Effective Hasse principle for two quadrics

Tony Quertier

ANTS XII

August 31, 2016

Notations

Let q_0 and q_1 be two homogenous quadratic forms in 13 variables with integral coefficients, with matrices Q_0 and Q_1.

Notations

Let q_0 and q_1 be two homogenous quadratic forms in 13 variables with integral coefficients, with matrices Q_0 and Q_1.

We set $\Delta(\lambda) = \det(\lambda Q_0 + Q_1)$.

Notations

Let q_0 and q_1 be two homogenous quadratic forms in 13 variables with integral coefficients, with matrices Q_0 and Q_1.

We set $\Delta(\lambda) = \det(\lambda Q_0 + Q_1)$.

Set $V_{q_0,q_1} := \{q_0 = q_1 = 0\} \subset \mathbb{P}^{n-1}$ be the projective variety defined by the two quadrics associated to q_0 and q_1.

Notations

Let q_0 and q_1 be two homogenous quadratic forms in 13 variables with integral coefficients, with matrices Q_0 and Q_1.

We set $\Delta(\lambda) = \det(\lambda Q_0 + Q_1)$.

Set $V_{q_0,q_1} := \{q_0 = q_1 = 0\} \subset \mathbb{P}^{n-1}$ be the projective variety defined by the two quadrics associated to q_0 and q_1.

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 $V_{q_0,q_1}(\overline{\mathbb{Q}})$.

Smoothness

Condition

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

Smoothness

Condition

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

Lemma

Two symmetric matrices Q_0 and Q_1 defined over $\mathbb{Q}$, satisfy the condition 1 if and only if $\det(Q_0) \neq 0$, and $\Delta(\lambda)$ has only simple roots in $\overline{\mathbb{Q}}$.

Smoothness

Condition

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

Lemma

Two symmetric matrices Q_0 and Q_1 defined over $\mathbb{Q}$, satisfy the condition 1 if and only if $\det(Q_0) \neq 0$, and $\Delta(\lambda)$ has only simple roots in $\overline{\mathbb{Q}}$.

Aim

Assuming condition 1, exhibit a rational point $x \in V_{q_0,q_1}(\mathbb{Q})$ if there is one.

Hasse Principle

The first step is to study if such a zero exists.

Hasse Principle

The first step is to study if such a zero exists.

In 1959, Mordell proved that the **Hasse Principle** holds for two quadratic forms in $n \geq 13$ variables.

Hasse Principle

The first step is to study if such a zero exists.

In 1959, Mordell proved that the **Hasse Principle** holds for two quadratic forms in $n \geq 13$ variables.

Then, we need to study if q_0 and q_1 have a zero over $\mathbb{Q}_p$ for every p prime and a zero over $\mathbb{R}$.

Hasse Principle

The first step is to study if such a zero exists.

In 1959, Mordell proved that the **Hasse Principle** holds for two quadratic forms in $n \geq 13$ variables.

Then, we need to study if q_0 and q_1 have a zero over $\mathbb{Q}_p$ for every p prime and a zero over $\mathbb{R}$.

Local obstructions

In 1956, Demyanov proved that, for every p prime, two quadratic forms over $\mathbb{Q}_p$ in $n \geq 9$ variables have always a p-adic zero.

Hasse Principle

The first step is to study if such a zero exists.

In 1959, Mordell proved that the **Hasse Principle** holds for two quadratic forms in $n \geq 13$ variables.

Then, we need to study if q_0 and q_1 have a zero over $\mathbb{Q}_p$ for every p prime and a zero over $\mathbb{R}$.

Local obstructions

In 1956, Demyanov proved that, for every p prime, two quadratic forms over $\mathbb{Q}_p$ in $n \geq 9$ variables have always a p-adic zero.

Then, the only obstruction is over $\mathbb{R}$.

Two main steps

Step 1

Decide whether q_0 and q_1 have a zero over $\mathbb{R}$.

Two main steps

Step 1

Decide whether q_0 and q_1 have a zero over $\mathbb{R}$.

Step 2

If q_0 and q_1 have a zero over $\mathbb{R}$, compute a zero over $\mathbb{Q}$.

Pencil of quadrics

We denote by $\mathcal{P}_{\mathbb{R}}(q_0, q_1)$ the pencil of quadrics associated to q_0 and q_1 over $\mathbb{R}$.

Pencil of quadrics

We denote by $\mathcal{P}_{\mathbb{R}}(q_0, q_1)$ the pencil of quadrics associated to q_0 and q_1 over $\mathbb{R}$. We have

$$\mathcal{P}_{\mathbb{R}}(q_0, q_1) = \{\lambda q_0 + \mu q_1 \mid (\lambda, \mu) \in \mathbb{R}^2 \backslash (0, 0)\}.$$

Pencil of quadrics

We denote by $\mathcal{P}_{\mathbb{R}}(q_0, q_1)$ the pencil of quadrics associated to q_0 and q_1 over $\mathbb{R}$. We have

$$\mathcal{P}_{\mathbb{R}}(q_0, q_1) = \{\lambda q_0 + \mu q_1 \mid (\lambda, \mu) \in \mathbb{R}^2 \backslash (0,0)\}.$$

Theorem

The quadratic forms q_0 and q_1 have a zero over $\mathbb{R}$ if and only if every forms in $\mathcal{P}_{\mathbb{R}}(q_0, q_1)$ is indefinite.

Forms in the pencil

Definition

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

Forms in the pencil

Definition

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

Lemma

Let Q_0 and Q_1 be two matrices of size n satisfying condition 1. Assume that $\Delta(\lambda)$ has $m \leq n$ real roots denoted by $\lambda_1 < \ldots < \lambda_m$. Set $\lambda_0 := -\infty$ and $\lambda_{n+1} := +\infty$. We have:

1. *If $m \neq n$ then $\lambda Q_0 + Q_1$ is never definite.*
2. *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.*

Algorithm

Algorithm

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.

Algorithm

Algorithm

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 $I = [-a - 1, a + 1]$.

Algorithm

Algorithm

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.

Algorithm

Algorithm

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 $-aQ_0 + Q_1$.

Algorithm

Algorithm

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 $-aQ_0 + Q_1$.
4. Let λ and μ be two rational numbers such that $\lambda \in]\lambda_r, \lambda_{r+1}[$ and $\mu \in]\lambda_s, \lambda_{s+1}[$.

Algorithm

Algorithm

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 $-aQ_0 + Q_1$.
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.

Algorithm

Algorithm

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 $-aQ_0 + Q_1$.
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.

Balanced quadratic form

Definition

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

Balanced quadratic form

Definition

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

Theorem

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

Balanced quadratic form

Definition

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

Theorem

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

Proof

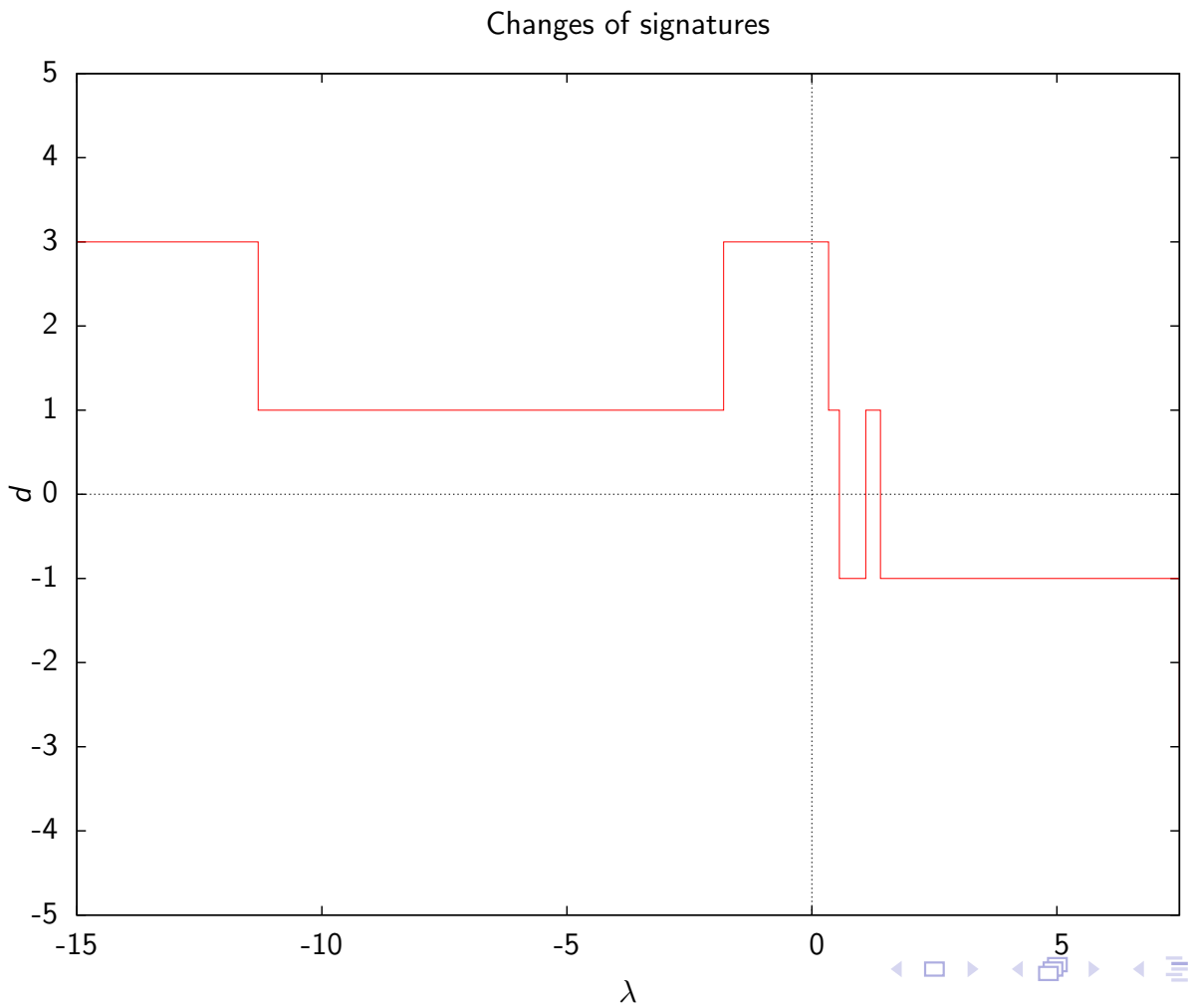
Assume $d(-\infty) = -a$ and $d(\infty) = a$. As Q_0 and Q_1 satisfy condition 1, d is piecewise constant. Moreover if λ_i is a real root of $\Delta(\lambda)$, we have $d(\lambda_i^-) = d(\lambda_i^+) \pm 2$. So there exists an interval I such that, for all x in I, $|d(x)| \leq 1$.

Fonction d

A picture is worth a thousand words.

Fonction d

A picture is worth a thousand words.



Algorithm

Algorithm

Let Q_0 and Q_1 be two matrices of size n satisfying condition 1. This algorithm computes a rational number λ such that $\lambda Q_0 + Q_1$ is balanced and nondegenerate.

Algorithm

Algorithm

Let Q_0 and Q_1 be two matrices of size n satisfying condition 1. This algorithm computes a rational number λ such that $\lambda Q_0 + Q_1$ is balanced and nondegenerate.

Principle: bissection method.

Algorithm

Algorithm

Let Q_0 and Q_1 be two matrices of size n satisfying condition 1. This algorithm computes a rational number λ such that $\lambda Q_0 + Q_1$ is balanced and nondegenerate.

Principle: bissection method.

In this algorithm, we don't need to compute the roots of Δ.

Reduction of q_0

We can now assume that q_0 is balanced and of signature $[7, 6]$. A rational indefinite quadratic form in $n \geq 5$ variables is always isotropic (Meyer).

Reduction of q_0

We can now assume that q_0 is balanced and of signature $[7, 6]$. A rational indefinite quadratic form in $n \geq 5$ variables is always isotropic (Meyer). Then, we can compute a rational zero of q_0 using the algorithm of Castel and a basis change such that

$$q_0 = x_1 x_{13} + q_2(x_2, \ldots, x_{12}),$$

in this basis. The signature of q_2 is $[6, 5]$, then we can iterate to have

$$q_0 = x_1 x_{13} + \ldots + x_5 x_9 + q_2(x_6, x_7, x_8).$$

MTIS of q_0

Let $W = \{x \in \mathbb{Q}^{13} \mid x_i = 0 \ \forall i > 5\}$ be a MTIS of q_0. The restriction $q_{1|_W}$ is a quadratic form in 5 variables.

MTIS of q_0

Let $W = \{x \in \mathbb{Q}^{13} \mid x_i = 0 \ \forall i > 5\}$ be a MTIS of q_0. The restriction $q_{1|_W}$ is a quadratic form in 5 variables.

If $q_{1|_W}$ is indefinite, we compute a zero of $q_{1|_W}$ and we deduce a zero of q_0 and q_1.

MTIS of q_0

Let $W = \{x \in \mathbb{Q}^{13} \mid x_i = 0 \ \forall i > 5\}$ be a MTIS of q_0. The restriction $q_{1|_W}$ is a quadratic form in 5 variables.

If $q_{1|_W}$ is indefinite, we compute a zero of $q_{1|_W}$ and we deduce a zero of q_0 and q_1.

Otherwise, we need to construct a MTIS W' of q_0 such that $q_{1|_{W'}}$ is indefinite.

Construction of a *good* MTIS

1. Compute a rational zero x of q_0 such that $q_1(x) > 0$.

Construction of a *good* MTIS

1. Compute a rational zero x of q_0 such that $q_1(x) > 0$.
2. Compute a real zero of q_0 and q_1.

Construction of a *good* MTIS

1. Compute a rational zero x of q_0 such that $q_1(x) > 0$.
2. Compute a real zero of q_0 and q_1.
3. Use this zero to compute a real zero y of q_0 such that $q_1(y) < 0$.

Construction of a *good* MTIS

1. Compute a rational zero x of q_0 such that $q_1(x) > 0$.
2. Compute a real zero of q_0 and q_1.
3. Use this zero to compute a real zero y of q_0 such that $q_1(y) < 0$.
4. Make an approximation of y to compute a rational zero z of q_0 such that $q_1(z) < 0$.

Construction of a *good* MTIS

1. Compute a rational zero x of q_0 such that $q_1(x) > 0$.
2. Compute a real zero of q_0 and q_1.
3. Use this zero to compute a real zero y of q_0 such that $q_1(y) < 0$.
4. Make an approximation of y to compute a rational zero z of q_0 such that $q_1(z) < 0$.

Rational zero of q_0 and q_1

We complete x and z in a basis of $\mathbb{Q}^{13}$ such that

$$q_0 = x_1x_{13} + \ldots + x_5x_9 + q_2(x_6, x_7, x_8),$$

in this basis.

Rational zero of q_0 and q_1

We complete x and z in a basis of $\mathbb{Q}^{13}$ such that

$$q_0 = x_1x_{13} + \ldots + x_5x_9 + q_2(x_6, x_7, x_8),$$

in this basis. We set $W = \{x \in \mathbb{Q}^{13} \mid x_i = 0 \ \forall i > 5\}$.

Rational zero of q_0 and q_1

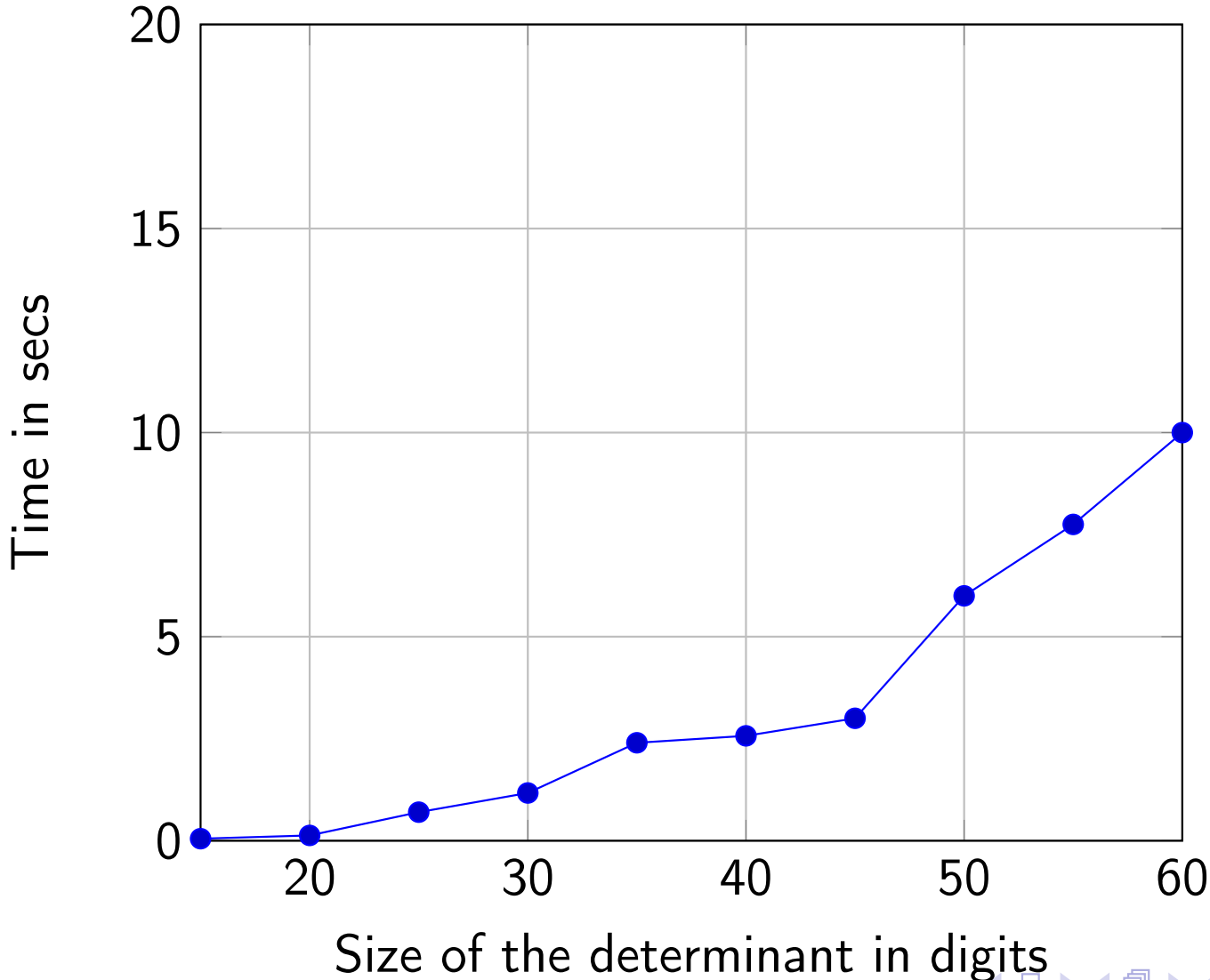
We complete x and z in a basis of $\mathbb{Q}^{13}$ such that

$$q_0 = x_1x_{13} + \ldots + x_5x_9 + q_2(x_6, x_7, x_8),$$

in this basis. We set $W = \{x \in \mathbb{Q}^{13} \mid x_i = 0 \ \forall i > 5\}$.

We can now compute a rational zero of $q_{1|_W}$ and deduce a zero of q_0 and q_1.

Time


20
15
10
5
0
Time in secs
20
30
40
50
60
Size of the determinant in digits

Thanks for your attention