Near-Optimal Parameterization of the Intersection of Quadrics: III. Parameterizing Singular Intersections

Laurent Dupont, Daniel Lazard, Sylvain Lazard, Sylvain Petitjean

Near-Optimal Parameterization of the Intersection of Quadrics: III. Parameterizing Singular Intersections

Laurent Dupont [a], Daniel Lazard [b], Sylvain Lazard [a], Sylvain Petitjean [a]

[a] *LORIA (INRIA, CNRS, Nancy Université) and VEGAS project (INRIA Nancy - Grand Est), Nancy, France*

[b] *LIP6 (Université Paris 6, CNRS) and SALSA project (INRIA Paris-Rocquencourt), Paris, France*

Abstract

We conclude, in this third part, the presentation of an algorithm for computing an exact and proper parameterization of the intersection of two quadrics. The coordinate functions of the parameterizations in projective space are polynomial, whenever it is possible. They are also near-optimal in the sense that the number of distinct square roots appearing in the coefficients of these functions is minimal except in a small number of cases (characterized by the real type of the intersection) where there may be an extra square root.

Our algorithm builds on the classification of pencils of quadrics of $\mathbb{P}^3(\mathbb{R})$ over the reals presented in Part II and the type-detection algorithm that we deduced from this classification. Moreover, since the algorithm presented in Part I is near-optimal when the intersection is a non-singular quartic, we focus here on the case where the intersection is singular and present, for all possible real types of intersection, algorithms for computing near-optimal rational parameterizations. We also give examples covering all the possible situations, in terms of both the real type of intersection and the number and depth of square roots appearing in the coefficients of the parameterizations.

Key words: Intersection of surfaces, pencils of quadrics, curve parameterization, singular intersections.
1991 MSC: 51-04, 68U05, 68U07, 68W30

1. Introduction

We present here an algorithm for computing a proper parameterization of the intersection of two quadrics. This parameterization lives in projective space and its coordinate functions are polynomial, when such a parameterization exists. Furthermore, for each possible real type of

Email address: `Firstname.Lastname@loria.fr` (Laurent Dupont, Sylvain Lazard, Sylvain Petitjean), `Firstname.Lastname@lip6.fr` (Daniel Lazard).

URLs: `www.loria.fr/~dupont/` (Laurent Dupont), `www-calfor.lip6.fr/~dl/` (Daniel Lazard), `www.loria.fr/~lazard/` (Sylvain Lazard), `www.loria.fr/~petitjea/` (Sylvain Petitjean).

intersection, it is near-optimal, that is its coefficients of the polynomials admit at most one extra square root. In other words, the algorithm satisfies Theorem I.3. [1]

Our algorithm builds on the classification of pencils of quadrics of $\mathbb{P}^3(\mathbb{R})$ over the reals presented in Part II and the type-detection algorithm that we deduced from this classification. Moreover, we focus here on the case where the intersection is singular since, otherwise, the algorithm presented in Part I computes a near-optimal parameterization. We thus present here, for every possible type of real intersection, an algorithm that computes an optimal or a near-optimal parameterization of the intersection or, more precisely, of each of the algebraic components of the intersection. (Examples of parameterizations computed by our algorithm can be found in Dupont et al. (2005) and Lazard et al. (2006).)

Moreover, for every type of intersection for which the computed parameterization is not always optimal (that is, the coefficients of the parameterization may contain an unnecessary square root), we describe a test to determine whether a particular parameterization is optimal. This test always amounts to determining whether a conic contains a rational point, and finding such a rational point leads to an optimal parameterization. Table 1 presents a summary of the form of the parameterizations and the test to assert optimality in all cases. We also discuss, in conclusion, algorithms for computing rational points on conics.

For every type of real intersection, we also give worst-case examples of pairs of quadrics for which the maximum number of square roots is reached (best-case examples are given by the canonical forms of Section II.3). A more exhaustive list of examples for all possible degrees of extension fields [2] of the coefficients and all types of real intersections is presented in Dupont et al. (2005) (Table 2).

The rest of the paper is organized as follows. Section 2 recalls some notation and preliminaries. Section 3 gives near-optimal parameterization algorithms for all types of real intersection when the pencil is regular, *i.e.*, when it contains quadrics that are non-singular. Section 4 does the same for singular pencils.

2. Preliminaries

All quadrics considered in the paper are defined in real projective space $\mathbb{P}^3(\mathbb{R})$, *i.e.*, they are of the form $Q_S = \{\mathbf{x} \in \mathbb{P}^3(\mathbb{R}) \mid \mathbf{x}^T S\mathbf{x} = 0\}$ where S is a 4 by 4 real symmetric matrix. Recall that the inertia of a quadric Q_R is the pair of the numbers of positive and negative eigenvalues of R (in a decreasing order); the rank of Q_R is the one of R. Recall also that a quadric is said to be rational if it is defined by an implicit equation with rational coefficients; similarly for lines, planes, and conics. Also, a parameterization is said to be rational if its coordinate functions are polynomials with rational coefficients.

We consider two input rational quadrics Q_S and Q_T. Recall that the characteristic polynomial, $\mathcal{D}(\lambda,\mu)$, of the pencil $\{R(\lambda,\mu) = \lambda\, S + \mu\, T \mid (\lambda,\mu) \in \mathbb{P}^1(\mathbb{R})\}$ generated by S and T is the determinant of $R(\lambda,\mu)$. Note that, since Q_S and Q_T are rational, the coefficients of the characteristic polynomial are rational.

Recall that a point $\mathbf{p} \in \mathbb{P}^3(\mathbb{C})$ of a quadric Q_S is said to be singular if the gradient of $\mathbf{x}^T S\mathbf{x}$ is zero at $\mathbf{p}$, that is if $\mathbf{p}$ is in the kernel of S; note that the set of singular points of a quadric with real coefficients is, if not empty, either a real point, a real line, or a real plane. The quadric Q_S is said to be singular if it contains at least one singular point (which is equivalent to $\det S = 0$). In the following, we refer to a singular line of a quadric as a line whose points are all singular

[1] When reference is made to a section or result in another part of the paper, it is prefixed by the part number.

[2] Recall that, if $\mathbb{K}$ is a field extension of $\mathbb{Q}$, its *degree* is defined as the dimension of $\mathbb{K}$ as a vector space over $\mathbb{Q}$.

Segre string	real type of intersection	worst-case format of parameterization	worst-case optimality of parameterization
[1111]	non-singular quartic (see part I)	$\mathbb{Q}(\sqrt{\delta})[\xi, \sqrt{\Delta}]$, $\Delta \in \mathbb{Q}(\sqrt{\delta})[\xi]$	rational point on degree-8 surface
[112]	point	$\mathbb{Q}$	optimal
	nodal quartic	$\mathbb{Q}(\sqrt{\delta})[\xi]$	rational point on conic
[13]	cuspidal quartic	$\mathbb{Q}[\xi]$	optimal
[22]	cubic and non-tangent line	$\mathbb{Q}[\xi]$	optimal
[4]	cubic and tangent line	$\mathbb{Q}[\xi]$	optimal
[11(11)]	two points	$\mathbb{Q}(\sqrt{\delta})$	optimal
	conic	$\mathbb{Q}(\sqrt{\delta}, \sqrt{\mu})[\xi]$, $\mu \in \mathbb{Q}(\sqrt{\delta})$	optimal if $\sqrt{\delta} \notin \mathbb{Q}$ rational point on conic if $\sqrt{\delta} \in \mathbb{Q}$
	two non-tangent conics	$\mathbb{Q}(\sqrt{\delta}, \sqrt{\delta'})[\xi]$	$\mathbb{Q}(\sqrt{\delta'})$-rational point on $\mathbb{Q}(\sqrt{\delta'})$-conic
[1(21)]	point	$\mathbb{Q}$	optimal
	two tangent conics	$\mathbb{Q}(\sqrt{\delta})[\xi]$	optimal
[1(111)]	double conic	$\mathbb{Q}(\sqrt{\delta})[\xi]$	rational point on conic
[2(11)]	point	$\mathbb{Q}$	optimal
	conic and point	$\mathbb{Q}(\sqrt{\delta})[\xi]$	rational point on conic
	conic and two lines not crossing on the conic	$\mathbb{Q}(\sqrt{\delta})[\xi]$	rational point on conic
[(31)]	conic	$\mathbb{Q}[\xi]$	optimal
	conic and two lines crossing on the conic	$\mathbb{Q}(\sqrt{\delta})[\xi]$	optimal
[(11)(11)]	two points	$\mathbb{K}[\xi]$, degree $(\mathbb{K}) = 4$	optimal
	two skew lines	$\mathbb{K}[\xi]$, degree $(\mathbb{K}) = 4$	optimal
	four lines (skew quadrilateral)	$\mathbb{K}[\xi]$, degree $(\mathbb{K}) = 4$	optimal
[(22)]	double line	$\mathbb{Q}[\xi]$	optimal
	two simple skew lines cutting a double line	$\mathbb{Q}(\sqrt{\delta})[\xi]$	optimal
[(211)]	point	$\mathbb{Q}$	optimal
	two double concurrent lines	$\mathbb{Q}(\sqrt{\delta})[\xi]$	optimal
[1{3}]	conic and double line	$\mathbb{Q}[\xi]$	optimal
[111]	point	$\mathbb{Q}$	optimal
	two concurrent lines	$\mathbb{K}[\xi]$, degree $(\mathbb{K}) = 4$	optimal
	four concurrent lines	$\mathbb{K}[\xi]$, degree $(\mathbb{K}) = 4$	optimal
[12]	double line	$\mathbb{Q}[\xi]$	optimal
	two simple and a double concurrent lines	$\mathbb{Q}(\sqrt{\delta})[\xi]$	optimal
[3]	concur. simple and triple lines	$\mathbb{Q}[\xi]$	optimal
[1(11)]	point	$\mathbb{Q}$	optimal
	two concurrent double lines	$\mathbb{Q}(\sqrt{\delta})[\xi]$	optimal
[(21)]	quadruple line	$\mathbb{Q}[\xi]$	optimal
[11]	quadruple line	$\mathbb{Q}[\xi]$	optimal

Table 1. Ring of definition of the coordinates of the parameterization of each component of the intersection and optimality, in all cases where the real part of the intersection is 0- or 1-dimensional. $\delta, \delta' \in \mathbb{Q}$.

points of the quadric. Similarly, a point $\mathbf{p} \in \mathbb{P}^3(\mathbb{C})$ of a curve C defined by the implicit equations $Q_S = Q_T = 0$ is singular if the rank of the Jacobian matrix of C (the matrix of partial derivatives of Q_S and Q_T) is at most 1 when evaluated at $\mathbf{p}$. A curve is singular if it contains at least a singular point (in $\mathbb{P}^3(\mathbb{C})$). Recall that all quadric intersections are singular except for the smooth (or non-singular) quartics in $\mathbb{P}^3(\mathbb{C})$, which can be, in $\mathbb{P}^3(\mathbb{R})$, smooth quartics or the empty set. Finally, a pencil of quadrics $\{Q_{\lambda S+\mu T} \mid (\lambda, \mu) \in \mathbb{P}^1(\mathbb{R})\}$ is said to be regular if it contains a non-singular quadric, *i.e.*, the characteristic polynomial does not vanish identically; otherwise, the pencil is singular.

Recall that a quadric of rank 3 is called a (projective) cone; it is real if its inertia is $(2, 1)$; otherwise, its inertia is $(3, 0)$, it is called imaginary and has a unique real point (in $\mathbb{P}^3(\mathbb{R})$) which is its singular point. A quadric of rank 2 is a pair of planes; it is real if its inertia is $(1, 1)$; otherwise, its inertia is $(2, 0)$, it is called imaginary and its real points (in $\mathbb{P}^3(\mathbb{R})$) are its singular line, that is, the line of intersection of the two planes. A quadric of inertia $(1, 0)$ is called a double plane and is necessarily real.

In what follows, Q_R (assumed to be distinct from Q_S) refers to the intermediate quadric used to parameterize the intersection, C, of Q_S and Q_T as in the algorithm presented in Section I.4.2. Also, as in Step 3 of this algorithm, denote by Ω the equation in the parameters $\Omega : \mathbf{X}_R^T S \mathbf{X}_R = 0$, where $\mathbf{X}_R$ is the parameterization of Q_R. Denote also by C_Ω the curve zero-set of Ω. Recall that the parameterization of Q_R defines an isomorphism between C and the plane curve C_Ω. When C is singular, its genus is 0 so it can be parameterized by polynomial functions in projective space.

Our general philosophy is to use for Q_R a rational quadric of the pencil of smallest rank (rather than one of largest rank, in Part I). This will lead us to use repeatedly the results of Section I.6 on the optimality of parameterizations of projective quadrics and to parameterize cones without a rational point, cones with a rational point, pairs of planes, etc. As will be seen, this philosophy has the double advantage of (i) avoiding $\sqrt{\Delta}$ in all singular cases, and (ii) minimizing the number of radicals. As an additional benefit, it helps keep the size of the numbers involved in intermediate computations and in the final parameterizations to a minimum – see Lazard et al. (2006).

In the following, we often need to compute a parameterization of the intermediate quadric Q_R; this is achieved (as in Part I) by (i) computing a rational congruence transformation sending the quadric Q_R with rational coefficients into diagonal form using Gauss reduction of quadratic forms into sums of squares and (ii) by using the parameterizations of Table I.2.

Finally, recall that the discriminant of a quadric is the determinant of the associated matrix. In the following, we also call *discriminant of a pair of planes* Q_R the product ab where $ax^2 - by^2 = 0$ is the canonical equation of a pair of planes obtained from Q_R by a real rational congruence transformation; the discriminant is defined up to a rational square factor.

3. Parameterizing singular intersections: regular pencils

In this section, we present parameterization algorithms for all cases of singular intersections when the characteristic polynomial does not identically vanish (the pencil is regular). Information gathered in the type-detection phase (Part II) is used as input; we use, in particular, the information of Table II.1 but also some details of the classification of pencils over the reals. In each case, we study optimality issues and give worst-case examples.

Note that the parameterizations, computed in this section and the next one, are trivially proper (*i.e.*, injective almost everywhere). Indeed, for each component curve of degree d of the intersection (line, conic, cubic, singular quartic), we exhibit a parameterization whose coordinate functions are polynomials of degree d (by definition of the degree, the curve generically intersects a plane in d distinct complex points, corresponding to d complex parameters, hence every real point on the curve is generically parameterized by one parameter).

3.1. *Nodal quartic in* $\mathbb{P}^3(\mathbb{C})$, $\sigma_4 = [112]$

If we parameterize C using the generic algorithm (see Part I), we will not be able to avoid the appearance of $\sqrt{\Delta}$ because C_Ω (as C) is irreducible. However, since the intersection curve is singular, we know that $\sqrt{\Delta}$ is avoidable by Proposition I.18. We thus proceed differently.

3.1.1. *Algorithms*

Let λ_1 be the real and rational double root of the characteristic polynomial. Let Q_R be the rational cone associated with λ_1. As we have found in Section II.3, there are essentially two cases depending on the real type of the intersection.

Point. Q_R is an imaginary cone. The intersection is reduced to a point, which is the apex of Q_R. Since λ_1 is rational, this apex is rational (otherwise its algebraic conjugate would also be a singular point of the cone). Thus the intersection in this case is defined in $\mathbb{Q}$.

Real nodal quartic (with or without isolated singularity). Q_R is a real cone. Let P be a real rational congruence transformation sending $(0, 0, 0, 1)$ to the apex of Q_R. The parameterization

$$\mathbf{X}(u, v, s) = P\,(x_1(u, v), x_2(u, v), x_3(u, v), s)^T, \quad (u, v, s) \in \mathbb{P}^{\star 2}$$

of the cone (where $\mathbb{P}^{\star 2}$ is the quasi-projective space – see Table I.2) introduces a square root $\sqrt{\delta}$. Equation Ω in the parameters is $as^2 + b(u, v)s + c(u, v) = 0$, with a and the coefficients of b, c defined in $\mathbb{Q}(\sqrt{\delta})$. The nodal quartic passes through the vertex of Q_R and this point corresponds to the value $(u, v, s) = (0, 0, 1)$ of the parameters. Thus $a = 0$ and Ω is linear in s. Moreover, $b(u, v)$ and $c(u, v)$ do not have a common root $(u, v) \neq (0, 0)$ because Ω is irreducible since C is irreducible (see Fact I.19). Thus the solutions to Ω are such that $(u, v) = (0, 0)$ or $b(u, v) \neq 0$. Solving Ω in s thus leads to the parameterization of the quartic by the point $P\,(0, 0, 0, 1)^T$ and

$$\mathbf{X}(u, v) = P\,(b(u, v)x_1(u, v), b(u, v)x_2(u, v), b(u, v)x_3(u, v), -c(u, v))^T$$

with $(u, v) \in \mathbb{P}^1(\mathbb{R})$ such that $b(u, v) \neq 0$. Furthermore, note that, if $b(u, v) = 0$, then $\mathbf{X}(u, v) = P\,(0, 0, 0, 1)^T$ (since then $c(u, v) \neq 0$). So when the node of the quartic is not isolated, that is when $b(u, v) = 0$ for some $(u, v) \in \mathbb{P}^1(\mathbb{R})$, the quartic is parameterized by

$$\mathbf{X}(u, v) = P\,(b(u, v)x_1(u, v), b(u, v)x_2(u, v), b(u, v)x_3(u, v), -c(u, v))^T, \quad (u, v) \in \mathbb{P}^1(\mathbb{R}).$$

When the node of the quartic is isolated, *i.e.*, when $b(u, v) \neq 0$ for all $(u, v) \in \mathbb{P}^1(\mathbb{R})$, the quartic is parameterized by $\mathbf{X}(u, v)$ plus the point $P\,(0, 0, 0, 1)^T$ (the node). Note finally that the four coordinates of $\mathbf{X}(u, v)$ clearly live in $\mathbb{Q}(\sqrt{\delta})[\xi]$, where $\xi = (u, v)$.

3.1.2. *Optimality*

By Proposition I.14, if the cone Q_R contains a rational point other than its vertex, it can be parameterized with rational coefficients and thus the parameterization of the nodal quartic is defined over $\mathbb{Q}[\xi]$. Otherwise, the nodal quartic contains no rational point other than its singular point and thus admits no parameterization over $\mathbb{Q}[\xi]$. Therefore, testing whether $\sqrt{\delta}$ can be avoided in the parameterization of real nodal quartics (and computing a parameterization in $\mathbb{Q}[\xi]$) is akin to deciding whether Q_R has a rational point outside its singular locus (and computing such a point if any).

There are cases where $\sqrt{\delta}$ cannot be avoided. Examples of such cases are given by $x^2 + y^2 - 3z^2 = xw + z^2 = 0$ when the singularity is not isolated and by $x^2 + y^2 - 3z^2 = zw + x^2 = 0$ when the singularity is isolated. In both cases, the projective cone corresponding to the double root of the characteristic polynomial is the first quadric. By Proposition I.14, this cone has no rational point except its singular point and thus $\sqrt{\delta}$ cannot be avoided in the parameterization of the intersection.

3.2. Cuspidal quartic in $\mathbb{P}^3(\mathbb{C})$, $\sigma_4 = [13]$

The intersection in this case is always a real cuspidal quartic. As above, using the generic algorithm is not good idea: it would introduce an unnecessary and unwanted $\sqrt{\Delta}$.

We consider instead the cone Q_R associated with the real and rational triple root of the characteristic polynomial. The singular point of the quartic is the vertex $\mathbf{p}$ of Q_R. The intersection of Q_R with the tangent plane of Q_S at $\mathbf{p}$ consists of the double line tangent to C at the cusp. Since it is double, this line is necessarily rational. So we have a rational cone containing a rational line. Thus, by Theorem I.12, we can compute a rational parameterization of this cone.

So we are left with an equation $\Omega : as^2 + b(u,v)s + c(u,v) = 0$ whose coefficients are defined on $\mathbb{Q}$. As above, the apex of the cone, corresponding to $(u,v,s) = (0,0,1)$, is the singular point of the quartic and thus $a = 0$. Thus Ω can be solved rationally for s and the parameterization of the intersection is in $\mathbb{Q}[\xi], \xi = (u,v)$, which is optimal.

3.3. Cubic and secant line in $\mathbb{P}^3(\mathbb{C})$, $\sigma_4 = [22]$

The real intersection consists of a cubic and a line. The cubic and the line are either secant or skew in $\mathbb{P}^3(\mathbb{R})$. Note that the line of the intersection is necessarily rational, otherwise its algebraic conjugate would also belong to the intersection.

When the double roots of the characteristic polynomial are real and rational, the pencil contains two rational cones Q_{R_1} and Q_{R_2}. The line of C is the rational line joining the vertices of Q_{R_1} and Q_{R_2}. Also, the vertex of Q_{R_2} is a rational point on Q_{R_1}, and vice versa, so the two cones can be rationally parameterized (see Theorem I.12). We have, as before, that Ω is linear in s, because the line and the cubic intersect at the vertex of the cone, corresponding to $(u,v,s) = (0,0,1)$. But here the content of Ω in s is linear in (u,v) and it corresponds to the line of C. The cubic is found after dividing by this content and rationally solving for s. The parameterization of the cubic is defined in $\mathbb{Q}[\xi]$.

When the double roots of the characteristic polynomial are either complex conjugate (the cubic and the line are not secant) or real algebraic conjugate (the cubic and the line are secant), there exist quadrics of inertia $(2,2)$ in the pencil (by Theorems I.3 and I.5). We use here the generic algorithm of Part I: we first compute a quadric Q_R of inertia $(2,2)$ of the pencil through a rational point. Since C contains a rational line, the discriminant of this quadric is a square by Lemma I.21 and Q_R can be rationally parameterized by Theorem I.12. We then compute the equation Ω of bidegree $(2,2)$, which factors into two terms of degree 1 and 3 (by Fact I.19) which necessarily have bidegree $(1,0)$ and $(1,2)$ (and are thus easy to compute). These two terms are linear in one of the parameters and can thus be solved rationally, leading to parameterizations of the cubic and the line that are defined in $\mathbb{Q}[\xi]$.

3.4. Cubic and tangent line in $\mathbb{P}^3(\mathbb{C})$, $\sigma_4 = [4]$

The real intersection consists of a cubic and a tangent line. The line is necessarily rational, by the same argument as above. The characteristic polynomial has a real and rational quadruple root. To it corresponds a real rational projective cone. Since this cone contains a rational line, it can be rationally parameterized (by Theorem I.12). The rest is as in the cubic and secant line case when the two roots are rational. The parameterization of the cubic is defined in $\mathbb{Q}[\xi]$.

3.5. Two secant conics in $\mathbb{P}^3(\mathbb{C})$, $\sigma_4 = [11(11)]$

In this case, the characteristic polynomial has a double root corresponding to a rational pair of planes Q_R. There are several cases depending on the real type of the intersection.

Two points. The pair of planes Q_R is imaginary. Its rational singular line intersects any other quadric of the pencil in two points. So parameterize the line and intersect it with any quadric of the pencil having rational coefficients. A square root is needed to parameterize the two points if and only if the equation in the parameters of the line has irrational roots.

This situation can happen as the following example shows: $z^2 + w^2 = x^2 - 2y^2 + w^2 = 0$. Clearly, the two points are defined by $z = w = 0$ and $x^2 - 2y^2 = 0$ so they live in $\mathbb{Q}[\sqrt{2}]$.

One conic. In this case, the pair of planes is real, the pencil has no quadric of inertia $(2, 2)$ and only one of the planes of Q_R intersects the other quadrics of the pencil.

The algorithm is as follows. First parameterize the pair of planes and separate the two individual planes. Plugging the parameterization of each plane into the equation of Q_S gives two equations of conics in parameter space, with coefficients in $\mathbb{Q}(\sqrt{\delta})$ where δ is the discriminant of the pair of planes. The conics in parameter space correspond to the components of the intersection, thus one of these conics is real and the other is imaginary. Determine the real conic, that is the one with inertia $(2, 1)$, and parameterize it. Substituting this parameterization into the parameterization of the corresponding plane gives a parameterization of the conic of the intersection. The parameterization is in $\mathbb{Q}(\sqrt{\delta}, \sqrt{\mu})$, where δ is the discriminant of the pair of planes Q_R and $\sqrt{\mu}$ is the square root needed to parameterize the conic in parameter space, $\mu \in \mathbb{Q}(\sqrt{\delta})$.

If δ is not a square, the parameterization is optimal. Indeed, if the conic of the intersection had a real $\mathbb{Q}(\sqrt{\delta})$-rational point, the conjugate of that point would be on the conjugate conic which is not real. So such a point does not exist and the parameterization is optimal. If δ is a square, the parameterization is defined in $\mathbb{Q}(\sqrt{\mu})[\xi]$ with $\mu \in \mathbb{Q}$. By Proposition I.14, it is optimal if and only if the (rational) conic contains no rational point; moreover, testing if the parameterization is not optimal and, if so, finding an optimal parameterization is equivalent to finding a rational point on this rational conic.

The situation where δ is a square but the conic has no rational point (the field of the coefficients is of degree two) can be attained for instance with the following pair of quadrics: $(x - w)(x - 3w) = x^2 + y^2 + z^2 - 4w^2 = 0$. The two planes of the first quadric are rational. The plane $x - w = 0$ cuts the second quadric in the conic $x - w = y^2 + z^2 - 3w^2 = 0$. By Proposition I.14, this conic has no rational point, so $\sqrt{\delta}$ cannot be avoided and the parameterization of the conic is in $\mathbb{Q}(\sqrt{3})$.

A field extension of degree 4 is obtained with the following quadrics: $x^2 - 4xw - 3w^2 = x^2 + y^2 + z^2 - w^2 = 0$. The pair of planes is defined on $\mathbb{Q}(\sqrt{7})$, so, by the above argument, a field extension of degree 4 is unavoidable.

Two (secant or non-secant) conics. By contrast to the one conic case, the pencil now contains quadrics of inertia $(2, 2)$. But using the generic algorithm and factoring C_Ω directly in two curves of bidegree $(1, 1)$ can induce nested radicals. So we proceed as follows. First, find a rational quadric Q_R of inertia $(2, 2)$ through a rational point. This introduces one square root, say $\sqrt{\delta}$. Independently, factor the pair of planes, which introduces another square root $\sqrt{\delta'}$. Now plug the parameterization of Q_R in each of the planes. This gives linear equations in the parameters of Q_R which can be solved without introducing nested radicals. The two conics have a parameterization defined in $\mathbb{Q}(\sqrt{\delta}, \sqrt{\delta'})$.

Note that when the two simple roots of the characteristic polynomial are rational, an alternate approach is to parameterize one of the two rational cones of the pencil instead of a quadric of inertia $(2, 2)$, and then proceed as above.

In terms of optimality, $\sqrt{\delta'}$ cannot be avoided if the planes are irrational. As for the other square root, it can be avoided if and only if the conics contain a point that is rational in $\mathbb{Q}(\sqrt{\delta'})$ (by Proposition I.14 in which the field $\mathbb{Q}$ can be replaced by $\mathbb{Q}(\sqrt{\delta'})$); moreover, testing if this square root can be avoided and, if so, finding a parameterization avoiding it is equivalent to finding a $\mathbb{Q}(\sqrt{\delta'})$-rational point on this conic whose coefficients are in $\mathbb{Q}(\sqrt{\delta'})$. Note that, if $\sqrt{\delta'}$ is not rational and one of the conic contains a $\mathbb{Q}(\sqrt{\delta'})$-rational point, then the other conic also contains such a point (the conjugate point obtained by changing the sign of $\sqrt{\delta'}$).

All cases can occur. We illustrate this in the non-secant case. An extension of $\mathbb{Q}$ of degree 4 is needed to parameterize the intersection of the following pair: $x^2 - 33w^2 = y^2 + z^2 - 3w^2 = 0$. Indeed, $\sqrt{\delta'} = \sqrt{33}$ cannot be avoided. In addition, by Proposition I.17, $y^2 + z^2 - 3w^2 - 11x^2 = 0$ has no rational point on $\mathbb{Q}(\sqrt{33})$, thus its intersection with the plane $x = 0$, the conic $y^2 + z^2 - 3w^2 = 0$, also has no rational point on $\mathbb{Q}(\sqrt{33})$; hence the cone $y^2 + z^2 - 3w^2 = 0$ has no rational point on $\mathbb{Q}(\sqrt{33})$ except for its singular locus.

An extension field of degree 2 can be obtained by having conics without rational point, but living in rational planes, as in this example: $x^2 - w^2 = y^2 + z^2 - 3w^2 = 0$. It can also be attained by having conics living in non-rational planes but having rational points in the extension of $\mathbb{Q}$ defined by the planes: $x^2 - 3w^2 = y^2 + z^2 - 3w^2 = 0$. As can be seen, the points of coordinates $(\sqrt{3}, 0, \pm\sqrt{3}, 1)$ belong to the intersection. So the conic has a parameterization in $\mathbb{Q}(\sqrt{3})[\xi]$.

3.6. Two tangent conics in $\mathbb{P}^3(\mathbb{C})$, $\sigma_4 = [1(21)]$

Here, the characteristic polynomial has a real and rational triple root, corresponding to a pair of planes Q_R. The other (real and rational) root corresponds to a real projective cone. There are two types of intersection over the reals.

Point. The pair of planes is imaginary and its rational singular line intersects the cone in a double point, which is the only component of the intersection. This point is necessarily rational, otherwise its conjugate would also be in the intersection. One way to compute it is to parameterize the singular line, plug the parameterization in the rational equation of the cone and solve the resulting equation in the parameters.

Two real tangent conics. The pair of planes is real and each of the planes intersects the cone. The singular line of Q_R is tangent to the cone. As above, the point of tangency of the two conics is rational. So, by Proposition I.14, the cone has a rational parameterization and thus the conics have parameterizations with coefficients in the extension of $\mathbb{Q}$ defined by the planes. In other words, the conics have a parameterization defined in $\mathbb{Q}[\xi]$ or $\mathbb{Q}(\sqrt{\delta})[\xi]$, where δ is the discriminant of the pair of planes Q_R.

One situation where $\sqrt{\delta}$ cannot be avoided is the following: $x^2 - 2w^2 = xy + z^2 = 0$.

3.7. Double conic in $\mathbb{P}^3(\mathbb{C})$, $\sigma_4 = [1(111)]$

The characteristic polynomial has a real rational triple root, corresponding to a double plane.

To obtain the parameterization of the double conic, first parameterize the double plane. Then plug this parameterization in the equation of any other rational quadric of the pencil. This gives the rational equation of the conic (in the parameters of the plane). If the conic has a rational point, it can be rationally parameterized. Otherwise, one square root is needed.

One worst-case situation where a square root is required is the following: $x^2 = y^2 + z^2 - 3w^2 = 0$. By Proposition I.14, the second quadric (a cone) has no rational point outside its vertex. Thus the conic cannot be parameterized rationally.

3.8. Conic and two lines not crossing on the conic in $\mathbb{P}^3(\mathbb{C})$, $\sigma_4 = [2(11)]$

The characteristic polynomial has two double roots, corresponding to a cone and a pair of planes which is always real. The two roots are necessarily real and rational, otherwise the quadrics associated with them in the pencil would have the same rank. So both the cone and the pair of planes are rational. Also, the vertex of the cone lies on the pair of planes outside its singular line. Thus, by Proposition I.13, the discriminant of the pair of planes is a square and each individual plane has a rational parameterization. Over the reals, there are three cases.

Point. The projective cone is imaginary. The intersection is limited to its real vertex. Since the cone is rational, its vertex is rational.

Point and conic. The cone is now real. One of the planes cuts the cone in a conic living in a rational plane, the other plane cuts the cone in its vertex. The point of the intersection is this vertex and it is rational. To parameterize the conic of the intersection, plug the parameterization of the one plane that does not go through the vertex of the cone in another rational quadric. This gives a rational conic in the parameters of the plane. One square root is possibly needed to parameterize this conic. It can be avoided if and only if the conic has a rational point.

One example where the square root cannot be avoided is the following: $xw = y^2+z^2-3w^2 = 0$. By Proposition I.14, the projective cone has no rational point other than its vertex $(1, 0, 0, 0)$. So the conic $x = y^2 + z^2 - 3w^2 = 0$ has no rational point.

Two lines and conic. Again, the cone is real and one plane cuts it in a rational non-singular conic. But now the second plane, going through the vertex of the cone, further cuts the cone in two lines. The parameterization of the conic goes as above. To represent the lines, we plug the second plane in the equation of the cone and parameterize.

Note that if the lines are rational, then the cone contains a rational line and can be rationally parameterized. Since the conic is the intersection of this cone with a rational plane, it has a rational parameterization. So in that case all three components have parameterizations in $\mathbb{Q}[\xi]$. If the lines are irrational, it can still happen that the conic has a rational point and thus a rational parameterization.

We give examples for the three situations we just outlined. First, the pair $xy = y^2+z^2-w^2 = 0$ induces the rational lines $y = z \pm w = 0$ and the rational conic $x = y^2 + z^2 - w^2 = 0$ which contains the rational point $(0, 0, 1, 1)$ and can thus be rationally parameterized. Second, the pair of quadrics $xy = 2y^2 + z^2 - 3w^2 = 0$ intersects in the two irrational lines $y = z \pm \sqrt{3}w = 0$ and the conic $x = 2y^2 + z^2 - 3w^2 = 0$ which contains the rational point $(0, 1, 1, 1)$ so can be rationally parameterized. Finally, the lines and the conic making the intersection of the quadrics $xy = y^2 + z^2 - 3w^2 = 0$ cannot be rationally parameterized. Indeed, by Proposition I.14, the cone has no rational point outside the vertex $(1, 0, 0, 0)$, so the conic $x = y^2 + z^2 - 3w^2 = 0$ has no rational point.

3.9. Conic and two lines crossing on the conic in $\mathbb{P}^3(\mathbb{C})$, $\sigma_4 = [(31)]$

The characteristic polynomial has a real pair of planes Q_R corresponding to a real and rational quadruple root. The asymmetry in the sizes of the Jordan blocks associated with this root (the two blocks have size 1 and 3) implies that the individual planes of this pair are rational. The conic of the intersection is always real and the two lines (real or imaginary) cross on the conic.

There are two types of intersection over the reals.

Conic. The point at which the two lines cross is the double point that is the intersection of the singular line of Q_R with any other quadric of the pencil. This point is necessarily rational. So the conic can be rationally parameterized by Proposition I.14.

Conic and two lines. To parameterize the intersection, first compute the parameterization of the two planes of Q_R. Plugging these parameterizations in the equation of any other quadric of the pencil yields a conic on one side and a pair of lines on the other side. As above, the conic can be rationally parameterized. As for the two lines, they have a rational parameterization if and only if the discriminant of the pair of lines is a square.

One situation where this discriminant is not a square is: $yz = y^2 + xz - 2w^2 = 0$. The conic is given by $y = xz - 2w^2 = 0$ which contains the rational point $(1, 0, 0, 0)$ and can be rationally parameterized. The lines are defined by $z = y^2 - 2w^2 = 0$. But the pair of planes $y^2 - 2w^2 = 0$ has no rational point outside its singular locus so the lines are parameterized over $\mathbb{Q}(\sqrt{2})$.

3.10. Two skew lines and a double line in $\mathbb{P}^3(\mathbb{C})$, $\sigma_4 = [(22)]$

The characteristic polynomial has a real and rational quadruple root, which corresponds to a pair of planes. The singular line of the pair of planes is contained in all the quadrics of the pencil. There are two cases.

Double line. The pair of planes is imaginary. The intersection is reduced to the rational singular line of the pair of planes which can be parameterized in $\mathbb{Q}[\xi]$.

Two simple lines and a double line. The pair of planes is real. We can factor it into simple planes, parameterize these planes and plug them in any other quadric of the pencil. The two resulting equations in the parameters of the planes are pairs of lines, each pair containing the double line of the intersection and one of the simple lines. The double line can be parameterized, as before, in $\mathbb{Q}[\xi]$ and the simple lines can be parameterized in $\mathbb{Q}[\xi]$ or $\mathbb{Q}(\sqrt{\delta})[\xi]$, where δ is the discriminant of the pair of planes Q_R.

A situation where $\sqrt{\delta}$ is required is for $y^2 - 2w^2 = xy - zw = 0$.

3.11. Two double lines in $\mathbb{P}^3(\mathbb{C})$, $\sigma_4 = [(211)]$

The characteristic polynomial has a real rational quadruple root, which corresponds to a double plane. The double plane cuts any other quadric of the pencil in two double lines in $\mathbb{P}^3(\mathbb{C})$. There are two cases.

Point. Except for the double plane, the pencil consists of quadrics of inertia $(3, 1)$. The two lines are imaginary. The intersection is reduced to their rational intersection point, that is, the point at which the double plane is tangent to the other quadrics of the pencil.

Two real double lines. Except for the double plane, the pencil consists of quadrics of inertia $(2, 2)$. The two lines are real. To parameterize them, first compute a parameterization of the double plane and then plug it in any quadric of inertia $(2, 2)$ of the pencil. The resulting pair of lines can easily be parameterized. The intersection is thus parameterized with one square root if and only if the lines are irrational.

One case where the square root cannot be avoided is as follows: $w^2 = x^2 - 2y^2 + zw = 0$. The lines $w = x^2 - 2y^2 = 0$ have no rational point except for their singular point $(0, 0, 1, 0)$ so their parameterization is in $\mathbb{Q}(\sqrt{2})[\xi]$.

3.12. Four lines forming a skew quadrilateral in $\mathbb{P}^3(\mathbb{C})$, $\sigma_4 = [(11)(11)]$

We start by describing the algorithms we use in this case. We then prove the optimality of the parameterizations and conclude the section by giving examples of pairs of rational quadrics for all possible types of real intersections and extension fields.

3.12.1. Algorithms

In this case the characteristic polynomial has two double roots that correspond to (possibly imaginary) pairs of planes. It can be written in the form $\mathcal{D}(\lambda, \mu) = \gamma \left(a\lambda^2 + b\lambda\mu + c\mu^2\right)^2 = 0$, with γ, a, b, and c in $\mathbb{Q}$.

In order to minimize the number and depth of square roots in the coefficients of the parameterization of the intersection, we proceed differently depending on the type of the real intersection and the values of $\gamma \neq 0$ and $\delta = b^2 - 4ac \neq 0$.

Note that the roots of the characteristic polynomial are defined in $\mathbb{Q}(\sqrt{\delta})$ and thus the coefficients of the pairs of planes in the pencil also live in $\mathbb{Q}(\sqrt{\delta})$. Let $d^+, d^- \in \mathbb{Q}(\sqrt{\delta})$ be the discriminants of the two pairs of planes. If $\delta > 0$, we suppose $d^+ > d^-$. In this case, if $d^+ > 0$ (resp. $d^- > 0$), the corresponding pair of planes is real and can be factored into two planes that are defined over $\mathbb{Q}(\sqrt{d^+})$ (resp. $\mathbb{Q}(\sqrt{d^-})$). The algorithms in the different cases are as follows.

Two points. In this case one pair of planes of the pencil is real (the one with discriminant d^+) and the other is imaginary. We factor the two real planes and substitute in each a parameterization of the (real) singular line of the imaginary pair of planes. The singular line is defined in $\mathbb{Q}(\sqrt{\delta})$ and each of the real planes are defined in $\mathbb{Q}(\sqrt{d^+})$. We thus obtain the two points of intersection with coordinates in $\mathbb{Q}(\sqrt{\delta}, \sqrt{d^+})$. The two points are thus defined over $\mathbb{Q}(\sqrt{d^+})$, $d^+ \in \mathbb{Q}(\sqrt{\delta})$, an extension field of degree 4 (in the worst case) with one nested square root.

Two or four lines. Since the intersection is contained in every quadric of the pencil, there are no quadric of inertia $(3, 1)$ in the pencil in this case (such quadrics contain no line) and thus $\gamma > 0$. Furthermore all the non-singular quadrics of the pencil have inertia $(2, 2)$ (by Theorem I.5) and their discriminant is equal to γ, up to a square factor (they are of the form $\gamma\left(a\lambda^2 + b\lambda\mu + c\mu^2\right)^2$). Hence we can parameterize a quadric Q_R of inertia $(2, 2)$ in the pencil using the parameterization of Table I.2 with coefficients in $\mathbb{Q}(\sqrt{\gamma})$ (see Section I.4.2). There are three sub-cases.

$\boldsymbol{\sqrt{\delta} \in \mathbb{Q}}$. The roots of the characteristic polynomial are real (since $\delta > 0$), thus the intersection consists of four real lines and the two pairs of planes of the pencil are real (see Table II.1). We factor the two pairs of planes into four planes with coefficients in $\mathbb{Q}(\sqrt{d^\pm})$ and intersect them pairwise. We thus obtain a parameterization of the four lines over $\mathbb{Q}(\sqrt{d^+}, \sqrt{d^-})$ with $d^\pm \in \mathbb{Q}$ (since δ is a square), an extension field of degree 4 (in the worst case) with no nested square root.

$\boldsymbol{\sqrt{\delta} \notin \mathbb{Q}}$ ***and*** $\boldsymbol{\sqrt{\gamma\delta} \in \mathbb{Q}}$. Here again $\delta > 0$ thus the intersection consists of four real lines and the two pairs of planes are real. We factor one of these pairs of planes (say the one with discriminant d^+) in two planes with coefficients in $\mathbb{Q}(\sqrt{d^+})$; if the discriminant of one of the pairs of planes is a square, we choose this pair of planes for the factorization. We then substitute the parameterization of the quadric Q_R into each plane. This leads to an equation of bidegree $(1, 1)$ in the parameters with coefficients in $\mathbb{Q}(\sqrt{d^+}, \sqrt{\gamma})$. This field is equal to $\mathbb{Q}(\sqrt{d^+})$ because $d^+ \in \mathbb{Q}(\sqrt{\delta})$ and $\gamma\delta$ is a square. We finally obtain each line by factoring the equation in the parameters into two terms of bidegree $(1, 0)$ and $(0, 1)$ and by substituting the solutions of these factors into the parameterization of Q_R. We thus obtain a parameterization of the four lines defined over $\mathbb{Q}(\sqrt{d^+})$, $d^+ \in \mathbb{Q}(\sqrt{\delta})$, an extension field of degree 4 (in the worst case) with one nested square root.

$\boldsymbol{\sqrt{\delta} \notin \mathbb{Q}}$ ***and*** $\boldsymbol{\sqrt{\gamma\delta} \notin \mathbb{Q}}$. In this case we apply the generic algorithm of Part I: we substitute the parameterization of Q_R into the equation of another quadric of the pencil (with rational coefficients). The resulting equation in the parameters of bidegree $(2, 2)$ has coefficients in $\mathbb{Q}(\sqrt{\gamma})$. We factor it into two terms of bidegree $(2, 0)$ and $(0, 2)$, whose coefficients also live in $\mathbb{Q}(\sqrt{\gamma})$. We solve each term separately and each real solution leads to a real line. At least one of the two factors has two real solutions, which are defined in an extension field of the form $\mathbb{Q}(\sqrt{\alpha_1 + \alpha_2\sqrt{\gamma}})$, $\alpha_i \in \mathbb{Q}$. If the other factor has real solutions, they are defined in $\mathbb{Q}(\sqrt{\alpha_1 - \alpha_2\sqrt{\gamma}})$. Thus in the case where the intersection consists of two real lines, we obtain parameterization defined over an extension field $\mathbb{Q}(\sqrt{\alpha_1 + \alpha_2\sqrt{\gamma}})$ of degree 4 (in the worst case), with one nested square root. In the case where the intersection consists of four real lines, the parameterization of the four lines altogether is defined over an extension field of degree 8 (in the worst case) but each of the lines is parameterized over an extension $\mathbb{Q}(\sqrt{\alpha_1 + \alpha_2\sqrt{\gamma}})$ or $\mathbb{Q}(\sqrt{\alpha_1 - \alpha_2\sqrt{\gamma}})$ of degree 4 (in the worst case), with one nested square root.

3.12.2. Optimality

We prove that the algorithms described above output parameterizations that are always optimal in the number and depth of square roots appearing in their coefficients. This proof needs some considerations of Galois theory. (A short primer on Galois theory in the context of geometric objects can be found in Dupont et al. (2005), Appendix A.)

The two input quadrics intersect here in four lines in $\mathbb{P}^3(\mathbb{C})$. The pencil contains two (possibly complex) pairs of planes and the four lines are the intersections between two planes taken in two different pairs of planes. Let $\mathbf{p}_1, \ldots, \mathbf{p}_4$ be the pairwise intersection points of the four lines. These points are the singular points of the intersection. They are also the intersections of the singular line of a pair of planes with the other pair of planes, and vice versa. Let the points be numbered such that $\mathbf{p}_1$ and $\mathbf{p}_3$ are on the singular line of one pair of planes; $\mathbf{p}_2$ and $\mathbf{p}_4$ are then on the singular line of the other pair of planes of the pencil. The four lines of intersection are thus $\mathbf{p}_1\mathbf{p}_2$, $\mathbf{p}_2\mathbf{p}_3$, $\mathbf{p}_3\mathbf{p}_4$, and $\mathbf{p}_4\mathbf{p}_1$. We now consider how the symmetries of the quadrilateral with vertices $\mathbf{p}_1, \ldots, \mathbf{p}_4$ act when this quadrilatere is a rectangle, a lozenge or a square.

Let $\mathbb{K}$ be the field extension of $\mathbb{Q}$ of smallest degree on which the four points $\mathbf{p}_i$ are rational. The above algorithms show that $\mathbb{K}$ has degree 1, 2, 4 or 8 (since two rational lines in $\mathbb{K}$ intersect in a rational point in $\mathbb{K}$). Let G be the Galois group of $\mathbb{K}$, which acts by permutations on the points $\mathbf{p}_i$. It follows that G is a subgroup of the dihedral group D_4 of order 8 of the symmetries of the square. This group D_4 acts on the four points $\mathbf{p}_i$ and on the lines joining them the way the 8 isometries of a square act on its vertices and edges. We show that the optimal number of square roots needed for parameterizing the four lines and the way this optimal number is reached only depend on G and on its action on the $\mathbf{p}_i$.

The eight elements of D_4 are the identity, the transpositions τ_{13} and τ_{24} which exchange $\mathbf{p}_1$ and $\mathbf{p}_3$ or $\mathbf{p}_2$ and $\mathbf{p}_4$ (symmetries with respect to the diagonal), the permutation $\tau_{12,34}$ (resp. $\tau_{14,23}$) of order 2 which exchanges $\mathbf{p}_1$ with $\mathbf{p}_2$ and $\mathbf{p}_3$ with $\mathbf{p}_4$ (resp. $\mathbf{p}_1$ with $\mathbf{p}_4$ and $\mathbf{p}_2$ with $\mathbf{p}_3$), the circular permutations ρ and ρ^{-1} of order 4, and the permutation $\rho^2 = \tau_{13}\tau_{24} = \tau_{12,34}\tau_{14,23}$ of order 2.

If G is included in the group $G_{\mathcal{L}}$ of order 4 generated by τ_{13} and τ_{24} (symmetries of the lozenge), its action leaves fixed the pairs $\{\mathbf{p}_1, \mathbf{p}_3\}$ and $\{\mathbf{p}_2, \mathbf{p}_4\}$ and thus also the lines $\mathbf{p}_1\mathbf{p}_3$ and $\mathbf{p}_2\mathbf{p}_4$ and the two singular quadrics of the pencil (the two pairs of planes). It follows that the roots of the characteristic polynomial $\mathcal{D}$ are rational. Conversely, if these roots are rational, the singular quadrics and their singular lines are invariant under the action of G, as well as the pairs $\{\mathbf{p}_1, \mathbf{p}_3\}$ and $\{\mathbf{p}_2, \mathbf{p}_4\}$, which implies that G is included in $G_{\mathcal{L}}$. A similar argument shows that G is the identity (resp. is generated by τ_{13} (or τ_{24}), or contains $\tau_{13}\tau_{24}$), if and only if 0 (resp. 1 or 2) of the singular quadrics consist of irrational planes. Moreover, in the case where G contains $\tau_{13}\tau_{24}$, the group is different from $G_{\mathcal{L}}$ if and only if any element which exchanges $\mathbf{p}_1$ and $\mathbf{p}_3$ also exchanges $\mathbf{p}_2$ and $\mathbf{p}_4$, *i.e.*, if and only if the conjugations exchanging the planes in each singular quadric are the same (implying that the square roots needed for factoring them are one and the same). As the degree of $\mathbb{K}$ is the order of G, this shows that the number of square roots needed in our algorithm is always optimal if the roots of $\mathcal{D}$ are rational (*i.e.*, δ is a square).

When the roots of $\mathcal{D}$ are not rational, we consider, in the algorithm, a rational quadric Q_R passing through a rational point $\mathbf{p}$. Let D be the line of Q_R passing through $\mathbf{p}$ and intersecting the lines $\mathbf{p}_1\mathbf{p}_2$ and $\mathbf{p}_3\mathbf{p}_4$; let $\mathbf{q}_1$ and $\mathbf{q}_2$ denote these intersection points. If the discriminant of Q_R is a square (and its parameterization is rational), then D is rational and is fixed by any Galois automorphism. It follows that the lines $\mathbf{p}_1\mathbf{p}_2$ and $\mathbf{p}_3\mathbf{p}_4$ are either fixed or exchanged, which implies that G is included in the group $G_{\mathcal{R}}$ of order 4 generated by $\tau_{12,34}$ and $\tau_{14,23}$ (symmetries of the rectangle). Conversely, if $G \subset G_{\mathcal{R}}$, the lines $\mathbf{p}_1\mathbf{p}_2$ and $\mathbf{p}_3\mathbf{p}_4$ are fixed or exchanged by any Galois automorphism; the image of D by such an automorphism is D itself or the other line of Q_R passing through $\mathbf{p}$; as this image contains the images of $\mathbf{q}_1$ and $\mathbf{q}_2$ which are on $\mathbf{p}_1\mathbf{p}_2$ or $\mathbf{p}_3\mathbf{p}_4$, we may conclude that D is fixed by any Galois automorphism, and is rational; this shows that the discriminant of Q_R is a square by Lemma I.21. Pushing these arguments a little more, it is easy to see that G is generated by $\tau_{12,34}$ or $\tau_{14,23}$ (or is the identity) if and only if the roots of either or both of the factors of bidegree $(2,0)$ and $(0,2)$ of Ω in the parameters are rational.

By similar arguments of invariance, we may also conclude that the group G is generated by the circular permutation ρ if and only if any Galois automorphism which exchanges the lines $\mathbf{p}_1\mathbf{p}_3$ and $\mathbf{p}_2\mathbf{p}_4$ exchanges also the lines of Q_R passing through $\mathbf{p}$ (if there is such an automorphism). It follows that this case occurs when the square root of the discriminant of Q_R and the roots of $\mathcal{D}$ generate the same field.

Finally, G is of order 8 if none of the preceding cases occur.

Optimality in all cases is proved by checking that, for each possible group, the algorithm involves exactly 0, 1 or 2 square roots for parameterizing the lines if the size of the orbit of a line is 1, 2 or 4 respectively.

3.12.3. Examples

Examples of pairs of rational quadrics for all possible types of real intersections and extension fields are given by $x^2 - \gamma y^2 - 2wz = \alpha x^2 + 2\gamma xy + \alpha\gamma y^2 - z^2 - (\alpha^2 - \gamma)w^2 = 0$, with $\alpha, \gamma \in \mathbb{Q}, \gamma \neq 0$. In particular, for $(\alpha,\gamma) = (3,3)$, it is straightforward to show that two lines of the intersection are defined in $\mathbb{Q}(\sqrt{6+2\sqrt{3}})$ and the other two lines are defined in $\mathbb{Q}(\sqrt{6-2\sqrt{3}})$. All the other cases of real intersection and extension fields are given for various values of (α,γ).[3] Note that we actually have that any pencil of rational quadrics whose characteristic polynomial has two double roots corresponding to two quadrics of rank 2 is generated, up to a rational change of coordinate system, by the two above quadrics (see Dupont et al. (2005)).

4. Parameterizing singular intersections: singular pencils

We now turn our attention to singular pencils. As in the previous section, the information gathered in the type-detection phase (Part II), and in particular Table II.2, is used as input.

4.1. Conic and double line in $\mathbb{P}^3(\mathbb{C})$, $\sigma_4 = [1\{3\}]$

As we have seen in Section II.4.1, the pencil contains in this case one pair of planes. Furthermore each of the planes is rational by Proposition I.13 because the pair of planes contains a rational point outside its singular locus (by Lemma II.7). One plane is tangent to all the cones of the pencil, giving a rational double line. The other plane intersects all the cones transversally, giving a conic. The conic contains a rational point (its intersection with the singular line of the planes), so it can be rationally parameterized.

To actually parameterize the line and the conic, we proceed as follows. If Q_S is a pair of planes, replace Q_S by $Q_S + Q_T$. Now, Q_S is a real projective cone whose vertex is on Q_T (Lemma II.7). Use this rational vertex to obtain a rational parameterization of Q_T. Plug this parameterization into the equation of Q_S. This equation in the parameters factors in a squared linear factor (corresponding to the double line) and a bilinear factor, corresponding to the conic. It can rationally be solved, leading to a parameterization of C defined in $\mathbb{Q}[\xi]$.

4.2. Four concurrent lines in $\mathbb{P}^3(\mathbb{C})$, $\sigma_3 = [111]$

We start by describing the algorithms and prove their optimality. We then discuss the degree of the extension of $\mathbb{Q}$ over which the parameterizations are defined.

[3] Namely, for $(5,9)$, $(3,5)$, $(5,16)$, $(6,20)$, $(2,2)$, $(3,1)$, $(2,1)$, $(3,25)$, $(1,4)$, $(1,3)$, $(0,-1)$, $(1,-3)$ and $(1,-2)$; for details, see Dupont et al. (2005).

4.2.1. Algorithms and optimality

In this case, the two quadrics Q_S and Q_T have a singular point, $\mathbf{p}$, in common and the intersection consists of $\mathbf{p}$ or two or four lines intersecting at $\mathbf{p}$ (see Table II.2).

We first compute the singular point $\mathbf{p}$ (for instance, by determining the intersection of the null spaces of the two matrices S, T). Point $\mathbf{p}$ has rational coordinates (since otherwise its conjugate would be in the intersection). If the intersection is not reduced to $\mathbf{p}$, we parameterize the lines of intersection as follows. Determine a plane $x = 0, y = 0, z = 0$, or $w = 0$, that does not contain $\mathbf{p}$ and substitute the equation of that plane (say $x = 0$) into the equations of Q_S and Q_T. This gives a system of two homogeneous degree-two equations in three variables having four distinct complex projective solutions $\mathbf{q}_i$. The real lines of C are then the two or four lines going through $\mathbf{p}$ and one of the $\mathbf{q}_i$ with real coordinates, $i = 1, \ldots, 4$.

This leads to an optimal parameterization of the lines of the intersection. Indeed, since $\mathbf{p}$ and the plane ($x = 0$) used to cut Q_S and Q_T are rational, the lines are rational if and only if their intersection with the plane (the points $\mathbf{q}_i$) are rational.

4.2.2. Degree of the extension

The following result shows that the roots of any polynomial of degree 4 without multiple root may be needed to parameterize four real concurrent lines.

Proposition 1. *For any rational univariate polynomial of degree 4 without multiple root, there are rational pencils of quadrics whose intersection is four (real or imaginary) concurrent lines, such that each of them is rational on the field generated by one of the roots of the polynomial and is not rational on any smaller field (for the inclusion and the degree).*

Proof. Consider the polynomial $f = t^4 + \alpha t^3 + \beta t^2 + \gamma t + \delta$ of degree 4 with rational coefficients and without multiple factors. Let $t_1, \ldots, t_4$ be its four distinct roots. The two quadrics $xz - y^2 = 0$ and $\delta x^2 + \gamma xy + \beta y^2 + \alpha yz + z^2 = 0$ are cones with vertex $(0, 0, 0, 1)$, which contain the four lines $(x = 1,\ y = t_i,\ z = t_i^2,\ w = 0)$, $i = 1, \ldots, 4$. Thus their intersection consists exactly in these four lines.

Each of these lines is clearly rational on the field generated by one of the t_i. It is not rational over a smaller field. In fact, if it where, the point of the line of coordinates $(1, t_i, t_i^2, 0)$ would be irrational over this field and the line would contain at least one of its conjugates, namely one of the other points $(1, t_i, t_i^2, 0)$, which is a contradiction. □

Section 4.2.1 and Proposition 1 imply that each line of the intersection is parameterized over an extension of $\mathbb{Q}$ of degree up to four. Note however that the parameterizations of the four lines may be globally defined over an extension of $\mathbb{Q}$ of higher degree; for instance, if the four roots $t_1, \ldots, t_4$ (in the proof of Proposition 1) are real, the degree of the extension of $\mathbb{Q}$ needed to parameterize the four lines together is the order of the Galois group of the degree-four polynomial f which is 1, 2, 3, 4, 6, 8, 12 or 24.

Note also that every of these extension degrees can be attained by considering the right polynomial $f = t^4 + \alpha t^3 + \beta t^2 + \gamma t + \delta$. For example, for $\alpha = \beta = 0$ and $\gamma = \delta = 1$, the intersection is four real concurrent lines that are globally defined on an extension of $\mathbb{Q}$ of degree 24 (since the Galois group of this specialization of f is the group S_4 of the permutations of four elements, which has order 24). As the polynomial is irreducible, each line is nonetheless defined in an extension of degree 4.

4.3. Remaining cases

In the remaining cases of Table II.2, the algorithms, if not trivial, are straightforward and amount to intersecting a double plane or pair of planes (real or imaginary) with another pair of planes, double plane, or cone whose apex lies on the singular line of the pair of planes (for more details, see Dupont et al. (2005)).

5. Conclusion

We have presented in Parts I, II, and III of this paper a new algorithm for computing an exact and proper parametric representation of the intersection of two quadrics in three-dimensional real space given by implicit equations with rational coefficients. We have shown that our algorithm computes projective parameterizations that are optimal in terms of the functions used in the sense that they are polynomials whenever it is possible and contain the square root of some polynomial otherwise. The parameterizations are also near-optimal in the sense that the number of square roots appearing in the coefficients of these functions is minimal except in a small number of cases (characterized by the real type of the intersection) where there may be an extra square root (see Table 1 for a summary). Furthermore, we have shown that, in the latter cases, testing whether the extra square root is unnecessary and, if so, finding an optimal parameterization are equivalent to finding a rational point on a curve or a surface. Hence, leaving for a moment that well-known problem aside, our algorithm closes the problem of finding parameterizations of the intersection that are optimal in the senses discussed above. It should be emphasized that our algorithm is not only theoretical but is also practical: a complete, robust and efficient C++ implementation is described in Lazard et al. (2006).

For most applications, the near-optimal parameterizations of intersections of quadrics computed by our algorithm are good enough since they are at most one square root away from being optimal. However, there may be situations where one is interested in fully asserting the optimality of a parameterization and, if a given parameterization is not optimal, in obtaining one. As we have seen, this is akin to deciding whether a given curve or surface has a rational point and to computing such a point. The problem of finding integer (or rational) points on an algebraic variety is known to be hard in general, and many instances of the problem are undecidable (Poonen, 2001). When the intersection is a smooth quartic, deciding whether the extra square root can be avoided amounts to finding a rational point on a surface of degree 8 (see Section I.7) and very little is known about this problem, to the best of our knowledge. The situation is, however, better for the other near-optimal cases, where finding an optimal parameterization amounts to finding a rational point on a conic whose coefficients are rational except in one case where the coefficients may be non-rational (when the intersection is two non-tangent conics). Several algorithms exist for finding a rational point on a conic with rational coefficients (Cremona and Rusin, 2003; Simon, 2005). We have implemented one of them, due to Simon (2005), which is based on a generalization of the LLL algorithm to quadratic forms that are not necessarily positive definite. Using this addition, our algorithm thus produces optimal parameterizations in all cases except when the intersection is a non-singular quartic or two non-tangent conics (see Table 1), cases for which the parameterization is sometimes only near-optimal.

References

Cremona, J., Rusin, D., 2003. Efficient solution of rational conics. Mathematics of Computation 72 (243), 1417–1441.

Dupont, L., Lazard, D., Lazard, S., Petitjean, S., Sept. 2005. Near-optimal parameterization of the intersection of quadrics: III. Parameterizing singular intersections. RR 5669, INRIA, 34 pp.

Lazard, S., Peñaranda, L. M., Petitjean, S., 2006. Intersecting quadrics: An efficient and exact implementation. Computational Geometry: Theory and Applications 35 (1-2), 74–99.

Poonen, B., 2001. Computing rational points on curves. In: Number Theory for the Millenium. A. K. Peters, Boston, pp. 149–172, proc. of Millennial Conference on Number Theory, 2000.

Simon, D., 2005. Solving quadratic equations using reduced unimodular quadratic forms. Math. Comp. 74 (251), 1531–1543.