Surface Parametrisation without Diagonalisation

Christiaan van de Woestijne
Institut für Mathematik B
Technische Universität Graz
8010 Graz, Austria
cvdwoest@opt.math.tu-graz.ac.at

ABSTRACT

For rationally fibred surfaces over $\mathbb{Q}$ and also over $\mathbb{R}$, an effective algorithm exists that decides if such a surface has a proper parametrisation. This algorithm uses a diagonalised form of the surface equation. We show, using recent algorithms for quadratic forms, that diagonalisation is not necessary. The resulting algorithm only uses operations on polynomials (as opposed to rational functions), which keeps all occurring degrees small and avoids spurious factors in the discriminant.

Categories and Subject Descriptors

F.2.1 [**Numerical Algorithms and Problems**]: Computations on matrices

General Terms

Algorithms,Design

Keywords

Quadratic forms, Rational surfaces, Parametrisation

1. INTRODUCTION

We consider the problem of computing a proper parametrisation of a rationally fibred surface. Such parametrisations are of obvious use in applications that must give a graphical presentation of a surface, seen as a subset of three-dimensional space; they give much easier access to the points on the surface than the defining equations of the surface usually do.

A *rationally fibred surface* is an algebraic surface S together with a rational map $\phi : S \to \mathbb{P}^1$ such that the generic fibre is an irreducible curve of genus zero. This definition is taken from J. Schicho's paper [4], which uses the equivalent name *surface with a rational pencil*. We would like to refer to this paper for further background on rationally fibred surfaces.

Implicit in the definition is the base field K over which the surface is defined. If K is the field of real or complex numbers, then computations on the surface will always encounter rounding errors and numerical analysis has to be used to bound these errors. If, instead, the field K admits exact arithmetic, then exact computations on the surface are possible; here, one thinks of the rational numbers $\mathbb{Q}$, an algebraic number field, or a finite field. The computations in this paper are generally independent of the base field, with the possible exception of fields of characteristic 2.

A special case of parametrisation is the case where the surface S is really isomorphic (over the base field K) to the two-dimensional plane over K. In this case, there exists a so-called *proper* parametrisation, i.e., there exist dominant rational maps $\phi : \mathbb{P}^2 \to S$ and $\psi : S \to \mathbb{P}^2$ that are inverses to each other; and the surface S is then called *rational*.

The cited paper [4] develops an algorithm for deciding whether a rationally fibred surface defined over $\mathbb{Q}$ is rational over $\mathbb{Q}$, and if it is, to compute a proper parametrisation. This is done by changing the defining equations of S in such a way that S is defined by one ternary quadratic form f over the function field $\mathbb{Q}(t)$, and then minimising the discriminant of this quadratic form. After this, one computes the *minimal index* of the defining equation, in order to decide if a parametrisation exists and which form it takes. The minimal index is a positive integer and at least the property of having minimal index greater or equal to 4 is a geometric invariant of the surface. A definition in terms of the surface equation is given in Section 4.

To do the minimisation, it is conceptually easy to *diagonalise* the form f, i.e., applying a change of variables so that f takes the form

$$D_0(t)x_0^2 + D_1(t)x_1^2 + D_2(t)x_2^2 \qquad (1)$$

for certain D_0, D_1, and D_2 in $K(t)$. For example, the discriminant of the form is now simply equal to $D_0D_1D_2$. However, as shown by examples in [4], the actual minimisation destroys again the diagonal form of the equation.

There are more disadvantages attached to the use of diagonalisation. Over $\mathbb{Q}(t)$, the coefficients D_i could easily get large denominators, also increasing the size of the discriminant of the equation when denominators are cleared. Keeping the discriminant as small as possible is particularly relevant if in the end the parametrisation problem must be solved by computing a zero of a quadratic form over $\mathbb{Q}$, as happens in some cases [4, Section 3].

When performing the computation over $\mathbb{R}$ or $\mathbb{C}$, the diagonalisation is a potential source of numerical instability,

ISSAC'06, July 9–12, 2006, Genova, Italy.
Copyright 2006 ACM 1-59593-276-3/06/0007 ...$5.00.

and it would be useful to be able to avoid it. The reason for this is that after diagonalisation we clear denominators, and hence these denominators will appear as square factors of the discriminant.

We present a modified version of Schicho's algorithm, using techniques developed by D. Simon [6] for discriminant reduction on non-diagonal quadratic forms. The techniques in [6] are only given for forms over $\mathbb{Z}$; we show how they can be applied when the form is defined over a polynomial ring. We also show how to compute the degree defect of the form when it is not diagonal; this allows us to replace many basis reductions (in the form of module Gröbner basis computations), in [4], by one final basis reduction.

Acknowledgements. The author acknowledges the hospitality of the Johann Radon Institute of the Austrian Academy of Sciences during the preparation of this paper. He would also like to thank Josef Schicho for helpful discussions and the referees for helpful references.

2. FINDING A SECTION

Let S be a rationally fibred surface over a field K; let $\phi : S \to \mathbb{P}^1$ denote its fibration map. We will assume that K does not have characteristic 2. By [4, Section 1], we may assume that S is given by an irreducible quadratic form

$$f = \sum_{0 \leq i,j \leq 2} a_{ij}(t) x_i x_j \qquad (2)$$

with coefficients a_{ij} in the polynomial ring $K[t]$. The coefficient matrix $A = [a_i j]_{ij}$ of f gives rise to the *discriminant* $\operatorname{disc} f$ of f, which is defined to be $\det(A)$. The discriminant is also a polynomial in t; we are only interested in $\operatorname{disc} f$ up to multiplication with scalars from K.

A parametrisation of S is obtained from a *section* of the fibration map ϕ, or equivalently, a *nontrivial zero* of the form f. Namely, consider the curve $\{f = 0\}$ in the projective plane $\mathbb{P}^2$ over $K(t)$, and let $\mathbf{x} = (x_0 : x_1 : x_2) \in \mathbb{P}^2(K(t))$ be a point on the curve. Then we can parametrise *all zeros* of f over $K(t)$ using the classical method of projecting lines from $\mathbf{x}$ in all directions and computing the second point of intersection of those lines with the curve $\{f = 0\}$. This parametrisation of the curve $\{f = 0\}$ has coefficients over $K(t)$; we now let t run over all elements of K to obtain a surface parametrisation.

The different cases that may arise from the index computation are as follows [4, Section 3]. If the index is either 0 or 2, the problem of finding a section is reduced to the solution of a ternary or a quaternary quadratic form over the base field K. The index cannot be 1; in the case of index 3, a parametrisation can be given without further computation; and for index 4 or higher, no proper parametrisation exists, as shown by results of Iskovshikh (quoted in [4]).

We want to comment on the case of index 0 or 2, when the base field is $\mathbb{Q}$. The problem of finding zeros of quadratic forms over $\mathbb{Q}$ has been long studied. Theoretically, the case of ternary forms was solved by Lagrange, who reduced the problem to the case of diagonalised forms (see [1]). The cited paper [6] gives a very efficient approach to the ternary case, by avoiding diagonalisation and hence the need to factor large integers. A preprint by the same author [5] handles the case of quaternary forms.

3. DISCRIMINANT MINIMISATION

In order to simplify the task of finding a zero of f, we try to make the *degree* of $\operatorname{disc} f$ as low as possible. This is done by looking at the irreducible factors of $\operatorname{disc} f$ one by one and seeing if they are removable. If a factor g is removable, then we can compute a change of variables, of determinant g or g^2, such that all coefficients of f become divisible by g; we divide f by g, and the factor is gone.

Diagonalisation. The classical Gram-Schmidt process gives us a matrix $T \in \mathrm{GL}(3, K(t))$ such that $A' = T^* A T$ is diagonal (here the star * denotes the transpose matrix), and hence $f(Tx)$ is of the form (1). As Lemma 1 of [4] shows, the use of the diagonal form of f makes the removal of squared factors from the discriminant easy.

However, the removal of *single* factors from $\operatorname{disc} f$ brings f in a non-diagonal form again, and this cannot be circumvented (see Example 5 in [4]). Besides, diagonalisation does not work over a field of characteristic 2. Finally, the diagonalisation process introduces denominators, as we have the following well-known relations, where the D_i are as in (1).

Lemma 3.1 *For $i = 0, \ldots, 2$, we have*

$$D_i = \frac{\det\left([a_{kl}]_{0 \leq k,l \leq i}\right)}{\det\left([a_{kl}]_{0 \leq k,l \leq i-1}\right)}.$$

If we now want to bring equation (1) back in a form with polynomial coefficients only by clearing denominators, then the determinants of the minor matrices of A will enter into these coefficients, and will therefore enter twice into the discriminant of f. Later on, we must remove these factors again.

There is one interesting aspect about diagonalisation that must be kept in mind. Depending on the base field, it is possible for one of the minor determinants of A to be zero. If this is the case, the Gram-Schmidt process cannot continue, and a diagonalisation must be found in another way (this more general process is known as Lagrange orthogonalisation). However, for our purposes this situation is very interesting, since if $D_i = 0$ while $D_{i-1} \neq 0$, it shows that the subform of f given by the variables $x_0, \ldots, x_i$ is *degenerate*, making it trivial to find a zero to f: just find a vector $(x_0, \ldots, x_i)$ in the kernel of the upper left ith minor of A, and then $(x_0, \ldots, x_i, 0, \ldots, 0)$ will be the desired zero of f.

An alternative approach. Having discussed the advantages and disadvantages of diagonalisation from an algebraic viewpoint, we now present an alternative approach to the minimisation of the discriminant that does not assume a diagonal form for f. The details of this approach are due to D. Simon for quadratic forms over $\mathbb{Z}$ (see [6]); we carry them over here to forms with coefficients in the polynomial ring $K[t]$. The method uses only linear algebra over the base field K, hence the results of this section would also be applicable if K would have characteristic 2.

Let g be an irreducible factor of $\operatorname{disc} f$. The first proposition shows that we can assume that all entries in the first row and column of A are divisible by g.

Proposition 3.2 *Let A be a $n \times n$-matrix over $K[t]$, and let g be an irreducible divisor of* $\det A$. *There exists an efficient deterministic algorithm that computes $U \in \mathrm{GL}(K[t])$ and $d \geq 0$ such that* *(i) the kernel of A modulo g has dimension d;*

(ii) the first d columns of U contain a basis of this kernel modulo g;

(iii) the entries in the $(n-k)$th column of U have degree at most $k \deg g$.

Proof. Algorithm 2.2 from [6] does exactly this, if everywhere $\mathbb{Z}$ is replaced by $K[t]$ and the prime number p is replaced by the irreducible polynomial g. The content of the algorithm is to reduce the matrix A modulo g, to transform this matrix over the field $K[t]/(g)$ by means of elementary column operations so that its first d columns are 0 and the others are linearly independent, and finally to lift the operations done over $K[t]/(g)$ to $K[t]$ and applying them to the matrix A. Because Algorithm 2.2 applies only elementary column operations on A, it is clear that U has determinant ± 1. □

Now because A is symmetric and AU has its first d columns divisible by g, we can assume that U^*AU has its first d columns and rows divisible by g. Let v_g denote the g-adic valuation on $K[t]$, i.e., for a polynomial $h \in K[t]$, $v_g(h)$ equals the number of factors g contained in h.

Lemma 3.3 *If $v_g(\operatorname{disc} f) = v$, and d is $\dim\ker(A \pmod g))$, then we have $v \geq d$.*

Proof. Obvious, because every row or column that is divisible by g adds a factor of g to the determinant. □

We first show that removal of repeated factors of $\operatorname{disc} f$ is easy.

Proposition 3.4 *Let A be a symmetric 3×3-matrix over $K[t]$, and let g be an irreducible polynomial in $K[t]$ such that g^2 divides $\det A$.*

(i) Assume that $\dim\ker(A \pmod g)) = 1$. Then there exists a 3×3-matrix T over $K[t]$ such that T^*AT/g^2 has entries in $K[t]$ and determinant $\det A/g^2$.

(ii) Assume that $\dim\ker(A \pmod g)) \geq 2$. Then there exists a 3×3-matrix T over $K[t]$ such that T^*AT/g has entries in $K[t]$ and determinant $\det A/g$.

In both situations, the matrix T can be efficiently computed.

Proof. Let U be the matrix given by the algorithm of Proposition 3.2 applied to A. Then the matrices

$$T = U\begin{pmatrix}1 & 0 & 0\\ 0 & g & 0\\ 0 & 0 & g\end{pmatrix} \text{ and } T = U\begin{pmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & g\end{pmatrix}$$

respectively, are the desired transformation matrices. In the first case, we use the fact that the top left element of A^*UA is divisible by g^2. □

Of course, if $\dim\ker(A \pmod g))$ turns out to be 3, the entire matrix A is divisible by g and we can trivially remove 3 factors g from $\det A$. Note also that the matrices given in the proof above correspond to the operations done in the proof of Lemma 1 of [4].

Proposition 3.5 *Let A be a symmetric 3×3-matrix over $K[t]$. Let g be an irreducible polynomial in $K[t]$ dividing $\det A$ exactly once, and such that the quadratic form defined by the matrix A factors modulo g. Then there exists a 3×3-matrix T over $K[t]$ such that T^*AT/g has entries in $K[t]$ and determinant $\det A/g$.*

Proof. This is Theorem 4 in [4]. Note that the proof given there works as stated in the non-diagonal case as well. □

As already indicated in [4, Remark 3], a simple factor g of $\operatorname{disc} f$ is removable if and only if the form f has a nontrivial zero in the *completion* of $K(t)$ with respect to the valuation defined by g. Such a nontrivial zero immediately leads to a factorisation of f modulo g, and vice versa, since f is degenerate modulo g. This proves the following result.

Theorem 3.6 *Let A be a symmetric 3×3-matrix over $K[t]$, where K is any field. Then there exists a 3×3-matrix T over $K[t]$ such that*

$$T^*AT = DA'$$

where D divides $\det A$ and $\det A'$ is squarefree and of minimal degree. The matrix T is efficiently computable, if we can compute efficiently in K.

4. THE DEGREE DEFECT

After we know the minimal degree of $\operatorname{disc} f$ that can be obtained by changing variables in f, we must minimise the *degree defect* of f by suitably weighing the variables x_i. This is done by a simple method that replaces the rather elaborate computations done in [4] for keeping the degree defect small. A degree defect of 0 or 1 can always be accomplished, and is enough for computing the minimal index of the surface. See also [4, Section 2] for the algebraic background, using weighted homogenisation of the equation (2), of the degree defect.

A *grading* W of the variables x_0, x_1, x_2 of f is a triple (w_0, w_1, w_2) of integers. We allow gradings with zero or negative components.

Definition 4.1 Let W be a grading of the variables of f.

(i) The *degree* of f with respect to W is

$$\deg_W(f) = \max_{i,j}(\deg a_{ij} + w_i + w_j).$$

(ii) The *degree defect* of f with respect to W is

$$\operatorname{def}_W(f) = 3\deg_W(f) - \deg\operatorname{disc} f - 2(w_0 + w_1 + w_2).$$

(iii) The *index* of f with respect to W is

$$\begin{aligned}\operatorname{ind}_W(f) &= \deg\operatorname{disc} f + \operatorname{def}_W(f)\\ &= 3\deg_W(f) - 2(w_0 + w_1 + w_2).\end{aligned}$$

From the definition, it follows that the degree, degree defect, and index are unchanged when we replace W by $W + k(1,1,1)$ for an integer k. Therefore, we may assume that one of the weights is 1 and that the others are at least 1. Also, because we have

$$\deg\operatorname{disc} f \leq 3\deg_W(f) - 2(w_0 + w_1 + w_2)$$

by properties of the determinant, we see that $\mathrm{def}_W(f) \geq 0$ for all W.

Now the existence and properties of a proper parametrisation of the surface S given by f over $K(t)$ depend on the index of f with respect to a suitable weight vector; in fact, we want the index to be as small as possible. This follows from the description of the possible cases in [4]; in particular, if $\mathrm{ind}_W(f) \geq 4$ for all gradings W, then no proper parametrisation for S exists over K, and we conclude that S is not rational over K.

By the definition, the minimal index is obtained by choosing W such that the degree defect is as small as possible; in fact, if diagonalisation is allowed, Schicho has showed that it is possible to have the defect at most 1 [4, Lemma 1]. To achieve the same goal for general forms, we may need to *reduce* the form f: if the matrix of f has off-diagonal entries whose degree exceeds the degrees of some diagonal entries, we will not be able to find a grading for which the degree defect is at most 1.

The reduction theory of quadratic forms is classical and has a large body of results. For a form given by a symmetric matrix $A = [a_{ij}]$, the property of being *reduced (in the sense of Hermite)* means that a_{11} has minimal size among all elements represented by the quadratic form, a_{ii} is not greater than a_{jj} if $i < j$, and a_{ij} is smaller than a_{ii} if $j > i$. The meaning of the term "smaller" varies with the base ring of the form. E.g., for forms over the integers, we use the ordinary absolute value for comparing elements. For forms over polynomial rings, we use the *degree* as a measure.

It turns out that the task of computing a reduced basis for a quadratic form over the integers is NP-complete; this holds in particular for finding the minimal element represented by the form, or, equivalently, for finding the shortest vector in a $\mathbb{Z}$-lattice. Therefore, many approximative concepts have been introduced, the most famous being LLL-reduction.

For forms over polynomial rings, the situation is much easier.

Theorem 4.2 *Let A be a symmetric $n \times n$-matrix with entries in $K[t]$. Then one can compute a matrix U with determinant in K^* such that U^*AU is reduced, using polynomially many operations in K.*

Proof. In fact, an algorithm for computing a reduced basis is given in [7]; Exercise 16.12 has an explicit algorithm. Another algorithm is given in Section 8 of [3]. The number of base ring operations used by these algorithms is polynomial in the dimension and in the maximum degree of the components of A.

We note that the algorithms just cited operate on a the basis vectors of a lattice such that the ordinary inner product, evaluated on this basis, gives the Gram matrix A. In fact, this means that $A = B^*B$, where B contains the basis vectors as columns. In our situation, we only have the Gram matrix, and it is not always possible to represent A in the form B^*B. However, both algorithms only apply elementary row and column operations to the basis matrix, and these are easily translated into operations on the Gram matrix: adding c times row i to row j corresponds to adding c times row i to row j, *and* adding c times column i to column j. Exchanging rows i and j corresponds to exchanging rows i and j, *and* columns i and j. □

It is also possible (in the ternary case) to obtain a reduced form by using the algorithms given in [2]. One needs to apply the necessary modifications, in order to translate the algorithms into the language of polynomials instead of integers. This also gives a polynomial time algorithm, in terms of operations in the base ring.

Theorem 4.3 *Let A be a symmetric 3×3-matrix over $K[t]$, such that the form f specified by A is reduced. Then there exists a grading W of the variables of f such that $0 \leq \mathrm{def}_W(f) \leq 1$.*

Proof. For any weight vector W, we define the weighted degrees $\deg_W(a_{ij})$ by

$$\deg_W(a_{ij}) = \deg a_{ij} + w_i + w_j.$$

By Definition 4.1 above, we have

$$\deg_W(f) = \max_{i,j}\{\deg_W(a_{ij})\}.$$

For the case where A is diagonal, a grading satisfying the requirements of the Theorem is given in Lemma 1 of [4]. If $\deg(a_{00}), \deg(a_{11}), \deg(a_{22})$ are all even, then set $w_i = -\deg(a_{ii})/2$. If they are all odd, set $w_i = -(\deg(a_{ii})-1)/2$. If one of the three, say $\deg(a_{00})$, is even and the others are odd, then set $w_0 = -\deg(a_{00})/2$ and $w_i = -(\deg(a_{ii})-1)/2$ for $i = 1, 2$. If $\deg(a_{00})$ is odd and the others are even, then set $w_0 = -(\deg(a_{00})+1)/2$ and $w_i = -\deg(a_{ii})/2$ for $i = 1, 2$. (If negative weights are undesirable, we can add a multiple of $(1, 1, 1)$ to W without changing the degree defect and the index.)

We now have $\deg_W(a_{ii}) \in \{-1, 0, 1\}$ in all cases, and the Theorem follows for diagonal A by simple verifications. One would have liked to take $w_i = \lfloor -\frac{\deg a_{ii}}{2} \rfloor$ in all cases, but this gives rise to a degree defect of 2 when exactly one of the $\deg a_{ii}$ is even.

Now assume A is reduced, but not necessarily diagonal. Let f be the form given by A. We recall that we have

$$\deg a_{ii} \leq \deg a_{jj} \text{ if } i < j,$$
$$\deg a_{ij} < \deg a_{ii} \text{ if } j > i.$$

From this, it follows directly that $\deg \det A = \deg a_{00} + \deg a_{11} + \deg a_{22}$. We use the same weight vectors as in the diagonal case, and therefore we are done if we show that

$$\deg_W(a_{ij}) < \deg_W(a_{ii}) \quad \text{if} \quad j > i. \qquad (3)$$

Namely, this means that both $\deg \det A$ and $\deg_W(f)$ only depend on the degrees of the diagonal entries, and the Theorem follows as in the diagonal case.

We prove the claim (3). First, assume $\deg a_{ii}$ are all even. We find

$$\deg_W(a_{ij}) = \deg a_{ij} - \frac{\deg a_{ii}}{2} - \frac{\deg a_{jj}}{2} <$$
$$< 0 = \deg a_{jj} - 2\frac{\deg a_{jj}}{2} = \deg_W(a_{jj}).$$

The inequality follows directly from the reducedness properties given above.

Next, assume $\deg a_{00}$ (say) is odd and the others are even.

We give the case of a_{0j}. We have

$$\deg_W(a_{0j}) = \deg a_{0j} - \frac{\deg a_{00}+1}{2} - \frac{\deg a_{jj}}{2} <$$
$$< -1 = \deg a_{00} - 2\frac{\deg a_{00}+1}{2} = \deg_W(a_{00}),$$

because $\deg a_{0j}$ is smaller than both $\deg a_{00}$ and $\deg a_{jj}$.

All other inequalities follow in the same way. □

We give one example. Suppose the *degrees* of the a_{ij} are given by the matrix $\begin{pmatrix}2 & 1 & 0\\ 1 & 4 & 3\\ 0 & 3 & 7\end{pmatrix}$; notice that coefficients having these degrees define a reduced quadratic form. We assign the weight vector $w = (-1,-2,-4)$ by the rules given above; we add $(5,5,5)$ to it to get positive weights $(4,3,1)$. The matrix with components $\deg_W(a_{ij})$ now becomes $\begin{pmatrix}10 & 8 & 5\\ 8 & 10 & 7\\ 5 & 7 & 9\end{pmatrix}$, which shows that $\deg_W(f) = 10$. We compute the degree defect: we have $3\deg_W(f) - 2(w_0+w_1+w_2) = 14$ whereas $\deg \operatorname{disc} f = 2+4+7 = 13$; the difference, and thus the defect, equals 1, as desired.

This ends the description of the method of applying Schicho's algorithm to a non-diagonal form f.

5. CONCLUSION

This paper gives the principal ideas of parametrising a rationally fibred surface over a field K using only operations on polynomials, and avoiding using rational functions over K with nontrivial denominators. This is done by extending the essential concepts of the algorithm given in [4] to quadratic forms over $K[t]$ given by a not necessarily diagonal symmetric matrix over $K[t]$.

The complexity of this algorithm in terms of amounts of operations in K is polynomial in the maximal degree of the entries of the input matrix. The complexity in terms of bit operations remains to be investigated; this pertains to the size of the coefficients of the occurring polynomials.

The author plans to give full details of the algorithm constructed here, as well as an investigation of the coefficient growth, in a later paper.

6. REFERENCES

[1] J. W. S. Cassels. *Rational quadratic forms.* London Mathematical Society Monographs, vol. 13. Academic Press Inc., London, 1978.

[2] Friedrich Eisenbrand and Günter Rote. Fast reduction of ternary quadratic forms. In *Cryptography and lattices (Providence, RI, 2001)*, volume 2146 of *Lecture Notes in Comput. Sci.*, pages 32–44. Springer, Berlin, 2001.

[3] T. Mulders and A. Storjohann. On lattice reduction for polynomial matrices. *J. Symbolic Comput.*, 35(4):377–401, 2003.

[4] Josef Schicho. Proper parametrization of surfaces with a rational pencil. In *Proceedings of the 2000 International Symposium on Symbolic and Algebraic Computation (St. Andrews)*, pages 292–300 (electronic), New York, 2000. ACM.

[5] Denis Simon. Quadratic equations in dimensions 4, 5 and more. Preprint, 2005. URL: `http://www.math.unicaen.fr/~simon/maths/dim4.html`.

[6] Denis Simon. Solving quadratic equations using reduced unimodular quadratic forms. *Math. Comp.*, 74(251):1531–1543 (electronic), 2005.

[7] Joachim von zur Gathen and Jürgen Gerhard. *Modern computer algebra.* Cambridge University Press, Cambridge, second edition, 2003.