Families of Ideals in Statistics

Massimo Caboara *
Dipartimento di Matematica
Università di Pisa
caboara@dm.unipi.it

Lorenzo Robbiano *
Dipartimento di Matematica
Università di Genova
robbiano@dima.unige.it

Poi neanche il verno si dimentica teco essere la villa liberale
L. B. Alberti (1404–1472)

Abstract

In this paper we use Gröbner basis theory and some methods of Algebraic Geometry to solve a relevant problem in Statistics, more specifically in the Design of Experiments. Namely suppose we are given a Full Factorial Design $\mathcal{D}$ and a complete polynomial model $\mathcal{P}$, whose support is contained in the order ideal of monomials defined by $\mathcal{D}$. We show how to construct families of ideals defining Fractions $\mathcal{F}$ of $\mathcal{D}$ which are minimally identified by $\mathcal{P}$.

1 Introduction

Design of Experiments is a branch of Statistics which has a long tradition (see for example [BHH],[D], [F], [RHF], [StS], [Y]). There have been several approaches to the mathematical theory of Design of Experiments. With some exceptions (see for instance [RHF]), the statistical literature is mainly concerned with explaining techniques rather than providing a mathematical foundation. Recently some methods of Computational Commutative Algebra were introduced into the topic by Diaconis, Sturmfels ([DS]) and even more recently by Pistone, Wynn (see [PW]) and by Pistone, Robbiano, Rogantin (see [PRR]). In particular [PW] was the first paper which highlighted the connection between Design of Experiments and Gröbner bases.

We recall that in Statistics a *Design* is a set of *treatments*, which can be described by their integral coordinates, hence they can be viewed as elements of $\mathbb{Z}^n$, and hence of $\mathbb{Q}^n$. In this frame they are called *experimental points* or simply *points*. Moreover, given two polynomials, they are said to be *confounded* by the Design if they take the same values on the given points.

A Fraction of a Design is simply a subset of it. The theory of *Gröbner bases* yields a complete solution to the problem of finding a *monomial basis* of the vector space of the polynomial functions on the Fraction. This problem is known in Statistics as the problem of finding a full set of *estimable terms*. This problem was studied in the pioneering paper by [PW].

*Partially supported by the Consiglio Nazionale delle Ricerche (CNR)

An even more relevant problem is the *inverse problem* and the main purpose of this paper is to yield a deeper insight into it.

So let us explain it in more detail. Given a *Full Factorial Design*, i.e. a special set $\mathcal{D}$ of experimental points, we embed it in $\mathbb{A}^m_{\mathbb{Q}}$, the affine m-space over the rational numbers. Then, given a polynomial $P(x) := \sum_\alpha c_\alpha x^\alpha$ and the corresponding polynomial model $y = P(x)$, we want to find minimal subsets (*Fractions*) $\mathcal{F}$ of $\mathcal{D}$, such that the power products in the support of P are not confounded by $\mathcal{F}$. We recall that in Statistics it is usual to start with models P which are complete in the following sense: if a power product x^α belongs to $\mathrm{Supp}(P)$ then all power products x^β such that $x^\beta | x^\alpha$ belong to $\mathrm{Supp}(P)$. This implies that $\mathrm{Supp}(P)$ is an *order ideal of monomials*. What we have denoted as the inverse problem simply requires to find some or (better) all the Fractions $\mathcal{F}$ of $\mathcal{D}$ such that, if $I(\mathcal{F})$ is the defining ideal of $\mathcal{F}$, then $\mathrm{Supp}(P)$ *is a* monomial basis *of* $\mathbb{Q}[X]/I(\mathcal{F})$ *viewed as a vector space over* $\mathbb{Q}$.

A first solution to the inverse problem was given in [PRR] by means of *distractions* (see [CR]). In this paper we go much further in that direction and solve a relevant subclass of the inverse problem by means of algebraic methods. The key is the construction of a suitable family of ideals.

Our paper is organized as follows. In Section 2 we state the main problem, which we call Problem 1, and a related problem, called Problem 2, which is formulated in such a way that it can take advantage of the Gröbner basis theory. Then the connection between the two is fully explored. In particular, it is shown that there are important situations where the two problems have the same solutions (Corollary 2.14). Suitably chosen examples are presented at the end of the section; the last one shows that there are indeed cases where the two problems may have different solutions.

Section 3 is devoted to the complete solution of Problem 2. Some basic facts from the theory of reduced Gröbner bases and some suitable algebraic methods allow us to construct an affine $\mathbb{Q}$-scheme, which is zero-dimensional, rational, fully computable and parametrizes the solutions of Problem 2 (see Theorem 3.3).

A Conjecture is stated at the end, which is supported by some experimental evidence.

The last section uses the algorithmic content of the theory developed before and carries on the full computation, leading to the full solution, of the examples introduced in Section 2.

For the fundamental notions about the theory of Gröbner bases, we refer to the basic literature, for instance [CLO],

[AL] and [E]. A product of our work has been the creation of a series of algorithms coded in CoCoAL, the programming language of CoCoA(see [CNR1] and [CNR2]). The name of this package is `statfamilies` and it is available upon request from the authors. A general reference for existing algorithms about Design of Experiments is [H].

At the very end of the paper we give an elementary example suggesting how our methods can be generalized (see Remark 4.1). As we said before, this branch of Statistics is lacking a strong mathematical foundation and our main goal is indeed to provide an algebraic setting for it. In view of this, the examples are chosen to be elementary and we have not attempted to optimize our algorithms.

2 Some Inverse Problems

As we said in the introduction, we start with a Full Factorial Design, which is defined by

Definition 2.1 *A* full Factorial Design *(or simply a* Factorial Design*) with levels* $(l_1, l_2, \ldots, l_m) \in \mathbb{N}^m$ *is the set of points* $\mathcal{D} := \{0, 1, \ldots, l_1 - 1\} \times \ldots \times \{0, 1, \ldots, l_m - 1\} \subset \mathbb{N}^m$. *An* l^m *Factorial Design is a Factorial Design with levels* $(l, l, \ldots, l)$. *A* Fractional Factorial Design *(or simply a* Fraction*) of* $\mathcal{D}$ *is a subset of* $\mathcal{D}$.

Remark 2.2 In Statistics it is also common to consider Designs with other points, namely points whose coordinates take their values over different sets of integers, such as for instance $\{-1, 0, 1\}$. More generally it is allowed to consider consecutive sets of integers. In our algebraic setting, this corresponds to a shift of the origin of the coordinates. It will be clear from the theory which we are going to develop, that this generalization does not change any of the following constructions.

Definition 2.3 *If we are given a Factorial Design* $\mathcal{D}$ *whose levels are* $(l_1, l_2, \ldots, l_m)$, *then we denote by* $I(\mathcal{D})$ *its defining ideal in* $\mathbb{Q}[x_1, \ldots, x_m]$, *i.e. the ideal generated by the* m *polynomials* $F_j := x_j\ (x_j - 1) \cdots (x_j - l_j + 1)$ *of degrees* l_j, $j := 1, \ldots, m$, *which are called the defining equations of* $\mathcal{D}$. *We denote by* $R(\mathcal{D})$ *the ring* $\mathbb{Q}[x_1, \ldots, x_m]/I(\mathcal{D})$. *Given a proper Fraction* $\mathcal{F}$ *of* $\mathcal{D}$, *of course* $I(\mathcal{D}) \subset I(\mathcal{F})$ *and we denote by* $R(\mathcal{F})$ *the ring* $\mathbb{Q}[x_1, \ldots, x_m]/I(\mathcal{F})$, *a quotient ring of* $\mathbb{Q}[x_1, \ldots, x_m]/I(\mathcal{D})$.

We recall that

Definition 2.4 *Any set of polynomial equations that, added to the equations of a Factorial Design* $\mathcal{D}$, *generates the ideal of a Fraction* $\mathcal{F}$, *is called a set of* confounding equations *of* $\mathcal{F}$ *(in* $\mathcal{D}$*).*

Definition 2.5 *Let* $\mathcal{F} \subset \mathcal{D}$ *be a Fraction of the design* $\mathcal{D}$. *Let* σ *be a term-order and* G_σ *the corresponding reduced Gröbner basis of* $I(\mathcal{F})$. *The set of those polynomials in* G_σ, *which are not among the defining equations of* $\mathcal{D}$ *is called* the σ-canonical set of confounding equations *of* $\mathcal{F}$.

Definition 2.6 *An* order ideal of monomials *is a set* E *of power products, with the following property: if* $t \in E$ *and* $t'|t$ *then* $t' \in E$.

Given a Factorial Design $\mathcal{D}$ with levels $(l_1, l_2, \ldots, l_m)$, it is clear that its defining equations $F_1, \ldots, F_m$ are a Gröbner basis of $I(\mathcal{D})$ with respect to *every* term-order. Therefore there is a *canonical order ideal of monomials* associated to $\mathcal{D}$.

Definition 2.7 *Given a Factorial Design* $\mathcal{D}$, *we denote by* $\mathcal{O}(\mathcal{D})$ *the order ideal of monomials associated to* $\mathcal{D}$. *It is clear that* $\mathcal{O}(\mathcal{D}) = \{x_1^{a_1} x_2^{a_2} \cdots x_m^{a_m} \mid a_j < l_j,\ j = 1, \ldots, m\}$. *Given a Fraction* $\mathcal{F}$ *of* $\mathcal{D}$ *and a term-order* σ, *we denote by* $\mathcal{O}_\sigma(\mathcal{F})$ *the order ideal of monomials contained in* $\mathcal{O}(\mathcal{D})$ *and corresponding to the associated reduced Gröbner basis of* $I(\mathcal{F})$ *with respect to* σ.

A *linear polynomial model* is a polynomial function $y = f(x_1, \ldots, x_n)$ such that the coefficients are algebraically independent parameters. When we deal with a linear polynomial model, the whole information is coded in the support of $f(x_1, \ldots, x_n)$. So we use the following

Definition 2.8 *A* complete (linear) polynomial model *is the vector-space generated by an order ideal of monomials, which is called the* support *of the model.*

Now we are ready to state the so-called *Inverse Problem*. The input is a Factorial Design $\mathcal{D}$ and a *complete polynomial model*, whose support is contained in $\mathcal{O}(\mathcal{D})$.

Problem 1 *If we are given a Factorial Design* $\mathcal{D}$ *and a* complete polynomial model, *whose support* $\mathcal{O}$ *is contained in* $\mathcal{O}(\mathcal{D})$, *then we want to find* all *the Fractions* $\mathcal{F}$ *of* $\mathcal{D}$ *and the corresponding ideals* $I(\mathcal{F})$ *such that* $\mathcal{O}$ *is a* monomial basis *of* $R(\mathcal{F})$ *as a* $\mathbb{Q}$*-vector space.*

Problem 2 *If we are given a Factorial Design* $\mathcal{D}$, *a* complete polynomial model *as above and a term-order* σ, *then we want to find* all *the Fractions* $\mathcal{F}$ *of* $\mathcal{D}$ *and the corresponding* σ*-canonical sets of confounding equations of* $\mathcal{F}$ *such that* $\mathcal{O} = \mathcal{O}_\sigma(\mathcal{F})$, *hence is a* monomial basis *of* $R(\mathcal{F})$ *as a* $\mathbb{Q}$*-vector space.*

Now we study the connection between the two problems.

Definition 2.9 *Given* m *indeterminates* $x_1, x_2, \ldots, x_m$, *we denote by* $X := \{x_1, x_2, \ldots, x_m\}$ *and by* $\mathbf{T}^m$ *the set of power products in* X. *Let* $\mathcal{D}$ *be a Factorial Design and* $\mathcal{O} \subset \mathcal{O}(\mathcal{D})$ *be an order ideal of monomials. Then there exists a unique minimal set* $\mathrm{Min}(\mathcal{O})$ *of power products which generate the mono-ideal* $\mathbf{T}^m \backslash \mathcal{O}$. *The set of power products in* $\mathrm{Min}(\mathcal{O})$, *which are not among the* leading terms *of the defining equations of* $\mathcal{D}$ *is called* $\mathrm{CutOut}(\mathcal{O})$.

Lemma 2.10 *Suppose we are given a Factorial Design* $\mathcal{D}$, *an order ideal of monomials* $\mathcal{O}$ *contained in* $\mathcal{O}(\mathcal{D})$ *and a Fraction* $\mathcal{F}$ *of* $\mathcal{D}$ *such that* $\mathcal{O}$ *is a* monomial basis *of* $R(\mathcal{F})$ *as a* $\mathbb{Q}$*-vector space. If* $\{T_1, \ldots, T_r\} = \mathrm{CutOut}(\mathcal{O})$ *then there exist unique polynomials* $G_i := T_i - R_i \in I(\mathcal{F})$ *with* $\mathrm{Supp}(R_i) \subseteq \mathcal{O}$, *for every* $i := 1, \ldots, r$.

Proof. The existence follows from the fact that the sets $\{T_i\} \cup \mathcal{O}$ are linearly dependent modulo $I(\mathcal{F})$ for $i := 1, \ldots, r$ and the uniqueness from the fact that the elements of $\mathcal{O}$ are linearly independent modulo $I(\mathcal{F})$. ∎

Definition 2.11 *We call the set $\{G_1,\dots,G_r\}$, defined by Lemma 2.10, the* $\mathcal{O}$-canonical set of confounding equations *of $\mathcal{F}$. Let now $\{F_{i_1},\dots,F_{i_t}\}$ be the set of those defining equations of $\mathcal{D}$, such that $\mathrm{Lt}(F_{i_h})$ is not divisible by any of the elements in $\mathrm{CutOut}(\mathcal{O})$, for $h := 1,\dots t$. Then the set $\{F_{i_1},\dots,F_{i_t},G_1,\dots,G_r\}$ is called the* reduced $\mathcal{O}$-basis *of $\mathcal{F}$.*

Definition 2.12 *Let $\mathcal{O} \subset \mathbf{T}^m$ be an order ideal of monomials, σ a term-order and T a power product. We put $\sigma(\mathcal{O},T) := \{T' \in \mathcal{O} \mid T' <_\sigma T\}$.*

Proposition 2.13 *Suppose we are given a Factorial Design $\mathcal{D}$, an order ideal of monomials $\mathcal{O}$ contained in $\mathcal{O}(\mathcal{D})$ and a fraction $\mathcal{F}$ of $\mathcal{D}$ such that $\mathcal{O}$ is a* monomial basis *of $R(\mathcal{F})$ as a $\mathbb{Q}$-vector space. Let $G := \{G_1,\dots,G_r\}$ be the $\mathcal{O}$-canonical set of confounding equations of $\mathcal{F}$ and let $S := \{F_{i_1},\dots,F_{i_t},G_1,\dots,G_r\}$ be the reduced $\mathcal{O}$-basis of $\mathcal{F}$. Finally, let σ be a term-order such that $\mathcal{O}_\sigma(\mathcal{F}) = \mathcal{O}$; then*

1) The set S is the reduced Gröbner basis of $I(\mathcal{F})$ with respect to σ.

2) If $G_i := T_i - R_i$, then $\mathrm{Supp}(R_i) \subseteq \sigma(\mathcal{O},T_i)$, for every $i := 1,\dots,r$.

3) The set G is the σ-canonical set of confounding equations of $\mathcal{F}$.

Proof. The assumption that $\mathcal{O}_\sigma(\mathcal{F}) = \mathcal{O}$ forces $\mathrm{Lt}_\sigma(I(\mathcal{F}))$ to be minimally generated by $\mathrm{Min}(\mathcal{O})$, hence if $\{\Gamma_1,\dots,\Gamma_s\}$ is the reduced Gröbner basis of $I(\mathcal{F})$ with respect to σ, then $\Gamma_i = T_i - S_i$ with $T_i \in \mathrm{Min}(\mathcal{O})$ and $\mathrm{Supp}(S_i) \subseteq \sigma(\mathcal{O},T_i) \subseteq \mathcal{O}$. Therefore the uniqueness, shown in Lemma 2.10 for the G_i's and clear for the F_{i_h}'s, implies 1). Statements 2) and 3) follow immediately. □

It is clear that every solution to Problem 2 is a solution to Problem 1. We produce a situation where also the converse holds.

Corollary 2.14 *Given a Factorial Design $\mathcal{D}$ and an order ideal of monomials $\mathcal{O} \subset \mathcal{O}(\mathcal{D})$, we let $\mathrm{CutOut}(\mathcal{O}) := \{T_1,\dots,T_r\}$ and assume that there exists a term-order σ such that $\sigma(\mathcal{O},T_i) = \mathcal{O}$ for every $i := 1,\dots,r$. Then the solutions to Problems 1 and 2 are the same.*

Proof. It is enough to prove that a solution to Problem 1 is also a solution to Problem 2. So let $\mathcal{F}$ be a Fraction of $\mathcal{D}$ such that $\mathcal{O}$ is a *monomial basis* of $R(\mathcal{F})$ as a $\mathbb{Q}$-vector space. Let $\{G_1,\dots,G_r\}$ be the $\mathcal{O}$-canonical set of confounding equations of $\mathcal{F}$ and let $\{F_{i_1},\dots,F_{i_t},G_1,\dots,G_r\}$ be the reduced $\mathcal{O}$-basis of $\mathcal{F}$. The assumption on σ implies that $\mathrm{Lt}_\sigma(G_i) = T_i$ for $i := 1,\dots,r$. Therefore it follows that all the elements $F_{i_1},\dots,F_{i_t},G_1,\dots,G_r$ belong to the reduced Gröbner basis of $I(\mathcal{F})$ with respect to σ; another element in that Gröbner basis would have the support contained in $\mathcal{O}$, which contradicts the assumption. We may conclude that $\{G_1,\dots,G_r\}$ is the σ-canonical set of confounding equations of $\mathcal{F}$ and this completes the proof. □

Example 1 Let $\mathcal{D}$ be a 2^3 Factorial Design given by the equations $F_1 := x^2 - x,\ F_2 := y^2 - y,\ F_3 := z^2 - z$; then $\mathcal{O}(\mathcal{D}) = \{1,x,y,z,xy,xz,yz,xyz\}$. If $\mathcal{O} := \{1,x,y,z\}$, then we get $\mathrm{CutOut}(\mathcal{O}) = \{xy,xz,yz\}$. If σ is any degree-compatible term-order, then we match the assumptions of Corollary 2.14 since $\sigma(\mathcal{O},xy) = \sigma(\mathcal{O},xz) = \sigma(\mathcal{O},yz) = \mathcal{O}$. To solve Problem 1 completely in this specific example, it suffices to find *all* the σ-canonical sets of confounding equations, whose *leading terms* are xy,xz,yz. All the corresponding Fractions $\mathcal{F}$ are such that $\mathrm{Lt}_\sigma(I(\mathcal{F}))$ is minimally generated by $\{x^2,y^2,z^2,xy,xz,yz\}$.

Example 2 Let $\mathcal{D}$ be a 3^2 Factorial Design given by the equations $F_1 := x^3 - x,\ F_2 := y^3 - y$; then we get $\mathcal{O}(\mathcal{D}) = \{1,x,y,x^2,xy,y^2,x^2y,xy^2,x^2y^2\}$. If we denote by $\mathcal{O} := \{1,x,y,xy,y^2,xy^2\}$, then we get $\mathrm{CutOut}(\mathcal{O}) = \{x^2\}$. If Lex denotes the lexicographic order with $x > y$, then again we match the assumptions of Corollary 2.14. The Fractions $\mathcal{F}$ which solve Problem 1 are such that $\mathrm{Lt}_{Lex}(I(\mathcal{F}))$ is generated by $\{x^3,y^3,x^2\}$, hence minimally generated by $\{y^3,x^2\}$.

With the following example we are going to show that, when Corollary 2.14 cannot be applied, it may be possible that Problem 1 has *more* solutions than Problem 2.

Example 3 Let $\mathcal{D}$ be a 3^2 Factorial Design given by the equations $F_1 := x^3 - x,\ F_2 := y^3 - y$; then we get $\mathcal{O}(\mathcal{D}) = \{1,x,y,x^2,xy,y^2,x^2y,xy^2,x^2y^2\}$. If $\mathcal{O} := \{1,x,y,x^2,y^2\}$, then $\mathrm{CutOut}(\mathcal{O}) = \{xy\}$. There is no term-order such that both $xy > x^2$ and $xy > y^2$ hold, therefore we cannot apply Corollary 2.14. For instance if Lex1 denotes the lexicographic order with $x > y$ and Lex2 denotes the lexicographic order with $y > x$, then $\mathrm{Lex1}(\mathcal{O},xy) = \{1,x,y,y^2\}$ and $\mathrm{Lex2}(\mathcal{O},xy) = \{1,x,y,x^2\}$, which are both strictly contained in $\mathcal{O}$.

But more than this is true. Namely, let us consider the fraction $\mathcal{F} := \{(0,0),\ (0,-1),\ (1,0),\ (1,1),\ (-1,1)\}$ of $\mathcal{D}$. Its Lex1-Gröbner basis is $\{x^2+xy-x-1/2y^2-1/2y,\ xy^2-xy,\ y^3-y\}$, so that $\mathcal{O}_{Lex1}(\mathcal{F}) = \{1,x,y,xy,y^2\}$. Let us see that $\mathcal{O}$ is a *monomial basis* of $R(\mathcal{F})$. Indeed it suffices to show that $\{1,x,y,x^2,y^2\}$ are linearly independent modulo $I(\mathcal{F})$. Given $a + bx + cy + dx^2 + ey^2 = 0$, we can rewrite the lefthand-side via the Lex1-Gröbner basis; we get $a + bx + cy + d(-xy + x + 1/2y^2 + 1/2y) + ey^2 = a + (b+d)x + (c+1/2d)y - dxy + (1/2d+e)y^2$. But we know that $\{1,x,y,xy,y^2\}$ are linearly independent modulo $I(\mathcal{F})$, hence we deduce that $a = b+d = c+1/2d = -d = 1/2d+e = 0$, whence $a = b = c = d = e = 0$. In this case the reduced $\mathcal{O}$-basis of $\mathcal{F}$ is $\{x^3-x,\ y^3-y,\ xy+x^2-1/2y^2-x-1/2y\}$. It follows that $\mathcal{F}$ is a solution to Problem 1 and *it cannot be a solution to Problem 2, no matter which term-order we choose.*

Remark 2.15 The above examples show that sometimes a full solution to Problem 1 can be achieved by solving Problem 2 and sometimes this is not possible. How can we decide whether a term-order σ exists, which matches the conditions of Corollary 2.14 ? We must find σ such that $T_i >_\sigma T$ for every $i := 1,\dots,r$ and every $T \in \mathcal{O}$. This can be done by imposing the positivity of all the differences of the vectors of exponents and then check by standard methods (e.g. the simplex method) if the so obtained set of integer inequalities has a solution.

3 A Solution

In this section we are going to show how to solve Problem 2.

Suppose we are given a Factorial Design $\mathcal{D}$ and an order ideal of monomials $\mathcal{O}$ contained in $\mathcal{O}(\mathcal{D})$, whose cardinality we denote by $\#(\mathcal{O})$.

The *first step* is to *construct* $\mathrm{CutOut}(\mathcal{O})$. This can be done with a straightforward procedure and so we get a finite set of independent power products $\{T_1, T_2, \ldots, T_r\}$.

Then let $N := \#(\mathcal{O}) \times r$ and $A := \{a_{T,i} \mid T \in \mathcal{O}\ ,\ i := 1, \ldots, r\}$ be a set of N new independent indeterminates. We denote by $\mathbb{Q}[A]$ the corresponding polynomial ring and by $\mathbb{A}^{\mathcal{O}}_{\mathbb{Q}}$ the corresponding affine space. We denote by $\mathbb{Q}[X] := \mathbb{Q}[x_1, \ldots, x_m]$, by $(\mathbb{Q}[A])[X]$ the polynomial ring in the x_i's over the polynomial ring in the a_T's.

Suppose we are given a term-order σ on $\mathbb{Q}[X]$. The *second step* is to *construct r generic polynomials*

$$G_i := T_i - R_i \quad \text{where} \quad R_i := \sum_{T \in \sigma(\mathcal{O}, T_i)} a_{T,i} T$$

The choice that $\mathrm{Supp}(R_i) \subseteq \sigma(\mathcal{O}, T_i)$ is meant to guarantee that $\mathrm{Lt}_\sigma(G_i) = T_i$. We denote by $\mathcal{S}$ the polynomials $\{F_1, \ldots, F_m, G_1, \ldots, G_r\}$, where $F_j = x_j\ (x_j - 1) \cdots (x_j - l_j - 1)$ for $i := 1, \ldots, m$, so that the F_j's are the *fixed* equations of $\mathcal{D}$ and the G_i's are the polynomials constructed above and depending on the *free parameters* $a_{T,i}$'s.

The *third step* is to *impose* that $\mathcal{S}$ is a Gröbner basis. We must be a little careful since $(\mathbb{Q}[A])[X]$ is not a polynomial ring over a field. We could embed $\mathbb{Q}[A]$ in its field of Fractions $\mathbb{Q}(A)$ and consequently consider $\mathcal{S}$ as a family of polynomials in $\mathbb{Q}(A)[X]$. But it turns out that this is not necessary. Namely all the polynomials F_j's and G_i's are *monic*, hence all the reduction steps do not require divisions. On the other hand we are going to see that the produced new polynomials have to be identically zero, hence we do not need divisions at all.

Let us see it in detail. If there are i, j such that $T_i \mid x_j^{l_j}$, then we reduce F_j with respect to the G_i's until we have a polynomial ϕ_j whose support is contained in $\mathcal{O}$. Imposing that such a polynomial is zero forces all the coefficients of ϕ_j in $\mathbb{Q}[A]$ to be zero. So we have produced a first set $\mathcal{E}_1$ of polynomials in $\mathbb{Q}[A]$.

At this point we have possibly deleted some of the F_i's and we are left with a set $\mathcal{S}' \subseteq \mathcal{S}$ of polynomials, such that among their *leading terms* there is no divisibility relation. Now we can construct the *critical pairs* and then minimalize them (see [CDNR]). For every critical pair left, we construct the corresponding S-polynomial and then we reduce it against the set $\mathcal{S}'$ until its support is contained in $\mathcal{O}$. Imposing again that such a polynomial is zero forces all its coefficients (in $\mathbb{Q}[A]$) to be zero. We have produced a second set $\mathcal{E}_2$ of polynomials in $\mathbb{Q}[A]$.

Definition 3.1 *Let us write $\mathcal{E} := \mathcal{E}_1 \cup \mathcal{E}_2$, by $I(\mathcal{O}, \sigma)$ the ideal of $\mathbb{Q}[A]$ generated by $\mathcal{E}$ and by $\mathbb{X}(\mathcal{O}, \sigma)$ the subscheme of $\mathbb{A}^{\mathcal{O}}_{\mathbb{Q}}$ defined by $I(\mathcal{O}, \sigma)$. Finally we denote by $Sol(\mathcal{O}, \sigma)$ the set of those Fractions of $\mathcal{D}$, which solve Problem 2.*

We are almost ready to prove our main result. First, we need the following

Lemma 3.2 *Let $F_1, F_2, \ldots, F_m$ denote as usual the equations of a Factorial Design $\mathcal{D}$ and let I be a proper ideal of $\mathbb{C}[X]$ which contains $\{F_1, F_2, \ldots, F_m\}$. Then*

1) I is a radical ideal, which defines a Fraction of $\mathcal{F}$.

2) I can be defined by polynomials in $\mathbb{Q}[X]$.

3) If σ is a term-order, then the polynomials of the reduced Gröbner basis of I with respect to σ are in $\mathbb{Q}[X]$.

Proof. Let $\mathcal{F}$ be the set of zeroes of I; then $\mathcal{F} \subset \mathbb{A}^m_{\mathbb{C}}$, the affine complex space of dimension m. From the fact that $\{F_1, F_2, \ldots, F_m\} \subset I$ it follows that $\mathcal{F} \subseteq \mathcal{D}$. By localizing the ring $A := \mathbb{C}[X]/I$ at the maximal ideals M corresponding to the points of $\mathcal{D}$, we have that either $IA_M = (1)$ or $IA_M = MA_M$. Therefore I is a radical ideal, hence it is the defining ideal of $\mathcal{F}$. But the defining ideal of a finite set of rational points can be clearly generated by polynomials with rational coefficients, hence also its reduced Gröbner basis has the same property. $\square$

To have a more complete insight into the problem of the fields of definitions of ideals and subalgebras see [RS].

Theorem 3.3 *Suppose we are given a Factorial Design $\mathcal{D}$, an order ideal of monomials $\mathcal{O}$ contained in $\mathcal{O}(\mathcal{D})$ and a term-order σ on $\mathbb{Q}[X]$. With the above definitions and notation the following conditions hold*

1) The subscheme $\mathbb{X}(\mathcal{O}, \sigma)$ of the parameter space $\mathbb{A}^{\mathcal{O}}_{\mathbb{Q}}$ is zero-dimensional and rational.

2) There is a bijection between $Sol(\mathcal{O}, \sigma)$ and the set of points of $\mathbb{X}(\mathcal{O}, \sigma)$.

3) $\#(Sol(\mathcal{O}, \sigma)) \leq \dim_{\mathbb{Q}}(\mathbb{Q}[A]/I(\mathcal{O}, \sigma))$.

Proof. Let $N := \#(\mathcal{O}) \times \#(\mathrm{CutOut}(\mathcal{O}))$ so that $\mathbb{Q}[A] = \mathbb{Q}[a_1, a_2, \ldots, a_N]$. We embed the affine space $\mathbb{A}^{\mathcal{O}}_{\mathbb{Q}} = \mathbb{A}^N_{\mathbb{Q}}$ in $\mathbb{A}^N_{\mathbb{C}}$ and we denote by $\mathcal{Z}$ the subscheme of $\mathbb{A}^N_{\mathbb{C}}$ defined by $I(\mathcal{O}, \sigma)$. Then $\mathcal{Z} = \mathbb{X}(\mathcal{O}, \sigma) \otimes_{\mathbb{Q}} \mathbb{C}$. Let $P \in \mathcal{Z}$ be a closed point; then $P := (\alpha_1, \ldots, \alpha_N)$, with the α_i's complex numbers. By the construction of $I(\mathcal{O}, \sigma)$, P corresponds to a reduced Gröbner basis with respect to σ of an ideal I containing $\{F_1, F_2, \ldots, F_m\}$, By Lemma 3.2 we know that I is radical and its reduced Gröbner basis has all the coefficients rational, which means that $P \in \mathbb{A}^N_{\mathbb{Q}}$. This shows that $\mathbb{X}(\mathcal{O}, \sigma)$ is rational and zero-dimensional and it is in one-to-one correspondence with those Fractions of $\mathcal{D}$ which solve Problem 2.
Condition 3 follows trivially. $\square$

This completes our construction and allows to actually devise an *algorithm* which computes all the solutions to Problem 2. As we said in the introduction, this has been done in CoCoAL.

Conjecture 3.4 *The ideal $I(\mathcal{O}, \sigma)$ is radical.*

Corollary 3.5 *If the Conjecture 3.4 is true, then equality holds in Condition 3) of Theorem 3.3.*

Proof. ¿From Condition 1 of Theorem 3.3 we know that the points of $\mathbb{X}(\mathcal{O}, \sigma)$ are all closed and rational. If $I(\mathcal{O}, \sigma)$ is radical, then $\dim_{\mathbb{Q}}(\mathbb{Q}[A]/I(\mathcal{O}, \sigma))$ coincides with the number of points and we are done. $\square$

4 Some Examples

Example 1 (continued) We show how to complete the discussion of Example 1. We recall that $\mathcal{O} := \{1, x, y, z\}$ and we have already seen that $\mathrm{CutOut}(\mathcal{O}) = \{xy, xz, yz\}$. Let us choose *DegRevLex* as a degree-compatible term-order. We know that $DegRevLex(\mathcal{O}, xy) = DegRevLex(\mathcal{O}, xz) = DegRevLex(\mathcal{O}, yz) = \mathcal{O}$. Then we construct the polynomials $G_i := T_i - R_i$ where $R_i := \sum_{T\in\mathcal{O}} a_{T,i}T$. We get

$$
\begin{aligned}
&G_1 := yz + a_4x + a_3y + a_2z + a_1,\\
&G_2 := xz + a_8x + a_7y + a_6z + a_5,\\
&G_3 := xy + a_{12}x + a_{11}y + a_{10}z + a_9.
\end{aligned}
$$

We impose that $\{F_1, F_2, F_3, G_1, G_2, G_3\}$ is a DegRevLex-Gröbner basis and we obtain the following set $\mathcal{E}$ of polynomials in $\mathbb{Q}[A]$:

$$
\begin{aligned}
&a_4a_6 - a_2a_8 - a_3a_{12} + a_8a_{12} + a_1 + a_4,\\
&a_3a_6 - a_2a_7 - a_3a_{11} + a_8a_{11} - a_5 - a_7,\\
&a_3a_{10} - a_8a_{10},\\
&a_2a_5 - a_1a_6 + a_3a_9 - a_8a_9,\\
&a_2a_8 - a_4a_{11} + a_3a_{12} - a_8a_{12} - a_1 - a_4,\\
&a_2a_7 - a_7a_{12},\\
&a_2a_6 + a_3a_{10} - a_2a_{11} - a_6a_{12} + a_9 + a_{10},\\
&a_2a_5 + a_3a_9 - a_1a_{11} - a_5a_{12},\\
&a_6a_8 + a_7a_{12} - a_5,\\
&a_6a_7 + a_7a_{11} + a_7,\\
&a_6^2 + a_7a_{10} + a_6,\\
&a_5a_6 + a_7a_9 + a_5,\\
&a_8a_{10} + a_{11}a_{12} - a_9,\\
&a_7a_{10} + a_{11}^2 + a_{11},\\
&a_6a_{10} + a_{10}a_{11} + a_{10},\\
&a_5a_{10} + a_9a_{11} + a_9,\\
&a_2a_4 + a_4a_{12} + a_4,\\
&a_2a_3 + a_4a_{11} - a_1,\\
&a_2^2 + a_4a_{10} + a_2,\\
&a_1a_2 + a_4a_9 + a_1,\\
&a_4a_{10} + a_{12}^2 + a_{12},\\
&a_3a_{10} + a_{11}a_{12} - a_9,\\
&a_2a_{10} + a_{10}a_{12} + a_{10},\\
&a_1a_{10} + a_9a_{12} + a_9,\\
&a_3a_4 + a_4a_8 + a_4,\\
&a_3^2 + a_4a_7 + a_3,\\
&a_2a_3 + a_4a_6 - a_1,\\
&a_1a_3 + a_4a_5 + a_1,\\
&a_4a_7 + a_8^2 + a_8,\\
&a_3a_7 + a_7a_8 + a_7,\\
&a_2a_7 + a_6a_8 - a_5,\\
&a_1a_7 + a_5a_8 + a_5.
\end{aligned}
$$

We compute the multiplicity of the associated ideal $I(\mathcal{E})$, which turns out to be 58 and indeed there are 58 distinct solutions out of the $70 = \binom{8}{4}$ 4-tuples of points in $\mathcal{D}$. They are the 4-tuples of points which are not planar.

Example 2 (continued) We show how to complete the discussion of Example 2. We have $\mathcal{O} := \{1, x, y, xy, y^2, xy^2\}$ and we have already seen that $\mathrm{CutOut}(\mathcal{O}) = \{x^2\}$. We have chosen *Lex* with $x > y$. We know that $Lex(\mathcal{O}, x^2) = \mathcal{O}$ and then we may construct the polynomial

$$G_1 := x^2 + a_6xy^2 + a_5xy + a_4x + a_3y^2 + a_2y + a_1.$$

We impose that $\{F_1, F_2, G_1\}$ is a Lex-Gröbner basis and we obtain the following set $\mathcal{E}$ of polynomials in $\mathbb{Q}[A]$

$$
\begin{aligned}
&a_5^2 + 2a_4a_6 + a_6^2 - a_3,\\
&2a_4a_5 + 2a_5a_6 - a_2,\\
&a_4^2 - a_1 - 1,\\
&a_3a_4 + a_2a_5 + a_1a_6 + a_3a_6,\\
&a_2a_4 + a_1a_5 + a_3a_5 + a_2a_6,\\
&a_1a_4.
\end{aligned}
$$

We compute the multiplicity of the associated ideal $I(\mathcal{E})$, which turns out to be 27 and indeed there are 27 distinct solutions out of the $84 = \binom{9}{6}$ 6-tuples of points in $\mathcal{D}$.

Remark 4.1 We observe that our method is suitable for many generalizations. We give a hint to one of them; suppose we want to find all the solutions of Example 2, *with the extra condition that the fractions contain the three points* $(-1,-1), (-1,0), (0,-1)$. It suffices to impose that the polynomial $G_1 := x^2 + a_6xy^2 + a_5xy + a_4x + a_3y^2 + a_2y + a_1$ vanishes at the three points. This yields three linear conditions L_1, L_2, L_3 on the a_i's. Now the solutions to our problem are coded in the ideal $I(\mathcal{E}) + Ideal(L_1, L_2, L_3)$. Computing its multiplicity, we get 6, and indeed there are 6 fractions of $\mathcal{D}$, which solve our problem. They are:

$$
\begin{aligned}
&\{\ (-1,-1),\ (-1,0),\ (0,-1),\ (0,0),\ (-1,1),\ (0,1)\ \},\\
&\{\ (-1,-1),\ (-1,0),\ (0,-1),\ (0,0),\ (-1,1),\ (1,1)\ \},\\
&\{\ (-1,-1),\ (-1,0),\ (0,-1),\ (0,0),\ \ (0,1),\ (1,1)\ \},\\
&\{\ (-1,-1),\ (-1,0),\ (0,-1),\ (1,0),\ (-1,1),\ (0,1)\ \},\\
&\{\ (-1,-1),\ (-1,0),\ (0,-1),\ (1,0),\ (-1,1),\ (1,1)\ \},\\
&\{\ (-1,-1),\ (-1,0),\ (0,-1),\ (1,0),\ \ (0,1),\ (1,1)\ \}.
\end{aligned}
$$

References

[AL] W. W. Adams, P. Loustaunau, *An Introduction to Gröbner Bases*, Graduate Studies in Mathematics, AMS (1994)

[BHH] George E. P. Box, W. G. Hunter, J. S. Hunter, *Statistics for Experimenters.* John Wiley & Sons, New York (1978)

[CDNR] A. Capani, G. De Dominicis, G. Niesi, L. Robbiano, *Computing Minimal Finite Free Resolutions*, J. Pure Appl. Algebra; Proceedings of MEGA96. To appear

[CNR1] A. Capani, G. Niesi, L. Robbiano, CoCoA*, a system for doing Computations in Commutative Algebra*, (1995). Available via anonymous ftp from `lancelot.dima.unige.it`

[CNR2] A. Capani, G. Niesi, L. Robbiano, *Some Features of* CoCoA 3, Moldova Journal of Computer Science. To appear

[CR] G. Carrà, L. Robbiano, *On SuperG-Bases*, J. Pure Appl. Algebra **68** (1990) 279–292

[CLO] D. Cox , J. Little, D. O'Shea, *Ideal, Varieties, and Algorithms*, Springer-Verlag New York (1992)

[D] A. Dey, *Orthogonal fractional factorial designs* John Wiley and Sons, New York (1985)

[DS] P. Diaconis, B. Sturmfels, *Algebraic Algorithms for Sampling from Conditional Distributions*, Preprint SC 93-17 (August 1993) ZIB Berlin (1993)

[E] D. Eisenbud, *Commutative Algebra with a View Toward Algebraic Geometry*, Springer Graduate Texts in Mathematics **150** (1995)

[F] R.A. Fisher, *The Design of Experiments*, Oliver and Boyd, Edinburgh (1935) (1st ed.)

[H] R.M. Heiberger, *Computation for the Analysis of Designed Experiments*, John Wiley and Sons, New York (1989)

[LI] C.T. Liao and H.K. Iyer, *Construction of orthogonal two-level designs of user-specified resolution where* $N \neq 2^k$, Technometrics **38** (1996), 342–353

[MR] F. Mora, L. Robbiano, *The Gröbner Fan of an Ideal*, in L. Robbiano, ed., *Computational Aspects of Commutative Algebra*, Academic Press, London, (1989)

[NS] A. Neumaier and J.J. Seidel, *Measures of strength* $2e$*, and optimal designs of degree* e, Sankhya **54** (1992), 299-309

[PRR] G. Pistone, L. Robbiano, M.P. Rogantin, *Factorial Designs, Distracted Fractions and Hilbert Functions*, In preparation

[PW] G. Pistone G., H.P. Wynn, *Generalised confounding and Gröbner bases*, Biometrika **83**-3, (1996), 653–666

[RHF] B.L. Raktoe, A. Hedayat, W.T. Federer, *Factorial Designs*, John Wiley and Sons, New York (1981)

[R1] L. Robbiano, *Term Orderings in the polynomial ring*, Proceedings of EUROCAL-85, Lecture Notes in Computer Science **203 II** (1985)

[R2] L. Robbiano, *On the Theory of Graded Structures*, J. Symbolic Comput. **2** (1986), 139–170

[RS] L. Robbiano, M. Sweedler, *Ideal and Subalgebra Coefficients*, Proc. Amer. Math. Soc. To appear

[StS] A.P. Street and D.J. Street, *Combinatorics of Experimental Design*, Oxford Clarendon, (1987)

[Y] F. Yates, *Design and Analysis of Factorial Experiments*, London: Imperial Bureau of Soil Sciences (1937) **.**