LMS J. Comput. Math. 19 (Special issue A) (2016) 73–82
doi:10.1112/S146115701600022X

Effective Hasse principle for the intersection of two quadrics

Tony Quertier

Abstract

We consider a smooth system of two homogeneous quadratic equations over $\mathbb{Q}$ in $n \geqslant 13$ variables. In this case, the Hasse principle is known to hold, thanks to the work of Mordell in 1959. The only local obstruction is over $\mathbb{R}$. In this paper, we give an explicit algorithm to decide whether a nonzero rational solution exists and, if so, compute one.

1. *Introduction*

Let $F_1, \ldots, F_m$ be polynomials in the variables $x_1, \ldots, x_n$ with coefficients in $\mathbb{Q}$. In the study of the rational solutions of the system $F_1(x_1, \ldots, x_n) = \ldots = F_m(x_1, \ldots, x_n) = 0$, four very natural and well-studied problems are:

- LS (= local solutions): for a completion of $\mathbb{Q}$, decide if there exist solutions;
- ELS (= everywhere locally solvable): decide whether the system is everywhere locally solvable;
- HP (= Hasse principle): show that the property ELS implies the existence of a global solution in $\mathbb{Q}$;
- EGS (= efficient global solution): if solutions exist in $\mathbb{Q}$, give an efficient algorithm to compute one.

In this paper, we consider a smooth system of two homogeneous quadratic equations over $K = \mathbb{Q}$ in $n \geqslant 13$ variables. Before studying the case of two equations, it is worth recalling what is known in the case of a single quadratic equation.

Let $q(x_1, \ldots, x_n)$ be a homogeneous quadratic form over $\mathbb{Q}$ and $q(x_1, \ldots, x_n) = 0$ the associated quadratic equation. For $n \leqslant 4$, the LS question is usually solved by computation of the Legendre or Hilbert symbol. The Hasse–Minkowski theorem asserts that a quadratic form with $n \geqslant 5$ variables is ELS except maybe over $\mathbb{R}$ and that HP holds for a single quadratic equation for any $n > 1$.

To solve EGS, Simon [8] and Castel [2] have written algorithms that quickly compute an explicit rational solution of $q(x_1, \ldots, x_n) = 0$. Consequently, for a single quadratic equation, we consider the four problems solved and now focus on the case of two quadratic equations.

Let $q_0(x_1, \ldots, x_n)$, $q_1(x_1, \ldots, x_n)$ be two quadratic forms over $\mathbb{Q}$. Demyanov [4] and Birch *et al.* [1] solved ELS except over $\mathbb{R}$ for $n \geqslant 9$, and gave a way to compute such a p-adic solution. Many people have worked on the HP problem for two quadratic forms. Let us mention the most general results. Mordell settled the case $n \geqslant 13$ in 1959 [6]. His result was lowered to $n \geqslant 11$ by Swinnerton-Dyer in 1964 [9] and later to $n \geqslant 9$ by Colliot-Thélène *et al.* in 1987 [3]. In 2006, Wittenberg [10] proved that, if we assume Schinzel's hypothesis and the finiteness of Tate–Shafarevich groups of elliptic curves over number fields, then HP holds as soon as $n \geqslant 6$.

Received 16 February 2016.

2010 Mathematics Subject Classification 11D09, 11Y50 (primary).

Contributed to the Twelfth Algorithmic Number Theory Symposium (ANTS-XII), Kaiserslautern, Germany, 29 August–2 September 2016.

It is well known that there exists a real solution of such a system if and only if there is no form $\lambda q_0 + \mu q_1$ which is definite for λ, $\mu \in \mathbb{R}$. I am not aware of any algorithms that decide if a system has a real solution; then we give an explicit algorithm which makes it.

Assume now that we know that there exists a nonzero rational solution. We could use an exhaustive search by ascending height to find it. We can imagine a bound on the size of the smallest solution as a power of the size of the coefficients of the quadratic forms. Then, an exhaustive search would have an exponential complexity. To our knowledge, no work exists on the EGS problem for two quadratic equations. In this paper, we describe a complete algorithm including low-level steps to solve EGS for $n \geqslant 13$. A nonnegligible part of our work is based on [**6**]. We have to study more precisely the real precision necessary to the computation, but if we use the program of Castel [**2**] to compute a solution of a quadratic form, we suspect that the complexity of this program is polynomial.

The outline of the article is as follows. In § 2, we fix the notation and recall the notion of smoothness. In § 3, we study the different signatures of the forms in the pencil, which govern the existence of a real solution. This leads to a simple algorithm that decides the existence of a real solution. In § 4, we give some low-level algorithms to split off a quadratic form into hyperbolic planes over $\mathbb{R}$ or $\mathbb{Q}$. These rely on the ability to compute a solution for a single quadratic equation. Over $\mathbb{Q}$, as already mentioned, we may use the algorithm of Castel [**2**]. Section 5 is devoted to the computation of an explicit nontrivial real solution of the system. In § 6, using this real solution, we can construct a rational totally isotropic subspace for $q_0(x)$ such that $q_1(x)$ is indefinite over this subspace. In the last § 7, we use this subspace to derive a nontrivial rational solution of the system.

2. *General notation*

Let $K \supset \mathbb{Q}$ be a field. Let q_0 and q_1 be two quadratic forms over K in n variables. Using the canonical basis of K^n, we have $q_0(x) = \sum_{i,j=1}^{n} a_{ij}x_ix_j$ and $q_1(x) = \sum_{i,j=1}^{n} b_{ij}x_ix_j$ with $a_{ij} = a_{ji}$ and $b_{ij} = b_{ji}$. We write $Q_0 = (a_{ij})$, $Q_1 = (b_{ij})$, the associated symmetric matrices. For $x = (x_1, \ldots, x_n)$, we have $q_0(x) = xQ_0{}^t x$ and $q_1(x) = xQ_1{}^t x$. We also use the notation $q_0(x, y) = xQ_0{}^t y$ for the associated bilinear form.

Let $V_{q_0,q_1} = \{x \in \mathbb{P}^{n-1}(\overline{K}) \mid q_0(x) = q_1(x) = 0\}$ be the projective variety defined by the two quadrics associated to q_0 and q_1. To study the intersection of two quadrics, it is necessary to study the pencil of quadrics through V_{q_0,q_1}. We denote by $\mathcal{P}_K$ the pencil of quadrics associated to the pair (q_0, q_1), that is, the family of quadrics $a_0q_0 + a_1q_1 = 0$ with $(a_0 : a_1) \in \mathbb{P}^1(K)$. In practice, we will mainly consider this pencil for $K = \mathbb{Q}$ and $K = \mathbb{R}$. If $\det(Q_0) = 0$, we replace q_0 by $a_0q_0 + a_1q_1$ for some $(a_0 : a_1) \neq (0 : 1)$ to assure that $\det(Q_0) \neq 0$ and similarly for Q_1. From now on, we can set $\lambda = a_0/a_1$ and $\Delta(\lambda) = \det(\lambda Q_0 + Q_1)$: this is a polynomial of degree exactly n in λ.

Let q be a quadratic form in n variables and Q the associated matrix. Let P be a transition matrix such that $PQ({}^t P) = D$, where D is diagonal. We denote by $[r, s]$ the *signature* of Q, where r is the number of positive coefficients of D and s the number of negative coefficients of D. If $\det(Q) \neq 0$, we have $r + s = n$, otherwise we have $r + s < n$.

We denote by $\oplus$ the traditional *orthogonal sum* for quadratic forms. Moreover, for two matrices A and B, we define $A \oplus B$ as the block diagonal matrix $\left(\begin{smallmatrix} A & 0 \\ 0 & B \end{smallmatrix}\right)$.

The variety V_{q_0,q_1} is *smooth* if the rank of the Jacobian of q_0 and q_1 is equal to 2 at every point of V_{q_0,q_1}.

CONDITION 1. We say that two symmetric matrices Q_0 and Q_1, defined over K, satisfy the *condition* 1 if $\det(Q_0) \neq 0$, $\det(Q_1) \neq 0$, and V_{q_0,q_1} is smooth over K.

https://doi.org/10.1112/S146115701600022X Published online by Cambridge University Press

We know, for example from [5], that we have the equivalent formulation, as follows.

We say that two symmetric matrices Q_0 and Q_1, defined over K, satisfy the *condition* 1 if $\det(Q_0) \neq 0$, $\det(Q_1) \neq 0$, and $\Delta(\lambda)$ has only simple roots in $\overline{K}$.

3. *Real quadratic forms*

3.1. *Simultaneous diagonalization*

We will not talk about precision in the next sections. In practice, we set the precision to 10^{-38} and we run the program. If that is not enough we double the precision and restart the program.

PROPOSITION 3.1. *Let Q_0 and Q_1 be two symmetric matrices of size n satisfying condition* 1 *over $\mathbb{R}$. Let m be the number of real roots of $\Delta(\lambda)$. There exists a matrix $P \in \mathrm{GL}_n(\mathbb{R})$ such that $PQ_0({}^tP)$ is diagonal, with only ± 1 on the diagonal, and $PQ_1({}^tP)$ is a block diagonal matrix, with m first blocks of size* 1 *and then $(n-m)/2$ blocks of size* 2 *of the form $\left(\begin{smallmatrix} a & b \\ b & -a \end{smallmatrix}\right)$. Furthermore, each such block in $PQ_1({}^tP)$ is face to face with a block $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ in $PQ_0({}^tP)$. Algorithm* 1 *computes such a matrix P.*

ALGORITHM 1. Let Q_0 and Q_1 be two matrices of size n satisfying condition 1 over $\mathbb{R}$. This algorithm computes a matrix $P \in \mathrm{GL}_n(\mathbb{R})$ using floats satisfying the conclusion of Proposition 3.1.

(1) Let $\Delta(\lambda) = \det(\lambda Q_0 + Q_1)$ and $\Lambda = \{\lambda_1, \ldots, \lambda_n\}$ be the list of the roots of $\Delta(\lambda)$ such that $\lambda_1, \ldots, \lambda_m \in \mathbb{R}$ and $\lambda_{m+i} = \overline{\lambda_{m+i+1}}$ for $i \geqslant 1$ odd.

(2) For i from 1 to n, find a generator v_i of $\ker(\lambda_i Q_0 + Q_1)$ such that, for $i \leqslant m$, $v_i \in \mathbb{R}^n$.

(3) Set $j = m+1$. While $j < n$, set $w_j = \mathrm{Re}(v_j)$, $w_{j+1} = \mathrm{Im}(v_j)$, and $j = j+2$.

(4) For i from 1 to m, set $w_i = v_i$.

(5) Let P be the square matrix of size n whose the ith row is w_i for $1 \leqslant i \leqslant n$. Set $Q_0' = PQ_0({}^tP)$.

(6) For i odd from 1 to $n-m-1$, set $a = Q'_{m+i,m+i}$, $b = Q'_{m+i,m+i+1}$, and $\mu = \mathrm{sign}(b)\sqrt{a^2+b^2}$. Set $P'_{m+i} = \begin{pmatrix} \sqrt{(1+a/\mu)/2} & \sqrt{(1-a/\mu)/2} \\ \sqrt{(1-a/\mu)/2} & -\sqrt{(1+a/\mu)/2} \end{pmatrix}$.

(7) Set $P' = \mathrm{Id}(m) \oplus \bigoplus_i P'_{m+i}$. Set $Q_0'' = P'Q_0'({}^tP')$ and $P = P'P$.

(8) For i from 1 to n, divide the ith row of P by $\sqrt{|Q''_{0_{ii}}|}$.

(9) Return P.

Proof. In Step 2, the dimension of each kernel is 1 because $\Delta(\lambda)$ has only simple roots. We know that $v_i(\lambda_i Q_0) + v_i Q_1 = 0$; then we deduce easily that $q_0(v_i, v_j) = q_1(v_i, v_j) = 0$. Since the v_i are orthogonal for q_0 and q_1, the w_i are also pairwise orthogonal for q_0 and q_1, except maybe w_{m+i} and w_{m+i+1}, for i odd. The matrices Q_0' and Q_1' are therefore block diagonal with blocks of size 1 for each real root λ and of size 2 for each pair of conjugate complex roots. For i odd, from the equality $q_0(v_{m+i}, v_{m+i+1}) = 0$, we deduce $q_0(w_{m+i}, w_{m+i}) = -q_0(w_{m+i+1}, w_{m+i+1})$. So, the shape of the blocks of size 2 associated to conjugate complex roots is $\left(\begin{smallmatrix} a & b \\ b & -a \end{smallmatrix}\right)$. The same is true for Q_1'. In Step 8, we can easily check that $P'_{m+i}A_i({}^tP'_{m+i})$ is diagonal and P'_{m+i} is orthogonal. We have again that $\mathrm{trace}(P'_{m+i}A_i({}^tP'_{m+i})) = 0$ and then the shape of the blocks $P'_{m+i}A_i({}^tP'_{m+i})$ is always $\left(\begin{smallmatrix} a & 0 \\ 0 & -a \end{smallmatrix}\right)$. Similarly, the shape of the $P'_{m+i}B_i({}^tP'_{m+i})$ is $\left(\begin{smallmatrix} c & d \\ d & -c \end{smallmatrix}\right)$. At the level of blocks, Step 8 divides the two rows of P'_{m+i} by the same constant $|a|$; therefore, the trace of the blocks is always zero. □

https://doi.org/10.1112/S146115701600022X Published online by Cambridge University Press

3.2. *Existence of a balanced quadratic form*

DEFINITION 1. We say that a quadratic form with signature $[r, s]$ is *balanced* if $|r - s| \leqslant 1$.

In this section, we want to determine if a pair of quadratic forms has nontrivial real solutions. After this we study the existence of a balanced quadratic form in the pencil $\mathcal{P}_{\mathbb{R}}$ and compute one if it exists.

LEMMA 3.2 (Cauchy's bound). *Let $P(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0$ be a monic polynomial of degree n. If $x \in \mathbb{C}$ is a root of P, then $|x| \leqslant 1 + \max_{1\leqslant i\leqslant n}(|a_i|)$.*

The constant $a = 1 + \max_{1\leqslant i\leqslant n}(|a_i|)$ is called *Cauchy's bound* for P.

DEFINITION 2. We define the function $d : \mathbb{R} \to \mathbb{Z}$ by $d(\lambda) = r - s$, where $[r, s]$ is the signature of $\lambda q_0 + q_1$.

THEOREM 3.3. *Let Q_0 and Q_1 be two matrices of size n satisfying condition 1 over $\mathbb{R}$. The function d is piecewise constant with discontinuities at the real roots of $\Delta(\lambda)$. The value of d at a discontinuity is the average of the two limit values of d on the left and on the right of this discontinuity. Moreover, if λ is a real root of $\Delta(\lambda)$, we have $d(\lambda_i^-) = d(\lambda_i^+) \pm 2$.*

COROLLARY 3.4. *There exists $\lambda \in \mathbb{Q}$ such that $\lambda q_0 + q_1$ is balanced.*

Proof. Assume $d(-\infty) = -a$ and $d(\infty) = a$. As Q_0 and Q_1 satisfy condition 1, d is piecewise constant. Moreover, if λ_i is a real root of $\Delta(\lambda)$, we have $d(\lambda_i^-) = d(\lambda_i^+) \pm 2$. So, there exists an interval I such that $|d(b)| < 1$ for all b in I. □

It is convenient for the next lemma to use the notation $\lambda_0 = -\infty$ and $\lambda_{n+1} = +\infty$.

LEMMA 3.5. *Let Q_0 and Q_1 be two matrices of size n satisfying condition 1 over $\mathbb{R}$. Assume that $\Delta(\lambda)$ has $m \leqslant n$ real roots denoted by $\lambda_1 < \ldots < \lambda_m$. We have:*

(i) *if $m \neq n$, then $\lambda Q_0 + Q_1$ is never definite;*
(ii) *if $m = n$, there exists at most one interval $]\lambda_i, \lambda_{i+1}[$ over which $\lambda Q_0 + Q_1$ is positive definite. Moreover, this interval is $]\lambda_s, \lambda_{s+1}[$, where $[r, s]$ is the signature of Q_0.*

Proof. Assume $d(-\infty) = a$; then $d(\infty) = -a$. If there exists a real λ such that $\lambda Q_0 + Q_1$ is positive definite, then we have $d(\lambda) = n$. Because d changes by ± 2 through each λ_i, going from a to n requires at least $(n-a)/2$ steps and going from n to $-a$ requires at least $(n+a)/2$ steps. Since $(n-a)/2+(n+a)/2 = n$, we need exactly n real roots, otherwise λQ_0+Q_1 cannot be definite. The observation that $s = (n - a)/2$ gives the conclusion. For the case of negative definite, the proof is the same. □

THEOREM 3.6 [6, 9]. *Let q_0 and q_1 be two quadratic forms of n variables. Then $V_{q_0,q_1}(\mathbb{R}) \neq \emptyset$ if and only if all the forms in $\mathcal{P}_{\mathbb{R}}$ are indefinite.*

ALGORITHM 2. Let Q_0 and Q_1 be two matrices of size n satisfying condition 1 over $\mathbb{R}$. This algorithm computes a rational number λ such that $\lambda Q_0 + Q_1$ is definite if there exists one, and returns a message otherwise.

(1) `Let` a `be Cauchy's bound of` $\Delta(\lambda) = \det(\lambda Q_0 + Q_1)$`. Set` $I = [-a - 1, a + 1]$`.`
(2) `Set` m`, the number of real roots of` Δ`. If` $m \neq n$`, return a message saying that` $\lambda Q_0 + Q_1$ `is never definite.`
(3) `Let` $\lambda_1 < \ldots < \lambda_n$ `be the roots of` $\Delta(\lambda)$ `and` $[r, s]$ `the signature of` $-aQ_0+Q_1$`.`

https://doi.org/10.1112/S146115701600022X Published online by Cambridge University Press

(4) Let λ and μ be two rational numbers such that $\lambda \in]\lambda_r, \lambda_{r+1}[$ and $\mu \in]\lambda_s, \lambda_{s+1}[$.
(5) If $\lambda Q_0 + Q_1$ is definite, return λ. If $\mu Q_0 + Q_1$ is definite, return μ.
(6) Return a message saying that $\lambda Q_0 + Q_1$ is never definite.

This algorithm is an effective test of Theorem 3.6. We are able to decide whether $V_{q_0,q_1}(\mathbb{R}) \neq \emptyset$ or equivalently q_0 and q_1 have a common nonzero real solution using this algorithm. The explicit construction of a real solution will be done in Algorithm 11 when $n \geqslant 3$. The next algorithm is also very useful.

ALGORITHM 3. Let Q_0 and Q_1 be two matrices of size n satisfying condition 1 over $\mathbb{R}$. This algorithm uses a bisection method to compute a rational number λ such that $\lambda Q_0 + Q_1$ is balanced and nondegenerate.
(1) Let a be Cauchy's bound of $\Delta(\lambda) = \det(\lambda Q_0 + Q_1)$.
(2) Set $\lambda_{\max} = a + 1$, $\lambda_{\min} = -\lambda_{\max}$, and $\lambda_b = 0$.
(3) If $|d(\lambda_b)| \leqslant 1$ and $\Delta(\lambda_b) \neq 0$, return λ_b.
(4) If $d(\lambda_b) = 0$, set $\lambda_{\max} = \lambda_b$ and go to Step 6.
(5) If $d(\lambda_b)$ and $d(\lambda_{\min})$ have opposite signs, set $\lambda_{\max} = \lambda_b$, else set $\lambda_{\min} = \lambda_b$.
(6) Set $\lambda_b = (\lambda_{\min} + \lambda_{\max})/2$ and go to Step 3.

4. *Reduction of a balanced quadratic form*

NOTATION. We set K a field, with $K = \mathbb{R}$ or $K = \mathbb{Q}$. We denote by $\mathbb{H} = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ the matrix associated to the quadratic form $2xy$: we call it a *hyperbolic plane*.

Now, we are going to give a set of algorithms to compute some transition matrix P such that $PQ_0({}^tP)$ is the block diagonal matrix $\mathbb{H} \oplus Q_2$. In this section, we only consider indefinite quadratic forms over K of dimension $n \geqslant 5$.

NOTATION. In this section, most algorithms take as an input a matrix $Q_0 = (a_{ij})$ associated to a quadratic form $\sum_{i,j=1}^{n} a_{ij} x_i x_j$ defined over K and compute a matrix $P \in \mathrm{GL}_n(K)$. We denote by a'_{ij} the entries of $PQ_0({}^tP)$.

ALGORITHM 4. Let $Q_0 = (a_{ij})$ be such that $\det(Q_0) \neq 0$ and y a nonzero vector in K^n such that $yQ_0{}^ty = 0$. This algorithm computes a matrix $P \in \mathrm{GL}_n(K)$ such that $a'_{12} = 1$ and $a'_{1i} = 0$ for $i \neq 2$.
(1) Let P be a square matrix of size n having y as first row. Complete the matrix P to have $P \in \mathrm{GL}_n(K)$.
(2) Set $Q_0^{(1)} = PQ_0({}^tP)$. Let $i \geqslant 2$ be the smallest i such that $(Q_0(1))_{1i} \neq 0$, and P' be the permutation matrix which exchanges the second and the ith rows.
(3) Set $P = P'P$ and $Q_0''^{(2)} = P'Q_0^{(1)}({}^tP')$.
(4) Set $R = \mathrm{Id}(n)$ and divide the first row of R by $(Q_0^{(2)})_{12}$.
(5) Set $Q_0^{(3)} = RQ_0^{(2)}({}^tR)$.
(6) Set $R' = \mathrm{Id}(n)$. For $i = 3$ to n, set $R'_{i2} = -(Q_0^{(3)})_{i1}$.
(7) Set $R = R'R$ and return $P = RP$.

ALGORITHM 5. Let $Q_0 = (a_{ij})$ be such that $a_{11} = 0$, $a_{12} = 1$, and $a_{1i} = 0$ for $3 \leqslant i \leqslant n$. This algorithm computes $P \in \mathrm{GL}_n(K)$ such that $PQ_0({}^tP)$ is of the form $\mathbb{H} \oplus Q_2$.
(1) Set $P = \mathrm{Id}(n)$ and $S = \mathrm{Id}(n)$.
(2) For $i = 2$ to n, set $P_{i1} = -a_{i2}$. Set $Q_3 = PQ_0({}^tP)$.
(3) For $i = 1$ to n, set $S_{2i} = 2S_{2i} - (Q_3)_{22}S_{1i}$.

https://doi.org/10.1112/S146115701600022X Published online by Cambridge University Press

(4) Set $S_{11} = 1/2$ and $P = SP$.
(5) Return P.

ALGORITHM 6. Let $Q_0 = (a_{ij})$ and y be a nonzero vector in K^n such that $yQ_0{}^t y = 0$. This algorithm computes a matrix $P \in \mathrm{GL}_n(K)$ such that $PQ_0({}^tP)$ is of the form $\mathbb{H} \oplus Q_2$.
(1) Apply Algorithm 4 to Q_0 and y and denote by P the result.
(2) Apply Algorithm 5 to $P'Q_0'({}^tP')$ and denote by P'' the result.
(3) Return $P = P''P'P$.

ALGORITHM 7. Let $Q_0 = (a_{ij})$ of size $n \geqslant 5$ be defined over $\mathbb{Q}$ and such that q_0 is balanced. This algorithm computes $P \in \mathrm{GL}_n(\mathbb{Q})$ such that $PQ_0({}^tP)$ is of the form $\mathbb{H} \oplus \ldots \mathbb{H} \oplus Q_2$, where Q_2 is of size 3 if n is odd or of size 4 if n is even.
(1) Set $P = \mathrm{Id}(n)$ and $i = 1$.
(2) Extract the square submatrix $(Q_{0_{jk}})_{i \leqslant j,k \leqslant n}$ and denote it by Q_2.
(3) Compute a nonzero rational vector z such that $zQ_0{}^t z = 0$.
(4) Apply Algorithm 6 to Q_2 and z and denote by P' the result.
(5) Set $C = \mathrm{Id}(i-1) \oplus P'$.
(6) Set $P = CP$, $Q_0 = CQ_0({}^tC)$, $i = i + 2$.
(7) If $n - i + 1 \geqslant 5$, go to Step 2.
(8) Return P.

Step 3 can be done using the algorithm of Castel [2], which quickly computes a nonzero rational solution of a rational indefinite quadratic form of dimension $n \geqslant 5$. The idea of Algorithm 7 is based on [6]. The main idea is that after each loop the signature changes from $[r, s]$ to $[r-1, s-1]$. While the dimension of Q_2 is greater than or equal to 5, we can continue because an indefinite quadratic form in $n \geqslant 5$ variables has always a nonzero rational solution.

5. *Computation of a nonzero real solution of the system*

Obviously we consider that all the forms in $\mathcal{P}_{\mathbb{R}}$ are indefinite, otherwise $V_{q_0,q_1}(\mathbb{R})$ is clearly empty (see Theorem 3.6). In order to compute a real solution, we are going to first simultaneously block diagonalize the two quadratic forms, and then find a solution using simple algorithms, depending on the roots of $\Delta(\lambda)$. If $\Delta(\lambda)$ has only complex roots, we use Algorithm 8; if it has only real roots, we use Algorithm 10. Otherwise, we use Algorithm 9.

ALGORITHM 8. Let $q_0(x,y,z,w) = x^2 - y^2 + z^2 - w^2$ and $q_1(x,y,z,w) = ax^2 - 2bxy - ay^2 + cz^2 - 2dzw - cw^2$. This algorithm computes $v \in \mathbb{R}^4 \backslash \{0\}$ such that $q_0(v) = q_1(v) = 0$.
(1) Set ε, the sign of b and ε', the sign of d.
(2) Compute a nonzero solution (x_1, w_1) of $|b|x^2 - |d|w^2 = 0$.
(3) Return $v = (x_1, x_1, -\varepsilon\varepsilon' w_1, w_1)$.

ALGORITHM 9. Let $q_0(x,y,z) = x^2 + y^2 - z^2$ and $q_1(x,y,z) = \lambda_1 x^2 + ay^2 - 2byz - az^2$. This algorithm computes a nonzero vector $v \in \mathbb{R}^3$ such that $q_0(v) = q_1(v) = 0$.
(1) If $a = \lambda_1$, return $(1,0,1)$.
(2) Let us denote by y_1, y_2 the solutions of $(a - \lambda_1)y^2 - 2by - (a - \lambda_1) = 0$.
(3) If $-y_1^2 + 1 \geqslant 0$, return $(\sqrt{-y_1^2+1}, y_1, 1)$, otherwise return $(\sqrt{-y_2^2+1}, y_2, 1)$.

LEMMA 5.1. *Let* $q_0(x) = \sum_{i=1}^{k} x_i^2 - \sum_{j=k+1}^{n} x_j^2$ *and* $q_1(x) = \sum_{i=1}^{n} b_i x_i^2$ *be two quadratic forms satisfying condition* 1 *over* $\mathbb{R}$. *Let us denote* $m_- = \min(b_i \mid i \in \{k+1, \ldots, n\})$ *and* $m_+ = \min(b_i \mid i \in \{1, \ldots, k\})$.

https://doi.org/10.1112/S146115701600022X Published online by Cambridge University Press

(i) *There exists a real* λ *such that* $\lambda q_0 + q_1$ *is a positive definite quadratic form if and only if* $-m_- < m_+$.
(ii) *Let us denote* $M_- = \max(b_i \mid i \in \{k+1, \dots, n\})$ *and* $M_+ = \max(b_i \mid i \in \{1, \dots, k\})$. *Then* $V_{q_0,q_1}(\mathbb{R})$ *is nonempty if and only if* $-m_- \geqslant m_+$ *and* $-M_- \leqslant M_+$.

Proof. (i) Let us assume that there exists a real λ such that $\lambda q_0 + q_1$ is a positive definite quadratic form. This implies $\lambda + b_i > 0$ for all $i \leqslant k$ and hence $\lambda + m_+ > 0$. Similarly, we have $-\lambda + m_- > 0$, which implies $-m_- < m_+$. Conversely, for any λ satisfying $-m_- < -\lambda < m_+$, $\lambda q_0 + q_1$ is positive definite. The assertion (ii) just follows from the assertion (i). □

ALGORITHM 10. Let q_0 and q_1 be two quadratic forms of the form $q_0(x) = \sum_{i=1}^n a_i x_i^2$ with $a_i = \pm 1$, and $q_1(x) = \sum_{i=1}^n b_i x_i^2$ satisfying condition 1 over $\mathbb{R}$, and such that $V_{q_0,q_1}(\mathbb{R}) \neq \emptyset$. This algorithm computes a nonzero vector $w \in \mathbb{R}^n$ such that $q_0(w) = q_1(w) = 0$.
(1) Let v_1 be the list of all the i such that $a_i = +1$ and v_2 containing the others.
(2) Search M such that $b_M = \max_{i \in v_1}(b_i)$ and m such that $b_m = \min_{i \in v_1}(b_i)$.
(3) If for all $k \in v_2$ we have $-b_k \notin [b_m, b_M]$, then set $q_0 = -q_0$ and go to Step 1.
(4) Choose $k \in v_2$ such that $b_m \leqslant -b_k \leqslant b_M$.
(5) If $b_m = -b_k$, set $x_m = 1$, $x_k = 1$, and $x_i = 0$ for the other i.
(6) Otherwise, set $x_M = 1$, $x_m = \sqrt{(-b_M - b_k)/(b_m + b_k)}$, $x_k = \sqrt{x_m^2 + 1}$, and $x_i = 0$ for the other i.
(7) Return $(x_1, \dots, x_n)$.

The proof of this algorithm is an easy application of Lemma 5.1.

ALGORITHM 11. Let Q_0 and Q_1 be two matrices of size n satisfying condition 1 over $\mathbb{R}$ and such that $V_{q_0,q_1}(\mathbb{R}) \neq \emptyset$. This algorithm computes a $y \in V_{q_0,q_1}(\mathbb{R})$.
(1) Set $\Delta(\lambda) = \det(\lambda Q_0 + Q_1)$.
(2) Set a, the number of real roots of $\Delta(\lambda)$.
(3) Apply Algorithm 1 to Q_0 and Q_1. Denote by P the result.
(4) Set $Q_0' = PQ_0({}^tP)$ and $Q_1' = PQ_1({}^tP)$.
(5) If $a = 0$, apply Algorithm 8 to $(Q_{0_{ij}}')_{1 \leqslant i,j \leqslant 4}$ and $(Q_{1_{ij}}')_{1 \leqslant i,j \leqslant 4}$. Denote by y the result and set $z = (y_1, y_2, y_3, y_4, 0, \dots, 0)$.
(6) If $a = n$, apply Algorithm 10 to Q_0' and Q_1'. Denote by z the result.
(7) If $0 < a < n$, apply Algorithm 9 to $(Q_{0_{ij}}')_{a \leqslant i,j \leqslant a+2}$ and $(Q_{1_{ij}}')_{a \leqslant i,j \leqslant a+2}$. Denote by (z_a, z_{a+1}, z_{a+2}) the result. Set $z = (0, \dots, 0, z_a, z_{a+1}, z_{a+2}, 0, \dots, 0)$.
(8) Return $z \cdot P$.

6. *A suitable change of basis*

In this section, we give some algorithms to construct a rational totally isotropic subspace for $q_0(x)$ such that $q_1(x)$ is indefinite over this subspace. We keep the notation of § 4 concerning the inputs and outputs of the algorithms.

ALGORITHM 12. Let $Q_0 = (a_{ij})$ be such that $a_{11} = 0$ and $a_{13} \neq 0$. This algorithm computes a matrix $P \in \mathrm{GL}_n(K)$ such that $a_{13}' = 1$ and $a_{1i}' = 0$ for $i \neq 3$. Moreover, the first two columns of P are the same as in $\mathrm{Id}(n)$.
(1) Set $P = \mathrm{Id}(n)$ and divide the third row of P by a_{13}.
(2) Set $Q_0' = PQ_0({}^tP)$.

https://doi.org/10.1112/S146115701600022X Published online by Cambridge University Press

(3) Set $P' = \mathrm{Id}(n)$. Set $P'_{23} = -(Q'_0)_{12}$ and, for $i \neq 3$, $P'_{i3} = -(Q'_0)_{i1}$.
(4) Return $P = P'P$.

ALGORITHM 13. Let Q_0 and Q_1 be two matrices of size $n \geqslant 3$ satisfying condition 1 over $\mathbb{R}$ and such that $V_{q_0,q_1}(\mathbb{R}) \neq \emptyset$. Let a nonzero $z \in \mathbb{R}^n$ be such that $q_0(z) = 0$ and $q_1(z) = 0$. This algorithm computes a matrix $P \in \mathrm{GL}_n(\mathbb{R})$ such that the first row of $PQ_0({}^tP)$ is $(0, 1, 0, \ldots, 0)$ and the first row of $PQ_1({}^tP)$ is $(0, 0, 1, 0, \ldots, 0)$.
(1) Apply Algorithm 4 to Q_0 and z and denote by P the result.
(2) Set $Q'_0 = PQ_0({}^tP)$ and $Q'_1 = PQ_1({}^tP)$.
(3) Let $i \geqslant 3$ be the smallest index such that $(Q'_1)_{1i} \neq 0$, and P' be the permutation matrix which exchanges the third and the ith rows. Set $P = P'P$.
(4) Apply Algorithm 12 to $P'Q'_1({}^tP')$ and denote by R the result. Set $P = RP$.
(5) Return P.

ALGORITHM 14. Let $Q_0 = (a_{ij})$ and $Q_1 = (b_{ij})$ be two matrices of size $n \geqslant 5$ satisfying condition 1 over $\mathbb{R}$. Let a nonzero $z \in \mathbb{R}^n$ be such that $q_0(z) = 0$ and $q_1(z) = 0$. This algorithm computes a nonzero $z^- \in \mathbb{R}^n$ such that $q_0(z^-) = 0$ and $q_1(z^-) < 0$.
(1) Apply Algorithm 13 to Q_0, Q_1, and z. Denote by P the result and set $Q'_0 = PQ_0({}^tP)$ and $Q'_1 = PQ_1({}^tP)$.
(2) Extract the submatrix $(Q'_{0_{ij}})_{2\leqslant i,j\leqslant n}$ of Q'_0, denote it by F, and let $f(x)$ be the associated quadratic form.
(3) Extract the submatrix $(Q'_{1_{ij}})_{2\leqslant i,j\leqslant n}$ of Q'_1, denote it by G, and let $g(x)$ be the associated quadratic form.
(4) If $F_{22} = 0$, set $z = ((-1 - G_{22})/2, 0, 1, 0, \ldots, 0)$ and go to Step 8.
(5) Set $\varepsilon = \mathrm{sign}(F_{22})$. Set $y_1 = 1$, $y_2 = \varepsilon$ and, for $i = 3$ to $n - 1$, set $y_i = 0$.
(6) While $g(y) - y_2 f(y) \geqslant 0$, set $y_2 = 2y_2$.
(7) Set $z = (-f(y)/2, y_1, \ldots, y_{n-1})$.
(8) Return $z^- = z \cdot P$.

Proof. At the end of Step 3, we have $q'_0(x) = 2x_1x_2 + f(x_2, \ldots, x_n)$ and $q'_1(x) = 2x_1x_3 + g(x_2, \ldots, x_n)$. For Step 4, we have $q'_0(z) = 0$ and $q'_1(z) = -1$. Otherwise, we consider the function $h(x) = x_2 g(x) - x_3 f(x)$. This is a polynomial of degree 3 in x_3 and the leading coefficient is $-F_{22}$. So, if we set $x_i = 0$ for $i > 3$, $h(x)$ is negative for $x_3 = \varepsilon x'_3$ with $x'_3 > 0$ large enough. Setting $y = (1, \varepsilon x'_3, 0, \ldots, 0)$ and $z = (-f(y)/2, 1, \varepsilon x'_3, 0, \ldots, 0)$, we have $q'_0(z) = 0$ and $q'_1(z) = -\varepsilon x'_3 f(y) + g(y) < 0$. □

ALGORITHM 15. Let $Q_0 = (a_{ij})$ and $Q_1 = (b_{ij})$ be two matrices with rational inputs of size $n \geqslant 5$ and a nonzero $y \in \mathbb{R}^n$ be such that $q_0(y) = 0$ and $q_1(y) < 0$. This algorithm computes a $z \in \mathbb{Q}^n$ such that $q_0(z) = 0$, $q_1(z) < 0$.
(1) Compute a rational solution w of $q_0(w) = 0$. Apply Algorithm 6 over $\mathbb{Q}$ to Q_0 and w; denote it by P'. Set $Q'_0 = P'Q_0({}^tP')$, $Q'_1 = P'Q_1({}^tP')$, and $y' = y \cdot P'^{-1}$.
(2) If $y'_i = 0$ for all $i \geqslant 2$, return $(1, 0, \ldots, 0)P'$.
(3) Denote by $i \geqslant 2$ the smallest index such that $y'_i \neq 0$. We set P'', the permutation matrix that exchanges the second row with the ith. Set $P = P''P'$, $y'' = y' \cdot P''$, $Q''_0 = P''Q'_0({}^tP'')$, $Q''_1 = P''Q'_1({}^tP'')$, and $\varepsilon = |y''_2|/2$.
(4) Extract the submatrix $(Q''_{0_{ij}})_{3\leqslant i,j\leqslant n}$ of Q''_0, denote it by F, and let $f(x)$ be the associated quadratic form.
(5) For $i = 1$ to n, choose a rational number z''_i such that $|y''_i - z''_i| < \varepsilon$. If $q''_1(z'') \geqslant 0$, set $\varepsilon = \varepsilon/2$ and go to Step 5.
(6) Set $u_1 = -f(z''_3, \ldots, z''_n)/2z''_2$ and $u = (u_1, z''_2, \ldots, z''_n)$.
(7) If $q''_1(u) < 0$, return $u \cdot P$. Otherwise, set $\varepsilon = \varepsilon/2$ and go to Step 5.

https://doi.org/10.1112/S146115701600022X Published online by Cambridge University Press

Proof. After Step 4, we have $q_0''(y'') = q_0(y) = 0$ and $q_1''(y'') = q_1(y) < 0$ with $Q_0'' = \mathbb{H} \oplus F$. Step 5 is possible because the function q_1'' is continuous and the set $\mathbb{Q}$ is dense in $\mathbb{R}$. Because $\varepsilon \leqslant |y_2''|$, we have $z_2'' \neq 0$. Since $Q_0'' = \mathbb{H} \oplus F$, the formula in Step 6 gives $q_0''(u) = 0$. As y'' also satisfies the relation $y_1'' = -f(y_3'', \ldots, y_n'')/2y_2''$, by continuity we deduce that, when ε is small enough, u_1 is close to y_1'', so that u is close to y'' and $q_1''(u) < 0$. □

7. *Computation of a nonzero rational solution*

In this section, we compute a nonzero rational solution of $q_0(x) = q_1(x) = 0$.

ALGORITHM 16. Let Q_0 and Q_1 be two matrices of size $n \geqslant 13$ satisfying condition 1 over $\mathbb{Q}$ and such that $V_{q_0,q_1}(\mathbb{R}) \neq \emptyset$. This algorithm computes some $x \in V_{q_0,q_1}(\mathbb{Q})$.

(1) Apply Algorithm 3 and find $\lambda_0 \in \mathbb{Q}$ such that $Q_0 + \lambda_0 Q_1$ is balanced and has nonzero determinant. Set $Q_0 = Q_0 + \lambda_0 Q_1$.
(2) Compute a nonzero solution $y \in \mathbb{Q}^n$ of $q_0(y) = 0$.
(3) If $q_1(y) = 0$, return y. If $q_1(y) < 0$, set $Q_1 = -Q_1$.
(4) Apply Algorithm 11 to Q_0 and Q_1. Denote by u the result.
(5) Apply Algorithm 14 to (Q_0, Q_1, u) and denote by v the result.
(6) Apply Algorithm 15 to (Q_0, Q_1, v) and denote by z the result.
(7) While $q_0(y, z) = 0$, do:
  (i) choose $y' \in \mathbb{Q}^n$ randomly until $q_0(y, y') \neq 0$;
  (ii) set $w = y' - (q_0(y')/2q_0(y, y'))y$;
  (iii) if $q_1(w) = 0$, return w;
  (iv) if $q_1(w) > 0$, set $y = w$, otherwise set $z = w$.
(8) Let $P^{(1)}$ be a matrix whose first $n-2$ rows generate the solutions in x of $xQ_0{}^t y = xQ_0{}^t z = 0$, and whose last two rows are y and z.
(9) Set $Q_0^{(1)} = P^{(1)}Q_0({}^tP^{(1)})$, $Q_1^{(1)} = P^{(1)}Q_1({}^tP^{(1)})$.
(10) Set $P^{(2)}$, the permutation matrix that exchanges the first row with the $(n-1)$th row and the second row with the nth row.
(11) Set $Q_0^{(2)} = P^{(2)}Q_0^{(1)}({}^tP^{(2)})$, $Q_1^{(2)} = P^{(2)}Q_1^{(1)}({}^tP^{(2)})$, and $P = P^{(2)}P^{(1)}$.
(12) Extract the submatrix $(Q_{0_{ij}}^{(2)})_{3 \leqslant i,j \leqslant n}$ of $Q_0^{(2)}$ and denote it by Q_2.
(13) Apply Algorithm 7 to Q_2 and denote by P' the result.
(14) Set $P^{(3)} = \mathrm{Id}(2) \oplus P'$, $Q_0^{(3)} = P^{(3)}Q_0^{(2)}({}^tP^{(3)})$, $Q_1^{(3)} = P^{(3)}Q_1^{(2)}({}^tP^{(3)})$, and $P = P^{(3)}P$.
(15) If $(Q_1^{(3)})_{33} > 0$, compute a nonzero rational solution of $q_1^{(4)}(x) = 0$ of the form $x = (0, x_2, x_3, 0, x_5, 0, x_7, 0, x_9, 0, 0, 0, \ldots)$. Otherwise, compute a nonzero rational solution of $q_1^{(4)}(x) = 0$ of the form $x = (x_1, 0, x_3, 0, x_5, 0, x_7, 0, x_9, 0, 0, 0, \ldots)$.
(16) Return xP.

Proof. After Step 1, $q_0(x)$ is balanced, so that in Step 2, such a rational y exists and, after Step 3, we have $q_1(y) > 0$. For Step 4, such a real solution exists because $V_{q_0,q_1}(\mathbb{R})$ is nonempty. Steps 4–6 compute a rational vector z such that $q_0(z) = 0$ and $q_1(z) < 0$. After Step 7, we have that y and z are not orthogonal for q_0; then the intersection of $\langle y, z\rangle$ and $\langle y, z\rangle^{\perp_{q_0}}$ is nonzero. Therefore, the matrix $P^{(1)}$ of Step 8 is invertible. Step 13 is possible because $Q_0^{(2)} = \mathbb{H} \oplus Q_2$ is balanced with signature $[r, s]$; thus, Q_2 is balanced with signature $[r-1, s-1]$ and dimension $n-2 \geqslant 11$. The subspaces of the elements of the form $x = (0, x_2, x_3, 0, x_5, 0, x_7, 0, x_9, 0, 0, 0, \ldots)$ and $x = (x_1, 0, x_3, 0, x_5, 0, x_7, 0, x_9, 0, 0, 0, \ldots)$ are both totally isotropic for $q_0^{(4)}$. To conclude, we just need to compute a solution of $q_1^{(4)}(x) = 0$ in one of these subspaces. Since $(Q_1^{(4)})_{11} > 0$

https://doi.org/10.1112/S146115701600022X Published online by Cambridge University Press

and $(Q_1^{(4)})_{22} < 0$, the choice made in Step 15 assures that $q_1^{(4)}(x)$ is indefinite on this subspace. Moreover, in this subspace $q_1^{(4)}(x)$ has at least five variables and, by the Hasse principle (cf. [7]), has rational solutions. This concludes the proof. □

References

1. B. J. Birch, D. J. Lewis and T. G. Murphy, 'Simultaneous quadratic forms', *Amer. J. Math.* 84 (1962) 110–115.
2. P. Castel, 'Solving quadratic equations in dimension 5 or more without factoring', *ANTS X — Proceedings of the Tenth Algorithmic Number Theory Symposium* (Mathematical Sciences Publishers, Berkeley, CA, 2013).
3. J.-L. Colliot-Thélène, J.-J. Sansuc and H. P. F. Swinnerton-Dyer, 'Intersections de deux quadriques et surfaces de Châtelet', *C. R. Acad. Sci. Paris Sér. I Math.* 298 (1984) 377–380.
4. V. B. Demyanov, 'Pairs of quadratic forms over a complete field with discrete norm with a finite field of residue classes', *Izv. Akad. Nauk SSSR Ser. Mat.* 20 (1956) 307–324.
5. J. Harris, *Algebraic geometry* (Springer, New York, 1995).
6. L. J. Mordell, 'Integer solutions of simultaneous quadratic equations', *Abh. Math. Semin. Univ. Hambg.* 23 (1959) 126–143.
7. J.-P. Serre, *A course in arithmetic* (Springer, 1996).
8. D. Simon, 'Solving quadratic equations using reduced unimodular quadratic forms', *Math. Comput.* 74 (2005) no. 251, 1531–1543.
9. H. P. F. Swinnerton-Dyer, 'Rational zeros of two quadratic forms', *Acta Arith.* 9 (1964) 261–270.
10. O. Wittenberg, 'Principe de Hasse pour les intersections de deux quadriques', *C. R. Acad. Sci. Paris, Ser. I* 342 (2006) no. 4, 223–227.

Tony Quertier
UMR 6139 - Laboratoire de Mathématiques Nicolas Oresme (LMNO)
Université de Caen Normandie
UFR des Sciences
Campus 2
Côte de nacre Bd Maréchal Juin
14032 Caen cedex 5
France
tony.quertier@unicaen.fr

https://doi.org/10.1112/S146115701600022X Published online by Cambridge University Press