\wp(E; K; P_1, \ldots, P_m)$ be the complex vector space of all complex polynomials $f = \sum_{k=0}^{n} a_k x^k$ of degree at most n and such that $f^{(k)}(P_i) = 0$ for all i, k such that $e_{i,k} = 1$. The

Received: July 28, 2004

Birkhoff problem associated to E is said to be regular at $P_1, \dots, P_m$ if and only $\wp(E; K; P_1, \dots, P_m) = \{0\}$. Evaluating each derivative we see that the regularity is equivalent to the non-vanishing at $X = (P_1, \dots, P_m) = (P_1, \dots, P_m)$ of the determinant $D(E, X)$ of a certain $(n+1) \times (n+1)$ matrix. The Birkhoff interpolation problem associated to E is said to be regular over K if and only if the corresponding problem is regular for all m-ples of distinct elements of K. The notion of regularity is not invariant for extensions of the base field (see [1], Example IV.9.3 (c) at p. 125, for an example of a Birkoff matrix E with $n = 4$ and $m = 3$ which is $\mathbb{R}$-regular, but not $\mathbb{C}$-regular). There are very few sufficient conditions for the regularity of a Birkhoff problem. However, when $K = \mathbb{R}$, a weaker notion is very important: order regularity. The Birkhoff problem over $\mathbb{R}$ is order regular if it is regular at all m-ples $(x_1, \dots, x_m)$ such that $x_1 < \cdots < x_m$. There is an easy sufficient codition for the order regularity of E ([3], Theorem 1.5). Of course, over a finite field the notion of order regularity make no sense. However we will be able to use it to prove the regularity for suitable m-ples $(P_1, \dots, P_m) \in GF(p)$. We stress that in our result we may take $p, P_1, \dots, P_m$ depending only from n and m, not the choice of the order regular Birkhoff matrix E. The aim of this short note is to prove the following result.

Theorem 1. *Fix integers $n > 0$, $m > 0$ and $M > 0$ such that $m \leq 2M+1$ and a prime $p > (M/2)^{n+1}(n+2)^{(n+2)/2}$. Let E be a Birkhoff matrix of type (n, m) whose associated Birkhoff problem is order regular. Then for all m-ples x_i, $1 \leq i \leq m$, of integers such that $-M \leq x_1 < \cdots < x_m \leq M$ the Birkhoff problem associated to E for the field $GF(p)$ is regular at the m-ple $(P_1, \dots, P_m)$, where $P_i \in GF(p)$ is the reduction modulo p of x_i.*

Proof. We will modify a proof given in [4], §3.3. Since $p > n$ all integers $k!$ with $0 \leq k \leq n$ are invertible in $GF(p)$. Hence both over $\mathbb{R}$ and $GF(p)$ we may take the monomials $x^k/k!$, $0 \leq k \leq n$, as a basis for the vector space of all polynomials of degree at most n in one variable. Hence we may use the usual formula (see [3], formula (1.3.2)) for the determinant $D(E, X)$ and evaluate it at $x_1, \dots, x_m$. Since $|x_i| \leq M$, we obtain the determinant of an $(n+1) \times \times (n+1)$ matrix with rational coefficients and with denominators prime to p. Multiplying the k-th colum by $k!$ (for every k) we obtain a matrix A in which each non-zero entry is an integer of type x_i^{n-k} and hence whose absolute value is at most M^n. By Hadamard's Maximal Determinantal Theorem (see [2], problem 523) we have $\det(A) \leq (M/2)^{n+1}(n+2)^{(n+2)/2}$. Hence $\det(A)$ is an integer not divible by P. Hence $D(E, P_1, \dots, P_m) \neq 0$ in $GF(p)$. □

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] D.K. Faddev, I.S. Sominskii, *Problems in Higher Algebra*, W.H. Freeman, San Francisco (1965).

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

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