Beiträge zur Algebra und Geometrie
Contributions to Algebra and Geometry
Volume 41 (2000), No. 1, 57-66.

Freeness, Linear Disjointness, and Implicitization – a Classical Approach

Rainer Steinwandt[1] **Jörn Müller-Quade**

Institut für Algorithmen und Kognitive Systeme
Arbeitsgruppe Computeralgebra, Fakultät für Informatik
Universität Karlsruhe, Germany

Abstract. A method for deciding linear disjointness and freeness of finitely generated extension fields is given. The techniques used are based on a classical description of linear disjointness and on the Chow form. The required Gröbner basis techniques do not depend on tag variables. Finally, the solution obtained can also be used to solve the implicitization problem without involving tag variables.

1. Introduction

Let $k(w) := k(w_1, \dots, w_l)$ be a field finitely generated over a ground field k, $k(x) := k(x_1, \dots, x_m)$ and $k(y) := k(y_1, \dots, y_n)$ subfields of $k(w)$, $k(z) := k(z_1, \dots, z_o)$ an intermediate field of k and $k(x) \cap k(y)$. In [9] a method for solving the following problems is given:

1. Decide if $k(x)$ and $k(y)$ are linearly disjoint over $k(z)$.
2. Decide if $k(x)$ and $k(y)$ have a subfield $k(z')$ in common such that $k(x)$ and $k(y)$ are linearly disjoint over $k(z')$ (where $z'_1, \dots, z'_{o'} \in k(w)$).
3. For $k(x)$ and $k(y)$ being linearly disjoint (necessarily over their intersection (see [9, Prop. 15])) construct generators for $k(x) \cap k(y)$ over k.
4. Decide if $k(x)$ is free from $k(y)$ over $k(z)$.

[1] grant DFG - GRK 209/3-98 “Beherrschbarkeit komplexer Systeme”

The present paper gives an alternate solution to the above problems which is based on the classical descriptions of linear disjointness and freeness as given in [18]. By means of the Chow form we obtain a solution which in contrast to the method described in [9] does not make use of so-called tag variables. Gröbner basis computations involving many variables tend to be costly. Therefore we do without these additional variables and make use of extensions of the ground field instead. The idea of extending the ground field in order to avoid additional variables also occurs in the context of the inversion of birational maps ([13]) and the functional decomposition of rational mappings ([10]), for instance.

In Section 5 we describe how the same technique can also be applied to solve the implicitization problem in computer aided geometric design without making use of tag variables.

In a short annotation we point out that in a sense the use of Gröbner basis techniques for deciding linear disjointness was suggested in [18] already. Therefore it might be appropriate to take Weil's work into account when dealing with the history of Gröbner bases.

2. Freeness, linear disjointness, and the Chow form

The key to the constructive solution of the above problems is the ideal[1]

$$\mathfrak{P}_{(y)/k(x)} := \{p \in k(x)[Z_1, \ldots, Z_n] : p(y_1, \ldots, y_n) = 0\}.$$

To illustrate its importance we remind of the following characterization of linear disjointness:

Recall 1. [18, Ch. I, §6, Theorem 3] *Let $k' \leq k(x)$. Then $k(x)$ and $k'(y)$ are linearly disjoint over k' if and only if $\mathfrak{P}_{(y)/k(x)}$ has a basis in $k'[Z] := k'[Z_1, \ldots, Z_n]$.*

In order to use this result to obtain a solution for the first of the above stated problems we also need

Recall 2. [18, Ch. I, §7, Lemma 2] *Let $\mathfrak{I} \trianglelefteq k[Z]$ be an ideal. Then, of all the subfields k' of k such that $\mathfrak{I}$ has a basis with coefficients in k there is a smallest field k_0, contained in all the others.*

In the sequel this field k_0 is referred to as the *minimal field of definition of* $\mathfrak{I}$. Using this terminology we immediately obtain the following three conceptual steps for solving the first of the above problems by applying Recall 1 to $k' = k(z)$:

1. Construct a basis of $\mathfrak{P}_{(y)/k(x)}$.
2. Derive a finite generating set of $\mathfrak{P}_{(y)/k(x)}$ with all coefficients being contained in the minimal field of definition of $\mathfrak{P}_{(y)/k(x)}$. Denote the set of coefficients in this basis by B.
3. Now $k(x)$ and $k(y)$ are linearly disjoint over $k(z)$ if and only if $B \subseteq k(z)$ (cf. [10] for deciding field membership without tag variables).

The second and third problem can be solved in the same manner: To check whether there is a common subfield $k(z')$ of $k(x)$ and $k(y)$ with $k(x)$ and $k(y)$ being linearly disjoint over $k(z')$ we simply have to verify whether the above set B (which by definition is a subset of $k(x)$) is

[1] In [9] this ideal is denoted by $J_{k(y)/k(x)}$. However, as the definition depends on the generating set y, we adopt the notation of [18].

contained in $k(y)$. Similarly, for the third problem we apply Recall 1 to $k' := k(x) \cap k(y)$: If the fields $k(x)$ and $k(y)$ happen to be linearly disjoint, the set B is necessarily the required generating set of $k(x) \cap k(y)$ over k.

Before dealing with the above three steps in detail we first consider the simpler problem of deciding freeness, as the technique used here will also prove useful when dealing with linear disjointness. The key for deciding freeness constructively is

Recall 3. [18, Ch. I, §2, Proposition 2] *$k(x)$ is free from $k(y)$ over $k(z)$ if and only if* $\operatorname{transdeg}(k(x,y)/k(x)) = \operatorname{transdeg}(k(y,z)/k(z))$.

To determine the required transcendence degrees we can use the trivial identitity

$$\operatorname{transdeg}(k(x,y)/k(x)) = \operatorname{transdeg}(k(w)/k(x)) - \operatorname{transdeg}(k(w)/k(x,y))$$

(and analogously $\operatorname{transdeg}(k(y,z)/k(z)) = \operatorname{transdeg}(k(w)/k(z)) - \operatorname{transdeg}(k(w)/k(y,z))$).

For computing $\operatorname{transdeg}(k(w)/k(x))$ resp. $\operatorname{transdeg}(k(w)/k(x,y))$ [10, Lemma 2] suggests to determine the dimension of the prime ideal $\mathfrak{P}_{(w)/k(x)}$ resp. $\mathfrak{P}_{(w)/k(x,y)}$. This can be done by means of a Gröbner basis computation, for instance ([8, Theorem 1]). Using the method in [10] a basis of $\mathfrak{P}_{(w)/k(x)}$ can be found without introducing tag variables; an approach to determine the transcendence degree by means of tag variables is discussed in [16] and [6].

In summary we have

Lemma 4. *Procedure* 1 *decides for finite subsets $x, y, z \subseteq k(w)$ whether $k(x)$ is free from $k(y)$ over $k(z)$ without introducing tag variables.*

Procedure 1

```
In:  $x, y, z \subseteq k(w)$
Out: true,  if $k(x)$ is free from $k(y)$ over $k(z)$
     false, otherwise

begin
  $G_1$ ← any Gröbner basis of $\mathfrak{P}_{(w)/k(x)}$ (see [10]).
  $G_2$ ← any Gröbner basis of $\mathfrak{P}_{(w)/k(x,y)}$ (see [10]).
  $G_3$ ← any Gröbner basis of $\mathfrak{P}_{(w)/k(z)}$ (see [10]).
  $G_4$ ← any Gröbner basis of $\mathfrak{P}_{(w)/k(y,z)}$ (see [10]).
  Derive $\dim(\mathfrak{P}_{(w)/k(x)})$, $\dim(\mathfrak{P}_{(w)/k(x,y)})$, $\dim(\mathfrak{P}_{(w)/k(z)})$, and $\dim(\mathfrak{P}_{(w)/k(y,z)})$ from
        $G_1$, $G_2$, $G_3$, and $G_4$ via [8, Theorem 1].
  if $\dim(\mathfrak{P}_{(w)/k(x)}) - \dim(\mathfrak{P}_{(w)/k(x,y)}) = \dim(\mathfrak{P}_{(w)/k(z)}) - \dim(\mathfrak{P}_{(w)/k(y,z)})$
    then return true
    else return false
  fi
end
```

Deciding linear disjointness is a bit more involved, as we do not only need the dimension but also a generating set of $\mathfrak{P}_{(y)/k(x)}$. To reach this goal without using tag variables we can apply a classical tool from algebraic geometry, namely, the Chow form:

Denote by $t := \dim(\mathfrak{P}_{(x)/k}) = \operatorname{transdeg}(k(x_1, \ldots, x_m)/k)$ the transcendence degree of the extension $k(x_1, \ldots, x_m)/k$, and let $\{u_{ij} : i = 1, \ldots, t+1,\ j = 1, \ldots, m\}$ be algebraically independent over $k(x)$. Furthermore, we write $F_{(x)/k}(u; Z) \in k[u_{11}, \ldots, u_{t+1m}, Z_1, \ldots, Z_{t+1}] \setminus \{0\}$ for the up to a constant factor in $k^{\times}$ unique irreducible polynomial with

$$F_{(x)/k}\Big(u; \sum_{j=1}^{m} u_{1j}x_j, \ldots, \sum_{j=1}^{m} u_{t+1j}x_j\Big) = 0.$$

Then following [15] we refer to $F_{(x)/k}$ as the Chow form of $\mathfrak{P}_{(x)/k}$. In particular, the number of indeterminates of the form Z_i occurring in $F_{(x)/k}$ equals $\operatorname{transdeg}(k(x)/k)$. Note that if $F_{(x)/k}$ did not contain all of $Z_1, \ldots, Z_{t+1}$ there would be an algebraic dependence over $k(u)$ among t sums of the form $\sum u_{ij}x_j$. This would contradict the equality $t = \operatorname{transdeg}(k(x)/k) = \operatorname{transdeg}(k(u)(x)/k(u))$.

Defining polynomials of the variety $\mathrm{V}(\mathfrak{P}_{(x)/k})$ in affine m-space over an algebraic closure of k can be derived from $F_{(x)/k}$ by means of [17, §5 B.]: Introduce new variables $X_1, \ldots, X_m$, and for $i = 1, \ldots, t+1$ replace Z_i by $\sum_{j=1}^{m} u_{ij}X_j$ in $F_{(x)/k}(u; Z)$. Then the coefficients of

$$F_{(x)/k}\Big(u; \sum_{j=1}^{m} u_{1j}X_j, \ldots, \sum_{j=1}^{m} u_{t+1j}X_j\Big) \in k[X][u]$$

form an ideal $\mathfrak{A}_{(x)/k} \trianglelefteq k[X]$ having $\mathrm{V}(\mathfrak{P}_{(x)/k})$ as associated locus. Unfortunately $\mathfrak{A}_{(x)/k}$ is not necessarily prime, and can even have embedded primes (see [15] for an example). However, $\mathfrak{A}_{(x)/k}$ has a unique isolated primary component whose associated prime equals $\mathfrak{P}_{(x)/k}$. In particular, we can determine generators for $\mathfrak{P}_{(x)/k}$ by computing the associated primes of $\mathfrak{A}_{(x)/k}$ (see [14], [4] and the references given there), followed by choosing the associated prime of maximal dimension (again, the dimension of the prime ideals can be determined by means of [8, Theorem 1]).

Note that $\mathfrak{P}_{(x)/k}$ is in particular the radical of the equidimensional hull of $\mathfrak{A}_{(x)/k}$ (resp. for $k(x)/k$ separable equal to the equidimensional hull of $\mathfrak{A}_{(x)/k}$, as in this case the isolated primary component is prime (see [7, Theorem 5])). Therefore also the algorithms in [4] for determining the (radical of the) equidimensional hull of an ideal can be applied here.

Having in mind the three conceptual steps given above we are left to find procedures for

- computing the Chow form $F_{(x)/k}$ and
- determining the minimal field of definition k_0 of an ideal $\mathfrak{I} \trianglelefteq k[Z]$.

3. Computing the Chow form and the minimal field of definition of an ideal

If the transcendence degree t of $k(x)/k$ is known then finding $F_{(x)/k}$ reduces to computing the minimal polynomial of $\sum_{j=1}^{m} u_{t+1j}x_j$ over $k(x, \sum u_{1j}x_j, \ldots, \sum u_{tj}x_j)$. In our concrete situation we have to find the transcendence degree of an extension of the form $k(x, y)/k(x)$

where x and y are rational functions in the generators w of $k(w)$. For this we can proceed as in the above procedure for deciding linear disjointness, namely, compute

$$\operatorname{transdeg}(k(x,y)/k(x)) = \dim(\mathfrak{P}_{(w)/k(x)}) - \dim(\mathfrak{P}_{(w)/k(x,y)})$$

via [10] and [8, Theorem 1].

Finally, to find the required minimal polynomial itself—again without tag variables—we can reuse the Gröbner basis of $\mathfrak{P}_{(w)/k(x)}$, which has proven useful in determining the transcendence degree, by applying [11, Algorithm 3.2]. The latter procedure actually was designed for computing minimal polynomials over intermediate fields of a purely transcendental extension $k(w)/k$; this restriction is not required in the proof of its correctness, however, and it is sufficient to have a Gröbner basis of the ideal $\mathfrak{P}_{(w)/k(x)}$ to apply this algorithm.

For finding the minimal field of definition k_0 of an ideal $\mathfrak{I} \trianglelefteq k[Z]$ in [9] and [12] the following approach is suggested: Determine a reduced Gröbner basis $G_{\mathfrak{I}}$ of $\mathfrak{I}$. Then k_0 is the field which over the prime field of k is generated by the coefficients of the elements of $G_{\mathfrak{I}}$. The correctness of this method is verified easily: $G_{\mathfrak{I}}$ is unique and —via Buchberger's algorithm—can be derived from any finite basis of $\mathfrak{I}$ without extending the field generated (over the prime field) by the coefficients of the polynomials in this initial generating set.

At first glance using a reduced Gröbner basis for determining the field of definition may seem a bit strange. But in fact, already the proof of the existence of the minimal field of definition of an ideal given in [18] makes use of a finite canonical generating set. To illustrate the connection between these (Weil) bases and Gröbner bases we restate part of Weil's proof of Recall 2.

To derive this result Weil looks at the set of terms (=monic monomials) $\mathrm{T}(Z)$ in the variables Z. Using some linear order $\preceq$ we may take $\mathrm{T}(Z)$ for a w. r. t. $\preceq$ increasing sequence $(t_i)_{i=0}^{\infty}$. Omitting all terms t_i from $\mathrm{T}(Z)$ with $t_i - \sum_{j=0}^{i-1} \alpha_j t_j \in \mathfrak{I}$ for some $\alpha_j \in k$ we obtain a subsequence $(t_{i_\lambda})_{\lambda=0}^{\infty}$. Now define the sequence of polynomials $(p_i)_{i=0}^{\infty}$ via

$$p_i := \begin{cases} 0, & \text{if } i = i_\lambda \text{ for some } \lambda \in \mathbb{N}_0, \\ t_i - \sum\limits_{i_\lambda < i} \alpha_\lambda t_{i_\lambda} \text{ with } \alpha_\lambda \in k \text{ such that } t_i - \sum\limits_{i_\lambda < i} \alpha_\lambda t_{i_\lambda} \in \mathfrak{I}, & \text{otherwise.} \end{cases}$$

Using Hilbert's basis theorem Weil concludes that for some $r \in \mathbb{N}_0$ the polynomials $p_0, \ldots, p_r$ form a basis of $\mathfrak{I}$. At this conclusion it is implicitly used that $\preceq$ is of type ω, otherwise the required integer r need not exist (think of $\mathfrak{I} = \langle Z_1, Z_2 \rangle \trianglelefteq k[Z_1, Z_2]$ and $\preceq$ a lexicographical term order). So after fixing a linear order of type ω and choosing r minimal with $p_0, \ldots, p_r$ being a basis of $\mathfrak{I}$ the set $\mathrm{W}_{\preceq}(\mathfrak{I}) := \bigcup_{i=0}^{r} \{p_i\} \setminus \{0\}$ forms a canonical generating set of $\mathfrak{I}$. Weil proves that the coefficients of the polynomials in this set over the prime field of k generate the required field of definition k_0.

Observation 5. *In general this canonical (Weil) basis is not a Gröbner basis w. r. t. $\preceq$.*

Proof. Let $\mathfrak{I} = \langle {Z_1}^2 - Z_2, Z_1 {Z_2}^2 - 1 \rangle \trianglelefteq \mathbb{Q}[Z_1, Z_2]$ and denote by $\preceq$ the graded reverse lexicographic term order with $Z_1 \prec Z_2$. Then the sequence of terms $(t_i)_{i=0}^{\infty}$ starts with

$$(t_0, t_1, t_2, \ldots) = \left(1, Z_1, Z_2, {Z_1}^2, Z_1 Z_2, {Z_2}^2, {Z_1}^3, {Z_1}^2 Z_2, Z_1 {Z_2}^2, {Z_2}^3, \ldots\right),$$

and we obtain

$$(p_0, p_1, p_2, \ldots) = \left(0, 0, 0, {Z_1}^2 - Z_2, 0, 0, {Z_1}^3 - Z_1 Z_2, {Z_1}^2 Z_2 - {Z_2}^2, Z_1 {Z_2}^2 - 1, {Z_2}^3 - Z_1\right).$$

So the canonical (Weil) basis computes to

$$\mathrm{W}_{\preceq}(\mathfrak{J}) = \{p_3, p_4, p_5, p_6\} = \left\{{Z_1}^2 - Z_2, {Z_1}^3 - Z_1 Z_2, {Z_1}^2 Z_2 - {Z_2}^2, Z_1 {Z_2}^2 - 1\right\}.$$

In particular, it is not a Gröbner basis, because $p_{10} = {Z_2}^3 - Z_1 \in \mathfrak{J}$ cannot be reduced modulo $\mathrm{W}_{\preceq}(\mathfrak{J})$. □

Note that if we add p_{10} to $\mathrm{W}_{\preceq}(\mathfrak{J})$ where $\mathfrak{J}$ is the ideal in the above proof we obtain a Gröbner basis of $\mathfrak{J}$. This is not by coincidence, as in fact a Weil basis can always be extended to a Gröbner basis by carrying on Weil's procedure:

Observation 6. *If $\preceq$ is a term order of type ω, $\mathfrak{J} \trianglelefteq k[Z]$, and $(p_i)_{i=0}^{\infty}$ defined as above then there exists an $s \in \mathbb{N}_0$ such that $\bigcup_{i=0}^{s}\{p_i\} \setminus \{0\}$ is a Gröbner basis of $\mathfrak{J}$ w. r. t. $\preceq$.*

Proof. As explained in [18, proof of Lemma 2] every polynomial in $\mathfrak{J}$ is a finite k-linear combination of some of the $p_i, i \in \mathbb{N}_0$. Hence, we may select a finite subset $W \subseteq \{p_i : i \in \mathbb{N}_0\}$ such that all elements of the reduced Gröbner basis of $\mathfrak{J}$ w. r. t. $\preceq$ can be expressed as a k-linear combination of the polynomials in W. Setting $s := \max\{i \in \mathbb{N}_0 : p_i \in W\}$ yields the desired natural number s. □

Observation 7. *If $\mathrm{W}_{\preceq}(\mathfrak{J})$ happens to be a Gröbner basis already it does neither have to be reduced nor minimal.*

Proof. Denote again by $\preceq$ the graded reverse lexicographical term order on $\mathrm{T}(Z_1, Z_2)$ with $Z_1 \prec Z_2$. Then the sequence of terms $(t_i)_{i=0}^{\infty}$ starts with

$$(t_0, t_1, t_2, \ldots) = (1, Z_1, Z_2, {Z_1}^2, Z_1 Z_2, {Z_2}^2, \ldots),$$

and the Weil basis of $\langle Z_1, {Z_2}^2\rangle \trianglelefteq \mathbb{Q}[Z_1, Z_2]$ computes to $\{Z_1, {Z_1}^2, Z_1 Z_2, {Z_2}^2\}$. In particular it is a non-minimal Gröbner basis w. r. t. $\preceq$. □

In summary we have

Lemma 8. *Procedure 2 decides for finite subsets $x, y, z \subseteq k(w)$ whether $k(x)$ is linearly disjoint from $k(y)$ over $k(z)$ without introducing tag variables.*

Procedure 2

```
In:  $x, y, z \subseteq k(w)$
Out: $true$,  if $k(x)$ and $k(y)$ are linearly disjoint over $k(z)$
     $false$, otherwise

begin
  Compute transdeg$(k(x,y)/k(x))$ (see above)
  Compute $F_{(y)/k(x)}$ (using [11, Algorithm 3.2])
  Derive equations for $\mathfrak{A}_{(y)/k(x)}$ (see above)
  Compute the associated prime $\mathfrak{P}_{(y)/k(x)}$ of the isolated primary component
    of $\mathfrak{A}_{(y)/k(x)}$ (using one of the methods described in [14], [4])
  $B \leftarrow$ the coefficients of a reduced Gröbner basis of $\mathfrak{P}_{(y)/k(x)}$ w.r.t. some term order
  if $B \subseteq k(z)$ (see [10])
    then return $true$
    else return $false$
  fi
end
```

Of course, to check whether there exists a common subfield $k(z')$ of $k(x)$ and $k(y)$ with $k(x)$ and $k(y)$ being linearly disjoint over $k(z')$ we simply have to verify the inclusion $B \subseteq k(y)$ instead of $B \subseteq k(z)$ in the **if**-statement. Similarly, if $k(x)$ and $k(y)$ are known to be linearly disjoint (necessarily over their intersection) then the set B computed above satisfies $k(x) \cap k(y) = k(B)$.

4. An example from invariant theory

To illustrate the above procedure we resume an example from invariant theory given in [9].

Let w_1, w_2 be algebraically independent over $\mathbb{C}$. Then the fields $\mathbb{C}({w_1}^{50}, {w_2}^{50}, w_1w_2)$ and $\mathbb{C}(w_1 + w_2, w_1w_2)$ are linearly disjoint over their intersection, and (using a suitable two-dimensional representation) the latter equals the field of invariants $\mathbb{C}^{D_{100}}$ of the dihedral group D_{100} (see [9, Section 6] for details).

Applying the above ideas we can construct generators for $\mathbb{C}^{D_{100}}$ over $\mathbb{C}$. For this we first determine the Chow form $F_{({w_1}^{50},{w_2}^{50},w_1w_2)/\mathbb{C}(w_1+w_2,w_1w_2)}$ of $\mathfrak{P}_{({w_1}^{50},{w_2}^{50},w_1w_2)/\mathbb{C}(w_1+w_2,w_1w_2)}$: Since both $\mathbb{C}(w_1, w_2)/\mathbb{C}({w_1}^{50}, {w_2}^{50}, w_1w_2)$ and $\mathbb{C}(w_1, w_2)/\mathbb{C}(w_1 + w_2, w_1w_2)$ are algebraic we have

$$F_{({w_1}^{50},{w_2}^{50},w_1w_2)/\mathbb{C}(w_1+w_2,w_1w_2)} \in \mathbb{C}(w_1 + w_2, w_1w_2)[u_{11}, u_{12}, u_{13}; Z_1].$$

Using [11, Algorithm 3.2] to compute the minimal polynomial of $u_{11}{w_1}^{50} + u_{12}{w_2}^{50} + u_{13}w_1w_2$ over $\mathbb{C}(u)(w_1 + w_2, w_1w_2)$ we obtain the Chow form:

$$\begin{aligned}{Z_1}^2 &- ((u_{11} + u_{12})({w_1}^{50} + {w_2}^{50}) + 2u_{13}w_1w_2) \cdot Z_1 \\ &+ (u_{11}{w_2}^{50} + u_{12}{w_1}^{50} + u_{13}w_1w_2)(u_{11}{w_1}^{50} + u_{12}{w_2}^{50} + u_{13}w_1w_2).\end{aligned}$$

From this we can derive defining polynomials of $\mathrm{V}(\mathfrak{P}_{({w_1}^{50},{w_2}^{50},w_1w_2)/\mathbb{C}(w_1+w_2,w_1w_2)})$ by substituting $Z_1 \leftarrow u_{11}X_1 + u_{12}X_2 + u_{13}X_3$ where X_1, X_2, X_3 are new variables, followed by extracting coefficients:

$$\begin{array}{l} {X_3}^2 - 2w_1w_2 \cdot X_3 + (w_1w_2)^2, \\ {X_1}^2 - ({w_1}^{50} + {w_2}^{50}) \cdot X_1 + (w_1w_2)^{50}, \\ {X_2}^2 - ({w_1}^{50} + {w_2}^{50}) \cdot X_2 + (w_1w_2)^{50}, \\ 2 \cdot X_1X_3 - 2w_1w_2 \cdot X_1 - ({w_1}^{50} + {w_2}^{50}) \cdot X_3 + ({w_1}^{50} + {w_2}^{50})w_1w_2, \\ 2 \cdot X_2X_3 - 2w_1w_2 \cdot X_2 - ({w_1}^{50} + {w_2}^{50}) \cdot X_3 + ({w_1}^{50} + {w_2}^{50})w_1w_2, \\ 2 \cdot X_1X_2 - ({w_1}^{50} + {w_2}^{50}) \cdot X_1 - ({w_1}^{50} + {w_2}^{50}) \cdot X_2 + {w_1}^{100} + {w_2}^{100} \end{array}$$

The ideal $\mathfrak{A}_{({w_1}^{50},{w_2}^{50},w_1w_2)/\mathbb{C}(w_1+w_2,w_1w_2)} \trianglelefteq \mathbb{C}(w_1 + w_2, w_1w_2)[X]$ spanned by these polynomials is prime (it is of dimension 0 and as $\operatorname{char}(\mathbb{C}) = 0$ the isolated primary component is prime (again [7, Theorem 5])) and hence coincides with $\mathfrak{P}_{({w_1}^{50},{w_2}^{50},w_1w_2)/\mathbb{C}(w_1+w_2,w_1w_2)}$. The reduced Gröbner basis w. r. t. the graded reverse lexicographic term order where $X_1 \prec X_2 \prec X_3$ is

$$\left\{{X_1}^2 - ({w_1}^{50} + {w_2}^{50})X_1 + (w_1w_2)^{50}, X_3 - w_1w_2, X_2 + X_1 - {w_1}^{50} - {w_2}^{50}\right\}.$$

Taking the coefficients as generators we obtain $\mathbb{C}(w_1, w_2)^{D_{100}} = \mathbb{C}({w_1}^{50} + {w_2}^{50}, w_1w_2)$ as one would expect.

5. Implicitization without tag variables

If k is an infinite field and $w_1, \ldots, w_l$ are algebraically independent over k we may think of $x_1, \ldots, x_m \in k(w)$ as rational functions in the indeterminates w parametrizing the set

$$\left\{(x_1(\alpha), \ldots, x_m(\alpha)) : \alpha \in k^l \text{ and } x_1, \ldots, x_m \text{ defined at } \alpha\right\}.$$

Using the above notation the implicitization problem in computer aided geometric design can be stated as: "Determine a generating set of $\mathfrak{P}_{(x)/k}$."

It ist well-known that this problem can be solved by introducing m additional tag variables (see [3, p. 131], [1]). Using the Chow form as described above we can compute $\mathfrak{P}_{(x)/k}$ without making use of tag variables. Moreover, if one is only interested in problems like testing whether certain points are contained in $\mathrm{V}(\mathfrak{P}_{(x)/k})$ it can be sufficient to solve the following weaker variant of the implicitization problem (see, e. g. [5]): "Determine an ideal $\mathfrak{I} \trianglelefteq k[Z]$ with $\mathrm{V}(\mathfrak{I}) = \mathrm{V}(\mathfrak{P}_{(x)/k})$."

To solve this variant it is sufficient to derive generators for the ideal $\mathfrak{A}_{(x)/k}$ from the coefficients of $F_{(x)/k}(u; \sum u_{1j}X_j, \ldots, u_{t+1j}X_j) \in k[X][u]$. The computation of the associated prime $\mathfrak{P}_{(x)/k}$ can be skipped then.

Finally, we want to remark that for efficiency reasons it would be very interesting to know of an alternate solution to the problem of finding the minimal field of definition of an ideal—in spite of the fact that the mentioned proof of Weil shows that Gröbner bases appear quite naturally in this context.

References

[1] Alonso, C.; Gutierrez, J.; Recio, Th.: *An implicitization algorithm with fewer variables.* Computer Aided Geometric Design **12** (1995), 251–258.

[2] Bosmar, W.; Cannon, J.; Playoust, C.: *The Magma Algebra System I: The User Language.* Journal of Symbolic Computation **24** (1997), 235–265.

[3] Cox, D.; Little, J.; O'Shea, D.: *Ideals, Varieties and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra.* Undergraduate Texts in Mathematics. Springer, New York 1992.

[4] Decker, W.; Greuel, G.-M.; Pfister, G.: *Primary Decomposition: Algorithms and Comparisons.* Preprint, Universität Kaiserslautern 1998.
At the time of writing this reference was available electronically at the URL
`http://kbibmp3.ub.uni-kl.de/Preprint/PS/no_series_20.ps.gz`.

[5] Kalkbrener, M.: *Implicitization of rational parametric curves and surfaces.* In: Shojiro Sakata (ed.), Applied Algebra, Algebraic Algorithms and Error-Correcting Codes 8th International Conference, AAECC-8. Lecture Notes in Computer Science **508**, 249–259, Springer, Berlin, Heidelberg 1991.

[6] Kemper, G.: *An Algorithm to Determine Properties of Field Extensions Lying over a Ground Field.* IWR Preprint 93-58, Heidelberg, Oktober 1993.

[7] Krull, W.: *Parameterspezialisierung in Polynomringen II. Das Grundpolynom.* Arch. Math. **1** (1948), 129–137.

[8] Kalkbrener, M.; Sturmfels, B.: *Initial Complexes of Prime Ideals.* Adv. Math. **116** (1995), 365–376.

[9] Müller-Quade, J.; Rötteler, M.: *Deciding Linear Disjointness of Finitely Generated Fields.* In: O. Gloor (ed.), Proceedings of the 1998 International Symposium on Symbolic and Algebraic Computation, 153–160. The Association for Computing Machinery, Inc. (ACM), August 1998.

[10] Müller-Quade, J.; Steinwandt, R.; Beth, Th.: *An application of Gröbner bases to the decomposition of rational mappings.* In: B. Buchberger and F. Winkler (eds.), Gröbner Bases and Applications. London Mathematical Society Lecture Note Series **251**, 448–462. Cambridge University Press 1998.

[11] Müller-Quade, J.; Steinwandt, R.: *Basic Algorithms for Rational Function Fields.* To appear in: Journal of Symbolic Computation.

[12] Robbiano, L.; Sweedler, M.: *Ideal and Subalgebra Coefficients.* Proc. Amer. Math. Soc. **126**(8) (1998), 2213–2219.

[13] Schicho, J.: *Inversion of Birational Maps with Gröbner Bases.* In: B. Buchberger and F. Winkler (eds.), Gröbner Bases and Applications. London Mathematical Society Lecture Note Series **251**, 495–503. Cambridge University Press 1998.

[14] Seidenberg, A.: *Constructions in Algebra.* Trans. Amer. Math. Soc. **197** (1974), 273–313.

[15] Seidenberg A.: *On the Chow Form.* Math. Ann. **212** (1975), 183–190.

[16] Sweedler, M.: *Using Groebner Bases to Determine the Algebraic and Transcendental Nature of Field Extensions: return of the killer tag variables.* In: G. Cohen, T. Mora, and O. Moreno (eds.), Applied Algebra, Algebraic Algorithms and Error-Correcting Codes 10th International Symposium, AAECC-10. LNCS **673**, 66–75. Springer Berlin, Heidelberg 1993.

[17] van der Waerden, B. L.: *Zur algebraischen Geometrie 19. Grundpolynom und zugeordnete Form.* Math. Ann. **136** (1958), 139–155.

[18] Weil, A.: *Foundations of algebraic geometry.* Amer. Math. Soc. Colloq. Publ. **29**, rev. and enl. edition Providence, Rhode Island 1946.

Received September 8, 1998