Systems of Algebraic Equations Solved by Means of Endomorphisms *

H. Michael Möller

FB Mathematik der FernUniversität Hagen, W-5800 Hagen, Germany

Abstract. Recently, several authors studied methods based on endomorphisms for localizing and computing the common zeros of systems of polynomial equations $f_i(x_1, \ldots, x_n) = 0,\ i = 1, \ldots, s$, in case the ideal $\mathcal{I}$ generated by $f_1, \ldots, f_s$ has dimension zero. The main idea is to consider the trace and the eigenvalues of the endomorphisms $\Phi_f : [g] \mapsto [g \cdot f]$, where [.] denotes equivalence classes modulo $\mathcal{I}$ in the polynomial ring. In this paper we give discuss some of these methods and combine them with the concept of dual bases for describing zero dimensional ideals.

1 Introduction

The interpretation of polynomial rings $\mathcal{P}$ and ideals $\mathcal{I} \subset \mathcal{P}$ as k-vector spaces has been fruitful for getting insight into the ideal structure and for improving existing methods. In computer algebra, Lazard investigated this connection early [La 77],[La 81], and Buchberger never failed in his development of Gröbner basis techniques to stress the connection to linear algebra e.g. [Bu 88], but also many other authors mentioned this connection and investigated ideals with linear techniques.

However, the multiplicative structure of $\mathcal{P}$ and $\mathcal{P}/\mathcal{I}$ has, at least implicitely, always been used. This was done by considering with a coefficient vector of a polynomial f the "shifted" coefficient vectors for power product multiples of f. And, mentioned just for curiosity, starting point for the development of Gröbner basis techniques was Gröbner's proposal to Buchberger to develop a method for computing the multiplication table of $\mathcal{P}/\mathcal{I}$, [Bu 65].

In recent years, the interest in the multiplicative structure has been renewed. By using the endomorphisms

$$\Phi_f : \mathcal{P}/\mathcal{I} \longrightarrow \mathcal{P}/\mathcal{I},\ \Phi_f([u]) := [f \cdot u]$$

where $[u]$ denotes the equivalence class modulo $\mathcal{I}$ generated by $u \in \mathcal{P}$, some new results or new interpretations of old results have been found. In this paper, we concentrate on zero dimensional ideals $\mathcal{I}$ and intend to present in a unified notation the method of Stetter [AS 88] for computing the set of all common zeros of the polynomials in $\mathcal{I}$ using eigenvectors of Φ_f, a method for computing this

* This work is supported in part by the CEC, ESPRIT Basic Research Action 6846 (PoSSo)

set of zeros by using minimal polynomials [YNT 92], and a real root isolating method based on a trace formula for quadratic forms in $\mathcal{P}/\mathcal{I}$, [PRS 92], [Be 91]. Using the concept of dual bases, [$M^3$91], [$M^3$92], we give new proofs, show the connection of the method by [FGLM] to the minimal polynomial computation, and discuss complexity aspects.

By the first two methods, systems of polynomial equations are solved directly; the real root isolating method can serve as preprocesor for a numerical calculation by Newton's method. Hence they all fit into the PoSSo project of solving systems of polynomial equations. An other very interesting method has been presented in a thesis by Cardinal (Université de Rennes), in which for zero dimensional ideals $\mathcal{I}$ generated by n polynomials the common zeros are computed. There, the space $\mathcal{P}/\mathcal{I}$ is equipped with an inner product structure allowing an elegant description of the Φ_f's. The computation of the zeros is then done by a method known in numerical analysis as the von-Mises-iteration. This thesis however became known to the author so recently, that the result can not included here in details.

2 Ideals and Dual Bases

In the following, k is always a field, $\mathcal{P} := k[x_1, \ldots, x_n]$, and $\mathcal{I} \subset \mathcal{P}$ is an ideal of dimension zero. Then $\mathcal{P}/\mathcal{I}$ is a finite dimensional k-vector space, i.e. $\mathcal{I}$ is a k-vector space of finite codimension. A basis of $\mathcal{P}/\mathcal{I}$ can be obtained by a Gröbner basis $\mathcal{G}$ of $\mathcal{I}$. Consider the set $\mathcal{B}$ of all power products $x_1^{i_1} \cdots x_n^{i_n}$ which are not divisible by the leading power product of a $g \in \mathcal{G}$. Then the corresponding equivalence classes $[x_1^{i_1} \cdots x_n^{i_n}]$ constitute a basis of $\mathcal{P}/\mathcal{I}$, see for instance [Bu 88]. We will denote this basis briefly by $[\mathcal{B}]$.

In this section, we resume some relevant parts of the concept of dual bases as described in [$M^3$92] or in the shorter version [$M^3$91], both based on Gröbner's exposition in [Gr 70]. Let $L_1, \ldots, L_s$ be functionals over $\mathcal{P}$, i.e. in $Hom_k(\mathcal{P}, k)$. They are linearly independent if and only if $q_1, \ldots, q_s \in \mathcal{P}$ exist, such that

$$L_i(q_j) = 0 \ \text{ if } \ i \neq j, \ L_i(q_i) = 1 \ . \tag{1}$$

Polynomials $q_1, \ldots, q_s$ satisfying (1) are called *biorthogonal to* $L_1, \ldots, L_s$.

Let $V \subset \mathcal{P}$ be a k-vector space of codimension s. Then there are s linearly independent functionals $L_1, \ldots, L_s$, such that $p \in V \Leftrightarrow L_1(p) = \ldots = L_s(p) = 0$. The set $\{L_1, \ldots, L_s\}$ is called a *dual basis of* V. Conversely, if s functionals L_i are linearly independent, then $\{p \in \mathcal{P} \mid L_1(p) = \ldots = L_s(p) = 0\}$ is a k-vector space of codimension s, i.e. every set of s linearly independent functionals is a dual basis.

If $\{L_1, \ldots, L_s\}$ is a dual basis of V, then V is a zero dimensional ideal if and only if the functionals

$$L_{ij} : p \longmapsto x_i \cdot p, \ L_{ij} \in Hom_k(\mathcal{P}, k), \ i = 1 \ldots, n, j = 1, \ldots, s \ , \tag{2}$$

belong to $span_k\{L_1, \ldots, L_s\}$.