International Journal of Pure and Applied Mathematics

Volume 30 No. 3 2006, 425-428

POLYNOMIAL INTERPOLATION OVER A COMMUTATIVE RING

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 give a few results on polynomial interpolation over a commutative ring.

AMS Subject Classification: 13B25
Key Words: polynomial interpolation over a ring, finite commutative rings

1. Polynomial Interpolation over a Commutative Ring

Let R be a commutative ring with identity. Let R^* denote the set of all invertible elements of R.

Following [2] and [1], pp. 412-413 (but our definition is the same as the one in [2] only when R^* is the set of all non-zero divisors of R, e.g. when R is a finite ring) we will say that $S \subseteq R$ is subtractive if $a - b \in R^*$ for all $a, b \in S$ such that $a \neq b$ and that $a_1, \dots, a_n \in R$ are well behaved if one of the following conditions are satisfied:

(i) $a_i - a_j \in R^*$ for all $i \neq j$;

(ii) there is $u \in \{1, \dots, n\}$ such that $a_j - a_h \in R^*$ for all $j, h \in \{1, \dots, n\}\backslash\{u\}$ such that $j \neq h$ and either $a_u = 0$ or R is local and $a_j - a_u \in R^*$ for all $j \neq u$.

Fix positive integers s, n_i and d_i, $1 \leq i \leq s$. Let $M(s; n_1, \dots, n_s; d_1, \dots,$

Received: July 3, 2006

$d_s; R)$ denote the R-module of all polynomials in the variables $x_{i,j}$, $1 \le i \le s$, $1 \le j \le d_i$, which have at most degree d_i with respect to the variables $x_{i,j}$, $1 \le j \le d_i$. Thus $M(s; n_1, \dots, n_s; d_1, \dots, d_s; R)$ is a free R-module with rank $\prod_{i=1}^{s} \binom{n_i+d_i}{n_i}$. Set $N := n_1 + \cdots + n_s$. Fix an integer $r > 0$, $P = (\bar{x}_{i,j}) \in R^N$ and a polynomial $f \in R[x_{i,j}]$. Consider the Taylor expansion of f at P (see [1]). We will say that f vanishes at P at least of order r if all the Taylor coefficients of f of with respect to $(x_{i,j} - \bar{x}_{i,j})^a$, a a multiindex with total degree $|a| \le r-1$, vanish. If V is a finitely-generated R-submodule of $R[x_{i,j}]$ and $T \subseteq R^n$ set $V(-rT) := \{f \in V : f \text{ vanishes at all } P \in E \text{ of order at least } r-1\}$. For any $P \in R^N$ and any $f \in R[x_{i,j}]$ let $\rho_{N,rP}(f)$ denote the set of all Taylor coefficients up to order $r-1$ and give an arbitrary ordering of it. Varying $f \in R[x_{i,j}]$ we get a free R-module $O(N, rP)$ of rank $\binom{N+r-1}{N}$. Fix an arbitrary ordering of the set of points of T and set $O(N, rT) = \oplus_{P \in T} O(N, rP)$. Thus $O(N, rT)$ is a free R-module of rank $\sharp(T) \cdot \binom{N+r-1}{N}$. Let $\rho_{N,rT} : R[x_{i,j}] \to O(N, rT)$ the associated map. We will call $\rho_{N,rT}$ the restriction map. Abusing notations, we will often write $\rho_{N,rT}$ instead of $\rho_{N,rT}|M(s; n_1, \dots, n_s; d_1, \dots, d_s; R)$. We will say that rT (or the pair (r, T)) has maximal rank with respect to $M(s; n_1, \dots, n_s; d_1, \dots, d_s; R)$ if $\mathrm{Im}(\rho_{N,rT}|M(s; n_1, \dots, n_s; d_1, \dots, d_s; R))$ is a free R-module with rank

$$\min\{\prod_{i=1}^{s} \binom{n_i + d_i}{n_i}, \sharp(T) \cdot \binom{N + r - 1}{N}\}.$$

Notice that if rT has maximal rank with respect to $\sharp(T) \cdot \binom{N+r-1}{N}$, then

$$\rho_{N,rT}|M(s; n_1, \dots, n_s; d_1, \dots, d_s; R))(-rT) = \mathrm{Ker}(\rho_{N,rT}|M(s; n_1, \dots, n_s; d_1, \dots, d_s; R))$$

is a free module with rank

$$\min\{0, \prod_{i=1}^{s} \binom{n_i + d_i}{n_i} - n^N \cdot \binom{N + r - 1}{N}\},$$

with the convention that $\{0\}$ is the only free R-module of rank 0. Fix a finite well adapted set $S \subseteq R$ and set $E := S^N$ (or E_N or $E_{N,S}$ if there is any danger of misunderstandings) and $n := \sharp(S)$.

Question 1. Find reasonable conditions on R, S, s, n_i, d_i, such that rE has maximal rank with respect to $M(s; n_1, \dots, n_s; d_1, \dots, d_s; R)$ or (a priori a weaker condition) such that $M(s; n_1, \dots, n_s; d_1, \dots, d_s; R)(-rE)$ is a free module of the expected rank

$$\min\{\prod_{i=1}^{s} \binom{n_i + d_i}{n_i} - n^N \cdot \binom{N + r - 1}{N}, 0\} \tag{1}$$

with the convention that $\{0\}$ is the only free R-module of rank 0. Do the same for all well adpted set with a fixed cardinality n.

Remark 1. Fix positive integers n, k, r and a well adpted set $S \subseteq R$ such that $\sharp(S) = n$. Let $u \in R[t]$ be a degree k polynomial vanishing at each point of S with order at least n. By [1], Lemma 2, u is divisible by the degree rn monic polynomial $\prod_{a\in S}(t-a)^r$. Thus $u \equiv 0$ if $k < rn$.

Remark 2. Take $s = 1$ and $n_1 = 1$. In this case Question 1 is true for all R, S, d_1, r ([1], Lemma 2).

Theorem 1. *Fix positive integers n, r, d and integers $n \geq x_1 \geq \cdots \geq x_n \geq 0$. Set $e := \lceil d/r \rceil$. Assume $rx_{ae+j} \geq d + 2 - j - ar$ for all integers $a \geq 0$, $1 \leq j \leq a$. Fix a well adapted $S \subset R$ such that $\sharp(S) = n$ and an ordering $a_1, \ldots, a_n$ of the elements of S. Fix any $T \subseteq E_{2,S}$ such that $\sharp(T \cap \{a_1\} \times R) = x_i$ for all i. Then $\rho_{2,rT}|M(1; 2; d; R)$ is injective and its cokernel is locally free.*

As a particular case of Theorem 1 we get the following result.

Corollary 1. *Fix positive integers n, r, d such that $rn \geq d+1$. Fix a well adapted $S \subset R$ such that $\sharp(S) = n$. Then $\rho_{2,rE_{2,S}}|M(1; 2; d; R)$ is injective and its cokernel is locally free.*

Theorem 2. *Fix positive integers n, r, d and integers $n \geq x_1 \geq \cdots \geq x_n \geq 0$. Set $e := \lceil d/r \lceil$. Assume $rx_{ae+j} \leq d + 2 - j - ar$ for all integers $a \geq 0$, $1 \leq j \leq a$. If $d = re$, then assume $x_j = 0$ for all $j > e$. If $d \neq re$, then assume $x_j = 0$ for all $j \geq e$. Fix a well adapted $S \subset R$ such that $\sharp(S) = n$ and an ordering $a_1, \ldots, a_n$ of the elements of S. Fix any $T \subseteq E_{2,S}$ such that $\sharp(T \cap \{a_1\} \times R) = x_i$ for all i. Then $\rho_{2,rT}|M(1; 2; d; R)$ is surjective.*

As a particular case of Theorem 2 we get the following result.

Corollary 2. *Fix positive integers n, r, d such that $d \geq 2rn$. Fix a well adapted $S \subset R$ such that $\sharp(S) = n$. Then $\rho_{2,rE_{2,S}}|M(1; 2; d; R)$ is surjective.*

In the general case we have the following result, whose easy proof by induction on N is omitted (see the proof of Theorem 1).

Theorem 3. *Fix positive integers s, n_i and d_i, $1 \leq i \leq s$, and a finite well adapted $S \subseteq R$. Set $n := \sharp(S)$. Assume $rn \geq d_i + 1$ for all i. Then $M(s; n_1, \ldots, n_s; d_1, \ldots, d_s; R)(-rE_{S,N}) = 0$.*

Proof of Theorem 1. Fix $f \in \mathrm{Ker}(\rho_{2,rT}|M(1; 2; d; R))$. We need to prove $f = 0$. Use coordinates z_1, z_2 on R^2. Notice that $M(1; 2; x; R)|\{a_i\} \times R = M(1; 1; x; R)$ for all $x \in \mathbb{N}$ (with the idetification of $\{a_i\} \times R$ with R.

(a) Here we will prove that $f = (\prod_{i=1}^{e}(z_1 - a_i)^r) \cdot u(z_1, z_2)$ for some

polynomial u such that $\deg(u) = d-re$ (with the convention $u \equiv 0$ if $d-re < 0$. By Remark 1 we get $f = (z_1 - a_1)g_1(z_1, z_2)$. Then we use $a_2, \dots, a_e$ instead of a_1. After $e-1$ steps we get $f = (\prod_{i=1}^{e}(z_1 - a_i)) \cdot u_1(z_1, z_2)$ for some polynomial u such that $\deg(u_1) = d - e$. Fix $a_h \in S$ and consider the Taylor expansion of f and u_1 at (a_1, a_h). We get that no monomial of the Taylor exapansion of u_1 with a non-zero coefficient is of the form $b(t - a_1)^c$ with $b(a_1, a_h) \neq 0$ and $c \leq r - 1$. Since this is true for all $a_h \in S$, Remark 1 implies the existence of a polynomial g_2 such that $u_1 = (z_1 - a_1)g_2$. Then using $a_2, \dots, a_r$ we get the existence of a polynomial u_2 such that $f = (\prod_{i=1}^{e}(z_1 - a_i)^2) \cdot u_2(z_1, z_2)$. If $r > 2$, then we repeat the same trick $r - 2$ times.

(b) Take $u(z_1, z_2)$ as in part (a). If $d - re < 0$, then $u \equiv 0$ and hence we are done. If $d-re \geq 0$, then we apply the proof of part (a) to the polynomial u using the points a_j with $e + 1 \leq j \leq 2e$, instead of the points $a_1, \dots, a_e$. After finitely many steps we get $f = 0$. □

Proof of Theorem 3. Repeat the proof of Theorem 2 using the word "injective" instead of the word "sujective". If at one step the proof that we get that a suitable R-submodule M of $M(1; 2; d; R)$ has the property that $\rho_{2,rT}|M$ is bijective. □

Acknowledgements

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

References

[1] M.A. Armand, List decoding of generalized Reed-Solomon codes over commutative rings, *IEEE Trans. Inf. Theory*, **51**, No. 1 (January 2005), 410-419.

[2] G.H. Norton, A. Sălăgean, On the key equation over a commutative ring, *Des., Codes Cryptogr.*, **20**, No. 2 (2000), 125-141.