Solving quadratic equations in dimension 5 or more without factoring

ANTS X
UCSD July, 9–13 2012

Pierre Castel
pierre.castel@unicaen.fr – http://www.math.unicaen.fr/~castel

Laboratoire de Mathématiques Nicolas Oresme
CNRS UMR 6139
Université de Caen (France)

Summary

What's next: Introduction

Quadratic equations...

We consider homogenous quadratic equations with integral coefficients and search for a nontrivial and integral solution.

Quadratic equations...

We consider homogenous quadratic equations with integral coefficients and search for a nontrivial and integral solution.
Dimension 1:

Equation:

$$ax^2 = 0$$

Solution:

$$x = 0$$

Quadratic equations...

We consider homogenous quadratic equations with integral coefficients and search for a nontrivial and integral solution.

Dimension 1:

Equation:

$$ax^2 = 0$$

Solution:

$$x = 0$$

Dimension 2:

Equation:

$$ax^2 + bxy + cy^2 = 0$$

Solution:

1. Compute $\Delta = b^2 - 4ac$
2. If Δ is a square, solutions are:

$$x = \frac{-b \pm \sqrt{\Delta}}{2a} y$$

Minimisation and Reduction

We use the matrix notation: Q is the n–dimensional symmetric matrix containing the coefficients of the equation.
The equation is now:

$$^{t}XQX = 0$$

with $X \in \mathbb{Z}^n$.

Minimisation and Reduction

We use the matrix notation: Q is the n–dimensional symmetric matrix containing the coefficients of the equation.
The equation is now:

$$^{t}XQX = 0$$

with $X \in \mathbb{Z}^n$.
Let Q be a quadratic form with determinant Δ.

- Minimising Q: finding transformations for Q in order to get another quadratic form Q' with same dimension as Q such that:
  - Q' and Q have the same solutions (up to a basis change),
  - $\det(Q')$ divides Δ.

Minimisation and Reduction

We use the matrix notation: Q is the n–dimensional symmetric matrix containing the coefficients of the equation.
The equation is now:

$$^{t}XQX = 0$$

with $X \in \mathbb{Z}^n$.
Let Q be a quadratic form with determinant Δ.

- Minimising Q: finding transformations for Q in order to get another quadratic form Q' with same dimension as Q such that:
  - Q' and Q have the same solutions (up to a basis change),
  - $\det(Q')$ divides Δ.
- Reducing the form Q: it's finding a basis change B such that:
  - $\det(B) = \pm 1$,
  - the coefficients of $Q' = {}^{t}BQB$ are smaller than the ones of Q.

Quadratic equations in dimensions 3, 4 and more: Simon's algorithm

1. Factor the determinant of Q,
2. Minimise Q relatively to each prime factor of $\det(Q)$,
3. Reduce Q using the LLL algorithm,
4. Use number theory tools in order to end the minimisation of Q,
5. Considering intersections of some isotropic spaces of good dimension, deduce a solution for the form of the beginning.

Quadratic equations in dimensions 3, 4 and more: Simon's algorithm

1. Factor the determinant of Q,
2. Minimise Q relatively to each prime factor of $\det(Q)$,
3. Reduce Q using the LLL algorithm,
4. Use number theory tools in order to end the minimisation of Q,
5. Considering intersections of some isotropic spaces of good dimension, deduce a solution for the form of the beginning.

This algorithm:

- creates a link between factoring and solving quadratic equations
- can be generalised to forms of higher dimension

The problem:

Pro:

As soon as the factorisation of the determinant is known, Simon's algorithm is very efficient.

The problem:

Pro:

As soon as the factorisation of the determinant is known, Simon's algorithm is very efficient.

Cons:

But as soon as the size of the determinant reaches $\simeq 50$ digits, the factorisation becomes prohibitively slow.

The problem:

Pro:

As soon as the factorisation of the determinant is known, Simon's algorithm is very efficient.

Cons:

But as soon as the size of the determinant reaches $\simeq 50$ digits, the factorisation becomes prohibitively slow.

So, we are given the following problem:

Problem:

Let Q be a dimension 5 quadratic form. We assume that $\det(Q)$ cannot be factored (in a reasonable amount of time). Find a non zero vector $X \in \mathbb{Z}^5$ such that:

$$ {}^tXQX = 0 $$

What's next: The algorithm

2. The algorithm
   - Principle
   - Completion
   - Computing a solution
   - Minimisations

Principle

Simon's algorithm is very efficient as soon as the factorization of $\det(Q)$ is known.

Principle

Simon's algorithm is very efficient as soon as the factorization of $\det(Q)$ is known.

Idea:

1. Build another quadratic form Q_6 starting from Q *for which computing a solution is " easy "*,

Principle

Simon's algorithm is very efficient as soon as the factorization of $\det(Q)$ is known.

Idea:

1. Build another quadratic form Q_6 starting from Q *for which computing a solution is " easy "*,
2. Use Simon's algorithm to find a solution for Q_6,

Principle

Simon's algorithm is very efficient as soon as the factorization of $\det(Q)$ is known.

Idea:

1. Build another quadratic form Q_6 starting from Q *for which computing a solution is " easy "*,
2. Use Simon's algorithm to find a solution for Q_6,
3. Deduce a solution for Q.

How to build Q_6?

If Q designs the matrix of the quadratic form Q, we build Q_6 in the following way:

$$Q_6 = \left[\begin{array}{c:c} Q & X \\ \hdashline {}^tX & z \end{array}\right]$$

Where $X \in \mathbb{Z}^5$ is randomly chosen and $z \in \mathbb{Z}$.

How to build Q_6?

If Q designs the matrix of the quadratic form Q, we build Q_6 in the following way:

$$Q_6 = \left[\begin{array}{c:c} Q & X \\ \hdashline {}^tX & z \end{array}\right]$$

Where $X \in \mathbb{Z}^5$ is randomly chosen and $z \in \mathbb{Z}$.
So we have:

$$\boxed{\det(Q_6) = \det(Q)z - {}^tX \operatorname{Co}(Q) X}$$

And we choose z such that:
$\det(Q_6) = -{}^tX \operatorname{Co}(Q) X \pmod{\det(Q)}$.

The way to the solution...

As the value of $\det(Q_6)$ is known in advance, we try some vector X until we have $\det(Q_6)$ prime.

Principle:

$\det(Q_6)$ being prime, it is possible to use Simon's algorithm in order to find a vector $T \in \mathbb{Z}^6$ such that:

$$^{t}TQ_6T = 0$$

The vector T is isotropic for Q_6. So, in a basis whose first vector is T, Q_6 has the form:

$$Q_6 = \begin{bmatrix} 0 & * & * & * & * & * \\ * & * & * & * & * & * \\ * & * & * & * & * & * \\ * & * & * & * & * & * \\ * & * & * & * & * & * \\ * & * & * & * & * & * \end{bmatrix}$$

Decomposition $Q_6 = H \oplus Q_4$

The vector T is a solution for Q_6 so there exists an hyperbolic plane which contains it. With linear algebra (GCD), we get a "correct" basis. In such a basis, Q_6 has the shape:

$$Q_6 = \left[\begin{array}{cc|cccc} 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & \alpha & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & & & & \\ 0 & 0 & & \multicolumn{2}{c}{Q_4} & \\ 0 & 0 & & & & \\ 0 & 0 & & & & \end{array}\right]$$

Where $\alpha \in \{0, 1\}$ and Q_4 is a dimension 4 quadratic form, with determinant $-\det(Q_6)$. So it's prime again...

Decomposition $Q_6 = H \oplus H' \oplus Q_2$

...so we do it again : Simon's algorithm and linear algebra with Q_4. In the new basis, Q_6 has the following shape:

$$Q_6 = \left[\begin{array}{cc|cc|cc} 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & \alpha & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & \beta & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & \multicolumn{2}{c}{\multirow{2}{*}{Q_2}} \\ 0 & 0 & 0 & 0 & & \end{array}\right]$$

where $\alpha,\ \beta \in \{0, 1\}$ and Q_2 is a dimension 2 quadratic form.

If we denote by e_1 and e_3 the following basis vectors:

$$Q_6 = \left[\begin{array}{cc:cc:cc} 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & \alpha & 0 & 0 & 0 & 0 \\ \hdashline 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & \beta & 0 & 0 \\ \hdashline 0 & 0 & 0 & 0 & \multicolumn{2}{c}{\multirow{2}{*}{Q_2}} \\ 0 & 0 & 0 & 0 & & \end{array}\right]$$

If we denote by e_1 and e_3 the following basis vectors:

$$\begin{array}{c} \begin{array}{cccccc} e_1 & & e_3 & & & \end{array} \\ Q_6 = \left[\begin{array}{cc|cc|cc} 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & \alpha & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & \beta & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & \multicolumn{2}{c}{\multirow{2}{*}{Q_2}} \\ 0 & 0 & 0 & 0 & & \end{array}\right] \end{array}$$

Then e_1 and e_3 are both isotropics and orthogonals.

If we denote by e_1 and e_3 the following basis vectors:

$$
Q_6 = \begin{array}{c} \begin{array}{cccccc} e_1 & & e_3 & & & \end{array} \\ \left[\begin{array}{cc:cc:cc} 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & \alpha & 0 & 0 & 0 & 0 \\ \hdashline 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & \beta & 0 & 0 \\ \hdashline 0 & 0 & 0 & 0 & \multicolumn{2}{c}{\multirow{2}{*}{Q_2}} \\ 0 & 0 & 0 & 0 & & \end{array}\right] \end{array}
$$

Then e_1 and e_3 are both isotropics and orthogonals.

The solution:

consider a linear combinaison whose last coordinate is zero.
Example:

$$\widetilde{S} = e_3(6) \times e_1 - e_1(6) \times e_3$$

So $\widetilde{S}$ has the shape:

$$\widetilde{S} = \left[\begin{array}{c} S \\ \hdashline 0 \end{array}\right] \text{ with } S \in \mathbb{Z}^5$$

Assuming that all of the basis changes have been applied, we have:

$$\begin{aligned} {}^t\widetilde{S} Q_6 \widetilde{S} &= \left[\begin{array}{c:c} {}^tS & 0 \end{array}\right] \left[\begin{array}{c:c} Q & X \\ \hdashline {}^tX & z \end{array}\right] \left[\begin{array}{c} S \\ \hdashline 0 \end{array}\right] \\ &= {}^tSQS \\ &= 0 \end{aligned}$$

We have then:

S is a solution to our problem.

The algorithm:

1. Complete Q in Q_6 in such a way that $\det(Q_6)$ is prime,
2. Use Simon's algorithm for Q_6,
3. Using linear algebra, decompose Q_6 in $Q_6 = H \oplus Q_4$ (H hyperbolic plane),
4. Do step 2 for Q_4,
5. Using linear algebra, decompose Q_6 in $Q_6 = H \oplus H' \oplus Q_2$ (H, H' hyperbolic planes),
6. Deduce a solution for Q.

Smith Normal Form:

SNF Decomposition

Let A be a $k \times k$ matrix with integer entries and non zero determinant. There exists a unique matrix in Smith Normal Form D such that $UAV = D$ with U and V unimodular and integer entries.

If we denote by $d_i = d_{i,i}$, the d_i are the *elementary divisors* of the matrix A, and we have :

$$UAV = \begin{bmatrix} d_1 & 0 & \dots & 0 \\ 0 & d_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & d_k \end{bmatrix}$$

with $d_{i+1} \mid d_i$ for $1 \leq i < k$

The problem:

In the algorithm, we are looking for $X \in \mathbb{Z}^5$ such that $\det(Q_6)$ is prime. However :

Lemma

Let Q be a dimension 5 quadratic form with determinant Δ. Then for all $X \in \mathbb{Z}^5$ and $z \in \mathbb{Z}$, $d_2(Q)$ divides $\det(Q_6)$.

The problem:

In the algorithm, we are looking for $X \in \mathbb{Z}^5$ such that $\det(Q_6)$ is prime. However :

Lemma

Let Q be a dimension 5 quadratic form with determinant Δ. Then for all $X \in \mathbb{Z}^5$ and $z \in \mathbb{Z}$, $d_2(Q)$ divides $\det(Q_6)$.

Problem

If $d_2(Q) \neq 1$, $\det(Q_6)$ will never be a prime !

The solution:

Solution

Do minimisations on Q to be in the case where $d_2(Q) = 1$.

The solution:

Solution

Do minimisations on Q to be in the case where $d_2(Q) = 1$.

We have the different cases:

1. Case $d_5(Q) \neq 1$,
2. Case $d_4(Q) \neq 1$ and $d_5(Q) = 1$,
3. Case $d_3(Q) \neq 1$ and $d_4(Q) = 1$,
4. Case $d_2(Q) \neq 1$ and $d_3(Q) = 1$.

Cases 1, 2 and 3

We apply the basis change given by the matrix V of the SNF of Q:

- if $d_5(Q) \neq 1$:
  - we just have to divide the matrix by d_5,
  - we have divided $\det(Q)$ by $(d_5)^5$.
- if $d_4(Q) \neq 1$ and $d_5(Q) = 1$:
  - we multiply the last row and column by d_4,
  - we divide the matrix by d_4,
  - we have multiplied $\det(Q)$ by $(d_4)^2$ and divided by $(d_4)^5$.
- if $d_3(Q) \neq 1$ and $d_4(Q) = 1$:
  - we multiply the two last rows and columns by d_3,
  - we divide the matrix by d_3,
  - we have multiplied $\det(Q)$ by $(d_3)^4$ and divided by $(d_3)^5$.

Case $d_2(Q) \neq 1$ and $d_3(Q) = 1$

We first apply the basis change given by the matrix V of the SNF of Q. In such a base, Q has the form :

$$\left[\begin{array}{cc|ccc} d_2* & d_2* & d_2* & d_2* & d_2* \\ d_2* & d_2* & d_2* & d_2* & d_2* \\ \hline d_2* & d_2* & * & * & * \\ d_2* & d_2* & * & * & * \\ d_2* & d_2* & * & * & * \end{array}\right]$$

Case $d_2(Q) \neq 1$ and $d_3(Q) = 1$

We first apply the basis change given by the matrix V of the SNF of Q. In such a base, Q has the form :

$$\left[\begin{array}{cc:ccc} d_2* & d_2* & d_2* & d_2* & d_2* \\ d_2* & d_2* & d_2* & d_2* & d_2* \\ \hdashline d_2* & d_2* & * & * & * \\ d_2* & d_2* & * & * & * \\ d_2* & d_2* & * & * & * \end{array}\right]$$

- We would like to multiply the 3 lasts rows and columns by d_2 and divide the matrix by d_2.

Case $d_2(Q) \neq 1$ and $d_3(Q) = 1$

We first apply the basis change given by the matrix V of the SNF of Q. In such a base, Q has the form :

$$\left[\begin{array}{cc|ccc} d_2* & d_2* & d_2* & d_2* & d_2* \\ d_2* & d_2* & d_2* & d_2* & d_2* \\ \hline d_2* & d_2* & * & * & * \\ d_2* & d_2* & * & * & * \\ d_2* & d_2* & * & * & * \end{array}\right]$$

- We would like to multiply the 3 lasts rows and columns by d_2 and divide the matrix by d_2.
- But if we do this, we multiply the determinant by d_2^6 and we divide it by $d_2^5\dots$

Case $d_2(Q) \neq 1$ and $d_3(Q) = 1$

We first apply the basis change given by the matrix V of the SNF of Q. In such a base, Q has the form :

$$\left[\begin{array}{cc|ccc} d_2* & d_2* & d_2* & d_2* & d_2* \\ d_2* & d_2* & d_2* & d_2* & d_2* \\ \hline d_2* & d_2* & * & * & * \\ d_2* & d_2* & * & * & * \\ d_2* & d_2* & * & * & * \end{array}\right]$$

- We would like to multiply the 3 lasts rows and columns by d_2 and divide the matrix by d_2.
- But if we do this, we multiply the determinant by d_2^6 and we divide it by $d_2^5 \ldots$

Solution:

Solve a quadratic equation modulo d_2 such that:
$Q_{3,3} \equiv 0 \pmod{d_2}$
and do the desired operation on the two lasts rows and columns.

How to get $Q_{3,3} \equiv 0 \pmod{d_2}$?

We begin by a Gram–Schmidt orthogonalisation on the 3×3 block modulo d_2. In that basis, the block Q_3 has the form:

$$\begin{bmatrix} a & & 0 \\ & b & \\ 0 & & c \end{bmatrix} \pmod{d_2}$$

How to get $Q_{3,3} \equiv 0 \pmod{d_2}$?

We begin by a Gram–Schmidt orthogonalisation on the 3×3 block modulo d_2. In that basis, the block Q_3 has the form:

$$\begin{bmatrix} a & & 0 \\ & b & \\ 0 & & c \end{bmatrix} \pmod{d_2}$$

It remains to solve the equation:

$$ax^2 + by^2 + cz^2 \equiv 0 \pmod{d_2}$$

How to get $Q_{3,3} \equiv 0 \pmod{d_2}$?

We begin by a Gram–Schmidt orthogonalisation on the 3×3 block modulo d_2. In that basis, the block Q_3 has the form:

$$\begin{bmatrix} a & & 0 \\ & b & \\ 0 & & c \end{bmatrix} \pmod{d_2}$$

It remains to solve the equation:

$$ax^2 + by^2 + cz^2 \equiv 0 \pmod{d_2}$$

How?

1. Simon's algorithm?

How to get $Q_{3,3} \equiv 0 \pmod{d_2}$?

We begin by a Gram–Schmidt orthogonalisation on the 3×3 block modulo d_2. In that basis, the block Q_3 has the form:

$$\begin{bmatrix} a & & 0 \\ & b & \\ 0 & & c \end{bmatrix} \pmod{d_2}$$

It remains to solve the equation:

$$ax^2 + by^2 + cz^2 \equiv 0 \pmod{d_2}$$

How?

1. Simon's algorithm?
2. CRT?

How to get $Q_{3,3} \equiv 0 \pmod{d_2}$?

We begin by a Gram–Schmidt orthogonalisation on the 3×3 block modulo d_2. In that basis, the block Q_3 has the form:

$$\begin{bmatrix} a & & 0 \\ & b & \\ 0 & & c \end{bmatrix} \pmod{d_2}$$

It remains to solve the equation:

$$ax^2 + by^2 + cz^2 \equiv 0 \pmod{d_2}$$

How?

1. Simon's algorithm?
2. CRT?
3. Pollard–Schnorr's algorithm.

Pollard–Schnorr's algorithm (1987)

Solves equations of type:

$$x^2 + ky^2 = m \pmod{n}$$

Pollard–Schnorr's algorithm (1987)

Solves equations of type:

$$x^2 + ky^2 = m \pmod{n}$$

Without factoring n

Principle:

- Based on the property of multiplicativity of the norm in quadratic extensions:
$$(x_1^2 + ky_1^2)(x_2^2 + ky_2^2) = X^2 + kY^2$$
- Variables changes to decrease the size of the coefficients
- To be in the case where:

$$(k, m) \in \{(1,1), (-1,1), (-1,-1)\}$$

Using Pollard–Schnorr

We'd like to solve:

$$ax^2 + by^2 + cz^2 = 0 \pmod{d_2}$$

Using Pollard–Schnorr

We'd like to solve:

$$ax^2 + by^2 + cz^2 = 0 \pmod{d_2}$$

We are going to use Pollard–Schnorr to solve:

$$x^2 + \frac{b}{a}y^2 = \frac{-c}{a} \pmod{d_2}$$

Taking $z = 1$ gives us a vector as we wish. ie in the basis containing the founded vector, Q has exactly the form:

$$\left[\begin{array}{cc|ccc} d_2* & d_2* & d_2* & d_2* & d_2* \\ d_2* & d_2* & d_2* & d_2* & d_2* \\ \hline d_2* & d_2* & d_2* & * & * \\ d_2* & d_2* & * & * & * \\ d_2* & d_2* & * & * & * \end{array}\right]$$

Finishing the minimisation

Now that Q has the right form, we are able to minimise:

$$\begin{bmatrix} d_2* & d_2* & d_2* & d_2* & d_2* \\ d_2* & d_2* & d_2* & d_2* & d_2* \\ d_2* & d_2* & d_2* & * & * \\ d_2* & d_2* & * & * & * \\ d_2* & d_2* & * & * & * \end{bmatrix}$$

Finishing the minimisation

Now that Q has the right form, we are able to minimise:

$$\begin{bmatrix} d_2* & d_2* & d_2* & d_2^2* & d_2^2* \\ d_2* & d_2* & d_2* & d_2^2* & d_2^2* \\ d_2* & d_2* & d_2* & d_2* & d_2* \\ d_2^2* & d_2^2* & d_2* & d_2^2* & d_2^2* \\ d_2^2* & d_2^2* & d_2* & d_2^2* & d_2^2* \end{bmatrix}$$

1. We multiply the two lasts rows and columns by d_2

Finishing the minimisation

Now that Q has the right form, we are able to minimise:

$$\begin{bmatrix} * & * & * & d_2* & d_2* \\ * & * & * & d_2* & d_2* \\ * & * & * & * & * \\ d_2* & d_2* & * & d_2* & d_2* \\ d_2* & d_2* & * & d_2* & d_2* \end{bmatrix}$$

1. We multiply the two lasts rows and columns by d_2
2. We divide the matrix by d_2

Finishing the minimisation

Now that Q has the right form, we are able to minimise:

$$\begin{bmatrix} * & * & * & d_2* & d_2* \\ * & * & * & d_2* & d_2* \\ * & * & * & * & * \\ d_2* & d_2* & * & d_2* & d_2* \\ d_2* & d_2* & * & d_2* & d_2* \end{bmatrix}$$

1. We multiply the two lasts rows and columns by d_2
2. We divide the matrix by d_2

Result:

We have multiplied $\det(Q)$ by d_2^4 and divided it by d_2^5,
$\Rightarrow$ we have gained a factor d_2.

What's next: Complexity

3. Complexity

Complexity

We write $g = \widetilde{\mathcal{O}}(f)$ if there exists $\alpha \in \mathbb{R}, \alpha \geq 0$ such that $g = \mathcal{O}\left(f \log(f)^{\alpha}\right)$.

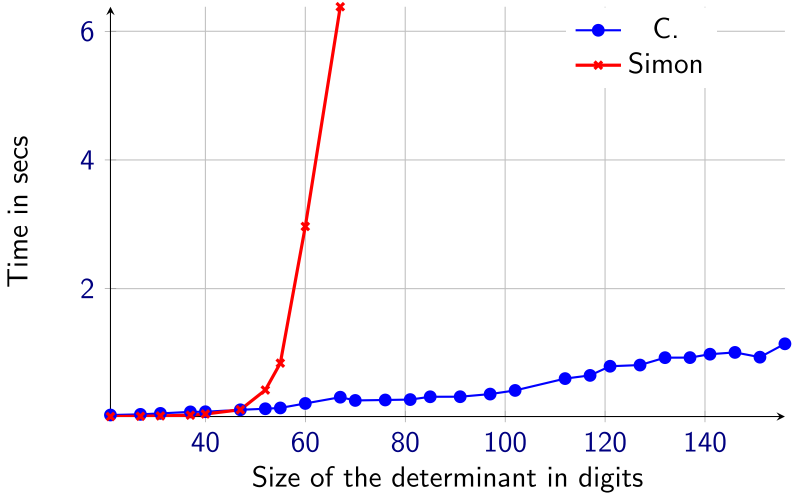
Complexity
Minimisation steps: $\widetilde{\mathcal{O}}\left(\log\left(\lvert\Delta_5\rvert\right)^7\right)$
Completion step: $\widetilde{\mathcal{O}}\left(\log\left(\lvert\Delta_5\rvert\right)^5\right)$
End of the algorithm: $\widetilde{\mathcal{O}}\left(P\left(\log\left(\lvert\Delta_5\rvert\right)\right)\right)$

P: non explicit polynomial given by the complexity of Simon's algorithm in dimensions 6 and 4.

Global complexity:

Probabilistic under GHR in $\widetilde{\mathcal{O}}\left(\log\left(\lvert\Delta_5\rvert\right)^7 + P\left(\log\left(\lvert\Delta_5\rvert\right)\right)\right)$

Comparison



(Average over 1000 random matrices)

What's next: Example

4. Example

A “ small ” example:

$$Q = \begin{bmatrix} -418105000674164527849160050701423800028380629870569441549000 & 83518512577517114747646424352631888328977479810328728243476 & -106925291812009463674835299087426622392534676281318101734834 & -288958684723436990814388551921682536351718619866618269301636 & -556501306905604232265677756922323378828559812716557759676052 \\ 83518512577517114747646424352631888328977479810328728243476 & -126062511925113121237919529715611084319190398703964769350556 & 185776784540788776402305037400499678716818843578928950121294 & 3745107863480724018442012775295861974842991834931244778188 & -356105859228665714571533522124276096694514576943891139250756 \\ -106925291812009463674835299087426622392534676281318101734834 & 185776784540788776402305037400499678716818843578928950121294 & -545592935965150260152406020564238196779607011854021564536 36 & 380141584563789254250264013395246052927728262305028815370318 & 576820218141554883231370211753653991715011357409823709130598 \\ -288958684723436990814388551921682536351718619866618269301636 & 3745107863480724018442012775295861974842991834931244778188 & 380141584563789254250264013395246052927728262305028815370318 & -159812368772709453779617053140789659086389870916860925597788 & -427354990954876695230906258142778963879993339848269234263938 \\ -556501306905604232265677756922323378828559812716557759676052 & -356105859228665714571533522124276096694514576943891139250756 & 576820218141554883231370211753653991715011357409823709130598 & -427354990954876695230906258142778963879993339848269234263938 & -694897613137043936682195463141779780518978104693920960770224 \end{bmatrix}$$

A “ small ” example:

$$Q = \begin{bmatrix} -418105000674164527849160050701423800028380629870569441549000 & 835185125775171147476464243526318883289774798103287282434 76 & -106925291812009463674835299087426622392534676281318101734834 & -288958684723436990814388551921682536351718619866618269301636 & -556501306905604232265677756922323378828559812716557759676052 \\ 835185125775171147476464243526318883289774798103287282434 76 & -126062511925113121237919529715611084319190398703964769350556 & 185776784540788776402305037400499678716818843578928950121294 & 374510786348072401844201277529586197484299183493124477818 8 & -356105859228665714571533522124276096694514576943891139250756 \\ -106925291812009463674835299087426622392534676281318101734834 & 185776784540788776402305037400499678716818843578928950121294 & -545592935965150260152406020564238196779607011854021564536 36 & 380141584563789254250264013395246052927728262305028815370318 & 576820218141554883231370211753653991715011357409823709130598 \\ -288958684723436990814388551921682536351718619866618269301636 & 374510786348072401844201277529586197484299183493124477818 8 & 380141584563789254250264013395246052927728262305028815370318 & -159812368772709453779617053140789659086389870916860925597788 & -427354990954876695230906258142778963879993339848269234263938 \\ -556501306905604232265677756922323378828559812716557759676052 & -356105859228665714571533522124276096694514576943891139250756 & 576820218141554883231370211753653991715011357409823709130598 & -427354990954876695230906258142778963879993339848269234263938 & -694897613137043936682195463141779780518978104693920960770224 \end{bmatrix}$$

$$\begin{aligned} \det(Q) = -&1186784045904606733707005606055274973979911 9 \\ &612329906860272443106184215243620398241227088686 \\ &567163766883478844593814634595440693436234949087 \\ &491127359642479616640449784173297408619004481068 \\ &892088901946331771235813312305187060960723053316 \\ &362644916580516538177629348730016210305936885561 \\ &563614993869248 \ (\simeq 300 \ \textit{digits}) \end{aligned}$$

Thanks for your attention.

Pierre Castel

pierre.castel@unicaen.fr
http://www.math.unicaen.fr/~castel