Optimization of polynomials for a problem in Number Theory

Francesco Battistoni

Università Cattolica del Sacro Cuore, Milano

19/01/2024

Table of contents

Number fields

$\mathbb{Q} :=$ rational numbers. $\mathbb{C} :=$ complex numbers.

Number field: a field K such that $\mathbb{Q} \subset K \subset \mathbb{C}$ and K has finite dimension as $\mathbb{Q}$-vector space.

Number fields

$\mathbb{Q} :=$ rational numbers. $\mathbb{C} :=$ complex numbers.

Number field: a field K such that $\mathbb{Q} \subset K \subset \mathbb{C}$ and K has finite dimension as $\mathbb{Q}$-vector space.

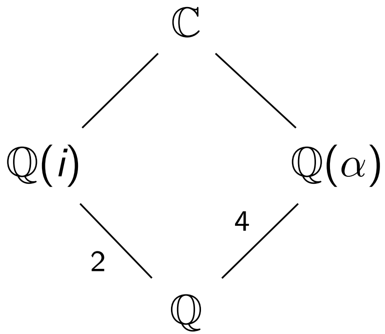
- $K = \mathbb{Q}(i) := \{a + ib\colon a, b \in \mathbb{Q}\}$ (with $i^2 = -1$) is a number field with dim $=$ 2.

Number fields

$\mathbb{Q}$:= rational numbers. $\mathbb{C}$:= complex numbers.

Number field: a field K such that $\mathbb{Q} \subset K \subset \mathbb{C}$ and K has finite dimension as $\mathbb{Q}$-vector space.

- $K = \mathbb{Q}(i) := \{a + ib \colon a, b \in \mathbb{Q}\}$ (with $i^2 = -1$) is a number field with dim = 2.
- Let $\alpha := e^{\frac{2\pi i}{5}}$. Then $K = \mathbb{Q}(\alpha) = \{a + b\alpha + c\alpha^2 + d\alpha^3 \colon a, b, c, d \in \mathbb{Q}\}$ is a number field with dim = 4.



Motivations

There are many reasons why people are interested in number fields. Some are:

- Better comprehension of integer equations (they were first used for partial study of Fermat's $x^n + y^n = z^n$).
- Algebraic varieties may be defined over number fields (e.g: conics, elliptic curves).

Motivations

There are many reasons why people are interested in number fields. Some are:

- Better comprehension of integer equations (they were first used for partial study of Fermat's $x^n + y^n = z^n$).
- Algebraic varieties may be defined over number fields (e.g: conics, elliptic curves).
- Cryptography.
- Algorithms for the factorization of prime numbers.
- Algorithms for the study of Euclidean lattices (e.g: LLL algorithm).

Classification of number fields

Goal: to classify and list all number fields satisfying certain properties.
E.g: number fields with minimal or sufficiently small values of the following invariants.

Classification of number fields

Goal: to classify and list all number fields satisfying certain properties.
E.g: number fields with minimal or sufficiently small values of the following invariants.

- **Discriminant:** an integer number Δ_K which generalizes the Δ of the second degree equations.
  $\Delta_{\mathbb{Q}(i)} = -4$, $\Delta_{\mathbb{Q}(\exp(2\pi i/5))} = 125$.

Classification of number fields

Goal: to classify and list all number fields satisfying certain properties.
E.g: number fields with minimal or sufficiently small values of the following invariants.

- **Discriminant:** an integer number Δ_K which generalizes the Δ of the second degree equations.
  $\Delta_{\mathbb{Q}(i)} = -4$, $\Delta_{\mathbb{Q}(\exp(2\pi i/5))} = 125$.
- **Regulator:** the determinant R_K of a matrix whose entries are logarithms of absolute values of numbers in K.
  $R_{\mathbb{Q}(i)} = 1$, $R_{\mathbb{Q}(\exp(2\pi i/5))} = 0.962423650119\ldots$

The classification is helped by softwares for Number Theory and Symbolic Algebra computations (PARI/GP, Magma, Sage...)

My Ph.D. work

2017-2020: my aim was to compute complete lists of number fields K with small discriminant and regulator in specific families which were not previously considered.

For these families finite lists can be obtained since:

- There are only finitely many K with $|d_K| \leq B$.
- There exist $C, D > 0$ such that $\log|d_K| \leq C + D \cdot R_K$.

My Ph.D. work

2017-2020: my aim was to compute complete lists of number fields K with small discriminant and regulator in specific families which were not previously considered.

For these families finite lists can be obtained since:

- There are only finitely many K with $|d_K| \leq B$.
- There exist $C, D > 0$ such that $\log |d_K| \leq C + D \cdot R_K$.

Small discriminants: I obtained the lists for all the families I considered.

Small regulators: The best we could get were conjectural results.

This happened because the constant C in the estimate above was not the best possible.

The main object of study

The constant C is the supremum of

$$P_n(\underline{\varepsilon}) := \prod_{1\leq i<j\leq n} \left|1 - \frac{\varepsilon_i}{\varepsilon_j}\right|$$

over all $\underline{\varepsilon} := (\varepsilon_1, \ldots, \varepsilon_n) \in \mathbb{C}^n$ such that $0 < |\varepsilon_1| \leq .. \leq |\varepsilon_n|$.

The main object of study

The constant C is the supremum of

$$P_n(\underline{\varepsilon}) := \prod_{1\le i<j\le n} \left|1 - \frac{\varepsilon_i}{\varepsilon_j}\right|$$

over all $\underline{\varepsilon} := (\varepsilon_1, \ldots, \varepsilon_n) \in \mathbb{C}^n$ such that $0 < |\varepsilon_1| \le .. \le |\varepsilon_n|$.

- Remak (1952): $P_n(\underline{\varepsilon}) \le n^{n/2}$. This was the value used in the procedure.

The main object of study

The constant C is the supremum of

$$P_n(\underline{\varepsilon}) := \prod_{1 \le i < j \le n} \left| 1 - \frac{\varepsilon_i}{\varepsilon_j} \right|$$

over all $\underline{\varepsilon} := (\varepsilon_1, \dots, \varepsilon_n) \in \mathbb{C}^n$ such that $0 < |\varepsilon_1| \le .. \le |\varepsilon_n|$.

- Remak (1952): $P_n(\underline{\varepsilon}) \le n^{n/2}$. This was the value used in the procedure.
- Pohst (1977): if every ε_i is real and $n \le 11$, then $P_n(\underline{\varepsilon}) \le 2^{\lfloor n/2 \rfloor}$ (where $\lfloor x \rfloor :=$ biggest integer $\le x$) and this bound is sharp.

The main object of study

The constant C is the supremum of

$$P_n(\underline{\varepsilon}) := \prod_{1 \leq i < j \leq n} \left| 1 - \frac{\varepsilon_i}{\varepsilon_j} \right|$$

over all $\underline{\varepsilon} := (\varepsilon_1, \ldots, \varepsilon_n) \in \mathbb{C}^n$ such that $0 < |\varepsilon_1| \leq .. \leq |\varepsilon_n|$.

- Remak (1952): $P_n(\underline{\varepsilon}) \leq n^{n/2}$. This was the value used in the procedure.
- Pohst (1977): if every ε_i is real and $n \leq 11$, then $P_n(\underline{\varepsilon}) \leq 2^{\lfloor n/2 \rfloor}$ (where $\lfloor x \rfloor :=$ biggest integer $\leq x$) and this bound is sharp.
- Friedman and Ramirez-Raposo (2018): if five of the ε_i are real and two are complex conjugated, then $P_7(\underline{\varepsilon}) \leq e^6 \simeq \frac{1}{2} \cdot 7^{7/2}$.

New settings of the problem

Summer-Autumn 2020: together with my Ph.D. advisor (Prof. Giuseppe Molteni, UniMi), we realized the following:

- The previous results suggest that among the n complex numbers ε_i, $2r$ of them should be complex conjugated couples, with the remaining being real.

New settings of the problem

Summer-Autumn 2020: together with my Ph.D. advisor (Prof. Giuseppe Molteni, UniMi), we realized the following:

- The previous results suggest that among the n complex numbers ε_i, $2r$ of them should be complex conjugated couples, with the remaining being real.
- Our families of fields are actually defined by numbers satisfying this relation.
- The smaller r, the smaller should be the true upper bound C of the "new" $P_{n,r}$.

New settings of the problem

Summer-Autumn 2020: together with my Ph.D. advisor (Prof. Giuseppe Molteni, UniMi), we realized the following:

- The previous results suggest that among the n complex numbers ε_i, $2r$ of them should be complex conjugated couples, with the remaining being real.
- Our families of fields are actually defined by numbers satisfying this relation.
- The smaller r, the smaller should be the true upper bound C of the "new" $P_{n,r}$.

We started with $r = 0$, i.e. Pohst's case with only real numbers ε_i.

Numerical experiments and some new insight led us to think that in this case $C = 2^{\lfloor n/2 \rfloor}$ was true for every $n \in \mathbb{N}$.

The real variables case

$$P_{n+1,0}(\underline{\varepsilon}) := \prod_{1\leq i<j\leq n+1} \left|1 - \frac{\varepsilon_i}{\varepsilon_j}\right|.$$

Remember that $0 < |\varepsilon_1| \leq |\varepsilon_2| \leq \cdots \leq |\varepsilon_{n+1}|$.

The real variables case

$$P_{n+1,0}(\underline{\varepsilon}) := \prod_{1\le i<j\le n+1} \left|1 - \frac{\varepsilon_i}{\varepsilon_j}\right|.$$

Remember that $0 < |\varepsilon_1| \le |\varepsilon_2| \le \cdots \le |\varepsilon_{n+1}|$.

The change of variables $x_i := \varepsilon_i/\varepsilon_{i+1}$ (for $i = 1, \dots, n$) gives

$$Q_n(x_1, \dots, x_n) := \prod_{i=1}^{n}\prod_{j=i}^{n}\left(1 - \prod_{k=i}^{j} x_k\right), \quad x_k \in [-1, 1] \quad \forall k.$$

We have obtained a multivariate polynomial over the hypercube $[-1, 1]^n$: if we prove that $\max_{\underline{x}\in[-1,1]^n} Q_n(\underline{x}) = 2^{\lfloor \frac{n+1}{2} \rfloor}$, we extend Pohst's result to every n.

The real variables case

$$P_{n+1,0}(\underline{\varepsilon}) := \prod_{1\le i<j\le n+1} \left|1-\frac{\varepsilon_i}{\varepsilon_j}\right|.$$

Remember that $0 < |\varepsilon_1| \le |\varepsilon_2| \le \cdots \le |\varepsilon_{n+1}|$.
The change of variables $x_i := \varepsilon_i/\varepsilon_{i+1}$ (for $i = 1, \ldots, n$) gives

$$Q_n(x_1,\ldots,x_n) := \prod_{i=1}^{n}\prod_{j=i}^{n}\left(1-\prod_{k=i}^{j} x_k\right), \quad x_k \in [-1,1] \quad \forall k.$$

We have obtained a multivariate polynomial over the hypercube $[-1,1]^n$: if we prove that $\max_{\underline{x}\in[-1,1]^n} Q_n(\underline{x}) = 2^{\lfloor \frac{n+1}{2} \rfloor}$, we extend Pohst's result to every n.

$$\max_{x_1\in[-1,1]} Q_1(x_1) = \max_{x_1\in[-1,1]}(1-x_1) = 2 = 2^{\lfloor \frac{1+1}{2} \rfloor},$$

$$\max_{(x_1,x_2)\in[-1,1]^2} Q_2(x_1,x_2) = \max_{(x_1,x_2)\in[-1,1]^2}(1-x_1)(1-x_1x_2)(1-x_2) = 2 = 2^{\lfloor \frac{2+1}{2} \rfloor}.$$

Configurations

Given a vector of signs $\boldsymbol{\rho} := (\rho_1, \ldots, \rho_n)$, we consider the function over $[0,1]^n$ defined as

$$Q_{n,\boldsymbol{\rho}}(x_1, \ldots, x_n) := \prod_{i=1}^{n} \prod_{j=i}^{n} \left(1 - \prod_{k=i}^{j} \rho_k \prod_{k=i}^{j} x_k\right)$$

which we call a **configuration of** Q_n.

Configurations

Given a vector of signs $\boldsymbol{\rho} := (\rho_1, \dots, \rho_n)$, we consider the function over $[0,1]^n$ defined as

$$Q_{n,\boldsymbol{\rho}}(x_1, \dots, x_n) := \prod_{i=1}^{n} \prod_{j=i}^{n} \left(1 - \prod_{k=i}^{j} \rho_k \prod_{k=i}^{j} x_k\right)$$

which we call a **configuration of** Q_n.

$$\begin{aligned} Q_{3,(+,-,-)}(x_1, x_2, x_3) = \quad & (1 - x_1) \quad (1 + x_1 x_2) \quad (1 - x_1 x_2 x_3) \\ & \qquad\qquad (1 + x_2) \qquad (1 - x_2 x_3) \\ & \qquad\qquad\qquad\qquad (1 + x_3) \end{aligned}$$

Calculus and constrained optimization show that the maximum of this configuration is $2 < 2^{\lfloor (3+1)/2 \rfloor} = 4$.We want to prove $Q_{n,\boldsymbol{\rho}} \leq 2^{\lfloor \frac{n+1}{2} \rfloor}$ for the 2^n choices of $\boldsymbol{\rho}$.

Problem: as n increases, the partial derivatives approach becomes unsustainable.

Graphical schemes

$$
Q_{3,(+,-,-)}(x_1,x_2,x_3) = \begin{array}{ccc} (1-x_1) & (1+x_1x_2) & (1-x_1x_2x_3) \\ & (1+x_2) & (1-x_2x_3) \\ & & (1+x_3) \end{array}
$$

We represent a configuration $Q_{n,\varepsilon}$ with a triangular array formed by signs $+$ and $-$, each sign at (i,j) being equal to $\prod_{k=i}^{j} \rho_k$.

$$
Q_{3,(+,-,-)} = \begin{array}{|c|c|c|} \hline + & - & + \\ \hline & - & + \\ \cline{2-3} & & - \\ \cline{3-3} \end{array}
\qquad
Q_{4,(-,+,+,-)} = \begin{array}{|c|c|c|c|} \hline - & - & - & + \\ \hline & + & + & - \\ \cline{2-4} & & + & - \\ \cline{3-4} & & & - \\ \cline{4-4} \end{array}
$$

Graphical schemes

$$Q_{3,(+,-,-)}(x_1,x_2,x_3) = \begin{array}{ccc} (1-x_1) & (1+x_1x_2) & (1-x_1x_2x_3) \\ & (1+x_2) & (1-x_2x_3) \\ & & (1+x_3) \end{array}$$

We represent a configuration $Q_{n,\varepsilon}$ with a triangular array formed by signs $+$ and $-$, each sign at (i,j) being equal to $\prod_{k=i}^{j} \rho_k$.

$$Q_{3,(+,-,-)} = \begin{array}{|c|c|c|} \hline + & - & + \\ \hline & - & + \\ \cline{2-3} & & - \\ \cline{3-3} \end{array} \qquad Q_{4,(-,+,+,-)} = \begin{array}{|c|c|c|c|} \hline - & - & - & + \\ \hline & + & + & - \\ \cline{2-4} & & + & - \\ \cline{3-4} & & & - \\ \cline{4-4} \end{array}$$

Every $n \times n$ triangular array A formed by $+$ and $-$ (we call it **graphical scheme of dimension** n) corresponds to a function $F_A : [0,1]^n \to \mathbb{R}$ defined as

$$F_A(x_1,\ldots,x_n) = \prod_{i=1}^{n} \prod_{j=i}^{n} \left(1 - A_{i,j} \prod_{k=i}^{j} x_k\right).$$

Estimates and patterns of graphical schemes

Pohst's original idea: in a graphical scheme A we can recognize patterns, corresponding to bounded factors of F_A. Consider a sign at place (i,j):

$$i\overset{j}{\boxed{+}} \leq 1$$ since it corresponds to $(1-u) \leq 1$ for $u \in [0,1]$.

Estimates and patterns of graphical schemes

Pohst's original idea: in a graphical scheme A we can recognize patterns, corresponding to bounded factors of F_A. Consider a sign at place (i, j):

- $\begin{array}{c|c|} & j \\ \cline{2-2} i & + \\ \cline{2-2} \end{array} \leq 1$ since it corresponds to $(1-u) \leq 1$ for $u \in [0,1]$.
- $\begin{array}{c|c|c|} & j & j' \\ \cline{2-3} i & + & - \\ \cline{2-3} \end{array} \leq 1$ since it corresponds to $(1-u)(1+uv) \leq 1$ for $u, v \in [0,1]$.
- $\begin{array}{c|c|} & j \\ \cline{2-2} i & - \\ \cline{2-2} i' & + \\ \cline{2-2} \end{array} \leq 1$ for the very same reason.

Estimates and patterns of graphical schemes

Pohst's original idea: in a graphical scheme A we can recognize patterns, corresponding to bounded factors of F_A. Consider a sign at place (i, j):

$$\begin{array}{c|c|}\multicolumn{1}{c}{} & \multicolumn{1}{c}{j}\\ \cline{2-2} i & + \\ \cline{2-2}\end{array} \leq 1$$ since it corresponds to $(1-u) \leq 1$ for $u \in [0, 1]$.

$$\begin{array}{c|c|c|}\multicolumn{1}{c}{} & \multicolumn{1}{c}{j} & \multicolumn{1}{c}{j'}\\ \cline{2-3} i & + & - \\ \cline{2-3}\end{array} \leq 1$$ since it corresponds to $(1-u)(1+uv) \leq 1$ for $u, v \in [0, 1]$.

$$\begin{array}{c|c|}\multicolumn{1}{c}{} & \multicolumn{1}{c}{j}\\ \cline{2-2} i & - \\ \cline{2-2} i' & + \\ \cline{2-2}\end{array} \leq 1$$ for the very same reason.

$$\begin{array}{c|c|c|}\multicolumn{1}{c}{} & \multicolumn{1}{c}{j} & \multicolumn{1}{c}{j'}\\ \cline{2-3} i & - & + \\ \cline{2-3} i' & + & - \\ \cline{2-3}\end{array} \leq 1$$ since $(1-u)(1+uv)(1+uw)(1-uvw) \leq 1$ for $u, v, w \in [0, 1]$.

$$\begin{array}{c|c|c|}\multicolumn{1}{c}{} & \multicolumn{1}{c}{j} & \multicolumn{1}{c}{j+1}\\ \cline{2-3} i & - & + \\ \cline{2-3} \multicolumn{1}{c}{i+1} & \multicolumn{1}{c|}{} & - \\ \cline{3-3}\end{array} \leq 2$$ since it is nothing but a consequence of $Q_2(x_1, x_2) \leq 2$, which we already know.

Covering the scheme with patterns gives an upper bound to F_A.

An example

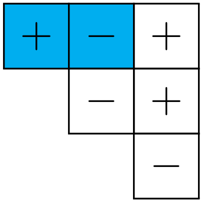
We can use Pohst's bounds to prove the result for the configuration shown before.

$$Q_{3,(+,-,-)} = \begin{array}{ccc} \boxed{+} & \boxed{-} & \boxed{+} \\ & \boxed{-} & \boxed{+} \\ & & \boxed{-} \end{array}$$

An example

We can use Pohst's bounds to prove the result for the configuration shown before.

$$Q_{3,(+,-,-)} =$$

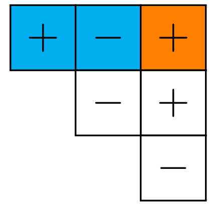


The blue factors correspond to $(1 - x_1)(1 + x_1 x_2) \leq 1$.

An example

We can use Pohst's bounds to prove the result for the configuration shown before.

$$Q_{3,(+,-,-)} =$$

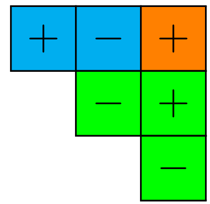


The blue factors correspond to $(1 - x_1)(1 + x_1 x_2) \leq 1$.
The orange factor corresponds to $(1 - x_1 x_2 x_3) \leq 1$.

An example

We can use Pohst's bounds to prove the result for the configuration shown before.

$$Q_{3,(+,-,-)} =$$



The blue factors correspond to $(1 - x_1)(1 + x_1 x_2) \leq 1$.
The orange factor corresponds to $(1 - x_1 x_2 x_3) \leq 1$.

The green factors correspond to $Q_{2,(-,-)} \leq 2$.

Therefore the function $Q_{3,(+,-,-)}$ associated to this scheme is ≤ 2.

We can use this technique to obtain estimates for certain configurations for every n.

Configuration with negative signs

Theorem

Let Q_{n,ρ_-} be the configuration of Q_n with all negative signs. Then, $Q_{n,\rho_-}(x_1, \ldots, x_n) \leq 2^{\lfloor (n+1)/2 \rfloor}$.

Configuration with negative signs

Theorem

Let Q_{n,ρ_-} be the configuration of Q_n with all negative signs. Then, $Q_{n,\rho_-}(x_1, \ldots, x_n) \leq 2^{\lfloor (n+1)/2 \rfloor}$.

Proof: If $n = 1$ or $n = 2$ the claim is trivial. Assume $n \geq 3$ is odd and the claim is true for every dimension $< n$. The configuration is represented by the scheme

$$A_{n,-} = \begin{array}{|c|c|c|c|c|c|c|}\hline - & + & - & + & \cdots & + & - \\ \hline & - & + & - & \cdots & - & + \\ \hline \end{array}_{\;A_{n-2,-}}$$

where $A_{n-2,-} \leq 2^{\lfloor (n-1)/2 \rfloor}$ by hypothesis.

Configuration with negative signs

Theorem

Let Q_{n,ρ_-} be the configuration of Q_n with all negative signs. Then, $Q_{n,\rho_-}(x_1,\ldots,x_n) \le 2^{\lfloor (n+1)/2 \rfloor}$.

Proof: If $n = 1$ or $n = 2$ the claim is trivial. Assume $n \ge 3$ is odd and the claim is true for every dimension $< n$. The configuration is represented by the scheme

$$A_{n,-} = \begin{array}{|c|c|c|c|c|c|c|} \hline - & + & - & + & \cdots & + & - \\ \hline & - & + & - & \cdots & - & + \\ \hline \end{array}_{\;A_{n-2,-}}$$

where $A_{n-2,-} \le 2^{\lfloor (n-1)/2 \rfloor}$ by hypothesis. In the first two rows we have one triangle $\begin{smallmatrix} & 1 & 2 \\ 1 & - & + \\ 2 & & - \end{smallmatrix} \le 2$, we have $\lfloor \frac{n-2}{2} \rfloor$ squares $\begin{smallmatrix} & j & j' \\ 1 & - & + \\ 2 & + & - \end{smallmatrix} \le 1$ and one final vertical segment $\begin{smallmatrix} & n \\ 1 & - \\ 2 & + \end{smallmatrix} \le 1$.

Configuration with negative signs

Theorem

Let Q_{n,ρ_-} be the configuration of Q_n with all negative signs. Then, $Q_{n,\rho_-}(x_1,\dots,x_n) \leq 2^{\lfloor (n+1)/2 \rfloor}$.

Proof: If $n=1$ or $n=2$ the claim is trivial. Assume $n \geq 3$ is odd and the claim is true for every dimension $< n$. The configuration is represented by the scheme

$$A_{n,-} = \begin{array}{|c|c|c|c|c|c|c|} \hline - & + & - & + & \cdots & + & - \\ \hline & - & + & - & \cdots & - & + \\ \hline \end{array}_{\;A_{n-2,-}}$$

where $A_{n-2,-} \leq 2^{\lfloor (n-1)/2 \rfloor}$ by hypothesis. In the first two rows we have one triangle $\begin{array}{c|c|c|} & 1 & 2 \\ \hline 1 & - & + \\ \hline 2 & & - \\ \hline \end{array} \leq 2,$ we have $\lfloor \frac{n-2}{2} \rfloor$ squares $\begin{array}{c|c|c|} & j & j' \\ \hline 1 & - & + \\ \hline 2 & + & - \\ \hline \end{array} \leq 1$ and one final vertical segment $\begin{array}{c|c|} & n \\ \hline 1 & - \\ \hline 2 & + \\ \hline \end{array} \leq 1$. The contribution of the first two rows is then ≤ 2 and so

$$A_{n,-} \leq 2 \cdot 2^{\lfloor (n-1)/2 \rfloor} = 2^{\lfloor \frac{n+1}{2} \rfloor}.$$

For $n \geq 4$ even the proof is completely similar.

Transforming patterns

If A, A' are graphical schemes of dimension n, we say $A \leq A'$ if $F_A \leq F_{A'}$.
New idea: instead of just detecting patterns, we replace them with other patterns as result of an estimate.

Transforming patterns

If A, A' are graphical schemes of dimension n, we say $A \leq A'$ if $F_A \leq F_{A'}$.
New idea: instead of just detecting patterns, we replace them with other patterns as result of an estimate.

P) $i\overset{j}{\boxed{+}} \;\leq\; i\overset{j}{\boxed{-}}$ since $(1-u) \leq (1+u)$ for $u \in [0,1]$.

H) $i\overset{j\ \ j'}{\boxed{+}\!\boxed{-}} \;\leq\; i\overset{j\ \ j'}{\boxed{-}\!\boxed{+}}$ since $(1-u)(1+uv) \leq (1+u)(1-uv)$ for $u, v \in [0,1]$.

Transforming patterns

If A, A' are graphical schemes of dimension n, we say $A \leq A'$ if $F_A \leq F_{A'}$.
New idea: instead of just detecting patterns, we replace them with other patterns as result of an estimate.

P) $\begin{array}{c|c|} & j \\ \cline{2-2} i & + \\ \cline{2-2} \end{array} \leq \begin{array}{c|c|} & j \\ \cline{2-2} i & - \\ \cline{2-2} \end{array}$ since $(1-u) \leq (1+u)$ for $u \in [0,1]$.

H) $\begin{array}{c|c|c|} & j & j' \\ \cline{2-3} i & + & - \\ \cline{2-3} \end{array} \leq \begin{array}{c|c|c|} & j & j' \\ \cline{2-3} i & - & + \\ \cline{2-3} \end{array}$ since $(1-u)(1+uv) \leq (1+u)(1-uv)$ for $u, v \in [0,1]$.

V) $\begin{array}{c|c|} & j \\ \cline{2-2} i & - \\ \cline{2-2} i' & + \\ \cline{2-2} \end{array} \leq \begin{array}{c|c|} & j \\ \cline{2-2} i & + \\ \cline{2-2} i' & - \\ \cline{2-2} \end{array}$ for the very same reason.

S) $\begin{array}{c|c|c|} & j & j' \\ \cline{2-3} i & - & + \\ \cline{2-3} i' & + & - \\ \cline{2-3} \end{array} \leq \begin{array}{c|c|c|} & j & j' \\ \cline{2-3} i & + & - \\ \cline{2-3} i' & - & + \\ \cline{2-3} \end{array}$ since for $u, v, w \in [0,1]$ we have

$$(1-u)(1+uv)(1+uw)(1-uvw) \leq (1+u)(1-uv)(1-uw)(1+uvw).$$

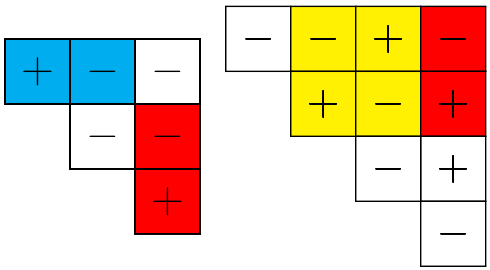
Every replacement is a move on A and produces a new scheme A' and an estimate $A \leq A'$.

Wrong and correct signs

Given a graphical scheme A, we say that the sign $A_{i,j}$ is **wrong** if $A_{i,j} = (-1)^{i-j}$, and is **correct** otherwise.
By definition, the only graphical scheme with every sign being correct is the configuration with negative signs $A_{n,-}$.

Wrong and correct signs

Given a graphical scheme A, we say that the sign $A_{i,j}$ is **wrong** if $A_{i,j} = (-1)^{i-j}$, and is **correct** otherwise.
By definition, the only graphical scheme with every sign being correct is the configuration with negative signs $A_{n,-}$.

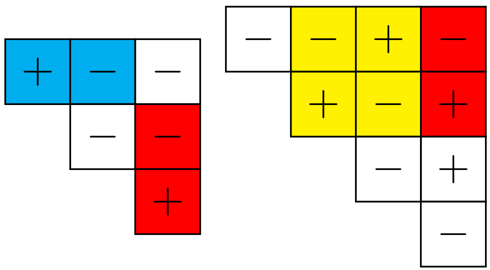


The labeled signs are wrong.

- The first scheme presents two patterns to which we apply a move H and a move V. These moves correct the scheme into the one with negative signs.
- The second scheme is corrected by a move S and a move V.

Wrong and correct signs

Given a graphical scheme A, we say that the sign $A_{i,j}$ is **wrong** if $A_{i,j} = (-1)^{i-j}$, and is **correct** otherwise.
By definition, the only graphical scheme with every sign being correct is the configuration with negative signs $A_{n,-}$.



The labeled signs are wrong.

- The first scheme presents two patterns to which we apply a move H and a move V. These moves correct the scheme into the one with negative signs.
- The second scheme is corrected by a move S and a move V.

But the correction of a scheme A with moves P, H, V and S gives $A \leq A_{n,-} \leq 2^{\lfloor \frac{n+1}{2} \rfloor}$. Is this always possible?

The theorem

Theorem (B., Molteni 2021)

Let A be a configuration of Q_n. There is a list $\mathcal{L}$ of moves P, H, V, S which corrects A into the configuration $C_{n,-}$ defined by negative signs.

Corollary

$$\max_{(x_1,\ldots,x_n)\in[-1,1]^n} Q_n(x_1,\ldots,x_n) = 2^{\lfloor \frac{n+1}{2} \rfloor}.$$

The theorem

Theorem (B., Molteni 2021)

Let A be a configuration of Q_n. There is a list $\mathcal{L}$ of moves P, H, V, S which corrects A into the configuration $C_{n,-}$ defined by negative signs.

Corollary

$$\max_{(x_1,\ldots,x_n)\in[-1,1]^n} Q_n(x_1,\ldots,x_n) = 2^{\lfloor \frac{n+1}{2} \rfloor}.$$

The list $\mathcal{L}$ is created by induction on the dimension n.

- $n = 1$: either $A = -$, and we are done, or $A = +$, and we apply P.

The theorem

Theorem (B., Molteni 2021)

Let A be a configuration of Q_n. There is a list $\mathcal{L}$ of moves P, H, V, S which corrects A into the configuration $C_{n,-}$ defined by negative signs.

Corollary

$$\max_{(x_1,\ldots,x_n)\in[-1,1]^n} Q_n(x_1,\ldots,x_n) = 2^{\lfloor \frac{n+1}{2} \rfloor}.$$

The list $\mathcal{L}$ is created by induction on the dimension n.

- $n = 1$: either $A = -$, and we are done, or $A = +$, and we apply P.
- $n - 1 \to n$: let A' be the configuration obtained removing the n-th column from A. By inductive hypothesis exists a list $\mathcal{L}'$ of moves which applied to A' gives $A' \leq A_{n-1,-}$ (the one in dimension $n-1$).

The theorem

Theorem (B., Molteni 2021)

Let A be a configuration of Q_n. There is a list $\mathcal{L}$ of moves P, H, V, S which corrects A into the configuration $C_{n,-}$ defined by negative signs.

Corollary

$$\max_{(x_1,\ldots,x_n)\in[-1,1]^n} Q_n(x_1,\ldots,x_n) = 2^{\lfloor \frac{n+1}{2} \rfloor}.$$

The list $\mathcal{L}$ is created by induction on the dimension n.

- $n = 1$: either $A = -$, and we are done, or $A = +$, and we apply P.
- $n - 1 \to n$: let A' be the configuration obtained removing the n-th column from A. By inductive hypothesis exists a list $\mathcal{L}'$ of moves which applied to A' gives $A' \leq A_{n-1,-}$ (the one in dimension $n - 1$).
- We look at the signs in the n-th column and correct them adding new moves which may overlap with old moves over A' in $\mathcal{L}'$.

Fundamental steps

- We examine the n-th column, and we look for the 1st wrong $-$ starting from the bottom. If $A_{i,j} = -$ is wrong, we have to decide whether applying V or H (or S).
- There is a precise criterion for this choice: sum the signs to the left of $A_{i,j}$ and the signs below. The two sums (we call them $\mathcal{H}(i,j)$ and $\mathcal{V}(i,j)$) are opposite to each other.

Fundamental steps

- We examine the n-th column, and we look for the 1st wrong $-$ starting from the bottom. If $A_{i,j} = -$ is wrong, we have to decide whether applying V or H (or S).
- There is a precise criterion for this choice: sum the signs to the left of $A_{i,j}$ and the signs below. The two sums (we call them $\mathcal{H}(i,j)$ and $\mathcal{V}(i,j)$) are opposite to each other.
- If $\mathcal{V}(i,j) > 0$, pick the first wrong $+$ available below $A_{i,j}$ and add a move V to the list.
- If $\mathcal{H}(i,j) > 0$, pick the first wrong $+$ to the left of $A_{i,j}$. If this $+$ is corrected by a V in $\mathcal{L}'$, replace V with a move S. If the wrong $+$ is corrected by P, replace it with a move H.

Fundamental steps

- We examine the n-th column, and we look for the 1st wrong $-$ starting from the bottom. If $A_{i,j} = -$ is wrong, we have to decide whether applying V or H (or S).
- There is a precise criterion for this choice: sum the signs to the left of $A_{i,j}$ and the signs below. The two sums (we call them $\mathcal{H}(i,j)$ and $\mathcal{V}(i,j)$) are opposite to each other.
- If $\mathcal{V}(i,j) > 0$, pick the first wrong $+$ available below $A_{i,j}$ and add a move V to the list.
- If $\mathcal{H}(i,j) > 0$, pick the first wrong $+$ to the left of $A_{i,j}$. If this $+$ is corrected by a V in $\mathcal{L}'$, replace V with a move S. If the wrong $+$ is corrected by P, replace it with a move H.
- Once every wrong $-$ on the n-th column has been corrected, correct every remaining wrong $+$ with a move P.

Remark: there are some subtle issues that need to be checked in order for this procedure to work (for example that wrong $+$ are always available whenever one applies a move V).

An instance of the algorithm

We want to apply the algorithm to the following configuration of dimension 6.

$+$	$-$	$-$	$-$	$+$	$+$
	$-$	$-$	$-$	$+$	$+$
		$+$	$+$	$-$	$-$
			$+$	$-$	$-$
				$-$	$-$
					$+$

An instance of the algorithm

We want to apply the algorithm to the following configuration of dimension 6.

$+$	$-$	$-$	$-$	$+$	$+$
	$-$	$-$	$-$	$+$	$+$
		$+$	$+$	$-$	$-$
			$+$	$-$	$-$
				$-$	$-$
					$+$

Column 1: there are no wrong $-$ and there is a wrong $+$. We get

$$\mathcal{L} = \{P[1;1]\}.$$

An instance of the algorithm

We want to apply the algorithm to the following configuration of dimension 6.

$+$	$-$	$-$	$-$	$+$	$+$
	$-$	$-$	$-$	$+$	$+$
		$+$	$+$	$-$	$-$
			$+$	$-$	$-$
				$-$	$-$
					$+$

Column 2: we have $\mathcal{H}(1,2) = 1$ and in the old list there was a P. We replace it with

$$\mathcal{L} = \{H[1;1,2]\}.$$

An instance of the algorithm

We want to apply the algorithm to the following configuration of dimension 6.

$+$	$-$	$-$	$-$	$+$	$+$
	$-$	$-$	$-$	$+$	$+$
		$+$	$+$	$-$	$-$
			$+$	$-$	$-$
				$-$	$-$
					$+$

Column 3: we have $\mathcal{V}(2,3) = 1$ and we get

$$\mathcal{L} = \{H[1;1,2], V[2,3;3]\}.$$

An instance of the algorithm

We want to apply the algorithm to the following configuration of dimension 6.

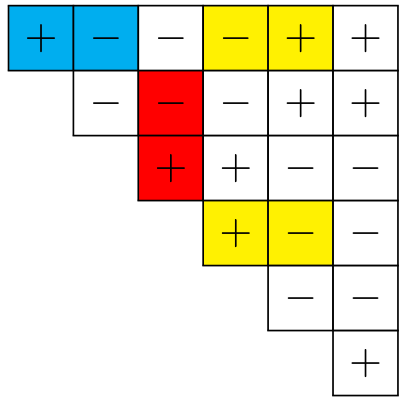
$+$	$-$	$-$	$-$	$+$	$+$
	$-$	$-$	$-$	$+$	$+$
		$+$	$+$	$-$	$-$
			$+$	$-$	$-$
				$-$	$-$
					$+$

Column 4: we have $\mathcal{V}(1,4) = 1$ and we get

$$\mathcal{L} = \{H[1;1,2], V[2,3;3], V[1,4;4]\}.$$

An instance of the algorithm

We want to apply the algorithm to the following configuration of dimension 6.

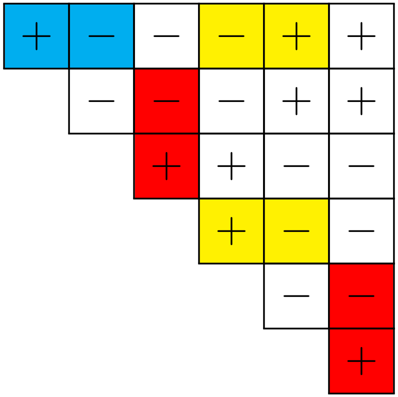


Column 5: we have $\mathcal{H}(4,5) = 1$ and previously we had $V[1,4;4]$, so we replace this move by a move S. We get

$$\mathcal{L} = \{H[1;1,2], V[2,3;3], S[1,4;4,5]\}.$$

.

We want to apply the algorithm to the following configuration of dimension 6.

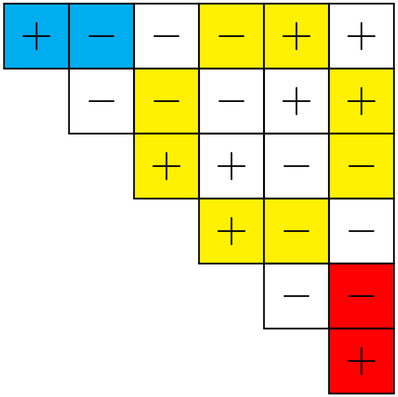


Column 6: we have $\mathcal{V}(5,6) = 1$ and we get

$$\mathcal{L} = \{H[1;1,2], V[2,3;3], S[1,4;4,5], V[5,6;6]\}.$$

An instance of the algorithm

We want to apply the algorithm to the following configuration of dimension 6.



Column 6: we have $\mathcal{H}(3,6) = 1$ and previously we had $V[2,3;3]$, so we replace this move by a move S. We get

$$\mathcal{L} = \{H[1;1,2], S[2,3;3,6], S[1,4;4,5], V[5,6;6]\}.$$

Remarks and new problems

- The maximum of Q_n is always attained at $(-1, 0, -1, 0, \ldots)$, hence at the boundary of the hypercube.
- It would be nice to have a property which immediately states that the maximum points are on the boundary. Unfortunately, Q_n is superharmonic, not subharmonic.

Remarks and new problems

- The maximum of Q_n is always attained at $(-1, 0, -1, 0, \ldots)$, hence at the boundary of the hypercube.
- It would be nice to have a property which immediately states that the maximum points are on the boundary. Unfortunately, Q_n is superharmonic, not subharmonic.
- The result is general but not yet applied to the classification of number fields: in fact, for $n \geq 10$ we do not have complete lists of number fields with small discriminant.

Remarks and new problems

- The maximum of Q_n is always attained at $(-1, 0, -1, 0, \ldots)$, hence at the boundary of the hypercube.
- It would be nice to have a property which immediately states that the maximum points are on the boundary. Unfortunately, Q_n is superharmonic, not subharmonic.
- The result is general but not yet applied to the classification of number fields: in fact, for $n \geq 10$ we do not have complete lists of number fields with small discriminant.

2021-2022: together with Molteni, we tried to investigate the case with $r = 1$ (i.e. one couple of complex conjugated ε_i's), since the easiest family for which I obtained the tables falls into this case.

The problem becomes more difficult.

The case with $r = 1$

$$P_{n+1,1}(\underline{\varepsilon}) := \prod_{1 \leq i < j \leq n+1} \left| 1 - \frac{\varepsilon_i}{\varepsilon_j} \right|.$$

For $n + 1 = 3, 4$, the old upper bounds $(3^{3/2}, 4^{4/2} = 16)$ are the correct ones.

The case with $r = 1$

$$P_{n+1,1}(\underline{\varepsilon}) := \prod_{1 \le i < j \le n+1} \left| 1 - \frac{\varepsilon_i}{\varepsilon_j} \right|.$$

For $n + 1 = 3, 4$, the old upper bounds $(3^{3/2}, 4^{4/2} = 16)$ are the correct ones.

FIRST PROBLEM: There is a couple of complex conjugated ε_k and ε_{k+1}: there are different changes of variables depending on the position of k.

$$\varepsilon_k = r_k e^{i\theta}, \quad g := \cos\theta, x_i := \begin{cases} \frac{\varepsilon_i}{\varepsilon_{i+1}} & i \neq k-1, k \\ \frac{\varepsilon_{k-1}}{r_k} & i = k-1, \\ \frac{r_k}{\varepsilon_{k+1}} & i = k \end{cases}$$

The case with $r = 1$

$$P_{n+1,1}(\underline{\varepsilon}) := \prod_{1\le i<j\le n+1} \left|1 - \frac{\varepsilon_i}{\varepsilon_j}\right|.$$

For $n+1 = 3, 4$, the old upper bounds ($3^{3/2}, 4^{4/2} = 16$) are the correct ones.

FIRST PROBLEM: There is a couple of complex conjugated ε_k and ε_{k+1}: there are different changes of variables depending on the position of k.

$$\varepsilon_k = r_k e^{i\theta}, \quad g := \cos\theta, x_i := \begin{cases} \frac{\varepsilon_i}{\varepsilon_{i+1}} & i \neq k-1, k \\ \frac{\varepsilon_{k-1}}{r_k} & i = k-1, \\ \frac{r_k}{\varepsilon_{k+1}} & i = k \end{cases}$$

This results in several functions arising from the same $P_{n+1,1}(\underline{\varepsilon})$ (**orderings**).
E.g: $n+1 = 5$, ε_4 and ε_5 conjugated (1st ordering)

$$\begin{array}{cccc} (1-x_1) & (1-x_1x_2) & (1-2x_1x_2x_3g+(x_1x_2x_3)^2) & \\ & (1-x_2) & (1-2x_2x_3g+(x_2x_3)^2) & \\ & & (1-2x_3g+x_3^2) & 2\sqrt{1-g^2} \end{array}$$

The case with $r = 1$

$$P_{n+1,1}(\underline{\varepsilon}) := \prod_{1\leq i<j\leq n+1} \left|1 - \frac{\varepsilon_i}{\varepsilon_j}\right|.$$

For $n+1 = 3, 4$, the old upper bounds $(3^{3/2}, 4^{4/2} = 16)$ are the correct ones.

FIRST PROBLEM: There is a couple of complex conjugated ε_k and ε_{k+1}: there are different changes of variables depending on the position of k.

$$\varepsilon_k = r_k e^{i\theta}, \quad g := \cos\theta, x_i := \begin{cases} \frac{\varepsilon_i}{\varepsilon_{i+1}} & i \neq k-1, k \\ \frac{\varepsilon_{k-1}}{r_k} & i = k-1, \\ \frac{r_k}{\varepsilon_{k+1}} & i = k \end{cases}$$

This results in several functions arising from the same $P_{n+1,1}(\underline{\varepsilon})$ (**orderings**).
E.g: $n+1 = 5$, ε_3 and ε_4 conjugated (<u>2nd ordering</u>)

$$\begin{array}{lll} (1-x_1) & (1-2x_1x_2g+(x_1x_2)^2) & (1-x_1x_2x_3) \\ & (1-2x_2g+x_2^2) & (1-x_2x_3) \\ & & (1-2x_3g+x_3^2) \quad 2\sqrt{1-g^2} \end{array}$$

The procedure for $n + 1 = 5$

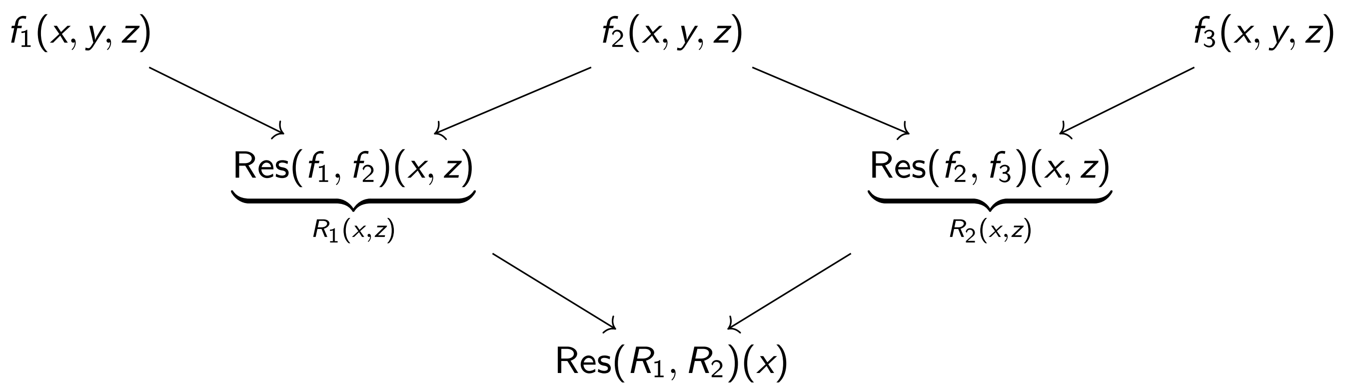
For the two orderings of $P_{5,1}$, we look for common zeros of polynomials associated to partial derivatives.

Algebraic Elimination Theory: common zeros of multivariate polynomials arise from zeros of successive *resultants*, with the number of variables decreasing.

The procedure for $n + 1 = 5$

For the two orderings of $P_{5,1}$, we look for common zeros of polynomials associated to partial derivatives.

Algebraic Elimination Theory: common zeros of multivariate polynomials arise from zeros of successive *resultants*, with the number of variables decreasing.



Common zeros of f_i have x component which is a zero of $\mathrm{Res}(R_1, R_2)(x)$.

From this, we prove (via Symbolic Algebra softwares) that there are no critical points for the orderings of $P_{5,1}$ in the interior of $[-1, 1]^4$.

Elimination Theory on the boundaries

We repeat this process on the boundaries of $[-1,1]^4$, so that we have less variables to deal with. We find (easy) critical points.

$$
\begin{array}{cccc}
(1-x_1) & (1-x_1x_2) & (1-2x_1x_2x_3g+(x_1x_2x_3)^2) & \\
 & (1-x_2) & (1-2x_2x_3g+(x_2x_3)^2) & \\
 & & (1-2x_3g+x_3^2) & 2\sqrt{1-g^2}
\end{array}
$$

Elimination Theory on the boundaries

We repeat this process on the boundaries of $[-1,1]^4$, so that we have less variables to deal with. We find (easy) critical points.

$$\begin{array}{cccc} (1-x_1) & (1-x_1x_2) & (1-2x_1x_2x_3g+(x_1x_2x_3)^2) & \\ & (1-x_2) & (1-2x_2x_3g+(x_2x_3)^2) & \\ & & (1-2x_3g+x_3^2) & 2\sqrt{1-g^2} \end{array}$$

Maximum point: $(x_1,x_2,x_3,g)=\left(\frac{-1}{\sqrt{7}},-1,1,\frac{-1}{2\sqrt{7}}\right)$.

Maximum value: $16M = 16.6965\ldots$ where $M = 3^{15/2}/(4\cdot 7^{7/2})$.

$$16.6965\ldots < 5^{5/2} = 55.90169\ldots$$

Elimination Theory on the boundaries

We repeat this process on the boundaries of $[-1,1]^4$, so that we have less variables to deal with. We find (easy) critical points.

$$\begin{array}{cccc} (1-x_1) & (1-x_1x_2) & (1-2x_1x_2x_3g+(x_1x_2x_3)^2) & \\ & (1-x_2) & (1-2x_2x_3g+(x_2x_3)^2) & \\ & & (1-2x_3g+x_3^2) & 2\sqrt{1-g^2} \end{array}$$

Maximum point: $(x_1,x_2,x_3,g) = \left(\frac{-1}{\sqrt{7}}, -1, 1, \frac{-1}{2\sqrt{7}}\right)$.

Maximum value: $16M = 16.6965\ldots$ where $M = 3^{15/2}/(4\cdot 7^{7/2})$.

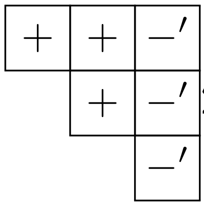
$$16.6965\ldots < 5^{5/2} = 55.90169\ldots$$

This improvement allows to expand the list of number fields with small regulator in the family associated to $P_{5,1}$.

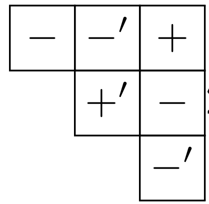
However, if we increase n, direct applications of Elimination Theory to our functions become computationally unsustainable.

Graphical schemes, again

We can use again graphical schemes and configurations, with a new notation for the terms containing g.



$2\sqrt{1-g^2}$



$2\sqrt{1-g^2}$

Graphical schemes, again

We can use again graphical schemes and configurations, with a new notation for the terms containing g.

$$\begin{array}{|c|c|c|}\hline + & + & -' \\ \hline \multicolumn{1}{c|}{} & + & -' \\ \cline{2-3} \multicolumn{1}{c}{} & \multicolumn{1}{c|}{} & -' \\ \cline{3-3}\end{array} 2\sqrt{1-g^2} \qquad \begin{array}{|c|c|c|}\hline - & -' & + \\ \hline \multicolumn{1}{c|}{} & +' & - \\ \cline{2-3} \multicolumn{1}{c}{} & \multicolumn{1}{c|}{} & -' \\ \cline{3-3}\end{array} 2\sqrt{1-g^2}$$

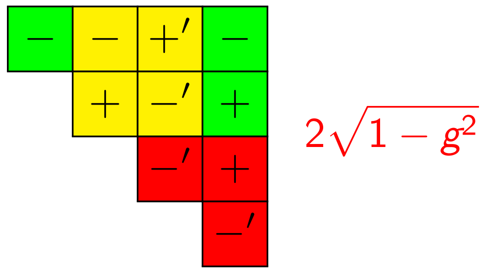
SECOND PROBLEM: Many of the moves detected in the real variables case are no longer available for the new factors.

E.g: no longer true that $\begin{array}{|c|c|}\hline + & -' \\ \hline\end{array} \leq \begin{array}{|c|c|}\hline - & +' \\ \hline\end{array}$ or $\begin{array}{|c|c|}\hline -' & + \\ \hline +' & - \\ \hline\end{array} \leq \begin{array}{|c|c|}\hline +' & - \\ \hline -' & + \\ \hline\end{array}$ but the move $\begin{array}{|c|}\hline -' \\ \hline +' \\ \hline\end{array} \leq \begin{array}{|c|}\hline +' \\ \hline -' \\ \hline\end{array}$ is still available.

The procedure for $n + 1 \in \{6, 7, 8, 9\}$

- For each of the 3 possible orderings (resp. 3, 4, 4) we consider the 16 (resp. 32, 64, 128) configurations available and the corresponding graphical schemes.
- Some of these schemes are estimated similarly to Pohst's procedure, by recognizing patterns.

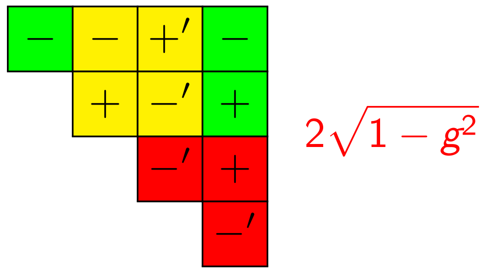
- For each of the 3 possible orderings (resp. 3, 4, 4) we consider the 16 (resp. 32, 64, 128) configurations available and the corresponding graphical schemes.
- Some of these schemes are estimated similarly to Pohst's procedure, by recognizing patterns.



Green ≤ 2, Red ≤ 5.2, Yellow $\leq 32/27$. Configuration ≤ 12.33.

The procedure for $n+1 \in \{6,7,8,9\}$

- For each of the 3 possible orderings (resp. 3, 4, 4) we consider the 16 (resp. 32, 64, 128) configurations available and the corresponding graphical schemes.
- Some of these schemes are estimated similarly to Pohst's procedure, by recognizing patterns.



Green ≤ 2, Red ≤ 5.2, Yellow $\leq 32/27$. Configuration ≤ 12.33.

- We now need more than 100 different patterns. Some are hard to estimate and need Elimination Theory.
- Other schemes are reduced to schemes we already bounded thanks to moves similar to those of the real variables case.

Results and consequences

Table of upper bounds for every configuration in every consiered case.

ordering \ $n+1$	5	6	7	8	9
1st	$16M$	32	$32M$	$64M$	155.1
2nd	$16M$	$32M$	$54M$	79.42	190.2
3rd		34.89	65.81	79.2	201.4
4th				80	233.1

Red values: sharp upper bound.
We conjecture an iterative behaviour similar to the one of the previous problem.
We conjecture the upper bound is independent of the ordering.

Results and consequences

Table of upper bounds for every configuration in every consiered case.

ordering \ $n+1$	5	6	7	8	9
1st	16M	32	32M	64M	155.1
2nd	16M	32M	54M	79.42	190.2
3rd		34.89	65.81	79.2	201.4
4th				80	233.1

Red values: sharp upper bound.
We conjecture an iterative behaviour similar to the one of the previous problem.
We conjecture the upper bound is independent of the ordering.

Corollary (B.-Molteni,2023)

The lists of fields with small regulator, $r = 1$ *and* $n + 1 \in \{5, 6, 7\}$ *are larger than the previously available lists.*

The list of four fields with $n + 1 = 8$, $r = 1$ *and smallest regulator is now available (previously unknown).*