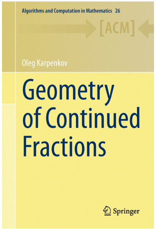
On Hermite's problem, Jacobi-Perron type algorithms, and Dirichlet groups

Oleg Karpenkov, University of Liverpool

7 September 2021

Contents

Contents


Algorithms and Computation in Mathematics 26
[ACM]
Oleg Karpenkov
Geometry of Continued Fractions
Springer

I. Hermite's problem

On periodicity of algebraic numbers

On periodicity of algebraic numbers

Rational numbers: periodic or finite decimal representations.

$$\frac{4}{3} = 1.3333333\ldots$$

On periodicity of algebraic numbers

Rational numbers: periodic or finite decimal representations.

$$\frac{4}{3} = 1.3333333\ldots$$

Quadratic numbers (roots of quadratic integer polynomials): periodic continued fractions (J.-L. Lagrange, 1770).

$$\frac{10+3\sqrt{7}}{4} = [4; (2, 15, 2, 3)].$$

On periodicity of algebraic numbers

Rational numbers: periodic or finite decimal representations.

$$\frac{4}{3} = 1.3333333\ldots$$

Quadratic numbers (roots of quadratic integer polynomials): periodic continued fractions (J.-L. Lagrange, 1770).

$$\frac{10+3\sqrt{7}}{4} = [4; (2, 15, 2, 3)].$$

Cubic numbers (roots of cubic integer polynomials):

Cubic numbers (roots of cubic integer polynomials):
Hermite's problem (1848): *Find a periodic description of cubic numbers.*

On periodicity of algebraic numbers

Cubic numbers (roots of cubic integer polynomials):
Hermite's problem (1848): *Find a periodic description of cubic numbers.*

First steps.
— C. G. J. Jacobi (1868): algorithmic approach

— O. Perron (1907): first realisation of algorithmic approach, which is believed to be non-periodic.

On periodicity of algebraic numbers

Cubic numbers (roots of cubic integer polynomials):
Hermite's problem (1848): *Find a periodic description of cubic numbers.*

Development of geometry of numbers.
— F. Klein, V. Arnold, A. Veselov, E. Korkina, O. German, A.Ustinov, O.K., etc.: geometric approach to continued fractions.

Remark: geometry of numbers was limitedly used (overlooked) for multidimensional Euclidaen algorithms.

On periodicity of algebraic numbers

Cubic numbers (roots of cubic integer polynomials):
Hermite's problem (1848): *Find a periodic description of cubic numbers.*

Periodic modifications of the J-P algorithm.
— O.K. (2021) based on the geometry of c.f.:

Cubic numbers (roots of cubic integer polynomials):
Hermite's problem (1848): *Find a periodic description of cubic numbers.*

Periodic modifications of the J-P algorithm.
— O.K. (2021) based on the geometry of c.f.:

- **Totally real case:** periodicity is **proved** for $\sin^2$-algorithm.

On periodicity of algebraic numbers

Cubic numbers (roots of cubic integer polynomials):
Hermite's problem (1848): *Find a periodic description of cubic numbers.*

Periodic modifications of the J-P algorithm.
— O.K. (2021) based on the geometry of c.f.:

- **Totally real case:** periodicity is **proved** for $\sin^2$-algorithm.
- **Complex case:** heuristic APD-algorithm that provides periodicity (**no proof**).

On periodicity of algebraic numbers

Cubic numbers (roots of cubic integer polynomials):
Hermite's problem (1848): *Find a periodic description of cubic numbers.*

Periodic modifications of the J-P algorithm.
— O.K. (2021) based on the geometry of c.f.:

- **Totally real case:** periodicity is **proved** for $\sin^2$-algorithm.
- **Complex case:** heuristic APD-algorithm that provides periodicity (**no proof**).
- **Algebraic case of degree** > 3**:** higher-dimensional heuristic APD-algorithm provides periodicity (**no proof**).

II. Euclidean algorithm and its generalisations

Euclid's algorithm ($\sim$ 300 BC)

Extended Euclid's algorithm

Input: **real** numbers $(p, q) = (p_0, q_0)$ such that $q_0 > 0$.

Euclid's algorithm ($\sim$ 300 BC)

Extended Euclid's algorithm

Input: **real** numbers $(p, q) = (p_0, q_0)$ such that $q_0 > 0$.

Step of the algorithm: If $q_i \geq 0$:

$$(p_i, q_i) \mapsto (p_{i+1}, q_{i+1}) = (q_i, p_i - \lfloor p_i/q_i \rfloor q_i)$$

Euclid's algorithm ($\sim$ 300 BC)

Extended Euclid's algorithm

Input: **real** numbers $(p, q) = (p_0, q_0)$ such that $q_0 > 0$.

Step of the algorithm: If $q_i \geq 0$:

$$(p_i, q_i) \mapsto (p_{i+1}, q_{i+1}) = (q_i, p_i - \lfloor p_i/q_i \rfloor q_i)$$

$a_i = \lfloor p_i/q_i \rfloor$ — the *i-th element* of the algorithm.

Euclid's algorithm ($\sim$ 300 BC)

Extended Euclid's algorithm

Input: **real** numbers $(p, q) = (p_0, q_0)$ such that $q_0 > 0$.

Step of the algorithm: If $q_i \geq 0$:

$$(p_i, q_i) \mapsto (p_{i+1}, q_{i+1}) = (q_i, p_i - \lfloor p_i/q_i \rfloor q_i)$$

$a_i = \lfloor p_i/q_i \rfloor$ — the *i-th element* of the algorithm.

Termination of the algorithm: (p_i, q_i) with $q_i = 0$.

Example

For $(21, 15)$ we have:

$$(21, 15) \mapsto (15, 6) \mapsto (6, 3) \mapsto (3, 0).$$

Euclid's algorithm ($\sim$ 300 BC)

Example

For $(21, 15)$ we have:

$$(21, 15) \mapsto (15, 6) \mapsto (6, 3) \mapsto (3, 0).$$

Output:

$$a_1 = 1, \quad a_2 = 2, \quad \text{and} \quad a_3 = 2.$$

Euclid's algorithm ($\sim$ 300 BC)

Example

For $(21, 15)$ we have:

$$(21, 15) \mapsto (15, 6) \mapsto (6, 3) \mapsto (3, 0).$$

Output:

$$a_1 = 1, \quad a_2 = 2, \quad \text{and} \quad a_3 = 2.$$

Note that

$$\gcd(21, 15) = 3 \quad \text{and} \quad \frac{21}{15} = 1 + \frac{1}{2 + 1/2}.$$

Euclid's algorithm ($\sim$ 300 BC)

Example

Now for $(2\sqrt{5}, 1)$:

$$(2\sqrt{5}, 1) \mapsto c_1(1+\sqrt{5}/2, 1) \mapsto c_2(4+2\sqrt{5}, 1) \mapsto c_3(1+\sqrt{5}/2, 1) \mapsto \ldots$$

where

$$c_1 = 2\sqrt{5} - 4, \quad c_2 = 9 - 4\sqrt{5}, \quad c_3 = 34\sqrt{5} - 76, \quad \ldots$$

Euclid's algorithm ($\sim$ 300 BC)

Example

Now for $(2\sqrt{5}, 1)$:

$$(2\sqrt{5}, 1) \mapsto c_1(1+\sqrt{5}/2, 1) \mapsto c_2(4+2\sqrt{5}, 1) \mapsto c_3(1+\sqrt{5}/2, 1) \mapsto \ldots$$

where

$$c_1 = 2\sqrt{5} - 4, \quad c_2 = 9 - 4\sqrt{5}, \quad c_3 = 34\sqrt{5} - 76, \quad \ldots$$

The vectors obtained on Step 1 and Step 3 are proportional.

Euclid's algorithm ($\sim$ 300 BC)

Example

Now for $(2\sqrt{5}, 1)$:

$$(2\sqrt{5}, 1) \mapsto c_1(1+\sqrt{5}/2, 1) \mapsto c_2(4+2\sqrt{5}, 1) \mapsto c_3(1+\sqrt{5}/2, 1) \mapsto \ldots$$

where

$$c_1 = 2\sqrt{5} - 4, \quad c_2 = 9 - 4\sqrt{5}, \quad c_3 = 34\sqrt{5} - 76, \quad \ldots$$

The vectors obtained on Step 1 and Step 3 are proportional.
Hence the output is periodic:

$$a_1 = 4, \quad a_{2k} = 2, \quad \text{and} \quad a_{2k+1} = 8$$

So $2\sqrt{5} = [4; 2 : 8 : 2 : 8 : 2 : 8 : \ldots] = [4; (2 : 8)]$.

Jacobi-Perron algorithm (1907)

Jacobi-Perron algorithm

Input: triples of real numbers (x, y, z).

Jacobi-Perron algorithm (1907)

Jacobi-Perron algorithm

Input: triples of real numbers (x, y, z).

Step of the algorithm: If $y_i \neq 0$.

$$(x_i, y_i, z_i) \mapsto (x_{i+1}, y_{i+1}, z_{i+1}) = \left(y_i, z_i - \left\lfloor \frac{z_i}{y_i} \right\rfloor y_i, x_i - \left\lfloor \frac{x_i}{y_i} \right\rfloor y\right).$$

Jacobi-Perron algorithm (1907)

Jacobi-Perron algorithm

Input: triples of real numbers (x, y, z).

Step of the algorithm: If $y_i \neq 0$.

$$(x_i, y_i, z_i) \mapsto (x_{i+1}, y_{i+1}, z_{i+1}) = \Big(y_i, z_i - \Big\lfloor \frac{z_i}{y_i} \Big\rfloor y_i, x_i - \Big\lfloor \frac{x_i}{y_i} \Big\rfloor y\Big).$$

The *i-th element* of the multidimensional continued fraction is

$$\Big(\Big\lfloor \frac{z_i}{y_i} \Big\rfloor, \Big\lfloor \frac{x_i}{y_i} \Big\rfloor\Big).$$

Jacobi-Perron algorithm (1907)

Jacobi-Perron algorithm

Input: triples of real numbers (x, y, z).

Step of the algorithm: If $y_i \neq 0$.

$$(x_i, y_i, z_i) \mapsto (x_{i+1}, y_{i+1}, z_{i+1}) = \left(y_i, z_i - \left\lfloor \frac{z_i}{y_i} \right\rfloor y_i, x_i - \left\lfloor \frac{x_i}{y_i} \right\rfloor y\right).$$

The *i-th element* of the multidimensional continued fraction is

$$\left(\left\lfloor \frac{z_i}{y_i} \right\rfloor, \left\lfloor \frac{x_i}{y_i} \right\rfloor\right).$$

Termination of the algorithm: (x_i, y_i, z_i) with $y_i = 0$.

Jacobi-Perron algorithm (1907)

Let ξ be a real root of the polynomial x^3+2x^2+x+4, namely

$$\xi = -\frac{(53+6\sqrt{78})^{1/3}}{3} - \frac{1}{3(53+6\sqrt{78})^{1/3}} - \frac{2}{3}.$$

Jacobi-Perron algorithm (1907)

Let ξ be a real root of the polynomial $x^3 + 2x^2 + x + 4$, namely

$$\xi = -\frac{(53+6\sqrt{78})^{1/3}}{3} - \frac{1}{3(53+6\sqrt{78})^{1/3}} - \frac{2}{3}.$$

Now consider the vector **(not a single number, which is senseless! One can have different periods with the same number)**

$$(1, \xi, \xi^2 + \xi).$$

Jacobi-Perron algorithm (1907)

Let ξ be a real root of the polynomial $x^3 + 2x^2 + x + 4$, namely

$$\xi = -\frac{(53+6\sqrt{78})^{1/3}}{3} - \frac{1}{3(53+6\sqrt{78})^{1/3}} - \frac{2}{3}.$$

Now consider the vector **(not a single number, which is senseless! One can have different periods with the same number)**

$$(1, \xi, \xi^2 + \xi).$$

Jacobi-Perron algorithm periodic output:

	1	2	3	4	5	6	$2k+1$	$2k+2$
$\lfloor x/y \rfloor$	-1	1	1	1	2	6	3	7
$\lfloor z/y \rfloor$	-2	0	0	0	2	4	1	1

Jacobi-Perron algorithm (1907)

Problem

(Jacobi's Last Theorem.) *Let K be a totally real cubic field. Let $y, z \in K$ satisfy*

- $0 < y, z < 1$;
- 1, y, *and* z *are independent over* $\mathbb{Q}$.

Does Jacobi-Perron algorithm generate an eventually periodic continued fraction starting with $v = (1, y, z)$?

Jacobi-Perron algorithm (1907)

Problem

(Jacobi's Last Theorem.) *Let K be a totally real cubic field. Let $y, z \in K$ satisfy*

- $0 < y, z < 1$;
- 1, y, *and* z *are independent over* $\mathbb{Q}$.

Does Jacobi-Perron algorithm generate an eventually periodic continued fraction starting with $v = (1, y, z)$*?*

It is believed that the answer is negative.

(I have learnt this fact from Cor Kraaikamp in 2006 in Leiden.)

Example

Let us consider the vector

$$v = (1, \sqrt[3]{4}, \sqrt[3]{16}).$$

Numerical computations (e.g., by L. Elsner and H. Hasse., 1967) shows

	1	2	3	4	5	6	7	8	9	10	11	12	...	94	.
$\lfloor x/y \rfloor$	0	1	13	1	6	1	1	3	2	3	4	1	...	476	.
$\lfloor z/y \rfloor$	1	1	9	1	2	0	0	2	0	1	1	1	...	388	.

Example

Let us consider the vector

$$v = (1, \sqrt[3]{4}, \sqrt[3]{16}).$$

Numerical computations (e.g., by L. Elsner and H. Hasse., 1967) shows

	1	2	3	4	5	6	7	8	9	10	11	12	...	94	.
$\lfloor x/y \rfloor$	0	1	13	1	6	1	1	3	2	3	4	1	...	476	.
$\lfloor z/y \rfloor$	1	1	9	1	2	0	0	2	0	1	1	1	...	388	.

Compare:

$$\pi = [3 : 7; 15; 1; 292; 1; 1; 1; 2; 1; 3; 1; 14; 2; 1; 1; 2; 2; 2; 2; 1; 84; \ldots]$$

Jacobi-Perron algorithm (1907)

Gauss-Kuzmin statistics:

$$\frac{1}{\ln(2)} \ln\left(1 + \frac{1}{k(k+1)}\right).$$

Jacobi-Perron algorithm (1907)

Gauss-Kuzmin statistics:

$$\frac{1}{\ln(2)} \ln\left(1+\frac{1}{k(k+1)}\right).$$

Observe:

$$\frac{1}{\ln(2)} \ln\left(1+\frac{1}{k(k+1)}\right) = \frac{\ln[-1,0,k,k+1]}{\ln[-1,0,1,\infty]}.$$

Hint for us: this question involves geometry.

Jacobi-Perron algorithm (1907)

The same problem arise with the other Jacobi-Perron type algorithms:

- V. Brun (subtractive algorithm) 1958
- E. S. Selmer (general subtractive algorithm) 1961
- F. Schweiger (fully subtractive algorithm) 1995

etc.

Part III

III. New algorithms

Markov-Davenport Characteristic

Definition

Consider $u, v, w \in \mathbb{C}^3$:

$$u = (u_1, u_2, u_3), \quad v = (v_1, v_2, v_3), \quad \text{and} \quad w = (w_1, w_2, w_3)$$

Markov-Davenport Characteristic

Definition

Consider $u, v, w \in \mathbb{C}^3$:

$$u = (u_1, u_2, u_3), \quad v = (v_1, v_2, v_3), \quad \text{and} \quad w = (w_1, w_2, w_3)$$

The *Markov-Davenport characteristic* is the form $\chi_{u,v,w}$:

$$\det \begin{pmatrix} x & y & z \\ v_1 & v_2 & v_3 \\ w_1 & w_2 & w_3 \end{pmatrix} \cdot \det \begin{pmatrix} u_1 & u_2 & u_3 \\ x & y & z \\ w_1 & w_2 & w_3 \end{pmatrix} \cdot \det \begin{pmatrix} u_1 & u_2 & u_3 \\ v_1 & v_2 & v_3 \\ x & y & z \end{pmatrix}$$

in variables x, y, and z (with respect to u, v, w).

Markov-Davenport Characteristic

Definition

Consider $u, v, w \in \mathbb{C}^3$:

$$u = (u_1, u_2, u_3), \quad v = (v_1, v_2, v_3), \quad \text{and} \quad w = (w_1, w_2, w_3)$$

The *Markov-Davenport characteristic* is the form $\chi_{u,v,w}$:

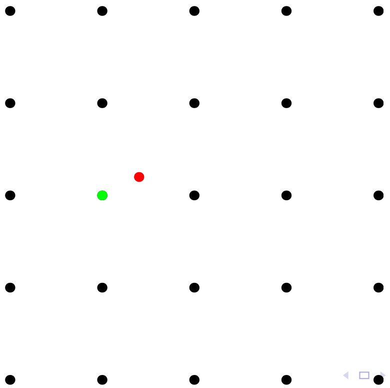
$$\det \begin{pmatrix} x & y & z \\ v_1 & v_2 & v_3 \\ w_1 & w_2 & w_3 \end{pmatrix} \cdot \det \begin{pmatrix} u_1 & u_2 & u_3 \\ x & y & z \\ w_1 & w_2 & w_3 \end{pmatrix} \cdot \det \begin{pmatrix} u_1 & u_2 & u_3 \\ v_1 & v_2 & v_3 \\ x & y & z \end{pmatrix}$$

in variables x, y, and z (with respect to u, v, w).

Remark: MD-characteristic provides a "proper distance" to the cone generated by u, v, and w.

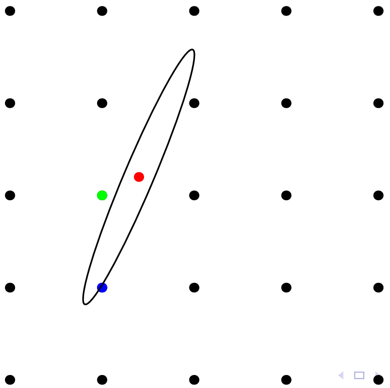
Markov-Davenport Characteristic

- JP-algorithm searching for the nearest lattice point. in a 2-plane $y = 1$.



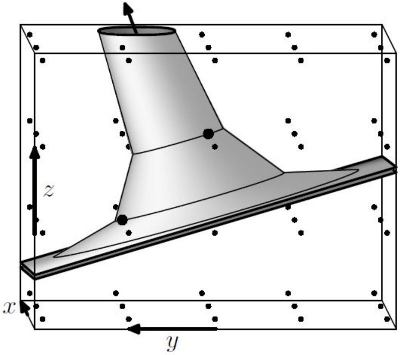
Markov-Davenport Characteristic

- JP-algorithm searching for the nearest lattice point. in a 2-plane $y = 1$.
- While a proper point could be different.



Markov-Davenport Characteristic

- JP-algorithm searching for the nearest lattice point. in a 2-plane $y = 1$.
- While a proper point could be different.
- Here are the "closest" integer points w.r.t. MD-characteristics:



Heuristic algebraic periodicity detecting algorithm

Heuristic APD-algorithm

Input: atriple of real vectors (ξ, ν, μ) where $\xi = (x_0, y_0, z_0)$ with $z_0 > 0$.

Step 0: Similar to JP-algorithm:

$$T_0 : (x, y, z) \mapsto \left(x - \left\lfloor \frac{x}{z} \right\rfloor z, y - \left\lfloor \frac{y}{z} \right\rfloor z, z\right),$$

namely we consider

$$(\xi_1, \nu_1, \mu_1) = \big(T_0(\xi), T_0(\nu), T_0(\mu)\big).$$

Heuristic algebraic periodicity detecting algorithm

Heuristic APD-algorithm

Step i for $i \geq 1$: We have $(\xi_i(x_i, y_i, z_i), \nu_i, \mu_i)$ with $\xi_i \in \mathbb{R}^3_+$.

Heuristic algebraic periodicity detecting algorithm

Heuristic APD-algorithm

Step i for $i \geq 1$: We have $(\xi_i(x_i, y_i, z_i), \nu_i, \mu_i)$ with $\xi_i \in \mathbb{R}^3_+$.

- **Stage 1: Determination of the element of the CF:**
  we pick (a_i, b_i) satisfying:
  — $0 \leq a_i \leq \lfloor x_i/z_i \rfloor$;
  — $0 \leq b_i \leq \lfloor y_i/z_i \rfloor$;
  — $(a_i, b_i) \neq (0, 0)$
  (exception: $(0, 0)$ if $\lfloor x_i/z_i \rfloor < 1$ and $\lfloor y_i/z_i \rfloor < 1$);

Heuristic algebraic periodicity detecting algorithm

Heuristic APD-algorithm

Step i for $i \geq 1$: We have $(\xi_i(x_i, y_i, z_i), \nu_i, \mu_i)$ with $\xi_i \in \mathbb{R}^3_+$.

- **Stage 1: Determination of the element of the CF:** we pick (a_i, b_i) satisfying:
  — $0 \leq a_i \leq \lfloor x_i/z_i \rfloor$;
  — $0 \leq b_i \leq \lfloor y_i/z_i \rfloor$;
  — $(a_i, b_i) \neq (0, 0)$
  (exception: $(0, 0)$ if $\lfloor x_i/z_i \rfloor < 1$ and $\lfloor y_i/z_i \rfloor < 1$);

  such that the triple $(a_i, b_i, 1)$ **has minimal possible abs. value of the MD-characteristic** $|\chi_{\xi,\nu,\mu}|$.

Heuristic algebraic periodicity detecting algorithm

Heuristic APD-algorithm

Step i **for** $i \geq 1$: We already have (ξ_i, ν_i, μ_i) with $\xi_i = (x_i, y_i, z_i) \in \mathbb{R}^3_+$ and (a_i, b_i).

- **Stage 2: Iteration step:**

$$T_i : (x, y, z) \mapsto (y - b_i z, z, x - a_i z).$$

Here we construct

$$(\xi_{i+1}, \nu_{i+1}, \mu_{i+1}) = \big(T_i(\xi_i), T_i(\nu_i), T_i(\mu_i)\big)$$

Heuristic algebraic periodicity detecting algorithm

Heuristic APD-algorithm

<u>**Step** i **for** $i \geq 1$</u>: We already have (ξ_i, ν_i, μ_i) with $\xi_i = (x_i, y_i, z_i) \in \mathbb{R}^3_+$ and (a_i, b_i).

- **Stage 2: Iteration step:**

$$T_i : (x, y, z) \mapsto (y - b_i z, z, x - a_i z).$$

Here we construct

$$(\xi_{i+1}, \nu_{i+1}, \mu_{i+1}) = \big(T_i(\xi_i), T_i(\nu_i), T_i(\mu_i)\big)$$

<u>**Termination of the algorithm:**</u> when $z_i = 0$.

Heuristic algebraic periodicity detecting algorithm

Conjecture

Heuristic APD-algorithm is periodic for all cubic triples of vectors.

Heuristic algebraic periodicity detecting algorithm

Conjecture

Heuristic APD-algorithm is periodic for all cubic triples of vectors.

Remark

A triple of cubic vectors
"="
a triple of linearly independent eigenvectors for an integer matrix (and irreducible characteristic polynomial).

Heuristic algebraic periodicity detecting algorithm

Conjecture

Heuristic APD-algorithm is periodic for all cubic triples of vectors.

Remark

A triple of cubic vectors
"="
a triple of linearly independent eigenvectors for an integer matrix (and irreducible characteristic polynomial).

Remark

APD algorithm is defined for both **totally real** and **complex cases**.

Remark

APD algorithm has a straightforward generalisation to **higher dimensional cases**.

Heuristic algebraic periodicity detecting algorithm

Consider:

$$\xi = (1, \sqrt[3]{4}, \sqrt[3]{16}) = (1, \sqrt[3]{4}, (\sqrt[3]{4})^2).$$

Note that $\sqrt[3]{4}$ is a root of $x^3 - 4$.

Heuristic algebraic periodicity detecting algorithm

Consider:

$$\xi = (1, \sqrt[3]{4}, \sqrt[3]{16}) = (1, \sqrt[3]{4}, (\sqrt[3]{4})^2).$$

Note that $\sqrt[3]{4}$ is a root of $x^3 - 4$.

Let β and γ be the complex roots of $x^3 - 4$. Consider:

$$\nu = (1, \beta, \beta^2) \quad \text{and} \quad \mu = (1, \gamma, \gamma^2).$$

Heuristic algebraic periodicity detecting algorithm

Consider:

$$\xi = (1, \sqrt[3]{4}, \sqrt[3]{16}) = (1, \sqrt[3]{4}, (\sqrt[3]{4})^2).$$

Note that $\sqrt[3]{4}$ is a root of $x^3 - 4$.

Let β and γ be the complex roots of $x^3 - 4$. Consider:

$$\nu = (1, \beta, \beta^2) \quad \text{and} \quad \mu = (1, \gamma, \gamma^2).$$

The output of the heuristic APD-algorithm for the triple (ξ, ν, μ) is **periodic**:

	0	1	2	3	4	5	6	$4k+3$	$4k+4$	$4k+5$	$4k+6$
a_1	0	0	1	0	0	0	1	1	1	0	0
b_1	0	0	2	1	1	1	5	0	1	1	6

$\sin^2$-algorithm (skipping technical details)

In a few words:
the $\sin^2$-algorithm repeats heuristic APD-algorithm but it works with $\sin^2 \alpha(u, v, w)$, where $\alpha(u, v, w)$ is the angle between the planes spanned by (u, v) and by (u, w).

$\sin^2$-algorithm (skipping technical details)

In a few words:
the $\sin^2$-algorithm repeats heuristic APD-algorithm but it works with $\sin^2 \alpha(u, v, w)$, where $\alpha(u, v, w)$ is the angle between the planes spanned by (u, v) and by (u, w).

The $\sin^2$-algorithm is proven to be periodic for algebraic triples.

$\sin^2$-algorithm (skipping technical details)

In a few words:
the $\sin^2$-algorithm repeats heuristic APD-algorithm but it works with $\sin^2 \alpha(u, v, w)$, where $\alpha(u, v, w)$ is the angle between the planes spanned by (u, v) and by (u, w).

The $\sin^2$-algorithm is proven to be periodic for algebraic triples.

Remark

It is defined for the totally real case (when all u, v and w are real vectors).

$\sin^2$-algorithm

$\sin^2$-algorithm

Input: We are given three vectors ξ, ν, μ such that
— $\xi(x, y, z)$ satisfy $x > y > z > 0$;
— all coordinates for ν and μ are neither simultaneously positive nor simultaneously negative.

Step of the algorithm: Let us apply the following linear transformation

$$(\xi_i, \nu_i, \mu_i) \to (\Phi_i(\xi_i), \Phi_i(\nu_i), \Phi_i(\mu_i))$$

with

$$\Phi_i = T_i M_i.$$

sin^2-algorithm

$$\Phi_i = T_i M_i.$$

Here M_i is taken to be the minimiser of the value of $\sin^2$. The minimisation is done among all the transformations

$$N_{\alpha,\beta,\gamma} : (x, y, z) \mapsto \big(x - \alpha z - \gamma(y - \beta z), y - \beta z, z\big) \quad \text{with}$$

$$0 \le \alpha \le \left\lfloor \frac{x_i}{z_i} \right\rfloor, \quad 0 \le \beta \le \left\lfloor \frac{y_i}{z_i} \right\rfloor, \quad \text{and} \quad 0 \le \gamma \le \left\lfloor \frac{x_i/z_i - \alpha}{y_i/z_i - \beta} \right\rfloor,$$

and the transformation

$$N_0 = (x, y, z) \mapsto \big(x - y, y, z - (x - y)\big),$$

which is considered only in case $z_i > x_i - y_i > 0$.

$\sin^2$-algorithm

$\sin^2$-algorithm

$$\Phi_i = T_i M_i.$$

Set T_i as a basis permutation that puts the coordinates of $M_i(\xi)$ in decreasing order.

At each step the algorithm returns Φ_i as an output.

Termination of the algorithm: In the case that the last coordinate of ξ_i is zero (i.e. $z_i = 0$).

IV. Application to Dirichlet groups

Example

Let

$$A = \begin{pmatrix} 2 & 5 & -1 \\ 3 & 6 & 1 \\ 4 & 7 & 1 \end{pmatrix}.$$

Find an integer matrix with unit determinant commuting with A?

Example

Let

$$A = \begin{pmatrix} 2 & 5 & -1 \\ 3 & 6 & 1 \\ 4 & 7 & 1 \end{pmatrix}.$$

Find an integer matrix with unit determinant commuting with A?

Let us first peek the answer to this question.

Example

Let

$$A = \begin{pmatrix} 2 & 5 & -1 \\ 3 & 6 & 1 \\ 4 & 7 & 1 \end{pmatrix}.$$

Find an integer matrix with unit determinant commuting with A?

Let us first peek the answer to this question.

$$B = \begin{pmatrix} 88778750433916 & 1881948516620816 & -1642359549748757 \\ -77918418013751 & -849278651461089 & 759124773173459 \\ 534000559063825 & -721564227716990 & 360094549931638 \end{pmatrix}$$

Example

Let

$$A = \begin{pmatrix} 2 & 5 & -1 \\ 3 & 6 & 1 \\ 4 & 7 & 1 \end{pmatrix}.$$

Find an integer matrix with unit determinant commuting with A?

Let us first peek the answer to this question.

$$B = \begin{pmatrix} 88778750433916 & 1881948516620816 & -1642359549748757 \\ -77918418013751 & -849278651461089 & 759124773173459 \\ 534000559063825 & -721564227716990 & 360094549931638 \end{pmatrix}$$

Brute force algorithm does not work...

Example

Let

$$A = \begin{pmatrix} 2 & 5 & -1 \\ 3 & 6 & 1 \\ 4 & 7 & 1 \end{pmatrix}.$$

Find an integer matrix with unit determinant commuting with A?

Let us first peek the answer to this question.

$$B = \begin{pmatrix} 88778750433916 & 1881948516620816 & -1642359549748757 \\ -77918418013751 & -849278651461089 & 759124773173459 \\ 534000559063825 & -721564227716990 & 360094549931638 \end{pmatrix}$$

Brute force algorithm does not work... even if one notices that

$$B = -147205796095883A^2 + 1347947957556991A - 399030223241821$$

Note: Input is nine 4-bit elements.

Dirichlet groups, Dirichlet's unit theorem

Definition. $A \in \mathrm{SL}(n, \mathbb{R})$. $\Gamma(A)$ — all integer matrices commuting with A.

(i) The *Dirichlet group* $\Xi(A)$ — all invertible matrices in $\Gamma(A)$.

(ii) The *positive Dirichlet group* $\Xi_+(A) \subset \Xi(A)$: only positive real eigenvalues.

Dirichlet groups, Dirichlet's unit theorem

Definition. $A \in \mathrm{SL}(n, \mathbb{R})$. $\Gamma(A)$ — all integer matrices commuting with A.

(i) The *Dirichlet group* $\Xi(A)$ — all invertible matrices in $\Gamma(A)$.

(ii) The *positive Dirichlet group* $\Xi_+(A) \subset \Xi(A)$: only positive real eigenvalues.

Dirichlet's unit theorem. *Let K be a field of algebraic numbers of degree $n = s + 2t$, (s – number of real roots; $2t$ – number of complex roots). Consider an arbitrary order D in K. Then D contains units $\varepsilon_1, \ldots, \varepsilon_r$ for $r = s + t - 1$ such that every unit ε in D has a unique decomposition of the form*

$$\varepsilon = \xi \varepsilon_1^{a_1} \cdots \varepsilon_r^{a_r} \ ,$$

where $a_1, \ldots, a_r$ are integers and ξ is a root of 1 contained in D.

Dirichlet groups, Dirichlet's unit theorem

Definition. $A \in \mathrm{SL}(n, \mathbb{R})$. $\Gamma(A)$ — all integer matrices commuting with A.

(i) The *Dirichlet group* $\Xi(A)$ — all invertible matrices in $\Gamma(A)$.

(ii) The *positive Dirichlet group* $\Xi_+(A) \subset \Xi(A)$: only positive real eigenvalues.

Dirichlet's unit theorem in the matrix form. *Let $A \in \mathrm{SL}(n, \mathbb{Z})$ with irreducible characteristic (s real and $2t$ complex eigenvalues). Then there exists a finite Abelian group G such that*

$$\Xi(A) \cong G \oplus \mathbb{Z}^{s+t-1}.$$
$$\Xi_+(A) \cong \mathbb{Z}^{s+t-1}.$$

Dirichlet groups, Dirichlet's unit theorem

Definition. $A \in \mathrm{SL}(n, \mathbb{R})$. $\Gamma(A)$ — all integer matrices commuting with A.

(i) The *Dirichlet group* $\Xi(A)$ — all invertible matrices in $\Gamma(A)$.

(ii) The *positive Dirichlet group* $\Xi_+(A) \subset \Xi(A)$: only positive real eigenvalues.

Example

In the three-dimensional case:

- **Complex case:** $s = 1, t = 1$ then

$$\Xi(A) \cong \Xi_+(A) \cong \mathbb{Z}.$$

- **Totally real case:** $s = 3, t = 0$. Then

$$\Xi(A) \cong G \oplus \mathbb{Z}^2 \quad \text{and} \quad \Xi_+(A) \cong \mathbb{Z}^2.$$

Question 1. Given ξ — a cubic vector.
Find $A \in \mathrm{SL}(3, \mathbb{Z})$ such that

$$A\xi = \lambda\xi.$$

Questions that JP-type algorithms answer

Question 1. Given ξ — a cubic vector.
Find $A \in \mathrm{SL}(3,\mathbb{Z})$ such that

$$A\xi = \lambda\xi.$$

Question 2. Given $M \in \mathrm{Mat}(3,\mathbb{Z})$ with irreducible characteristic polynomial over $\mathbb{Q}$.
Find an $A \in \mathrm{SL}(3,\mathbb{Z})$ such that

$$AM = MA.$$

Questions that JP-type algorithms answer

Question 1. Given ξ — a cubic vector.
Find $A \in \mathrm{SL}(3, \mathbb{Z})$ such that

$$A\xi = \lambda\xi.$$

Question 2. Given $M \in \mathrm{Mat}(3, \mathbb{Z})$ with irreducible characteristic polynomial over $\mathbb{Q}$.
Find an $A \in \mathrm{SL}(3, \mathbb{Z})$ such that

$$AM = MA.$$

Question 3. (in totally real case). Let $M \in \mathrm{SL}(3, \mathbb{Z})$-matrix.
Find an $\mathrm{SL}(3, \mathbb{Z})$-matrix commuting with M that is not a power of M.

Answer to Question 1: Example 1

Consider $(1, \xi, \xi^2 + \xi)$ with ξ satisfying

$$x^3 + 2x^2 + x + 4 = 0.$$

The JP-algorithm generates a periodic sequence:

Answer to Question 1: Example 1

Consider $(1, \xi, \xi^2 + \xi)$ with ξ satisfying

$$x^3 + 2x^2 + x + 4 = 0.$$

The JP-algorithm generates a periodic sequence:

	1	2	3	4	5	6	$2k+1$	$2k+2$
$\lfloor x/y \rfloor$	-1	1	1	1	2	6	3	7
$\lfloor z/y \rfloor$	-2	0	0	0	2	4	1	1

Answer to Question 1: Example 1

Consider $(1, \xi, \xi^2+\xi)$ with ξ satisfying

$$x^3 + 2x^2 + x + 4 = 0.$$

The JP-algorithm generates a periodic sequence:

	1	2	3	4	5	6	$2k+1$	$2k+2$
$\lfloor x/y \rfloor$	-1	1	1	1	2	6	3	7
$\lfloor z/y \rfloor$	-2	0	0	0	2	4	1	1

Matrix for the pre-period:

$$M_1 = \begin{pmatrix} -1 & 1 & 0 \\ 1 & 0 & 0 \\ -2 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}^3 \cdot \begin{pmatrix} 2 & 1 & 0 \\ 1 & 0 & 0 \\ 2 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 6 & 1 & 0 \\ 1 & 0 & 0 \\ 4 & 0 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} -22 & -1 & -3 \\ 51 & 2 & 7 \\ -67 & -3 & -9 \end{pmatrix};$$

Answer to Question 1: Example 1

Consider $(1, \xi, \xi^2+\xi)$ with ξ satisfying

$$x^3+2x^2+x+4=0.$$

The JP-algorithm generates a periodic sequence:

	1	2	3	4	5	6	$2k+1$	$2k+2$
$\lfloor x/y \rfloor$	-1	1	1	1	2	6	3	7
$\lfloor z/y \rfloor$	-2	0	0	0	2	4	1	1

Matrix for the period:

$$M_2 = \begin{pmatrix} 3 & 1 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 7 & 1 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 22 & 1 & 3 \\ 7 & 0 & 1 \\ 8 & 0 & 1 \end{pmatrix}.$$

Answer to Question 1: Example 1

Consider $(1, \xi, \xi^2 + \xi)$ with ξ satisfying

$$x^3 + 2x^2 + x + 4 = 0.$$

The JP-algorithm generates a periodic sequence:

	1	2	3	4	5	6	$2k+1$	$2k+2$
$\lfloor x/y \rfloor$	-1	1	1	1	2	6	3	7
$\lfloor z/y \rfloor$	-2	0	0	0	2	4	1	1

Finally we get

$$M = M_1 M_2 (M_1)^{-1} = \begin{pmatrix} 5 & -4 & 3 \\ -12 & 9 & -7 \\ 16 & -12 & 9 \end{pmatrix}.$$

This concludes the computation of M.

Answer to Question 1: Example 2

Consider $v = (1, \sqrt[3]{4}, \sqrt[3]{16})$.

Answer to Question 1: Example 2

Consider $v = (1, \sqrt[3]{4}, \sqrt[3]{16})$.
Here Jacobi-Perron algorithm does not work.

Answer to Question 1: Example 2

Consider $v = (1, \sqrt[3]{4}, \sqrt[3]{16})$.
Here Jacobi-Perron algorithm does not work.
Heuristic APD-algorithm produces

$$M = \begin{pmatrix} 5 & 8 & 12 \\ 3 & 5 & 8 \\ 2 & 3 & 5 \end{pmatrix}.$$

Answer to Question 3: Example

Consider an irreducible cubic polynomial

$$p(x) = 2x^3 - 4x^2 - 7x - 2$$

with roots $\alpha, \beta, \gamma \in \mathbb{R}$.

Answer to Question 3: Example

Consider an irreducible cubic polynomial

$$p(x) = 2x^3 - 4x^2 - 7x - 2$$

with roots $\alpha, \beta, \gamma \in \mathbb{R}$.

Our goal is to compute two independent $\mathrm{SL}(3, \mathbb{Z})$-matrices with eigenvectors

$$\xi = (1, \alpha, \alpha^2), \quad \nu = (1, \beta, \beta^2), \quad \text{and} \quad \mu = (1, \gamma, \gamma^2).$$

Answer to Question 3: Example

Consider an irreducible cubic polynomial

$$p(x) = 2x^3 - 4x^2 - 7x - 2$$

with roots $\alpha, \beta, \gamma \in \mathbb{R}$.

Direct computations using the heuristic APD-algorithm applied to triples

$$(\xi, \nu, \mu), \quad (\nu, \mu, \xi), \quad \text{and} \quad (\mu, \xi, \nu)$$

result in the following three matrices:

$$A = \begin{pmatrix} 55 & 210 & 176 \\ 176 & 671 & 562 \\ 562 & 2143 & 1795 \end{pmatrix}; \quad B = \begin{pmatrix} -497 & -1122 & 400 \\ 400 & 903 & -322 \\ -322 & -727 & 259 \end{pmatrix};$$

$$C = \begin{pmatrix} 185 & 172 & -72 \\ -72 & -67 & 28 \\ 28 & 26 & -11 \end{pmatrix}.$$

Answer to Question 3: Example

Consider an irreducible cubic polynomial

$$p(x) = 2x^3 - 4x^2 - 7x - 2$$

with roots $\alpha, \beta, \gamma \in \mathbb{R}$.

$$A = \begin{pmatrix} 55 & 210 & 176 \\ 176 & 671 & 562 \\ 562 & 2143 & 1795 \end{pmatrix}; \quad B = \begin{pmatrix} -497 & -1122 & 400 \\ 400 & 903 & -322 \\ -322 & -727 & 259 \end{pmatrix};$$
$$C = \begin{pmatrix} 185 & 172 & -72 \\ -72 & -67 & 28 \\ 28 & 26 & -11 \end{pmatrix}.$$

Brute force search of the powers of matrices show that

$$A^3 B^5 C^7 = \mathrm{Id}\,.$$

Answer to Question 3: Example

Consider an irreducible cubic polynomial

$$p(x) = 2x^3 - 4x^2 - 7x - 2$$

with roots $\alpha, \beta, \gamma \in \mathbb{R}$.

Brute force search of the powers of matrices show that

$$A^3 B^5 C^7 = \mathrm{Id}\,.$$

All these matrices represent different eigenvectors with maximal eigenvalue, hence they there are two of them that are not powers of each other.

Part V

V. Idea of the proof

Separating ξ-states

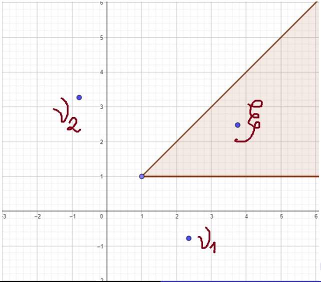
- Given a basis $s_0(\xi, \nu_1, \nu_2)$. Then

$$s = ((x_0, y_0, 1), (x_1, y_1, 1), (x_2, y_2, 1))$$

is a ξ-*state* if in some $\mathbb{Z}^3$-basis the coordinates the vectors of s are proportional to the vectors of s_0.

- Given a basis $s_0(\xi, \nu_1, \nu_2)$. Then
$$s = ((x_0, y_0, 1), (x_1, y_1, 1), (x_2, y_2, 1))$$
is a ξ-*state* if in some $\mathbb{Z}^3$-basis the coordinates the vectors of s are proportional to the vectors of s_0.

- A ξ-state $(\xi(x_0, y_0, 1), \nu_1, \nu_2)$ is *separating* if
— $\xi \in \mathbb{R}^3_+$ and $x_0 > y_0 > 1$
— $\nu_1, \nu_2 \notin \mathbb{R}^3_+$.



Separating ξ-states

- Given a basis $s_0(\xi, \nu_1, \nu_2)$. Then

$$s = ((x_0, y_0, 1), (x_1, y_1, 1), (x_2, y_2, 1))$$

  is a ξ-*state* if in some $\mathbb{Z}^3$-basis the coordinates the vectors of s are proportional to the vectors of s_0.

- A ξ-state $(\xi(x_0, y_0, 1), \nu_1, \nu_2)$ is *separating* if
  — $\xi \in \mathbb{R}^3_+$ and $x_0 > y_0 > 1$
  — $\nu_1, \nu_2 \notin \mathbb{R}^3_+$.

Proposition (Nose sharpening.)

If s is a separating ξ-state, then $\Phi(s)$ is a separating ξ-state.

(Here $\Phi(s)$ is the iterative step of $\sin^2$-algorithm).

Main theorem

Let s_0 be the input separating state. Denote

Main theorem

Let s_0 be the input separating state. Denote

- $\Omega_\varepsilon(s_0)$ — the set of all ξ-states s where $\sin\alpha(s) > \varepsilon$.

Main theorem

Let s_0 be the input separating state. Denote

- $\Omega_\varepsilon(s_0)$ — the set of all ξ-states s where $\sin\alpha(s) > \varepsilon$.
- $\Omega_{\max}(\xi;\nu_1,\nu_2)$ — the set of all ξ-states s satisfying

$$\sin^2\alpha(s) > \sin^2\alpha(\Phi(s)).$$

Main theorem

Let s_0 be the input separating state. Denote

- $\Omega_\varepsilon(s_0)$ — the set of all ξ-states s where $\sin\alpha(s) > \varepsilon$.
- $\Omega_{\max}(\xi;\nu_1,\nu_2)$ — the set of all ξ-states s satisfying

$$\sin^2\alpha(s) > \sin^2\alpha(\Phi(s)).$$

Theorem

Let $s = (\xi,\nu_1,\nu_2)$ be three conjugate cubic vectors. Assume that s is separating. Then

(i) $\Omega_\varepsilon(\xi;\nu_1,\nu_2)$ is finite ($\forall\varepsilon > 0$).

(ii) $\Omega_{\max}(\xi;\nu_1,\nu_2)$ is finite.

Main theorem

Let s_0 be the input separating state. Denote

- $\Omega_\varepsilon(s_0)$ — the set of all ξ-states s where $\sin\alpha(s) > \varepsilon$.
- $\Omega_{\max}(\xi;\nu_1,\nu_2)$ — the set of all ξ-states s satisfying

$$\sin^2\alpha(s) > \sin^2\alpha(\Phi(s)).$$

Theorem

Let $s = (\xi, \nu_1, \nu_2)$ be three conjugate cubic vectors. Assume that s is separating. Then

(i) $\Omega_\varepsilon(\xi;\nu_1,\nu_2)$ is finite $(\forall\varepsilon > 0)$.

(ii) $\Omega_{\max}(\xi;\nu_1,\nu_2)$ is finite.

Corollary

The dynamical system with a map Φ (on separating states) is periodic for triples of cubic conjugate vectors.

Main theorem

Let s_0 be the input separating state. Denote

- $\Omega_\varepsilon(s_0)$ — the set of all ξ-states s where $\sin\alpha(s) > \varepsilon$.
- $\Omega_{\max}(\xi;\nu_1,\nu_2)$ — the set of all ξ-states s satisfying

$$\sin^2\alpha(s) > \sin^2\alpha(\Phi(s)).$$

Theorem

Let $s = (\xi, \nu_1, \nu_2)$ be three conjugate cubic vectors. Assume that s is separating. Then

(i) $\Omega_\varepsilon(\xi;\nu_1,\nu_2)$ is finite ($\forall \varepsilon > 0$).

(ii) $\Omega_{\max}(\xi;\nu_1,\nu_2)$ is finite.

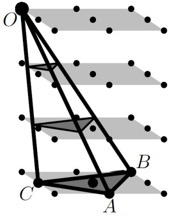
Corollary

The dynamical system with a map Φ (on separating states) is periodic for triples of cubic conjugate vectors.

Remark: There is a simple way to find the basis for s in which it is separating.

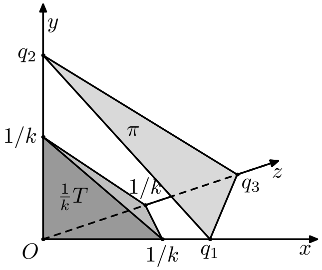
Proof of Item (i): finiteness statements

Integer distance = number of integer planes plus 1 between the point and our plane:



Proposition

Let P be a triangular pyramid with vertex at $O(0,0,0)$.
Let C be Cone(P) and $d \in \mathbb{Z}_+$.
Only finitely many: *integer planes π satisfying*
— integer distance$(O, \pi) \leq d$;
— π divides C into two parts, one of which is bounded and contains P.



Proof of Item (i): finiteness statements

Definition

Consider an integer plane π and a convex polygon P in it.
Let S be the basis square of the integer lattice in it.
Set *integer area*

$$\mathrm{Area}_\pi(P) = \frac{\mathrm{Area}(P)}{\mathrm{Area}(S)}.$$

Proof of Item (i): finiteness statements

Definition

Consider an integer plane π and a convex polygon P in it.
Let S be the basis square of the integer lattice in it.
Set *integer area*

$$\mathrm{Area}_\pi(P) = \frac{\mathrm{Area}(P)}{\mathrm{Area}(S)}.$$

Proposition

Consider a totally-real cubic cone C in $\mathbb{R}^3$ centered at the origin. Then there exists M s.t.

$$\mathrm{Area}_\pi(C \cap \pi) < M$$

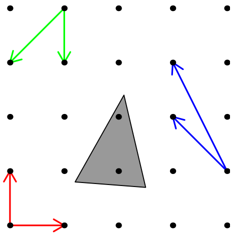
uniformly *for all planes at distance 1 to the origin and cutting C.*

Proof of Item (i): finiteness statements

Proof of Item (i): finiteness statements

Proposition

Let T be an arbitrary triangle on an integer plane π, and $M \in \mathbb{R}_+$. **Only finitely many**: *integer affine bases (O, e_1, e_2) in which all absolute values of the coordinates of vertices of T are bounded by M from above.*



Proof of Item (i): finiteness statements

Proposition

Consider a totally-real cubic cone in $\mathbb{R}^3$ *centered at* $O(0,0,0)$. *Let* $\varepsilon \in \mathbb{R}_+$.
Only finitely many (up to the action of $\Xi_+(C)$): *integer base planes* π *on the* **unit integer distance** *to the origin satisfying*

$$\mathrm{Vol}\big(\mathrm{Pyr}(C,\pi)\big) > \varepsilon.$$

Proof of Item (i): finiteness statements

Proposition

Consider a totally-real cubic cone in $\mathbb{R}^3$ *centered at* $O(0,0,0)$. *Let* $\varepsilon \in \mathbb{R}_+$.
Only finitely many (up to the action of $\Xi_+(C)$**)**: *integer base planes* π *on the* **unit integer distance** *to the origin satisfying*

$$\mathrm{Vol}\big(\mathrm{Pyr}(C,\pi)\big) > \varepsilon.$$

Remark. This is due to finiteness of affine types of faces for two-dimensional Klein's continued fraction.

Proof of Item (ii): case study

Ideas of the proof:

— Compactify the configuration space of all possible ξ-states (use projectivisation and certain asymptotics).

— Split the configuration space to several cases and comute finiteness for each of them separately.

The end

Thank you.

Klein polyhedra

F. Klein(1895) – geometric generalization.

H. Tsuchihasi(1973) – relation to cusp singularities.

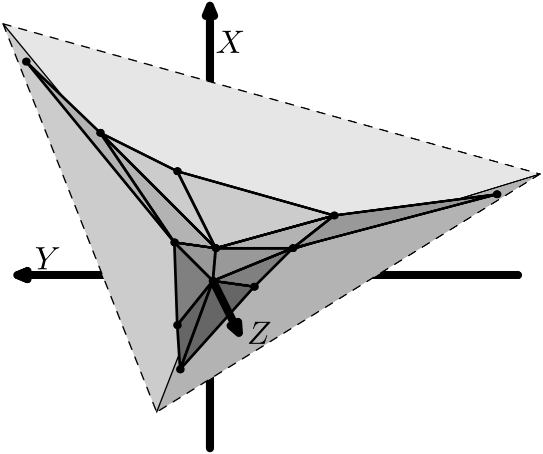
V. Arnold(1990) – formulated many problems.

M. Kontsevich, Yu. Suhov (1998) – existence of Gauss-Kuzmin statistic.
O. Karpenkov – general explicit formula via conformal geometry (2007).

J. Lachaud (1993), E. Korkina (1993), O. German (2009) – Lagrange theorem.

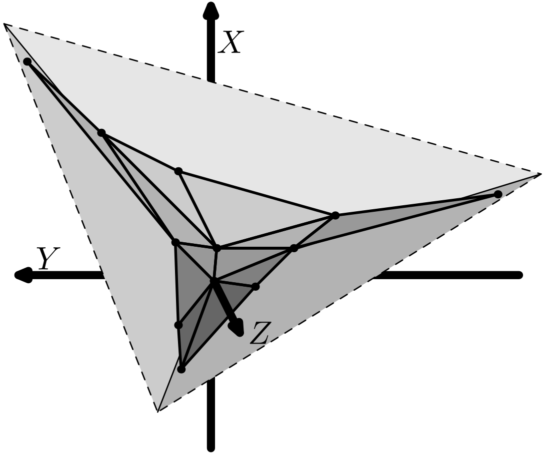
...

From sail to torus decomposition



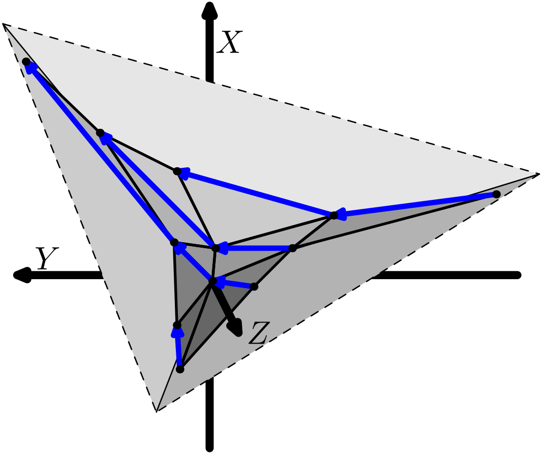
A sail for an algebraic operator A.

From sail to torus decomposition



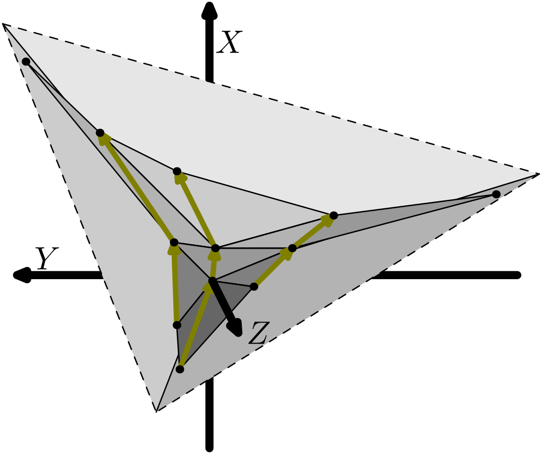
Let $\Xi(A)$ is generated by X and Y.

From sail to torus decomposition



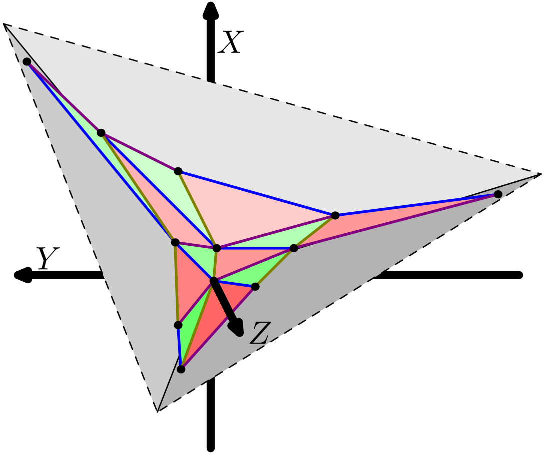
X acts on the sail as a shift.

From sail to torus decomposition



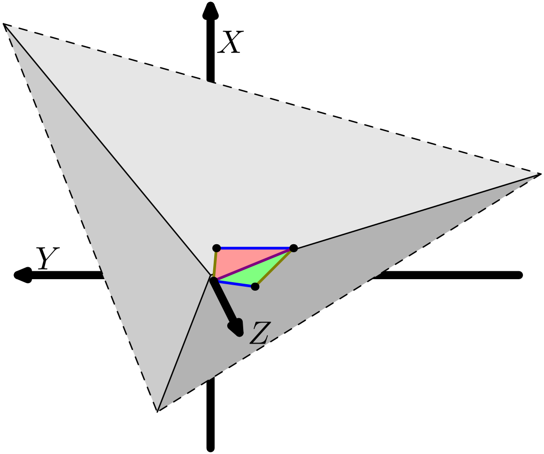
Y acts on the sail as a shift.

From sail to torus decomposition



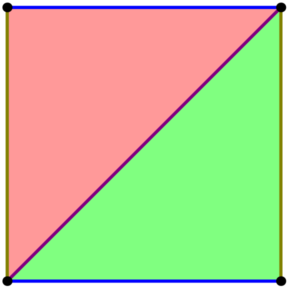
The orbits under the action of $\Xi(A)$.

From sail to torus decomposition



The fundamental domain of the action of $\Xi(A)$.

From sail to torus decomposition



So the factor of the sail under the action of $\Xi(A)$ is a compact torus (finitely many faces).