## Modelling in Geometry

In this chapter we present an example of an algebraic modeling of logical statements derived from geometrical problems. More precisely, we show how geometrical problems can be translated to systems of polynomial equations, and how the truth or falsity of the original statement corresponds to solvability of the resulting system of equations. Finally, we present an algorithm that can decide the solvability of systems of algebraic equations.

### 1.1 An Introductory Example

Consider the very simple geometrical configuration illustrated in Figure 1.1:

- Given two points $A$ and $C$ and the line passing through $A$ and $C$.
- Given a point $B$ such that the line $A B$ is perpendicular to the line $A C$.
- Given a point $D$ such that the line $C D$ is perpendicular to the line $A C$.

Then

- the lines $A B$ and $C D$ must be parallel.


Figure 1.1: Parallel lines
The logical statement describing the geometric situation is

$$
\begin{equation*}
\underset{A, B, C, D}{\forall}((\operatorname{perpendicular}(A, B, A, C) \wedge \operatorname{perpendicular}(C, A, C, D)) \Rightarrow \operatorname{parallel}(A, B, C, D)) \tag{1.1}
\end{equation*}
$$

with appropriate predicates 'perpendicular' and 'parallel'.

### 1.2 Modelling Geometry in Algebra

The first step in modelling geometry is to introduce a coordinate system. Using coordinates we will then be able to describe properties such as 'perpendicular' and 'parallel' by polynomial equalities and inequalities. Continuing the example from above, let

$$
A=(0,0) \quad B=\left(b_{1}, b_{2}\right) \quad C=\left(c_{1}, c_{2}\right) \quad D=\left(d_{1}, d_{2}\right)
$$

### 1.2.1 First Approach

Using the coordinates as described above,

$$
\begin{align*}
& \operatorname{perpendicular}(A, B, A, C) \text { means }\binom{b_{1}}{b_{2}} \cdot\binom{c 1}{c_{2}}=b_{1} c_{1}+b_{2} c_{2}=0  \tag{1.2}\\
& \text { perpendicular }(C, A, C, D) \text { means }\binom{c_{1}}{c_{2}} \cdot\binom{d_{1}-c_{1}}{d_{2}-c_{2}}=c_{1}\left(d_{1}-c_{1}\right)+c_{2}\left(d_{2}-c_{2}\right)=0  \tag{1.3}\\
& \operatorname{parallel}(A, B, C, D) \text { means } \quad\binom{b_{2}}{-b_{1}} \cdot\binom{d_{1}-c_{1}}{d_{2}-c_{2}}=b_{2}\left(d_{1}-c_{1}\right)-b_{1}\left(d_{2}-c_{2}\right)=0 \tag{1.4}
\end{align*}
$$

For short we write the equalities in (1.2), (1.3), and (1.4) as $p_{1}=0, p_{2}=0$, and $p_{3}=0$, respectively. Essentially, formula (1.1) is now

$$
\underset{b_{1}, b_{2}, c_{1}, c_{2}, d_{1}, d_{2}}{\forall}\left(p_{1}=0 \wedge p_{2}=0 \Rightarrow p_{3}=0\right),
$$

which is by de'Morgan's rule equivalent to

$$
\begin{equation*}
\neg_{b_{1}, b_{2}, c_{1}, c_{2}, d_{1}, d_{2}}^{\exists} p_{1}=0 \wedge p_{2}=0 \wedge p_{3} \neq 0 . \tag{1.5}
\end{equation*}
$$

Now the trick: the inequality $p_{3} \neq 0$ is equivalent to $\underset{\alpha_{0}}{\exists} \alpha_{0} p_{3}-1=0$, hence, (1.5) is equivalent to

$$
\begin{equation*}
\neg_{b_{1}, b_{2}, c_{1}, c_{2}, d_{1}, d_{2}}^{\exists \exists} p_{1}=0 \wedge p_{2}=0 \wedge \underset{\alpha_{0}}{\exists} \alpha_{0} p_{3}-1=0, \tag{1.6}
\end{equation*}
$$

and, under the assumption that $\alpha_{0}$ is a variable different from all previously used variables, we finally arrive at

$$
\begin{equation*}
\neg_{b_{1}, b_{2}, c_{1}, c_{2}, d_{1}, d_{2}, \alpha_{0}}^{\exists} p_{1}=0 \wedge p_{2}=0 \wedge \alpha_{0} p_{3}-1=0 . \tag{1.7}
\end{equation*}
$$

It is easy to see, that (1.7) just expresses that there is no solution for the system of equations

$$
\begin{equation*}
p_{1}=0 \quad p_{2}=0 \quad \alpha_{0} p_{3}-1=0, \tag{1.8}
\end{equation*}
$$

substituting back the original expressions for $p_{1}, p_{2}$, and $p_{3}$ we have a system of polynomial (algebraic) equations

$$
\begin{aligned}
b_{1} c_{1}+b_{2} c_{2} & =0 \\
c_{1} d_{1}-c_{1}^{2}+c_{2} d_{2}-c_{2}^{2} & =0 \\
\alpha_{0} b_{2} d_{1}-\alpha_{0} b_{2} c_{1}-\alpha_{0} b_{1} d_{2}+\alpha_{0} b_{1} c_{2}-1 & =0 .
\end{aligned}
$$

Solving this system (e.g. with Mathematica) gives us solutions, e.g.

$$
\begin{equation*}
c_{1}=0 \quad c_{2}=0 \quad b_{1}=0 \quad b_{2}=1 \quad d_{1}=1 \quad d_{2}=0 \quad \alpha_{0}=1, \tag{1.9}
\end{equation*}
$$

which means that this does not constitute a proof of the original statement (1.1). In fact, the statement is not true, because the solution of the system of equations gives a counterexample. If we take $A=C, B=(0,1)$, and $D=(1,0)$, then the 'line passing through $A$ and $C$ ' degenerates to a point such that the hypotheses 'perpendicular $(A, B, A, C)$ ' and 'perpendicular $(C, A, C, D)$ ' trivially become true whereas the conclusion 'parallel $(A, B, C, D)$ ' is false because $A B$ and $C D$ are perpendicular (and not parallel).

### 1.2.2 Improved Approach

Obviously, something must have gone wrong in the previous section, because the statement under investigation is true. The system of equations derived in the previous section, whose solvability should be equivalent to the statement that we want to prove, however, was an inaccurate model, because it allowed the 'wrong solution' (1.9). Note, however, that clearly $C$ should be different from $A$ when we talk about 'the line passing through $A$ and $C^{\prime}$, but our model did not contain any hypothesis expressing $C \neq A$. Strictly speaking, (1.9) is of course a correct solution of the system of equations (check by substitution!), but the equations are a wrong model for the original proof problem.

Using coordinates $C \neq A$ means $c_{1} \neq 0 \vee c_{2} \neq 0$. Applying the trick like in (1.6) again, this is equivalent to

$$
\underset{\alpha_{1}}{\exists} \alpha_{1} c_{1}-1=0 \vee \underset{\alpha_{2}}{\exists} \alpha_{2} c_{2}-1=0
$$

which is equivalent to

$$
\underset{\alpha_{1}, \alpha_{2}}{\exists} q_{1}=0 \quad \text { with } \quad q_{1}=\left(\alpha_{1} c_{1}-1\right)\left(\alpha_{2} c_{2}-1\right) .
$$

In other words, (1.1) is equivalent to the unsolvability of

$$
\begin{aligned}
b_{1} c_{1}+b_{2} c_{2} & =0 \\
c_{1} d_{1}-c_{1}^{2}+c_{2} d_{2}-c_{2}^{2} & =0 \\
\left(\alpha_{1} c_{1}-1\right)\left(\alpha_{2} c_{2}-1\right) & =0 \\
\alpha_{0} b_{2} d_{1}-\alpha_{0} b_{2} c_{1}-\alpha_{0} b_{1} d_{2}+\alpha_{0} b_{1} c_{2}-1 & =0
\end{aligned}
$$

If we pass this system of equations to Mathematica, it will in fact tell us that there is no solution, so the original statement (1.1) is proved.

### 1.2.3 The General Model

Let us assume we have a geometrical configuration described by

$$
p_{1}=0 \quad \ldots \quad p_{n}=0 \quad q_{1} \neq 0 \quad \ldots \quad q_{m} \neq 0
$$

and a conclusion described by

$$
c=0
$$

where $p_{i}, q_{j}, c \in \mathbb{Q}\left[x_{1}, \ldots, x_{l}\right]$ for $1 \leq i \leq n$ and $1 \leq j \leq m$. Then

$$
\underset{x_{1}, \ldots, x_{l}}{\forall}\left(p_{1}=0 \wedge \ldots \wedge p_{n}=0 \wedge q_{1} \neq 0 \wedge \ldots \wedge q_{m} \neq 0 \Rightarrow c=0\right)
$$

is equivalent to

$$
\neg_{x_{1}, \ldots, x_{l}}^{\exists} \neg\left(p_{1}=0 \wedge \ldots \wedge p_{n}=0 \wedge q_{1} \neq 0 \wedge \ldots \wedge q_{m} \neq 0 \Rightarrow c=0\right),
$$

which is in turn equivalent to

$$
\neg_{x_{1}, \ldots, x_{l}}^{\exists} p_{1}=0 \wedge \ldots \wedge p_{n}=0 \wedge q_{1} \neq 0 \wedge \ldots \wedge q_{m} \neq 0 \wedge c \neq 0
$$

The inequalities can then be turned into equalities by the so-called Rabinovich-Trick

$$
\neg_{x_{1}, \ldots, x_{l}}^{\exists} p_{1}=0 \wedge \ldots \wedge p_{n}=0 \wedge \underset{\alpha_{1}}{\exists} \alpha_{1} q_{1}-1=0 \wedge \ldots \wedge \underset{\alpha_{m}}{\exists} \alpha_{m} q_{m}-1=0 \wedge \underset{\alpha_{0}}{\exists} \alpha_{0} c-1=0
$$

and since we assume that $\alpha_{0}, \alpha_{1}, \ldots, \alpha_{m}$ are new variables distinct from $x_{1}, \ldots, x_{n}$ this is equivalent to

$$
\neg_{x_{1}, \ldots, x_{l}, \alpha_{0}, \alpha_{1}, \ldots, \alpha_{m}}^{\exists} p_{1}=0 \wedge \ldots \wedge p_{n}=0 \wedge \alpha_{1} q_{1}-1=0 \wedge \ldots \wedge \alpha_{m} q_{m}-1=0 \wedge \alpha_{0} c-1=0 .
$$

This is nothing else than saying that the system of polynomial equations in the variables $x_{1}, \ldots, x_{l}, \alpha_{0}, \alpha_{1}, \ldots, \alpha_{m}$

$$
\begin{gathered}
p_{1}=0 \\
\vdots \\
p_{n}=0 \\
\alpha_{1} q_{1}-1=0 \\
\vdots \\
\alpha_{m} q_{m}-1=0 \\
\alpha_{0} c-1=0
\end{gathered}
$$

has no solutions for $x_{1}, \ldots, x_{l}, \alpha_{0}, \alpha_{1}, \ldots, \alpha_{m}$.

## Example 1.1: Theorem of Thales

Let $A$ and $B$ be two points and $M$ the midpoint between $A$ and $B$. Let $c$ be the circle with center $M$ through $A$ and $B$, and let $C$ be any point on $c$. Then $A C$ and $B C$ are perpendicular.

We introduce coordinates and fix $M=(0,0)$. We have $A=\left(a_{1}, a_{2}\right), B=\left(b_{1}, b_{2}\right)$, and $C=\left(c_{1}, c_{2}\right)$. Since $M$ is the midpoint between $A$ and $B$, we have

$$
a_{1}+b_{1}=0 \quad a_{2}+b_{2}=0
$$

and since $C$ and $A$ are on a circle, their distance to the center $M$ must be equal, i.e.

$$
a_{1}^{2}+a_{2}^{2}-c_{1}^{2}-c_{2}^{2}=0
$$

$A C$ and $B C$ are perpendicular can be formulated as

$$
\left(c_{1}-a_{1}\right)\left(c_{1}-b_{1}\right)+\left(c_{2}-a_{2}\right)\left(c_{2}-b_{2}\right)=0 .
$$

Using the model from above with $n=3, m=0$, and $l=6$ we have the following system of equations in the variables $a_{1}, a_{2}, b_{1}, b_{2}, c_{1}, c_{2}$ :

$$
\begin{aligned}
a_{1}^{2}+a_{2}^{2}-c_{1}^{2}-c_{2}^{2} & =0 \\
a_{1}+b_{1} & =0 \\
a_{2}+b_{2} & =0 \\
\alpha_{0}\left(\left(c_{1}-a_{1}\right)\left(c_{1}-b_{1}\right)+\left(c_{2}-a_{2}\right)\left(c_{2}-b_{2}\right)\right)-1 & =0
\end{aligned}
$$

In this example it is easy to convince oneself that this system has no solution, because equations 2 and 3 mean

$$
a_{1}=-b_{1} \quad a_{2}=-b_{2},
$$

and substituting in equation 4 yields

$$
\begin{equation*}
\alpha_{0}\left(c_{1}^{2}-a_{1}^{2}+c_{2}^{2}-a_{2}^{2}\right)-1=0 . \tag{1.10}
\end{equation*}
$$

From equation 1 we get $a_{1}^{2}+a_{2}^{2}=c_{1}^{2}+c_{2}^{2}$, which turns (1.10) into

$$
\alpha_{0} \cdot 0-1=0, \quad \text { i.e. } \quad-1=0,
$$

hence, the above system of polynomial equations has no solutions.

### 1.2.4 Deciding Solvability of a System of Polynomial Equations

In general, it is not as easy as in Example 1.1 to decide, whether a system of polynomial equations has a solution or not. The theory of Gröbner bases plays a key role in this field, but we will not go into much detail.

Given a set of polynomials $G$, a Gröbner basis of $G$ is a set of polynomials $B$, such that

$$
\underset{g \in G}{\forall} g=0 \Leftrightarrow \underset{b \in B}{\forall} b=0,
$$

i.e. the zero set of $G$ equals the zero set of $B$, and $B$ has some special properties that make the system $\underset{b \in B}{\forall} b=0$ 'easier to solve' than the original system $\underset{g \in G}{\forall} g=0$. In many respects, a Gröbner basis of $G$ is the polynomial analogy to the triangular form of a matrix representing a system of linear equations. Fortunately ${ }^{1}$, there is an algorithm that computes a Gröbner basis for any given set of polynomials $G$. Similar to Gaussian elimination, the Gröbner basis algorithm subsequently eliminates variables by a process called polynomial reduction, which is a generalization of the univariate polynomial division to multivariate polynomials. Every computer algebra system (like Mathematica, Maple, or Sage) offers a command to compute Gröbner bases, in Mathematica this command is called GroebnerBasis.

[^0]
## THEOREM 1.2

A system of polynomial equations

$$
g_{1}=0, \quad \ldots \quad, g_{n}=0
$$

has no solutions over $\mathbb{C}$ if and only if the Gröbner basis of $\left\{g_{1}, \ldots, g_{n}\right\}$ contains a constant polynomial unequal to 0 .

## Example 1.3: Thales with Gröbner Basis

Using Mathematica, we compute

$$
\begin{aligned}
& \text { GroebnerBasis }\left[\left\{a_{1}^{2}+a_{2}^{2}-c_{1}^{2}-c_{2}^{2}, a_{1}+b_{1}, a_{2}+b_{2}\right.\right. \\
& \left.\left.\qquad \alpha_{0}\left(\left(c_{1}-a_{1}\right)\left(c_{1}-b_{1}\right)+\left(c_{2}-a_{2}\right)\left(c_{2}-b_{2}\right)\right)-1\right\},\left\{a_{1}, a_{2}, b_{1}, b_{2}, c_{1}, c_{2}, \alpha_{0}\right\}\right]
\end{aligned}
$$

and the answer is $\{1\}$, thus, the Gröbner basis contains the constant polynomial 1 and the system of equations corresponding to the Theorem of Thales is unsolvable, therefore the theorem is proven.

### 1.2.5 Describing Frequently Used Geometrical Properties by Polynomials

In this section we assume some coordinate system and four points

## THEOREM 1.4

Let

$$
X_{1}=\binom{x_{1}}{y_{1}} \quad X_{2}=\binom{x_{2}}{y_{2}} \quad X_{3}=\binom{x_{3}}{y_{3}} \quad X_{4}=\binom{x_{4}}{y_{4}}
$$

1. $X_{1}, X_{2}$, and $X_{3}$ are collinear if and only if

$$
\operatorname{det}\left(\left(\begin{array}{ccc}
1 & x_{1} & y_{1} \\
1 & x_{2} & y_{2} \\
1 & x_{3} & y_{3}
\end{array}\right)\right)=0
$$

2. $X_{1}, X_{2}, X_{3}$, and $X_{4}$ are collinear if and only if

$$
\operatorname{det}\left(\left(\begin{array}{cccc}
1 & x_{1} & y_{1} & x_{1}^{2}+y_{1}^{2} \\
1 & x_{2} & y_{2} & x_{2}^{2}+y_{2}^{2} \\
1 & x_{3} & y_{3} & x_{3}^{2}+y_{3}^{2} \\
1 & x_{4} & y_{4} & x_{4}^{2}+y_{4}^{2}
\end{array}\right)\right)=0
$$

3. $X_{1} X_{2}$ and $X_{3} X_{4}$ are perpendicular if and only if

$$
\left(x_{2}-x_{1}\right)\left(x_{4}-x_{3}\right)+\left(y_{2}-y_{1}\right)\left(y_{4}-y_{3}\right)=0 .
$$

## 4. $X_{1} X_{2}$ and $X_{3} X_{4}$ are parallel if and only if

$$
\left(y_{2}-y_{1}\right)\left(x_{4}-x_{3}\right)-\left(x_{2}-x_{1}\right)\left(y_{4}-y_{3}\right)=0 .
$$

## Example 1.5: Theorem of Pappus

Given one set of collinear points $R, S$, and $T$, and another set of collinear points $U, V$, and $W$, then the intersection points $X, Y$, and $Z$ of line pairs $R V$ and $S U, R W$ and $T U$, $S W$ and TV are collinear, see Figure 1.2. We introduce coordinates:

$$
\begin{array}{llr}
R=\binom{r_{1}}{r_{2}} & S=\binom{s_{1}}{s_{2}} & T=\binom{t_{1}}{t_{2}} \\
U=\binom{u_{1}}{u_{2}} & V=\binom{v_{1}}{v_{2}} & W=\binom{w_{1}}{w_{2}} \\
X=\binom{x_{1}}{x_{2}} & Y=\binom{y_{1}}{y_{2}} & Z=\binom{z_{1}}{z_{2}} .
\end{array}
$$

That point $X$ is the intersection of $R V$ and $S U$ means that both $R, V$, and $X$ as well as $S, U$, and $X$ are collinear, and by Theorem 1.4 this can be described by

$$
\begin{aligned}
& \operatorname{det}\left(\left(\begin{array}{ccc}
1 & r_{1} & r_{2} \\
1 & v_{1} & v_{2} \\
1 & x_{1} & x_{2}
\end{array}\right)\right)=-r_{2} v_{1}+r_{1} v_{2}+r_{2} x_{1}-r_{1} x_{2}-v_{2} x_{1}+v_{1} x_{2}=0 \\
& \operatorname{det}\left(\left(\begin{array}{ccc}
1 & s_{1} & s_{2} \\
1 & u_{1} & u_{2} \\
1 & x_{1} & x_{2}
\end{array}\right)\right)=-s_{2} u_{1}+s_{1} u_{2}+s_{2} x_{1}-s_{1} x_{2}+u_{1} x_{2}-u_{2} x_{1}=0
\end{aligned}
$$

Applying the same technique for the remaining hypotheses and the conclusion of the theorem we arrive at a model $^{2}$ with $n=8, m=2$, and $l=18$

$$
\begin{aligned}
-r_{2} v_{1}+r_{1} v_{2}+r_{2} x_{1}-r_{1} x_{2}+v_{1} x_{2}-v_{2} x_{1} & =0 \\
-s_{2} u_{1}+s_{1} u_{2}+s_{2} x_{1}-s_{1} x_{2}+u_{1} x_{2}-u_{2} x_{1} & =0 \\
-r_{2} w_{1}+r_{1} w_{2}+r_{2} y_{1}-r_{1} y_{2}+w_{1} y_{2}-w_{2} y_{1} & =0 \\
-t_{2} u_{1}+t_{1} u_{2}+t_{2} y_{1}-t_{1} y_{2}+u_{1} y_{2}-u_{2} y_{1} & =0 \\
-s_{2} w_{1}+s_{1} w_{2}+s_{2} z_{1}-s_{1} z_{2}+w_{1} z_{2}-w_{2} z_{1} & =0 \\
-t_{2} v_{1}+t_{1} v_{2}+t_{2} z_{1}-t_{1} z_{2}+v_{1} z_{2}-v_{2} z_{1} & =0 \\
-r_{2} s_{1}+r_{1} s_{2}+r_{2} t_{1}-r_{1} t_{2}+s_{1} t_{2}-s_{2} t_{1} & =0 \\
-u_{2} v_{1}+u_{1} v_{2}+u_{2} w_{1}-u_{1} w_{2}+v_{1} w_{2}-v_{2} w_{1} & =0 \\
\alpha_{1}\left(-r_{2} s_{1}+r_{1} s_{2}+r_{2} u_{1}-r_{1} u_{2}+s_{1} u_{2}-s_{2} u_{1}\right)-1 & =0 \\
\alpha_{2}\left(-r_{2} s_{1}+r_{1} s_{2}+r_{2} v_{1}-r_{1} v_{2}+s_{1} v_{2}-s_{2} v_{1}\right)-1 & =0 \\
\alpha_{0}\left(-x_{2} y_{1}+x_{1} y_{2}+x_{2} z_{1}-x_{1} z_{2}+y_{1} z_{2}-y_{2} z_{1}\right)-1 & =0
\end{aligned}
$$

The Gröbner basis of the set of left-hand sides of these equations is in fact $\{1\}$, hence, the Theorem of Pappus is proved.

[^1]

Figure 1.2: Theorem of Pappus

### 1.3 A Generalization Beyond Geometry

Statements derived from geometrical theorems usually have the form of universally quantified implications. We will now see that not only these can be translated into systems of polynomial equations. The same technique as shown in the previous section can be applied to arbitrary universally quantified boolean combinations of polynomial equalities ${ }^{3}$. We want to prove

$$
\begin{equation*}
\underset{x_{1}, \ldots, x_{l}}{\forall} \Phi, \tag{1.11}
\end{equation*}
$$

where $\Phi$ is a boolean combination of polynomial equations with polynomials in $\mathbb{Q}\left[x_{1}, \ldots, x_{l}\right]$. First we rewrite the statement as

$$
\neg_{x_{1}, \ldots, x_{l}}^{\exists} \neg \Phi,
$$

and then we convert $\neg \Phi$ into conjunctive normal form, thus, (1.11) can be written as

$$
\begin{equation*}
\neg_{x_{1}, \ldots, x_{l}}^{\exists}\left(\Phi_{1,1} \vee \ldots \vee \Phi_{1, j_{1}}\right) \wedge \ldots \wedge\left(\Phi_{n, 1} \vee \ldots \vee \Phi_{n, j_{n}}\right), \tag{1.12}
\end{equation*}
$$

where each $\Phi_{i, j}$ has the form either $P_{i, j}=0$ or $\neg\left(P_{i, j}=0\right)$. Now we introduce new polynomials

$$
Q_{i, j}:= \begin{cases}P_{i, j} & \text { if } \Phi_{i, j} \text { has the form } P_{i, j}=0 \\ \alpha_{i, j} P_{i, j}-1 & \text { if } \Phi_{i, j} \text { has the form } \neg\left(P_{i, j}=0\right)\end{cases}
$$

with new variables $\alpha_{i, j}$. Note that the $\alpha_{i, j}$ can be thought of as existentially quantified in $Q_{i, j}=0$, compare to the Rabinovich-Trick explained in the previous section. Since the $\alpha_{i, j}$

[^2]are all new and distinct from $x_{1}, \ldots, x_{l}$ the existential quantifiers can be pushed outside such that (1.12) can be written as
$$
\neg_{x_{1}, \ldots, x_{l},\left\{\alpha_{i, j}\right\}}\left(Q_{1,1}=0 \vee \ldots \vee Q_{1, j_{1}}=0\right) \wedge \ldots \wedge\left(Q_{n, 1}=0 \vee \ldots \vee Q_{n, j_{n}}=0\right) .
$$

The $\left\{\alpha_{i, j}\right\}$ in the existential quantifier should indicate that we quantify over all $\alpha_{i, j}$ that occur in the $Q_{i, j}$. Now remember that a product is zero if and only if one of the factors is zero ${ }^{4}$, in other words

$$
Q_{i, 1}=0 \vee \ldots \vee Q_{i, j_{i}}=0 \quad \text { if and only if } \quad Q_{i, 1} \cdot \ldots \cdot Q_{i, j_{i}}=0
$$

thus, finally

$$
\neg_{x_{1}, \ldots, x_{l},\left\{\alpha_{i, j}\right\}}^{\exists}\left(Q_{1,1} \cdot \ldots \cdot Q_{1, j_{1}}=0\right) \wedge \ldots \wedge\left(Q_{n, 1} \cdot \ldots \cdot Q_{n, j_{n}}=0\right) .
$$

Hence, the original statement (1.11) is equivalent to the unsolvability of the system of polynomial equations

$$
\begin{array}{ccc}
Q_{1,1} \cdot \ldots \cdot Q_{1, j_{1}} & =0 \\
\vdots & \vdots & \vdots \\
Q_{n, 1} \cdot \ldots \cdot Q_{n, j_{n}} & =0
\end{array}
$$

which can be decided by computing

$$
B=\operatorname{GroebnerBasis}\left[\left\{Q_{1,1} \cdot \ldots \cdot Q_{1, j_{1}}, \ldots, Q_{n, 1} \cdot \ldots \cdot Q_{n, j_{n}}\right\}\right]
$$

and checking, whether $B$ contains a constant polynomial unequal to 0 .

## EXAMPLE 1.6

We come back to our introductory example (1.1). It is easy to see that this statement can be generalized: if we have two perpendicular lines, then being parallel to one of them is obviously the same as being perpendicular to the other. To make a theorem out of that we need two side-conditions, which guarantee that the given lines will not degenerate to points, in other words,

$$
\begin{aligned}
& \underset{A, B, C, D}{\forall} A \neq C \wedge A \neq B \wedge \operatorname{perpendicular}(A, B, A, C) \Rightarrow \\
& \quad \quad \operatorname{perpendicular}(C, A, C, D) \Leftrightarrow \operatorname{parallel}(A, B, C, D)
\end{aligned}
$$

After introducing coordinates

$$
A=(0,0) \quad B=\left(b_{1}, b_{2}\right) \quad C=\left(c_{1}, c_{2}\right) \quad D=\left(d_{1}, d_{2}\right)
$$

the conjunctive normal form of the negated expression inside the quantifier gives

$$
\begin{gathered}
\quad\left(b_{1} \neq 0 \vee b_{2} \neq 0\right) \wedge\left(c_{1} \neq 0 \vee c_{2} \neq 0\right) \wedge \\
\wedge(\neg \operatorname{parallel}(A, B, C, D) \vee \neg \operatorname{perpendicular}(C, A, C, D)) \wedge \\
\wedge(\operatorname{parallel}(A, B, C, D) \vee \operatorname{perpendicular}(C, A, C, D)) \wedge \\
\wedge \operatorname{perpendicular}(A, B, A, C)
\end{gathered}
$$

[^3]Using Theorem 1.4 we get the following combination of equations an inequations

$$
\begin{gathered}
\left(b_{1} \neq 0 \vee b_{2} \neq 0\right) \wedge\left(c_{1} \neq 0 \vee c_{2} \neq 0\right) \wedge \\
\wedge\left(b_{2}\left(d_{1}-c_{1}\right)-b_{1}\left(d_{2}-c_{2}\right) \neq 0 \vee-c_{1}\left(d_{1}-c_{1}\right)-c_{2}\left(d_{2}-c_{2}\right) \neq 0\right) \wedge \\
\wedge\left(b_{2}\left(d_{1}-c_{1}\right)-b_{1}\left(d_{2}-c_{2}\right)=0 \vee-c_{1}\left(d_{1}-c_{1}\right)-c_{2}\left(d_{2}-c_{2}\right)=0\right) \wedge \\
\wedge b_{1} c_{1}+b_{2} c_{2}=0 .
\end{gathered}
$$

Applying the Rabinovich-Trick and combining disjunctions to products results in the following set of polynomials

$$
\begin{gathered}
\left\{-\alpha_{0} b_{1}+\alpha_{1} \alpha_{0} b_{1} b_{2}-\alpha_{1} b_{2}+1,-\alpha_{2} c_{1}+\alpha_{3} \alpha_{2} c_{1} c_{2}-\alpha_{3} c_{2}+1,\right. \\
-\alpha_{4} \alpha_{5} b_{2} c_{1}^{3}+\alpha_{4} \alpha_{5} b_{1} c_{2} c_{1}^{2}+\alpha_{4} b_{2} c_{1}-\alpha_{4} \alpha_{5} b_{2} c_{2}^{2} c_{1}-\alpha_{4} b_{1} c_{2}+\alpha_{4} \alpha_{5} b_{1} c_{2}^{3}+ \\
2 \alpha_{4} \alpha_{5} b_{2} c_{1}^{2} d_{1}-\alpha_{4} \alpha_{5} b_{1} c_{1}^{2} d_{2}-\alpha_{4} \alpha_{5} b_{2} c_{1} d_{1}^{2}-\alpha_{4} \alpha_{5} b_{1} c_{2} c_{1} d_{1}+\alpha_{4} \alpha_{5} b_{2} c_{2} c_{1} d_{2}+ \\
\alpha_{4} \alpha_{5} b_{1} c_{1} d_{1} d_{2}+\alpha_{4} \alpha_{5} b_{1} c_{2} d_{2}^{2}+\alpha_{4} \alpha_{5} b_{2} c_{2}^{2} d_{1}-2 \alpha_{4} \alpha_{5} b_{1} c_{2}^{2} d_{2}-\alpha_{4} \alpha_{5} b_{2} c_{2} d_{1} d_{2}-\alpha_{4} b_{2} d_{1}+ \\
\alpha_{4} b_{1} d_{2}-\alpha_{5} c_{1}^{2}-\alpha_{5} c_{2}^{2}+\alpha_{5} c_{1} d_{1}+\alpha_{5} c_{2} d_{2}+1, \\
2 b_{2} c_{1}^{2} d_{1}-b_{1} c_{1}^{2} d_{2}-b_{2} c_{1} d_{1}^{2}-b_{1} c_{2} c_{1} d_{1}+b_{2} c_{2} c_{1} d_{2}+b_{1} c_{1} d_{1} d_{2}+b_{1} c_{2} d_{2}^{2}+b_{2} c_{2}^{2} d_{1}- \\
2 b_{1} c_{2}^{2} d_{2}-b_{2} c_{2} d_{1} d_{2}-b_{2} c_{1}^{3}+b_{1} c_{2} c_{1}^{2}-b_{2} c_{2}^{2} c_{1}+b_{1} c_{2}^{3}, \\
\left.b_{1} c_{1}+b_{2} c_{2}\right\},
\end{gathered}
$$

whose Gröbner basis is again $\{1\}$, hence, the statement is proved.


[^0]:    ${ }^{1}$ The concept of Gröbner bases and, most importantly, the first algorithm to compute a Gröbner basis for arbitrary $G$ were invented by Bruno Buchberger, the founder of RISC, the Research Institute for Symbolic Computation at JKU Linz.

[^1]:    ${ }^{2}$ There are two additional hypotheses in the model that are not mentioned explicitly. Usually, one assumes all the points being different, which would result in a huge amount of side conditions. It turns out, however, that it suffices to require that $R, S$, and $U$ and $R, S$, and $V$, respectively, are not collinear.

[^2]:    ${ }^{3}$ Note that inequations of the form $p \neq 0$ are covered in this setting as well because $p \neq 0 \equiv \neg(p=0)$, hence, an inequation is a boolean combination of an equality.

[^3]:    ${ }^{4}$ We used the product trick also when we expressed the condition $c_{1} \neq 0 \vee c_{2} \neq 0$ in Section 1.2.2.

