The Construction of Multivariate Polynomials with Preassigned Zeros

H.M. MÖLLER, B. BUCHBERGER

April 1982

CAMP-Publ.-Nr.: 82-22.0
Type: Lecture Notes
(Proc. EUROCAM '82, LNCS 144, pp. 24-31)

Sponsored by: Österr. Fonds zur Förderung der wissenschaftlichen Forschung (Projekt Nr. 4567)

Working Group

CAMP-LINZ

(Computer-Aided Mathematical Problem Solving)

Address: Ordinariat Mathematik III
Johannes Kepler Universität
A4040 Linz, Austria (Europe)

THE CONSTRUCTION OF MULTIVARIATE POLYNOMIALS WITH PREASSIGNED ZEROS

H.M. Möller
Fernuniversität Hagen
D-5800 Hagen
W.-Germany

B. Buchberger
Universität Linz
A-4040 Linz
Austria

Abstract

We present an algorithm for constructing a basis of the ideal of all polynomials, which vanish at a preassigned set of points $\{y_1,\dots,y_m\} \subset K^n$, K a field. The algorithm yields also Newton-type polynomials for pointwise interpolation. These polynomials admit an immediate construction of interpolating polynomials and allow to shorten the algorithm, if it is applied to an enlarged set $\{y_1,\dots,y_{m_1}\} \subset K^n$, $m_1 > m$.

Introduction

In the univariate case n=1, the polynomials vanishing at a preassigned set of points $\{y_1,\dots,y_m\} \subset K^n$, K a field, are multiples of a fixed one, since they constitute an ideal and $K[x]$ is a principal ideal domain. For $n>1$ the situation is more complicated. The polynomials vanishing at $\{y_1,\dots,y_m\}$ constitute still an ideal $\underline{a}$, but $s>n$ polynomials $f_1,\dots,f_s$ are required to present the elements of $\underline{a}$ as $q_1f_1+\dots+q_sf_s$, $q_1,\dots,q_s$ polynomials, and the way to find the ideal basis $\{f_1,\dots,f_s\}$ is no longer as trivial as in the univariate case.

The knowledge of $\underline{a}$ or at least of its elements up to a certain polynomial degree is required in some areas of mathematics: In multivariate interpolation theory it facilitates answering questions of uniqueness and solvability in $K[x_1,\dots,x_n]/\underline{a}$, and representations of errors, c.f. G.Birkhoff [1]. In numerical integration theory ideals are used for the construction of cubature formulae, cf. H.M. Möller [5], H.J. Schmid [6]. And in approximation theory Ph. Defert and J.P. Thiran [3] recently showed an algorithm for constructing polynomials of best approximation, where the common zeros of the elements of $\underline{a}$ up to a fixed polynomial degree are required.

Especially for applications in numerical integration C. Günther [4] formulated an algorithm to find a (linear) basis for the space of polynomials in $\underline{a}$ of degree k, if $\underline{a}$ contains no non-zero polynomial of degree less than k. Our goal is to obtain all polynomials of $\underline{a}$. For this our algorithm constructs an ideal basis $\{f_1,\dots,f_l\}$ of $\underline{a}$ and, for reasons of application, the algorithm is constructed such that for any $f \in \underline{a}$

there are polynomials $q_1,\dots,q_l$ with $f = \Sigma q_i f_i$ and the degree of $q_i f_i$ is not greater than the degree of f, $i=1,\dots,l$.

In addition, polynomials $q_1,\dots,q_m$ of moderate degrees are constructed in the algorithm satisfying

$$q_j(y_{s_i}) = 0,\ i=1,\dots,j-1,\ q_j(y_{s_j}) = 1,$$

where $(s_1,\dots,s_m)$ denotes a permutation of $(1,\dots,m)$. In the univariate case, these are apart of normalization the Newton-polynomials

$$1,\ x-y_{s_1},\ (x-y_{s_1})(x-y_{s_2}),\dots,\ (x-y_{s_1})\dots(x-y_{s_{m-1}}).$$

Like the Newton-polynomials, $q_1,\dots,q_m$ admit an immediate construction of a polynomial, which interpolates a given function at $y_1,\dots,y_m$, and they are well suited for an enlargement of the number of interpolating conditions.

1. Basic definitions

In the following, N denotes the set of positive integers, K an arbitrary field, $\underline{F} := K[x_1,\dots,x_n]$ the ring of all polynomials over K in n indeterminates. Throughout the paper, we fix n and K. The special polynomials $x_1^{i_1}\dots x_n^{i_n}$ are called <u>monomials</u> <u>(terms)</u>.

1.1 Definition:

Degree $(x_1^{i_1}\dots x_n^{i_n}) := i_1+\dots+i_n$ (<u>degree of a monomial</u>).

$x_1^{i_1}\dots x_n^{i_n} <_T x_1^{j_1}\dots x_n^{j_n}$:

$\Longleftrightarrow$ Degree $(x_1^{i_1}\dots x_n^{i_n}) <$ Degree $(x_1^{j_1}\dots x_n^{j_n})$

or

(Degree$(x_1^{i_1}\dots x_n^{i_n}) =$ Degree$(x_1^{j_1}\dots x_n^{j_n})$

and $i_1 = j_1,\dots,\ i_k = j_k,\ i_{k+1} < j_{k+1}$ for some k with $1 \le k+1 \le n$)

(<u>graduated lexicographical ordering of monomials</u>).

1.2 Convention:

We assume the monomials to be ordered by $<_T$

$\phi_1,\phi_2,\dots$

i.e. $\{\phi_i; i\in N\} = \{x_1^{i_1}\dots x_n^{i_n}; i_1,\dots,i_n \in N\cup\{0\}\}$,

$\phi_1 <_T \phi_2 <_T \dots$

The symbols $f,g,\dots$ always denote polynomials,

$h,i,j,k,l,m,\dots$ non-negative integers,

$\underline{F},\underline{G},\dots$ sets of polynomials, and

$\underline{a}$ ... an ideal.

1.3 Example:

For n=2 we have

$\phi_1 = x_1^0 x_2^0,\ \phi_2 = x_1^0 x_2^1,\ \phi_3 = x_1^1 x_2^0,\ \phi_4 = x_1^0 x_2^2,\ \phi_5 = x_1^1 x_2^1,\ \ldots$.

1.4 Definition:

$$\underline{F}_k := \begin{cases} \{0\} & \text{if } k=0, \\ \mathrm{span}\{\phi_1,\ldots,\phi_k\} & \text{if } k>0. \end{cases}$$

$\mathrm{Hterm}(f) := \phi_{k+1}$ if $f \in \underline{F}_{k+1} \setminus \underline{F}_k$ (head-term of $f \neq 0$).

$\mathrm{Multiple}\ (x_1^{i_1} \ldots x_n^{i_n},\ x_1^{j_1} \ldots x_n^{j_n}) : \longleftrightarrow i_1 \geq j_1, \ldots, i_n \geq j_n$

($x_1^{i_1} \ldots x_n^{i_n}$ is a multiple of $x_1^{j_1} \ldots x_n^{j_n}$).

Degree (f) := Degree (Hterm(f)) (degree of a polynomial $f \neq 0$).

Degree (0) := -1.

1.5 Definition:

$\underline{a} = (f_1,\ldots,f_l) : \longleftrightarrow \underline{a} = \{\sum_{i=1}^{l} q_i f_i,\ q_1,\ldots,q_l \in \underline{F}\}$

($f_1,\ldots,f_l$ constitute a basis of a).

$\underline{a} = \langle f_1,\ldots,f_l \rangle : \longleftrightarrow \underline{a} = (f_1,\ldots,f_l)$ and for all k and all $f \in \underline{a} \cap \underline{F}_k$ there exist

$q_1,\ldots,q_l \in \underline{F}$ such that $f = \sum_{i=1}^{l} q_i f_i,\ q_1 f_1,\ldots,q_l f_l \in \underline{F}_k$

($f_1,\ldots,f_l$ constitute a Gröbner-basis of a).

$\underline{P}_k := \{f \in \underline{F}:\ \mathrm{Degree}\ (f) < k\}$.

We define inductively $\underline{G}_0(\underline{a}) := \underline{G}_0 := 0$, and if an $f \in \underline{a}$ exists with

(i) $\mathrm{Hterm}(f) = \phi_k$

(ii) $f - \phi_k \in \underline{F}_{k-1}$

(iii) For all $q \in \underline{G}_{k-1} = \underline{G}_{k-1}(\underline{a}) : \neg\ \mathrm{Multiple}\ (\phi_k, \mathrm{Hterm}(q))$

then $\underline{G}_k := \underline{G}_k(\underline{a}) := \underline{G}_{k-1} \cup \{f\}$ and else $\underline{G}_k := \underline{G}_k(\underline{a}) := \underline{G}_{k-1}$

(Gröbner-basis-generators).

If $\{\underline{G}_i\}_{i>0}$ is a set of Gröbner-basis-generators, then

$\underline{CC}(\{\underline{G}_i\};k_0) : \longleftrightarrow$ for all $q \in \underline{a} \setminus \underline{F}_{k_0}$ there exists $f \in \underline{G}_{k_0}$:

Multiple (Hterm(q), Hterm(f)) (Chain-condition of order k_0 for $\{\underline{G}_i\}$).

2. Elementary properties

2.1 Lemma:

(E1) Property of $<_T$

$\phi_i <_T \phi_k \longrightarrow \phi_i \cdot \phi_l <_T \phi_k \cdot \phi_l$.

(E2) Property of Multiple

Multiple $(\mathrm{Hterm}(f_1), \mathrm{Hterm}(f_2)) \longrightarrow$ there exists $q \in \underline{F}$ such that

$\mathrm{Hterm}(f_1 - qf_2) <_T \mathrm{Hterm}(f_1)$.

(E3) Connection of $\underline{P}_l$ and $\underline{F}_k$

$$k = \binom{l+n}{n} \longrightarrow \underline{P}_l = \underline{F}_k.$$

(E4) Property of Gröbner-basis

$\underline{a}$ ideal $\longrightarrow$ there exist $f_1,\dots,f_l \in \underline{a}$ such that $\underline{a} = \langle f_1,\dots,f_l \rangle$.

(E5) Property of Gröbner-basis-generators

If $\{\underline{G}_i\}$ are Gröbner-basis-generators for $\underline{a}$, then for $k>1$ and for all $f \in \underline{a} \cap \underline{F}_k$

there exist $q_1,\dots,q_l \in \underline{F}$ such that $f = \sum_{i=1}^{l} q_i f_i$, $q_1 f_1,\dots,q_l f_l \in \underline{F}_k$,

where $\{f_1,\dots,f_l\} = \underline{G}_k$.

(E6) Chain-condition

$\underline{CC}(\{\underline{G}_i\},k_0) \longrightarrow \underline{G}_0 \subseteq \underline{G}_1 \quad \dots \subseteq \underline{G}_{k_0} = \underline{G}_{k_0+1} = \underline{G}_{k_0+2} = \dots \longrightarrow \underline{a} = \langle \underline{G}_{k_0} \rangle$.

2.2 Proofs:

In general the proofs for these properties are immediate.

Ad (E4): The existence of a Gröbner-basis follows from the fact, that the ring $K[x_1,\dots,x_n]$ is noetherian. A constructive proof is given by B. Buchberger [2].

Ad (E5): Induction on k. Evidently (E5) holds for $k=1$. Let $f \in \underline{a} \cap \underline{F}_k$ with $\mathrm{Hterm}(f) = \phi_k$. By normalization $f - \phi_k \in \underline{F}_{k-1}$.

Case 1: $\underline{G}_k = \underline{G}_{k-1}$. Then there exists $f_2 \in \underline{G}_{k-1}$ such that Multiple $(\phi_k, \mathrm{Hterm}(f_2))$.

Hence, by (E2) there exists $q \in \underline{F}$ such that $qf_2 \in \underline{F}_k$ and $f - qf_2 \in \underline{F}_{k-1}$.

Now, $f - qf_2 \in \underline{a}$. The induction hypothesis applied to $f - qf_2$ yields finally the required representation for f.

Case 2: $\underline{G}_k = \underline{G}_{k-1} \cup \{f_l\}$. Then $f - f_l \in \underline{a} \cap \underline{F}_{k-1}$, and the induction hypothesis applied to $f - f_l$ yields the assertion.

Ad (E6): By the chain condition, we have especially:

For all $k>k_0$ and for all $q \in \underline{a} \cap \underline{F}_k$ there exists $f \in \underline{G}_{k_0}$ such that Multiple $(\mathrm{Hterm}(q), \mathrm{Hterm}(f))$.

Hence $\underline{G}_{k_0+1}, \underline{G}_{k_0+2}, \dots$ do not contain more elements than $\underline{G}_{k_0}$.

3. Description of the algorithm

Let points $y_1,\dots,y_m \in K^n$ be given.

3.1 Problem:

Construct a Gröbner-basis $\langle f_1,\dots,f_l \rangle$ for the ideal

$\underline{a} = \{f \in \underline{F};\ f(y_1) = \dots = f(y_m) = 0\}$

and find a permutation $(s_1,\dots,s_m)$ of $(1,\dots,m)$ and m polynomials $q_1,\dots,q_m$ with

$q_i(y_{s_j}) = 0,\ j = 1,\dots,i-1,$

$q_i(y_{s_i}) = 1.$

3.2 Algorithm:

STEP 0 (The constant polynomials):

$s_1 := 1;\ q_1 := \phi_1;\ z_1 := (\phi_1(y_1),\dots,\phi_1(y_m));$

$l_2 := 1;\ h_0 := 1;\ l_1 := 0;$

STEP 1 (Preparation of the first loop):

$h_1 := 0;\ k := 2;\ j := 1;$

STEP 2 (Elimination):

$z := (\phi_k(y_1),\dots,\phi_k(y_m));$

$f := \phi_k;$

<u>for</u> $i = 1(1)l_2$ <u>do</u> <u>begin</u>

$z := z - z^{(s_i)} z_i;$

$f := f - z^{(s_i)} q_i$ <u>end</u>;

STEP 3 (f into the basis or into $\{q_1,\dots,q_m\}$):

<u>If</u> $z \neq o$ <u>then</u> <u>begin</u>

$l_2 := l_2 + 1;\ s_{l_2} := \min\{i; z^{(i)} \neq 0\}$;

$z_{l_2} := z/z^{(s_{l_2})};\ q_{l_2} := f/z^{(s_{l_2})};$

$h_j := h_j + 1$ <u>end</u>

<u>else</u> <u>begin</u>

$l_1 := l_1 + 1;\ f_{l_1} := f$ <u>end</u>;

STEP 4 (Termination test):

<u>If</u> $k = \binom{j+n}{n}$ <u>then</u> <u>begin</u>

<u>if</u> $h_j = 0$ <u>then</u> <u>go</u> <u>to</u> FINALLY

<u>else</u> <u>begin</u>

$j := j+1;\ h_j := 0$ <u>end</u> <u>end</u> ;

STEP 5 (From $\underline{F}_k$ to $\underline{F}_{k+1}$):

$k := k+1;$

<u>for</u> $i = 1(1)l_1$ <u>do</u>

<u>if</u> Multiple (ϕ_k, H term(f_i)) <u>then</u> <u>go</u> <u>to</u> STEP 4;

<u>go</u> <u>to</u> STEP 2;

FINALLY: $l := l_1;\ m_0 := j;\ k_0 := k;\ m_1 := l_2;$

3.3 Meaning of the symbols used in the algorithm:

k: index of the space $\underline{F}_k$, which is actually analyzed

l_1: number of polynomials f_i in $\underline{F}_k$

l_2: number of polynomials q_i in $\underline{F}_k$

$j := \text{Degree}(\phi_k)$

h_j: number of polynomials $q_i \in \underline{F}_k$ with Degree $(q_i) = j$

f: polynomial with H coeff$(f) = \phi_k$

$z := (f(y_1),\ldots,f(y_m))$

$z_i := (q_i(y_1),\ldots,q_i(y_m))$

$z^{(i)}$: the i-th component of z

l: total number of polynomials f_i

m_0: upper bound for max $\{\text{Degree}(f_i);\ i=1,\ldots,l\}$

m_1: total number of polynomials q_i

3.4 Theorem:

(P1): The algorithm terminates.

(P2): The sets $\underline{G}_k := \{f_i; i \in \{1,\ldots,l\}, f_i \in \underline{F}_k\}$ constitute a set of Gröbner-basis-generators for $\underline{a}$, satisfying a chain condition of order k_0.

(P3): $\underline{a} = \langle f_1,\ldots,f_l\rangle$.

(P4): $m=m_1$.

(P5): $q_i(y_{s_i})=1,\ q_i(y_{s_j})=0$ for $j=1,\ldots,i-1;\ i=1,\ldots,m$.

(P6): $\text{Degree}(q_1) < \text{Degree}(q_2) < \ldots < \text{Degree}(q_m) = m_0-1$.

3.5 Proofs:

In the algorithm $h_0+h_1+\ldots+h_j$ denotes, how many components of z at least can be reduced to 0 in the next STEP2. This yields

$$h_0 + \ldots + h_j \leq m.$$

Ad (P1): The algorithm terminates not later than for $k = \binom{m+n}{n}$, because assuming

$k = \binom{j+n}{n}$ and $h_j \geq 1$ for $j=0,\ldots,m$, we obtain

$$h_0 + \ldots + h_m \geq m + 1 > m,$$

a contradiction, and hence there is a

$$k_0 \in \{ \binom{n}{n}, \binom{1+n}{n}, \ldots, \binom{m+n}{n} \} \text{ such that } k_0 = \binom{m_0+n}{n},\ h_{m_0} = 0.$$

Ad (P2): By construction $\{\underline{G}_k\}_{k\geq 0}$ constitutes a set of Gröbner-basis-generators. $h_{m_0} = 0$ for $k_0 = \binom{m_0+n}{n}$ implies Degree $(q_i) \neq m_0$ for all $i \in \{1,\ldots,m_1\}$

or, equivalently,

Degree $(\phi_k) = m_0 \dashrightarrow$ there exists $f_i \in \underline{F}_k$ such that Hterm $f_i = \phi_k$, $f_i \in \underline{G}_k \subset \underline{a}$

or

there exists $f_i \in \underline{F}_{k-1}$ such that Multiple $(\phi_k, \text{Hterm}(f_i))$.

Now let $f \in \underline{F} \setminus \underline{F}_{k_0}$. Because of $\underline{F}_{k_0} = \underline{P}_{m_0}$ we have Degree $(f) > m_0$.
Therefore there exists ϕ_k such that Degree $(\phi_k) = m_0$, Multiple $(\text{Hterm}(f), \phi_k)$, $k<k_0$.
Combining with the implication for Degree $(\phi_k) = m_0$, we obtain:
There exists $f_i \in \underline{G}_k$ such that Multiple $(\text{Hterm}(f), \underbrace{\text{Hterm}(f_i)}_{=\phi_k})$, $k<k_0$, or there exists $f_i \in \underline{G}_{k-1}$ such that Multiple $(\phi_k, \text{Hterm}(f_i))$, $k<k_0$.

Using the transitivity of Multiple, the latter alternative gives:
There exists $f_i \in \underline{G}_{k-1}$ such that Multiple $(\text{Hterm}(f), \text{Hterm}(f_i))$.

This conclusion holds true especially for $f \in \underline{a} \setminus \underline{F}_{k_0}$. Thus $\{\underline{G}_k\}_{k>0}$ satisfies the chain-condition of order k_0.

Ad (P3): (P2) and (E6) imply (P3).

Ad (P4) and (P5): Obviously Newton polynomials q_i^* exist satisfying $q_i^*(y_{s_i}) = 1$ and $q_i^*(y_{s_j}) = 0$, $j=1,\ldots,i-1$; $i=1,\ldots,m$.

Assume $m_1 < m$. Then $q_i^* \in \underline{F}_{k_0}$ for some i.

Using (E2) and the chain condition of order k_0, we obtain inductively:
For all $i \in \{1,\ldots,m\}$ there exist $q_{i_1},\ldots,q_{i_l} \in \underline{F}$ and an $h_i \in \underline{F}_{k_0}$ such that

$$q_i^* = h_i + \sum_{j=1}^{l} q_{i_j} f_j,$$

where h_i contains only terms that are not multiple of any $\text{Hterm}(f_j)$ and $h_i(y_k) = q_i^*(y_k)$. Hence we may assume $h_i = q_i^*$, but $h_i \in \underline{F}_{k_0}$ for $i=1,\ldots,m$, contradicting $q_i^* \in \underline{F}_{k_0}$ for some i. Thus, we have (P4). (P5) holds by construction of $q_1,\ldots,q_{m_1}$.

Ad (P6): By construction $\text{Hterm}(q_i) <_T \text{Hterm}(q_{i+1})$, hence there exists $i \in \{1,\ldots,m-1\}$ such that Degree $(q_i) <$ Degree (q_{i+1}).
The algorithm terminates if and only if for a $j \in N$ no headterm of degree j leads to a polynomial q_i in STEP3, whereas for any $j_1 < j$, $j_1 \in N$ such a headterm exists. This gives Degree $(q_m) = m_0 - 1$.

4. Concluding remarks

At some passages in the algorithm, properties of the graduated lexicographical ordering are used implicitly. Analyzing these passages, we found that apart of the termination criterion only properties (E1) and $\phi_1 = x_1^0 \dots x_n^0$ of the ordering were required. Using any other ordering of the monomials, which satisfies (E1) and $\phi_1 = x_1^0 \dots x_n^0$, e.g. the lexicographical ordering

$x_1^{i_1} \dots x_n^{i_n} < x_1^{j_1} \dots x_n^{j_n}$: $\Longleftrightarrow$ there exists a $k \leq n$ such that

$i_1 = j_1, \dots, i_{k-1} = j_{k-1}, i_k < j_k$,

"only" an appropriate termination criterion must be found. The remaining steps of the algorithm stay unchanged.

For termination our algorithm uses an a-posteriori-criterion ($h_j^* = 0$ and $k = \binom{k+n}{n}$) and in the proofs 3.5 we showed the a-priori-criterion $k < \binom{m+n}{n}$ for the termination. These bounds are the only sharp bounds for $n=1$. For $n>1$ various examples exist to show their sharpness. Dependent on m and the degrees of $f_1, \dots, f_l$ other a-posteriori-criteria for termination can be found at least for $n=2$. Their derivation requires some auxiliary results from ideal theory and are omitted in this paper. Finally, we mention that the set-up realized in the above algorithm should be useful for obtaining (Gröbner-)bases also in other situations where ideals are "given" by properties and not by bases.

Acknowledgement: This work has been sponsored by the Österr. Fonds zur Förderung der wissenschaftlichen Forschung (Project Nr. 3877).

References

[1] G. Birkhoff, The algebra of multivariate interpolation, in: Constructive Approaches to Mathematical Models (ed.: C.V. Coffman and G.J. Fix), Academic Press 1979, p. 345-363.

[2] B. Buchberger, A theoretical basis for the reduction of polynomials to canonical forms, ACM SIGSAM Bulletin 39, August 1976, p. 19-29.

[3] Ph. Defert and J.P. Thiran, Chebyshev approximation by multivariate polynomials, Report 80/10, Facultés Universitaires de Namur, Belgium, 1980.

[4] C. Günther, IPOL - Ein Fortran-Programm zur zweidimensionalen Interpolation, Report KFK 2175, Kernforschungszentrum Karlsruhe, W.-Germany, November 1975.

[5] H.M. Möller, Mehrdimensionale Hermite-Interpolation und numerische Integration, Math. Z. 148 (1976), 107-118.

[6] H.J. Schmid, Interpolatory cubature formulae and real ideals, in: Quantitative Approximation (ed.: Ronald A. deVore and K. Scherer), Academic Press 1980, p. 245-254.