COMPUTATIONAL ALGEBRAIC GEOMETRY OF PROJECTIVE CONFIGURATIONS

BERND STURMFELS*

Abstract. This article gives an exposition of certain algorithmic and algebraic aspects related to the computer-aided study of plane incidence configurations. It is computationally hard to decide whether a configuration can be coordinatized over a field K, and for the field of rational numbers it may even be undecidable. The algebraic techniques to be discussed, such as the computation of final polynomials using Gröbner bases, are very general and thus apply to many other geometry problems as well.

1. Introduction.

A *configuration* $\mathcal{C} = (\mathcal{P}, \mathcal{L})$ consists of a finite set $\mathcal{P}$ of *points* and a set $\mathcal{L} \subset 2^{\mathcal{P}}$ of *lines* such that any two lines have at most one point in common. Incidence relations between points and lines play a decisive role for many applications of projective geometry, such as scene analysis, realizability of polyhedra, or rigidity of frameworks. In order to design a reasonably general interactive computer system for applied projective geometry it is therefore important to study some basic properties of configurations.

This article provides an introductory exposition on the computational algebraic geometry of configurations by discussing geometric constructions, symbolic algorithms, complexity results, related algebraic geometry results, and many non-trivial examples. In particular, we shall emphasize the fact that, in general, configurations possess a very rich algebraic structure, and consequently various straightforward questions about them are extremely difficult.

Most of the ideas and results in this paper generalize immediately to incidence configurations in higher dimensions. Such configurations can be axiomatized in a very natural manner as *matroids* or *combinatorials geometries* [27]. For the sake of simplicity, however, we restrict ourselves to the rank 3 planar case.

A *coordinatization* or *realization* of a configuration $\mathcal{C}$ over a field K is a mapping $\mathbf{X} : \mathcal{P} \to K^3$, $p \mapsto \mathbf{x}_p$ such that, for all distinct $i, j, k \in \mathcal{P}$, $\det(\mathbf{x}_i, \mathbf{x}_j, \mathbf{x}_k) = 0$ if and only if $\{i, j, k\}$ is contained in some line of $\mathcal{C}$.

We will assume that $\mathcal{P} = \{1, 2, \ldots, n\}$ for some $n \in \mathbb{N}$. The set of $3 \times n$-matrices over K is identified as usual with K^{3n}, and thus every coordinatization $\mathbf{X}$ of $\mathcal{C}$ can be thought of as a point $\mathbf{X} = (\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_n)$ in K^{3n}. The subset of K^{3n} corresponding to realizations of $\mathcal{C}$ is the *realization space* of $\mathcal{C}$, and it will be denoted by $\mathcal{R}_K(\mathcal{C})$ (or $\mathcal{R}(\mathcal{C})$ if the specific field is understood).

*Institute for Mathematics and its Applications, University of Minnesota, Vincent Hall 514, 206 Church Street S.E., Minneapolis, MN 55455, U.S.A.

Two $3 \times n$-matrices $\mathbf{X}$ and $\mathbf{X}'$ are *projectively equivalent* if $\mathbf{X}' = A \cdot \mathbf{X} \cdot D$, where A is a non-singular 3×3-matrix and D is a non-singular diagonal $n \times n$-matrix. If $\mathbf{X}$ is a realization of a configuration $\mathcal{C}$, so is every matrix $\mathbf{X}'$ projectively equivalent to $\mathbf{X}$. Hence the realizations of $\mathcal{C}$ correspond to labelled subsets of the projective plane $P^2(K)$ over K which satisfy the given incidence structure; see the examples below.

It seems appropriate at this point to briefly comment on some mathematical tools to be used throughout this paper. We shall assume that the reader is familiar with few basic concepts of algebraic geometry such as introduced in the first chapters of [17] or [21]. Section 5 deals with recent improvements of *Hilbert's Nullstellensatz*, and it might be helpful to review the usual (non-constructive) proofs given for this classical result. In Section 6 we discuss *final polynomials*, *final syzygies* and their application to configurations. That section makes use of the concept of *Gröbner bases* for polynomial ideals [5] and some ideas related to the *Main Theorem of Elimination Theory* [21, Chapter 2].

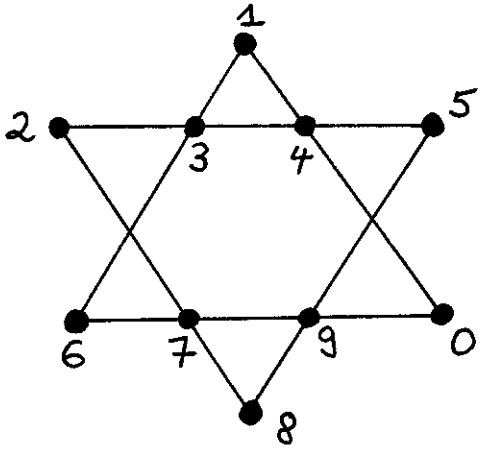
In our study of configurations we frequently use the so-called *Zariski topology*. For any field K, the Zariski topology on K^n can be defined as the weakest topology with respect to which all zero sets of polynomials functions (or *affine algebraic varieties*) are closed. The Zariski topology is in general <u>not</u> Hausdorff, and the Zariski topology on K^{m+n} is <u>not</u> the product of the Zariski topologies on K^m and K^n. If K is a subfield of $\mathbb{C}$, then every *Zariski-closed* subset of K^n is also closed in the classical real topology, but not vice versa. For example, the only non-trivial closed sets in the Zariski topology on $\mathbb{C}^1$ are the finite sets. This implies that every infinite subset of $\mathbb{C}^1$ is *Zariski-dense* in $\mathbb{C}^1$.

The realization space $\mathcal{R}_K(\mathcal{C})$ of a configuration $\mathcal{C}$ is in general not a Zariski-closed subset of K^{3n} because it is defined by inequalities as well as equations, and, if K is a subfield of $\mathbb{C}$, it is also not closed in the classical topology on K^{3n}.

Let us now discuss the configurations depicted in Figure 1. The configuration $\mathcal{C}_1$ can be realized over every field of characteristic 0. For example, a coordinatization of $\mathcal{C}_1$ over the field $\mathbb{Q}(u, v, x, y)$ of rational functions in 4 variables is given by

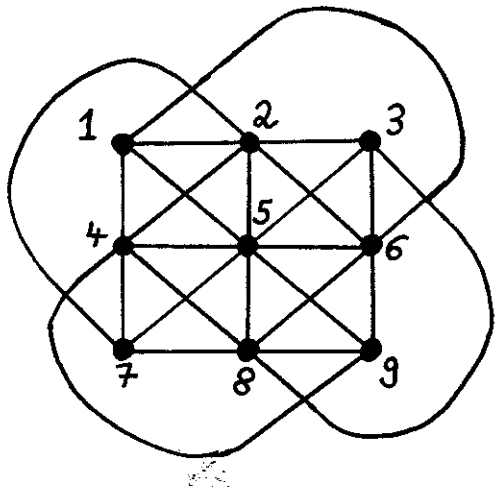
$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1-v & 1 & 1-u & 1 \\ 0 & 1 & 1 & u & 0 & 1 & y-v+u-uy & x & x-xu & u \\ 0 & 0 & 1 & v & 1 & 1 & y-vy & y & x-u+v-vx & v \end{pmatrix}$$

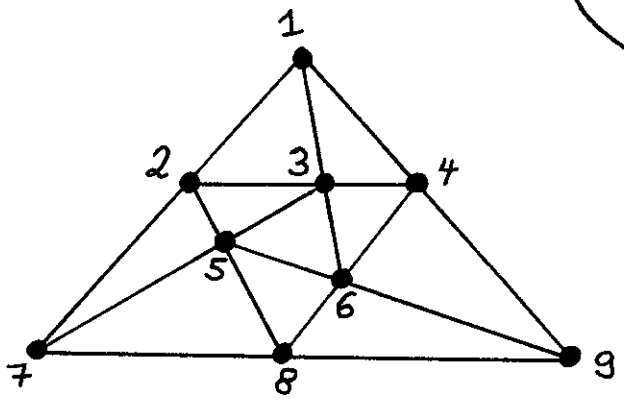
From this matrix we obtain a realization of $\mathcal{C}$ over $\mathbb{Q}$ by substituting "sufficiently generic" rational numbers for u, v, x and y. For example, we can choose $u = 2, v = 3, x = 5$ and $y = 11$. The above matrix is set up in such a way that *every* realization of $\mathcal{C}$ over $\mathbb{Q}$ (modulo projective equivalence) can be obtained by specializing u, v, x and y. In other words, $\mathcal{R}(\mathcal{C})$ is Zariski-dense in the set of matrices projectively equivalent to the ones parameterized above.



$\mathcal{C}_1$: 136 140 2345
278 589 6790

$\mathcal{C}_2$: 123 147 159 168
249 258 267 348
357 369 456 789





$\mathcal{C}_3$: 127 136 149
234 258 357
468 569 789

Figure 1. Three configurations, given by their lines.

The matrix

$$\begin{pmatrix} 1 & 0 & 1+\sqrt{-3} & 0 & 1 & 1-\sqrt{-3} & -1+\sqrt{-3} & -2 & 0 \\ 0 & 1 & 2 & 0 & 1 & 1-\sqrt{-3} & 0 & -1+\sqrt{-3} & -1 \\ 0 & 0 & 0 & 1 & 1 & 2 & -2 & -2 & -1 \end{pmatrix}$$

is a coordinatization of the (Sylvester-Gallai) configuration $\mathcal{C}_2$ over the complex numbers. This implies that $\mathcal{C}_2$ can be coordinatized over every field of characteristic 0 in which the polynomial x^2+3 has a root. It can be seen using the methods to be introduced in Section

6 that this condition is also necessary, and therefore $\mathcal{C}_2$ cannot be coordinatized over the real numbers $\mathbb{R}$.

On the other hand, the configuration $\mathcal{C}_3$ is realizable over $\mathbb{R}$. It is also realizable over $\mathbb{Q}$ (i.e. the figure $\mathcal{C}_3$ can be constructed with ruler and pencil), but finding rational coordinates involves more complicated geometric or algebraic arguments.

Let us give a summary of some properties of configurations to be considered in this paper. Given a configuration $\mathcal{C}$ in terms of its combinatorial description, we are interested in the following questions:

(i) *Is there a realization of $\mathcal{C}$ over some field K ?*

There is an extensive literature in matroid theory [27] and finite geometry [9] dealing with coordinatizations over characteristic p and embeddings of configurations into finite projective planes. Throughout this paper, however, we will be concerned exclusively with fields of characteristic 0.

(ii) *Can $\mathcal{C}$ be coordinatized over some field K of characteristic 0 ?*

Note that the answer to (ii) is "yes" if and only if $\mathcal{C}$ can be coordinatized over the complex numbers $\mathbb{C}$. From the computational geometry point of view, one is certainly more interested in the Euclidean plane:

(iii) *Can $\mathcal{C}$ be coordinatized over the reals $\mathbb{R}$?*

It is natural to ask whether a realization of $\mathcal{C}$ can constructed with pencil and ruler alone.

(iv) *Can $\mathcal{C}$ be coordinatized over the rationals $\mathbb{Q}$?*

If so, can we find a rational parameter representation for the variety of all real realizations ? Or, slightly more general :

(v) *Is the set of rational matrices realizing $\mathcal{C}$ dense in the set of all real realizations ?*

Note that this question makes sense in the classical real topology as well as in the Zariski topology.

(vi) *If the answer to (iv) is "yes", then find "reasonably small" integer coordinates !*

(vii) *If the answer to (i),(ii),(iii) or (iv) is "no", then find a "reasonably short" nonrealizability proof !*

More precisely, in the latter case one would like to have a single refutational condition which encodes the entire argument. Such a condition can always be given in form of a *final polynomial* [2], [23], [25]. See Sections 5 and 6 for details and some new results on the algorithmic construction of final polynomials.

Some configurations, such as the Desargues configuration (see Figure 3), express a geometric theorem. By this we mean that one (or more) of the given incidences is a consequence of the other incidences in every coordinatization.

(viii) *Does $\mathcal{C}$ express a geometric theorem ?*

Every such incidence theorem can also be phrased as a non-realizability result with respect to possible counterexamples (e.g. the Non-Desargues-configuration), and hence we can ask :

(ix) *If $\mathcal{C}$ does express a geometric theorem, then find a final polynomial proof !*

In the following we shall discuss to what extent it is theoretically possible and practically feasible to use computer-aided geometric reasoning to answer some of the above questions.

2. A construction method and more examples of configurations.

Consider the configuration $\mathcal{L}_1$ which is given by the following set of lines

$$\mathcal{L}_1 \quad := \quad \{\, 124,\ 138,\ 179,\ 237,\ 259,\ 350,\ 456,\ 480,\ 678,\ 690 \,\};$$

see Figure 2. How can we find a realization of $\mathcal{L}_1$ over $\mathbb{R}$ (or even over $\mathbb{Q}$) ? Since each of the ten points is incident to three lines in $\mathcal{L}_1$, it is not possible to use a direct inductive argument to establish the realizability of $\mathcal{L}_1$. There is no proper subconfiguration each of whose realizations extends to a realization of $\mathcal{L}_1$. For example, a realization of the induced configuration on $\{1, 2, \ldots, 9\}$ can be extended by a point 0 if and only if the lines $\overline{35}, \overline{48}$ and $\overline{69}$ intersect.

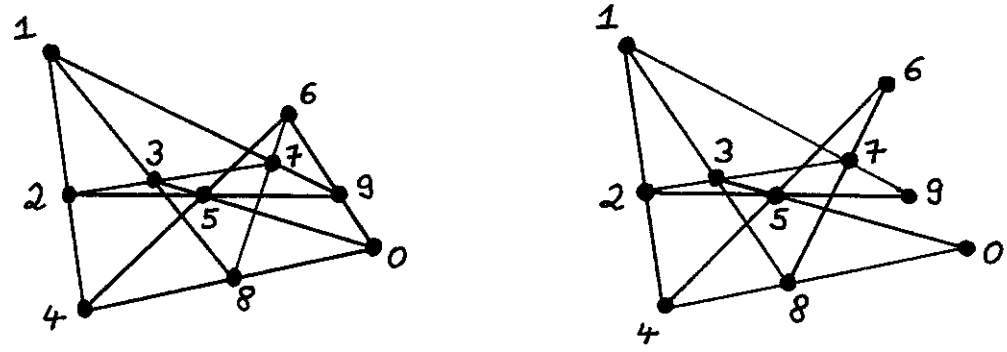


Figure 2. The configurations $\mathcal{L}_1$ and $\widetilde{\mathcal{L}}_1$.

We suggest the following strategy. First construct a parameterization of the realization space of a slightly relaxed configuration, and then try to solve the algebraic equations for the additional dependency in terms of the given parameters. One word of caution: by "a parameterization of the realization space" we mean, of course, a parameterization of a subset of its Zariski-closure $\overline{\mathcal{R}(\mathcal{C})}$ in $K^{3\cdot 10}$.

Consider the configuration with set of lines $\widetilde{\mathcal{L}}_1 := \mathcal{L}_1 \setminus \{690\}$. This relaxed configuration admits a linear construction sequence, that is, every realization of $\widetilde{\mathcal{L}}_1$ can be obtained

through arbitrarily choosing some of the points and succesive construction of the remaining points as intersections of spanned lines. The computation of such a construction sequence is straightforward, and in this case we obtain the following result.

A construction sequence for the configuration $\widetilde{\mathcal{L}}_1$*:*

(1) Pick the points $1, 2, 3, 5$ and 6 in general position in the projective plane.

(2) Pick the point 7 in general position on the line $\overline{23}$.

(3) Define 4 as the intersection of $\overline{12}$ and $\overline{56}$.

(4) Define 8 as the intersection of $\overline{13}$ and $\overline{67}$.

(5) Define 9 as the intersection of $\overline{17}$ and $\overline{25}$.

(6) Define 0 as the intersection of $\overline{35}$ and $\overline{48}$.

It is clear that every realization of $\widetilde{\mathcal{L}}_1$ can be obtained from this construction sequence by suitable choices in (1) and (2). And, conversely, every choice in (1) and (2) (up to a Zariski-closed proper subset defined by unwanted additional degeneracies) yields a realization of $\widetilde{\mathcal{L}}_1$.

The points $1, 2, 3$ and 5 are chosen in (1) to be in general position, and hence it can be assumed that, after a projective transformation, these points have homogeneous coordinate vectors $\mathbf{x}_1 := (1,0,0)^t$, $\mathbf{x}_2 := (0,1,0)^t$, $\mathbf{x}_3 := (0,0,1)^t$, $\mathbf{x}_5 := (1,1,1)^t$. For point 6 we write $\mathbf{x}_6 := (a,b,c)^t$ where a, b and c are indeterminants. According to the rule (2), we set $\mathbf{x}_7 := u \cdot \mathbf{x}_2 + v \cdot \mathbf{x}_3$ where u and v are indeterminants.

Finally, the rules (3) – (6) can be applied to compute the (homogeneous) coordinates of the remaining points as polynomial functions in the variables a, b, c, u and v. This is done most easily using the simple Grassmann algebra formula

$$(\mathbf{x}_i \vee \mathbf{x}_j) \wedge (\mathbf{x}_k \vee \mathbf{x}_l) \quad = \quad -\det(\mathbf{x}_i, \mathbf{x}_j, \mathbf{x}_k) \cdot \mathbf{x}_l + \det(\mathbf{x}_i, \mathbf{x}_j, \mathbf{x}_l) \cdot \mathbf{x}_k.$$

An introduction to Cayley or Grassmann algebra and its applications is given in the article of N. White in this volume [29]. For our purposes it suffices to think of the symbols "$\vee$" and "$\wedge$" as denoting sum and intersection of vector subspaces, respectively.

From (1) – (6) we obtain

$$\mathbf{X} \quad = \quad \begin{pmatrix} 1 & 0 & 0 & a-c & 1 & a & 0 & ua & v & ua(b-c) \\ 0 & 1 & 0 & b-c & 1 & b & u & 0 & u & ua(b-c) \\ 0 & 0 & 1 & 0 & 1 & c & v & -bv+uc & v & -(bv-uc)(b-a) \end{pmatrix}$$

Let us rephrase this result in algebraic geometry terms: The above matrix represents a birational isomorphism [17, Chapter III] between K^5 and $\mathcal{R}(\widetilde{\mathcal{L}}_1)$. Alternatively, the matrix $\mathbf{X}$ can be viewed as a coordinatization of $\widetilde{\mathcal{L}}_1$ over a field extension of transcendence degree 5 over the rational numbers $\mathbf{Q}$. An interesting discussion of transcendence degrees of coordinatizations of combinatorial geometries is found in [28].

Now it is easy to obtain a birational isomorphism between $\mathcal{R}(\mathcal{L}_1)$ and a hypersurface in K^5. The desired hypersurface is defined by the determinant corresponding to the missing line 670. We have

$$\det(\mathbf{x}_6, \mathbf{x}_9, \mathbf{x}_0) \quad = \quad u^2a^2c - vua^2c - b^3v^2 + vb^2uc + ab^2v^2 - vbuac + vuac^2 - u^2ac^2.$$

It remains to find a real or rational point on this hypersurface which is also contained in $\mathcal{R}(\mathcal{L}_1)$. In other words, we need to find $a, b, c, u, v \in \mathbb{Q}$ such that $\det(\mathbf{x}_6, \mathbf{x}_9, \mathbf{x}_0) = 0$ and such that all 3×3-subdeterminants of $\mathbf{X}$ which are non-zero in $\mathbb{Q}(a, b, c, u, v)$ remain non-zero after the specialization. An example of such a solution is given by $a := -4$, $b := 3$, $c := 1$, $u := 7$ and $v := 4$. We do not know whether for this configuration the rational realizations $\mathcal{R}_{\mathbb{Q}}(\mathcal{L}_1)$ are dense in the real realizations $\mathcal{R}_{\mathbb{R}}(\mathcal{L}_1)$.

Next consider the *Desargues-configuration* which is given by the lines

$$\mathcal{L}_2 := \{\, 125, 136, 148, 237, 249, 340, 567, 589, 680, 790 \,\}, \qquad \text{see Figure 3.}$$

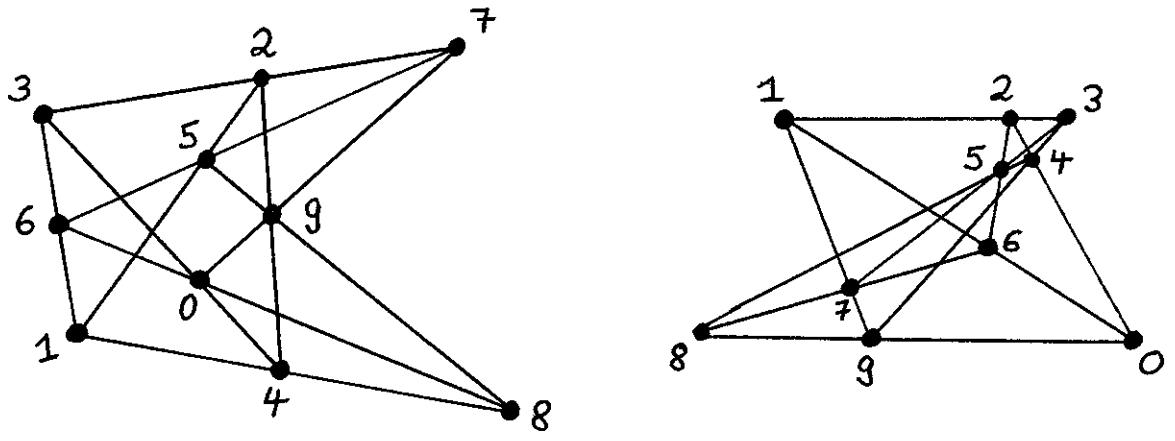


Figure 3. The Desargues configuration $\mathcal{L}_2$ and the non-realizable 10_3-configuration $\mathcal{L}_3$.

Constructing the (seemingly) relaxed configuration $\mathcal{L}_2 \setminus \{790\}$ we obtain the following parameterized matrix

$$\mathbf{X} \quad = \quad \begin{pmatrix} a & 1 & 0 & 0 & 1 & a & a-c & -ua & u(a-c) & 0 \\ c & 0 & 1 & 0 & 1 & b & b-c & -uc & 0 & ua(b-c) \\ c & 0 & 0 & 1 & 1 & c & 0 & -uc+v & -v & av \end{pmatrix}.$$

We have $\det(\mathbf{x}_7, \mathbf{x}_9, \mathbf{x}_0) = 0$ in $\mathbb{Q}(a, b, c, u, v)$ which proves Desargues' theorem, or equivalently, the non-realizability of $\mathcal{L}_2 \setminus \{790\}$.

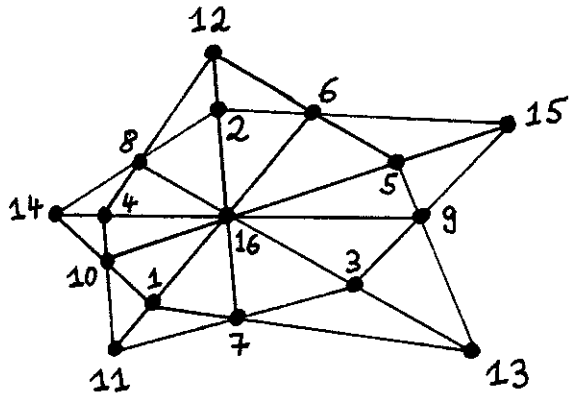


Figure 4. Saam's configuration $\mathcal{L}_{Saam}$.

The second diagram in Figure 3 shows another very interesting example. This configuration on ten points has the following ten lines:

$$\mathcal{L}_3 := \{\, 123, 160, 179, 240, 256, 349, 357, 458, 678, 890 \,\}.$$

Constructing the relaxation $\mathcal{L}_3 \setminus \{890\}$, we obtain $\mathbf{X} =$

$$\begin{pmatrix} 1 & 0 & u & 0 & cu & 1 & a & cu(a-b) & ub & 0 \\ 0 & 1 & v & 0 & ub+(c-a)v & 1 & b & (a-b)(ub+cv-av) & bv & 1 \\ 0 & 0 & 0 & 1 & cu & 1 & c & (c^2-2cb+ab)u+(2ac-c^2-a^2)v & cv & 1 \end{pmatrix}.$$

This configuration is not realizable over any field, as is seen from the identity

$$\det(\mathbf{x}_8, \mathbf{x}_9, \mathbf{x}_0) \;=\; -u\cdot(b-c)^2\cdot(-ub+av) \;=\; \det(\mathbf{x}_2, \mathbf{x}_3, \mathbf{x}_4)\det(\mathbf{x}_1, \mathbf{x}_6, \mathbf{x}_7)^2\det(\mathbf{x}_3, \mathbf{x}_4, \mathbf{x}_7),$$

which shows that the collinearity of 890 would imply the collinearity of 167, 234 or 347, all of which are not contained in $\mathcal{L}_3$. See e.g. [18] for an alternative non-realizability proof for this configuration.

The Grassmann expansion of linear construction sequences is also a very efficient method for automated theorem proving in projective geometry. As a non-trivial example for that statement we consider an incidence theorem which has recently been discovered by A. Saam [22]. It can be stated in terms of the following configuration, see Figure 4.

$$\mathcal{L}_{Saam} \;=\; \{\{1,6,11,16\},\{2,7,12,16\},\{3,8,13,16\},\{4,9,14,16\},\{5,10,15,16\},\{1,7,13\},$$
$$\{2,8,14\},\{3,9,15\},\{4,10,11\},\{5,6,12\},\{1,10,14\},\{2,6,15\},\{3,7,11\},\{4,8,12\},\{5,9,13\}\}.$$

PROPOSITION 2.1. [22] *Let* $\mathbf{X}$ *be a configuration of* 16 *points in* $P^2(K)$, *where* K *is any field, such that* $\mathbf{X}$ *realizes the five* 4*-point lines and nine of the ten* 3*-point lines in* $\mathcal{L}_{Saam}$. *Then also the remaining fifteenth line of* $\mathcal{L}_{Saam}$ *is collinear in* $\mathbf{X}$.

Proof. This proposition can be proved by showing that for a linear construction of $\mathcal{L}_{Saam} \setminus \{\{1, 10, 14\}\}$ also the points $\mathbf{x}_1, \mathbf{x}_{10}$ and $\mathbf{x}_{14}$ are collinear. Consider the following construction sequence.

Construction sequence for Saam's configuration :

$$\begin{gathered}
\mathbf{x}_1 := (1,0,0)^t,\ \mathbf{x}_2 := (0,1,0)^t,\ \mathbf{x}_3 := (0,0,1)^t,\ \mathbf{x}_5 := (1,1,1)^t, \\
\mathbf{x}_6 := (a,b,c)^t,\ \mathbf{x}_7 := (d,e,f)^t, \\
\mathbf{x}_{16} := (\mathbf{x}_1 \vee \mathbf{x}_6) \wedge (\mathbf{x}_2 \vee \mathbf{x}_7) \\
\mathbf{x}_8 := u \cdot \mathbf{x}_3 + v \cdot \mathbf{x}_{16} \\
\mathbf{x}_{13} := (\mathbf{x}_3 \vee \mathbf{x}_8) \wedge (\mathbf{x}_1 \vee \mathbf{x}_7) \\
\mathbf{x}_{15} := (\mathbf{x}_5 \vee \mathbf{x}_{16}) \wedge (\mathbf{x}_2 \vee \mathbf{x}_6) \\
\mathbf{x}_9 := (\mathbf{x}_3 \vee \mathbf{x}_{15}) \wedge (\mathbf{x}_5 \vee \mathbf{x}_{13}) \\
\mathbf{x}_{12} := (\mathbf{x}_2 \vee \mathbf{x}_7) \wedge (\mathbf{x}_5 \vee \mathbf{x}_6) \\
\mathbf{x}_4 := (\mathbf{x}_9 \vee \mathbf{x}_{16}) \wedge (\mathbf{x}_8 \vee \mathbf{x}_{12}) \\
\mathbf{x}_{11} := (\mathbf{x}_1 \vee \mathbf{x}_6) \wedge (\mathbf{x}_3 \vee \mathbf{x}_7) \\
\mathbf{x}_{10} := (\mathbf{x}_5 \vee \mathbf{x}_{15}) \wedge (\mathbf{x}_4 \vee \mathbf{x}_{11}) \\
\mathbf{x}_{14} := (\mathbf{x}_4 \vee \mathbf{x}_9) \wedge (\mathbf{x}_2 \vee \mathbf{x}_8)
\end{gathered}$$

Using the computer algebra system MAPLE, we computed the corresponding the 3×16-matrix $\mathbf{X}$. The entries of $\mathbf{X}$ are polynomials in the variables a, b, c, d, e, f, u and v of maximal total degree 24. Finally, we evaluate the determinant $\det(\mathbf{x}_1, \mathbf{x}_{10}, \mathbf{x}_{14})$ which reduces to zero in the ring $\mathbb{Q}[a, b, c, d, e, f, u, v]$. This proves Proposition 2.1. □

3. On the existence of coordinatization algorithms.

In this section we summarize some known results concerning the existence of coordinatization algorithms, that is, algorithms to decide the questions (i)–(iv) from Section 1. In the general case we have the following situation.

THEOREM 3.1. *For any field* K, *the following statements are equivalent.*

(1) There exists an algorithm to decide for any finite set of polynomials $\mathcal{F} = \{f_1, \ldots, f_m\} \subset \mathbb{Z}[x_1, \ldots, x_n]$, $m, n \in \mathbb{N}$, *whether the* f_i *have a common zero in* K^n.

(2) There exists an algorithm to decide for an arbitrary plane incidence configuration $\mathcal{C}$ *(or rank* 3 *matroid) whether* $\mathcal{C}$ *is realizable over* K.

A proof for this theorem is outlined in [24] and worked out in detail in [23]. It uses the classical constructions of *projective addition* and *multiplication*. The application of these techniques to coordinatizability of (rank 3) matroids goes back to MacLane. In his 1936 paper [19] he proved that all algebraic numbers are needed in order to coordinatize all C-realizable rank 3 matroids. In other words: arbitrary univariate polynomials with integer

coefficients can be encoded in suitable configurations. Two examples are given in the next section.

A nice description of projective addition and multiplication and a characteristic free proof of MacLane's result can be found in [27, Chapter 1]. The underlying idea generalizes in a straightforward manner to multivariate polynomials [23],[24].

What is the situation for the specific fields we are interested in, namely the rationals, the reals and the complexes ?

Statement (1) is clearly true for algebraically closed fields. By Hilbert's Nullstellensatz (Theorem 5.1), the solvability of polynomial equations over $\mathbb{C}$ reduces to the ideal membership problem which is known to be decidable. Classical decision procedures for the ideal membership problem (see e.g. G. Herrmann [13]) are based on the sucessive computation of resultants and pseudoremainders, and these are still very useful for specific purposes [12],[15]. The best general purpose method in polynomial ideal theory, however, is Buchberger's Gröbner bases method (see Section 6).

Statement (1) is also known to be true for real closed fields, e.g. the reals $\mathbb{R}$ or the real algebraic numbers. The first decision procedure for real closed fields was given by Tarski [26], and the currently most practical such method appears to be Collins' *cylindrical algebraic decomposition* algorithm [7].

It is known that there exist algorithms with the same asymptotic time complexity, namely singly-exponential in the input size, for solving polynomial equations over $\mathbb{R}$ and over $\mathbb{C}$ [6],[10]. Nevertheless, in practice problem (1) is still substantially harder for real closed fields. There is still much work to be done before serious problems in geometry over the real numbers can be solved faster by using a computer than they can using paper and pencil.

Geometric realizability problems are still much more difficult over the field $\mathbb{Q}$ of rational numbers. It is not even known whether there exists a decision procedure for rational polynomials over $\mathbb{Q}$.

PROBLEM 3.2. *Does there exist an algorithm to decide for an arbitrary polynomial* $f \in \mathbb{Q}[x_1, \ldots, x_n]$, $n \in N$, *whether* f *has zeros in* $\mathbb{Q}^n$ *?*

The analogous problem for the integers, Hilbert's 10th problem, has been answered to the negative by Matijasevic in 1971, and this result strongly suggests that (1) does not hold for $\mathbb{Q}$. An introduction and further references to Hilbert's 10th problem and its above rational variant can be found in [16],[20]. From Theorem 3.1 we obtain the following interesting corollary.

COROLLARY 3.3. *Suppose that Problem 3.2, the rational version of Hilbert's 10th problem, has a negative answer. Then the problem whether a given configuration can be constructed with ruler and pencil alone is undecidable.*

4. Complex versus real versus rational realizability.

It follows from the results in the previous section that for every irreducible polynomial $p \in \mathbb{Q}[x]$ of degree ≥ 2 there exist configurations which are not $\mathbb{Q}$-realizable but realizable over every splitting field of p over $\mathbb{Q}$. There also are well-known configurations with eight and nine points [11, Chapter 5],[19],[23] which encode the polynomials $x^2 + x + 1$ and $x^2 - x + 1$ respectively, but which are not obtained by projective addition and multiplication on a line.

In this section we shall discuss two slightly larger examples, namely a $\mathbb{C}$-realizable configuration $\mathcal{L}_{\sqrt{-1}}$ on 12 points which fails to be $\mathbb{R}$-realizable and an $\mathbb{R}$-realizable configuration $\mathcal{L}_{\sqrt{2}}$ on 11 points which fails to be $\mathbb{Q}$-realizable. These configurations are constructed by projective addition and multiplication on a line, and therefore they provide examples to show how these operations work in practice.

Our results will be represented by suitable final polynomials, and thus this section provides also non-trivial examples for the next two sections. We use the abbreviations 0 := 10, A := 11, and B := 12 for point labels in these configurations.

EXAMPLE 4.1. *The projective construction of* $\sqrt{-1}$.

The configuration $\mathcal{L}_{\sqrt{-1}}$ on 12 points is given by the following 11 lines:

1269 1370B 145 2358A 24B 346 567 680 6AB 789 90A

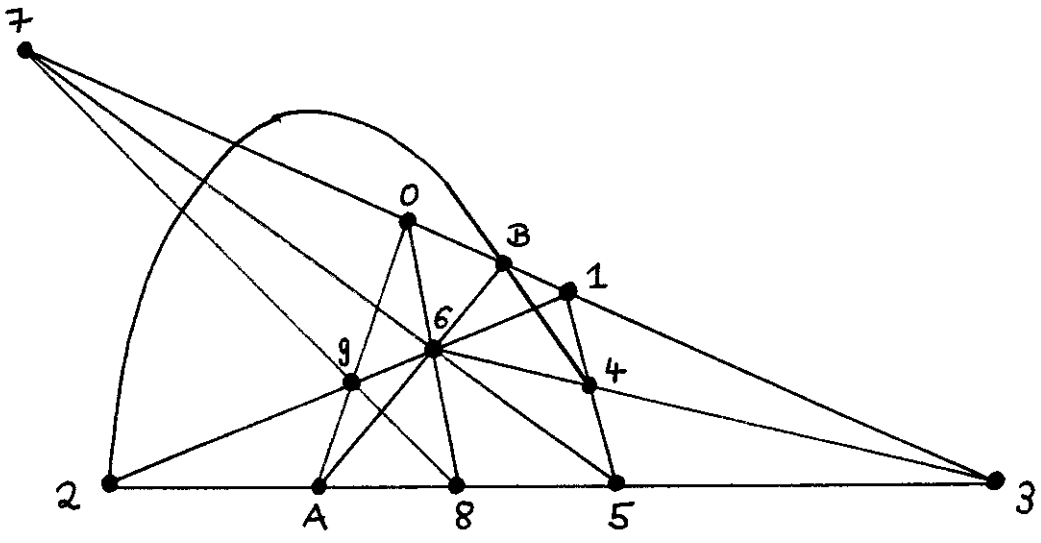


Figure 5. The projective construction of $\sqrt{-1}$ ($\mathcal{L}_{\sqrt{-1}}$).

Choosing the points $1, 2, 3$ and 4 as a projective basis, and prescribing the incidences on the lines $1269, 1370\mathrm{B}$ and $2358\mathrm{A}$, we find that every coordinate matrix for $\mathcal{L}_{\sqrt{-1}}$ is projectively equivalent to

$$\mathbf{X} = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & x_6 & 0 & 1 & x_9 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & y_5 & 0 & y_7 & y_8 & 0 & y_{10} & y_{11} & y_{12} \end{pmatrix}.$$

In the following we use the bracket notation $[ijk]$ for the subdeterminants of $\mathbf{X}$, that is, $[ijk] := \det(\mathbf{x}_i, \mathbf{x}_j, \mathbf{x}_k)$ for all $i, j, k \in \{1, 2, \ldots, 9, 0, A, B\}$.

Each $[ijk]$ can now be expressed as a polynomial in the seven variables y_5, x_6, $y_7, y_8, x_9, y_{10}, y_{11}$ and y_{12}. In the polynomial ring $\mathbb{Q}[y_5, x_6, y_7, y_8, x_9, y_{10}, y_{11}, y_{12}]$ we have the following identity, which has been found by the methods to be described in Section 6.

$$\begin{aligned} 1 + y_8^2 \;=\; & y_8\,\big([346][680] + [346][90\mathrm{A}] + [90\mathrm{A}] + [680]\big) \;-\; y_8^2\,(2\,[346] + [346]^2) \\ & + \big([24\mathrm{B}] - 1 - [346] + [346][24\mathrm{B}] + [346][6\mathrm{AB}] + [6\mathrm{AB}]\big)\,[145] \;+\; (1 + [567])\,[24\mathrm{B}] \\ & + ([24\mathrm{B}] + [6\mathrm{AB}] - 1)\,[346] \;+\; ([6\mathrm{AB}] - 1)\,[567] \;+\; [6\mathrm{AB}] \;+\; \big(1 - [24\mathrm{B}] - [6\mathrm{AB}]\big)\,[789]. \end{aligned}$$

Since at least one factor in every term on the right hand side of this equation must vanish in any realization of $\mathcal{L}_{\sqrt{-1}}$, in order for the matrix $\mathbf{X}$ to be such a realization the left side of the above equation has to vanish, i.e., $\mathcal{L}_{\sqrt{-1}}$ cannot be coordinatized unless $1 + y_8^2 = 0$. In particular, this configuration cannot be realized over $\mathbb{R}$. A complex realization of $\mathcal{L}_{\sqrt{-1}}$ is given by $y_5 = 1\,, x_6 = 1$, $y_7 = -1$, $y_8 = -\sqrt{-1}$, $x_9 = \sqrt{-1}$, $y_{10} = \sqrt{-1}$, $y_{11} = -1$, $y_{12} = 1$.

EXAMPLE 4.2. *The projective construction of* $\sqrt{2}$.

The configuration $\mathcal{L}_{\sqrt{2}}$ on 11 points is given by the following 10 lines:

$$1269 \quad 1370 \quad 145 \quad 2358\mathrm{A} \quad 346 \quad 47\mathrm{A} \quad 567 \quad 680 \quad 789 \quad 90\mathrm{A}$$

As above, we can see that every coordinate matrix for $\mathcal{L}_{\sqrt{2}}$ is projectively equivalent to

$$\mathbf{X} = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & x_6 & 0 & 1 & x_9 & 0 & 1 \\ 0 & 0 & 1 & 1 & y_5 & 0 & y_7 & y_8 & 0 & y_{10} & y_{11} \end{pmatrix}.$$

In the polynomial ring $\mathbb{Q}[y_5, x_6, y_7, y_8, x_9, y_{10}, y_{11}]$ we have the following identity, which shows that $\mathcal{L}_{\sqrt{2}}$ cannot be coordinatized over $\mathbb{Q}$.

$$\begin{aligned} y_{10}^2 - 2 \;=\; & [567][346]([789] + [47\mathrm{A}]) - 4[145][346][567] - [47\mathrm{A}][346][789] - 3[145] \\ & - 5[346] - 3[567] + [47\mathrm{A}][145][346](2 + [346]) - 2[145][346]^2[567] + 2[145][346][789] \\ & + 2[789] + [47\mathrm{A}] + [145][346]^2([789] - 7) - 8[145][346] + 3[346][789] - 5[346][567] \\ & - 4[346]^2 + y_{10}[90\mathrm{A}] - 3[145]^2[346]^2 - 3[145]^2[346] - [346]^3([145]^2 + 2[145]) + [145][789] \\ & - 2[145][567] - [145]^2 + [346]^2([789] - 2[567]) + [567][789] - [567]^2 - [346][567]^2 - [346]^3 \\ & + [47\mathrm{A}]([567] - [789] + 2[346] + [145] + [346]^2) - [680]y_{10} - [680][90\mathrm{A}] \end{aligned}$$

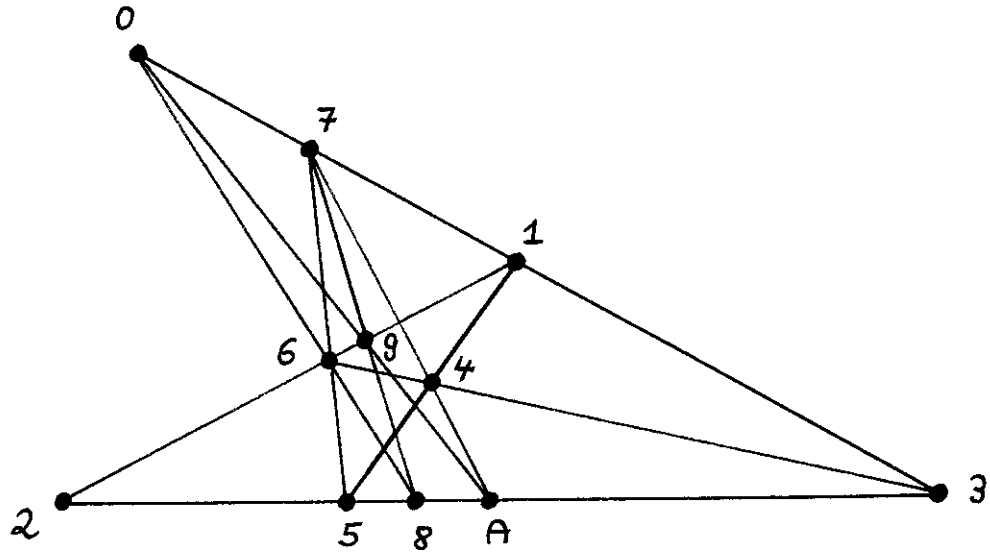


Figure 6. The projective construction of $\sqrt{2}$ ($\mathcal{L}_{\sqrt{2}}$), see also [11, Figure 5.5.3].

Also this identity has been derived with a single Gröbner bases computation as described in Section 6.

On the other hand, the configuration $\mathcal{L}_{\sqrt{2}}$ is realizable over the real numbers $\mathbb{R}$. One such realization is obtained by specializing $y_5 = 1, x_6 = 1, y_7 = -1, y_8 = \sqrt{2}, x_9 = 1/\sqrt{2}$, $y_{10} = -\sqrt{2}$ and $y_{11} = 2$ in the above matrix. This shows that $\mathcal{L}_{\sqrt{2}}$ be coordinatized over a field extension K of $\mathbb{Q}$ if and only if $\sqrt{2}$ is contained in K.

5. Variants of the Nullstellensatz.

In the previous section we have given two non-realizability proofs for configurations by establishing a single polynomial identity in the projective variables. This elegant and compact way of encoding geometry proofs has been introduced (independently) by W. Whiteley as an application of invariant theory to projective geometry [30] and by J. Bokowski to represent non-polytopality proofs for triangulated spheres [2],[3]. It has been proved (independently) by A. Dress and the author that such an identity, called *final polynomial* or *Hilbert polynomial*, exists for every non-realizable configuration, oriented matroid or triangulated sphere. The reader is referred to [23] for details.

We have seen in Section 3 that every polynomial with integer coefficients can be encoded in a suitable configuration. In the following we will therefore consider arbitrary polynomial systems, and only in the end of Section 6 our results will be applied to automatically derive a proof for an incidence theorem. Recall the following classical "duality theorem in polynomial programming".

THEOREM 5.1. (Hilbert's Nullstellensatz, [17, Theorem 3.1]) *Let K be any field, $\overline{K}$ its algebraic closure, and $f_1, \ldots, f_m \in K[x_1, \ldots, x_n]$. Then either there exists an $\mathbf{x} = (x_1, \ldots, x_n) \in \overline{K}^n$ such that $f_1(\mathbf{x}) = \ldots = f_m(\mathbf{x}) = 0$, or there exist $g_1, \ldots, g_m \in K[x_1, \ldots, x_n]$ such that $\sum_{i=1}^m g_i f_i = 1$.*

Assume that the system $f_1(\mathbf{x}) = \ldots = f_m(\mathbf{x}) = 0$ has no solutions. Then Hilbert's Nullstellensatz tells us that the ideal I generated by $\{f_1, \ldots, f_m\}$ contains the unit 1, or, equivalently, I equals $K[\mathbf{x}]$. In the application of computer algebra to computer-aided geometric reasoning one is often interested to have an explicit representation $\sum_{i=1}^m g_i f_i$ of 1 as linear combination of the f_i rather than just the information "$1 \in I$".

Let us be precise and give a slightly more general definition. A *final polynomial* for a finite subset $\{f_1, \ldots, f_m\}$ of $K[\mathbf{x}]$ is a polynomial $p \in K[\mathbf{x}, \mathbf{y}]$, where $\mathbf{y} := (y_1, \ldots, y_m)$, and such that $p(\mathbf{x}, f_1, \ldots, f_m) = 0$ and $p(\mathbf{x}, 0, \ldots, 0) = 1$ in $K[\mathbf{x}]$.

COROLLARY 5.2. *A subset $\{f_1, \ldots, f_m\}$ of polynomials in $K[\mathbf{x}]$ has either a final polynomial or a common zero in $\overline{K}^n$.*

This corollary is a direct consequence of Theorem 5.1 which asserts that if the f_i have no common root, then there exists always a final polynomial of the form $p(\mathbf{x}, \mathbf{y}) = -\sum_{i=1}^m g_i(\mathbf{x}) y_i + 1$.

Most proofs of Hilbert's Nullstellensatz are non-constructive, and hence they do not lead to any a priori upper bound on the size of final polynomials. The constructive proof given by G. Herrmann [13] implies that in Theorem 5.1 one can choose g_i with $\deg(g_i) \leq (2D)^{2^n}$ where D bounds the degrees of the f_i. The following very recent result due to W.D. Brownawell shows that Herrmann's doubly exponential bound can be replaced by a singly exponential bound for the degrees of final polynomials.

THEOREM 5.3. (Brownawell [4]) *Let $f_1, \ldots, f_m \in \mathbb{C}[\mathbf{x}]$ such that $\deg(f_i) \leq D$ for $i = 1, \ldots, n$. Then either there exists an $\mathbf{x} \in \mathbb{C}^n$ such that $f_1(\mathbf{x}) = \ldots = f_m(\mathbf{x}) = 0$, or there exist $g_1, \ldots, g_m \in \mathbb{C}[\mathbf{x}]$ such that $\sum_{i=1}^m g_i f_i = 1$, and such that*

$$\deg(g_i) \quad \leq \quad \mu\, n\, D^{\mu} \; + \; \mu\, D,$$

where $\mu := \min\{m, n\}$.

Brownawell's proof of Theorem 5.3 uses very powerful estimates from several complex variables, and it is substantially more difficult than the usual non-constructive proofs for Theorem 5.1. A comparatively simple family of examples given in [4, Section 1] shows that the bound in Theorem 5.3 is asymptotically optimal.

Let us now come to the case of real closed fields such as the real numbers $\mathbb{R}$. In Section 4 we have proved that the configuration $\mathcal{L}_{\sqrt{-1}}$ is not realizable over $\mathbb{R}$ by establishing a representation of $1 + y_8^2$ as linear combination of polynomials $[ijk]$ which are supposed

to vanish. It is clear that, for any ordered field K, the sum of 1 and some squares in $K[\mathbf{x}]$ cannot be zero. Conversely, it turns out that such a representation necessarily exists whenever a polynomial system has no solution in a real closed field [1],[8].

First versions of this result which is usually referred to as the *real Nullstellensatz* were given by J.L. Krivine (1964), D.W. Dubois (1969) and G. Stengle (1974). For the history and basic concepts of real algebraic geometry and many more references we refer the reader to the survey articles of E. Becker [1] and M.A. Dickmann [8]. In these expositions one finds also several versions of *semi-algebraic Nullstellensätze* which deal with sharp and weak inequalities as well as equations. Here we state only the following basic version of the real Nullstellensatz.

THEOREM 5.4. (Real Nullstellensatz) *Let K be a subfield of the real numbers $\mathbb{R}$, and let $f_1, \ldots, f_m \in K[x_1, \ldots, x_n]$. Then either there exists an $\mathbf{x} \in \mathbb{R}^n$ such that $f_1(\mathbf{x}) = \ldots = f_m(\mathbf{x}) = 0$, or there exist $g_1, \ldots, g_m, h_1, \ldots, h_r \in K[x_1, \ldots, x_n]$ and positive numbers $\alpha_1, \ldots, \alpha_r \in K$ such that $g_1 f_1 + \ldots + g_m f_m + \alpha_1 {h_1}^2 + \ldots + \alpha_r {h_r}^2 = -1$.*

Let us close this section by suggesting a natural but probably very difficult question.

PROBLEM 5.5. *Is there an efficient version of the real Nullstellensatz which gives asymptotically the same estimate as Brownawell's Theorem 5.3 ?*

6. Computation of final polynomials and final syzygies.

In this section we describe an algorithm based on Buchberger's Gröbner bases method for the construction of final polynomials. It turns out that in many cases a final polynomial $p(\mathbf{x}, \mathbf{y})$ can be found which does not depend on $\mathbf{x}$ at all. We call such a polynomial $p(\mathbf{y})$ a *final syzygy*. We shall see that the suggested Gröbner basis computation produces a final syzygy whenever one exists. This situation is characterized by an interesting topological condition.

Let us recall some basic definitions concerning Gröbner bases. For a detailed introduction and many references the reader is referred to [5]. In that survey article Buchberger emphasizes the algorithmic point of view, and several methods for the computation of Gröbner bases are described. Here we shall simplify things substantially by taking the non-constructive algebraic geometry point of view. Our Gröbner bases computations were carried out with an implementation in the computer algebra system MAPLE; similar versions are found in many other systems such as MACSYMA or SCRATCHPAD.

Let K be any infinite field and $K[\mathbf{x}]$ the polynomial ring on n variables $x_1, x_2, \ldots, x_n$. We wish to extend the indexing order on the variables to a total order on the set $\mathcal{P} := \{ x_i^{i_1} x_2^{i_2} \ldots x_n^{i_n} \mid \text{all } i_j \geq 0 \}$ of all power products. Such an extension $<$ to $\mathcal{P}$ is *admissible* if $1 < p$ for all $p \in \mathcal{P}, p \neq 1$, and if for all $p, q, r \in \mathcal{P}$, $p < q$ implies $p \cdot r < q \cdot r$. All results of this section are restricted to the *purely lexicographical order* ($x_1^{i_1} \ldots x_n^{i_n} < x_1^{h_1} \ldots x_n^{h_n}$ if there exists m, $1 \leq m \leq n$, with $i_m < h_m$ and for all $j > m$, $i_j = h_j$).

Let us first assume that $<$ is an arbitrary admissible order. Given $f \in K[\mathbf{x}]$, we define $\mathrm{init}(f)$ to be the greatest (with respect to $<$) power product which has non-zero coefficient in f. For any ideal I in $K[\mathbf{x}]$, the *initial ideal* $\mathrm{Init}(I)$ of I is the monomial ideal generated by the set $\{\mathrm{init}(f) \mid f \in I\}$. A *Gröbner basis* for I is a finite subset $\mathcal{G}$ of I with the property that $\mathrm{Init}(I)$ is generated by $\{\mathrm{init}(g) \mid g \in \mathcal{G}\}$. It follows from Theorem 5.1 that $\mathcal{F}$ has no roots in $\overline{K}^n$ if and only if $\mathcal{G}$ contains a non-zero scalar $u \in K$.

In the following it will be assumed that we have an algorithm which takes as input a finite set $\mathcal{F}$ of polynomials in $K[\mathbf{x}]$ and which computes a Gröbner basis $\mathcal{G}$ for the ideal I generated by $\mathcal{F}$.

Example 6.1. Let $n = 2$ and consider the polynomials

$$f_1 := x_1^2 - x_2^2 - 1\,, \quad f_2 := x_1 + 2x_2\,, \quad f_3 := x_1 + x_2^2 + 5\,, \quad f_4 := x_1 + x_2$$

in $\mathbb{C}[x_1, x_2]$.

(1) Let $\mathcal{F} = \{f_1, f_2\}$. A Gröbner basis for $\mathcal{F}$ with respect to purely lexicographic order is given by $\mathcal{G} = \{x_1 + 2x_2,\, 3x_1^2 - 4\}$.

(2) Let $\mathcal{F} = \{f_1, f_2, f_3\}$. $\mathcal{F}$ has no roots in $\mathbb{C}^2$, and thus a Gröbner basis for $\mathcal{F}$ with respect to purely lexicographic order is given by $\mathcal{G} = \{1\}$.

(3) Let $\mathcal{F} = \{f_1, f_4\}$. $\mathcal{F}$ has no roots in $\mathbb{C}^2$, and thus a Gröbner basis for $\mathcal{F}$ with respect to purely lexicographic order is given by $\mathcal{G} = \{1\}$. How can we find a final polynomial ?

Assume that $\mathcal{F} := \{f_1, \ldots, f_m\} \subset K[\mathbf{x}]$ has no solutions in $\overline{K}^n$. In order to compute a final polynomial for $\mathcal{F}$, we introduce a slack variable y_i for each element of $\mathcal{F}$. Define

$$\widehat{f}_i(\mathbf{x}, \mathbf{y}) \quad := \quad f_i(\mathbf{x}) - y_i \qquad \in \quad K[\mathbf{x}, \mathbf{y}]$$

for all $f_i \in \mathcal{F}$, and let $\widehat{\mathcal{F}} := \{\widehat{f}_1, \ldots, \widehat{f}_m\}$. Applying an appropriate Gröbner basis computation to the new set $\widehat{\mathcal{F}}$ of m polynomials in $m + n$ variables yields the desired results.

THEOREM 6.2. *Let $\mathcal{F}$ be a finite subset of $K[\mathbf{x}]$ which has no zeros in $\overline{K}^n$, and let $\widehat{\mathcal{G}} \subset K[\mathbf{x}, \mathbf{y}]$ be a Gröbner basis with respect to purely lexicographic order induced from $y_1 < \ldots < y_m < x_1 < \ldots < x_n$ for the set $\widehat{\mathcal{F}}$ as defined above. Then $\widehat{\mathcal{G}}$ contains a final polynomial for $\mathcal{F}$.*

The basic idea in the proof of Theorem 6.2 is to take any final polynomial p for $\mathcal{F}$ and to compute its normal form modulo the Gröbner basis $\widehat{\mathcal{G}}$. Since p is contained in the ideal generated by $\widehat{\mathcal{F}}$, this normal form must be zero. On the other hand one can see that a final polynomial cannot reduce to zero modulo a set $\widehat{\mathcal{G}}$ (with respect to the given purely lexicographical order) unless $\widehat{\mathcal{G}}$ contains a final polynomial p'. The details of this argument are straightforward but fairly technical and will be omitted. Let us instead take a second look at two earlier examples.

Example 6.3.

(1) Let $\mathcal{F} = \{f_1, f_4\}$ as in Example 6.1 (3). Then $\widehat{\mathcal{F}} = \{\widehat{f_1}, \widehat{f_4}\} \subset K[x_1, x_2, y_1, y_4]$ where $\widehat{f_1} = x_1^2 - x_2^2 - 1 - y_1$ and $\widehat{f_4} = x_1 + x_2 - y_4$. Consider the purely lexicographical order on the power products in $K[x_1, x_2, y_1, y_4]$ which is induced from the variable order $y_1 < y_4 < x_1 < x_2$. A Gröbner basis for $\widehat{\mathcal{F}}$ with respect to that order is given by

$$\widehat{\mathcal{G}} \quad = \quad \{\, x_1 + x_2 - y_4 \,,\, \underline{1 + y_1 - 2x_1y_4 + y_4^2} \,\}.$$

The polynomial $p(\mathbf{x}, \mathbf{y}) := 1 + y_1 - 2x_1y_4 + y_4^2$ is a final polynomial for $\mathcal{F}$.

(2) Let $\mathcal{F} = \{f_1, f_2, f_3\}$ as in Example 6.1 (2). A corresponding Gröbner basis for $\widehat{\mathcal{F}} = \{\widehat{f_1}, \widehat{f_2}, \widehat{f_3}\} \subset K[x_1, x_2, y_1, y_2, y_3]$ is given by $\widehat{\mathcal{G}} \quad =$

$$\{\, -12x_1y_3 + 4x_1y_1 + 64 + 19y_1 + 7y_2^2 + 73x_1 - 9y_3 + 64y_2 - 6y_2y_1 + 2y_2^3 - 14y_2y_3,$$
$$x_1 + 2x_2 - y_2,\ x_1^2 + x_1 + 4 - y_1 - y_3,\ -16 - y_1 + (2y_2 - 3)x_1 - y_2^2 + 3y_3,\ \underline{y_1^2 + 9y_3^2 +}$$
$$\underline{(6y_3 - 16)y_2 + y_2^4 - 96y_3 + (45 - 10y_3)y_2^2 + (20 - 2y_2^2 - 6y_3 + 14y_2)y_1 + 2y_2^3 + 244}\}.$$

The underlined polynomial is (up to scaling) a final polynomial for $\mathcal{F}$.

The two final polynomials in Example 6.3 are different in the following aspect. The final polynomial in (1) contains slack variables y_j as well as old variables x_i while the one in (2) is a polynomial entirely in the slack variables y_j. In general, we define a *final syzygy* for a subset $\mathcal{F} = \{f_1, \ldots, f_m\}$ of $K[\mathbf{x}]$ to be a polynomial $p \in K[\mathbf{y}]$ such that $p(f_1, \ldots, f_m) = 0$ and $p(0, \ldots, 0) = 1$ in $K[\mathbf{x}]$.

Assume in the following that $K = \mathbb{C}$, the complex numbers. With the set $\mathcal{F}$ we associate the polynomial mapping

$$\mathbf{f} : \mathbb{C}^n \to \mathbb{C}^m, \quad \mathbf{x} \mapsto \big(f_1(\mathbf{x}), \ldots, f_m(\mathbf{x})\big).$$

Denoting the zero vector in $\mathbb{C}^m$ with 0, we have that $\mathcal{F}$ admits a final polynomial if and only if 0 is not contained in the image $\mathrm{Im}(\mathbf{f})$ of $\mathbf{f}$. We have a similar criterion for the existence of final syzygies.

LEMMA 6.4. *$\mathcal{F} \subset \mathbb{C}[\mathbf{x}]$ has a final syzygy if and only if 0 is not contained in $\overline{\mathrm{Im}(\mathbf{f})}$, the Zariski-closure in $\mathbb{C}^m$ of $\mathrm{Im}(\mathbf{f})$.*

Proof. Assume that 0 is contained in $\overline{\mathrm{Im}(\mathbf{f})}$. Then, by definition of the Zariski topology, $p(0) = 0$ for every polynomial $p \in \mathbb{C}[\mathbf{y}]$ which vanishes on $\mathrm{Im}(\mathbf{f})$. $\mathbb{C}$ being an infinite field, p vanishes on $\mathrm{Im}(\mathbf{f})$ if and only if $p(f_1(\mathbf{x}), \ldots, f_m(\mathbf{x})) = 0$ in $\mathbb{C}[\mathbf{x}]$. Hence there is no final syzygy for $\mathcal{F} = \{f_1, \ldots, f_n\}$.

On the other hand, if 0 is not contained in $\overline{\mathrm{Im}(\mathbf{f})}$, then there exists $p \in \mathbb{C}[\mathbf{y}]$ which vanishes on $\mathrm{Im}(\mathbf{f})$ but not at 0. After scaling, p is a final syzygy for $\mathcal{F}$. □

Lemma 6.4 remains valid if $\mathbb{C}$ is replaced by any infinite field. For the special case of the complex numbers, however, one has the following much stronger statement.

THEOREM 6.5. *$\mathcal{F} \subset \mathbb{C}[\mathbf{x}]$ has a final syzygy if and only if 0 is not contained in the closure of $\mathrm{Im}(\mathbf{f})$ with respect to the classical real topology on $\mathbb{C}^m$.*

Proof. By Lemma 6.4, it suffices to show that in the above situation the closure of $\mathrm{Im}(\mathbf{f})$ with respect to the classical real topology is also Zariski-closed in $\mathbb{C}^m$. Our argumentation is based on results given in [21, Chapter 2].

We embed the affine spaces $\mathbb{C}^n$ and $\mathbb{C}^m$ into complex projective spaces $\mathbb{P}^n$ and $\mathbb{P}^m$ respectively, and we consider the induced mapping $\widetilde{\mathbf{f}} : \mathbb{P}^n \to \mathbb{P}^m$. Given a set $A \subset \mathbb{P}^m$, we write $\mathrm{zcl}(A)$ for its Zariski-closure in $\mathbb{P}^m$ and $\mathrm{rcl}(A)$ its closure in the classical real topology on $\mathbb{P}^m$, and similarly for subsets of $\mathbb{P}^n$.

By the *Main Theorem of Elimination Theory* [21, Theorem 2.23], we have that the image of $\widetilde{\mathbf{f}}$ is Zariski-closed in $\mathbb{P}^m$. In other words,

$$\mathrm{zcl}\left(\widetilde{\mathbf{f}}(\mathbb{P}^n)\right) \quad = \quad \mathrm{rcl}\left(\widetilde{\mathbf{f}}(\mathbb{P}^n)\right) \quad = \quad \widetilde{\mathbf{f}}(\mathbb{P}^n).$$

This can be rewritten as

$$\mathrm{zcl}\left(\widetilde{\mathbf{f}}(\,\mathrm{zcl}\,(\mathbb{C}^n))\right) \quad = \quad \mathrm{rcl}\left(\widetilde{\mathbf{f}}(\,\mathrm{rcl}\,(\mathbb{C}^n))\right).$$

Since $\widetilde{\mathbf{f}}$ is a continuous mapping with respect to both topologies, the inner closure operators can be dropped.

$$\mathrm{zcl}\left(\widetilde{\mathbf{f}}(\mathbb{C}^n)\right) \quad = \quad \mathrm{rcl}\left(\widetilde{\mathbf{f}}(\mathbb{C}^n)\right).$$

Finally, we need the fact that both the classical topology and the Zariski topology on $\mathbb{C}^m$ are induced from the respective topologies on $\mathbb{P}^m$ [21, Proposition 2.5]. This shows that $\mathrm{Im}(\mathbf{f})$ has the same closure $\overline{\mathrm{Im}(\mathbf{f})}$ in $\mathbb{C}^m$ relative to both topologies. For, by the above equation we can write

$$\overline{\mathrm{Im}(\mathbf{f})} \quad = \quad \mathrm{zcl}\,(\widetilde{\mathbf{f}}(\mathbb{C}^n)) \cap \mathbb{C}^m \quad = \quad \mathrm{rcl}\,(\widetilde{\mathbf{f}}(\mathbb{C}^n)) \cap \mathbb{C}^m.$$

This completes the proof of Theorem 6.5. □

This result provides a nice topological interpretation for the existence of final syzygies. There exists a final syzygy whenever $\{f_1(\mathbf{x}), \ldots, f_m(\mathbf{x})\}$ has no zeros and it is *stable* with this property. In other words, $\mathcal{F}$ has a final syzygy if and only if

$$\exists\, \epsilon > 0 \text{ such that } \forall\, \delta_1, \ldots, \delta_m \text{ with } |\delta_i| \leq \epsilon : \{\, f_1(\mathbf{x})+\delta_1, \ldots, f_m(\mathbf{x})+\delta_m \,\} \text{ has no zeros.}$$

Moreover, it turns out that the suggested Gröbner basis computation with slack variables yields final syzygies whenever possible. This follows from the well known fact that Gröbner bases with respect to the purely lexicographic order are in triangular form [5]. In other words, generators for the elimination ideals are obtained by computing Gröbner bases with respect to the purely lexicographic order. We have

PROPOSITION 6.6. *Let $\mathcal{F}$ be a finite subset of $K[\mathbf{x}]$ which admits a final syzygy $p \in K[\mathbf{y}]$, and let $\widehat{\mathcal{F}}, \widehat{\mathcal{G}}$ as defined in Theorem 6.2. Then the Gröbner basis $\widehat{\mathcal{G}}$ contains a final syzygy for $\mathcal{F}$.*

Let us remark that the idea underlying Theorem 6.2 can also be used to find non-realizability proofs or final polynomials in the following more general situation. Assume that K is a field which is not algebraically closed. It is, of course, possible (and frequently the case) that $\mathcal{F}$ does have roots in $\overline{K}^n$ but $\mathcal{F}$ fails to have roots in K^n. Then $\mathcal{F}$ has neither a final syzygy nor a final polynomial in the above sense.

Still, one can carry out the Gröbner bases computation suggested in Theorem 6.2. In many cases the Gröbner basis $\widehat{\mathcal{G}}$ will contain a polynomial which shows "obviously" that $\mathcal{F}$ has no roots in K. Moreover, such a final polynomial will provide necessary conditions for field extensions of K to allow roots of $\mathcal{F}$.

The final polynomials for the configurations $\mathcal{L}_{\sqrt{-1}}$ and $\mathcal{L}_{\sqrt{2}}$ in Section 4 were both found by this method. In that situation we had $K = \mathbb{Q}$, and the appearance of the terms $1 + y_8^2$ and $y_{10}^2 - 2$ as summands in the respective final polynomials gave us a characterization of those field extensions of $\mathbb{Q}$ over which the given configurations can be coordinatized.

Let us close this last section with another application to configurations.

EXAMPLE 6.7. *Derivation of a final polynomial proof for Desargues theorem using Gröbner bases.*

Statement of Desargues theorem (see Figure 3)
Let $\mathbf{X}$ be a 3×10 matrix over a field K, and denote the 3×3-subdeterminants of $\mathbf{X}$ by $[ijk]$ where $i, j, k \in \{1, 2, \ldots, 9, 0\}$. If nine of the ten expressions

$$[125],\ [136],\ [148],\ [237],\ [249],\ [340],\ [567],\ [589],\ [680],\ [790]$$

vanish and all $[ijk]$ not contained in this list are non-zero, then also the tenth $[ijk]$ in this list has to vanish.

Final polynomial proof. By projective equivalence it may be assumed that

$$\mathbf{X} \quad = \quad \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \\ x_1 & 1 & 0 & x_5 & 1 & x_6 & x_7 & x_8 & x_9 & 0 \\ z_1 & 1 & 0 & z_5 & 0 & z_6 & z_7 & z_8 & z_9 & 1 \end{pmatrix}$$

It is easily verified (at least with MAPLE) that the expression

$$\begin{aligned} &(z_9x_8 - x_9x_8 - z_9[680] - [589][680] + x_9[340] + [589]x_8 - [340] + [680])[125] \\ &+ (1 - z_9 - [589])[136] + (x_9 - 1)[148] + (z_9 + [589] - 1)x_1[237] + (x_1 - x_8)[249] \\ &+ (z_9 - x_9[589] - x_9z_9 - x_1z_9 + x_1 + x_8z_9 - 1 + [589] + x_9 - x_8)[340] + (1 - z_9)[680] \\ &+ (x_1 - [589]x_1 - z_9x_1)[567] + (x_1[790] - x_1 + x_8 - [680])[589] + (z_9x_1 - x_1)[790] \end{aligned}$$

is zero in the ring $K[x_1, z_1, \ldots, x_9, z_9]$. This proves Desargues' theorem (in the above version). □

Derivation of the final polynomial. Let

$$\begin{aligned}\widehat{\mathcal{F}} = \{ & -1 + z_1 - [125],\ x_5 z_8 - z_5 x_8 - x_1 z_8 + z_1 x_8 + x_1 z_5 - z_1 x_5 - [148], \\ & x_5 z_9 - z_5 x_9 - z_9 + x_9 + z_5 - x_5 - [249],\ x_5 - [340],\ -z_7 + z_6 - [567],\ -z_9 + z_8 - [589], \\ & -x_1 z_6 + z_1 x_6 - [136],\ x_8 - x_6 - [680],\ x_9 - x_7 - [790],\ -z_7 + x_7 - [237] \},\end{aligned}$$

where the $[ijk]$ are now thought of as slack variables. The above polynomial is contained in the Gröbner basis $\widehat{\mathcal{G}}$ for $\widehat{\mathcal{F}}$ with respect to purely lexicographic order induced from ordering the 22 variables as follows

$$x_1 > z_1 > x_5 > \ldots > x_9 > z_9 > [125] > [136] > \ldots > [680] > [790].$$

This Gröbner basis computation can be carried out in few seconds with the presently available implementations.

REFERENCES

[1] E. Becker, *On the real spectrum of a ring and its applications to semialgebraic geometry*, Bull. Amer. Math. Soc. 15 (1986) 19-60.

[2] J. Bokowski, J. Richter and B. Sturmfels, *Nonrealizability proofs in computational geometry*, TH Darmstadt, Preprint # 1045, April 1987.

[3] J. Bokowski and B. Sturmfels, *Polytopal and non-polytopal spheres. An algorithmic approach*, Israel J. Math. 57 (1987) 257–271.

[4] W.D. Brownawell, *Bounds for the degree in the Nullstellensatz*, Annals of Math. 126 (1987) 577-591.

[5] B. Buchberger, *Gröbner bases – an algorithmic method in polynomial ideal theory*, Chapter 6 in N.K. Bose (ed.) : "Multidimensional Systems Theory", D. Reidel Publ. Comp., 1985.

[6] J.F. Canny, *The Complexity of Robot Motion Planning*, Ph.D. Dissertation, Massachussetts Institute of Technology, 1987.

[7] G. Collins, *Quantifier Elimination for Real Closed Fields by Cyclindrical Algebraic Decomposition*, Proc. 2nd GI Conf. on Automata and Formal Languages, Lect. Notes in Comp. Sci., Springer Verlag 33 (1975) 134–163.

[8] M.A. Dickmann, *Applications of model theory to real algebraic geometry*, in "Methods in Mathematical Logic", Springer Lect. Notes Math. 1130 (1983) 77–150.

[9] P. Dembrowski, *Finite Geometries*, Springer, New York, 1968.

[10] D.Y. Grigor'ev and N.N. Vorobjov, *Solving systems of polynomial inequalities in subexponential time*, J. Symbolic Computation, special issue on decision algorithms for the theory of real closed fields, to appear (1987).

[11] B. Grünbaum, *Convex Polytopes*, Interscience, London, 1967.

[12] T. Havel, *The use of distances as coordinates in computer-aided proofs of theorems in Euclidean geometry*, in this volume.

[13] G. Herrmann, *Die Frage der endlich vielen Schritte in der Theorie der Polynomideale*, Math. Ann. 95 (1926) 736–788.

[14] D. HILBERT AND S. COHN-VOSSEN, *Geometry and the Imagination*, (English Edition), Chelsea, New York, 1983.

[15] D. KAPUR, *A Refutational Approach to Geometry Theorem Proving*, Proceedings of the International Workshop on Geometry, Oxford, England, 1986.

[16] V. KLEE AND S. WAGON, *Unsolved Problems in Mathematics*, in preparation.

[17] E. KUNZ, *Introduction to Commutative Algebra and Algebraic Geometry*, Birkhäuser, Boston, 1985.

[18] R. LAUFFER, *Die nichtkonstruierbare Konfiguration* (10_3), Math. Nachrichten 11 (1954) 303–304.

[19] S. MACLANE, *Some interpretations of abstract linear dependence in terms of projective geometry*, Amer. J. Math. 58 (1936) 236–240.

[20] B. MAZUR, *Arithmetic on curves*, Bull. Amer. Math. Soc. 14 (1986) 207–259.

[21] D. MUMFORD, *Algebraic Geometry I : Complex Projective Varieties*, Springer. Berlin, 1976.

[22] A. SAAM, *Ein neuer Schließungssatz für projektive Ebenen*, Journal of Geometry 29 (1987) 36–42.

[23] B. STURMFELS, *Computational Synthetic Geometry*, Ph.D. Dissertation, University of Washington, Seattle, 1987.

[24] B. STURMFELS, *On the decidability of diophantine problems in combinatorial geometry*, Bull. Amer. Math. Soc. 17 (1987) 121–124.

[25] B. STURMFELS, *Applications of final polynomials and final syzygies*, I.M.A. Preprint # 372, University of Minnesota, December 1987.

[26] A. TARSKI, *A Decision Method for Elementary Algebra and Geometry*, 2nd revised ed., Univ. of California Press, 1951.

[27] N. WHITE (ED.), *Combinatorial Geometries*, Cambridge Univ. Press (1987).

[28] N. WHITE, *The transcendence degree of a coordinatization of a combinatorial geometry*, Journ. Comb. Th. B 29 (1980) 168–175.

[29] N. WHITE AND T. MCMILLAN, *Cayley factorization*, I.M.A. Preprint # 371, University of Minnesota, December 1987.

[30] W. WHITELEY, *Logic and Invariant Theory*, Ph.D. dissertation, Harvard University, 1971.