SOLVING PARAMETRIC POLYNOMIAL EQUATIONS AND INEQUALITIES BY SYMBOLIC ALGORITHMS

VOLKER WEISPFENNING
Fakultät für Mathemantik und Informatik, Universität Passau
D-94030 Passau, Germany
Tel: 0851-5093120, Fax: 0851-5091802
e-mail: weispfen@alice.fmi.uni-passau.de

ABSTRACT

The talk gives a survey on some symbolic algorithmic methods for solving systems of algebraic equations with special emphasis on parametric systems. Besides complex solutions I consider also real solutions of systems including inequalities. The techniques described include the Euclidean algorithm, Gröbner bases, characteristic sets, univariate and multivariate Sturm-Sylvester theorems, comprehensive Gröbner bases and elimination methods for parametric optimization problems. Some examples illustrate the use of symbolic algorithms for the solution of parametric systems.

1. Introduction

Many problems in applied mathematics can be reduced to the problem of solving a system of polynomial equations in several variables in the domain of real or complex numbers. Traditionally such systems are solved numerically. Numerical method can solve systems of impressive size; they are – as a rule – however restricted to systems with finitely many solutions. Moreover, the output often yields no information on the precise structure of the solution set (such as the number of solutions) and the output has to be analyzed with respect to quality of the approximation, stability, etc.[27]

Similar remarks apply to numerical real solutions of systems of inequalities and of optimization problems.

The goal of symbolic-algebraic methods, on the other hand, is to provide an exact description of the structure of the solution set (number of solutions or dimension of the solution set) and an exact description of the individual solutions. This includes the case that the solution set is infinite or depends on some parameters in the given system of equations.

As a prerequisite, this goal requires an exact symbolic representation of the input-data and of the possible solutions, i.e. infinite precision rational numbers (e.g. for linear systems) and suitable representations of real and complex algebraic numbers (for nonlinear systems).

The main problem arising in symbolic-algebraic computation is the size of the expressions arising during computations. If a symbolic computation concerning polynomial systems fails, this is more often due to storage limitations rather than time limitations.

Generally speaking symbolic methods for the solution of systems of polynomial equations and inequations are at present limited to problems of modest size. They are, however, able to attack successfully problems that are – by the nature of the question posed – outside the scope of numerical methods.

A combination of both methods by suitable interfaces between symbolic an numeric packages may in the near future yield a significant computational progress.

The talk will give **a survey on some symbolic methods for the following problems**:

- Solving univariate systems of polynomial equations in $\mathbb{C}$ and in $\mathbb{R}$.
- Solving multivariate systems of polynomial equations in $\mathbb{C}$ and in $\mathbb{R}$.
- Solving (parametric) multivariate systems of polynomial inequalities in $\mathbb{C}$ and in $\mathbb{R}$.
- (Parametric) linear, fractional linear and quadratic optimization.

I will try to give the flavour of the various methods and to demonstrate the applicability of symbolic methods to parametric problems by some examples.

2. Computing Complex and Real Zero-sets of Univariate Polynomials

The ideas that are used in the general case of multivariate polynomials are best understood by considering the easier case of a system $F \subset \mathbb{Q}[X]$ of univariate polynomials first. Here the *problem* is as follows:

Given a finite $F \subset \mathbb{Q}[X]$, determine the structure of the complex and real zero sets $V_{\mathbb{C}}(F)$ and $V_{\mathbb{R}}(F)$ as closely as possible by exact symbolic methods.

This can viewed either as a goal in itself or as an important preprocessing step for subsequent approximate numerical computations of individual zeros.

The basic step is the reduction of a polynomial f by a polynomial g with $\deg(f) \geq \deg(g) \geq 0$: If f has highest monomial aX^m and g has highest monomial bX^n, then $f \underset{g}{\longrightarrow} f_1 = a/bX^{m-n}g$ and $\deg(f_1) < \deg(f)$ or $f_1 = 0$. This simple reduction step can be applied iteratively to a finite non-empty set F of non-zero polynomials in $\mathbb{Q}[X]$ as follows: Choose $g \in F$ of minimal degree; replace all other polynomials $f \in F$ by there reducts f_1 w.r.t. g and discard all zero polynomials from the result. Iterate this procedure, until F contains only one polynomial f. Notice that in each iteration the maximal degree of all polynomials in F will decrease; so termination is guaranteed. Moreover, after each iteration the set $\mathrm{Id}(F)$ of all linear combinations of polynomials in F using arbitrary polynomials from $\mathbb{Q}[X]$ as factors (the *ideal* $\mathrm{Id}(F)$ generated by F) remains the same. So at the end we have $\mathrm{Id}(F) = \mathrm{Id}(f)$, which means that f is the gcd of all polynomials in F. This is a version of *Euclid's algorithm* for univariate polynomials.

Let $V_K(F)$ denote the *variety* of F in some extension field K of $\mathbb{Q}$, i.e. the set of all common zeros of F in K. Then we have the obvious equation $V_K(F) = V_K(\mathrm{Id}(F))$, and hence $V_K(F) = V_K(f)$ for the gcd f of F. Thus we have reduced the problem to determining the zeros of a single polynomial f. Next we can use another gcd computation, viz. $f^* = f/\gcd(f, f')$, where f' is the derivative of f, to get the *square-free part* f^* of f with the property that again $V_K(f) = V_K(f^*)$. Since f^* splits into different linear factors in $\mathbb{C}[X]$, $\deg(f^*)$ gives us the number of points in $V_{\mathbb{C}}(F)$. In particular $V_{\mathbb{C}}(F) = \emptyset$ iff f^* is a constant. (Notice that so far we have no information on the position of the zeros of f^* in $\mathbb{C} = \mathbb{R}^2$, since this is in fact a question about real zeros of two bivariate real polynomials representing the real and imaginary part of $f^*(X + iY)$.) Subsequent factorization of f^* into irreducible polynomials in $\mathbb{Q}[X]$ may split $V_{\mathbb{C}}(f^*)$ into disjoint parts and hence may help actually solve the equation by numeric methods.

In order to determine the real zeros of f^* and hence of F one may proceed as follows: For two given polynomials $f, g \in \mathbb{R}[X]$ consider the iterated reduction process described above that leads to the gcd of f and g. This time, however, we record not only the output of the algorithm but also the sequence of different divisors occurring during the reduction process. Let $f_2, \ldots, f_k$ be the sequence of new divisors occurring in the reduction process, and put $f_0 = f$, $f_1 = g$. Then the sequence $\mathbf{f} = (f_0, f_1, -f_2, -f_3, f_4, f_5, -f_6, -f_7, \ldots, \pm f_k)$ is the *Sturm-Sylvester-sequence* $S(f, g)$ of (f, g). For a real number c let $\mathbf{f}(c)$ denote the sequence of real values taken by the polynomials in $\mathbf{f}$ at the point c. Let $\mathrm{sc}(\mathbf{f}(a))$ denote the number of sign changes in this sequence of real numbers, when zeros are ignored. Then a beautiful theorem due to Sturm and Sylvester[4] says:

Let f, g be non-zero relative polynomials in $\mathbb{R}[X]$, let f be square-free, and let $a < b$ be real numbers that are non-zeros of f. Let $\mathbf{f}$ be the Sturm-Sylvester sequence of $(f, f' \cdot g)$. Denote the number of zeros of f in the interval $[a, b]$, where g is positive, zero, negative by $N(f, g, 1, a, b)$, $N(f, g, 0, a, b)$, and $N(f, g, -1, a, b)$, respectively. Then

$$\mathrm{sc}(\mathbf{f}(a)) - \mathrm{sc}(\mathbf{f}(b)) = N(f, g, 1, a, b) - N(f, g, -1, a, b) \tag{1}$$

In particular, for $g = 1$

$$\mathrm{sc}(\mathbf{f}(a)) - \mathrm{sc}(\mathbf{f}(b)) \tag{2}$$

is the number of zeros of f in the interval $[a, b]$, and for g replaced by g^2

$$\mathrm{sc}(\mathbf{f}(a)) - \mathrm{sc}(\mathbf{f}(b)) \tag{3}$$

is the number of zeros of f in $[a, b]$, where g does not vanish.

With the obvious sign evaluation of real polynomials at $\pm\infty$ this theorem can also be applied to the case $a = -\infty$ and/or $b = \infty$. The proof employs only the most elementary algebraic facts about real polynomials and their continuity.

An easy *corollary* concerns the general case, where the hypothesis that f is square-free and f and g are relatively prime is deleted:

Let f^* be the square-free part of f and let $h = f^*/\gcd(f^*, g)$ and let $\mathbf{f}$, $\mathbf{h}$, $\mathbf{k}$ be the Sturm-Sylvester sequences of $(f^*, f^{*\prime})$, $(h, h' \cdot g)$ and of $(h, h' \cdot g^2)$, respectively. Then *the numbers $N(f,g,1,a,b)$, $N(f,g,0,a,b)$, $N(f,g,-1,a,b)$ are the unique solution of the following system linear equations:*

$$\begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & -1 \\ 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} N(f,g,1,a,b) \\ N(f,g,0,a,b) \\ N(f,g,-1,a,b) \end{pmatrix} = \begin{pmatrix} \mathrm{sc}(\mathbf{f}(a)) - \mathrm{sc}(\mathbf{f}(b)) \\ \mathrm{sc}(\mathbf{h}(a)) - \mathrm{sc}(\mathbf{h}(b)) \\ \mathrm{sc}(\mathbf{k}(a)) - \mathrm{sc}(\mathbf{k}(b)) \end{pmatrix} \tag{4}$$

The corollary is derived from the theorem in a purely combinatorial way. So it can be applied to any other method for the calculation of $N(f,g,1,a,b) - N(f,g,-1,a,b)$. In fact there is another such calculation due to Hermite that has recently found a beautiful generalization to the multivariate case (comp. [2,28] and section 4 below): It does not require f to be square-free and g to be relatively prime to f. It asserts that the number $N(f,g,1,a,b) - N(f,g,-1,a,b)$ is the signature (i.e. the number of positive eigenvalues minus the number of negative eigenvalues) of a symmetric $n \times n$ matrix (a_{ij}) that is computed as follows: $n = \deg(f)$ and a_{ij} is the trace of the linear map $h \mapsto X^{i+j}gh$ on the real vector space $\mathbb{R}[X]/f$ of residues modulo f with respect to the canonical basis $\{1, X, \ldots, X^{n-1}\}$.

Moreover, there is a far-reaching generalization of the corollary to the counting of real zeros c of f satisfying several side conditions, say $g_1(c) > 0, \ldots, g_m(c) > 0$. Again this generalization is derived in a purely combinatorial way employing tensor-powers of the 3×3-matrix above.[4,33] Since over the reals the common zeros of a finite polynomial system $F = \{f_1, \ldots, f_r\}$ can be expressed as the zeros of a single polynomial $f = f_1^2 + \ldots + f_r^2$, this generalization solves all point counting problems for finite systems of univariate polynomial inequalities.

A priory bounds for the size of the real zeros of univariate polynomials are given by the *Cauchy bounds*:[26]

Let $f = \sum_{i=0}^{n} a_i X^i \in \mathbb{Q}[X]$ with $a_n \neq 0$. Then the absolute value of every real zero of f is bounded by the following expressions:

$$C_1 = 1 + \max\left\{ \frac{|a_i|}{|a_n|} \;\middle|\; 0 \leq i \leq n-1 \right\}, \qquad C_2 = \max\left\{ 1, \sum_{i=0}^{n-1} \frac{|a_i|}{|a_n|} \right\}. \tag{5}$$

Once a Sturm-Sylvester sequence for (f, f') has been computed for a square-free polynomial f, one can evaluate the number of sign changes of $S(f, f')$ at the endpoints of intervals obtained from the starting interval $[-C_i, C_i]$ ($i = 1$ or $i = 2$) by successive bisection until one has found a finite sequence of pairwise disjoint open intervals with rational endpoints each of which contains exactly one real root of f. Call these the *isolating intervals* for the real roots of f. Using only the endpoints a, b of such an isolating interval and the coefficients of f one can now evaluate any other polynomial $g \in \mathbb{Q}[X]$ at the unique zero α of f in the open interval (a, b) using again the theorem of Sturm-Sylvester: Assume without restriction that f is square-free and let $\mathbf{h}$ be defined as above. Then

$$g(\alpha) > 0 \ (= 0, \ < 0) \iff \mathrm{sc}(\mathbf{h}(a)) - \mathrm{sc}(\mathbf{h}(b)) = 1 \ (= 0, \ = -1) \tag{6}$$

This shows that the *isolating interval* $[a, b]$ for α can be used as an exact algebraic code for the algebraic real number α in algebraic computations. Moreover by iterating the bisection of intervals and the evaluation the number of sign changes of $S(f, f')$ at the endpoints of these intervals, one obtains arbitrarily good numeric approximations of α. This coding of real algebraic numbers is used extensively in the SAC-2 computer algebra system.[7] Another possible code for a real zero α of f is the sequence of signs of all higher derivatives of f at α (Thom's Lemma[3]).

3. Computing Complex and Real zero-sets of Multivariate Polynomials

In the univariate case the computation of the variety of a finite system F of polynomials was reduced to that of a single polynomial by taking a gcd. While gcd's still can be computed in multivariate polynomial rings R over fields, they do not serve the same purpose for solving equations, since $\gcd(F)$ is no longer a R-linear combination of polynomials in F, since R is not a principal ideal ring. Nevertheless, the role of $\gcd(F)$ for the solution of equations can be simulated to a certain extent by certain finite polynomial systems G that have the same R-linear combinations as F, but exhibit the structural properties of the complex or real variety of F more clearly. As in the univariate case $\mathrm{Id}(F)$ denotes the ideal generated by F, i.e. the set of all R-linear combination of polynomials in F.

There are two essentially different generalizations of the Euclidean algorithm (and hence the gcd):

The computation of characteristic sets (*Ritt-Wu*)[6,26] and the computation of Gröbner bases (*Buchberger*)[2,8]. They are based on two different generalizations of the univariate reduction step to the multivariate case corresponding to recursive and the distributive representation of multivariate polynomials. In the recursive representation a polynomial f over a field K in indeterminates $X_1, \ldots, X_n$ are viewed as objects in $(\ldots(K[X_1])\ldots)[X_n]$, whereas in the distributive representation f is regarded as a K-linear combination of *terms*, i.e. power-products $X_1^{e_1} \cdots X_n^{e_n}$ of the indeterminates.

We begin with a sketch of the **characteristic set method**. In the recursive representation one can define a quasi-order on polynomials by putting $f < g$ if g contains an indeterminate with higher index then the highest indeterminate occurring in f, or both have the same highest indeterminate X_i, but g has higher degree in X_i than f. If f is written as univariate polynomial in its highest indeterminate X_j with coefficients in the remaining indeterminates, then the highest coefficient of f is called the *initial* I_f of f. Suppose now g is another polynomial with $m = \deg_{X_j}(g) \geq \deg_{X_j}(f) = k$ and g is written as univariate polynomial in the indeterminate X_j with coefficients in the remaining indeterminates. (We do not require X_j to be the highest indeterminate in g.) Then we have the following *(Ritt-)reduction* of g by the *divisor* f:

$$g \xrightarrow[f]{} g^* = I_f g - I_g X_j^{m-k+1} f \quad \text{with} \quad \deg_{X_j}(g) \geq \deg_{X_j}(g^*). \tag{7}$$

g is called reduced w.r.t. f if no such reduction is possible, i.e. if $\deg_{X_j}(g) < \deg_{X_j}(f)$.

Notice that any chain of reductions using the same divisor f will terminate after finitely many steps, since $\deg_{X_j}$ decreases in each step.

An *ascending set* is either a non-zero constant or a finite sequence A of non-constant polynomials with strictly increasing highest indeterminates, such that each polynomial in A is reduced w.r.t. all the previous ones. Ascending sets are quasi-ordered by first differences in their entries from left to right. If no such difference in quasi-order is encountered the longer sequence is declared smaller than the shorter one. This yields a well-founded quasi-order on ascending sets. As a consequence, every non-empty set F of polynomials in the given polynomial ring contains a minimal ascending set C. Any such C is called a *characteristic set* of F. For finite F such a characteristic set can be determined in an obvious way by inspection.

Let now F be finite and let $C \subseteq F$ be a characteristic set of F. Then each polynomial $f \in F$ can be reduced as long as possible, using the polynomials in C successively in decreasing order, to a polynomial f^* (which may coincide with f if no such reduction is possible). Call f^* the *remainder* of f upon reduction by the ascending set C. Adding all the non-zero remainders f^* of polynomials $f \in F$ obtained in this way to the set F, we obtain finite set F_1 extending F. If F_1 is strictly larger than F, then F_1 contains a new characteristic set C_1 smaller than C in the quasi-order of ascending sets.

Iterating this procedure we arrive at an increasing chain of polynomial sets $F = F_0 \subset F_1 \subset F_2 \subset \ldots$ with an associated strictly decreasing chain of characteristic sets $C = C_0 > C_1 > C_2 > \ldots$. Since the quasi-order on characteristic sets is well-founded, this iteration will terminate after finitely many steps, say with F_k and C_k. By construction, every polynomial in F_k is still in the ideal $\mathrm{Id}(F)$, and so $\mathrm{Id}(F_k) = \mathrm{Id}(F)$, and so $V_K(F_k) = V_K(F)$ for $K = \mathbb{C}$ or $K = \mathbb{R}$. Moreover, the remainder of every $f \in F_k$ upon reduction by C_k is zero. As a consequence, we have the following relation between the variety of F_k and the variety of C_k: Let J be the product of all the initials of the polynomials in C_k. Then

$$V_K(F) \setminus V_K(J) = V_K(C_k) \setminus V_K(J) \quad \text{for} \quad K = \mathbb{C} \text{ or } K = \mathbb{R}. \tag{8}$$

Call the characteristic set $C' = C_k$ of $F' = F_k$ obtained in this way an *extended characteristic set* of F. Notice that C' has triangular shape. So $V_{\mathbb{C}}(C')$ is finite iff every X_j is the highest indeterminate of the j-th polynomial in C'. If this is the case, then the individual points in $V_{\mathbb{C}}(C')$ can be computed e.g. numerically by solving successive univariate polynomials. In particular $V_{\mathbb{C}}(C') = \emptyset$ iff C' consists of a constant only. If C' contains less than n polynomials, there will be gaps in the sequence of highest variables of these polynomials, which are related to the dimension of $V_{\mathbb{C}}(C')$. So we have got some structural information on the set $V_{\mathbb{C}}(F) \setminus V_{\mathbb{C}}(J) = V_{\mathbb{C}}(C_k) \setminus V_{\mathbb{C}}(J)$.

In order to determine the remaining part of $V_{\mathbb{C}}(F)$, i.e. $V_{\mathbb{C}}(F) \cap V_{\mathbb{C}}(J)$, we proceed as follows: For each initial I_h of some polynomial h in C', we consider the set $F_h = F' \cup \{I_h\}$ we compute as before an extended characteristic set C_h''. By construction $C_h'' < C'$.

Iterating these steps of adding initials and computing extended characteristic sets will lead to a finitely branching tree of ascending sets. Each branch of the tree is finite, since the ascending sets in this branch are decreasing, and so by König's lemma the whole tree is finite. Let $C_1, \ldots, C_m$ be the extended characteristic sets that form the leaves of this tree. Then for any extension field K of $\mathbb{Q}$ we have a disjoint decomposition

$$V_K(F) = \bigcup_{i=1}^{m} (V_K(C_i) \setminus V_K(J_i)), \tag{9}$$

where the systems C_i are ascending sets (and hence of triangular form) and the J_i are products of all initials of the polynomials in C_i.

This decomposition can then be used for numeric computations of individual elements of $V_{\mathbb{C}}(F)$ and of $V_{\mathbb{R}}(F)$ in case these sets are finite. Alternatively, individual solutions in $\mathbb{C}$ can be computed symbolically in iterated algebraic extension fields of $\mathbf{Q}$. This requires, however, factorization of polynomials over iterated algebraic extension fields and can get too complex. Individual real solutions can be computed symbolically from the decomposition using their description by isolating rational intervals described in the previous section.

The method has been employed most successfully in order to show for given polynomial f that $V_{\mathbb{C}}(F) \subseteq V_{\mathbb{C}}(F)$ and hence $V_{\mathbb{R}}(F) \subseteq V_{\mathbb{R}}(F)$ by showing that f Ritt-reduces to zero w.r.t. all C_i. This yields automatic proofs of many interesting geometrical theorems.[6,26]

Next we give a quick sketch of the **Gröbner basis method** and its applications to equation solving.[2] The basic idea as in the Ritt-Wu method is to modify a given finite system of polynomials to another finite system G with the property that the varieties of F and G are closely related, and structural properties of the complex and real variety of G can be derived from the shape of G rather directly. In contrast to the construction of characteristic sets, the construction of a Gröbner basis G from F does not yield a decomposition of the variety of F. Instead, the variety remains the same, $V_K(G) = V_K(F)$. In fact even the ideal generated by F is preserved, $\mathrm{Id}(F) = \mathrm{Id}(G)$.

A central concept is again a kind of polynomial reduction, here *Buchberger reduction*. Recall that Ritt-reduction regarded polynomials as univariate polynomials in the highest indeterminate allowing multiplication of the dividend with polynomials in lower variables. For Buchberger reduction we think of polynomials as finite $\mathbb{Q}$-linear combinations of terms (power-products of the X_i). In order to perform some kind of division with remainder, we should know what we shall regard as the "highest" term in the divisor polynomial.

This is achieved by introducing a *term order* i.e. a linear order on the set T of terms which has 1 as smallest element and for which multiplication is monotonic. Examples are the *lexicographic* term order (induced by the lexicographic order of the exponent tuples), the *inverse lex* term order (just as the lex order with the order of variables reversed), and the *degree-lex* term order (which orders by total-degree first and breaks ties using the lex order on the set T of terms). With respect to a fixed term order we can then speak of the "highest monomial" $\mathrm{HM}(f)$ of a non-zero polynomial f just as in the univariate case. (By convention all monomials will have non-zero coefficients.)

The resulting reduction concept is straightforward: $g \xrightarrow[f]{} g_1 = g - \frac{b}{a}uf$, if g contains a monomial bt $(b \in K, t \in T)$ and $\mathrm{HM}(f) = as$ and $t = us$ in T. Iterated Buchberger reduction of a polynomial g using divisors f from a given set F is denoted by $g \xrightarrow[F]{*} h$. Any chain of reductions is finite. This can be seen as follows: By Dickson's lemma, divisibility on T is a well-quasi-order; since any term order refines the divisibility relation on T, term orders are well-orders; any reduction decreases the highest term of the polynomials w.r.t. the chosen term order.

At first glance Buchberger reduction for the inverse lexicographical term order appears to be very close to Ritt reduction. Notice that Ritt reduction will be applicable much more often than Buchberger reduction since it allows multiplication of the dividend by the initial of the divisor. So it may not be surprising that the addition of all remainders of polynomials in F by iterated Buchberger reduction with divisors in F will in general (except in the univariate case) not yield much more structural information on $\mathrm{Id}(F)$ and hence on $V_K(F)$.

So another process is needed for generating new polynomials in $\mathrm{Id}(F)$. It takes account of cancellations of highest monomials in R-linear combinations of elements of F, that are not discovered by the reduction process. Take e.g. the set $F = \{f, g\} \subset \mathbb{Q}[X, Y]$ with $f = X^2Y + 1$, $g = XY^2 + 1$. Here no Buchberger reduction is possible, but $Yf - Xg = Y - X \in \mathrm{Id}(F)$. For every pair of polynomials $f, g \in \mathbb{Q}[X_1, \ldots, X_n]$ there is an obvious way of constructing the "minimal" such cancellation, as in the example. Call the resulting "subtraction"-polynomial the *S-polynomial* $\mathrm{SPol}(f, g)$ of f and g.

The construction of a Gröbner basis G (w.r.t a fixed term order) from F proceeds by an iteration of adding all non-zero remainders of all S-polynomials w.r.t. reduction using the set of polynomials at hand as possible divisors. Again Dickson's lemma guarantees that this iteration stops after finitely many steps. The output will be a finite set G with $\mathrm{Id}(G) = \mathrm{Id}(F)$ with the property that all S-polynomials of pairs from G can be reduced to zero using polynomials from G. Such a set G is called a *Gröbner basis* of $\mathrm{Id}(F)$ (w.r.t the given term order).

In practice the computation of normal forms of S-polynomials w.r.t. the Buchberger reduction is the bottleneck of the construction, since it may involve computations with very large coefficients. So a number of sophisticated criteria and methods has been developed in order to recognize without lengthy computations superfluous S-polynomials, i.e. S-polynomials, whose normal form will not contribute to the construction of the Gröbner basis.

In order to simplify a given Gröbner basis G one may interreduce all polynomials in G (by Buchberger reduction) as long as possible. This process terminates as well and yields a *reduced Gröbner basis* of $\mathrm{Id}(F)$. Rather surprisingly reduced Gröbner bases are uniquely determined by $\mathrm{Id}(F)$ and the term order, provided all polynomials are made monic.

What is the information on $V_{\mathbb{C}}(F)$ that can be obtained from a Gröbner basis G of $\mathrm{Id}(F)$ without much further effort?

- The decision, whether $V_{\mathbb{C}}(F) = \emptyset$ (check if G contains a non-zero constant).
- The decision, whether $V_{\mathbb{C}}(F)$ is finite. If this is not the case, the computation of the dimension of $V_{\mathbb{C}}(F)$ and of of a maximal set of independent variables (inspection of the highest terms in G).
- If $V_{\mathbb{C}}(F)$ is finite, explicit computations in the residue class ring $\mathbb{Q}[X_1, \ldots, X_n]/\mathrm{Id}(F)$, computation of the radical of $\mathrm{Id}(F)$, computation of the number of complex zeros of F.

All the above works for arbitrary term orders. The complexity of a Gröbner basis computation for a given system F may vary enormously according to the term order chosen. There are some heuristic principles but no definite theoretical results for the choice of a "good" term order. For numerical (or symbolic algebraic) computation of individual solutions, one requires the reduced Gröbner basis G to be in triangular form; this is guaranteed for the lexicographical term orders. For a detailed study of solutions of algebraic systems in triangular form by symbolic methods.[20,21]

Moreover, Gröbner bases have numerous other applications in computational commutative algebra.[2] At present computations of $V_{\mathbb{C}}(F)$ via Gröbner bases are limited – as a rule of thumb – to systems of say at most 10 variables and of total degree at most 10.

This scope can sometimes be extended considerably by combining the Gröbner bases construction with intermediate factorization of polynomials.[25,16] This yields a decomposition of $V_{\mathbb{C}}(F)$ as a finite union of smaller varieties $V_{\mathbb{C}}(G_i)$ given by their respective Gröbner bases G_i.

For zero-dimensional systems F (i.e. systems with finite complex variety) the computation of an *involutive basis* provides sometimes a faster alternative to the Buchberger algorithm for the computation of a Gröbner basis.[37] The method is an adaptation of ideas developed by Janet for non-commutative rings of differential operators to the case of commutative polynomial rings.

In case $V_{\mathbb{C}}(F)$ is finite, the real zero set $V_{\mathbb{R}}(F)$ can be computed e.g. as follows (compare [2], section 8.8): One introduces a new variable Z as random linear combination ℓ of $X_1, \ldots, X_n$ such that the variety $V_{\mathbb{C}}(F \cup \{\ell\})$ is in normal position with respect to Z, a fact that is checked by a Gröbner basis computation. Then Z satisfies a univariate polynomial equation $f(Z) = 0$ over $\mathbb{Q}$ and all X_i are given as polynomial functions of Z. Hence the real zeros of F can now be determined from the real zeros of the univariate polynomial f.

An alternative method dealing directly is based on a *multivariate version of the Sturm-Sylvester theorem* discovered recently.[2,28] It uses an extension of the computation of signatures of certain quadratic forms sketched for the univariate case in the next section.

4. Computing Parametric Complex and Real Zero-sets

Next we consider the **corresponding parametric problems**. They arise either if the coefficients of the polynomials in the system $F = 0$ depend on (complex or real) parameters or, if F is parameter-free but $V_{\mathbb{C}}(F)$ has positive dimension and one wants to determine the zeros of F in dependence of a set $\mathcal{Y} \subseteq \{X_1 \ldots X_n\}$ of independent variables acting as parameters. Since the latter case may be considered as a special case of the former, we restrict our attention to the first case.

So we consider finite $F \subseteq \mathbb{Q}[U_1, \ldots, U_m][X_1, \ldots, X_n]$, and we want to determine $V_{\mathbb{C}}(F_{\mathbf{a}})$ and $V_{\mathbf{R}}(F_{\mathbf{a}})$ in dependence of arbitrary complex or real values $\mathbf{a} = (a_1, \ldots, a_m)$ of the parameters $\mathbf{U} = (U_1, \ldots, U_m)$. (Here $F_{\mathbf{a}} = \{ f(\mathbf{a}, \mathbf{X}) \mid f(\mathbf{U}, \mathbf{X}) \in F \}$.)

What is the answer we expect for questions like $|V_{\mathbb{C}}(F_{\mathbf{a}})| = d$ or $|V_{\mathbb{R}}(F_{\mathbf{a}})| = d$ or $\dim V_{\mathbb{C}}(F_{\mathbf{a}}) = d$ for a natural number d for arbitrary values of $\mathbf{a}$? Obviously it should consist of conditions on the parameters $\mathbf{U}$ that are easy to evaluate for given a given value $\mathbf{a}$ of $\mathbf{U}$. Typically such a condition is a boolean combination of polynomial equations in $\mathbf{U}$ in the complex case, and of a boolean combination of polynomial inequalities in the real case. Such a condition will then constitute a *uniform solution* to the parametric problem. It is well-known from algebraic model theory that conditions of this form do indeed exist. In the following I sketch some methods that can be useful for computing such conditions in practice.

The basic idea is to use the methods applied in the non-parametric cases in such a way as to split the computation into a tree depending on case distinctions concerning the vanishing (or the signs in the real case) of certain coefficients that enter the computation step in an essential way.

In principle it suffices to treat systems of parametric univariate polynomial equations and disequations (equations and inequalities in the real case), since the case of several main variables can then be handled by induction. Recall from the univariate case that Euclidean algorithm and its variants (Sturm-Sylvester-sequences) form the centerpiece of the non-parametric univariate algorithms. Unfortunately in the parametric case, the Euclidean algorithm will require an enormous number of case distinctions on the possible vanishing of highest coefficients of polynomials used as divisors. So in general it is not advisable for complexity reasons to follow this route. (See however the next section for a counterexample). Various replacements for the Euclidean algorithm and Sturm-Sylvester sequences have been considered in the literature that behave better in the parametric case. (comp. [15,17,29]).

For multivariate parametric systems, the method of computation of an extended characteristic set is by its inherent cases distinctions well fitted for parameters and does not require essential changes from the non-parametric case (comp.[13]). But again the number of case distinctions may be prohibitive in practice. For parametric systems of linear equations a symbolic solution method has been presented in [30].

For the rest of this section I will consider the use of **Gröbner bases in the parametric case**.

The basic observation here is that it is not sufficient to compute a Gröbner basis G of F with respect to the variables $\mathbf{X}$ and indeterminate parameters $\mathbf{U}$, since under specialization of $\mathbf{U}$ to some value $\mathbf{a}$, $G_{\mathbf{a}}$ may no longer be a Gröbner basis. This problem is remedied by the more subtle construction of a *comprehensive* Gröbner basis for F that does in fact remain stable under specialization of parameters (see [32]). The idea of the construction is to perform a tree of Gröbner basis computations w.r.t. the necessary case distinctions on the parameters, but to keep all the coefficients in the computation that have been asserted to vanish in some case. In this manner all the Gröbner bases obtained at the leaves of the tree stay inside the given input ideal; so the whole case distinction can be discarded and the different Gröbner bases at the leaves can be joint into one single polynomial system which turns out to be a comprehensive Gröbner basis of F.

Once a comprehensive Gröbner basis G has been computed from F, the structure of $V_{\mathbb{C}}(F_{\mathbf{a}})$ can easily and uniformly obtained from G in dependence of the complex values $\mathbf{a}$ of the parameters $\mathbf{U}$. In particular there are boolean combinations of polynomial equations in the parameters that are necessary and sufficient conditions for the following properties: $V_{\mathbb{C}}(F_{\mathbf{a}}) = \emptyset$, $|V_{\mathbb{C}}(F_{\mathbf{a}})| = d$, $\dim(V_{\mathbb{C}}(F_{\mathbf{a}})) = d$ for a given natural number d.

The corresponding problem concerning the structure of $V_{\mathbb{R}}(F_{\mathbf{a}})$ is much more subtle. Due to the presence of parameters, it is in practice impossible to reduce the problem to the univariate case as in the non-parametric case, since this would involve too many case different Gröbner basis calculations.

Progress has, however, been made recently in an important special case, viz. when $V_{\mathbb{C}}(F_{\mathbf{a}})$ is finite for all relevant values of $\mathbf{a}$. In this case the construction of comprehensive Gröbner bases can be combined with the powerful multivariate Sturm theorem mentioned earlier[1,28] to obtain the structure of $V_{\mathbb{R}}(F_{\mathbf{a}})$ in dependence of the relevant values of $\mathbf{a}$.[33] One proceeds as follows: Using a comprehensive Gröbner basis of $\mathrm{Id}(F)$, one computes $\mathbb{Q}$-linear bases and structure constants for the finitely many residue class rings $\mathbb{Q}[X_1, \ldots, X_n]/(F_{\mathbf{a}})$ that may occur for all values of the parameters. In each case one computes a certain quadratic form on the respective $\mathbb{Q}$-linear space. Then the number of real zeros of F in each case is determined by the signature of the corresponding quadratic form in much the same way as in the univariate case described in section 2. For any fixed $k \in \mathbb{N}$ one can write down a boolean combination of polynomial inequalities in the parameters $\underline{U}$ expressing the fact that this signature equals k. In this way one gets conditions on the parameters that express the fact that $|V_{\mathbb{R}}(F_{\mathbf{a}})| = d$. Unfortunately these conditions tend to become very long for large dimensions of the $\mathbb{Q}$-linear space; so applications so far are limited. Again as in the non-parametric case, side conditions can in principle be incorporated into the method.[10]

5. Solving Systems of Inequalities and Optimization Problems

Finally we consider **systems of inequalities and optimization**. The general problem is to decide whether such a system has a solution and to determine a solution that minimizes a given polynomial objective function. Here symbolic methods have had little success so far in comparison to the sophisticated numerical methods available.

But here again, symbolic methods have a potential for applicability concerning parameterized problems. The parameterized feasibility and optimization problem are a special cases of the *quantifier elimination problem* for the elementary theory of reals. Its algorithmic solvability was proved by A. Tarski in the 1930s and is realized in the sophisticated general-purpose SAC-2-package QEPCAD by Collins and Hong[7] (compare [23], for applications). In addition, special purpose packages have been developed in order to extend the fairly limited scope of applicability of the QEPCAD-package for problems of a special form. [14,18,24,31,33,34,35]

Let us consider e.g. the problem of parametric linear optimization. Here the classical symbolic method (generalizing Gauss elimination) is due to Fourier-Motzkin (see [9] and [11] for the parametric case). Since the method is worst-case doubly exponential even in the non-parametric case, its applicability is very limited (say well below 10 variables). Here an alternative symbolic elimination method has been found recently[36], that is only singly exponential in the worst case and performs significantly better in practice. This applies in particular to inputs, where the parameters occur only additively. It takes advantage of equations occurring in the input and of a possible sparsity of the input matrix. So it is able to handle problems of interesting size – say 50 variables as a rule of thumb. It is an instance of the idea of eliminating one variable after another by a finite selection of explicitly given well-chosen parametric test points. In contrast to the Fourier-Motzkin method it is also applicable to parametric optimization of quadratic and fractional linear objective function under linear constraints.

6. Examples

The following examples concern only the methods for solving parametric problems developed by the author's working group at the university of Passau. For the applicability of the characteristic set method and the Gröbner basis method in general we refer to the references below and the examples collected by the PoSSo project.

Example 1: The following complex elimination problem was posed by M. Weis of the working group of Prof. Zimmer, Universität Saarbrücken.
Given the following polynomials $f, g, h \in \mathbb{Q}[A, B, N_1, N_2, N_3][X, Y, Z]$:

$$\begin{aligned} f &= ZYX - BYX - BZX + B^2X - BZY + B^2Y + B^2Z - (N_3 + B^3), \\ g &= ZYX - AYX - AZX + A^2X - AZY + A^2Y + A^2Z - (N_2 + A^3), \\ h &= ZYX - N_1. \end{aligned} \tag{10}$$

Determine necessary and sufficient conditions on the parameters A, B, N_1, N_2, N_3 for $V_{\mathbb{C}}\{f, g, h\} \neq \emptyset$.
The problem was solved by computation of a comprehensive Gröbner basis G for $\mathrm{Id}\{f, g, h\}$ and automatic simplification of the resulting conditions. The result was:

$$(A = 0 \Longrightarrow N_2 - N_1 = 0) \wedge (B = 0 \Longrightarrow N_3 - N - 1 = 0) \wedge (B - A = 0 \Longrightarrow N_3 - N_2 = 0) \tag{11}$$

Example 2 (The Whitney umbrella): Consider the map $\omega : \mathbf{R}^2 \longrightarrow \mathbf{R}^3$ given by

$$x = uv, \quad y = v, \quad z = u^2 \tag{12}$$

The Whitney umbrella U is the smallest real variety containing the image of this map.[8]We are trying to find the image of ω inside U, i.e. a condition $\varphi'(x,y,z)$ equivalent in $\mathbb{R}$ to

$$\varphi(x,y,z) \;=\; \exists u \exists v (x = uv \;\wedge\; y = v \;\wedge\; z = u^2). \tag{13}$$

To this end, we compute a comprehensive Gröbner basis H of I in $\mathbf{Q}[x,y,z][u,v]$ with respect to the total-degree-inverse-lex order on u, v.

$$H = \{y^2z - x^2, yu - x, v - y, u^2 - z\}. \tag{14}$$

From H we automatically get the following condition equivalent to φ in the field $\mathbb{R}$ of real numbers:

$$\varphi'(x,y,z) \;=\; y^2z - x^2 \;\wedge\; (y = 0 \implies z \geq 0). \tag{15}$$

The remaining examples have been computed by the REDUCE-implementation.[19] Timings refer to a SUN Sparc-10.

Example 3: This is the three-dimensional transportation problem, with the bounds $(3,2,2)$ for the range of the 3 indices (see [24] for a more detailed discussion).
Input:
$\exists x_{322} \exists x_{222} \exists x_{122} \exists x_{321} \exists x_{221} \exists x_{121} \exists x_{312} \exists x_{212} \exists x_{112} \exists x_{311}$
$\exists x_{211} \exists x_{111} (-a_{11} + x_{111} + x_{112} = 0 \;\wedge\; -a_{12} + x_{121} + x_{122} = 0 \;\wedge$
$-a_{21} + x_{211} + x_{212} = 0 \;\wedge\; -a_{22} + x_{221} + x_{222} = 0 \;\wedge\; -a_{31} + x_{311} + x_{312} = 0$
$\wedge\; -a_{32} + x_{321} + x_{322} = 0 \;\wedge\; -b_{11} + x_{111} + x_{121} = 0 \;\wedge$
$-b_{12} + x_{112} + x_{122} = 0 \;\wedge\; -b_{21} + x_{211} + x_{221} = 0 \;\wedge\; -b_{22} + x_{212} + x_{222} = 0$
$\wedge\; -b_{31} + x_{311} + x_{321} = 0 \;\wedge\; -b_{32} + x_{312} + x_{322} = 0 \;\wedge$
$-c_{11} + x_{111} + x_{211} + x_{311} = 0 \;\wedge\; -c_{12} + x_{112} + x_{212} + x_{312} = 0 \;\wedge$
$-c_{21} + x_{121} + x_{221} + x_{321} = 0 \;\wedge\; -c_{22} + x_{122} + x_{222} + x_{322} = 0 \;\wedge\; x_{111} \geq 0$
$\wedge\; x_{112} \geq 0 \;\wedge\; x_{121} \geq 0 \;\wedge\; x_{122} \geq 0 \;\wedge\; x_{211} \geq 0 \;\wedge\; x_{212} \geq 0 \;\wedge\; x_{221} \geq 0 \;\wedge\; x_{222} \geq 0 \;\wedge$
$x_{311} \geq 0 \;\wedge\; x_{312} \geq 0 \;\wedge\; x_{321} \geq 0 \;\wedge\; x_{322} \geq 0)$
Output:
$((a_{12} - a_{31} - b_{11} + b_{32} + c_{11} - c_{22} \geq 0 \;\wedge$
$a_{11} + a_{12} - b_{11} + b_{32} - c_{12} - c_{22} \leq 0 \;\wedge$
$a_{12} - a_{31} - b_{11} - b_{21} + b_{32} + c_{11} - c_{22} \leq 0 \;\wedge$
$b_{11} + b_{21} + b_{31} - c_{11} - c_{21} = 0 \;\wedge\; a_{31} + a_{32} - b_{31} - b_{32} = 0 \;\wedge$
$a_{11} + a_{21} + a_{31} - c_{11} - c_{12} = 0 \;\wedge\; a_{11} + a_{12} - b_{11} - b_{12} = 0 \;\wedge$
$a_{11} + a_{12} - b_{11} + b_{22} + b_{32} - c_{12} - c_{22} = 0 \;\wedge$
$a_{12} + a_{22} - a_{31} - b_{11} - b_{21} + b_{32} + c_{11} - c_{22} = 0 \;\wedge\; a_{31} - b_{32} + c_{22} \geq 0 \;\wedge$
$a_{12} - a_{31} - b_{11} + b_{32} - c_{22} \leq 0 \;\wedge\; b_{31} \geq 0 \;\wedge\; a_{31} \geq 0 \;\wedge$
$a_{12} - a_{31} + b_{32} - c_{22} \geq 0 \;\wedge\; a_{11} + a_{12} - a_{31} - b_{11} + b_{32} - c_{22} \geq 0 \;\wedge$
$a_{31} - b_{32} \leq 0)$
$\vee\; (a_{12} - a_{31} - b_{11} + b_{32} + c_{11} - c_{22} \geq 0 \;\wedge\; \ldots$

(the output would continue here for 2 more pages)
Time: 1428 ms

Example 4: This example, AFIRO, is one of a series of benchmark examples for linear programming provided to us by H. Melenk at the ZIB, Berlin. Here and in the following examples the last entry of the input is the objective function to be minimized and the last entry of the output (in each parametric case) is the minimal value of the objective function.
Input:

$$\exists vx_{01}\exists vx_{02}\exists vx_{03}\exists vx_{04}\exists vx_{06}\exists vx_{07}\exists vx_{08}\exists vx_{09}\exists vx_{10}\exists vx_{11}$$
$$\exists vx_{12}\exists vx_{13}\exists vx_{14}\exists vx_{15}\exists vx_{16}\exists vx_{22}\exists vx_{23}\exists vx_{24}\exists vx_{25}\exists vx_{26}$$
$$\exists vx_{28}\exists vx_{29}\exists vx_{30}\exists vx_{31}\exists vx_{32}\exists vx_{33}\exists vx_{34}\exists vx_{35}\exists vx_{36}\exists vx_{37}$$
$$\exists vx_{38}\exists vx_{39}(vx_{01} \geq 0 \ \wedge \ vx_{02} \geq 0 \ \wedge \ vx_{03} \geq 0 \ \wedge \ vx_{04} \geq 0 \ \wedge \ vx_{06} \geq 0 \ \wedge$$
$$vx_{07} \geq 0 \ \wedge \ vx_{08} \geq 0 \ \wedge \ vx_{09} \geq 0 \ \wedge \ vx_{10} \geq 0 \ \wedge \ vx_{11} \geq 0 \ \wedge \ vx_{12} \geq 0 \ \wedge \ vx_{13} \geq 0 \ \wedge$$
$$vx_{14} \geq 0 \ \wedge \ vx_{15} \geq 0 \ \wedge \ vx_{16} \geq 0 \ \wedge \ vx_{22} \geq 0 \ \wedge \ vx_{23} \geq 0 \ \wedge \ vx_{24} \geq 0 \ \wedge \ vx_{25} \geq 0 \ \wedge$$
$$vx_{26} \geq 0 \ \wedge \ vx_{28} \geq 0 \ \wedge \ vx_{29} \geq 0 \ \wedge \ vx_{30} \geq 0 \ \wedge \ vx_{31} \geq 0 \ \wedge \ vx_{32} \geq 0 \ \wedge \ vx_{33} \geq 0 \ \wedge$$
$$vx_{34} \geq 0 \ \wedge \ vx_{35} \geq 0 \ \wedge \ vx_{36} \geq 0 \ \wedge \ vx_{37} \geq 0 \ \wedge \ vx_{38} \geq 0 \ \wedge \ vx_{39} \geq 0 \ \wedge$$
$$-vx_{01} + vx_{02} + vx_{03} = 0 \ \wedge \ -53vx_{01} + 50vx_{04} = 0 \ \wedge \ vx_{01} - 80 \leq 0 \ \wedge$$
$$-5vx_{02} + 7vx_{14} \leq 0 \ \wedge \ -vx_{06} - vx_{07} - vx_{08} - vx_{09} + vx_{14} + vx_{15} = 0 \ \wedge$$
$$-53vx_{06} - 53vx_{07} - 48vx_{08} - 43vx_{09} + 50vx_{16} = 0 \ \wedge$$
$$vx_{06} - vx_{10} - 80 \leq 0 \ \wedge \ vx_{07} - vx_{11} \leq 0 \ \wedge \ vx_{08} - vx_{12} \leq 0 \ \wedge \ vx_{09} - vx_{13} \leq 0$$
$$\wedge \ -vx_{22} + vx_{23} + vx_{24} + vx_{25} = 0 \ \wedge \ -43vx_{22} + 100vx_{26} = 0 \ \wedge$$
$$vx_{22} - 500 \leq 0 \ \wedge \ -5vx_{23} + 7vx_{36} \leq 0 \ \wedge$$
$$-43vx_{28} - 43vx_{29} - 39vx_{30} - 37vx_{31} + 100vx_{38} = 0 \ \wedge$$
$$vx_{28} + vx_{29} + vx_{30} + vx_{31} - vx_{36} + vx_{37} + vx_{39} - 44 = 0 \ \wedge$$
$$vx_{28} - vx_{32} - 500 \leq 0 \ \wedge \ vx_{29} - vx_{33} \leq 0 \ \wedge \ vx_{30} - vx_{34} \leq 0 \ \wedge$$
$$vx_{31} - vx_{35} \leq 0 \ \wedge$$
$$2364vx_{10} + 2386vx_{11} + 2408vx_{12} + 2429vx_{13} - 1000vx_{25} + 2191vx_{32}$$
$$+2219vx_{33} + 2249vx_{34} + 2279vx_{35} \leq 0$$
$$\wedge \ -1000vx_{03} + 109vx_{22} \leq 0 \ \wedge$$
$$-1000vx_{15} + 109vx_{28} + 108vx_{29} + 108vx_{30} + 107vx_{31} \leq 0 \ \wedge$$
$$301vx_{01} - 1000vx_{24} \leq 0 \ \wedge$$
$$301vx_{06} + 313vx_{07} + 313vx_{08} + 326vx_{09} - 1000vx_{37} \leq 0 \ \wedge$$
$$vx_{04} + vx_{26} - 310 \leq 0 \ \wedge \ vx_{16} + vx_{38} - 300 \leq 0 \ \wedge$$
$$10vx_{02} + 8vx_{14} + 15vx_{23} + 12vx_{36} - 250vx_{39} + 25z \geq 0)$$
$$\frac{-10vx_{02} - 8vx_{14} - 15vx_{23} - 12vx_{36} + 250vx_{39}}{25}$$

Output:

$$\{\{(875z + 406659 \geq 0 \ \wedge \ 70000z + 31917303 \leq 0), \{z = \frac{-406659}{875}, vx_{01} = 80,$$
$$vx_{22} = 500, vx_{23} = \frac{11898}{25}, vx_{06} = 80, vx_{09} = 0, vx_{08} = 0, vx_{07} = 0, vx_{10} = 0,$$
$$vx_{11} = 0, vx_{12} = 0, vx_{14} = \frac{255}{14}, vx_{02} = \frac{51}{2}, vx_{24} = \frac{602}{25}, vx_{13} = 0, vx_{28} = 0,$$
$$vx_{31} = 0, vx_{32} = 0, vx_{29} = 0, vx_{33} = 0, vx_{30} = 0, vx_{34} = 0, vx_{35} = 0,$$
$$vx_{36} = \frac{11898}{35}, vx_{37} = \frac{13438}{35}, vx_{03} = \frac{109}{2}, vx_{04} = \frac{424}{5}, vx_{15} = \frac{865}{14},$$

$vx_{16} = \frac{424}{5}, vx_{25} = 0, vx_{26} = 215, vx_{38} = 0, vx_{39} = 0\}, \frac{-406659}{875}\}\}$

Time: 762025 ms plus GC time: 8194 ms

Example 5: Find the minimum point of $q = 3x^2 + 3y^2 - 2xy$ under the constraints $P = \{-x - y + u \geq 0,\ x - v \geq 0,\ y - v \geq 0\}$ in dependence of the parameters u, v.
Input:
$\exists x \exists y (u - x - y \geq 0 \ \wedge \ -v + x \geq 0 \ \wedge \ -v + y \geq 0) \ \ 3x^2 - 2xy + 3y^2$
Output (consisting of triplets giving conditions on the parameters, coordinates of possible minimum points of q w.r.t. the constraints, and the corresponding value of q):
$\{\{u - 2v \geq 0, \{x = v, y = v\}, 4v^2\},$
$\{u - 2v \geq 0, \{x = u - v, y = v\}, 3u^2 - 8uv + 8v^2\},$
$\{u - 2v \geq 0, \{x = \frac{u}{2}, y = \frac{u}{2}\}, u^2\},$
$\{(u - 4v \geq 0 \ \wedge \ v \geq 0), \{x = 3v, y = v\}, 24v^2\},$
$\{(3u - 4v \geq 0 \ \wedge \ v \leq 0), \{x = v, y = \frac{v}{3}\}, \frac{8v^2}{3}\},$
$\{(3u - 4v \geq 0 \ \wedge \ u - 4v \geq 0), \{x = \frac{3u}{4}, y = \frac{u}{4}\}, \frac{3u^2}{2}\},$
$\{(u \geq 0 \ \wedge \ v \leq 0), \{x = 0, y = 0\}, 0\}\}$
Time: 85 ms

Example 6: This example is taken from [12]. Find the minimum point of

$$q = \frac{x_1^2 - 2x_1x_2 - 6x_1 + 2x_2^2 - 8x_2}{2}$$

under the constraints

$$P = \{2x_1 + x_2 + x_3 = 6 \ \wedge \ -x_1 + x_2 + x_4 = 5 \ \wedge \ x_1 \geq 0 \ \wedge \ x_2 \geq 0 \ \wedge \ x_3 \geq 0 \ \wedge \ x_4 \geq 0\}.$$

Input:
$\exists x_1 \exists x_2 \exists x_3 \exists x_4 (2x_1 + x_2 + x_3 = 6 \ \wedge \ -x_1 + x_2 + x_4 = 5 \ \wedge \ x_1 \geq 0 \ \wedge \ x_2 \geq 0 \ \wedge$
$x_3 \geq 0 \ \wedge \ x_4 \geq 0)$
$\frac{x_1^2 - 2x_1x_2 - 6x_1 + 2x_2^2 - 8x_2}{2}$
Output:
$\{\{true, \{x_1 = \frac{25}{13}, x_2 = \frac{28}{13}, x_3 = 0, x_4 = \frac{62}{13}\}, \frac{-313}{26}\}\}$
Time: 68 ms

7. References

1. E. Becker, T. Woermann, On the trace formula for quadratic forms, *Contemporary Mathematics* **Vol. 155**, 1994, pp. 271-291.
2. T. Becker, V. Weispfenning, *Gröbner Bases*, Springer Verlag, 1993.

3. R. Benedetti, J.-J. Risler, *Real algebraic and semi-algebraic sets*, Hermann, 1990.
4. M. Ben-Or, D. Kozen, J. Reif, The complexity of elementary algebra and geometry, *J. Comp. System. Sciences* **32** (1986), pp. 251-264.
5. W. Böge, R. Gebauer, H. Kredel, Some examples for solving algebraic equations by calculating Gröbner bases, *J. Symb. Comp.* **1** (1986), pp. 83-98.
6. S.-C. Chou, *Mechanical Geometry Theorem Proving*, Reidel, 1988.
7. G.E. Collins, H. Hong, Partial cylindrical algebraic decomposition for quantifier elimination, *Journal of Symbolic Computation* **12** (1991), pp. 299-328.
8. D. Cox, J. Little, D. O'Shea, *Ideals, Varieties, and Algorithms*, Springer Verlag, Undergraduate Texts in Mathematics, 1992.
9. G.B. Dantzig, B.C. Eaves, Fourier-Motzkin elimination and its dual, *Journal of Combinatorial Theory*, Series A 14 (1973), pp. 288-297.
10. A. Dolzmann, *Reelle Quantorenelimination durch parametrisches Zählen von Nullstellen*, Diplomarbeit, Universität Passau, 1994.
11. B.C. Eaves, U.G. Rothblum, *Formulation of linear problems and solution by a universal machine*, Mathematical Programming, to appear.
12. R.F. Gabasov, F.M. Kirillova, *Methods for optimization*, Optimization Software Inc. Publications, New York, 1988.
13. X.S. Gao, S.C. Chou, Computing with parametric equations, *ISSAC'91*, S.M. Watt Ed., pp. 122-127.
14. L. Gonzales-Vega, A combinatorial algorithm solving some quantifier elimination problems, *Proc. Collins Symposium Linz*, Oct. 1993, to appear.
15. L Gonzales-Vega, H. Lombardi, T. Recio, M.-F. Roy, Strum-Habicht sequence, determinants and real roots of univariate polynomials, *Proc. Collins Symposium Linz*, Oct. 1993, to appear.
16. H. G. Graebe, On factorized Gröbner bases, these Proceedings.
17. D. Yu. Grigor'ev, Complexity of quantifier elimination in the theory of ordinary differential equations, *EUROCAL '87*, J.H. Davenport, Ed., Springer LNCS **Vol. 378**, pp. 11-25.
18. H. Hong, Quantifier elimination for formulas constrained by quadratic equation, *The Computer Journal* **36, 5** (1993), pp. 440-449.
19. M. Kappert, *Eliminationsverfahren zur linearen und quadratischen Optimierung*, Diplomarbeit, Universität Passau, 1994.
20. D. Lazard, A new method for solving algebraic systems of positive dimension, *Discrete Applied Math.* **33** (1991), pp. 147-160.
21. D. Lazard, Solving zero-dimensional algebraic systems, *J. Symb. Comp.* **13** (1992), pp. 117-131.
22. F. Lippold, *Implementierung eines Verfahrens zum Zählen reeller Nullstellen multivariater Polynome*, Diplomarbeit, Universität Passau, 1993.
23. R. Liska, S. Steinberg, Applying quantifier elimination to stability analysis of difference schemes, *The Computer Journal* **36** (1993), pp. 497-509.
24. R. Loos, V. Weispfenning, Applying linear quantifier elimination, *The Computer Journal* **36** (1993), pp. 450-462.

25. H. Melenk, H.M. Möller, W. Neun, Symbolic solution of large sationary chemical kinetics problems, *Impact of Computing* **1** (1989), 138-167.
26. B. Mishra, *Algorithmic Algebra*, Springer Verlag, 1993.
27. A. Morgan, *Solving polynomial systems using continuation for engineering and scientific problems*, Prentice Hall Inc., Englewood Cliffs, New Jersey, 1987.
28. P. Pedersen, M.-F. Roy, A. Szpirglas, Counting real zeros in the multivariate case, in Computational Algebraic Geometry, *Proc. MEGA'92*, F. Eyssette, A. Galligo, Eds., Birkhäuser Boston 1993, pp. 203-224.
29. J. Renegar, Recent progress on the complexity of the decision problem for the reals, *DIMACS series in discrete math. and theor. comp. science* **6** (1991), pp. 287-308.
30. W.Y. Sit, A theory for parametric linear systems, *ISSAC'91*, S.M. Watt Ed., pp. 112-121.
31. V. Weispfenning, The complexity of linear problems in fields, *Journal of Symbolic Computation* **5** (1988), pp. 3-27.
32. V. Weispfenning, Comprehensive Gröbner bases, *J. Symb. Comp.* **14** (1991), 1-29.
33. V. Weispfenning, A new approach to quantifier elimination for real algebra, *Proc. Collings Symposium Linz*, Oct. 1993, to appear.
34. V. Weispfenning, *Quantifier elimination for real algebra – the quadratic case and beyond*, preprint, Nov. 1993.
35. V. Weispfenning, Quantifier elimination for real algebra – the cubic case, *Proc. ISSAC'94*, Oxford, 1994, ACM Press.
36. V. Weispfenning, *Parametric linear and quadratic optimization by elimination*, Preprint MIP-9404, Universität Passau, April 1994.
37. A. Yu. Zharkov, Yu. A. Blinkov, Involution approach to solving systems of algebraic equations, *Proc. IMACS'93*, 1993, pp. 11-16.