Quadratic equations in dimensions 4, 5 and more.

Denis SIMON (simon@math.unicaen.fr)
LMNO - UMR 6139
Université de Caen – France
Campus II – Boulevard Mal Juin
BP 5186 – 14032 Caen Cedex

4th July 2006

Abstract

Although the solvability over the rationals of a quadratic equation of dimension 4 is easy to test using local information, no efficient algorithm has been described yet for constructing a solution. We describe here such an algorithm and prove its correctness. It uses many different tools such as linear algebra over finite fields, the theory of class groups of binary quadratic forms, and the reduction of indefinite unimodular quadratic forms. We extend this algorithm to all the dimensions $n \geqslant 5$, by considering separately two cases, depending on the parity of n. These algorithms can be used to find a totally isotropic subspace of maximal dimension.

Introduction

The well–known Theorem of Hasse–Minkowski ([7, Th. IV.8]) asserts that a homogeneous quadratic equation $Q(X_1, \ldots, X_n) = 0$ over $\mathbb{Q}$, has a nontrivial solution in $\mathbb{Q}^n$ if and only if it has a nontrivial solution everywhere locally. It is also known that the local solvability is automatically satisfied, except at a finite number of places, namely over the reals, over $\mathbb{Q}_2$, and over $\mathbb{Q}_p$, for all prime divisors p of the determinant of Q, see [7, Th. IV.6]. If $n \geqslant 5$, the solvability is even simpler to test, since in this situation, Meyer's Theorem (see [7, Cor IV.2]) asserts that the equation is solvable over $\mathbb{Q}$ if and only if Q is indefinite.

If $\det Q = 0$, a solution can be found by linear algebra, and we will never consider this case any more. The theory of local symbols gives a very efficient way to decide the existence of local solutions at a given place. As soon as the factorization of $\det Q$ is known, it gives therefore a very efficient way to determine the existence of a nontrivial global solution (this is even more efficient when $n \geqslant 5$ since in this case only the real signature has to be computed).

For many applications, it is not enough to know that a solution exists, and we really need an algorithm to construct such a solution. The special case $n = 3$ is probably the most studied one, and several efficient algorithms exist (see [6, §294–295], and more recently [5] and [8]). For higher dimensions, very little has been done, and to our knowledge, no efficient algorithm has been implemented nor described. The classical proof of the Hasse–Minkowski Theorem in the case $n = 4$ explicitely constructs a solution and runs as follows : using a standard diagonalization process, we reduce the problem to an equation of the form $a_1X_1^2 + a_2X_2^2 + a_3X_3^2 + a_4X_4^2 = 0$; then, using the Theorem of Dirichlet on primes in arithmetic progressions, it is proved that the binary

quadratic forms $a_1X_1^2 + a_2X_2^2$ and $-a_3X_3^2 - a_3X_3^2$ represent a common prime number p ; these representations can be found using the well–known case $n = 3$. It is possible to turn this proof into an algorithm. However, it rapidly becomes inefficient, and a careful analysis of this algorithm would be very difficult. This is essentially due to the use of the Theorem of Dirichlet, which is still highly ineffective. Another drawback of this algorithm is that it requires the factorization of the coefficients a_i, which may be huge compared to $\det Q$, and therefore impossible to factor in practice (see [8, §4] for a similar discussion in the case $n = 3$).

The goal of this paper is to fill in this gap. We will give an algorithm that gives a solution in the case $n \geqslant 4$. As we will see, using linear algebra and recursive application of the algorithm, we are also able to find a totally isotropic subspace of maximal dimension. ********** We are able to prove that, for a fixed dimension n, the running time of the algorithm is polynomial in the input. **********

Our strategy is to generalize the algorithm of [8], written for the specific case $n = 3$, to the higher dimensions $n \geqslant 4$. The general algorithm runs in three steps:

Step 1 – Factorization of $\det Q$.

Step 2 – Minimization: using linear algebra and square roots modulo p, we are reduced to the case of a unimodular quadratic form ($\det Q = \pm 1$).

Step 3 – Reduction: using the reduction algorithm for indefinite quadratic forms given in [8], we reduce the size of the coefficients until a very simple solution can be found.

However, contrary to the case $n = 3$, the minimization step can not in general be achieved within a fixed dimension $n \geqslant 4$. As we will see, the solution of an equation in dimension n will require to work in dimension greater than n (but at most $n+3$). In [2, §14.7] and [3], Cassels gives a proof of the Hasse–Minkowski Theorem in the case $n = 4$, where he does not make use of the Theorem of Dirichlet on primes in arithmetic progressions. His strategy consists of incrementing the dimension by 2 and using the knowledge of the 2–Sylow of the class group, for a well–chosen discriminant. We will follow this trick, and our strategy for the minimization of the determinant of Q will be the following:

Step 2a – Remove as many prime factors as possible within dimension n.

Step 2b – Increase n by 1 to remove the square factors of $\det Q$.

Step 2c – Increase again n by 2 to remove all the remaining factors of $\det Q$.

In fact, after step 2a, $\det Q$ will contain square factors only if n is even. If $n = 4$, the prime divisors of this square are precisely those at which our equation is not solvable. Therefore, if the local solvability has been tested before calling this algorithm, there is no step 2b for $n = 4$, otherwise, this step can serve as as a test for the local solvability. Hence, for $n = 4$, the minimization is achieved in dimension 4 or 6. For higher dimensions, it is easy to write down examples for which the minimization will be done in either dimension n or $n + 2$ if n is odd, and in either dimension n, $n + 1$, $n + 2$, $n + 3$ if n is even.

This paper is divided as follows. In section 1, we investigate the case of a unimodular quadratic form of an arbitrary dimension. In sections 2 and 3, we give the numerous lemmas usefull for the minimization algorithm. In section 4, we consider a special case of the 4–dimensional equation. In the following sections 5, 6, and 7, we consider separately the generic cases when the dimension n is 4, odd and $n \geqslant 5$, and finally even and $n \geqslant 6$. The final two sections tackle the question of the performance of the algorithm and its possible improvements.

Notation:

We will always identify a quadratic form Q and its Gram matrix in a given basis. For a symmetric matrix $Q \in \mathcal{M}_n(\mathbb{Q})$ and $X \in \mathbb{Q}^n$, we have $Q(X) = X^t Q X$. More specifically for binary quadratic forms, we use the notation (a, b, c) for the quadratic form $aX^2 + bXY + cY^2 = \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}$. If Q and R are two quadratic forms over two distinct spaces, we write $Q \oplus R$ for their orthogonal sum. We also use the notation $Q^{\oplus n}$ for $Q \oplus Q \oplus \cdots \oplus Q$ (n times). For a given quadratic form Q over a space E, and a subspace $F \subset E$, $F^\perp$ is the orthogonal complement of F in E for Q.

If a and b are p–adic numbers, $(a, b)_p$ is the usual Hilbert symbol, and if $Q \in \mathcal{M}_n(\mathbb{Q}_p)$ is a quadratic form over the p–adic numbers, $\varepsilon_p(Q)$ is its local Witt invariant (also called the Hasse–Minkowski invariant and denoted by $c_p(Q)$ in [2], or the ε invariant in [7]). For a real quadratic form Q, $sign(Q) = (r, s)$ is its signature (for example, $sign(Q) = (n, 0)$ means that Q is positive definite).

1 Solution in the unimodular case

In this part, we want to solve $Q(x) = 0$, where $Q \in \mathcal{M}_n(\mathbb{Z})$ is a symmetric matrix with determinant ± 1 and dimension $n \geqslant 2$. Using an easy induction, we can also obtain a totally isotropic subspace of maximal dimension.

Algorithm 1 (Solution in the unimodular case) *Let $Q \in \mathcal{M}_n(\mathbb{Z})$ be a symmetric matrix with determinant $\Delta = \pm 1$ and signature (r, s). This algorithm finds a nontrivial solution of $Q(X) = 0$.*

1- If $r = 0$ or $s = 0$, return $\emptyset$.

2- Apply the reduction algorithm of [8] to Q. If a solution X has been found, return X.

3- Compute the Gram-Schmidt orthogonal basis $(\mathbf{b}_k^*)_{1 \leqslant k \leqslant n}$ associated to Q.

4- For $k = 1, \ldots, n$, compute $d_k = \det(Q_{i,j})_{1 \leqslant i \leqslant k, 1 \leqslant j \leqslant k}$ and $d_0 = 1$.

5- If $\frac{d_i}{d_{i-1}} = -\frac{d_j}{d_{j-1}}$, for some $i \neq j$, return $\mathbf{b}_i^* + \mathbf{b}_j^*$.

6- Let $l \geqslant 1$ be the smallest index such that $\frac{d_l}{d_{l-1}}, \ldots, \frac{d_{l+4}}{d_{l+3}}$ contains at least a sign change, and E be the subspace generated by $(\mathbf{b}_k^*)_{l \leqslant k \leqslant l+4}$.

7- Find a nontrivial solution $X \in E$ of $Q(X) = 0$ using Algorithm 6 and return X.

Proof: In [8] we saw that the reduction algorithm builds a solution exactly when $d_k = 0$ for some k, and that the Gram–Schmidt basis exists if and only if the d_k are all nonzero. This proves that Step 3 is correct. Steps 4 and 5 are clear, since we have $Q(\mathbf{b}_k^*) = \frac{d_k}{d_{k-1}}$. In [10], it was proved that, if $n \leqslant 9$, a solution of $Q(X) = 0$ must be found at Step 5. This proves the validity of the algorithm for $n \leqslant 9$.

Assume now that we arrive at Step 6. We have $n \geqslant 10$. Among the $\frac{d_l}{d_{l-1}}$ exactly r of them are positive, and s are negative. Since r and s are both nonzero, the quantity l of Step 6 is well defined. The restriction of Q to the 5–dimensional subspace E is indefinite, and by Meyer's Theorem ([7, §IV.3.2]), we know that it represents 0. The validity of Step 7 is proved if we prove the validity of Algorithm 6. As we will see, Algorithm 6 requires Algorithm 1, so it seems unsolvable. In fact, we only need Algorithm 6 in dimension $n = 5$, and in this case Algorithm 6 only requires Algorithm 1 in dimension $n + 2 = 7$, which we already know to be valid. ■

After billions of random experiments up to dimension 25, I have never encountered the slightest need to go further than Step 5 in this algorithm. However, it remains possible, at least in principle, to find a counter–example. If we have such a Q, we see that Step 7 requires the factorization of $\det Q_{|E}$. Since the basis is orthogonal, this determinant is the product $Q(\mathbf{b}_l^*) \times \cdots \times Q(\mathbf{b}_{l+4}^*)$, and the factorization of $\det Q_{|E}$ is given by the factorization of the integers $d_{l-1}, \ldots, d_{l+4}$, which are bounded in [10] by

$$| d_k | \leqslant \gamma^{k(n-k)/2} \leqslant \gamma^{n^2/8}$$

for a real constant γ close to $\frac{4}{3}$. For $n \leqslant 25$, it gives $| d_k | \leqslant 10^{10}$ and for $n \leqslant 50$, it gives $| d_k | \leqslant 10^{40}$.

By [7, Th V.3] we know that the indefinite unimodular quadratic form Q represents 0. Algorithm 1 can be used to solve this problem. By induction, we can therefore find a basis change, such that in the new basis $(\mathbf{b}_i)$, Q has the shape $Q = H^{\oplus m} \oplus D$, where D is a (positive or negative) definite quadratic form, $m = \min(r, s)$, and H is a hyperbolic plane, that is $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ or $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$. We have thus found a totally isotropic subspace of maximal dimension m, and basis $\mathbf{b}_1$, $\mathbf{b}_3$,…,$\mathbf{b}_{2m-1}$. The corresponding recursive algorithm is the following:

Algorithm 2 (maximal totally isotropic subspace) *Let $Q \in \mathcal{M}_n(\mathbb{Z})$ be a symmetric matrix with determinant $\Delta = \pm 1$ and signature (r, s). This algorithm finds a basis of $\mathbb{Z}^n$ such that in this basis Q has the shape $Q = H^{\oplus m} \oplus D$, where $m = \min(r, s)$ and D is a (positive or negative) definite quadratic form of dimension $n - 2m$.*

`1- If` $r = 0$ `or` $s = 0$ `or` $n \leqslant 1$, `return` $D = Q$.

`2- Using Algorithm 1, determine a solution of` $X_1^t Q X_1 = 0$. `Choose a new basis` $X_1, \ldots, X_n$ `starting with` X_1.

`3- Apply standard linear algebra over` $\mathbb{Z}$ `and find a new basis for which` Q `has the form` $Q = H \oplus Q'$, `where` $H = \begin{pmatrix} 0 & 1 \\ 1 & \varepsilon \end{pmatrix}$ `with` $\varepsilon = 0$ `or` 1. `This` Q' `has dimension` $n - 2$, `determinant equal to` $\det Q' = -\det Q$, `and signature` $(r - 1, s - 1)$.

`4- Return` $H \oplus R$, `where` R `is the result of Algorithm 2 applied to` Q'.

2 Totally isotropic subspaces over $\mathbb{F}_p$

In this section, we recall some very classical results about quadratic forms over the finite field $\mathbb{F}_p$. Nevertheless, we write them here to give an idea of the corresponding algorithms. We use here the language of quadratic spaces (see [2] or [7]).

Lemma 1 *Let p be a prime number, and $\overline{Q} \in \mathcal{M}_3(\mathbb{F}_p)$ a symmetric matrix with nonzero determinant. Then $\overline{Q}$ represents 0 nontrivially.*

Proof: This result is well known (see for example [7, prop IV.4]). From a computational point of view, we can fix two variables at random, and solve for the third one. It corresponds to a quadratic equation with a random discriminant. This discriminant is a square with a probability close to 1/2. The corresponding probabilistic algorithm is extremely efficient. Another algorithm has been described by Van de Woestijne ([11]), which is deterministic, but sometimes less efficient. ■

Lemma 2 *Let $n \geqslant 1$ be an integer, and $\overline{Q} \in \mathcal{M}_n(\mathbb{F}_p)$ a symmetric matrix with nonzero determinant. Set*

$$m = \begin{cases} (n-1)/2 & \text{if } n \text{ is odd} \\ n/2 & \text{if } n \text{ is even and } (-1)^{n/2} \det \overline{Q} \text{ is a square} \\ n/2 - 1 & \text{otherwise} \end{cases}$$

There is a subspace of dimension m, which is totally isotropic for $\overline{Q}$.

Proof: We will prove that the full space can be decomposed into the orthogonal sum of m hyperbolic planes and another space of dimension $n - 2m$. The proof is done by induction on n. If $n = 1$ or $n = 2$, the result is clear (and a square root computation may be necessary to exhibit explicitly the hyperbolic plane). Assume now that it is true for all dimensions up to $n - 1 \geqslant 2$, and consider a quadratic form of $\overline{Q_n}$ of dimension n and nonzero determinant. By Lemma 1, $\overline{Q_n}$ is isotropic, and using standard linear algebra over $\mathbb{F}_p$, we can write $\overline{Q_n} = H \oplus \overline{Q_{n-2}}$. The result follows by induction, since we have $\det \overline{Q_{n-2}} = -\det \overline{Q_n}$, and $\dim \overline{Q_{n-2}} = n - 2$. ■

Lemma 3 *With the same notation as in Lemma 2, every subspace, which is totally isotropic for $\overline{Q}$, is contained in another such subspace of dimension m.*

Proof: Let E be a subspace of dimension e, totally isotropic for $\overline{Q_n}$. Using standard linear algebra, we can find another subspace E' of dimension e, such that $E \oplus E' = H^{\oplus e}$, where H is a hyperbolic plane. Now, the quadratic space is $\mathbb{F}_p^n = (E \oplus E') \oplus (E \oplus E')^{\perp}$, where the quadratic space $(E \oplus E')^{\perp}$ has dimension $n - 2e$ and determinant $(-1)^d \det \overline{Q}$. Applying Lemma 2 to $(E \oplus E')^{\perp}$, we get the result. ■

Remark: In order to find a totally isotropic subspace of dimension m, we see that we have to compute m square roots modulo p. In [11], there is a way to find it with at most one square root. The integer m itself can be computed with no effort if n is odd, and requires only the computation of the Legendre symbol $\left(\frac{(-1)^{n/2} \det \overline{Q}}{p}\right)$ if n is even.

3 Minimization

The goal of this part is to minimize the determinant of Q; that is, to apply a linear transformation to Q over $\mathbb{Q}$, such that the coefficients of Q remain integral, but the determinant of Q becomes as small as possible. For this purpose, we work successively with each prime divisor p of $\det Q$, and use the classical algorithms of linear algebra and square root in $\mathbb{F}_p$.

Let $Q \in \mathcal{M}_n(\mathbb{Z})$ be a symmetric matrix with determinant $\Delta \neq 0$. Choose a prime $p \mid \Delta$ and let v be the valuation of Δ at p. We use the notation $\overline{Q}$ for the reduction of Q modulo p and $d = \dim_{\mathbb{F}_p} \ker \overline{Q}$. We have $1 \leqslant d \leqslant n$ and $d \leqslant v$.

After a linear transformation, and without loss of generality, we can assume that the first d columns of Q are divisible by p. We also consider $\tilde{Q} = (\frac{1}{p} Q_{i,j})_{1 \leqslant i,j \leqslant d}$. With all these conventions, Q has the form

$$Q = \begin{pmatrix} p\tilde{Q} & p* \\ p* & U \end{pmatrix}$$

where $U \in \mathcal{M}_{n-d}(\mathbb{Z})$ is invertible modulo p.

Lemma 4 *If $d = n$, then $Q' = \frac{1}{p} Q \in \mathcal{M}_n(\mathbb{Z})$ and $\det Q' = p^{-n} \Delta$.*

Lemma 5 *If $d < v$, then there exists an integer $\tilde{d}$, $1 \leqslant \tilde{d} \leqslant d$, and a matrix $M \in \mathcal{M}_n(\mathbb{Q})$ such that $Q' = M^t Q M \in \mathcal{M}_n(\mathbb{Z})$ with $\det Q' = p^{-2\tilde{d}}\Delta$.*

Proof: The condition $d < v$ implies that the matrix $\tilde{Q}$ also has a nontrivial kernel modulo p. Let $\tilde{d}$ be its dimension, $1 \leqslant \tilde{d} \leqslant d$. After a basis change, we get that the first $\tilde{d}$ columns of $\tilde{Q}$ are divisible by p. We can extend the basis change to Q, and we see that the block $(Q_{i,j})_{1\leqslant i,j\leqslant \tilde{d}}$ extracted from Q is divisible by p^2. The matrix M can be chosen to be diagonal, with the first $\tilde{d}$ coefficients equal to $\frac{1}{p}$, and the last coefficients equal to 1. ■

Lemma 6 *If n is odd and if $d = v$ is even and $d \geqslant 2$, then there exists a matrix $M \in \mathcal{M}_n(\mathbb{Q})$ such that $Q' = \frac{1}{p} M^t Q M \in \mathcal{M}_n(\mathbb{Z})$, $Q' \notin \mathcal{M}_n(p\mathbb{Z})$, with $\det Q' = p^{n-2d}\Delta$.*

Proof: The matrix M can be chosen to be diagonal, with the first d coefficients equal to 1 and the last coefficients equal to p. We obtain $Q' = \begin{pmatrix} \tilde{Q} & p* \\ p* & pU \end{pmatrix}$. ■

With an obvious notation, we have, in Lemma 6, $d(Q') = v(Q') = n - d$ is odd.

Lemma 7 *If $d = v$ and $d \geqslant 3$, then there exists a matrix $M \in \mathcal{M}_n(\mathbb{Q})$ such that $Q' = M^t Q M \in \mathcal{M}_n(\mathbb{Z})$ with $\det Q' = p^{-2}\Delta$.*

Proof: By Lemma 1, we can find a new basis, for which the coefficient $\tilde{Q}_{1,1}$ is divisible by p. We extend this linear transformation to Q, and see that the first line and column of Q are divisible by p, and that the coefficients $Q_{1,1}$ is divisible by p^2. We can therefore choose for M the diagonal matrix having $\frac{1}{p}$ as the first coefficient, and 1 as the other coefficients. ■

Lemma 8 *If $d = v = 2$ and if $-\det \tilde{Q}$ is a square modulo p, then there exists a matrix $M \in \mathcal{M}_n(\mathbb{Q})$ such that $Q' = M^t Q M \in \mathcal{M}_n(\mathbb{Z})$ with $\det Q' = p^{-v}\Delta$.*

Proof: Since $-\det \tilde{Q}$ is a square modulo p, $\tilde{Q}$ represents an integer divisible by p. The end of the proof is similar to the proof of Lemma 7. ■

For the remaining cases, we make a supplementary transformation. We denote by m the maximal dimension of a totally isotropic subspace for $\overline{U}$ modulo p. After a new basis change, we get that the block $(U_{i,j})_{1\leqslant i,j\leqslant m}$ is divisible by p (we use Lemma 2, and the underlying algorithm). It is worthwhile to note that this decomposition is necessary only when the conditions of the next lemma are fulfilled. The corresponding test can be done as soon as we know the values of d,v, and m (see Lemma 2).

Lemma 9 *Assume that $d = v = 1$ and n is odd, or that $d = v = 2$ and n is even.*

If $m = (n - d)/2$, then there exists a matrix $M \in \mathcal{M}_n(\mathbb{Q})$ such that $Q' = \frac{1}{p} M^t Q M \in \mathcal{M}_n(\mathbb{Z})$ with $\det Q' = p^{-v}\Delta$.

Proof: After the transformation already performed on Q, we see that it is enough to consider a diagonal matrix M having its first $d + m$ coefficients equal to 1, and the other equal to p. ■

We can now use all theses lemmas, and deduce an algorithm of minimization:

Algorithm 3 (Minimization) *Consider a symmetric matrix $Q \in \mathcal{M}_n(\mathbb{Z})$ with determinant $\Delta \neq 0$. This algorithm applies linear transformations on Q and minimizes its determinant.*

For each prime $p \mid \Delta$, apply the following transformations:

1- Apply Lemma 4 and Lemma 5 as long as possible.

2- If n is odd, apply Lemma 6.

3- If $d = v \geqslant 3$, apply Lemma 7.

4- If n is even and $d = v = 2$, apply Lemma 8.

5- Compute m with the formula given in Lemma 2. If the condition of Lemma 9 is fulfilled apply Lemma 9.

6- Return the new matrix $Q \in \mathcal{M}_n(\mathbb{Z})$ and the matrix $M \in \mathcal{M}_n(\mathbb{Q})$ of the corresponding basis change.

Remark: We remark that step 1 and step 2 of this algorithm use only linear algebra over $\mathbb{F}_p$, and that step 3 to step 5 require taking square roots in $\mathbb{F}_p$. In consideration for computational efficiency, it may be interesting to reduce the size of the linear transformations M after some steps, for example using LLL.

Proposition 10 *The output of Algorithm 3 is a matrix Q such that*

– if n is odd, then $\det Q$ is odd, and for all prime $p \mid \det Q$, we have $d = v = 1$ and $m = (n-3)/2$.

– if n is even, then for all prime $p \mid \det Q$, we have $d = v \leqslant 2$. If $p = 2$, then $d = v \leqslant 1$. If $d = v = 2$, then $m = (n-4)/2$.

– if $n = 3$ and $p > 2$, then the condition $v = 1$ is equivalent to the local unsolvability of $X^t Q X = 0$ over $\mathbb{Q}_p$.

– if $n = 4$ and $p > 2$, then the condition $v = 2$ is equivalent to the local unsolvability of $X^t Q X = 0$ over $\mathbb{Q}_p$.

Proof: The first two points are a reformulation of Lemma 4 to Lemma 9, and the remark that every integer is a square modulo 2. The next points are the famous criteria of solvability of the quadratic equations, see for example [7, Th. IV.6]. ■

Remark: This minimization algorithm can be used as a solvability test at any prime $p \neq 2$ for the dimensions 3 and 4. At $p = 2$, a specific test is necessary.

4 Solution in the general case when $n = 3$, or in a specific case when $n = 4$

The algorithm described in [8], for the solution of quadratic equations in dimension 3, can immediately be generalized in dimension 4, but only in the specific case when the determinant is of the form $\det Q_0 = \pm\delta^2$. The algorithm is the following:

Algorithm 4 *Given a symmetric matrix Q_0 with determinant $\Delta_0 \neq 0$, which is either in $\mathcal{M}_3(\mathbb{Z})$, or in $\mathcal{M}_4(\mathbb{Z})$ such that $\Delta_0 = \pm\delta^2 \neq 0$. Either this algorithm proves the unsolvability of $X^t Q_0 X = 0$, or it returns a solution.*

1- Compute the signature (r, s) of Q_0. If $r = 0$ or $s = 0$, then there is no real solution, and stop.

2- Minimize Q_0 using Algorithm 3. Let Q be the new matrix, and Δ its determinant.

3- If Δ has a prime divisor p, then there is no p-adic solution, and stop.
4- Apply Algorithm 2 and find a solution for Q. Deduce a solution for Q_0.

Remark: The validity of this algorithm results directly from sections 1 and 3. Here, we make the observation that, in both dimensions 3 and 4, the local solvability at 2 needs not to be tested after step 3. Indeed, an indefinite integral quadratic form of determinant ± 1 always represents 0.
Remark: It is not difficult to see that this algorithm produces a totally isotropic subspace of maximal dimension ($= \min(r, s)$).

5 Solution in the generic case when $n = 4$

We now describe an algorithm for solving quadratic equations in dimension 4. This algorithm originates in the mixture of the algorithm given in [8] for the dimension 3, and the theoretical proof given by Cassels in [2, §14.7] and [3], for the Theorem of Hasse in dimension 4. Cassels gives a new proof of this theorem, which avoids using Dirichlet's Theorem on primes in arithmetic progressions that caused all classical proofs to be ineffective (see for example [2, §6.5] or [7, ch. IV,Th. 8]). The trick of Cassels consists of increasing the dimension by 2 and using the explicit knowledge of the 2–class group of some well chosen discriminant.

Algorithm 5 (Solution in dimension 4) *Given a symmetric matrix $Q_0 \in \mathcal{M}_4(\mathbb{Z})$ with determinant $\Delta_0 \neq 0$, with $|\Delta_0|$ non–square. We assume that the factorization of Δ_0 is known. Either this algorithm proves the unsolvability of $X^t Q_0 X = 0$, or it returns a solution.*

1- Compute the signature (r, s) of Q_0. If $r = 0$ or $s = 0$, then there is no real solution, and stop. If $r < s$, change Q_0 into $-Q_0$, and exchange r and s.

2- Minimize Q_0 with Algorithm 3. Let Q be the new matrix, and Δ its determinant.

3- If Δ has a square divisor p^2, for a prime p, then there is no p-adic solution, stop the algorithm.

4- Set $\delta = 4\Delta$. Compute the local Witt invariants $\varepsilon_p(Q)$ of Q (for $p \mid \delta$).

5- If $\Delta \equiv 1 \mod 8$ and $\varepsilon_2(Q) = +1$, then there is no 2-adic solution, stop the algorithm.

6- Compute a set of generators $g_1, \ldots g_r$ of the 2-Sylow subgroup $Cl_2(\delta)$ of the group $Cl(\delta)$ of classes of primitive quadratic forms with discriminant δ, using the algorithm given in [1].

7- Compute the Witt invariants $\varepsilon_p(g_i)$ of the g_i (for $p \mid \delta$). Apply linear algebra over $\mathbb{F}_2$ and find a product $g = \prod g_i^{\alpha_i}$ with invariants either $\varepsilon_p(g) = \varepsilon_p(Q)(-1, -\delta)_p$ (case 1), or $\varepsilon_p(g) = \varepsilon_p(Q)(-1, -\delta)_p(2, \delta)_p$ (case 2).

8- Write $g = (a, 2b, c)$. In case 1, set $Q_2' = \begin{pmatrix} a & b \\ b & c \end{pmatrix}$. In case 2, replace g by one of the three forms $(a, 2b, c)$, $(c, -2b, a)$ or $(a + 2b + c, 2b + 2c, c)$ whose first coefficient is even. Write $g = (2a', 2b, c)$, and set $Q_2' = \begin{pmatrix} a' & b \\ b & 2c \end{pmatrix}$.

9- Set $Q_6 = Q \oplus -Q_2'$. Let E be the subspace $\mathbb{Q}^4$ of $\mathbb{Q}^6$ corresponding to this decomposition into orthogonal subspaces. Minimize Q_6, using Algorithm 3 (only step 4 of this algorithm is necessary). Let Q_6' be this new minimized matrix, with determinant -1.

10- Apply Algorithm 2 and find a subspace F of dimension 3, totally isotropic for Q'_6.

11- Determine a nonzero vector in the intersection $E \cap F$. This vector is a solution for Q. Deduce a solution for Q_0.

Remark: Since Δ_0 is not a square, there is no totally isotropic subspace of dimension 2, and we deduce that this algorithm finds a totally isotropic subspace of maximal dimension.

The end of this section will be devoted to the step by step proof of the validity of this algorithm.

Steps 1 – 3 : these steps have already been justified by Proposition 10.

Step 4: If we arrive at this step, we know that $\det Q = \Delta$ is a squarefree integer. The computation of the local Witt invariants $\varepsilon_p(Q)$ can easily be done after diagonalizing Q and computing a few Hilbert symbols (see [7, §IV.2.1]).

In order to justify the next steps, we need a proposition:

Proposition 11 *Let $Q \in \mathcal{M}_4(\mathbb{Z})$ be a symmetric matrix, with $\det Q = \Delta \neq 0$, and Δ squarefree.*

1. Let $p > 2$ be a prime number. Then $X^t Q X = 0$ has a nontrivial solution in $\mathbb{Q}_p^4$.

2. The equation $X^t Q X = 0$ has only the trivial solution in $\mathbb{Q}_2^4$ if and only if $\Delta \equiv 1 \mod 8$ and $\varepsilon_2(Q) = +1$.

Proof: We have to distinguish between the cases $p \mid \Delta$ and $p \nmid \Delta$. But in both cases, it is a direct application of [7, Ch. IV, Th. 6]. ■

Step 5 : We know from the last proposition, that, if the algorithm does not stop after this test, the equation $X^t Q X = 0$ has nontrivial local solutions everywhere, and hence by the Theorem of Hasse also a nontrivial rational solution.

Step 6 : The multiplication by 4 forces δ to be a discriminant, fundamental or not. It is certainly much faster to compute directly the 2–part of the class group of discriminant δ using the algorithm given in [1], which runs in polynomial time, rather than to compute the full class group, in sub–exponential time using the algorithms described in [4, §5.4], and extract its 2–part.

Step 7 : We have to prove the existence of a quadratic form having the given invariants.

Proposition 12 *Consider a symmetric matrix Q with $\det Q = \Delta \neq 0$, Δ squarefree, and signature (r, s). Assume that $X^t Q X = 0$ has a nontrivial solution $\mathbb{Q}^4$. Then there exists a $U \in SL_4(\mathbb{Z})$ such that*

$$U^t Q U = \begin{pmatrix} H & 0 \\ 0 & Q_2 \end{pmatrix}$$

where H is a hyperbolic plane of the form $\begin{pmatrix} 0 & 1 \\ 1 & \alpha \end{pmatrix}$, $\alpha \in \{0, 1\}$. We have

$$\begin{aligned} \det Q_2 &= -\Delta \\ sign(Q_2) &= (r-1, s-1) \\ \varepsilon_p(Q_2) &= \varepsilon_p(Q)(-1, -\Delta)_p \end{aligned}$$

Proof: Let X_1 be a nontrivial solution in $\mathbb{Q}^4$. Without loss of generality, we can assume that the coefficients of X_1 are integers, not all divisible by a common prime. Let $U_1 \in SL_4(\mathbb{Z})$ be a matrix having X_1 as its first column, and define $Q' = U_1^t Q U_1$. Then we have $Q'_{1,1} = 0$. Let $V_2 \in SL_3(\mathbb{Z})$

be a matrix, such that $(Q'_{1,2}, Q'_{1,3}, Q'_{1,4})V_2 = (a, 0, 0)$ (V_2 is given by the Hermite Normal Form algorithm). Set $U_2 = \begin{pmatrix} 1 & 0 \\ 0 & V_2 \end{pmatrix}$. We have then

$$Q'' = U_2^t Q' U_2 = \begin{pmatrix} 0 & a & 0 & 0 \\ a & b_2 & b_3 & b_4 \\ 0 & b_3 & * & * \\ 0 & b_4 & * & * \end{pmatrix} .$$

Since the determinant of Q is squarefree, we have $a^2 = 1$. After a possible scaling of the second and third column of U_2 by -1, we get $a = 1$. Define

$$U_3 = \begin{pmatrix} 1 & -[b_2/2] & -b_3 & -b_4 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} .$$

We see that $U = U_1 U_2 U_3$ satisfies the conclusion of the proposition. The determination of the invariants of Q_2, from those of Q and H, is an easy exercise. ■

At this step, we do not have a solution of $X^t Q X = 0$, and we do not know Q_2. But the existence of such a solution has been proved, and this implies the existence of Q_2. Steps 6 to 8 are building a binary quadratic form Q'_2 having exactly the same invariants as the unknown Q_2. We note here that the choice of the sign, made at step 1, forces the signature of Q_2 to be either $(1, 1)$, or $(2, 0)$, and that Q_2 can not be negative definite. We can write Q_2 in the form $Q_2 = \begin{pmatrix} a & b \\ b & c \end{pmatrix}$ with $\det Q_2 = -\Delta$, or equivalently $Q_2 = aX^2 + 2bXY + cY^2$ with $\operatorname{Disc} Q_2 = 4\Delta$. The problem now comes from the possibility of Q_2 to be imprimitive.

If $\Delta \not\equiv 1 \mod 4$, we see that $\operatorname{Disc} Q_2 = 4\Delta = \delta$ is a fundamental discriminant. In this case, Q_2 is a primitive quadratic form, and the class group $Cl(\delta)$ must contain a form equivalent to Q_2. We remark further, that in $Cl(\delta)$, the forms having an odd order have trivial invariants. This remark shows that Q'_2 can be built inside the 2–Sylow subgroup $Cl_2(\delta)$ of $Cl(\delta)$.

If $\Delta \equiv 1 \mod 4$, $\operatorname{Disc} Q_2 = \delta$ is not a fundamental discriminant any more. If Q_2 is primitive, with discriminant δ, then case 1 will succeed in finding a form with the correct invariants. If Q_2 is not primitive, it is of the form $Q_2 = 2R$, where R is primitive of discriminant $\frac{1}{4}\delta$, and with invariants $\varepsilon_p(R) = \varepsilon_p(Q_2)(2, \delta)_p$. Write $R = (a, b, c)$. We have to prove that R is equivalent to another form with its first coefficients a odd. Indeed, the form R is equivalent to all the three forms (a, b, c), $(c, -b, a)$, and $(a + b + c, b + 2c, c)$, and since $b^2 - 4ac = \delta$ is odd, at least one among the three integers a, c, and $a + b + c$ is odd. We can therefore assume that a is odd, in which case the form $(a, 2b, 4c)$ is primitive if discriminant δ, and has exactly the invariants given by the formulas given in case 2 of step 7.

Step 8 : The discriminant of g is 4δ, hence is even. This proves that g is of the form $(a, 2b, c)$, and that Q'_2 has integral coefficients. In case 1, Q'_2 has the same discriminant and the same invariants as the matrix Q_2 of Proposition 12. In case 2, it is more subtle. By the same arguments as in case 1, we prove that $2g$ has the same local invariants as Q_2, but its discriminant is 4 times larger. We have $g = (2a', 2b, c)$, and $2g = (4a', 4b, 2c)$. The form $(a', 2b, 2c)$ is equivalent over $\mathbb{Q}$ to $2g$, by a transformation matrix of determinant $\frac{1}{2}$. It has thus the same local invariants as $2g$, and its discriminant is divided by 4. This proves that the form Q'_2 has exactly the same invariants as Q_2.

Step 9 : Everything is proved in the following proposition:

Proposition 13 *Let $Q'_2 \in \mathcal{M}_2(\mathbb{Z})$ be a symmetric matrix, such that $\det Q'_2 = -\Delta$, $sign(Q'_2) = (r-1, s-1)$ and $\varepsilon_p(Q'_2) = \varepsilon_p(Q)(-1,-\Delta)_p$ for all prime $p \mid 2\Delta$. Consider $Q_6 = Q \oplus -Q'_2$.*

We have $\det Q_6 = -\Delta^2$ and $sign(Q_6) = (3,3)$.

Furthermore, there exists an $M \in \mathcal{M}_6(\mathbb{Q})$, such that $M^t Q_6 M = Q'_6 \in \mathcal{M}_6(\mathbb{Z})$ with $\det Q'_6 = -1$.

Proof: The invariants of Q_6 are easily checked. We have to prove that Q_6 can be minimized by Lemma 8 for each prime $p \mid \Delta$.

Consider a prime $p \mid \Delta$. Let H and Q_2 be given by Proposition 12. Since Δ is squarefree, we have $\dim_{\mathbb{F}_p} \ker(\overline{Q_2}) = 1 = \dim_{\mathbb{F}_p} \ker(\overline{Q'_2})$, and $\dim_{\mathbb{F}_p} \ker(\overline{Q_6}) = 2$. In a well chosen basis, Q_2 is of the form $Q_2 = \begin{pmatrix} pa & pb \\ pb & c \end{pmatrix}$, as well as $Q'_2 = \begin{pmatrix} pa' & pb' \\ pb' & c' \end{pmatrix}$, where a and a' are coprime to p. Hence, after a unimodular change of basis, we see that Q_6 is equivalent to a new matrix of the form

$$\begin{pmatrix} H & 0 & 0 \\ 0 & Q_2 & 0 \\ 0 & 0 & -Q'_2 \end{pmatrix}$$

and, with the notation of part 3, we have $\tilde{Q}_6 = \begin{pmatrix} a & 0 \\ 0 & -a' \end{pmatrix}$. In particular, $-\det \tilde{Q}_6 = aa'$. By assumption, we have $\varepsilon_p(Q'_2) = \varepsilon_p(Q)(-1,-\Delta)_p$, and by Proposition 12, the Witt invariants $\varepsilon_p(Q_2)$ and $\varepsilon_p(Q'_2)$ are equal. This implies that the Hilbert symbols $(pa, -\Delta)_p$ and $(pa', -\Delta)_p$ are equal. We deduce from this, that $(aa', -\Delta)_p = +1$, where the product aa' is coprime to p. If $p = 2$, then $aa' = 1 \mod 2$ is a square modulo 2. If $p > 2$, then $+1 = (aa', -\Delta)_p = (aa', p)_p$, hence aa' is a square modulo p.

All this proves that we can minimize Q_6 with Lemma 8 for each prime $p \mid \Delta$, and proves the proposition. ■

Steps 10–11 : We have proved that after minimization, the new determinant of Q_6 is -1 and that its signature is $(3,3)$. Using Algorithm 2, we obtain a totally isotropic subspace F of dimension 3. To conclude, it remains only to see that a solution for Q is given by a solution of $Q \oplus -Q'_2$ having 0 in its last two coordinates, that is lying in a 4–dimensional subspace E. Since the subspaces E and F have an intersection of dimension at least $4 + 3 - 6 = 1$, we are certain to get at least one nontrivial solution for Q within step 11.

6 Solution in odd dimension $n \geqslant 5$

The algorithm given now for solving quadratic equations in odd dimensions $n \geqslant 5$ is very similar to the algorithm 5 for the dimension 4. For these high dimensions, the test of the signature is the only test for the solvability of the equation. Since the dimension is odd, the minimization algorithm 3 always leads to a squarefree determinant. Afterwards, the reduction is also done in dimension $n + 2$, using a similar construction of a binary quadratic form with given local invariants.

Algorithm 6 (Solution in odd dimension $n \geqslant 5$) *Given an odd dimension $n \geqslant 5$, and a symmetric matrix $Q_0 \in \mathcal{M}_n(\mathbb{Z})$ with determinant $\Delta_0 \neq 0$. Assume that the factorization of Δ_0 is*

known. This algorithm returns a totally isotropic subspace of maximal dimension (possibly the null space).

1- Compute the signature (r, s) of Q_0. If $r = 0$ or $s = 0$, then there is no real solution: return $\{0\}$. If $r < s$, change Q_0 into $-Q_0$, and exchange r and s.

2- For each prime $p \mid \Delta_0$, minimize Q_0 using Algorithm 3. Let Q be be the minimized matrix, and Δ its determinant.

3- If $\Delta = \pm 1$, apply Algorithm 2, and find a subspace of dimension s, totally isotropic for Q. Deduce a totally isotropic subspace for Q_0 with the same dimension, and return it.

4- Set $\delta = -8|\Delta|$, and compute generators $g_1, \ldots g_r$ of the 2-Sylow subgroup $Cl_2(\delta)$ of the class group $Cl(\delta)$ using the algorithm given in [1].

5- Compute the local Witt invariants $\varepsilon_p(g_i)$ of the g_i (for $p \mid \Delta$). Use linear algebra over $\mathbb{F}_2$ and find a product $g = \prod g_i^{\alpha_i}$ with invariants

$$\varepsilon_p(g) = -((-1)^{(n-1)/2+s} \times 2, p)_p$$

for all $p \mid \Delta$.

6- Write $g = (a, 2b, c)$, and set $Q_2' = \begin{pmatrix} a & b \\ b & c \end{pmatrix}$.

7- Define $Q_{n+2} = Q \oplus -Q_2'$. Let E be the subspace $\mathbb{Q}^n$ of $\mathbb{Q}^{n+2}$ corresponding to this decomposition into orthogonal subspaces. Minimize Q_{n+2}, using Algorithm 3 (only step 4 of this algorithm is necessary for $p \mid \Delta$, $p > 2$, and step 5 for $p = 2$). Let Q_{n+2}' be this new minimized matrix, with determinant ± 1.

8- Apply Algorithm 2 and find a subspace F of dimension $m = \min(r, s+2) \geqslant 3$ totally isotropic for Q_{n+2}'.

9- Determine the intersection $G = E \cap F$, of dimension $M = m - 2 \geqslant 1$, and deduce a subspace of dimension M, totally isotropic for Q_0.

We have to prove this algorithm, step by step.

Step 1: After step 1, we have $s < r$ (because $s \leqslant r$ and $n = r + s$ is odd).

Step 2: By Proposition 10, we know, that after minimization, Δ is an odd squarefree integer, and that for all prime $p \mid \Delta$, Q is such that $(-1)^{m+1} \frac{\Delta}{Q_{1,1}}$ is not a square modulo p, where $m = (n-3)/2$ and $Q_{1,1} = X^t Q X$, where the kernel of Q modulo p is generated by X modulo p.

Step 3: This step is described in part 1. We have $s = \min(r, s)$ because of the choice that we made for the sign at step 1. The dimension of the totally isotropic subspace found at this step is clearly maximal.

Step 4: Since Δ is odd and squarefree, $\delta = -8|\Delta|$ is a fundamental discriminant, and the quadratic forms in $Cl_2(\delta)$ are positive definite.

Step 5: Here, we build a new positive definite quadratic form. Its real Witt invariant is $+1$. Since Δ is odd, we will not consider any Witt invariant at 2: indeed, this invariant will be fixed by the value of the Witt invariants at the other primes, and the product formula. We now have to prove the existence of a form with discriminant δ having the given invariants. As already seen, it is enough to consider the 2–class group $Cl_2(\delta)$. The existence is proved be the proposition:

Proposition 14 *Let Δ be an odd integer, and $\delta = -8|\Delta|$.*

For each prime $p \mid \Delta$, choose any value $\varepsilon_p \in \{+1, -1\}$.

There exists a positive definite quadratic form g in $Cl_2(\delta)$, such that its Witt invariants are

$$\begin{array}{rll} \varepsilon_\infty(g) & = +1 & \\ \varepsilon_p(g) & = \varepsilon_p & \text{for } p \mid \Delta \\ \varepsilon_p(g) & = +1 & \text{for } p \nmid \Delta, p > 2 \end{array}$$

Proof: By the Theorem of Gauss (see [2, §14.5]), such a form exists if and only if these invariants satisfy the product formula and are such that, there exists everywhere locally an integral quadratic form with discriminant δ and having the corresponding Witt invariant. Since the local invariant $\varepsilon_2(g)$ is not fixed by the conditions of the proposition, we can define ε_2 as the product of the other ε_p, and the product formula is automatically satisfied.

It now remains to prove the existence, everywhere locally, of an integral quadratic form with discriminant δ and Witt invariant ε_p.

If $\varepsilon_p = +1$, the form $X^2 - \frac{\delta}{4}Y^2$ is suitable. This is, for example, the case for the real place (it is positive definite), as well as for all $p \nmid 2\Delta$.

Consider now a prime $p \mid \Delta$, such that $\varepsilon_p = -1$. We have $p \neq 2$. Let $e \in \mathbb{Z}_p$, $e \notin p\mathbb{Z}_p$, be such that e is not a p–adic square. The form $eX^2 - \frac{\delta}{4e}Y^2$ is integral, with discriminant δ and Witt invariant $\varepsilon_p = (e, \delta)_p = -1$.

Consider the last case $p = 2$. The form $X^2 - \frac{\delta}{4}Y^2$ is suitable if $\varepsilon_2 = +1$. If $|\Delta| \equiv 1 \mod 4$, then the form $-X^2 + \frac{\delta}{4}Y^2$ has discriminant δ and Witt invariant $\varepsilon_2 = (-1, \delta)_2 = -1$. If $|\Delta| \equiv -1 \mod 4$, then the form $3X^2 + \frac{\delta}{12}Y^2$ has discriminant δ and Witt invariant $\varepsilon_2 = (3, \delta)_2 = -1$. ■

Remark: The existence of a form with the same Witt invariants is not guaranteed among the forms of discriminant $-|\Delta|$ or $-4|\Delta|$. Indeed, if $|\Delta| \equiv -1 \mod 8$, we can see that any form of discriminant $\delta = -|\Delta|$ or $-4|\Delta|$ has its Witt invariant $\varepsilon_2 = +1$, and there are choices of the other ε_p which do not satisfy the product formula.

Step 6: Since δ is even, g is of the form $(a, 2b, c)$, which implies that $Q_2' \in \mathcal{M}_2(\mathbb{Z})$ has a determinant equal to $\det Q_2' = 2|\Delta|$.

Step 7: Let us show that the choice of the invariants of Q_2' allow a complete minimization of Q_{n+2}.

Proposition 15 *Let $n \geqslant 5$ be an odd dimension, and $Q \in \mathcal{M}_n(\mathbb{Z})$ be a symmetric matrix with an odd squarefree determinant Δ. Let (r, s) be its signature. Assume that for all prime $p \mid \Delta$, Q satisfies the conclusion of Proposition 10.*

Let $Q_2' \in \mathcal{M}_2(\mathbb{Z})$ be a symmetric matrix, such that $\det Q_2' = 2|\Delta|$, $\varepsilon_p(Q_2') = -((-1)^{(n-1)/2+s} \times 2, p)_p$ for all prime $p \mid \Delta$.

Consider $Q_{n+2} = Q \oplus -Q_2'$.

There exists an $M \in \mathcal{M}_{n+2}(\mathbb{Q})$ such that $\frac{1}{2}M^t Q_{n+2} M = Q_{n+2}' \in \mathcal{M}_4(\mathbb{Z})$ with $\det Q_{n+2}' = \pm 1$.

Proof: We have $|\det Q_{n+2}| = 2|\Delta|^2$. Since $n + 2$ is odd and $v_2(\det Q_{n+2}) = 1$, we can certainly minimize Q_{n+2} at 2 using Lemma 2 and Lemma 9. We shall show that the minimization of Q_{n+2} at a prime $p \mid \Delta$ is possible using Lemma 8. We use the notation of this lemma. Since $v_p(\det Q) = 1 = v_p(\det Q_2')$, we already get $d = v = 2$. Now, Q satisfies the conclusion of Proposition 10, and we know that Q is equivalent to a matrix of the form $\begin{pmatrix} pa & p* \\ p* & Q_{n-1} \end{pmatrix}$, where $a \in \mathbb{Z}$ and $Q_{n-1} \in \mathcal{M}_{n-1}(\mathbb{Z})$ with $p \nmid a$ and $p \nmid \det Q_{n-1}$. If we write Q_2' in the form $(b, 2c, d)$, we

have $4(c^2 - bd) = \delta$. But we have $p \mid \delta$, so we can assume that $b = pb'$ with $p \nmid b'$. Using the same notation as in Lemma 8, we have $\tilde{Q} = \begin{pmatrix} a & 0 \\ 0 & -b' \end{pmatrix}$, and $-\det \tilde{Q} = ab' \mod p$.

In order to be able to apply Lemma 8, it remains to prove that ab' is a square modulo p, or equivalently that the Hilbert symbols $(pa, p)_p$ and $(pb', p)_p$ are equal. We know that Q satisfies the conclusion of Proposition 10, and we have $m = (n-3)/2$. By Proposition 2 (applied to Q_{n-1}), we get that $(-1)^{(n-1)/2} \det Q_{n-1}$ is not a square modulo p. We have then

$$-1 = ((-1)^{(n-1)/2} \det Q_{n-1}, p)_p = \left((-1)^{(n-1)/2} \frac{\Delta}{pa}, p \right)_p ,$$

and then

$$(pa, p)_p = -((-1)^{(n-1)/2} \Delta, p)_p$$

Since we have $\delta = -8|\Delta|$ and $\Delta = (-1)^s |\Delta|$, we obtain $\delta = -(-1)^s 8\Delta$, and then

$$(pa, p)_p = -((-1)^{(n-1)/2+s} \times 2, p)_p (-\delta, p)_p = \varepsilon_p(Q_2')(-\delta, p)_p .$$

By definition of the Witt invariant, we have $\varepsilon_p(Q_2') = (pb', \delta)_p$, and then

$$(pa, p)_p = (pb', \delta)_p (-\delta, p)_p = (b', \delta)_p (-1, p)_p = (b', p)_p (p, p)_p = (pb', p)_p$$

■

Step 8: The signature of Q is (r, s) with $r > s$, and the signature of Q_2' is $(2, 0)$. The signature of Q_{n+2}' is therefore $(r, s+2)$. After applying Algorithm 1, we obtain a totally isotropic subspace F of dimension $m = \min(r, s+2)$. The condition $r > s$ implies $r > \frac{n}{2}$, and $r \geqslant \frac{n+1}{2} \geqslant 3$. We also have $s \geqslant 1$, and $s + 2 \geqslant 2$, which proves that the subspace F has dimension at least 3.

Step 9: Let M be the dimension of $G = E \cap F$. The subspaces E and F have dimension n and $m \geqslant 3$, in a space of dimension $n + 2$. Their intersection has then a dimension $M \geqslant m - 2 \geqslant 1$.

Let us show that $M = m - 2$. This dimension is also the dimension of a totally isotropic subspace for Q_0. Since Q_0 has a nonzero determinant, this dimension is bounded by $\min(r, s) = s$. We have then $\min(r-2, s) \leqslant M \leqslant \min(r, s)$. If $s \leqslant r - 2$, this gives the equality $M = m$. Since n is odd, we can not have $r = s$, and the only possible remaining case is $s = r - 1$. In that case, the inequality becomes $m - 2 = s - 1 \leqslant M \leqslant s$.

Suppose that we have $M = s = r - 1$. This means that we can make a change of variables over $\mathbb{Z}$, such that Q is of the form $Q = H^{\oplus s} \oplus u$, where $u \in \mathcal{M}_1(\mathbb{Z})$ has coefficient $(-1)^s \det Q$. Using Lemma 2 and Lemma 9, we can minimize Q at any prime $p \mid \det Q$. But Q has already been minimized at step 2, which implies that $\Delta = \pm 1$, and that the algorithm would have already stopped at step 3. This proves that at step 9, this can not happen, and we must have $M = s - 1 = m - 2$.

It also proves that the totally isotropic subspace that the algorithm produces is maximal.

7 Solution in even dimension $n \geqslant 6$

Algorithm 7 (Solution in even dimension $n \geqslant 6$) *Given an even dimension $n \geqslant 6$, and a symmetric matrix $Q_0 \in \mathcal{M}_n(\mathbb{Z})$ with determinant $\Delta_0 \neq 0$ and signature (r, s). We assume that*

the factorization of Δ_0 is known. This algorithm either proves the unsolvability of the equation $X^t Q_0 X = 0$, or it returns a totally isotropic subspace of dimension $g \geqslant 1$ with

$$\begin{array}{rll} & g = \min(r,s) & \text{if } |r-s| > 2 \\ \min(r,s) - 1 \leqslant & g \leqslant \min(r,s) & \text{if } |r-s| = 2 \\ \min(r,s) - 2 \leqslant & g \leqslant \min(r,s) & \text{if } |r-s| = 0 \end{array}$$

`1- Compute the signature` (r,s) `of` Q_0`. If` $r = 0$ `or` $s = 0$`, then there is no real solution, and stop the algorithm. If` $r < s$`, change` Q_0 `into` $-Q_0$`, and exchange` r `and` s`.`

`2- Minimize` Q_0 `using Algorithm 3. Let` Q `be the new matrix, and` Δ `its determinant.`

`3- If` $\Delta = \pm 1$`, apply Algorithm 2 to` Q`, and find a totally isotropic subspace for` Q `of dimension` s`. Deduce a totally isotropic subspace for` Q_0 `of the same dimension and stop the algorithm.`

`4- Set` $Q_{n+1} = Q \oplus -1$`. Let` E `be the subspace` $\mathbb{Q}^n$ `of` $\mathbb{Q}^{n+1}$ `corresponding to this decomposition into orthogonal subspaces.`

`5- Apply Algorithm 6, and get a totally isotropic subspace` F `for` Q_{n+1}`, of dimension` $f \geqslant 2$`.`

`6- Determine the intersection` $G = E \cap F$`, of dimension` $g \geqslant f-1 \geqslant 1$`. This subspace is totally isotropic of` Q`. Deduce from it a totally isotropic subspace for` Q_0 `of dimension` g`.`

Remark: Using this algorithm, we can obtain a decomposition of Q_0 in the form $Q_0 = H^{\oplus g} \oplus D$, where D is of even dimension at most 4. Since we know how to solve $D = 0$, it is an easy task to deduce a totally isotropic subspace for Q_0 of maximal dimension.

We will now prove the valididy of the algorithm.

Steps 1–3: these steps are similar to the steps 1–3 of Algorithm 6.

Step 4: The form Q_{n+1} has an odd dimension, and its signature is $(r, s+1)$.

Step 5: If $s+1 \geqslant r$, this implies that $r = s = \frac{n}{2}$. In this case, Algorithm 6 finds a totally isotropic subspace F for Q_{n+1} of dimension $f \geqslant r-1 = \min(r-1, s-1) \geqslant 2$. If $s+1 = r-1$, we have $f \geqslant s = \min(r,s)$. In the other cases, we have $s \leqslant r-4$, and $f = s+1 = \min(r+1, s+1)$. In any case, we have $f \geqslant 2$.

Step 6: In the case $|r-s| \leqslant 2$, we have $f \geqslant \min(r-1, s-1)$. Taking the intersection with E of codimension 1, we obtain $g \geqslant f-1 \geqslant \min(r-2, s-2)$. In the other cases, we have $f = \min(r+1, s+1)$, and then $g \geqslant \min(r,s)$. But we have the trivial inequality $g \leqslant \min(r,s)$, which is true in all cases (because it corresponds to the maximal dimension of a totally isotropic subspace over the reals). All this proves that the dimension g is indeed the dimension announced in front of the algorithm. This dimension is $g \geqslant 1$, which means that the algorithm finds at least one nontrivial solution.

Remark: It would be interesting to prove that Algorithm 7 indeed produces an isotropic subspace of maximal dimension, or to modify it so as to get one.

8 Performance of the general algorithm

We have implemented Algorithm 5 in GP, and we report here the speed of this implementation. The tested matrices have random integer coefficients in the range $[-2^t, 2^t]$, where the value of t

Figure 1: Performance in dimension 4

Figure 2: Performance in various dimensions

runs from 4 to 57. For each value of t, we have tested our algorithm with 100 different symmetric matrices Q_0. The total time spent in Algorithm 5, as well as the time needed for the factorization is given by Figure 1.

We observe that the major difficulty in solving quadratic equations in dimension 4 is the factorization of the determinant. No other factorization is needed in the rest of the algorithm, which seems to run (on average) in linear time. It should not be difficult to prove that it runs in polynomial time. A small irregularity is observed in Figure 1 around $t = 50$: this reflects the fact that the determination of the 2–class group of a given quadratic discriminant δ using the algorithm of [1], has a different behaviour in the average and in the worst case.

We have made the same tests for Algorithm 6 and Algorithm 7. The results of our experiments are given in Figure 2, where we can compare their behaviour when the dimension varies. If we apply Algorithm 7 in dimension $2n$ and Algorithm 6 in dimension $2n + 1$, they both work in dimension $2n + 3$: this explains the similarity between the behaviour in dimensions $2n$ and $2n + 1$.

We have also made a few experiments for higher dimensions. However, we have been limited to $n \leqslant 25$, because of the neverending time necessary for the factorization of the determinant. For these high dimensions, we can make exactly the same remarks as for dimension 4: the running time seems to be almost linear in t, but exponential in n.

9 Possible improvements

In [8], the reduction algorithm is described using exact arithmetic. It is highly conceivable that an implementation of this algorithm using floating point arithmetic would dramatically improve the total running time of Algorithm 5. Indeed, this reduction algorithm is used at several places. First, it is used (in dimension 4) in step 2 (it is not necessary, but it reduces the transformation matrix significantly). It is also used in step 10 (in dimension 6), where we have to reduce a matrix, whose coefficients are typically of the size of Δ_0. But it can also be used several times in step 6. Indeed, the algorithm given in [1] for computing the 2–class group of a given discriminant, relies in an essential way on the computation of square roots in this group. As we can see in [9], this particular problem is equivalent to solving a ternary quadratic equation, a task that is solved in [8] using the reduction algorithm in dimension 3.

For the same reason, a floating point reduction algorithm would certainly give a significant improvement for the solution of quadratic equations in higher dimensions by Algorithm 6 or Algorithm 7.

References

[1] W. Bosma and P. Stevenhagen : *On the computation of quadratic 2-class groups*, J. Théor. Nombres Bordeaux **8** (1996), no. 2, 283–313.

[2] J.W.S. Cassels : *Rational Quadratic Forms*, L.M.S. Monographs, Academic Press (1978).

[3] J.W.S. Cassels : *Note on quadratic forms over the rational field* , Proc. Cambridge Philos. Soc. **55** (1959), 267–270.

[4] H. Cohen: *A Course in Computational Algebraic Number Theory*, Graduate Texts in Math. **138**, Third corrected printing, Springer–Verlag (1996).

[5] J.E. Cremona, D. Rusin: *Efficient solution of rational conics*, Math. Comp. **72** (2003), 1417–1441.

[6] C.F. Gauss: *Disquisitiones Arithmeticae*, Springer Verlag (1986).

[7] J.P. Serre : *Cours d'Arithmétique*, P.U.F. (1970).

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

[9] D. Simon: *Sur la paramétrisation des solutions des équations quadratiques*, preprint (2004).

[10] D. Simon: *Formes quadratiques unimodulaires réduites en petite dimension*, preprint (2005).

[11] C. van de Woestijne: *Deterministic equation solving over finite fields*, Ph.D. thesis, Leiden University (2005).