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
A-4040 Linz, Austria (Europe)

Permission to copy is granted provided the author's copyright notice, the title of the publication and its date appear.
THE CONSTRUCTION OF MULTIVARIATE POLYNOMIALS WITH PREASSIGNED ZEROS

H.M. Müller
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 \( \{y_1, \ldots, y_m\} \subseteq \mathbb{K}^n \), \( \mathbb{K} \) 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 \( \{y_1, \ldots, y_m\} \subseteq \mathbb{K}^n \), \( m > m \).

Introduction
In the univariate case \( n=1 \), the polynomials vanishing at a preassigned set of points \( \{y_1, \ldots, y_m\} \subseteq \mathbb{K}^n \), \( \mathbb{K} \) a field, are multiples of a fixed one, since they constitute an ideal and \( \mathbb{K}[x] \) is a principal ideal domain. For \( n \geq 2 \) the situation is more complicated. The polynomials vanishing at \( \{y_1, \ldots, y_m\} \) constitute still an ideal \( \mathfrak{a} \), but \( \mathfrak{a} \) is not a principal ideal domain. The polynomials \( f_1, \ldots, f_5 \) are required to present the elements of \( \mathfrak{a} \) as \( q_1 f_1 \ldots f_5 \). The way to find the ideal basis \( \{f_1, \ldots, f_5\} \) is no longer as trivial as in the univariate case.

The knowledge of \( \mathfrak{a} \) 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 \( \mathbb{K}[x_1, \ldots, x_n] / \mathfrak{a} \), and representations of errors, c.f. G. Birkhoff [1]. In numerical integration theory ideals are used for the construction of cubature formulae, c.f. H.M. Müller [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 \( \mathfrak{a} \) 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 \( \mathfrak{a} \) of degree \( k \), if \( \mathfrak{a} \) contains no non-zero polynomial of degree less than \( k \). Our goal is to obtain all polynomials of \( \mathfrak{a} \). For this our algorithm constructs an ideal basis \( \{f_1, \ldots, f_1\} \) of \( \mathfrak{a} \) and, for reasons of application, the algorithm is constructed such that for any \( f \in \mathfrak{a} \)
there are polynomials $q_1, \ldots, q_l$ with $f = \Sigma i q_i f_i$ and the degree of $q_i f_i$ is not greater than the degree of $f$, $i=1, \ldots, l$.

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

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

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

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

Like the Newton-polynomials, $q_1, \ldots, q_m$ admit an immediate construction of a polynomial, which interpolates a given function at $y_1, \ldots, y_m$, 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, $F := K[x_1, \ldots, x_n]$ the ring of all polynomials over $K$ in $n$ indeterminates. Throughout the paper, we fix $n$ and $K$. The special polynomials $x_1^{i_1} \ldots x_n^{i_n}$ are called monomials (terms).

1.1 Definition:

Degree $(x_1^{i_1} \ldots x_n^{i_n}) := i_1 + \ldots + i_n$ (degree of a monomial).

$x_1^{i_1} \ldots x_n^{i_n} \preceq \Sigma x_1^{j_1} \ldots x_n^{j_n}$:

$\Longleftrightarrow$ Degree $(x_1^{i_1} \ldots x_n^{i_n}) \preceq$ Degree $(x_1^{j_1} \ldots x_n^{j_n})$

or

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

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

(graded lexicographical ordering of monomials).

1.2 Convention:

We assume the monomials to be ordered by $\preceq$

$1, 2, \ldots,

\text{i.e. } \{x_1^{i_1} \ldots x_n^{i_n} \mid i_1, \ldots, i_n \in N \cup \{0\}\setminus\{0\} \},$

$\preceq \preceq 2 \preceq \ldots$

- upper case letters $f, g, \ldots$ always denote polynomials,
- $h, i, j, k, l, m, \ldots$ non-negative integers,
- $\mathcal{E}, \mathcal{G}, \ldots$ sets of polynomials, and
- $\mathfrak{a}$ ... an ideal.
1.3 Example:
For \( n = 2 \) we have:
\[
q_1 = x_1^0 \cdot x_2^0, \quad q_2 = x_1^0 \cdot x_2^1, \quad q_3 = x_1^1 \cdot x_2^0, \quad q_4 = x_1^0 \cdot x_2^2, \quad q_5 = x_1^1 \cdot x_2^1, \ldots
\]

1.4 Definition:

\[
F_k := \begin{cases} 
  \{0\} & \text{if } k = 0, \\
  \text{span}\{q_1, \ldots, q_k\} & \text{if } k > 0.
\end{cases}
\]

\( H_{\text{term}}(f) := q_{k+1} \) if \( f \in F_k \cap F_{k+1} \) (head-term of \( f \neq 0 \)).

Multiple \( (x_1^{i_1} \ldots x_n^{i_n}, x_1^{j_1} \ldots x_n^{j_n}) \) : \( \langle \ldots \rangle \)

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

Degree \( (f) := \text{Degree } (H_{\text{term}}(f)) \) (degree of a polynomial \( f \neq 0 \)).
Degree \( (0) := -1 \).

1.5 Definition:

\( \mathfrak{a} = (f_1, \ldots, f_l) : \langle \ldots \rangle \mathfrak{a} = \left\{ \sum_{i=1}^1 q_i f_i, q_1, \ldots, q_l \in F \right\} \)

\( (f_1, \ldots, f_l \) constitute a basis of \( \mathfrak{a} \).

\( \mathfrak{a} = \langle f_1, \ldots, f_l \rangle : \langle \ldots \rangle \mathfrak{a} = (f_1, \ldots, f_l) \) and for all \( k \) and all \( f \in \mathfrak{a} \cap F_k \) there exist \( q_1, \ldots, q_l \in F \) such that
\[
\sum_{i=1}^1 q_i f_i, q_1 f_1, \ldots, q_l f_l \in F_k
\]

\( (f_1, \ldots, f_l \) constitute a Gröbner-basis of \( \mathfrak{a} \).

\( P_k := \{ f \in F : \text{Degree } (f) < k \} \).

We define inductively \( G_0(\mathfrak{a}) := G_0 := 0 \), and if an \( f \in \mathfrak{a} \) exists with

(i) \( H_{\text{term}}(f) = q_k \)
(ii) \( f = q_k \in F_{k-1} \)
(iii) For all \( q \in G_{k-1} \) \( \Rightarrow \) Multiple \( (q_k, H_{\text{term}}(q)) \) then \( G_k := G_k(\mathfrak{a}) := G_{k-1} \cup \{ f \} \) and else \( G_k := G_k(\mathfrak{a}) := G_{k-1} \)
(Gröbner-basis-generators).

If \( \{ q_i \}_{i \geq 0} \) is a set of Gröbner-basis-generators, then

\( CC(\{ q_i \}, k_0) : \langle \ldots \rangle \) for all \( q \in \mathfrak{a} \cap F_{k_0} \) there exists \( f \in G_{k_0} \);
Multiple \( (H_{\text{term}}(q), H_{\text{term}}(f)) \) (Chain-condition of order \( k_0 \) for \( \{ q_i \} \)).
2. Elementary properties

2.1 Lemma:

(E1) Property of \( T \)

\[ q_i \in T_k \quad \rightarrow \quad q_i \in T_{k+1} \]

(E2) Property of Multiple

Multiple \((\text{Hterm}(f_1), \text{Hterm}(f_2))\) \(\rightarrow\) there exists \( q \in F \) such that \( \text{Hterm}(f_1 - qf_2) \subseteq \text{Hterm}(f_1) \).

(E3) Connection of \( P_l \) and \( F_k \)

\[ k = \binom{l+m}{m} \quad \rightarrow \quad P_l = F_k. \]

(E4) Property of Gröbner-basis

\( a \) ideal \(\rightarrow\) there exist \( f_1, \ldots, f_l \in a \) such that \( a = \langle f_1, \ldots, f_l \rangle \).

(E5) Property of Gröbner-basis-generators

If \( \{g_i\} \) are Gröbner-basis-generators for \( a \), then for \( k \leq 1 \) and for all \( f \in a \cap F_k \)

there exist \( q_1, \ldots, q_l \in F_k \) such that \( f = \sum_{i=1}^{l} q_if_i \),

where \( \{f_1, \ldots, f_l\} = G_k \).

(E6) Chain-condition

\[ \text{CC}(\{g_i\}, k_0) \quad \rightarrow \quad G_0 \subseteq G_1 \quad \subseteq \cdots \subseteq G_{k_0} = G_{k_0+1} = G_{k_0+2} = \cdots \quad \rightarrow \quad a = \langle G_{k_0} \rangle. \]

2.2 Proofs:

In general the proofs for these properties are immediate.

\( \text{Ad.} \) (E4): The existence of a Gröbner-basis follows from the fact, that the ring \( \mathbb{k}[x_1, \ldots, x_n] \) is noetherian. A constructive proof is given by B. Buchberger [2].

\( \text{Ad.} \) (E5): Induction on \( k \). Evidently (E5) holds for \( k = 1 \). Let \( f \in a \cap F_k \) with \( \text{Hterm}(f) = \phi_k \). By normalization \( f - \phi_k \in F_{k-1} \).

Case 1: \( G_k = G_{k-1} \). Then there exists \( f_2 \in G_{k-1} \) such that Multiple \((\phi_k, \text{Hterm}(f_2))\).

Hence, by (E2) there exists \( q \in F_k \) such that \( qf_2 \in F_k \) and \( f - qf_2 \in F_{k-1} \).

Now, \( f - qf_2 \in \phi \). The induction hypothesis applied to \( f - qf_2 \) yields finally the required representation for \( f \).

Case 2: \( G_k = G_{k-1} \cup \{f_1\} \). Then \( f - f_1 \in a \cap F_{k-1} \), and the induction hypothesis applied to \( f - f_1 \) yields the assertion.

\( \text{Ad.} \) (E6): By the chain condition, we have especially:

for all \( k \leq 0 \) and for all \( a \in a \cap F_k \) there exists \( f \in G_{k_0} \) such that

\( \text{Multiple}(a, \text{Hterm}(f)) \).

\( G_{k_0}, G_{k_0+1}, G_{k_0+2}, \ldots \) do not contain more elements than \( G_{k_0} \).
3. Description of the algorithm

Let points \( y_1, \ldots, y_m \in K^n \) be given.

3.1 Problem:
Construct a Gröbner-basis \( \langle f_1, \ldots, f_l \rangle \) for the ideal
\[
\mathfrak{a} = \{ f \in K[x_1, \ldots, x_n] : f(y_1) = \ldots = f(y_m) = 0 \}
\]
and find a permutation \( (s_1, \ldots, s_m) \) of \( (1, \ldots, m) \) and \( m \) polynomials \( q_1, \ldots, q_m \) with
\[
q_i(y_{s_j}) = 0, j = 1, \ldots, i-1, \\
q_i(y_{s_j}) = 1.
\]

3.2 Algorithm:

**STEP 0** (The constant polynomials):
\[
s_1 := 1; \quad q_1 := \phi_1; \quad z_1 := (q_1(y_1), \ldots, q_1(y_m)); \\
l_2 := 1; \quad h_0 := 1; \quad l_1 := 0;
\]

**STEP 1** (Preparation of the first loop):
\[
h_1 := 0; \quad k := 2; \quad j := 1;
\]

**STEP 2** (Elimination):
\[
z := (q_k(y_1), \ldots, q_k(y_m)); \\
f := \phi_k;
\]

for \( i = 1 \) to \( l_1 \) do begin
\[
z := z - z(s_i)z_j; \\
f := f - f(s_i)q_i
\]
end;

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

If \( z = 0 \) then begin
\[
l_2 := l_2 + 1; \quad s_{l_2} := \min \{ i : z(i) \neq 0 \}; \\
z_{l_2} := z/s_{l_2}; \quad q_{l_2} := f/z(s_{l_2}); \\
h_j := h_j + 1
\]
end;

else begin
\[
l_1 := l_1 + 1; \quad f_{l_1} := f
\]
end;

**STEP 4** (Termination test):

If \( k = \ell \) then begin
\[
\text{if } h_j = 0 \text{ then go to FINALLY}
\]
else begin
\[
\text{j := j+1; \quad h_j := 0 end end;}
\]

**STEP 5** (From \( f_k \) to \( f_{k+1} \)):
\[
k := k+1;
\]

for \( i = 1 \) to \( l_1 \) do
\[
\text{if Multiple } (q_k, H \text{ term}(f_i)) \text{ then go to STEP 4;}
\]
\[
\text{go to STEP 2;}
\]

FINALLY: \( l := l_1; \quad m_0 := j; \quad k_0 := k; \quad m_1 := l_2;\)
3.3 Meaning of the symbols used in the algorithm:

k: index of the space \( F_k \), which is actually analyzed

11: number of polynomials \( f_1 \) in \( F_k \)

12: number of polynomials \( q_1 \) in \( F_k \)

\( j = \text{Deg}(q_k) \)

\( h_j \): number of polynomials \( q_j \in F_k \) with \( \text{Deg}(q_j) = i \)

\( f : \) polynomial with \( H \text{coeff}(f) = q_k \)

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

\( z_j := (q_j(y_1), \ldots, q_j(y_m)) \)

\( z(i) \): the \( i \)-th component of \( z \)

\( n \): total number of polynomials \( f_1 \)

\( m_0 \): upper bound for \( \max \{ \text{Deg} (f_i) ; i=1, \ldots, n \} \)

\( m_1 \): total number of polynomials \( q_i \)

3.4 Theorem:

(P1): The algorithm terminates.

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

(P3): \( a = \langle f_1, \ldots, f_1 \rangle \).

(P4): \( m = m_1 \).

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

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

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

\( h_0 + \ldots + h_j < m \).

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

\( k = \binom{k}{n} \) and \( h_j > 1 \) for \( j=0, \ldots, m \), we obtain

\( h_0 + \ldots + h_m > m + 1 \geq m \),

a contradiction, and hence there is a

\( k_0 \in \{ \binom{m}{n} , \binom{m+n}{n}, \ldots, \binom{m+n}{n} \} \) such that \( k_0 = \binom{m+n}{n} \), \( h_{m_0} = 0 \).

Ad (P2): By construction \( \langle F_k \rangle k \geq 0 \) constitutes a set of Gröbner-basis-generators.

\( m = 0 \) for \( k_0 = \binom{m+n}{n} \) implies \( \text{Deg}(q_i) < m_0 \) for all \( i \in \{ 1, \ldots, m_1 \} \)

\( m = 0 \). Equivalently,
Degree \( (\phi_k) = m_0 \rightarrow \) there exists \( f_i \in F_k \) such that \( \text{Hterm} f_i = \phi_k, f_i \in \mathcal{S}_k \subset \mathcal{F}_k \)
or there exists \( f_i \in F_{k-1} \) such that \( \text{Multiple} (\phi_k, \text{Hterm}(f_i)). \)

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

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

This conclusion holds true especially for \( f \in \mathcal{S}_1 \cap \mathcal{F}_{k_0}. \) Thus \( \{ \mathcal{S}_k \}_{k>0} \) satisfies the chain-condition of order \( k_0. \)

\text{Ad}_-(\text{P3}): \text{P2} \) and \( \text{E6} \) imply \( \text{P3}. \)

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

Assume \( m_0 \mid m. \) Then \( q_i^* \in \mathcal{F}_{k_0} \) for some \( i. \)

Using \( \text{E2} \) and the chain condition of order \( k_0, \) we obtain inductively:
For all \( i \in \{1, ..., m\} \) there exist \( q_{i_1}, ..., q_{i_1} \in \mathcal{F}_k \) and an \( h_i \in \mathcal{F}_{k_0} \) such that
\[
1 = q_i^* = h_i + \sum_{j=1}^{i} q_{i_j}^* f_{i_j},
\]
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 \( h_i = 1, \) but \( h_i \in \mathcal{F}_{k_0} \) for \( i=1, ..., m, \) contradicting \( q_i^* \in \mathcal{F}_{k_0} \) for some \( i. \) Thus, we have \( \text{P4}. \) \( \text{P5} \) holds by construction of \( q_1, ..., q_m. \)

\text{Ad}_-(\text{P5}): \) By construction \( \text{Hterm}(q_i) \subset \text{Hterm}(q_{i+1}), \) hence there exists
\( i \in \{1, ..., m-1\} \) such that \( \text{Degree} (q_i) < \text{Degree} (q_{i+1}). \)
The algorithm terminates if and only if for \( a_i \in N \) no headterm of degree \( i \) leads to
a polynomial \( q_i \) in \text{STEP3}, whereas for any \( i_1 < i, j_1 \in N \) such a headterm exists. This
\( q_i \) gives \( \text{Degree} (q_m) = m_0 - 1. \)

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 $\phi_1 = x_1^0 \ldots x_n^0$ of the ordering were required. Using any other ordering of the monomials, which satisfies (E1) and $\phi_1 = x_1^0 \ldots x_n^0$, e.g. the lexicographical ordering $x_1^{j_1} \ldots x_n^{j_n} \prec x_1^{i_1} \ldots x_n^{i_n}$ implies there exists a $k \in \mathbb{N}$ such that $i_1 = j_1, \ldots, i_{k-1} = j_{k-1}, i_k \prec j_k$. "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 $n \geq 1$ various examples exist to show their sharpness. Dependent on $m$ and the degrees of $f_1, \ldots, f_1$ other a-posteriori-criteria for termination can be found at least for $n \geq 2$. 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 OeSterr. Fonds zur Förderung der wissenschaftlichen Forschung (Project Nr. 3877).

References


