Rational sums-of-squares lengths of biquadratic forms and orthogonal dilations

Carles Marín

Statements

Definition 1.1 4
Proposition 2.1 7
Definition 2.2 7
Proposition 2.3 8
Theorem 3.1 8
Proposition 3.2 9
Proposition 3.3 10
Theorem 4.1 11
Theorem 4.2 — Period eight 12
Proposition 4.3 12
Proposition 4.4 13
Proposition 4.5 14
Proposition 4.6 14
Theorem 5.1 15
Remark 5.2 — Why roots appear 16
Remark 5.3 16
Corollary 5.4 16
Theorem 5.5 17
Remark 5.6 17
Lemma 6.1 18
Theorem 6.2 18
Remark 6.3 19
Lemma 6.4 20
Proposition 6.5 20
Lemma 6.6 21
Theorem 6.7 22
Corollary 6.8 23
Theorem 6.9 23
Example 6.10 24
Proposition 6.11 24
Example 6.12 25
Remark 6.13 25
Lemma 6.14 25
Theorem 6.15 27
Example 6.16 29
Theorem 7.1 29
Proposition 7.2 — the case $q = e^{\perp}$ of Theorem 6.2 32
Example 7.3 33
Proposition 7.4 — after Bailey–Craigen 33
Theorem 8.1 34
Remark 8.2 35
Theorem 9.1 35
Remark 9.2 35
Example 9.3 — One variable y 36
Example 9.4 36
Proposition 9.5 37
Example 9.6 — Weights 37
Proposition 10.1 37
Example 10.2 38
Remark 10.3 38
Question 1 41
Question 2 41
Question 3 41
Question 4 41

At a glance

🚀 **Start here: Theorem 8.1**: integer length: degree at most two, and the exact count.

Main results:

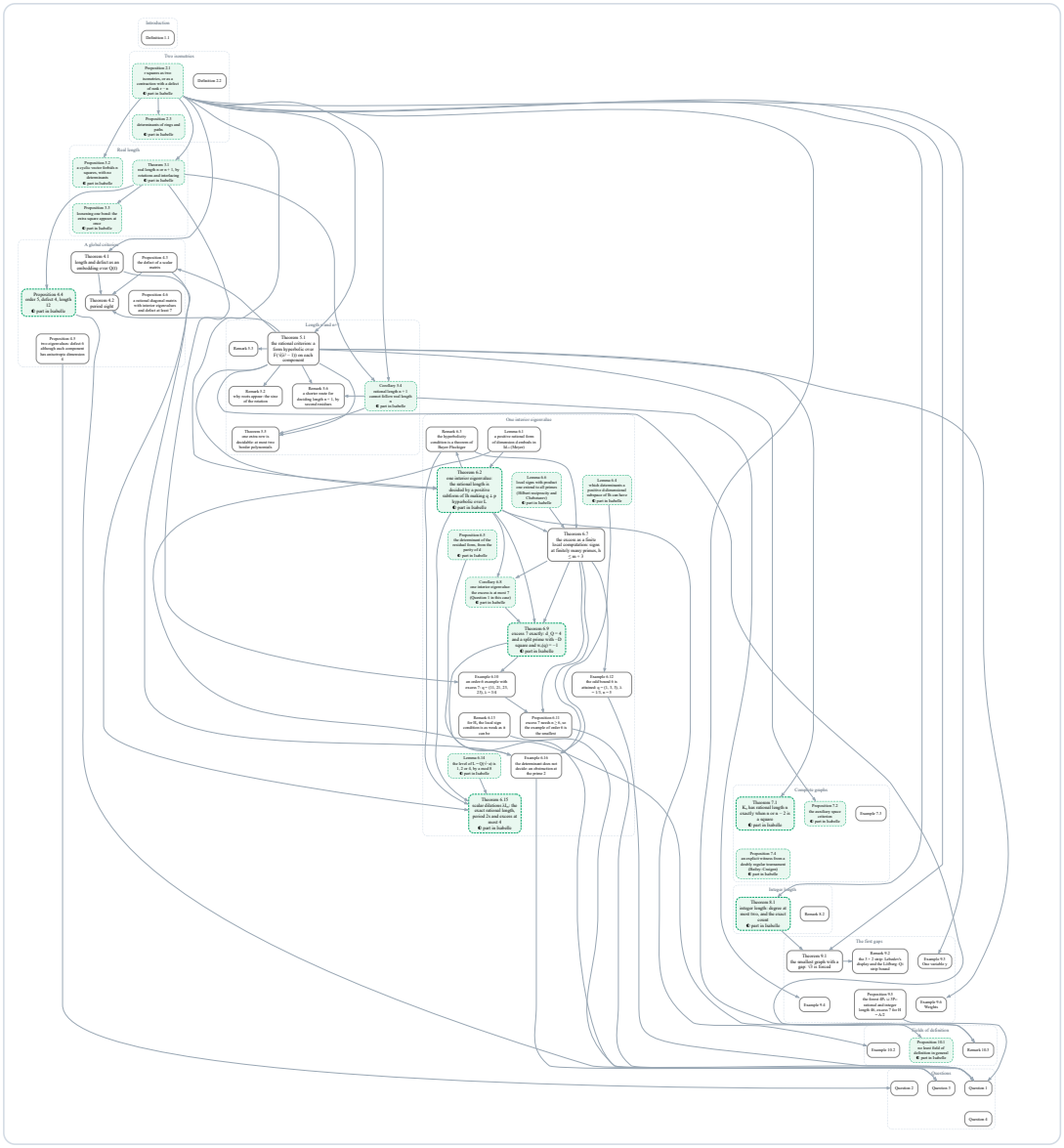
- **Theorem 4.1**: length and defect as an embedding over Q(t)
- **Theorem 4.2**: period eight
- **Proposition 4.4**: order 5, defect 4, length 12
- **Theorem 5.1**: the rational criterion: a form hyperbolic over $F(\sqrt{(\lambda^2 - 1)})$ on each component
- **Theorem 6.2**: one interior eigenvalue: the rational length is decided by a positive subform of Ih making $q \perp p$ hyperbolic over L
- **Theorem 6.7**: the excess as a finite local computation: signs at finitely many primes, $h \leq m + 3$
- **Theorem 6.9**: excess 7 exactly: $d_Q = 4$ and a split prime with $-D$ square and $w_v(q) = -1$
- **Theorem 6.15**: scalar dilations λI_m: the exact rational length, period 2s and excess at most 4
- **Theorem 7.1**: K_n has rational length n exactly when n or $n - 2$ is a square
- **Theorem 8.1**: integer length: degree at most two, and the exact count
- **Theorem 9.1**: the smallest graph with a gap: $\sqrt{3}$ is forced

54 results | ✅ **0** entirely in Lean | ◐ **20** partly in Lean | 💻 **0** checked by a program | written proof only

(a result can carry several tags)

🗺️ Map of the results (click a box to go to it)

Dependencies in the written proof: an arrow A → B means that this proof of B uses A. Every result rests on its written proof; the tags record what was checked besides, and each statement's "Evidence & scope" block says how far. The colour of a box is its strongest tag, in the order above; the tags in the box give the rest. Boxes with a thick border are the main results; click a box to read the statement.



📐 Setting (copied from the paper, §§1–2)

Let H be a real symmetric $n \times n$ matrix with spectrum in $[-1, 1]$, and

$$P_H(x, y) = (x_1^2 + x_2^2)\,|y|^2 + 2x_1x_2\,y^\top Hy, \qquad M(t) = (1 + t^2)I + 2tH.$$

For a subring $R \subseteq \mathbb{R}$, $\ell_R(H)$ is the least number of squares of bilinear forms with coefficients in R whose sum is P_H. For a graph G, $\ell_R(G) = \ell_R(\frac{1}{2}A_G)$. We write $H_n = (J - I)/(n - 1)$ and $\operatorname{sym} T = (T + T^\top)/2$.

Abstract.

For a rational symmetric matrix H of order n with spectrum in $[-1, 1]$, how many squares of rational bilinear forms are needed to write $P_H(x, y) = (x_1^2 + x_2^2)|y|^2 + 2x_1x_2\,y^\top Hy$? Over $\mathbb{R}$ the answer is n or $n + 1$ (Blekherman–Plaumann–Sinn–Vinzant, Hanselka–Sinn). Over $\mathbb{Q}$ it is the least dimension of a sum of squares carrying an orthogonal dilation of a contraction with symmetric part H, and the obstruction is arithmetic: a rotation with rational cosine λ has the real sine $\sqrt{1 - \lambda^2}$, and what decides is the imaginary quadratic field $\mathbb{Q}(\sqrt{\lambda^2 - 1})$ of its eigenvalues. For H with one interior eigenvalue we reduce the length to a positive complement inside a sum of squares and decide it by an exact finite local procedure; the excess over n is at most 7, and 7 is attained. Two consequences are explicit: $\ell_{\mathbb{Q}}(\lambda I_m)$ in closed form, governed by the number of rational squares needed for $1 - \lambda^2$, and the length of the normalized complete graphs $(J - I)/(n - 1)$ for every n, which for odd n is n, $n + 3$ or $n + 5$ according to squares and n modulo 8. We also give a criterion over $\mathbb{Q}(t)$, the integer length of every graph and the smallest graph with a gap between $\mathbb{R}$ and $\mathbb{Q}$.

Companion site.

https://karlesmarin.github.io/blueprints/real-rational-integer/: every statement with its dependencies, its formal proofs and checks, and labs in the browser. The small arrow in the left margin of each statement opens it there. This paper, its Spanish version, sources and scripts: doi:10.5281/zenodo.24387752.

[enhanced,breakable,before skip=8pt,after skip=4pt,colback=accent!4,colframe=accent!60,boxrule=0.6pt,arc=3pt,left=4pt,right=8pt,top=4pt,bottom=4pt,title=**Results at a glance**,coltitle=white,colbacktitle=accent!85,fonttitle=]

-
-
- **A global criterion over $\mathbb{Q}(t)$ and period** 8 (Theorems 4.1, 4.2). written proof
- **Length n and $n+1$** (Theorems 5.1, 5.5); the local form of the criterion is Bayer-Fluckiger's [4] , and Corollary 5.4 follows from Hanselka–Sinn [20] . written proof known, cited; parts formalised
- **One interior eigenvalue** (Section 6): reduction to an isometry problem with a positive complement in I_h (Theorem 6.2), an exact finite procedure (Theorem 6.7), and $\ell_{\mathbb{Q}}(\lambda I_m)$ in closed form (Theorem 6.15); the bound $\ell_{\mathbb{Q}}(H) - n \le 7$ is sharp, with an exact criterion in multiplicity 4 and a least example of order 6 (Theorem 6.9). written proof; parts formalised (Section 11); procedure and formula checked in 275 cases, the criterion tested against the procedure in 8008 cases (a test, not the proof) exact computation
- **Complete graphs $H_n = (J-I)/(n-1)$**: length and defect for every n (Theorem 7.1). written proof; witnesses $n \le 17$ exact computation; parts formalised
- **Integer length of every graph, and the smallest graph with a gap** (Theorems 8.1, 9.1). written proof; selected statements formalised (Section 11); exhaustive counts and the Gröbner computation exact computation

formalised Isabelle/HOL or Lean exact computation exact computation with failing controls written proof written proof in the text, not machine-checked known, cited known result, cited.

1 Introduction

Let H be a real symmetric $n \times n$ matrix with spectrum in $[-1, 1]$. The form

$$P_H(x, y) = (x_1^2 + x_2^2)\,|y|^2 + 2x_1x_2\,y^{\top}Hy \quad (1) \tag{1}$$

is nonnegative. If $H = \frac{1}{2}A$ with A the adjacency matrix of a graph, then H is, up to an affine change, the Hückel matrix of the graph. Since x has two variables, P_H is a sum of squares of bilinear forms, and Blekherman, Plaumann, Sinn and Vinzant [8] and Hanselka and Sinn [20] give the real length: at most $n+1$, and n exactly when $\det M(t)$ is a square, where $M(t) = (1+t^2)I + 2tH$.

We ask what happens to this length when the coefficients are restricted. Comparing degrees shows that a representation of $M(t) = P^{\top}P$ over $R[t]$ has P of degree at most one, so the length below is the length $\ell(M(t))$ of Fernando, Ruiz and Scheiderer [16] , whose theorem gives $\ell_{\mathbb{Q}}(H) \le 8n$. In another language, $\ell_K(H)$ is the least dimension of a standard space K^r carrying an orthogonal one-step dilation of a contraction T with $\operatorname{sym}T = H$. Over $\mathbb{R}$ a contraction T has a dilation of dimension $n + \operatorname{rank}(I - T^{\top}T)$ [23] . Over $\mathbb{Q}$ the ambient space must be a sum of unit squares, and this is where arithmetic enters.

Definition 1.1. p. 2

For a subring $R \subseteq \mathbb{R}$ with $2H$ over R, let $\ell_R(H) \in \mathbb{N} \cup \{\infty\}$ be the least r such that P_H is a sum of r squares of bilinear forms with coefficients in R. For a graph G write $\ell_R(G) = \ell_R(\frac{1}{2}A_G)$.

↳ Not used by another result of the paper.

The motivation is computational. In work on second order Zarankiewicz numbers [25] , Gram matrices of minimal rank kept appearing with entries in fields such as $\mathbb{Q}(\sqrt{3})$ and $\mathbb{Q}(\sqrt{2})$. This note studies the

arithmetic behind such fields in the simplest family, where x has two variables.

G	$\ell_{\mathbb{R}}$	$\ell_{\mathbb{Q}}$	$\ell_{\mathbb{Z}}$
cycle C_n, $n \geq 3$	n	n	n
path P_n, $n \geq 2$	$n+1$	$n+1$	$n+1$
$P_2 \sqcup K_1$	4	5	5
$P_2 \sqcup P_2$	4	6	6
$K_{1,4}$	6	6	∞
$C_4 \sqcup K_1$	6	6	6
H_5	5	8	–
H_7	7	12	–

Table 1: Lengths in small cases. Orange: a gap between $\mathbb{R}$ and $\mathbb{Q}$ for graphs. Green: a cospectral pair separated over $\mathbb{Z}$. The rows H_5, H_7 are the normalized complete graphs of Section 7, whose entries are not half-integers.

Colour: blue shade = the number's size within its column.

The picture. Over $\mathbb{R}$, the length is n when H is the symmetric part of an orthogonal matrix, which is a sum of plane rotations: an interior eigenvalue $\lambda = \cos\theta$ is the cosine of a rotation, whose sine $\sqrt{1-\lambda^2}$ always exists. Over $\mathbb{Q}$ the rotation of cosine λ lives on a rational plane only if the plane can carry its sine, a condition governed by the field $L = \mathbb{Q}(\sqrt{\lambda^2-1})$ of its eigenvalues $\lambda \pm \sqrt{\lambda^2-1}$; what is missing has to be completed by extra rational squares. For $H = \frac{3}{4} I_2$ the real length is 2, a rotation by $\cos\theta = \frac{3}{4}$, $\sin\theta = \frac{\sqrt{7}}{4}$. Over $\mathbb{Q}$ the sine is not available, 7 needs four rational squares, and the length is 6: with

$$A = \begin{pmatrix} I_2 \\ 0 \end{pmatrix}, \qquad B = \begin{pmatrix} \frac{3}{4} & 0 \\ 0 & \frac{3}{4} \\ \frac{1}{2} & -\frac{1}{4} \\ \frac{1}{4} & \frac{1}{2} \\ \frac{1}{4} & \frac{1}{4} \\ \frac{1}{4} & -\frac{1}{4} \end{pmatrix} \in \mathbb{Q}^{6\times 2},$$

one has $A^\top A = B^\top B = I$ and $A^\top B + B^\top A = 2H$, the last four rows of B being the first two columns of the left multiplication by the quaternion $\frac{1}{4}(2+i+j+k)$, of norm $\frac{7}{16}$; Theorem 6.15 shows that 6 is optimal.

Where the numbers come from. Four mechanisms account for every number in the paper.

1. *The sine.* A rotation of cosine λ exists on a rational plane exactly when the plane is $\langle a, a\delta\rangle$ with $\delta = 1-\lambda^2 = \sin^2\theta$, up to isometry: the plane must carry the sine. So length n means that each interior eigenspace splits into such planes, and this is a hyperbolicity condition over $L = \mathbb{Q}(\sqrt{\lambda^2-1})$ (Theorem 5.1).
2. *The complement.* When it fails, what is missing must be supplied inside a sum of squares: it is supplied by a positive rational form p that embeds in I_h, such that the eigenspace form together with p splits (Theorem 6.2); the number of extra squares is h, which need not equal $\dim p$. A positive rational form of dimension d needs at most $d+3$ squares, by the four-square theorem and Hasse–Minkowski (Lemma 6.1); this is the 3 in the bounds $\ell_{\mathbb{Q}} \leq n + d_{\mathbb{Q}} + 3$, and with $d_{\mathbb{Q}} \leq 4$ it gives the 7 of Corollary 6.8.
3. *The split primes.* Locally, the condition is felt only where L splits: there $L \otimes \mathbb{Q}_p = \mathbb{Q}_p \times \mathbb{Q}_p$, so splitting over L means splitting over $\mathbb{Q}_p$, and a local sign (a Hasse invariant) must match; at the other primes the local conditions can be met by choosing p (Theorem 6.7). This is why every failure of the determinant bound that we found comes from a split prime (Example 6.16).
4. *The level.* The least number s of squares with sum -1 in L is 1, 2 or 4, and I_{2s} is the first sum of squares that becomes hyperbolic over L; so $\langle 1\rangle$ has order $2s$ in the Witt group of L, and $2s$ divides 8, the period that holds for every such L. For $\lambda = \frac{3}{4}$, $L = \mathbb{Q}(\sqrt{-7})$ has $s = 4$, so I_8 is the first one: this is the 8 of the period (Theorem 4.2) and of the general bound $8n$ of [16] . The level is read off from

$\tau(\delta)$, the number of rational squares needed for $\sin^2\theta$ (Lemma 6.14), and this is the τ in the scalar formula.

For the complete graphs the only interior eigenvalue is $\lambda = -1/(n-1)$, with $\delta = n(n-2)/(n-1)^2$, so δ is $n(n-2)$ up to squares, and its eigenspace $\mathbf{1}^\perp \subseteq I_n$ has determinant n; this is why squares among n and $n-2$, and the residues of n modulo 8, decide $\ell_{\mathbb{Q}}(H_n)$.

The main question. Fernando, Ruiz and Scheiderer give $\ell_{\mathbb{Q}}(H) \le 8n$, which allows an excess $\ell_{\mathbb{Q}}(H) - n$ of order $7n$. Is the excess bounded independently of H? This is Question 1 of Section 12. We answer it for one interior eigenvalue: the bound is 7, and it is attained (Corollary 6.8, Theorem 6.9). In general it is open.

Main results. The core of the paper is Section 6, items 2 and 3 below, and the complete graphs, item 4; item 1 is the general frame.

1. A criterion for length and defect by an embedding over $\mathbb{Q}(t)$ (Theorem 4.1), period 8 (Theorem 4.2), and a decision procedure for $\ell_{\mathbb{Q}} \le n+1$ (Theorem 5.5).
2. For every H with one interior eigenvalue, the reduction of the length to a positive complement inside a sum of squares (Theorem 6.2), an exact finite local procedure (Theorem 6.7) and the bound $\ell_{\mathbb{Q}}(H) - n \le 7$ (Corollary 6.8), attained by an explicit 6×6 matrix, the least order possible, with an exact local criterion in multiplicity 4 (Theorem 6.9).
3. For scalar matrices, $\ell_{\mathbb{Q}}(\lambda I_m)$ in closed form, decided by $\tau(1-\lambda^2)$ through the level of L (Theorem 6.15).
4. For the normalized complete graphs, length and defect for every n (Theorem 7.1).

We also give the integer length of every graph (Theorem 8.1), the smallest graph with a gap between $\mathbb{R}$ and $\mathbb{Q}$ (Theorem 9.1), a matrix of order 5 with excess 7 (Proposition 4.4), components that interact and a defect of 7 (Propositions 4.5, 4.6), and fields of definition (Section 10). Sums of squares with more variables x are treated in a separate note.

What is known and what is new. We have tried to credit everything that is not ours.

- The real length is due to Blekherman, Plaumann, Sinn and Vinzant [8] and Hanselka and Sinn [20] ; Corollary 5.4 is a short consequence of [20 , Lemma 4.3, Corollaries 2.7 and 4.5] and Witt cancellation.
- The criterion for length n (Theorem 5.1) is close to the classical theory of isometries and hermitian forms: Milnor [31] , Milnor–Husemoller [29 , Appendix 2] , Lewis [24] , and Bayer-Fluckiger [4 , Theorem 9.1, Corollary 9.2] , whose criterion is also the input of Section 6; what is ours there is the constraint that the complement lies in a sum of squares, the finite procedure and the bound.
- In Theorem 6.15, the case $2s \mid m$ is a special case of Fernando–Ruiz–Scheiderer [16 , Proposition 1.7] , and $m = 1$ is elementary, in the spirit of Pourchet [27] ; we have not found the general formula.
- For Theorem 7.1, the case where $n-2$ is a square is the construction of Bailey and Craigen from doubly regular tournaments [1 , Theorem 4.2] ; ± 1 matrices of this shape are conference matrices [19 , 14] , rational orthogonal matrices with zero pattern $J - I$ appear in [13 , Proposition 12] , and regular rational orthogonal matrices are parametrized in [36 , Theorem 4] . None of these determines when a rational orthogonal matrix, of size n or larger, has symmetric part $(J-I)/(n-1)$.
- Theorem 8.1 follows from the coefficient comparison of Yiu [38 , § 1] ; the four real squares of Theorem 9.1 are known (Remark 9.2).
- The context is the line of Bender [7] , Bass–Estes–Guralnick [2] , Friedland [17] and Bayer-Fluckiger–Berhuy–Chuard-Koulmann [3] on rational symmetric and orthogonal matrices; over $\mathbb{C}$, de la Cruz and Paras [12] describe $X + X^\top$ with X orthogonal.

Bass–Estes–Guralnick [2] , which we read in full, study the least size of a symmetric matrix with a given eigenvalue with the same device of forms represented by sums of squares; Lemma 6.1 is the case $A = \mathbb{Q}$ of their Lemma 8.1 (with $u(\mathbb{Q}) = 4$ in their notation: a positive diagonal form of dimension 4 over $\mathbb{Q}$ represents every positive rational), and they do not consider the length of P_H or orthogonal dilations. We could not consult Pfister's and Cassels' books on multiples of forms, nor Friedland [17] in full; by its review, Friedland gives a criterion for rational orthogonal similarity of rational symmetric matrices, a different question. Not having found a result is not a proof of novelty.

2 Two isometries

Proposition 2.1. p. 5

black!35↗

Huckel_SOS.represents_iff Let $K \subseteq \mathbb{R}$ be a field, H symmetric over K of size $n \geq 1$, and $r \geq n$. The following are equivalent:

1. *$\ell_K(H) \leq r$;*
2. *there are $A, B \in K^{r\times n}$ with $A^\top A = B^\top B = I$ and $A^\top B + B^\top A = 2H$;*
3. *there is $T \in K^{n\times n}$ with $\mathrm{sym}T = H$ such that $I - T^\top T = D^\top D$ for some $D \in K^{(r-n)\times n}$.*

In particular $\ell_K(H) = n$ if and only if $H = \mathrm{sym}T$ with $T \in O_n(K)$.

Isabelle · ours · part **show**

Only a part is in Isabelle: partly: (1) ⇔ (2) over the reals (represents_iff); the rational case and (3) use Witt cancellation and are not formalized

`represents_iff` · `Isabelle/AFP/Biquadratic_SOS_Length/Huckel_SOS.thy`, line 85 — (1) ⇔ (2) over the reals

```
theorem represents_iff:
  fixes A B :: "real^'n^'r" and H :: "real^'n^'n"
  assumes symH: "sym_mat H"
  shows "represents A B H \<longleftrightarrow>
    transpose A ** A = mat 1 \<and> transpose B ** B = mat 1 \<and>
    transpose A ** B + transpose B ** A = H + H"
```

`represents_iff` · `Isabelle/AFP/Biquadratic_SOS_Length/Huckel_SOS.thy`, line 85

```
theorem represents_iff:
  fixes A B :: "real^'n^'r" and H :: "real^'n^'n"
  assumes symH: "sym_mat H"
  shows "represents A B H \<longleftrightarrow>
    transpose A ** A = mat 1 \<and> transpose B ** B = mat 1 \<and>
    transpose A ** B + transpose B ** A = H + H"
```

Trust base: 🔒 kernel only — **only part of the statement is formal** (see the box). Isabelle: 2 results, no oracles

Proof: in this note · **Formalized:** Isabelle/HOL, by the author (public formalizations repository) · **Covers:** part: (1) ⇔ (2) over the reals (represents_iff); the rational case and (3) use Witt cancellation and are not formalized · **Cite:** Proposition 2.1, p. 5, doi:10.5281/zenodo.24387751

↳ Used in: Proposition 2.3 (p. 8), Theorem 3.1 (p. 8), Proposition 3.2 (p. 9), Theorem 4.1 (p. 11), Theorem 5.1 (p. 15), Corollary 5.4 (p. 16), Theorem 6.2 (p. 18), Theorem 8.1 (p. 34), Theorem 9.1 (p. 35), 9.3 (p. 36), Proposition 10.1 (p. 37)

Proof

A sum of r squares is $|x_1Ay + x_2By|^2$, and comparing coefficients in (1) gives (2). Given (2), the space K^r with the standard form is the orthogonal sum of $A(K^n) \cong n\langle 1\rangle$ and a complement which, by Witt cancellation, is isometric to $(r-n)\langle 1\rangle$. So we may take $A = \binom{I}{0}$ and $B = \binom{T}{D}$. The converse is the same computation.

Definition 2.2. p. 5

The *defect* $d_K(H)$ is the least rank of $I - T^\top T$ over $T \in K^{n\times n}$ with $\mathrm{sym}T = H$ and $T^\top T \leq I$.

↳ Not used by another result of the paper.

The matrix $\mathcal{G} = \left(\begin{smallmatrix} I & T \\ T^\top & I \end{smallmatrix}\right)$ is a Gram matrix of P_H on the products x_iy_j, and its rank is $n + \mathrm{rank}(I - T^\top T)$ by the Schur complement. So $n + d_{\mathbb{Q}}(H)$ is the least rank of a rational positive semidefinite Gram matrix, and $d_{\mathbb{Q}}(H) \leq \ell_{\mathbb{Q}}(H) - n$. Over $\mathbb{R}$ the two agree. Over $\mathbb{Q}$ they do not, because a rational form of rank d need not be a sum of d rational squares.

Proposition 2.3. p. 5

black!35↗

Huckel_SOS.det_pencil_square With $M(t) = (1+t^2)I + 2tH$: the cycle, $n \geq 3$, gives $\det M = (1-(-t)^n)^2$; the cycle with one negative bond gives $(1+(-t)^n)^2$; the path gives $1 + t^2 + \cdots + t^{2n}$, which is not a square for $n \geq 1$.

Isabelle · ours · part **show**

Only a part is in Isabelle: the named pieces are machine-checked; the statement as a whole is not marked as formalized in the paper

`det_pencil_square` · `Isabelle/AFP/Biquadratic_SOS_Length/Huckel_SOS.thy`, line 196

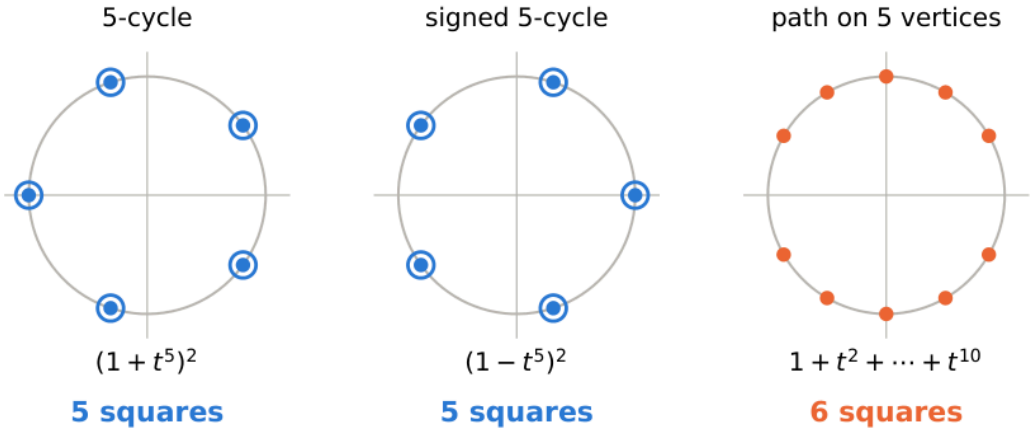
```
theorem det_pencil_square:
  fixes A B H :: "real^'n^'n"
  assumes sym: "sym_mat H" and r: "represents A B H"
  shows "\<exists>p :: real poly. \<forall>t. Determinants.det (pencil H t) = (poly p
t)\<^sup>2"
```

↳ Not used by another result of the paper.

Proof

For the cycle, $M = (I+tQ)^\top(I+tQ)$ with Q the cyclic shift, and $\det(I+tQ) = \prod_{\zeta^n=1}(1+t\zeta)$; the negative bond gives $Q^n = -I$. For the path the levels are $\cos(j\pi/(n+1))$, so the factors $(t+\omega^j)(t+\omega^{-j})$, with $\omega = e^{i\pi/(n+1)}$, run over the $(2n+2)$-th roots of unity except ± 1. If the result were p^2, then p would divide $G = t^{2n+2} - 1$ and G', hence the nonzero constant $tG' - (2n+2)G$.

Figure 1



Roots of $\det M(t)$. Double in both closed rings, simple on the path. Try your own graph in the lab.

3 Real length

Theorem 3.1. p. 6

black!35↗

Huckel_SOS.blocks_orthogonal, Huckel_SOS.blocks_symmetric_part Let H have spectrum in $[-1,1]$.

1. *$\ell_{\mathbb{R}}(H) = n$ if every eigenvalue in $(-1,1)$ has even multiplicity, and $\ell_{\mathbb{R}}(H) = n+1$ otherwise.*

2. *Let $Q \in O_{n+1}(\mathbb{R})$ with $\mathrm{sym}Q = \left(\begin{smallmatrix} H & b \\ b^\top & c \end{smallmatrix}\right)$, and let $\lambda \in (-1,1)$ have even multiplicity m in H. Then b is orthogonal to the eigenspace E_λ, and Q preserves it.*

Isabelle · ours · part **show**

Only a part is in Isabelle: the named pieces are machine-checked; the statement as a whole is not marked as formalized in the paper

`blocks_orthogonal` · `Isabelle/AFP/Biquadratic_SOS_Length/Huckel_SOS.thy`, line 836

```
lemma blocks_orthogonal:
  fixes d s :: "'n::finite \<Rightarrow> real" and \<sigma> :: "'n \<Rightarrow> 'n"
  assumes inv: "\<And>i. \<sigma> (\<sigma> i) = i"
    and dsig: "\<And>i. d (\<sigma> i) = d i"
    and ssig: "\<And>i. \<sigma> i \<noteq> i \<Longrightarrow> s (\<sigma> i) = - s i"
    and sfix: "\<And>i. \<sigma> i = i \<Longrightarrow> s i = 0"
    and norm: "\<And>i. (d i)\<^sup>2 + (s i)\<^sup>2 = 1"
  shows "transpose (blocks d s \<sigma>) ** blocks d s \<sigma> = mat 1"
```

`blocks_symmetric_part` · `Isabelle/AFP/Biquadratic_SOS_Length/Huckel_SOS.thy`, line 933

```
lemma blocks_symmetric_part:
  fixes d s :: "'n::finite \<Rightarrow> real" and \<sigma> :: "'n \<Rightarrow> 'n"
  assumes inv: "\<And>i. \<sigma> (\<sigma> i) = i"
    and ssig: "\<And>i. \<sigma> i \<noteq> i \<Longrightarrow> s (\<sigma> i) = - s i"
    and sfix: "\<And>i. \<sigma> i = i \<Longrightarrow> s i = 0"
  shows "blocks d s \<sigma> + transpose (blocks d s \<sigma>) =
    (\<chi> i j. kron i j * d j) + (\<chi> i j. kron i j * d j)"
```

🆕 **Classical and new:** the length is due to Blekherman–Plaumann–Sinn–Vinzant and Hanselka–Sinn; the proof and the splitting are ours

↳ Used in: Proposition 3.3 (p. 10), Proposition 4.4 (p. 13), Corollary 5.4 (p. 16), 6.10 (p. 24)

Proof

A real orthogonal matrix is a sum of plane rotations and ± 1, and a rotation of angle θ gives $\cos\theta$ twice in $\mathrm{sym}Q$. With Proposition 2.1, $r = n$ forces parity, and conversely a parity spectrum is realized by rotation blocks.

Remove the even part and ± 1. There remain simple interior values $\lambda_1 > \cdots > \lambda_s$. If s is odd take $\mu = (\lambda_1, \lambda_1, \lambda_3, \lambda_3, \ldots, \lambda_s, \lambda_s)$, and if s is even take $\mu = (1, \lambda_2, \lambda_2, \lambda_4, \lambda_4, \ldots, \lambda_s, \lambda_s)$. These $s+1$ values interlace the λ_i, $\mu_1 \geq \lambda_1 \geq \mu_2 \geq \cdots \geq \lambda_s \geq \mu_{s+1}$, so by Fan–Pall [15] there is a symmetric matrix with spectrum μ containing $\mathrm{diag}(\lambda_i)$ as a principal block. Explicitly, the bordered matrix $S = \left(\begin{smallmatrix} \mathrm{diag}(\lambda) & b \\ b^\top & c \end{smallmatrix}\right)$ has $\det(x - S) = (x-c)\prod_k (x-\lambda_k) - \sum_i b_i^2 \prod_{k \neq i}(x-\lambda_k)$, so it suffices to take $c = \sum \mu_j - \sum \lambda_i$ and $b_i^2 = -\prod_j (\lambda_i - \mu_j) / \prod_{k \neq i}(\lambda_i - \lambda_k)$, which is ≥ 0 by interlacing, with equality exactly when λ_i is one of the μ_j. The interior eigenvalues of S are paired and the remaining one, if any, is 1, so $S = \mathrm{sym}Q$ for an orthogonal Q of order $s+1$ made of rotation blocks in an eigenbasis of S; the direct sum with the removed part gives sym of an orthogonal matrix of order $n+1$.

For (2): if $b \not\perp E_\lambda$ then λ has multiplicity exactly $m-1$ in $\mathrm{sym}Q$, which is odd. So $b \perp E_\lambda$; the multiplicity is then m, as $m+1$ is also odd, and E_λ is an eigenspace of $\mathrm{sym}Q$, with which Q commutes.

Proposition 3.2. p. 6

black!35↗

Huckel_SOS.chain_needs_more_than_n_squares, Huckel_SOS.geometric_not_square If $H = \mathrm{sym}T$ with T orthogonal and H has a cyclic vector, then $H^2 = I$. In particular no path on $n \geq 2$ vertices has $\ell_{\mathbb{R}} = n$.

Isabelle · ours · part **show**

Only a part is in Isabelle: the named pieces are machine-checked; the statement as a whole is not marked as formalized in the paper

chain_needs_more_than_n_squares ·
Isabelle/AFP/Biquadratic_SOS_Length/Huckel_SOS.thy, line 546

```
theorem chain_needs_more_than_n_squares:
  fixes A B H :: "real^'n^'n" and v :: "nat \<Rightarrow> real^'n"
  assumes symH: "sym_mat H" and n: "2 \<le> n"
    and orth: "\<And>i j. i < n \<Longrightarrow> j < n \<Longrightarrow> v i \<bullet>
v j = (if i = j then 1 else 0)"
    and sp: "span (v ` {..<n}) = UNIV"
    and first: "(H + H) *v v 0 = v 1"
    and mid: "\<And>i. 0 < i \<Longrightarrow> i + 1 < n \<Longrightarrow> (H + H) *v v
i = v (i - 1) + v (i + 1)"
    and last: "(H + H) *v v (n - 1) = v (n - 2)"
  shows "\<not> represents A B H"
```

geometric_not_square ·
Isabelle/AFP/Biquadratic_SOS_Length/Huckel_SOS.thy, line 290

```
theorem geometric_not_square:
  fixes p :: "real poly"
  assumes n: "0 < n"
  shows "(\<Sum>j\<le>n. [:0, 0, 1:] ^ j) \<noteq> p\<^sup>2"
```

↳ Not used by another result of the paper.

Proof

Let $S = T - T^\top$. As $TT^\top = T^\top T = I$, S commutes with H. Then $\langle H^a e, SH^b e\rangle = \langle H^{a+b} e, Se\rangle$ is symmetric in a, b, while S is skew. So it vanishes, $S = 0$, $T = H$ and $H^2 = I$. On a path the first coordinate vector is cyclic, by the tridiagonal recurrence, and $H^2 \neq I$ for $n \geq 2$.

Proposition 3.3. p. 7

black!35↗

Huckel_SOS.weighted_ring_identity Let S_a be the shift with $S_a e_n = a e_1$ and $H_a = \mathrm{sym} S_a$, $|a| \leq 1$. Then $M_a = (I + tS_a)^\top (I + tS_a) + (1 - a^2) t^2 e_n e_n^\top$, and $\ell_{\mathbb{R}}(H_a) = n + 1$ for $|a| < 1$, $n \geq 3$, while $\ell_{\mathbb{R}}(H_{\pm 1}) = n$.

Isabelle · ours · part **show**

Only a part is in Isabelle: the named pieces are machine-checked; the statement as a whole is not marked as formalized in the paper

weighted_ring_identity ·
Isabelle/AFP/Biquadratic_SOS_Length/Huckel_SOS.thy, line 368

```
lemma weighted_ring_identity:
  fixes y :: "nat \<Rightarrow> real"
  assumes a: "\<bar>a\<bar> \<le> 1"
  shows "(x1 * y 0 + x2 * a * y (Suc m))\<^sup>2 + (\<Sum>i\<le>m. (x1 * y (Suc i) + x2
* y i)\<^sup>2)
     + (sqrt (1 - a\<^sup>2) * x2 * y (Suc m))\<^sup>2 =
    (x1\<^sup>2 + x2\<^sup>2) * (\<Sum>i\<le>Suc m. (y i)\<^sup>2)
      + 2 * x1 * x2 * (a * y 0 * y (Suc m) + (\<Sum>i\<le>m. y i * y (Suc i)))"
```

↳ Not used by another result of the paper.

Proof

The identity is a direct expansion. Let $|a| < 1$. A value ± 1 would force $S_a v = \pm v$, against $S_a^n = aI$. A double value would have an eigenvector with $v_1 = 0$, whose remaining coordinates form an eigenvector of a path on $n - 1$ vertices, with end entries nonzero and equal in modulus; the equation at site 1 reads $v_2 + a v_n = 0$, so $|a| = 1$. Now apply Theorem 3.1.

4 A global criterion

Let $F = \mathbb{Q}(t)$, $M_H = (1+t^2)I + 2tH$, and write $I_j = j\langle 1\rangle$. Note that T need not commute with H: for $T = H + S$ with S skew, $I - T^\top T = I - H^2 + S^2 + SH - HS$, and the last term mixes eigenspaces. So positive defect is a global problem.

Theorem 4.1. p. 7

black!35↗

Let H be rational symmetric with spectrum in $[-1,1]$, and p a positive definite rational form, possibly zero. The following are equivalent:

1. *there is a rational contraction T with $\mathrm{sym}T = H$ whose nondegenerate defect form embeds in p;*
2. *$(M_H)_F$ embeds in $(I_n \perp p)_F$.*

In particular $\ell_{\mathbb{Q}}(H) = \min\{r : (M_H)_F \hookrightarrow (I_r)_F\}$, and $d_{\mathbb{Q}}(H)$ is the least dimension of a positive p satisfying (2).

Classical and new: applies the Harder and Gerstein lattice argument to the normalized pencil

↳ Used in: Theorem 4.2 (p. 12), Proposition 4.4 (p. 13), 6.16 (p. 29)

Proof

Let $Q_0 = I_n \perp p$, of dimension N, write $R = \mathbb{Q}[t]$ and let $\Lambda_0 = R^N$ be its constant lattice, which is unimodular. A lattice is a finitely generated R-submodule of F^N of rank N, and it is integral if the form takes values in R on it. Suppose $v_1, \dots, v_n \in F^N$ have Gram matrix M_H.

Step 1: a maximal lattice. Since $\det M_H \neq 0$, the v_i span a nondegenerate subspace; adding a basis of its orthogonal complement, scaled to make the Gram matrix polynomial, gives an integral lattice $N_0 \ni v_1, \dots, v_n$. Its dual $N_0^{\#} = \{x \in F^N : Q_0(x, N_0) \subseteq R\}$ is again a lattice, since the Gram matrix of N_0 is invertible over F. An integral lattice $L \supseteq N_0$ satisfies $L \subseteq L^{\#} \subseteq N_0^{\#}$, so the integral lattices containing N_0 are submodules of the finitely generated module $N_0^{\#}$ over the noetherian ring R, and every ascending chain of them stabilizes: there is a maximal integral lattice $L \supseteq N_0$.

Step 2: its local shape. Let π be a prime of R, $k_\pi = R/\pi$ and L_π the completion of L over the completed ring $\hat{R}_\pi$. As 2 is a unit, L_π has an orthogonal basis; grouping its vectors by the valuation of their norms, $L_\pi = U \perp \pi V \perp W'$, where U and V are unimodular, πV denotes V with its form multiplied by π, and every basis vector of W' has norm of valuation at least 2. An integral lattice can be changed at one prime and kept at the others: if $L'' \supsetneq L_\pi$ is an integral $\hat{R}_\pi$-lattice with $L'' \subseteq \pi^{-k} L_\pi$, then, viewing $\pi^{-k}L$ inside F_π^N, $L' = \pi^{-k}L \cap L''$ is an R-lattice with $L'_\pi = L''$ and $L'_\rho = L_\rho$ for $\rho \neq \pi$, as π is a unit at ρ; it is integral because integrality is checked prime by prime, $R = \bigcap_\rho R_{(\rho)}$. (This is the usual local–global correspondence for lattices over a Dedekind domain [26] ; L' is a global lattice by construction, not merely a completed one.) So maximality of L gives maximality of L_π. If $W' \neq 0$, a basis vector e of W' can be replaced by e/π, whose norm still lies in $\hat{R}_\pi$ and which is orthogonal to the other basis vectors; the new lattice is integral and strictly larger, so $W' = 0$. If $\bar{V}$ is isotropic, take $v \in V$ primitive with $b_V(v,v) \in \pi\hat{R}_\pi$, where b_V is the unimodular form of V, so that the vector $x = v$ of the summand πV has norm $\pi b_V(v,v) \in \pi^2 \hat{R}_\pi$. Then x/π has norm $b_V(v,v)/\pi \in \hat{R}_\pi$, it is orthogonal to U, and its product with $w \in \pi V$ is $b_V(v,w) \in \hat{R}_\pi$. So $L_\pi + \hat{R}_\pi\, x/\pi$ is integral, and strictly larger since v is primitive. So $\bar{V}$ is anisotropic.

Step 3: $V = 0$. By Springer's theorem over the complete field F_π [21 , Ch. VI] , the second residue of $L_\pi \otimes F_\pi$ is the class $[\bar{V}] \in W(k_\pi)$, and it depends only on the space. The same space contains the unimodular lattice Λ_0, whose second residue is 0. So $[\bar{V}] = 0$, and since $\bar{V}$ is anisotropic, $\bar{V} = 0$: an anisotropic form with zero Witt class has dimension zero. Hence

$V = 0$ and L is unimodular at every prime, that is, unimodular over R. (Metabolic residues cannot occur, because maximality has already made $\bar{V}$ anisotropic.)

Step 4: L is constant. We use the theorem of Harder and Djoković in the form [16 , Theorem 1.11] : every symmetric matrix in $\mathrm{GL}_N(\mathbb{Q}[t])$ is congruent over $\mathbb{Q}[t]$ to a matrix with rational entries. By Step 3 the Gram matrix of L in any R-basis (one exists, as R is a principal ideal domain) is symmetric with determinant a unit of R, that is, it lies in $\mathrm{GL}_N(R)$. So L has an R-basis with constant Gram matrix Q_1. The constant forms Q_0, Q_1 are isometric over F; specializing an isometry at a rational t_0 where it and its inverse are defined shows $Q_1 \cong Q_0$ over $\mathbb{Q}$. Composing, there is an isometry φ of $(Q_0)_F$ with $\varphi(L) = \Lambda_0$, and the vectors $\varphi(v_i)$ are polynomial.

Step 5: degree one. In a rational basis diagonalizing Q_0 with positive coefficients c_k, the norm $\sum_k c_k w_k(t)^2$ of a polynomial vector $w \neq 0$ has degree $2 \max_k \deg w_k$, since the leading terms cannot cancel. The diagonal of M_H has degree two, so the matrix of the $\varphi(v_i)$ is $A_0 + tB_0$, and comparing coefficients in $(1+t^2)I + 2tH$ gives $A_0^* A_0 = B_0^* B_0 = I$ and $A_0^* B_0 + B_0^* A_0 = 2H$, with * the adjoint for Q_0. By Witt's theorem A_0 may be taken to be the inclusion of I_n; then $B_0 = \binom{T}{D}$ with $\mathrm{sym} T = H$ and $I - T^\top T = D^* D$, whose nondegenerate part is the restriction of p to the image of D, so it embeds in p. This is (1). Conversely, given (1), an embedding of the defect form in p gives D with $D^* D = I - T^\top T$, and the columns of $\binom{I}{0} + t\binom{T}{D}$ have Gram matrix M_H. For the length take $p = I_{r-n}$: a polynomial matrix of degree one with Gram matrix M_H in I_r is a representation of P_H by r squares.

In plain words (commentary, not part of the paper)

Asking for rational squares of bilinear forms looks like a problem about two matrices. It is really one embedding of quadratic forms over the field of rational functions: the pencil $M_H(t)$ must fit inside a sum of unit squares. A rational embedding can have denominators, but a lattice argument clears all of them at once.

Theorem 4.2. (Period eight) p. 8

black!35↗

For rational symmetric H, K with spectrum in $[-1, 1]$, with H of order n,

$$\ell_{\mathbb{Q}}(H^{\oplus 8} \oplus K) = 8n + \ell_{\mathbb{Q}}(K), \qquad d_{\mathbb{Q}}(H^{\oplus 8} \oplus K) = d_{\mathbb{Q}}(K).$$

Eight is the least integer with this property for all H.

Classical and new: not found in the literature so far; not a proof of novelty

↳ Not used by another result of the paper.

Proof

In a totally imaginary number field L, I_5 is isotropic by Hasse–Minkowski, so -1 is a sum of four squares, and a quaternion of norm -1 gives $I_4 \cong -I_4$. Thus I_8 is hyperbolic over each L_p , and Theorem 5.1 below gives $\ell_{\mathbb{Q}}(H^{\oplus 8}) = 8n$. So there is $T \in O_{8n}(\mathbb{Q})$ with $\mathrm{sym} T = H^{\oplus 8}$, whence $M_{H^{\oplus 8}} = (I+tT)^\top (I+tT) \cong (I_{8n})_F$. Witt cancellation and Theorem 4.1 give both equalities. For minimality take $H = (\frac{3}{4})$ and $L = \mathbb{Q}(\sqrt{-7})$. Here $[I_8]_L = 0$ and $[I_4]_L \neq 0$, so $\langle 1 \rangle$ has order exactly 8 in $W(L)$, and by Proposition 4.3 $d_{\mathbb{Q}}(H^{\oplus e}) = 0$ only for $8 \mid e$. So every universal period is a multiple of 8.

In plain words (commentary, not part of the paper)

Eight copies of a block cost nothing extra: they are always a rational rotation. The reason is that -1 is a sum of four squares in every totally imaginary number field. So repeating a block never makes the excess grow.

Proposition 4.3. p. 8

black!35↗

For $\lambda \in (-1, 1)$ rational and $L = \mathbb{Q}(\sqrt{\lambda^2 - 1})$, $d_{\mathbb{Q}}(\lambda I_n)$ is the dimension of the anisotropic part of $(I_n)_L$. For instance $d_{\mathbb{Q}}(\frac{3}{4} I_4) = 4$.

↳ Used in: Theorem 4.2 (p. 12), Theorem 6.15 (p. 27)

Proof

Here $T = \lambda + S$ commutes with H, and with $\delta = 1 - \lambda^2$, $\Delta = \delta + S^2$ we have $\mathbb{Q}^n = \ker \Delta \perp W$. The kernel is a sum of planes $\langle a, a\delta \rangle$, hyperbolic over L, so $\dim W$ is at least the anisotropic dimension. Conversely, extract such planes until the rest is anisotropic, and take $S = 0$ on the rest. Finally, for $\lambda = \frac{3}{4}$, $L = \mathbb{Q}(\sqrt{-7})$ has a place over 2 with completion $\mathbb{Q}_2$, where I_4 is anisotropic: no primitive solution exists modulo 8.

Proposition 4.4. p. 9

black!35↗

Rational_Gap.witness_G For $G = \mathrm{diag}(\frac{1}{4}, \frac{1}{4}, \frac{1}{4}, \frac{1}{4}, -\frac{1}{2})$*:* $\ell_{\mathbb{R}}(G) = 6$*,* $d_{\mathbb{Q}}(G) = 4$ *and* $\ell_{\mathbb{Q}}(G) = 12$*.*

Isabelle · ours · part **show**

Only a part is in Isabelle: the named pieces are machine-checked; the statement as a whole is not marked as formalized in the paper

`witness_G` · `Isabelle/RationalGap/Rational_Gap.thy`, line 24

```
lemma witness_G:
  fixes x1 x2 y1 y2 y3 y4 y5 :: rat
  shows
    "(x1 * y1 + x2 * (y1 / 4))^2 + (x1 * y2 + x2 * (y2 / 4))^2 +
     (x1 * y3 + x2 * (y3 / 4))^2 + (x1 * y4 + x2 * (y4 / 4))^2 +
     (x1 * y5 - x2 * (y5 / 2))^2 +
     (x2 * ((3/4) * y1 - (1/2) * y2 - (1/4) * y3 - (1/4) * y4))^2 +
     (x2 * ((3/4) * y2 + (1/2) * y1 + (1/4) * y4 - (1/4) * y3))^2 +
     (x2 * ((3/4) * y3 - (1/2) * y4 + (1/4) * y1 + (1/4) * y2))^2 +
     (x2 * ((3/4) * y4 + (1/2) * y3 - (1/4) * y2 + (1/4) * y1))^2 +
     (x2 * (y5 / 2))^2 + (x2 * (y5 / 2))^2 + (x2 * (y5 / 2))^2 =
     (x1^2 + x2^2) * (y1^2 + y2^2 + y3^2 + y4^2 + y5^2) +
       2 * x1 * x2 * ((1/4) * y1^2 + (1/4) * y2^2 + (1/4) * y3^2 + (1/4) * y4^2 - (1/2)
* y5^2)"
```

Classical and new: not found in the literature so far; not a proof of novelty

↳ Used in: 1 (p. 41)

Proof

The real length follows from Theorem 3.1. For the upper bounds, $T = G$ has defect $\frac{15}{16} I_4 \perp \langle \frac{3}{4} \rangle$, and $\frac{15}{16} I_4 \cong I_4$ by a quaternion of norm $\frac{15}{16}$, while $\frac{3}{4}$ is a sum of three squares. So $\ell_{\mathbb{Q}} \le 5 + 4 + 3$. For the defect take

$$T = G + \begin{pmatrix} 0 & v \\ -v^{\top} & 0 \end{pmatrix}, \qquad v = \tfrac{1}{4}(1, 1, 2, 0)^{\top}.$$

Since $\|v\|^2 = \frac{3}{8} = (1 - \frac{1}{4})(1 - \frac{1}{2})$, a computation gives that $I - T^{\top}T$ has spectrum $\{0, (\frac{15}{16})^{[4]}\}$, so T is a contraction of defect 4.

For the lower bounds let $a = t^2 + \frac{t}{2} + 1$ and $b = t^2 - t + 1$, so $M_G = aI_4 \perp \langle b \rangle$. Since 3 is a root of $u^2 + u + 4$ modulo 8 with odd derivative, Hensel gives a root $u \in \mathbb{Z}_2$ with $u \equiv 3 \pmod 8$. Put $\theta = u/2$. Then $a(\theta) = 0$, and $-b(\theta) = 3u/4$ is a square in $\mathbb{Q}_2$ because $3u \equiv 1 \pmod 8$. Over $\mathbb{Q}_2((t - \theta))$, a has valuation one, as $a'(\theta) = u + \frac{1}{2} \neq 0$, and b is a unit, so Springer's theorem gives the residues

cabezawhiteform	whitefirst residue	whitesecond residue
I_r, p (constant)	$[I_r]$, $[p]$	0
aI_4	0	$[a'(\theta) I_4] = [I_4]$
$\langle b \rangle$	$[\langle b(\theta) \rangle] = [\langle -1 \rangle]$	0

using that every scalar multiple of I_4 over $\mathbb{Q}_2$ is isometric to I_4, the norm form of the quaternion division algebra, whose norm is surjective. The anisotropic dimension of a form is the sum of those of its two residues. A complement B of M_G in $I_5 \perp p$ has second residue $-[I_4]$, anisotropic of dimension 4 over $\mathbb{Q}_2$, so $\dim B \geq 4$ and $d_{\mathbb{Q}}(G) \geq 4$ by Theorem 4.1. If $\ell_{\mathbb{Q}}(G) \leq 11$, a complement in I_{11} has rank 6, the same second residue, and first residue $[I_{11}] - [\langle -1 \rangle] = [I_{12}] = [I_4]$, since I_8 is a Pfister form of dimension $8 > u(\mathbb{Q}_2) = 4$, hence isotropic and so hyperbolic. Its anisotropic dimension would be $4 + 4 = 8 > 6$, a contradiction.

In plain words (commentary, not part of the paper)

Five variables, and three different numbers: real length 6, rational Gram rank 9, rational length 12. The Gram matrix only needs a form of rank four, but writing that form as honest rational squares costs three more.

The components do not decide the defect separately. We use Springer's theorem in this form: over $k((s))$ a form is $U \perp sV$ with U, V unimodular, its two residue classes are $[\bar{U}], [\bar{V}]$, and its anisotropic dimension is the sum of theirs [21 , Ch. VI] . A class in $W(F)$ with all second residues zero is constant [30 , Theorem 5.3] .

Proposition 4.5. p. 9

black!35

Let $E_1 = \langle e_1, e_2, e_3, e_4 \rangle$ and $E_2 = \langle e_5, e_6, 3e_7 + e_8 + e_9, -e_7 + 3e_8 + e_{10} \rangle$ in $\mathbb{Q}^{10}$, and let H be $\frac{3}{4}$ on E_1, $\frac{57}{64}$ on E_2 and 1 on the complement. Then $d_{\mathbb{Q}}(H) = 6$, while each component has anisotropic dimension 4.

↳ Used in: 2 (p. 41)

Proof

The blocks are $q_1 = I_4$ and $q_2 = \langle 1, 1, 11, 11 \rangle$, and both levels have residue field $L = \mathbb{Q}(\sqrt{-7})$, as $1 - (\frac{57}{64})^2 = 7(\frac{11}{64})^2$. For $d \leq 6$ add to H the skew blocks of upper entry $\frac{7}{16}$ on the pairs (e_1, e_5) and (e_2, e_6): each pair has a positive defect block of rank one, and four interior directions remain.

Suppose $d \leq 5$. Then $I_{10} \perp C \cong M_H \perp B$ over F with C constant positive of rank 5 and $\dim B = 5$, and $\det B \sim c = \det C$ since $\det M_H$ is a square. Let f_1, f_2 be the two quadratic factors. At f_i, the odd residue of B is $[-q_i]$, anisotropic of dimension 4 over L: for q_1 at a place over 2 with completion $\mathbb{Q}_2$, and for q_2 at a place over 11, where $-7 \equiv 4$ is a square. So B has an even line of class $\langle c \rangle$ at f_i, and $\eta = \langle f_1 f_2 \rangle([B] - [\langle c \rangle])$ has zero second residues everywhere. By Milnor's exact sequence [30 , Theorem 5.3] , $\eta = [\eta_0]$ for some $\eta_0 \in W(\mathbb{Q})$. Its first residue at f_i is then $\eta_0 \otimes k_{f_i}$, while by construction it is $\bar{f}_{3-i}$ times the second residue of $-[M_H]$ there, a scalar multiple $\alpha_i q_i$ over $k_{f_i} \cong L$. Both k_{f_i} have a place over 2 with completion $\mathbb{Q}_2$, and η_0 is defined over $\mathbb{Q}$, so $\eta_0 \otimes \mathbb{Q}_2 \cong \alpha_1 q_1 \cong \alpha_2 q_2$ in $W(\mathbb{Q}_2)$. But $\alpha_1 q_1 = \alpha_1 I_4$ is anisotropic, and $q_2 = \langle\langle -1, -11 \rangle\rangle$ is hyperbolic over $\mathbb{Q}_2$, as $-11 = 2^2 + (\sqrt{-15})^2$ there. This is a contradiction.

Proposition 4.6. p. 10

black!35

There is a rational diagonal matrix H with interior eigenvalues and $d_{\mathbb{Q}}(H) \geq 7$.

↳ Not used by another result of the paper.

Proof

Let $\rho_1, \ldots, \rho_k$ be the even classes of $W(\mathbb{Q}_2)$, each with a representative of rank 8. Choose distinct rationals $a_i \in (-1, 1)$ close to $\frac{3}{4}$ in $\mathbb{Q}_2$, so that $f_{a_i} = t^2 + 2a_i t + 1$ has a simple root $\theta_i \in \mathbb{Q}_2$. For each i put on the diagonal four copies of a_i and eight rationals $b_{ij} \in (-1, 1)$ with $\sum_j [\langle f_{b_{ij}}(\theta_i) \rangle] = \rho_i$ and $f_{b_{ij}}(\theta_l) \sim f_{a_i}(\theta_l)$ for $l \neq i$. This is possible: since $f_{a_i}(\theta_i) = 0$,

$f_b(\theta_i) = 2\theta_i(b - a_i)$, so the first condition asks $b - a_i$ to lie in one square class of $\mathbb{Q}_2$, an open set containing elements of arbitrarily large valuation; the second is an open condition at $b = a_i$, because $f_{a_i}(\theta_l) \neq 0$ for $l \neq i$ (the roots of f_a are θ, θ^{-1} and determine a). So for each j the admissible b form a nonempty open subset of $\mathbb{Q}_2$ accumulating at a_i, and $\mathbb{Q}$ is dense in $\mathbb{Q}_2 \times \mathbb{R}$, so we can take b_{ij} rational, distinct and in $(-1, 1)$. The a_i exist for the same reason: f_a has a simple root in $\mathbb{Q}_2$ as long as $a^2 - 1$ is a nonzero square there, which holds at $a = \frac{3}{4}$ ($a^2 - 1 = -\frac{7}{16}$) and so near it. The number k of classes is finite, as $W(\mathbb{Q}_2)$ has order 32. If $d \leq 6$, there are a constant C and a complement B of rank 6 with $[B] = [I_{12k}] + [C] - [M_H]$. Choose i with $[C_{\mathbb{Q}_2}] = \rho_i$ and work in $\mathbb{Q}_2((t - \theta_i))$. The odd residue is a multiple of I_4. The even one is $[I_{12k}] + \rho_i - (k-1)[I_4] - \rho_i = [I_4]$, since scalar multiples of I_4 over $\mathbb{Q}_2$ are isometric and I_8 is hyperbolic. So $\dim B \geq 8$, a contradiction.

Comparing with $d_{\mathbb{Q}}$: a positive rational form of rank $d{>}0$ embeds in I_{d+3} by Lemma 6.1, so $d_{\mathbb{Q}}(H) \leq \ell_{\mathbb{Q}}(H) - n \leq d_{\mathbb{Q}}(H) + 3$, and G attains the upper bound. In particular $\ell_{\mathbb{Q}}(H) - n$ is bounded in H if and only if $d_{\mathbb{Q}}(H)$ is.

5 Length n and $n + 1$

Let H be symmetric over $\mathbb{Q}$ with spectrum in $[-1, 1]$. Then $\mathbb{Q}^n$ is the orthogonal sum of the primary components $V_p = \ker p(H)$ over the irreducible factors p of the characteristic polynomial. For $p \neq x \mp 1$ let $F = \mathbb{Q}[x]/(p)$ with λ the class of x. Then F is totally real, and V_p is an F-space carrying a unique symmetric F-bilinear form h_p with $\mathrm{Tr}_{F/\mathbb{Q}}(a\, h_p(u, v)) = \langle au, v\rangle$ for all $a \in F$. Let $L_p = F(\sqrt{\lambda^2 - 1})$, which is totally imaginary.

The following criterion is closely related to the isometry criteria of [4] and is stated here in the language of lengths; what is ours is the translation to $\ell_{\mathbb{Q}}$ and its use below.

Theorem 5.1. p. 10

black!35↗

$\ell_{\mathbb{Q}}(H) = n$ if and only if $h_p \otimes L_p$ is hyperbolic for every $p \neq x \mp 1$.

🆕 **Classical and new:** a componentwise reading of the Milnor--Husemoller and Lewis exact sequence; same forms as Friedland 1993, for a different question

↳ Used in: Theorem 4.2 (p. 12), Proposition 4.3 (p. 12), 5.2 (p. 16), 5.3 (p. 16), Theorem 5.5 (p. 17), 5.6 (p. 17), Theorem 6.2 (p. 18), Theorem 7.1 (p. 29), Proposition 7.2 (p. 32), 9.6 (p. 37), 10.3 (p. 38)

Proof

Suppose $H = \mathrm{sym}T$ with $T \in O_n(\mathbb{Q})$. Then T commutes with H and preserves each $V = V_p$, on which $T^2 - 2\lambda T + 1 = 0$. By trace nondegeneracy, $h(Tu, Tv) = h(u, v)$. Put $\omega = T - \lambda$. Then $\omega^2 = \lambda^2 - 1$, ω is skew for h, and $h(\omega u, \omega v) = (1 - \lambda^2)h(u, v)$. For u with $h(u, u) \neq 0$, the plane $\langle u, \omega u\rangle$ is ω-stable and isometric to $h(u, u)\langle 1, 1 - \lambda^2\rangle$. By induction on the orthogonal complement, $h \cong \langle 1, 1 - \lambda^2\rangle \otimes g$, which is hyperbolic over L_p.

Conversely, let $h \otimes L_p$ be hyperbolic. The form h is definite at each real place of F, because the trace form is positive, so it is anisotropic. An isotropic vector $v + w\sqrt{\lambda^2 - 1}$ of $h \otimes L_p$ then gives $h(v, w) = 0$ and $h(v, v) = (1 - \lambda^2)h(w, w) \neq 0$, and this plane splits off [24 , Lemma 1] . By induction $h \cong \langle 1, 1 - \lambda^2\rangle \otimes g$, and the proof is effective once isotropic vectors are found. On a plane with orthogonal basis u, v and $h(v, v) = (1 - \lambda^2)h(u, u)$ put $Tu = \lambda u + v$ and $Tv = -(1 - \lambda^2)u + \lambda v$. This T is an F-linear isometry with $T + T^{-1} = 2\lambda$. Put $T = \pm 1$ on $V_{x \mp 1}$ and add up.

💡 **In plain words (commentary, not part of the paper)**

A rational rotation of cosine λ cannot live on just any plane: the plane must have the right discriminant, $1 - \lambda^2 = \sin^2\theta$. The theorem says this is the only obstruction. Each eigenspace must be built out of such

planes, which is the same as saying that its form becomes hyperbolic once $\sqrt{\lambda^2-1}$ is adjoined. That can be tested prime by prime. The language is classical (Milnor–Husemoller, Lewis): what is specific here is that H dictates the extension on each component.

Remark 5.2. (Why roots appear) p. 11

black!35↗

A rational rotation with $\cos\theta=\lambda$ lives on a plane of discriminant class $1-\lambda^2=\sin^2\theta$. A plane of class d needs the root $\sqrt{d(1-\lambda^2)}$. This is $\sin\theta$ up to a rational factor only when d is a square: for $\langle 1,2\rangle$ and $\lambda=\frac{1}{2}$ the root is $\sqrt{6}$, not $\sqrt{3}$.

↳ Not used by another result of the paper.

Remark 5.3. p. 11

In Lewis's Corollary [24] a form is the underlying form of a hermitian form over a quadratic extension if and only if it has even dimension $2r$, becomes hyperbolic, and has the determinant $(-a)^r$. Here h is anisotropic, so the extraction of planes forces the determinant. Theorem 5.1 says that $\ell_{\mathbb{Q}}(H)=n$ if and only if each h_p is the underlying form of a hermitian form over L_p/F. Compare also [4 , Proposition 3.6] . The condition $T+T^{-1}=2\lambda$ says that T has minimal polynomial $x^2-2\lambda x+1$ over F_p, so [4 , Corollary 9.2] applies on each component, and its determinant condition is the one above.

↳ Not used by another result of the paper.

Corollary 5.4. p. 11

black!35↗

Real_Jump_Locale.cor_jump *If $\ell_{\mathbb{R}}(H)=n$ and $\ell_{\mathbb{Q}}(H)\le n+1$, then $\ell_{\mathbb{Q}}(H)=n$.*

Isabelle · ours · part **show**

Only a part is in Isabelle: Witt cancellation over Q is the only named assumption (locale witt_over_Q)

`cor_jump` · `Isabelle/RealJump/Real_Jump_Locale.thy`, line 902 — the jump corollary (locale witt_over_Q)

```
theorem (in witt_over_Q) cor_jump:
  fixes H :: "real^'a^'a"
  assumes real_n: "\<exists>T0. orth_mat T0 \<and> sympart T0 = H"
    and rat_n1: "\<exists>A B::real^'a^('a option). rational_mat A \<and> rational_mat B
\<and> rep_mat A B H"
  shows "\<exists>T. rational_mat T \<and> orth_mat T \<and> sympart T = H"
```

`real_part2` · `Isabelle/RealJump/Real_Jump_Locale.thy`, line 679 — Theorem real (2)

```
theorem real_part2:
  assumes l: "l\<^sup>2 < 1" and ev: "even (dim (Eh l))" and v: "v \<in> Eh l"
  shows "bv \<bullet> v = 0" and "\<exists>w\<in>Eh l. Q *v emb v = emb w"
```

`cor_jump` · `Isabelle/RealJump/Real_Jump_Locale.thy`, line 902

```
theorem (in witt_over_Q) cor_jump:
  fixes H :: "real^'a^'a"
  assumes real_n: "\<exists>T0. orth_mat T0 \<and> sympart T0 = H"
    and rat_n1: "\<exists>A B::real^'a^('a option). rational_mat A \<and> rational_mat B
\<and> rep_mat A B H"
  shows "\<exists>T. rational_mat T \<and> orth_mat T \<and> sympart T = H"
```

Trust base: 🔒 kernel only — **only part of the statement is formal** (see the box). Isabelle: 3 results, no oracles

Proof: in this note · **Formalized:** Isabelle/HOL, by the author (public formalizations repository) · **Covers:** part: the named pieces are machine-checked; the statement as a whole is not marked as formalized in the paper · **Cite:** Proposition 2.3, p. 5, doi:10.5281/zenodo.24387751

🆕 **Classical and new:** not found in the literature so far; not a proof of novelty

↳ Used in: Theorem 5.5 (p. 17), 5.6 (p. 17), 9.4 (p. 36)

Proof

Take T and D over $\mathbb{Q}$ as in Proposition 2.1 with $r = n+1$. The complement of the columns of $\binom{T}{D}$ in $\mathbb{Q}^{n+1}$ is $\langle 1\rangle$ by Witt cancellation, so they extend to $Q \in O_{n+1}(\mathbb{Q})$. By Theorem 3.1, Q preserves each interior eigenspace of H, hence their sum V, which is defined over $\mathbb{Q}$ as the kernel of a factor of the characteristic polynomial. Then $Q|_V$ is rational orthogonal with symmetric part $H|_V$. On $V^\perp \subseteq \mathbb{Q}^n$ we have $H^2 = I$, so $T' = Q|_V \oplus H|_{V^\perp}$ gives $\ell_{\mathbb{Q}}(H) = n$.

Theorem 5.5. p. 11

black!35↗

For rational H it is decidable whether $\ell_{\mathbb{Q}}(H) \le n+1$. More precisely, let f be the characteristic polynomial of H. There are at most two monic $g \in \mathbb{R}[X]$ of degree $n+1$ whose roots lie in $[-1,1]$, interlace those of f, have even multiplicity in $(-1,1)$ and keep the multiplicities of ± 1 in f from dropping. Then $\ell_{\mathbb{Q}}(H) \le n+1$ if and only if, for one such g with rational coefficients:

1. *writing $g/f = X - c - \sum_p \mathrm{Tr}_{F_p/\mathbb{Q}}\big(w_p/(X-\lambda_p)\big)$, each h_p represents w_p over F_p, by some b_p, with $w_p = 0$ for $p = x \mp 1$;*
2. *the bordered matrix $S = \left(\begin{smallmatrix} H & b \\ b^\top & c \end{smallmatrix}\right)$, $b = \sum_p b_p$, has $\ell_{\mathbb{Q}}(S) = n+1$.*

The outcome of (2) does not depend on the choice of the b_p. All steps are effective: real algebraic numbers are isolated, the rationality of the candidates is tested exactly, representations are decided by local invariants, and a representing vector is then found by enumeration.

NEW **Classical and new:** not found in the literature so far; not a proof of novelty

↳ Not used by another result of the paper.

Remark 5.6. p. 11

black!35↗

For the mere decision there is a shorter route. With $D = \det M_H$, the complement of an embedding in I_{n+1} is a line of class $\langle D\rangle$, so $\ell_{\mathbb{Q}}(H) \le n+1$ if and only if $M_H \perp \langle D\rangle \cong I_{n+1}$ over F. The second residues at the factors of D are effective over number fields, and a class with zero residues is constant [30 , Theorem 5.3] , hence zero by specialization at $t = 0$. If moreover $\ell_{\mathbb{R}}(H) = n$, then D is a square in $\mathbb{Q}[t]$, and cancellation gives Corollary 5.4 again. The proof below gives more: the possible characteristic polynomials of the bordered matrix, the border itself, and so explicit witnesses.

↳ Not used by another result of the paper.

Proof

As in Corollary 5.4, $\ell_{\mathbb{Q}}(H) \le n+1$ means $S = \mathrm{sym}Q$ with $Q \in O_{n+1}(\mathbb{Q})$ for some border b, c. Let g be the characteristic polynomial of S, and for $x \in \mathbb{R}$ let $N_f(x)$, $N_g(x)$ count the roots, with multiplicity, that are $> x$. Cauchy interlacing says exactly that $e(x) = N_g(x) - N_f(x) \in \{0,1\}$ for all x. Interior roots of g have even multiplicity, as $S = \mathrm{sym}Q$. Within an open interval free of roots of f, e can only grow by one, so such an interval contains at most one simple root of g, which must then be ± 1. Now let x decrease from above 1, where $e = 0$, and record $m = m_f(\nu)$, $m' = m_g(\nu)$ and the jump $e \mapsto e + m' - m$ at each value ν:

cabezawhitevalue ν	**whitebefore**	**white$m' = m_g(\nu)$**	**whiteafter**
$\nu = 1$	$e = 0$	m or $m+1$ (the free bit)	$e = m' - m$
interior, m even	e	m (as $m \pm 1$ is odd)	e
interior, m odd	$e = 0$	$m+1$ (as $m-1$ would give $e = -1$)	1

interior, m odd	$e=1$	$m-1$ (as $m+1$ would give $e=2$)	0
$\nu=-1$	e	$m+1-e$ (degree $n+1$)	1

Here m may be 0 at ±1, and the condition that ±1 do not lose multiplicity is $m'\geq m$ in the first and last rows. Every row except the first has exactly one entry, so g is determined by the bit at $+1$, which gives at most two candidates.

The Schur complement gives $g/f = X - c - \langle b,(X-H)^{-1}b\rangle$, and the primary decomposition turns the last term into $\sum_p \operatorname{Tr}\big(h_p(b_p,b_p)/(X-\lambda_p)\big)$. So g determines c and $w_p = h_p(b_p,b_p)$. If $\lambda_p=\pm1$ then the quadratic form of $I\mp S\geq 0$ vanishes on V_p, so the operator does too, hence $b_p=0$. Whether h_p represents w_p is decided by Hasse–Minkowski over F_p, and a representing vector is then found by enumeration. Two vectors of equal nonzero norm are conjugate under $O(h_p)$ by Witt's theorem. Such isometries commute with H and are rational orthogonal for the trace form, so they conjugate the two borders, and $\ell_{\mathbb{Q}}(S)$ does not change. Finally (2) is decided by Theorem 5.1.

By the Hasse–Minkowski theorem the condition of Theorem 5.1 is local. For $F=\mathbb{Q}$ and $\delta=1-\lambda^2$, it says: $\dim h$ is even, the signed discriminant lies in $\{1,-\delta\}$ modulo squares, and h is hyperbolic over $\mathbb{Q}_p$ at each prime p where $-\delta$ is a square. At the other primes the quadratic extension kills the Hasse invariant.

6 One interior eigenvalue

In this section H is rational with spectrum in $\{-1,\lambda,1\}$ for one rational $\lambda\in(-1,1)$. Let $V=\ker(H-\lambda)$ with the form $q=I_n|_V$, $m=\dim V$, $\delta=1-\lambda^2$ and $L=\mathbb{Q}(\sqrt{-\delta})$. The complete graphs of Section 7 are the case $q=e^{\perp}$. Write w_v for the Hasse invariant $\prod_{i<j}(a_i,a_j)_v$ of a diagonal form and $\tau(c)$ for the number of rational squares needed for $c>0$.

We use the following local facts [21 , Ch. V–VI] . A nondegenerate quadratic form over $\mathbb{Q}_v$ is determined by its dimension, determinant and Hasse invariant. Let $\mathcal{R}_v(t,D)\subseteq\{\pm1\}$ be the set of Hasse invariants of t -dimensional forms of determinant D over $\mathbb{Q}_v$: for $t=0$ it is $\{1\}$ and requires D to be a square; for $t=1$ it is $\{1\}$; for $t=2$ it is $\{\pm1\}$ if $-D$ is not a square in $\mathbb{Q}_v$ and $\{1\}$ if it is, since $\langle x,D/x\rangle$ has Hasse invariant $(x,-D)_v$; for $t\geq3$ it is $\{\pm1\}$. Over $\mathbb{Q}$, a family of local forms of the same dimension and determinant, positive at the real place, almost all with trivial Hasse invariant and with $\prod_v w_v=1$, comes from a positive rational form [26 , 72:1] , unique up to isometry by Hasse–Minkowski.

Lemma 6.1. p. 12

black!35↗

A positive rational form p of dimension d embeds in I_{d+3}. (This is the case $A=\mathbb{Q}$ of [2 , Lemma 8.1] ; we include the short proof.)

↳ Used in: Theorem 6.2 (p. 18), Lemma 6.4 (p. 20), 10.3 (p. 38)

Proof

Let $D=\det p$. Prescribe a ternary positive form b of determinant D with $w_v(b)=w_v(p)(D,D)_v$ at every v. Ternary forms realize both Hasse invariants, and $\prod_v w_v(p)(D,D)_v=1$ by Hilbert reciprocity, so b exists. Then $p\perp b$ and I_{d+3} have the same local invariants, as $w(p\perp b)=w(p)w(b)(D,D)$, and they are isometric by Hasse–Minkowski.

Theorem 6.2. p. 13

black!35↗

Lengths_One_Core.factor_transpose, Lengths_One_Core.range_dim_parity For $h \geq 0$, $\ell_{\mathbb{Q}}(H) \leq n + h$ if and only if some positive definite subform p of I_h makes $(q \perp p)_L$ hyperbolic. The defect $d_{\mathbb{Q}}(H)$ is the least dimension of a positive rational form p with $(q \perp p)_L$ hyperbolic. In particular $\ell_{\mathbb{Q}}(H) \leq n + m + 3$.

Isabelle · ours · part **show**

Only a part is in Isabelle: the named pieces are machine-checked; the statement as a whole is not marked as formalized in the paper

`factor_transpose` · `Isabelle/LengthsOneCore/Lengths_One_Core.thy`, line 260

```
theorem factor_transpose:
  assumes "skew_mat S" and "\<iota> * \<iota> = - complex_of_real d"
  shows "transpose (mat \<iota> + cplx S) ** (mat \<iota> + cplx S) = - cplx (delta_mat
d S)"
```

`range_dim_parity` · `Isabelle/LengthsOneCore/Lengths_One_Core.thy`, line 464

```
theorem range_dim_parity: "dim (ran_set d S) mod 2 = CARD('n) mod 2"
```

↳ Used in: 6.3 (p. 19), Proposition 6.5 (p. 20), Theorem 6.7 (p. 22), Corollary 6.8 (p. 23), Theorem 6.9 (p. 23), Theorem 6.15 (p. 27), 10.2 (p. 38)

Proof

Let $\ell_{\mathbb{Q}}(H) \leq n + h$, and take T, D as in Proposition 2.1, $D : \mathbb{Q}^n \to \mathbb{Q}^h$. For v in $E_{\pm} = \ker(H \mp 1)$ we have $\langle Tv, v\rangle = \pm|v|^2$ and $|Tv|^2 + |Dv|^2 = |v|^2$, so $Tv = \pm v$ and $Dv = 0$ by Cauchy–Schwarz, and $T^{\top} v = 2Hv - Tv = \pm v$. So T preserves V, and $T|_V = \lambda + S$ with S skew. Put $\Delta = \delta + S^2 = D^{\top} D|_V$, a polynomial in S; so $U = \ker \Delta$ and $W = \operatorname{im} \Delta$ are rational, orthogonal and S-stable. On U we have $S^2 = -\delta$. For $x \in U$ the vectors x and Sx are orthogonal, as S is skew, and $q(Sx, Sx) = -q(S^2 x, x) = \delta q(x, x)$; so x, Sx span an S-stable plane $\langle a, a\delta\rangle$, $a = q(x, x)$, whose orthogonal complement in U is again S-stable. By induction q_U is a sum of such planes, each hyperbolic over L, where $-\delta$ is a square; and the residual form $r = q(\Delta\cdot, \cdot)|_W$ is isometric to $p = D(W) \subseteq I_h$. With $\iota^2 = -\delta$ in L, $q((\iota + S)x, (\iota + S)y) = -q(\Delta x, y)$, and $\iota + S$ is invertible on W_L because $(\iota - S)(\iota + S) = -\Delta$ is. So $q_{W,L} \cong -r_L$ and $(q \perp p)_L$ is hyperbolic. Here $\dim p = \operatorname{rank} D$ is exactly the defect of this T.

Conversely, $q \perp p$ is positive, hence anisotropic, and hyperbolic over L, so the extraction in Theorem 5.1 writes it as a sum of planes $\langle a, a\delta\rangle$ and gives an isometry R of $q \perp p$ with $\operatorname{sym} R = \lambda$. Extend R by ± 1 on $E_{\pm}$ and by the identity on $p^{\perp} \subseteq I_h$, and compress to the first n coordinates. This gives $\ell_{\mathbb{Q}}(H) \leq n + h$ by a contraction whose defect is at most $\dim p$. For the defect statement p need not lie in a given I_h, by Lemma 6.1. Finally $T = H$ has defect form δq on V, of dimension m, which embeds in I_{m+3} by Lemma 6.1.

💡 **In plain words (commentary, not part of the paper)**

With one interior eigenvalue λ, the squares needed beyond the first n are a positive form p sitting inside h unit squares. The theorem says exactly what p must do: together with the eigenspace form q, it must become hyperbolic over the quadratic field $L = \mathbb{Q}(\sqrt{-\delta})$, $\delta = 1 - \lambda^2$. So the rational length is the size of the smallest sum of unit squares that contains such a p; and since every positive form of dimension b fits in $b + 3$ squares, at most $m + 3$ extra squares are ever needed.

Remark 6.3. p. 13

black!35↗

The condition on $q \perp p$ is a theorem of Bayer-Fluckiger. By Milnor [31] and [4 , Proposition 3.6] , $(q \perp p)_L$ is hyperbolic exactly when $q \perp p$ carries an isometry with minimal polynomial $x^2 - 2\lambda x + 1$, and by [4 , Theorem 9.1 and Corollary 9.2] this holds if and only if $\dim(q \perp p) = 2k$ is even, $\det(q \perp p) = \delta^k$ modulo squares, and $q \perp p$ is hyperbolic over $\mathbb{Q}_v$ at every prime v that splits in L; see also [5 , 6] . At the other primes there is no condition beyond the determinant, since $L_w/\mathbb{Q}_v$ is quadratic and kills every quaternion class. What Theorem 6.2 adds is the constraint that p is a subform of a sum of squares, and the minimization over h.

↳ Used in: Theorem 6.7 (p. 22), Theorem 6.15 (p. 27)

Lemma 6.4. p. 13

black!35↗

Rational_SOS_Lengths_One_Eigenvalue.lagrange_three Let $0 \le d \le h$, $a = \min(d, h-d)$ *and* $c>0$ *rational. There is a positive* d*-dimensional subspace of* I_h *with determinant* c *modulo squares if and only if:* c *is a square, when* $a = 0$*;* c *is a sum of* h *squares, when* $a = 1$*;* c *is a sum of three squares, when* $a = 2$ *and* $h = 4$*; and always, when* $a = 2$ *and* $h \ge 5$*, or* $a \ge 3$*.*

Isabelle · ours · part **show**

Only a part is in Isabelle: the named pieces are machine-checked; the statement as a whole is not marked as formalized in the paper

`lagrange_three` · `Isabelle/RationalSOSLengths/Rational_SOS_Lengths_One_Eigenvalue.thy`, line 20

```
lemma lagrange_three:
  fixes a b c e f g :: "'a::comm_ring_1"
  shows "(a^2 + b^2 + c^2) * (e^2 + f^2 + g^2) - (a * e + b * f + c * g)^2
       = (b * g - c * f)^2 + (c * e - a * g)^2 + (a * f - b * e)^2"
```

↳ Used in: 6.16 (p. 29)

Proof

A subspace and its complement in I_h have the same determinant modulo squares, as the product is $\det I_h = 1$; so we treat the one of dimension a. A line has determinant c exactly when c is a sum of h squares. A plane with rational basis v, w of $\mathbb{Q}^3$ has determinant $|v \times w|^2$, a sum of three squares, and every nonzero vector of $\mathbb{Q}^3$ is a cross product. In $I_4 = \mathbb{H}_{\mathbb{Q}}$, an orthonormal-type basis v, w of a plane gives $\bar{v}w$, whose real part is $\langle v, w\rangle$; after Gram–Schmidt the determinant is the norm of a pure quaternion, a sum of three squares, and $I_3 \subset I_4$ gives the converse. In I_h with $h \ge 5$ any c occurs, by four squares in the complement of a unit vector. If $a \ge 3$, the form $\langle 1, \dots, 1, c\rangle$ of dimension d embeds in $I_{d+3} \subseteq I_h$ by Lemma 6.1.

Proposition 6.5. p. 14

black!35↗

Rational_SOS_Lengths_One_Eigenvalue.skew_two, Rational_SOS_Lengths_One_Eigenvalue.skew_three In the proof of Theorem 6.2, $d = \dim W$ *has the parity of* m*, and with* $\epsilon \in \{0, 1\}$, $\epsilon \equiv d \pmod 2$,

$$\det r \equiv \det q \cdot \delta^{(m-d)/2+\epsilon} \pmod{\mathbb{Q}^{\times 2}}.$$

Isabelle · ours · part **show**

Only a part is in Isabelle: the named pieces are machine-checked; the statement as a whole is not marked as formalized in the paper

`skew_two` · `Isabelle/RationalSOSLengths/Rational_SOS_Lengths_One_Eigenvalue.thy`, line 48

```
lemma skew_two:
  fixes d s :: "'a::comm_ring_1"
  shows "(d - s^2) * (d - s^2) - 0 * 0 = (d - s^2)^2"
```

`skew_three` · `Isabelle/RationalSOSLengths/Rational_SOS_Lengths_One_Eigenvalue.thy`, line 57

```
lemma skew_three:
  fixes d x y z :: "'a::comm_ring_1"
  defines "m11 \<equiv> d - x^2 - y^2" and "m12 \<equiv> - (y * z)" and "m13 \<equiv> x
* z"
    and "m22 \<equiv> d - x^2 - z^2" and "m23 \<equiv> - (x * y)" and "m33 \<equiv> d -
y^2 - z^2"
```

```
  shows "m11 * (m22 * m33 - m23 * m23) - m12 * (m12 * m33 - m23 * m13) + m13 * (m12 *
m23 - m22 * m13)
       = d * (d - x^2 - y^2 - z^2)^2"
```

↳ Used in: 6.16 (p. 29)

Proof

U is a sum of planes, so $\dim U = m - d$ is even and $\det q_U = \delta^{(m-d)/2}$. The characteristic polynomial of $S|_W$ is $X^\epsilon P(X^2)$, so $\det \Delta|_W = \delta^\epsilon P(-\delta)^2$, and $\det r = \det q_W \cdot \det \Delta|_W$ with $\det q_W = \det q / \det q_U$.

With Lemma 6.4 this is a lower bound: $\ell_{\mathbb{Q}}(H) - n$ is at least the least h for which some $d \equiv m \pmod 2$, $d \le h$, admits a d-dimensional subspace of I_h with determinant $\det q \cdot \delta^{(m-d)/2+\epsilon}$. For H_n it gives the lower bounds of Theorem 7.1. It is not sharp in general (Example 6.16). The exact value is local.

Lemma 6.6. p. 14

black!35↗

Local_Aux_Locale.aux Let $D>0$ be rational, $d, r \ge 0$, S a finite set of primes containing 2 and the primes dividing δ and D, and let signs $\epsilon_v \in \mathcal{R}_v(d, D)$ with $\epsilon_v(D,-1)_v \in \mathcal{R}_v(r, D)$ be given for $v \in S$. Then they extend to signs at all primes, equal to 1 outside S except at most at one prime inert in L, with the same two local conditions everywhere and $\prod_v \epsilon_v = 1$.

Isabelle · ours · part **show**

Only a part is in Isabelle: proved inside a locale whose only unproved facts are named assumptions (values of the Hilbert symbol, Hilbert reciprocity, Chebotarev for an inert prime); a model shows it is not vacuous

aux · Isabelle/LocalAuxSigns/Local_Aux_Locale.thy, line 81 — Lemma aux inside the locale local_quadratic_data

```
lemma aux:
  fixes d r :: nat and eps :: "'p \<Rightarrow> int"
  assumes loc: "\<forall>v\<in>S. ok v d r (eps v)"
    and dim0: "(d = 0 \<or> r = 0) \<longrightarrow> (\<forall>v. v \<notin> S \
<longrightarrow> sq v D)"
  shows "\<exists>e. (\<forall>v\<in>S. e v = eps v)
       \<and> (\<forall>v. v \<notin> S \<longrightarrow> e v \<noteq> 1 \
<longrightarrow> inert v \<and> (\<forall>w. w \<notin> S \<longrightarrow> e w \<noteq>
1 \<longrightarrow> w = v))
       \<and> (\<forall>v. ok v d r (e v))
       \<and> finite {v. e v \<noteq> 1} \<and> (\<Prod>v\<in>{v. e v \<noteq> 1}. e v)
= 1"
```

aux · Isabelle/LocalAuxSigns/Local_Aux_Locale.thy, line 81

```
lemma aux:
  fixes d r :: nat and eps :: "'p \<Rightarrow> int"
  assumes loc: "\<forall>v\<in>S. ok v d r (eps v)"
    and dim0: "(d = 0 \<or> r = 0) \<longrightarrow> (\<forall>v. v \<notin> S \
<longrightarrow> sq v D)"
  shows "\<exists>e. (\<forall>v\<in>S. e v = eps v)
       \<and> (\<forall>v. v \<notin> S \<longrightarrow> e v \<noteq> 1 \
<longrightarrow> inert v \<and> (\<forall>w. w \<notin> S \<longrightarrow> e w \<noteq>
1 \<longrightarrow> w = v))
       \<and> (\<forall>v. ok v d r (e v))
       \<and> finite {v. e v \<noteq> 1} \<and> (\<Prod>v\<in>{v. e v \<noteq> 1}. e v)
= 1"
```

Trust base: 🔒 kernel only — **only part of the statement is formal** (see the box). Isabelle: 2 results, no oracles

Proof: in this note · **Covers:** not formalized · **Cite:** Theorem 5.5, p. 11, doi:10.5281/zenodo.24387751

↳ Used in: Theorem 6.7 (p. 22), Theorem 6.9 (p. 23)

Proof

Here v runs over the primes: at the real place positive forms have Hasse invariant 1 and $(D,-1)_\infty = 1$, as $D>0$, so the product formula only involves primes. Put $\epsilon_v = 1$ outside S; this is admissible there, as D is a unit and $(D,-1)_v = 1$. If the product is 1 we are done. If

$d \le 1$ the signs are forced to be 1 and the product is 1; if $r \le 1$ they are forced to be $(D,-1)_v$, whose product is 1 by Hilbert reciprocity; in dimension 0 the condition at S makes D a square at every prime dividing it and at 2, hence a rational square, and the signs are again forced. If $d, r \ge 2$, choose by Chebotarev an odd prime $v_1 \notin S$ inert in L and in $\mathbb{Q}(\sqrt{-D})$, or only in L if the two fields coincide; both fields are imaginary quadratic, as $\delta, D>0$, so neither is trivial; if they differ, their compositum has Galois group $(\mathbb{Z}/2)^2$, and Chebotarev density gives infinitely many primes whose Frobenius is the element nontrivial on both fields, that is, primes inert in both. There $-D$ is not a square, so $\mathcal{R}_{v_1}(t, D) = \{\pm 1\}$ for $t \ge 2$, and $(D,-1)_{v_1} = 1$. Setting $\epsilon_{v_1} = -1$ corrects the product.

Theorem 6.7. p. 14

black!35↗

For $d \equiv m \pmod 2$ put $k = (m+d)/2$ and $D_d = \det q \cdot \delta^k$. Let S_d consist of 2 and the primes dividing δ, D_d and the entries of a diagonalization of q. Then $\ell_{\mathbb{Q}}(H) - n$ is the least $h \le m+3$ for which there is $d \equiv m \pmod 2$ with $0 \le d \le h$ such that at every $v \in S_d$ some sign ϵ_v satisfies:

1. *$\epsilon_v \in \mathcal{R}_v(d, D_d)$ and $\epsilon_v (D_d, -1)_v \in \mathcal{R}_v(h-d, D_d)$;*
2. *if v splits in L, then $\epsilon_v = w_v(q)\,(\det q, D_d)_v\,(-1,-1)_v^{k(k-1)/2}$.*

The defect $d_{\mathbb{Q}}(H)$ is the least $d \le m$ for which (2) and the first condition in (1) hold; the condition on the complement, of dimension $h-d$, is dropped. The procedure decides the two numbers; a witness needs an additional explicit embedding.

↳ Used in: Corollary 6.8 (p. 23), Theorem 6.9 (p. 23), Proposition 6.11 (p. 24), 6.12 (p. 25), 6.16 (p. 29)

Proof

Suppose the conditions hold. By Lemma 6.6 the signs extend to all primes with product 1 and with both local conditions everywhere; at split primes outside S_d the extended signs are 1, which is what (2) gives there, as all the symbols involved are of units. By the existence theorem there are positive rational forms p and b of dimensions d and $h-d$, determinant D_d, and Hasse invariants ϵ_v and $\epsilon_v(D_d,-1)_v$; the product formula for b follows from that for p by Hilbert reciprocity. Then $w(p \perp b) = \epsilon_v \cdot \epsilon_v(D_d,-1)_v \cdot (D_d, D_d)_v = 1$, so $p \perp b \cong I_h$ by Hasse–Minkowski, that is, $p \subseteq I_h$. The form $q \perp p$ has dimension $2k$ and determinant $\det q \cdot D_d \equiv \delta^k$; at a split prime $-\delta$ is a square, so the determinant is $(-1)^k$, and (2) says that the Hasse invariant $w_v(q)\epsilon_v(\det q, D_d)_v$ is that of k hyperbolic planes, so $q \perp p$ is hyperbolic over $\mathbb{Q}_v$. By Remark 6.3 and Theorem 6.2, $\ell_{\mathbb{Q}}(H) \le n + h$.

Conversely, let $p \subseteq I_h$ be as in Theorem 6.2 and b its complement. Remark 6.3 gives $\det p \equiv D_d$; (1) holds for the local forms of p and b, since $w(b) = w(p)(D_d, -1)$ from $p \perp b \cong I_h$; and at split primes (2) follows from the hyperbolicity of $q \perp p$ and $w(\alpha \perp \beta) = w(\alpha)w(\beta)(\det\alpha, \det\beta)$. The bound $h \le m+3$ is Theorem 6.2. The defect is the same argument with p not required to lie in I_h.

💡 **In plain words (commentary, not part of the paper)**

The search for the form p of Theorem 6.2 is a finite computation. For each candidate dimension d and each $h \le m+3$ it reduces to choosing a sign at finitely many primes (2, and the primes of δ, of the determinant D_d and of q), subject to two local conditions and to the product of all signs being 1. So the excess $\ell_{\mathbb{Q}}(H) - n$ of a given H is decided by a finite check, prime by prime.

The search in Theorem 6.7 is finite and local: $h \le m+3$, $d \le h$, and two signs at each prime of S_d, tested separately; there is never a global (reciprocity) obstruction. Our implementation reproduces Theorem 7.1 for $3 \le n \le 66$, length and defect, and the case $n = 1$ of Example 9.3; for $n = 1$ the length is also given by Pourchet's criteria for sums of squares in $\mathbb{Q}[t]$ [27] . The written proof of Theorem 7.1, not this computation, establishes it for every n. Three things should be kept apart. Theorem 6.7 decides $\ell_{\mathbb{Q}}(H)$ and $d_{\mathbb{Q}}(H)$. A representation attaining them needs, in addition, an explicit form $p \subseteq I_h$ and the extraction of Theorem 5.1, which we carry out only in examples. The computations reported in this paper test the

implementation and the statements on finitely many cases; they are not part of any proof. For scalar matrices the procedure has a closed form.

Corollary 6.8. p. 15

black!35↗

Lengths_Local_Criterion.cor_bounded For H with one interior eigenvalue, of multiplicity m,

$$d_{\mathbb{Q}}(H) \le \min(m,\, c_m), \qquad \ell_{\mathbb{Q}}(H) - n \le \min(m,\, c_m) + 3, \qquad c_m = \begin{cases} 3, & m \text{ odd}, \\ 4, & m \text{ even}. \end{cases}$$

So for one interior eigenvalue the excess is at most 7, which answers Question 1 in this case.

Isabelle · ours · part **show**

Only a part is in Isabelle: the named pieces are machine-checked; the statement as a whole is not marked as formalized in the paper

`cor_bounded` · `Isabelle/LengthsLocalCriterion/Lengths_Local_Criterion.thy`, line 330

```
theorem cor_bounded:
  "def_le (min m (cm m)) \<and> exc_le (min m (cm m) + 3)"
```

↳ Used in: Theorem 6.9 (p. 23), Proposition 6.11 (p. 24)

Proof

$T = H$ has defect m, and Theorem 6.2 gives the bound $m + 3$. Otherwise take $d = c_m$, which has the parity of m, and $h = d + 3$ in Theorem 6.7. Forms of dimension $d \ge 3$ and $h - d = 3$ realize both Hasse invariants at every prime, so (1) holds for any sign, and the sign prescribed by (2) at the split primes is admissible.

Both bounds are attained, and for multiplicity 4 the excess 7 has an exact local description. Write w_v for the Hasse invariant.

Theorem 6.9. p. 15

black!35↗

Lengths_Local_Criterion.sharp Let H have one interior eigenvalue λ, of multiplicity 4, with eigenspace form q and $D = \det q$ modulo squares. Then $\ell_{\mathbb{Q}}(H) - n = 7$ if and only if $d_{\mathbb{Q}}(H) = 4$ and some prime v that splits in L has $-D \in \mathbb{Q}_v^{\times 2}$ and $w_v(q) = -1$.

Isabelle · ours · part **show**

Only a part is in Isabelle: the named pieces are machine-checked; the statement as a whole is not marked as formalized in the paper

`sharp` · `Isabelle/LengthsLocalCriterion/Lengths_Local_Criterion.thy`, line 537

```
theorem sharp:
  assumes m4: "m = 4"
  shows "(exc_le 7 \<and> \<not> exc_le 6)
         \<longleftrightarrow> (def_le 4 \<and> \<not> def_le 3 \<and> (\<exists>v.
split v \<and> sq v (-D) \<and> wq v = -1))"
```

↳ Used in: 6.10 (p. 24), 1 (p. 41)

Proof

Let $d_{\mathbb{Q}}(H) = 4$. Since $\mathcal{R}_v(t, D) \subseteq \mathcal{R}_v(t+1, D)$ for every t, conditions (1) and (2) of Theorem 6.7 for (h, d) imply them for $(h+1, d)$, so the excess is at most 6 exactly when they hold for $h = 6$ and some d. Only $d \in \{4, 6\}$ can occur in Theorem 6.7 for $h = 6$, since $d \equiv m \pmod 2$ and $d \ge d_{\mathbb{Q}}(H)$ exclude $d = 0, 2$. For $d = 4$ the determinant condition of Theorem 6.2 gives $\det p \equiv D\delta^4 \equiv D$, and at a split place v hyperbolicity of

$(q \perp p)_{L_w} = (q \perp p)_{\mathbb{Q}_v}$ forces $p_v \cong -q_v$, so $w_v(p) = w_v(q)(-1, D)_v$. A binary complement b of p in I_6 has determinant D and $w_v(b) = w_v(p)(D, D)_v = w_v(q)$. If $-D$ is not a square in $\mathbb{Q}_v$, binary forms of determinant D realize both signs; if it is, b is a hyperbolic plane and $w_v(b) = +1$. At a place that does not split, $(q \perp p)_{L_w}$ only constrains the determinant, because restriction to a quadratic extension of a local field kills the Brauer group of order two, so the sign of p is free there. Hence, by Theorem 6.7 and Lemma 6.6, the case $d = 4$, $h = 6$ is possible exactly when no split v has $-D$ square and $w_v(q) = -1$; such a v lies in S_d, since $w_v(q) = 1$ at the primes outside S_d. At such a v the case $d = 6$, $h = 6$ also fails: then $p \cong I_6$, and $w_v(q \perp I_6) = w_v(q) = -1$, while a hyperbolic form of dimension 10 has Hasse invariant $(-1, -1)_v^{10} = 1$. So the condition gives $h = 7$ by Corollary 6.8. Conversely, if the excess is 7, then $d_{\mathbb{Q}}(H) = 4$, since a defect form of rank at most 2 lies in I_5, and the case $d = 4$, $h = 6$ must fail, which is the condition.

💡 **In plain words (commentary, not part of the paper)**

Seven extra squares is the most one interior eigenvalue can cost (Corollary 6.8), and this theorem says exactly when it happens: the eigenvalue has multiplicity 4, its defect form has dimension 4, and at some prime that splits in L the number $-D$ is a square while the Hasse invariant of q is -1. Example 6.10 realizes it at order 6, which Proposition 6.11 shows is the smallest possible.

The cases of the proof for $h = 6$, at a split prime v with $-D \in \mathbb{Q}_v^{\times 2}$ and $w_v(q) = -1$:

d	**at such a v**	**at the other places**
$0, 2$	excluded, as $d \geq d_{\mathbb{Q}}(H) = 4$	excluded
4	fails: the complement is a hyperbolic plane, with $w_v = +1 \neq w_v(q)$	the signs can be met
6	fails: $w_v(q \perp I_6) = -1$, while five hyperbolic planes have $+1$	–

Colour: red = no / fails; blue shade = the number's size within its column.

Example 6.10. p. 16

black!35↗

For $q = \langle 11, 21, 23, 23\rangle$ and $\lambda = \frac{3}{4}$, $L = \mathbb{Q}(\sqrt{-7})$ and 2, 23 split. At 23, $q_v = \langle 11, 21\rangle \perp 23\langle 1, 1\rangle$ has both residue forms anisotropic, as $-231 \equiv -1$ and -1 are not squares modulo 23, so q_v is anisotropic of dimension 4 and $d_{\mathbb{Q}} = 4$. At 2, $D = 231 \equiv 7 \pmod 8$, so $-D$ is a square in $\mathbb{Q}_2$, and $w_2(q) = -1$ (the symbols $(11, 23)_2$ and $(23, 23)_2$ are -1, the others $+1$). The columns of

$$W = \frac{1}{55}\begin{pmatrix} -32 & -156 & 14 & -23 \\ 107 & 6 & -64 & 168 \\ 80 & -50 & 185 & -80 \\ -119 & 18 & 83 & 119 \\ -15 & -80 & -155 & -95 \\ 4 & -173 & 12 & 106 \end{pmatrix}$$

satisfy $W^\top W = \operatorname{diag}(11, 21, 23, 23)$, so for $H = I_6 - \frac{1}{4}P_W$, with P_W the orthogonal projection on the column space, Theorem 3.1 gives $\ell_{\mathbb{R}}(H) = 6$, and Theorem 6.9 gives $\ell_{\mathbb{Q}}(H) = 13$. The same holds for $\lambda = \frac{7}{8}$, with $L = \mathbb{Q}(\sqrt{-15})$, where 2 and 23 split again.

↳ Used in: Proposition 6.11 (p. 24)

Proposition 6.11. p. 16

black!35↗

With one interior eigenvalue, excess 7 requires $n \geq 6$; so Example 6.10 has the least possible order.

↳ Used in: 1 (p. 41)

Proof

Excess 7 needs m even and $m \geq 4$ by Corollary 6.8, so $m = 4$ when $n \leq 5$; and $n = 4$ gives $q = I_4$, of excess at most 4 by Theorem 6.15. Let $n = 5$, so $q \perp \langle c \rangle \cong I_5$ with $c>0$. If $\tau(c) \leq 3$, take $p = \langle c \rangle \perp I_3 \subseteq I_{\tau(c)+3}$: then $q \perp p \cong I_8$, hyperbolic over the totally imaginary field L, and the excess is at most 6. If $\tau(c) = 4$, take $d = 2$, $h = 5$; here $k = (4+2)/2 = 3$ and $D_2 = \det q \cdot \delta^3 \equiv c\,\delta$, since $\det q \equiv c$ from $q \perp \langle c \rangle \cong I_5$. At an odd split prime I_4 is hyperbolic, so $[q_v] = [\langle 1, -c \rangle]$ and $-[q_v]$ is binary of the right determinant; if 2 splits, c and δ are both $\equiv 7$ modulo squares in $\mathbb{Q}_2$, so $[q_2] = [I_6]$ and $-[q_2] = [I_2]$. In both cases the binary form required at the split primes exists, so the sign prescribed by condition (2) of Theorem 6.7 lies in $\mathcal{R}_v(2, D_2)$; at a prime that does not split, (2) is void and the sign $+1$ is admissible for p. The complement of p in I_5 has dimension 3, so its local signs are free, and Theorem 6.7 gives excess at most 5.

The search of Theorem 6.7 over the 1001 diagonal q of dimension 4 with entries in $\{1, 2, 3, 5, 6, 7, \allowbreak 11, 14, 21, 22, 23\}$ and eight values of λ, 8008 cases, finds 45 cases of excess 7 , exactly those predicted by Theorem 6.9; for $n = 5$, the eigenspaces $\mathbf{v}^\perp \subseteq I_5$ of the 55 nonzero vectors $\mathbf{v} \in \{0, 1, 2, 3\}^5$ with nondecreasing entries, with the same eight values of λ, give excess at most 5 in all 440 cases. For odd multiplicity the bound 6 is attained too.

Example 6.12. p. 16

black!35↗

Let $V \subseteq \mathbb{Q}^5$ be spanned by e_1, $(0, 1, 1, 1, 0)$ and $(0, 1, -1, 0, 1)$, so that $q = \langle 1, 3, 3 \rangle$, and $H = \frac{1}{3} P_V + (I - P_V)$. Then $\delta = \frac{8}{9}$, $L = \mathbb{Q}(\sqrt{-2})$, and 3 splits in L. Over $\mathbb{Q}_3$, $q = \langle 1 \rangle \perp 3\langle 1, 1 \rangle$ has both residue forms anisotropic, so it is anisotropic of dimension 3 and $d_{\mathbb{Q}}(H) = 3$. For $h = 5$ Theorem 6.7 leaves $d \in \{3, 5\}$, with $D_3 = 2$ and $D_5 = 1$, and $w_3(q) = -1$. At 3, hyperbolicity of $(q \perp p)_{L_w}$ forces $\epsilon_3(p) = -1$ in both cases. For $d = 3$ the complement b in I_5 is binary of determinant 2 with $w_3(b) = \epsilon_3(p)(2, 2)_3 = -1$, impossible since -2 is a square in $\mathbb{Q}_3$ and b would be a hyperbolic plane, with $w_3(b) = +1$; for $d = 5$ the complement is 0-dimensional and needs $+1$. For $h = 6$ and $d = 3$ the complement is ternary and both signs occur, so $h = 6$ is attained. These local signs are printed by the script `tabla_local_sharpodd.py` of the supplement. The procedure of Theorem 6.7 confirms $\ell_{\mathbb{R}}(H) = 6$, $d_{\mathbb{Q}}(H) = 3$ and $\ell_{\mathbb{Q}}(H) = 11$, an excess of 6. With $n = 4$, in 552 cases tried the excess was at most 4.

↳ Used in: 1 (p. 41)

Remark 6.13. p. 17

black!35↗

For H_n, condition (2) is as weak as it can be. Here $\det q \equiv n$ and $w_v(q) = (n, -1)_v$, as $q \perp \langle n \rangle \cong I_n$, and $D_d \in \{n, n-2\}$. If v splits in $L = \mathbb{Q}(\sqrt{-n(n-2)})$ then $(n, -1)_v = 1$: for odd $v \mid n$ the valuation of n is even, as $v \nmid n - 2$; for $v = 2$ the odd part of n is $\equiv 1 \pmod 4$, by the square condition on $-n(n-2)$. And $(n, -D_d)_v = 1$, since $-(n-2) \equiv n$ there. So (2) reads $\epsilon_v = 1$ at odd split primes and $\epsilon_2 = (-1, -1)_2^{k(k-1)/2}$ when 2 splits. This is consistent with the determinant bound being sharp for H_n: the lower bounds of Theorem 7.1 are exactly the determinant bound, and Theorem 7.1 attains them for every n, so the remaining sign at 2 never excludes a determinant-minimal candidate.

↳ Used in: 3 (p. 41)

Lemma 6.14. p. 17

black!35↗

Level_Quadratic_Fields.level_one, Level_Quadratic_Fields.level_two, Level_Quadratic_Fields.level_ge3_le4, Level_Quadratic_Fields.level_four Let a be the positive

> *squarefree integer with $\delta \equiv a$, so $L = \mathbb{Q}(\sqrt{-a})$, and let $s(L)$ be its level, the least number of squares with sum -1. Then $s(L) = 1$ if $a = 1$, $s(L) = 4$ if $a \equiv 7 \pmod 8$, and $s(L) = 2$ otherwise. Equivalently $s = 1, 2, 4$ according as $\tau(\delta) = 1$, $\tau(\delta) \in \{2, 3\}$, $\tau(\delta) = 4$. In $W(L)$ the class of $\langle 1 \rangle$ has order $2s$, and I_j is anisotropic over L for $j \leq s$.*

Isabelle · ours · part **show**

Only a part is in Isabelle: the values of the level; level 4 uses Pfister's theorem (a level is never 3) as a named locale assumption, without it the proof gives 3 ≤ s ≤ 4

`level_one` · `Isabelle/LevelQuadraticFields/Level_Quadratic_Fields.thy`, line 354 — level 1 for a = 1

```
theorem level_one:
  fixes a :: nat
  assumes "squarefree a" and "a = 1"
  shows "level (of_nat a) = 1"
```

`level_two` · `Isabelle/LevelQuadraticFields/Level_Quadratic_Fields.thy`, line 360 — level 2 off a ≡ 7 (mod 8)

```
theorem level_two:
  fixes a :: nat
  assumes "squarefree a" and "a \<noteq> 1" and "a mod 8 \<noteq> 7" and "a > 0"
  shows "level (of_nat a) = 2"
```

`level_ge3_le4` · `Isabelle/LevelQuadraticFields/Level_Quadratic_Fields.thy`, line 374 — level 3 or 4 for a ≡ 7 (mod 8)

```
theorem level_ge3_le4:
  fixes a :: nat
  assumes "a mod 8 = 7"
  shows "neg1_sos (of_nat a) 4" and "\<not> neg1_sos (of_nat a :: rat) 1" and "\<not>
neg1_sos (of_nat a :: rat) 2"
```

`level_four` · `Isabelle/LevelQuadraticFields/Level_Quadratic_Fields.thy`, line 394 — level 4 for a ≡ 7 (mod 8), with Pfister as a named assumption

```
theorem level_four:
  fixes a :: nat
  assumes "a mod 8 = 7"
  shows "level (of_nat a) = 4"
```

`level_one` · `Isabelle/LevelQuadraticFields/Level_Quadratic_Fields.thy`, line 354

```
theorem level_one:
  fixes a :: nat
  assumes "squarefree a" and "a = 1"
  shows "level (of_nat a) = 1"
```

`level_two` · `Isabelle/LevelQuadraticFields/Level_Quadratic_Fields.thy`, line 360

```
theorem level_two:
  fixes a :: nat
  assumes "squarefree a" and "a \<noteq> 1" and "a mod 8 \<noteq> 7" and "a > 0"
  shows "level (of_nat a) = 2"
```

`level_ge3_le4` · `Isabelle/LevelQuadraticFields/Level_Quadratic_Fields.thy`, line 374

```
theorem level_ge3_le4:
  fixes a :: nat
  assumes "a mod 8 = 7"
  shows "neg1_sos (of_nat a) 4" and "\<not> neg1_sos (of_nat a :: rat) 1" and "\<not>
neg1_sos (of_nat a :: rat) 2"
```

`level_four` · `Isabelle/LevelQuadraticFields/Level_Quadratic_Fields.thy`, line 394

```
theorem level_four:
  fixes a :: nat
  assumes "a mod 8 = 7"
  shows "level (of_nat a) = 4"
```

Trust base: 🔒 kernel only — **only part of the statement is formal** (see the box). Isabelle: 8 results, no oracles

Proof: in this note · **Covers:** not formalized · **Cite:** Theorem 6.7, p. 14, doi:10.5281/zenodo.24387751

↳ Used in: Theorem 6.15 (p. 27)

Proof

$s(L)=1$ means $-1\in L^{\times 2}$, that is $L=\mathbb{Q}(i)$. Since L has no real place, I_5 is isotropic over L by Hasse–Minkowski, so $s(L)\le 4$, and $s(L)\le 2$ if and only if I_3 is isotropic over L, again a local question. At a place w over an odd prime I_3 is isotropic. At a dyadic place, if $L_w=\mathbb{Q}_2$ then I_3 is anisotropic, as $-1\equiv 7 \pmod 8$ is not a sum of two squares in $\mathbb{Q}_2$; if $L_w/\mathbb{Q}_2$ is quadratic, then for $x,y\in\mathbb{Q}_2$ one has $(x,y)_{L_w}=(x,N_{L_w/\mathbb{Q}_2}y)_{\mathbb{Q}_2}=(x,y^2)_{\mathbb{Q}_2}=1$, so $\langle 1,1\rangle$ represents -1 and I_3 is isotropic. Thus $s(L)=4$ exactly when 2 splits in L, that is when $-a\equiv 1 \pmod 8$. By Legendre's theorem, for which rational and integer representations agree, $a\equiv 7 \pmod 8$ is $\tau(a)=4$, and $\tau(\delta)=\tau(a)$. The statements about $W(L)$ are Pfister's: the level is a power of 2, I_{2s} is hyperbolic, and I_s is anisotropic [21 , Ch. XI] .

Theorem 6.15. p. 17

black!35↗

Rational_SOS_Lengths_One_Eigenvalue.quaternion_columns Let $\lambda\in(-1,1)$ be rational, $\tau=\tau(1-\lambda^2)$, and $s=1,2,4$ according as $\tau=1$, $\tau\in\{2,3\}$, $\tau=4$. Write $m\equiv\rho \pmod{2s}$ with $0\le\rho<2s$. Then

$$\boxed{\ell_{\mathbb{Q}}(\lambda I_m)=m+\min\big((-m) \bmod 2s,\ \tau\big),\qquad d_{\mathbb{Q}}(\lambda I_m)=\min(\rho,2s-\rho).}$$

In particular $\ell_{\mathbb{Q}}(\lambda I_{m+2s})=\ell_{\mathbb{Q}}(\lambda I_m)+2s$, $2s$ is the least such period, and $0\le\ell_{\mathbb{Q}}(\lambda I_m)-m\le 4$.

Isabelle · ours · part **show**

Only a part is in Isabelle: the named pieces are machine-checked; the statement as a whole is not marked as formalized in the paper

`quaternion_columns` · `Isabelle/RationalSOSLengths/Rational_SOS_Lengths_One_Eigenvalue.thy`, line 36

```
lemma quaternion_columns:
  fixes a b c d :: "'a::comm_ring_1"
  defines "N \<equiv> a^2 + b^2 + c^2 + d^2"
  shows "dot4 (a, b, c, d) (a, b, c, d) = N" and "dot4 (-b, a, d, -c) (-b, a, d, -c) =
N"
    and "dot4 (-c, -d, a, b) (-c, -d, a, b) = N" and "dot4 (-d, c, -b, a) (-d, c, -b, a)
= N"
    and "dot4 (a, b, c, d) (-b, a, d, -c) = 0" and "dot4 (a, b, c, d) (-c, -d, a, b) =
0"
    and "dot4 (a, b, c, d) (-d, c, -b, a) = 0" and "dot4 (-b, a, d, -c) (-c, -d, a, b) =
0"
    and "dot4 (-b, a, d, -c) (-d, c, -b, a) = 0" and "dot4 (-c, -d, a, b) (-d, c, -b, a)
= 0"
```

↳ Not used by another result of the paper.

Proof

By Lemma 6.14, s is the level of L and the anisotropic dimension of $(I_m)_L$ is $\min(\rho,2s-\rho)$, which is the defect by Proposition 4.3.

Upper bound. The form $p=I_{(-m) \bmod 2s}$ makes $(I_m\perp p)_L$ hyperbolic. If $\tau<(-m) \bmod 2s$, take $p=\delta I_\rho$: since $-\delta$ is a square in L, $(I_m\perp\delta I_\rho)_L$ has the class of $I_{m-\rho}$, which vanishes. It embeds in I_τ: if $\tau=4$ then $s=4$ and $\rho\le 3$, and left multiplication by a quaternion of norm $\delta=a^2+b^2+c^2+e^2$ has orthogonal columns of norm δ, so $\delta I_4\cong I_4$ and $\delta I_\rho\subseteq I_4$; if $\tau\le 3$ the inequality forces $s=2$, $\rho=1$, $\tau=2$, and $\langle\delta\rangle\subseteq I_2$.

Lower bound. By Theorem 6.2, $h\ge\dim p\ge d_{\mathbb{Q}}=\min(\rho,2s-\rho)$, which is the claim except when $s=2$, $\rho=1$ and when $s=4$, $1\le\rho\le 3$.

For $s=2$, $\rho=1$: if $h=1$ then $p=\langle 1\rangle$ and $(I_{m+1})_L$ would be hyperbolic, so $4\mid m+1$, which is false. If $h=2$, the dimension of p is odd, so $p=\langle D\rangle$, and Remark 6.3 gives

$D \equiv \delta^{(m+1)/2} \equiv \delta$, as $(m+1)/2$ is odd. Then $p \subseteq I_2$ makes δ a sum of two squares. So $h \geq \tau$.

For $s = 4$ and $1 \leq \rho \leq 3$, suppose $h \leq 3$. Since 2 splits in L, some completion of L is $\mathbb{Q}_2$, where $(I_m \perp p)$ is hyperbolic, so $[p] = -[I_m]$ in $W(\mathbb{Q}_2)$. In $W(\mathbb{Q}_2)$ the class of $\langle 1 \rangle$ has order 8 and I_j is anisotropic for $j \leq 4$, so the anisotropic dimension of I_j is $\min(j, 8-j)$ for $0 \leq j \leq 8$. The complement b of p in I_h has class

$$[b] = [I_h] - [p] = [I_h] + [I_m] = [I_{h+\rho}],$$

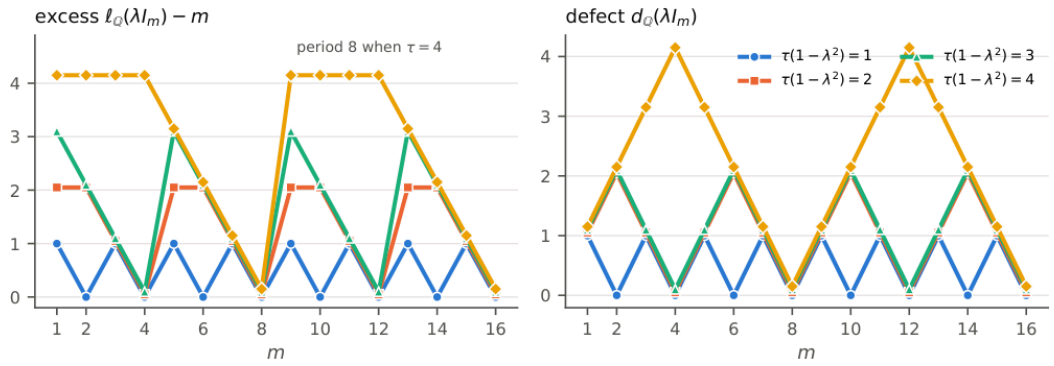
of anisotropic dimension $\min(h+\rho, 8-h-\rho)$. But $\dim b = h - \dim p \leq h - \rho$, since $\dim p \geq d_{\mathbb{Q}} = \rho$, and $\min(h+\rho, 8-h-\rho) > h - \rho$ because $\rho \geq 1$ and $h \leq 3$. A representative of a Witt class cannot have smaller dimension than its anisotropic part, so $h \geq 4 = \tau$.

The period follows from the formula, and it is least because $\ell_{\mathbb{Q}}(\lambda I_j) = j$ only for $2s \mid j$. The excess is at most $\tau \leq 4$.

💡 **In plain words (commentary, not part of the paper)**

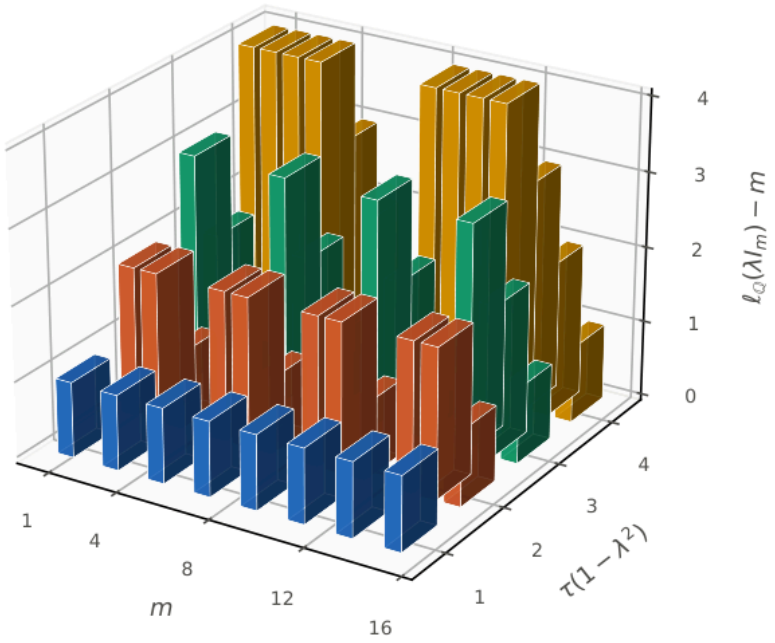
For a scalar dilation λI_m everything is explicit. What matters is how many squares $1 - \lambda^2$ needs (τ), which fixes the level $s \in \{1, 2, 4\}$ of L. The extra squares depend only on m modulo $2s$, are never more than 4, and the pattern repeats with period exactly $2s$.

🖼️ **Figure 2**



Excess and defect of λI_m against m, one series per $\tau(1-\lambda^2)$, from Theorem 6.15. The period is 2, 4, 4, 8; series are shifted slightly upwards where they coincide. The values agree with the exact search of Theorem 6.7 in 275 cases (49 values of λ). The lab draws it for your λ.

Figure 3



The excess $\ell_{\mathbb{Q}}(\lambda I_m) - m$ over (m, τ). Only $\tau(1-\lambda^2)$, the number of rational squares needed for $\sin^2\theta$ with $\cos\theta = \lambda$, enters. Turn it in 3D in the lab.

So for scalar matrices everything is decided by $\tau(\sin^2\theta)$, with $\cos\theta = \lambda$: by Legendre, by the level of L, and by the splitting of 2 in L, which are three forms of the same condition. For $\lambda = \frac{3}{4}$ this recovers $\ell_{\mathbb{Q}}(\frac{3}{4}I_4) = 8$ and $d_{\mathbb{Q}} = 4$ (Proposition 4.3).

Example 6.16. p. 18

black!35↗

The determinant does not decide in general. Let $H = \lambda I + (1-\lambda)vv^{\top}/|v|^2$ with $v = (0,2,2)$ and $\lambda = \frac{5}{8}$, so $q = v^{\perp}$, $\det q \equiv 2$ and $\delta \equiv 39$. Lemma 6.4 and Proposition 6.5 give $\ell_{\mathbb{Q}} \geq 6$, while Theorem 6.7 gives $\ell_{\mathbb{Q}}(H) = 7$: the obstruction sits at the prime 2, which splits in $\mathbb{Q}(\sqrt{-39})$, through condition (2). The Springer residues of Theorem 4.1 at the primes of $\mathbb{Q}[t]$ also give 7. In 120 members of the family $H = \lambda I + (\mu-\lambda)vv^{\top}/|v|^2$ with $\mu = \pm 1$ (three of them H_n, the others random with $n \leq 9$, $v \in \{-3,\dots,3\}^n$ and $\lambda = a/b$, $2 \leq b \leq 8$), the determinant bound is sharp in 102; in the other 18 the excess is 4 or 5 instead of at most 3, always through a split prime.

↳ Used in: 3 (p. 41)

7 Complete graphs

Let $H_n = (J-I)/(n-1)$, the normalized complete graph, with eigenvalues 1 and $\lambda = -1/(n-1)$, the latter of multiplicity $n-1$. So $\ell_{\mathbb{R}}(H_n) = n$ for odd n and $n+1$ for even $n \geq 4$. Note that $H_n = \frac{1}{2}A_{K_n}$ only for $n = 3$. For a positive rational s let $\tau(s)$ be the least number of rational squares with sum s. By the theorems of two, three and four squares, $\tau(s) \leq 4$ and it is read off the factorization of s.

Theorem 7.1. p. 19

black!35↗

Kn_Witness.witness_H5, Kn_Witness.witness_H7, Kn_Witness.plane_in_four_squares, Kn_Witness.two_squares_over_L, Kn_Witness.quaternion_pure_norm, Kn_Witness.seven_mod_8_rat $\ell_{\mathbb{Q}}(H_2) = 2$. *For odd* $n \geq 3$,

$$\ell_{\mathbb{Q}}(H_n) = \begin{cases} n & \text{if } n \text{ or } n-2 \text{ is a square,} \\ n+3 & \text{otherwise, if } n \equiv 3,5 \pmod 8, \\ n+5 & \text{otherwise, if } n \equiv 1,7 \pmod 8, \end{cases}$$

and the defect $d_{\mathbb{Q}}(H_n)$ *is* 0 *in the first case and* 2 *in the others. For even* $n \geq 4$, *let* s *be the one of* $n, n-2$ *divisible by* 4. *Then* $\ell_{\mathbb{Q}}(H_n) = n + \tau(s)$ *and* $d_{\mathbb{Q}}(H_n) = 1$.

Isabelle · ours · part **show**

Only a part is in Isabelle: the named pieces are machine-checked; the statement as a whole is not marked as formalized in the paper

witness_H5 · Isabelle/AFP/Biquadratic_SOS_Length/Kn_Witness.thy, line 19

```
lemma witness_H5:
  fixes x1 x2 y1 y2 y3 y4 y5 :: "'a::comm_ring_1"
  shows
    "(4 * x1 * y1 + x2 * ((-1) * y2 + 3 * y3 + 2 * y4))^2 +
    (4 * x1 * y2 + x2 * (3 * y1 + (-1) * y4 + 2 * y5))^2 +
    (4 * x1 * y3 + x2 * ((-1) * y1 + 2 * y2 + 1 * y4 + 2 * y5))^2 +
    (4 * x1 * y4 + x2 * (3 * y2 + 1 * y3))^2 +
    (4 * x1 * y5 + x2 * (2 * y1 + 2 * y4))^2 +
    (x2 * ((-1) * y1 + (-1) * y2 + 1 * y3 + (-1) * y4 + 2 * y5))^2 +
    (x2 * (1 * y1 + 1 * y2 + 1 * y3 + (-1) * y4 + (-2) * y5))^2 +
    (x2 * ((-2) * y3 + 2 * y4))^2 =
    16 * ((x1^2 + x2^2) * (y1^2 + y2^2 + y3^2 + y4^2 + y5^2)) + 16 * (x1 * x2 * (y1 * y2
+ y1 * y3 + y1 * y4 + y1 * y5 + y2 * y3 + y2 * y4 + y2 * y5 + y3 * y4 + y3 * y5 + y4 *
y5))"
```

witness_H7 · Isabelle/AFP/Biquadratic_SOS_Length/Kn_Witness.thy, line 35

```
lemma witness_H7:
  fixes x1 x2 y1 y2 y3 y4 y5 y6 y7 :: "'a::comm_ring_1"
  shows
    "(12 * x1 * y1 + x2 * (12 * y2))^2 +
    (12 * x1 * y2 + x2 * ((-8) * y1 + 4 * y3 + 4 * y4 + 4 * y5 + 4 * y6 + 4 * y7))^2 +
    (12 * x1 * y3 + x2 * (4 * y1 + 10 * y4 + 1 * y5 + 1 * y6 + (-4) * y7))^2 +
    (12 * x1 * y4 + x2 * (4 * y1 + (-6) * y3 + 3 * y5 + 3 * y6 + 8 * y7))^2 +
    (12 * x1 * y5 + x2 * (4 * y1 + 3 * y3 + 1 * y4 + 2 * y6 + 2 * y7))^2 +
    (12 * x1 * y6 + x2 * (4 * y1 + 3 * y3 + 1 * y4 + 2 * y5 + 2 * y7))^2 +
    (12 * x1 * y7 + x2 * (4 * y1 + 8 * y3 + (-4) * y4 + 2 * y5 + 2 * y6))^2 +
    (x2 * ((-5) * y5 + 5 * y6))^2 +
    (x2 * ((-2) * y5 + 2 * y6))^2 +
    (x2 * ((-1) * y5 + 1 * y6))^2 +
    (x2 * (1 * y3 + 1 * y4 + 4 * y5 + (-8) * y6 + 2 * y7))^2 +
    (x2 * (3 * y3 + 3 * y4 + (-8) * y5 + (-4) * y6 + 6 * y7))^2 =
    144 * ((x1^2 + x2^2) * (y1^2 + y2^2 + y3^2 + y4^2 + y5^2 + y6^2 + y7^2)) + 96 * (x1
* x2 * (y1 * y2 + y1 * y3 + y1 * y4 + y1 * y5 + y1 * y6 + y1 * y7 + y2 * y3 + y2 * y4 +
y2 * y5 + y2 * y6 + y2 * y7 + y3 * y4 + y3 * y5 + y3 * y6 + y3 * y7 + y4 * y5 + y4 * y6
+ y4 * y7 + y5 * y6 + y5 * y7 + y6 * y7))"
```

plane_in_four_squares · Isabelle/AFP/Biquadratic_SOS_Length/Kn_Witness.thy, line 68

```
lemma plane_in_four_squares:
  fixes a b c d e f g h :: "'a::comm_ring_1"
  assumes "a * e + b * f + c * g + d * h = 0"
  shows "(a^2 + b^2 + c^2 + d^2) * (e^2 + f^2 + g^2 + h^2) =
    (a * f - b * e - c * h + d * g)^2 + (a * g + b * h - c * e - d * f)^2 + (a * h - b *
g + c * f - d * e)^2"
```

two_squares_over_L · Isabelle/AFP/Biquadratic_SOS_Length/Kn_Witness.thy, line 216

```
lemma two_squares_over_L:
  fixes n j :: "'a::field_char_0"
  assumes "j^2 = - (n * (n - 2))"
  shows "((n + j) / 2)^2 + ((n - j) / 2)^2 = n"
```

quaternion_pure_norm · Isabelle/AFP/Biquadratic_SOS_Length/Kn_Witness.thy, line 235

```
lemma quaternion_pure_norm:
  fixes a b c d p q r :: "'a::comm_ring_1"
  shows "(- b * p - c * q - d * r)^2 + (a * p + c * r - d * q)^2
       + (a * q - b * r + d * p)^2 + (a * r + b * q - c * p)^2
       = (a^2 + b^2 + c^2 + d^2) * (p^2 + q^2 + r^2)"
```

seven_mod_8_rat · Isabelle/AFP/Biquadratic_SOS_Length/Kn_Witness.thy, line 193

```
lemma seven_mod_8_rat:
  fixes x y z :: rat and c :: int
  assumes c: "c mod 8 = 7"
  shows "x^2 + y^2 + z^2 \<noteq> of_int c"
```

🆕 **Classical and new:** not found in the literature so far (searches of 6-nov-2026); not a proof of novelty

↳ Used in: Proposition 7.4 (p. 33)

💡 **In plain words (commentary, not part of the paper)**

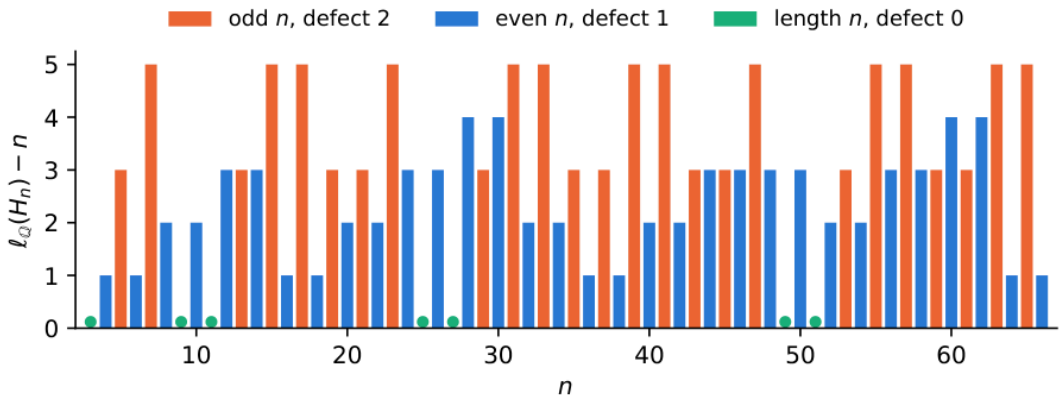
Put the same small weight on every bond of a complete graph with an odd number n of sites. Over the reals, n squares always suffice. Over the rationals they suffice exactly when n or $n-2$ is a perfect square: $3, 9, 11, 25, 27, 49, 51, \ldots$ The obstruction to the other values is a discriminant, and the two families are rescued by quaternions and by Pfister forms.

n	3	4	5	6	7	8	9	10	11	12	13	15	17	28
$\ell_{\mathbb{R}}(H_n) - n$	0	1	0	1	0	1	0	1	0	1	0	0	0	1
$d_{\mathbb{Q}}(H_n)$	0	1	2	1	2	1	0	1	0	1	2	2	2	1
$\ell_{\mathbb{Q}}(H_n) - n$	0	1	3	1	5	2	0	2	0	3	3	5	5	4

Table 2: Real excess, defect and rational excess. In this family the defect, the excess rank of a rational Gram matrix, never exceeds 2; the length depends on how the residual form sits in a sum of squares.

Colour: blue shade = the number's size within its column.

🖼️ **Figure 4**



Excess $\ell_{\mathbb{Q}}(H_n) - n$ for $3 \le n \le 66$. The lab checks any n, with an exact Paley witness.

7.1 Reduction

In this section the letters m and k have their own meaning, $n = 2m + 1$ for odd n and $k = n(n-2)$, not that of Section 6. Let e be the all-one vector, $V = e^{\perp}$ with form q, and $\delta = 1 - \lambda^2 = n(n-2)/(n-1)^2$. Then $q \perp \langle n \rangle \cong I_n$, where $I_j = j\langle 1 \rangle$, so $\det q = n$ modulo squares. Take T, D as in Proposition 2.1, with D of height h, and let $n \ge 3$. Since $\langle Te, e \rangle = \langle He, e \rangle = |e|^2$ and $|Te|^2 + |De|^2 = |e|^2$, we get $Te = e$, $De = 0$ and $T^{\top} e = e$. So $T|_V = \lambda + S$ with S skew, and $\Delta = I - T^{\top} T|_V = \delta + S^2 \ge 0$. Put $U = \ker \Delta$, $W = \operatorname{im} \Delta$, $d = \dim W$. These are rational, orthogonal and S-stable, and D embeds the residual form $r = q(\Delta \cdot, \cdot)|_W$ isometrically in I_h. Conversely such data on V give T, D. As in Theorem 5.1, U is a sum of planes $\langle a, a\delta \rangle$, so $\dim U$ is even and $\det q_U = \delta^{\dim U/2}$. The characteristic polynomial of $S|_W$ is $X^{\epsilon} P(X^2)$ with $\epsilon \equiv d \pmod 2$, so $\det(\delta + S^2)|_W = \delta^{\epsilon} P(-\delta)^2$, and modulo squares

$$\det r = n\, \delta^{(n-1-d)/2+\epsilon}. \quad (2) \tag{7}$$

7.2 The auxiliary space

Put $k = n(n-2)$, so $\delta \sim k$, and $L = \mathbb{Q}(\sqrt{-k})$, with $j^2 = -k$.

Proposition 7.2. (the case $q = e^{\perp}$ of Theorem 6.2) p. 20

black!35↗

Prop_Aux.prop_aux $\ell_{\mathbb{Q}}(H_n) \le n + h$ if and only if there is a subspace $p \subseteq I_h$ with $(q \perp p)_L$ hyperbolic. In that case one may take $d_{\mathbb{Q}}(H_n) \le \dim p$.

Isabelle · ours · part **show**

Only a part is in Isabelle: the named pieces are machine-checked; the statement as a whole is not marked as formalized in the paper

`prop_aux` · `Isabelle/LengthsPlaneRotations/LengthsPropAux/Prop_Aux.thy`, line 914

```
theorem prop_aux:
  assumes witt_normalization:
    "\<And>A B::rat^'n^('n + 'h). repr_Q (Hn::rat^'n^'n) A B
        \<Longrightarrow> \<exists>B'. repr_Q (Hn::rat^'n^'n) (iota_mat::rat^'n^('n +
'h)) B'"
  shows "len_le (TYPE('n + 'h)) (Hn::rat^'n^'n) \<longleftrightarrow> (\<exists>p.
lin_sub p \<and> hyp (Vset p))"
```

↳ Not used by another result of the paper.

Proof

If $(q \perp p)_L$ is hyperbolic, the positive form $q \perp p$ is a sum of planes $\langle a, a\delta\rangle$, by the extraction in Theorem 5.1, so it carries an isometry R with $\operatorname{sym} R = \lambda$. Extend R by the identity on e and on $p^{\perp} \subseteq I_h$, and compress to the first n coordinates. Then $\operatorname{sym} T = H_n$ and the columns leave $\mathbb{Q}^n$ only inside p, so $\operatorname{rank} D \le \dim p$. Conversely, take $p = D(W) \cong r$. With $\iota^2 = -\delta$ in L and the bilinear adjoint, which fixes ι, we have $q((\iota + S)x, (\iota + S)y) = -q(\Delta x, y)$ on W_L, and $\iota + S$ is invertible as $\Delta|_W$ is. So $W_L \cong -r_L$, and since U_L is hyperbolic, so is $(q \perp p)_L$.

Three facts suffice. Beyond the theorems of two, three and four squares, the proof needs neither Meyer's theorem nor Hasse–Minkowski.

1. I_8 is hyperbolic over L: a rational quaternion of norm k gives $I_4 \cong kI_4$, and $\langle k\rangle_L = \langle -1\rangle_L$.
2. If k is a sum of three squares, I_4 is hyperbolic over L: with j this gives an isotropic vector, and I_4 is a Pfister form.
3. Over L, $nI_2 \cong I_2$, since $n = (\frac{n+j}{2})^2 + (\frac{n-j}{2})^2$ for $j^2 = -k$. Also $\langle n - 2\rangle_L = \langle -n\rangle_L$.

7.3 Odd $n = 2m + 1$: length n

Here d is even and $\epsilon = 0$. If $h = 0$ then (2) reads $n \sim \delta^m$, so n is a square for m even and $n - 2$ is a square for m odd. Conversely, if $n = s^2$ then $n \equiv 1 \pmod 8$ and $[q_L] = [I_{n-1}] = 0$ by (F1). If $n - 2 = a^2$ then $n \equiv 3 \pmod 8$, $k \sim n$ and $k \equiv 3 \pmod 8$, so $\langle n\rangle_L = \langle -1\rangle_L$ and $[q_L] = [I_{n+1}] = 0$ by (F2), as $4 \mid n + 1$. Over $\mathbb{Q}$, this case is also an instance of [4 , Corollary 9.2] .

7.4 Odd n: lower bounds

Suppose neither is a square. Then $d \ge 2$ by the previous step. For $d = 2$, (2) gives $\det r \sim c$, with $c = n - 2$ for m even and $c = n$ for m odd; in both cases $c \equiv 3 \pmod 4$. A plane in I_2 has square determinant, so $h \ge 3$. If $n \equiv 1, 7 \pmod 8$ then $c \equiv 7 \pmod 8$. For orthogonal v, w in the quaternions, $\bar{v}w$ is pure of norm $N(v)N(w)$, so the determinant of a plane in I_4 is a sum of three squares. This excludes c, and $d = 2$ forces $h \ge 5$. If $d = h = 4$ the determinant of r would be a square, which by (2) is again $n \sim \delta^m$. So $h \ge 5$ for these n.

7.5 Odd n: upper bounds

We apply Proposition 7.2. If $n \equiv 7 \pmod 8$ take $p = \langle 1, n\rangle \subset I_5$, by four squares for n. Then $[q_L] + [p_L] = [I_{n+1}] = 0$ by (F1).

If $n \equiv 1 \pmod 8$ take $p = \langle n, k\rangle$. Then $[q_L] + [p_L] = [I_n] + [\langle -1\rangle] = [I_{n-1}] = 0$. To embed p in $I_5 = \mathbb{H}_{\mathbb{Q}} \perp \langle 1\rangle$, take a quaternion x of norm n and a pure quaternion z of norm $(3n - 8)/4$, which exists because $3n - 8 \equiv 3 \pmod 8$. The vectors $(x, 0)$ and $(xz, n/2)$ are orthogonal, of norms n and $n(3n - 8)/4 + n^2/4 = k$.

If $n \equiv 3,5 \pmod 8$ then $c \equiv 3 \pmod 8$ is a sum of three squares, so $I_3 = \langle c\rangle \perp p$ with p binary, and

$$[q_L] + [p_L] = [I_{n+3}] - [\langle n, c\rangle].$$

If $n \equiv 5$ then $c = n-2$, the form $\langle n, c\rangle_L$ is hyperbolic by (F3), and $8 \mid n+3$. If $n \equiv 3$ then $c = n$ and $k \equiv 3 \pmod 8$, so I_4 vanishes by (F2), and what remains is $[I_2] - [nI_2] = 0$ by (F3). So $h \le 3$. In all these cases, outside the square cases, $\dim p = 2$, and $d_{\mathbb{Q}}(H_n) = 2$ because $d = 0$ is excluded.

7.6 Even $n \geq 4$

Now d is odd and $\epsilon = 1$. Let c be the element of $\{n, n-2\}$ other than s, so $c \equiv 2 \pmod 4$ and $\delta \sim sc$. If $d = 1$, (2) gives $\det r \sim s$, so $h \geq \tau(s)$. If $d = h = 3$ then $\det r \sim c$ would be a square, which it is not. Since $\tau(s) \le 4$, this gives $h \geq \tau(s)$ in all cases.

For the converse take $p = \langle s\rangle \subset I_{\tau(s)}$. If $s = n$ then $[q_L] + [p_L] = [I_n]$. If $s = n-2$ then $\langle s\rangle_L = \langle -n\rangle_L$ and $[q_L] + [p_L] = [I_n] - [nI_2] = [I_{n-2}]$ by (F3). So the class is $[I_s]$. If $8 \mid s$ it vanishes by (F1). If $s \equiv 4 \pmod 8$ then $k = 4 \cdot 2m$ with m odd, a sum of three squares, and it vanishes by (F2). Here $\dim p = 1$, so the defect is 1. For $n = 2$, H_2 itself is orthogonal. □

Example 7.3. p. 21

The bound $\ell_{\mathbb{Q}}(H_5) \le 8$ has a short certificate. With $A = \binom{I_5}{0}$ and $B = C/4$, where

$$C^{\top} = \begin{pmatrix} 0 & 3 & -1 & 0 & 2 & -1 & 1 & 0 \\ -1 & 0 & 2 & 3 & 0 & -1 & 1 & 0 \\ 3 & 0 & 0 & 1 & 0 & 1 & 1 & -2 \\ 2 & -1 & 1 & 0 & 2 & -1 & -1 & 2 \\ 0 & 2 & 2 & 0 & 0 & 2 & -2 & 0 \end{pmatrix},$$

one checks $C^{\top}C = 16I$ and that the top 5×5 block C_0 has $C_0 + C_0^{\top} = 2(J - I)$. The last three rows of C have rank two, so the Gram matrix of the columns of $(A\ B)$ has rank 7.

↳ Not used by another result of the paper.

7.7 Tournaments

The second family of length n has a known explicit form. Bailey and Craigen [1 , Theorem 4.2] build, for a doubly regular tournament with adjacency matrix A on $q \neq 3$ vertices, the real matrices $M = \alpha A + J - I$ with zero diagonal and $MM^{\top} = cI$, $\alpha = -2(q - 2 \pm \sqrt{q-2})/(q-3)$. When $q - 2 = a^2$ the number α is rational, and the matrix is a scalar multiple of the following one, with $S = 2A - J + I$ or its transpose. The only additions here are that remark and the value of the symmetric part.

Proposition 7.4. (after Bailey–Craigen) p. 22

black!35↗

Tournament_Orthogonal.bailey_craigen Let $n - 2 = a^2$ and let S be the skew matrix of a doubly regular tournament on n vertices, so $SS^{\top} = nI - J$ [33 , 14] and $SJ = 0$. Then

$$T = \frac{J - I + aS}{n-1}$$

is rational orthogonal with $\operatorname{sym} T = H_n$.

Isabelle · ours · part **show**

Only a part is in Isabelle: the named pieces are machine-checked; the statement as a whole is not marked as formalized in the paper

`bailey_craigen` · `Isabelle/AFP/Biquadratic_SOS_Length/Tournament_Orthogonal.thy`, line 228

```
theorem bailey_craigen:
  fixes S :: "real^'n::finite^'n" and a :: real
  assumes skew: "transpose S = - S" and SJ: "S ** Jmat = 0" and JS: "Jmat ** S = 0"
```

```
    and SSt: "S ** transpose S = real CARD('n) *\<^sub>R mat 1 - Jmat"
    and a2: "a\<^sup>2 = real CARD('n) - 2" and n2: "2 \<le> CARD('n)"
  defines "N \<equiv> Jmat - mat 1 + a *\<^sub>R S"
    and "T \<equiv> (1 / (real CARD('n) - 1)) *\<^sub>R (Jmat - mat 1 + a *\<^sub>R S)"
  shows "N ** transpose N = (real CARD('n) - 1)\<^sup>2 *\<^sub>R mat 1"
    and "transpose N ** N = (real CARD('n) - 1)\<^sup>2 *\<^sub>R mat 1"
    and "orthogonal_matrix T"
    and "(1 / 2) *\<^sub>R (T + transpose T) = (1 / (real CARD('n) - 1)) *\<^sub>R (Jmat
- mat 1)"
```

🆕 **Classical and new:** Theorem 4.2 of Bailey and Craigen up to a scalar; only the rationality remark and the symmetric part are added

↳ Not used by another result of the paper.

Proof

With $N = J - I + aS$ we get
$NN^\top = (J-I)^2 + a^2(nI - J) = (n-2)J + I + (n-2)(nI - J) = (n-1)^2 I.$

For prime $n \equiv 3 \pmod 4$ the Paley tournament applies: $n = 3, 11, 83, 227$. Theorem 7.1 also gives rational solutions when no tournament is involved, as for $n = 9$.

8 Integer length

Theorem 8.1. p. 22

black!35↗

Huckel_SOS.integer_representation_degree, IL_Formula.integer_length Let G be a finite simple graph. If G has a vertex of degree at least three, then $\ell_{\mathbb{Z}}(G) = \infty$. Otherwise

$$\ell_{\mathbb{Z}}(G) = n + p + (z \bmod 2),$$

with p the number of path components with at least two vertices and z the number of isolated vertices.

Isabelle · ours · part **show**

Only a part is in Isabelle: the named pieces are machine-checked; the statement as a whole is not marked as formalized in the paper

`integer_representation_degree` · `Isabelle/AFP/Biquadratic_SOS_Length/Huckel_SOS.thy`, line 722

```
theorem integer_representation_degree:
  fixes A B :: "real^'n^'r" and H :: "real^'n^'n"
  assumes symH: "sym_mat H" and r: "represents A B H"
    and iA: "integer_mat A" and iB: "integer_mat B"
  shows "card {j. (H + H) $ i $ j \<noteq> 0} \<le> 2"
```

↳ Used in: Theorem 9.1 (p. 35)

Proof

As in Yiu [38 , § 1] , an integer column of norm one is $\pm e_k$. So the columns of A and B are signed coordinate vectors, at distinct coordinates by orthogonality, and $T = A^\top B$ is a signed partial permutation matrix: each row and column has at most one nonzero entry. Thus each row of $T + T^\top = A_G$ has at most two nonzero entries.

Moreover $r = 2n - \mathrm{nnz}(T)$ for the coordinates actually used. Each edge needs exactly one nonzero entry among T_{ij}, T_{ji}. A pair $T_{ij} = -T_{ji} \neq 0$ on a non-edge uses a free row and a free column at both vertices, which only isolated vertices have. So $\mathrm{nnz}(T) \leq |E| + 2\lfloor z/2 \rfloor$, where z is the number of isolated vertices. Equality is attained: orient each cycle and each path, so

that each edge carries one entry, and pair the isolated vertices by quarter turns; unused indices of the two families go to distinct coordinates. Since $|E|$ is n minus the number of path components, isolated vertices included, this gives the formula.

In plain words (commentary, not part of the paper)

With integer coefficients a rigid list can only send each site to one coordinate, with a sign. So each site can be joined to at most two others, and only rings and chains survive. A star has no integer representation at all, however many squares are allowed.

Remark 8.2. p. 22

$K_{1,4}$ and $C_4 \sqcup K_1$ have the same spectrum $2, 0, 0, 0, -2$ and the same real length 6, but $\ell_{\mathbb{Z}}(K_{1,4}) = \infty$ and $\ell_{\mathbb{Z}}(C_4 \sqcup K_1) = 6$. Thus integer sums of squares separate some cospectral graphs. For $K_{1,4}$ rational coefficients suffice: in the orthonormal basis given by a Hadamard matrix of order four divided by two, H is a swap plus three zeros, so $\ell_{\mathbb{Q}} = 6$.

↳ Not used by another result of the paper.

9 The first gaps

Theorem 9.1. p. 23

black!35↗

For $H = \frac{1}{2}A$ with $G = P_2 \sqcup K_1$: $\ell_{\mathbb{R}}(G) = 4$ and $\ell_{\mathbb{Q}}(G) = 5$. Every representation by four squares has T with an entry $\pm\sqrt{3}/2$.

↳ Used in: 9.2 (p. 35)

Proof

By Proposition 2.1, four squares mean $T = H + S$ with S skew and $\operatorname{rank}(I - T^\top T) \le 1$. Take $H_{12} = H_{21} = \frac{1}{2}$ and write $S_{12} = p$, $S_{13} = q$, $S_{23} = r$. A Gröbner basis of the 2×2 minors of $I - T^\top T$ contains $r(r^2-1)(4r^2-3)$, $p(r^2-1)$, $qr(r^2-1)$, $4p^2 + 12r^4 - 9r^2$ and $4q^2 - 20r^4 + 19r^2 - 3$. If $r = \pm 1$ then $4p^2 = -3$. If $r = 0$ then $p = 0$, $q^2 = 3/4$. If $4r^2 = 3$ then $p = q = 0$. These five polynomials lie in the ideal of the minors, so every real solution is among the four points found this way, and at each of the four $I - T^\top T$ is positive semidefinite of rank exactly one, with eigenvalues $1, 0, 0$; so there are exactly four real solutions, each with an entry $\pm\sqrt{3}/2$. The rank zero case does not occur, as the entries of $I - T^\top T$ generate the unit ideal. The basis is computed in SymPy with the lexicographic order $p{>}q{>}r$, and the membership of the five polynomials, a failing control ($r(r^2-1)$ is not in the ideal) and the ranks at the four points are checked by `certificados_paper/numeros.py`. Finally $\ell_{\mathbb{Q}} \le \ell_{\mathbb{Z}} = 5$ by Theorem 8.1.

In plain words (commentary, not part of the paper)

Two bonded sites and one lone site need four real squares, and all such representations are known: exactly four, each containing $\sqrt{3}/2$. That number is $\sin(\pi/3)$, the sine of the rotation whose cosine is the level $\frac{1}{2}$. Over the rationals one more square is needed.

Remark 9.2. p. 23

black!35↗

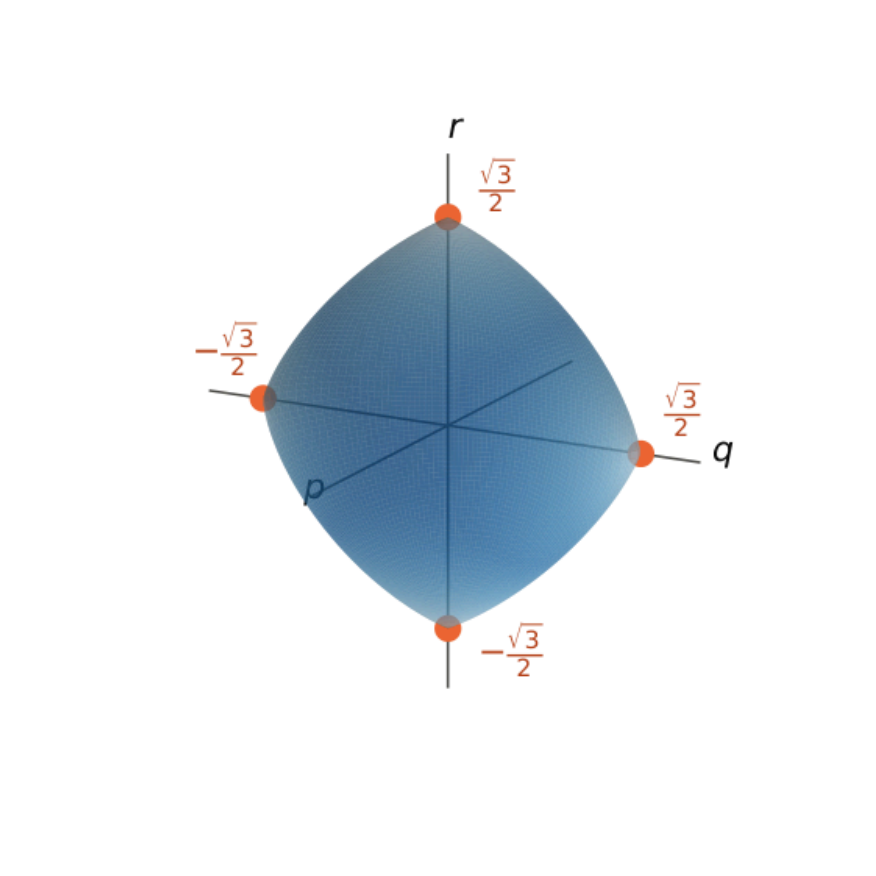
With $(u, v) = (x_1, x_2)$ and $(A, B, C) = (y_1, y_2, y_3)$ the form of Theorem 9.1 is

$$(Au + Bv)^2 + (Av)^2 + (Bu)^2 + (Cu)^2 + (Cv)^2,$$

five integer squares on a 3×2 strip. This is the display (18) of Lebedev [22] . That five such squares reduce to four real ones is the strip bound of Löfberg and Qi [25 , Lemma B.1] , and Lebedev's formula (19) gives four explicit squares with coefficients in $\mathbb{Q}(\sqrt{3})$. So $\ell_{\mathbb{R}} \leq 4$ is not new. Theorem 9.1 adds that $\sqrt{3}$ cannot be avoided: every four-square representation has it, and over $\mathbb{Q}$ the five squares above are optimal. The two bounds are also checked in Lean: four real squares, and no four rational bilinear forms with nonnegative rational weights.

↳ Not used by another result of the paper.

Figure 5



The body of contractions $T = H + S$ with $\operatorname{sym} T = H$ for $P_2 \sqcup K_1$, in the coordinates (p, q, r) of S. Every point of it gives a representation; rational points give rational ones. Only the four tips, at distance $\sqrt{3}/2$ from the origin, have defect of rank one, and none is rational. Turn it in 3D in the lab, and test your own rational point.

The level $\frac{1}{2} = \cos(\pi/3)$ gives $\sin(\pi/3) = \sqrt{3}/2$; compare Remark 5.2.

Example 9.3. (One variable y) p. 23

For $n = 1$ and $H = (\lambda)$, Proposition 2.1 forces $T = \lambda$, so $\ell_{\mathbb{Q}}(\lambda)$ is one plus the number of rational squares needed for $1 - \lambda^2$. For $\lambda = \frac{1}{2}$ the form is $x_1^2 + x_1 x_2 + x_2^2$ and $\frac{3}{4}$ needs three squares: $\ell_{\mathbb{R}} = 2$ and $\ell_{\mathbb{Q}} = 4$. For $\lambda = \frac{3}{4}$ the residue $\frac{7}{16}$ needs four squares, so $\ell_{\mathbb{Q}} = 5$. In general $T = H$ gives $\ell_{\mathbb{Q}}(H) \leq n + \ell(I - H^2)$, where ℓ is the number of rational squares of linear forms needed for the positive semidefinite form $I - H^2$.

↳ Not used by another result of the paper.

Example 9.4. p. 23

For $P_2 \sqcup P_2$, $\ell_{\mathbb{R}} = 4$. Each $E_{\pm 1/2}$ is the plane $\langle 2, 2 \rangle$, of signed discriminant $-1 \notin \{1, -3\}$, so $\ell_{\mathbb{Q}} \neq 4$, and Corollary 5.4 excludes 5. Thus $\ell_{\mathbb{Q}} = \ell_{\mathbb{Z}} = 6$.

↳ Not used by another result of the paper.

Proposition 9.5. p. 23

black!35↗

For the forest $\Gamma = 4P_6 \sqcup 3P_5$ on 39 vertices, $\ell_{\mathbb{Q}}(\Gamma) = \ell_{\mathbb{Z}}(\Gamma) = 46$, so excess 7 already occurs for $H = \frac{1}{2}A$.

↳ Used in: 1 (p. 41)

Proof

Let $D_j = 1 + t^2 + \cdots + t^{2j}$. The shift embeds M_{P_j} in I_{j+1}, and the determinant identifies the complement, so $[M_{P_j}] = [I_{j+1}] - [\langle D_j \rangle]$. This gives 46 squares. If 45 sufficed, the complement of M_Γ in I_{45} would have rank 6 and class $-[\langle 1 \rangle] + 4[\langle D_6 \rangle] + 3[\langle D_5 \rangle]$. Work at the prime Φ_7, with residue field $L = \mathbb{Q}(\zeta_7)$. There $D_6 = (t^{14}-1)/(t^2-1) = \Phi_7\Phi_{14}$ has valuation one, and $D_5 = (t^{12}-1)/(t^2-1)$ is a unit with $D_5(\zeta_7) = -\zeta_7^{12} = -(\zeta_7^6)^2 \sim -1$, since $\zeta_7^{12} - 1 = \zeta_7^5 - 1$ and $(\zeta_7^5 - 1)/(\zeta_7^2 - 1) = -\zeta_7^5$ (checked as $D_5 + t^{12} \equiv 0 \bmod \Phi_7$). So the first residue is $-[\langle 1 \rangle] + 3[\langle -1 \rangle] = 4[\langle -1 \rangle] = [-I_4]$, and the second is $4[\langle \Phi_{14}(\zeta_7) \rangle]$, a scalar multiple of I_4. Both are anisotropic over L: as 2 has order 3 modulo 7, a place of L over 2 has completion the unramified cubic extension of $\mathbb{Q}_2$, and I_4, anisotropic over $\mathbb{Q}_2$, stays anisotropic over an extension of odd degree by Springer's theorem [21] ; a scalar multiple of an anisotropic form is anisotropic. The anisotropic dimension is $8 > 6$.

Example 9.6. (Weights) p. 24

For prescribed rational weights Theorem 5.1 decides length n. If the support is connected, the weights are positive and $\rho(H) < 1$, then length n is impossible: the Perron eigenvalue is interior and simple. For a star with k leaves and positive rational weights w_i in H, the eigenvalues are $\pm\|w\|$ and 0 with multiplicity $k-1$. So $\ell_{\mathbb{Q}}(H) = n$ exactly when $\|w\| = 1$ and k is odd: the centre is swapped with the unit vector w, and its complement in $\mathbb{Q}^k$ is I_{k-1} by cancellation, with quarter turns on pairs.

↳ Not used by another result of the paper.

10 Fields of definition

Over $\mathbb{R}$ the length is known, so one can ask for the fields over which it is attained.

Proposition 10.1. p. 24

black!35↗

Fields_Three_Quarter_I4.dilation_iff_seven, Fields_Three_Quarter_I4.no_rational_dilation, Fields_Three_Quarter_I4.real_dilation

1. *For $H = \frac{3}{4}I_4$ we have $\ell_{\mathbb{R}}(H) = 4$, and for a subfield $F \subseteq \mathbb{R}$, $\ell_F(H) = 4$ if and only if 7 is a sum of three squares in F. So $\mathbb{Q}(\sqrt{3})$ and $\mathbb{Q}(\sqrt{7})$ both work, $\mathbb{Q} = \mathbb{Q}(\sqrt{3}) \cap \mathbb{Q}(\sqrt{7})$ does not, and there is no least such field with respect to inclusion.*
2. *Let $p_1, \ldots, p_k$ be distinct primes and $\lambda_j = (p_j - 1)/(p_j + 1)$. For $H = \bigoplus_j \lambda_j I_2$, a field $F \subseteq \mathbb{R}$ has $\ell_F(H) = 2k$ if and only if it contains all $\sqrt{p_j}$.*

Isabelle · ours · part **show**

Only a part is in Isabelle: part (1): the dilation 3/4 inside I_4 over Q versus over R

`dilation_iff_seven` · `Isabelle/LevelQuadraticFields/Fields_Three_Quarter_I4.thy`, line 123 — the dilation 3/4 in I_4 exists iff 7 is a sum of three squares

```
theorem dilation_iff_seven:
  "(\<exists>T :: nat \<Rightarrow> nat \<Rightarrow> 'a::field_char_0. orth4 T \<and>
```

```
sym_part_is_3_4 T) \<longleftrightarrow> (\<exists>p q r :: 'a. p^2 + q^2 + r^2 = 7)"
```

no_rational_dilation · Isabelle/LevelQuadraticFields/Fields_Three_Quarter_I4.thy, line 145 — no rational dilation

```
corollary no_rational_dilation: "\<not> (\<exists>T :: nat \<Rightarrow> nat \
<Rightarrow> rat. orth4 T \<and> sym_part_is_3_4 T)"
```

real_dilation · Isabelle/LevelQuadraticFields/Fields_Three_Quarter_I4.thy, line 148 — a real dilation exists

```
corollary real_dilation: "\<exists>T :: nat \<Rightarrow> nat \<Rightarrow> real. orth4
T \<and> sym_part_is_3_4 T"
```

dilation_iff_seven · Isabelle/LevelQuadraticFields/Fields_Three_Quarter_I4.thy, line 123

```
theorem dilation_iff_seven:
  "(\<exists>T :: nat \<Rightarrow> nat \<Rightarrow> 'a::field_char_0. orth4 T \<and>
sym_part_is_3_4 T) \<longleftrightarrow> (\<exists>p q r :: 'a. p^2 + q^2 + r^2 = 7)"
```

no_rational_dilation · Isabelle/LevelQuadraticFields/Fields_Three_Quarter_I4.thy, line 145

```
corollary no_rational_dilation: "\<not> (\<exists>T :: nat \<Rightarrow> nat \
<Rightarrow> rat. orth4 T \<and> sym_part_is_3_4 T)"
```

real_dilation · Isabelle/LevelQuadraticFields/Fields_Three_Quarter_I4.thy, line 148

```
corollary real_dilation: "\<exists>T :: nat \<Rightarrow> nat \<Rightarrow> real. orth4
T \<and> sym_part_is_3_4 T"
```

Trust base: 🔒 kernel only — **only part of the statement is formal** (see the box). Isabelle: 6 results, no oracles

Proof: in this note · **Formalized:** Isabelle/HOL, by the author (public formalizations repository) · **Covers:** part: the named pieces are machine-checked; the statement as a whole is not marked as formalized in the paper · **Cite:** Theorem 6.15, p. 17, doi:10.5281/zenodo.24387751

↳ Not used by another result of the paper.

Proof

(1) If $T = \frac{3}{4} + S$ is orthogonal then $4Se_1 \perp e_1$ has norm 7, in three coordinates. Conversely, multiplication by a pure quaternion of norm 7 gives the skew matrix $4S$. Finally $7 = (\sqrt{7})^2 = 2^2 + (\sqrt{3})^2$, and 7 is not a sum of three rational squares.

(2) T commutes with H, so it preserves each plane. There it is orthogonal with symmetric part λ_j, so it is a rotation of cosine λ_j, with sine $2\sqrt{p_j}/(p_j + 1)$.

Example 10.2. p. 25

For $a = \pm 1$ and $H = aI + bJ$ with $c = a + nb \in [-1, 1]$, the matrix T is forced to be a on $e^{\perp}$ and c on e. So $\ell_{\mathbb{Q}}(H) = n + \tau(n(1 - c^2))$, with $\tau(0) = 0$. This is the case $m = 1$, $q = \langle n \rangle$, of Theorem 6.2. For $n = 4$, $a = 1$, $b = -\frac{1}{8}$ this gives $c = \frac{1}{2}$ and length 7.

↳ Not used by another result of the paper.

Remark 10.3. p. 25

A spectral bound follows from Theorem 5.1. On each interior component extract planes until the rest is anisotropic over the totally imaginary field L_p, of dimension at most 4 over F_p since $u(L_p) = 4$: a form of dimension 5 over L_p is isotropic at every non-archimedean completion, where the u-invariant is 4, and L_p has no real places, so it is isotropic by Hasse–Minkowski [26] . Take the rotation on the planes and $T = H$ on the rest. A positive rational form of dimension $b>0$ embeds in I_{b+3} by Lemma 6.1, so $\ell_{\mathbb{Q}}(H) \le n + 4\sum_p \deg p + 3$, the sum over the interior

factors of the characteristic polynomial. For $n \geq 2$ this improves the general bound $8n$ of [16] for these forms.

↳ Not used by another result of the paper.

11 Formal verification and certificates

The Isabelle/HOL statements are in fifteen sessions of the public repository, all checked without `quick_and_dirty`: `Biquadratic_SOS_Length`, `Rational_Gap` (for `witness_G` and the statement on 3), `Integer_Length`, `RationalSOSLengths` and `LevelQuadraticFields` for Section 6, `RationalHilbertSymbol`, `LengthsExample610`, `LengthsPlaneRotations`, `LengthsPropTenUpper` and `LengthsPropForestUpper`, and five partial ones, `LengthsPropAux`, `LocalAuxSigns`, `RealJump`, `LengthsLocalCriterion` and `LengthsOneCore`, in which a named assumption of a locale stands for a classical theorem that is not formalized (the extraction of planes over L for Proposition 7.2; Hilbert reciprocity and Chebotarev density for Lemma 6.6; Witt cancellation over $\mathbb{Q}$ for Theorem 3.1(2) and Corollary 5.4; Theorem 6.7, Theorem 6.2 and standard facts on Hilbert symbols for Corollary 6.8 and Theorem 6.9; the extraction of planes of Theorem 5.1 for the parity in Theorem 6.2). In the table, green rows are machine-checked statements, yellow rows are machine-checked under such a named assumption, blue rows are exact computations, and orange rows have a written proof only. One Lean 4 file with Mathlib, `Franja`, has the two bounds of Theorem 9.1. The exact computations use rational arithmetic only, each with controls that must fail, and one command repeats all of them. The last rows are the results with a written proof and no machine check. So the paper as a whole is not formally verified: green rows are machine-checked; yellow rows are machine-checked only relative to the named classical theorems; blue rows test statements on finitely many cases; and the core results of Section 6 beyond those rows, as well as Theorem 7.1, rest on the written proofs.

Result	Status
Prop. 2.1, (1)⇔(2) over $\mathbb{R}$	Isabelle: `represents_iff`
$\ell_{\mathbb{R}} = n \Rightarrow \det M$ square	Isabelle: `det_pencil_square`
Identities for cycle and path, all n	Isabelle
Path determinant not a square	Isabelle: `geometric_not_square`
Prop. 3.2 and paths	Isabelle: `chain_needs_more_than_n_squares`
Weighted identity	Isabelle: `weighted_ring_identity`
Thm. 8.1, degree bound	Isabelle: `integer_representation_degree`
Thm. 3.1, paired levels give n squares	Isabelle: `blocks_orthogonal`, `blocks_symmetric_part`
Prop. 7.4	Isabelle: `bailey_craigen`
Thm. 7.1, witnesses for H_5, H_7	Isabelle: `witness_H5`, `witness_H7`
Thm. 7.1, plane determinants in I_2, I_4	Isabelle: `plane_in_four_squares`
Facts (F3), quaternion embedding	Isabelle: `two_squares_over_L`, `quaternion_pure_norm`
$c \equiv 7 \pmod 8$ is no sum of three rational squares	Isabelle: `seven_mod_8_rat`
Prop. 4.4, 12 squares	Isabelle: `witness_G`
3 is no sum of two rational squares	Isabelle: `three_not_two_rational_squares`
Thm. 8.1, attained maximum of $\operatorname{nnz} T$, for unions of cycles and paths given as a list	Isabelle: `integer_length`

Thm. 6.9, Ex. 6.10, Prop. 6.11	exact procedure on the explicit H of orders 6 and 7; criterion against the procedure in 8008 cases; order 5 sampled
Thm. 3.1, the bordered matrix with the chosen μ	exact, 600 cases including eigenvalues near ± 1, with failing controls
Thm. 8.1, exact formula	exhaustive for graphs with $\Delta \leq 2$, up to 6 vertices
Thm. 7.1, case of length n	local criterion checked for odd $n \leq 401$
Witnesses for $n = 3, 9, 11, 83$	exact rational, independent checker
Thm. 7.1, upper bounds, $3 \leq n \leq 17$	exact witnesses, same rows and defect as stated
Thm. 9.1, four real squares	Lean: `Franja.real_four_squares`
Thm. 9.1, no four rational squares, also with weights	Lean: `Franja.not_rational_four_squares`
Thm. 9.1, exactly four real solutions	exact Gröbner computation
Rem. 9.2, the form is the strip (18) of [22]	exact computation
Prop. 4.4, witnesses and 2-adic data	exact computation
Thm. 6.7 on H_n, $3 \leq n \leq 66$, and Thm. 6.15, 275 cases	exact local search against the closed formulas, with failing controls
Lemma 6.4, planes in I_3 (Lagrange); Thm. 6.15, $\delta I_4 \cong I_4$; Prop. 6.5 for $d \leq 3$	Isabelle: `lagrange_three`, `quaternion_columns`, `skew_two`, `skew_three`
Lemma 6.14: $s(L) = 1$ iff $a = 1$, $s(L) = 2$ for $a \neq 1$, $a \not\equiv 7 \pmod 8$, $3 \leq s(L) \leq 4$ for $a \equiv 7 \pmod 8$	Isabelle: `level_one`, `level_two`, `level_ge3_le4`
Lemma 6.14: $s(L) = 4$ for $a \equiv 7 \pmod 8$	Isabelle: `level_four`, assuming Pfister's theorem that a level is never 3
Prop. 10.1(1), the dilation $\frac{3}{4}$ in I_4 over $\mathbb{Q}$ and over $\mathbb{R}$	Isabelle: `dilation_iff_seven`, `no_rational_dilation`, `real_dilation`
Lemma 6.6	Isabelle: `aux`, assuming the values of the Hilbert symbol, Hilbert reciprocity and Chebotarev density for an inert prime; a model shows the assumptions are consistent
Thm. 3.1(2) and Cor. 5.4	Isabelle: `real_part2`, `cor_jump`, assuming Witt cancellation over $\mathbb{Q}$
Thm. 6.2, algebraic core: $(\iota + S)^\top(\iota + S) = -\Delta$, kernel and range of Δ orthogonal and S-stable	Isabelle: `factor_transpose`, `kernel_orthogonal_range`, `range_stable`
Thm. 6.2, parity $\dim W \equiv m \pmod 2$	Isabelle: `range_dim_parity`, assuming the extraction of planes
Cor. 6.8 and Thm. 6.9 (both directions)	Isabelle: `cor_bounded`, `sharp`, assuming Thm. 6.7, Thm. 6.2 and Hilbert-symbol facts
Prop. 4.5, the upper bound $d_{\mathbb{Q}}(H) \leq 6$	Isabelle: `prop_ten_defect_le_6`, by an exact certificate
Prop. 9.5, the upper bound 46	Isabelle: `forest_upper_Q`
Ex. 6.10, $W^\top W$, the spectrum of H and the local data at 2 and 23	Isabelle: `example_6_10_witness`, with an executable Hilbert symbol
Thm. 5.1, the rotation on orthogonal planes of type λ	Isabelle: `orthogonal_planes_rotation`

Prop. 7.2	Isabelle: `prop_aux`; the direction from planes is unconditional, the statement assumes the extraction of planes over L, that a representation gives a hyperbolic form, and the normalization $A = (I; 0)$ of Prop. 2.1
Thm. 6.2, 6.7, 6.15, Lemmas 6.1, 6.4, Prop. 6.5	proved here; the isometry criterion is [4] ; not formalized beyond the rows above
Thm. 3.1, 4.1, 4.2, 5.1, 5.5, 7.1	proved here; not formalized beyond the rows above; Cor. 5.4 after [20]
Prop. 4.4 (lower bounds), 4.6, and the lower bounds of Prop. 4.5 and 9.5	proved here; not formalized

12 Questions

Question 1. p. 27

1. Is $\ell_{\mathbb{Q}}(H) - n$ bounded, equivalently is $d_{\mathbb{Q}}(H)$ bounded? For one interior eigenvalue it is at most 7, attained first in order 6 (Theorem 6.9, Proposition 6.11); for odd multiplicity it is at most 6, also attained (Example 6.12). In general the question is open. For the matrix G of Proposition 4.4, $\ell_{\mathbb{Q}}(G) - 5 = 7$, the forest of Proposition 9.5 has excess 7, and any bound on $d_{\mathbb{Q}}$ is at least 7.

↳ Not used by another result of the paper.

Question 2. p. 27

What is the rational length for two interior eigenvalues, for instance $H = aI + bJ$ with both eigenvalues interior, or normalized strongly regular graphs? Section 6 settles one interior eigenvalue. The components interact (Proposition 4.5): for its matrix we only know $16 \le \ell_{\mathbb{Q}} \le 18$: the contraction of that proposition has a defect form of rank 6, with square determinant and nontrivial Hasse invariant, which embeds in I_8 but not in I_7.

↳ Not used by another result of the paper.

Question 3. p. 27

For which q is the determinant bound of Section 6 sharp? It is for H_n (Remark 6.13) and for scalar matrices, and not always (Example 6.16).

↳ Not used by another result of the paper.

Question 4. p. 27

Is there a closed form for $d_{\mathbb{Q}}(H)$ in terms of the components h_p? The anisotropic dimensions of the h_p over L_p give bounds, but positive defect mixes components.

↳ Not used by another result of the paper.

Question

Formula sheet

1azulwhite

$\ell_{\mathbb{R}}(H)$	n **if interior multiplicities are even, else** $n+1$
$\ell_{\mathbb{Z}}(G)$	$n+p+(z \bmod 2)$, with p the paths with at least two vertices and z the isolated vertices; ∞ if $\Delta \geq 3$
$\ell_{\mathbb{Q}}(H)=n$	$h_p \otimes F(\sqrt{\lambda^2-1})$ hyperbolic for all $p \neq x \mp 1$
$\ell_{\mathbb{Q}}(H_n)$, n odd	n if n or $n-2$ a square; else $n+3$ ($n \equiv 3,5$), $n+5$ ($n \equiv 1,7$) mod 8
$\ell_{\mathbb{Q}}(H_n)$, $n \geq 4$ even	$n+\tau(s)$, $s \in \{n, n-2\}$, $4 \mid s$
$d_{\mathbb{Q}}(H_n)$	0 if $\ell_{\mathbb{Q}}(H_n)=n$; else 2 (odd n), 1 (even $n \geq 4$)
$\ell_{\mathbb{R}}=n$ and $\ell_{\mathbb{Q}} \leq n+1$	$\Rightarrow\ \ell_{\mathbb{Q}}=n$
$\ell_{\mathbb{Q}}(H)$	$\min\{r : (M_H)_F \hookrightarrow (I_r)_F\}$, $F=\mathbb{Q}(t)$
$\ell_{\mathbb{Q}}(H^{\oplus 8} \oplus K)$	$8n+\ell_{\mathbb{Q}}(K)$
$\det M$	$(1-(-t)^n)^2$; $(1+(-t)^n)^2$; $\sum_{j \leq n} t^{2j}$
$\ell_{\mathbb{R}}, \ell_{\mathbb{Q}}$ of $P_2 \sqcup K_1$	4, 5
$\ell_{\mathbb{Q}}(\lambda I_m)$, $\lambda \in \mathbb{Q} \cap (-1,1)$	$m+\min\big((-m) \bmod 2s,\ \tau(1-\lambda^2)\big)$, $s=1,2,4$ for $\tau=1$, 2 or 3, 4
$d_{\mathbb{Q}}(\lambda I_m)$	$\min(r, 2s-r)$, $r \equiv m \pmod{2s}$
$\ell_{\mathbb{Q}}(H) \leq n+h$, spectrum $\{-1,\lambda,1\}$, $\lambda \in \mathbb{Q} \cap (-1,1)$	$\exists\, p \subseteq I_h$ positive with $(q \perp p)_{\mathbb{Q}(\sqrt{-\delta})}$ hyperbolic

The companion site

This paper has a companion website, its *blueprint*, at https://karlesmarin.github.io/blueprints/real-rational-integer/. There one finds:

- *The statements.* Every theorem, proposition and lemma of the paper, with what it uses and where it is used.
- *The dependencies.* As a list and as a graph.
- *The map.* The results, the tools they rest on and the questions they answer.
- *Labs in the browser.* The body of contractions of Figure 5 in 3D; scalar dilations λI_m; the real length of your graph; its integer length; complete graphs with an exact Paley witness; the local test, prime by prime; loosening a bond.
- *Formal proofs.* For each statement, which part is checked in Isabelle/HOL or Lean and which is not.
- *The paper itself.* Its PDF, in English and in Spanish, opened at the right page from every statement.

Acknowledgements

We worked with an AI assistant. Drafts of the proofs were also read in AI-assisted referee-style rounds; this is neither independent peer review nor a machine check.

Tables

Every table of the paper, in its order: click one to unfold it, with where the paper cites it, how its numbers were checked, and its data as CSV. The typeset table is one click away, on its page of the PDF.

Table 1. Lengths in small cases. Orange: a gap between $\mathbb{R}$ and $\mathbb{Q}$ for graphs. Green: a cospectral pair separated over $\mathbb{Z}$. The rows H_5, H_7 are the normalized complete graphs of Section 7, whose entries are not half-integers.

white$G$	white$\ell_{\mathbb{R}}$	white$\ell_{\mathbb{Q}}$	white$\ell_{\mathbb{Z}}$
cycle C_n, $n \geq 3$	n	n	n
path P_n, $n \geq 2$	$n+1$	$n+1$	$n+1$
$P_2 \sqcup K_1$	4	5	5
$P_2 \sqcup P_2$	4	6	6
$K_{1,4}$	6	6	∞
$C_4 \sqcup K_1$	6	6	6
H_5	5	8	–
H_7	7	12	–

Colour: blue shade = the number's size within its column.

p. 3 in the PDF | ⬇ CSV | not cited in the text

Table without a number, in the text of §4 A global criterion

whiteform	whitefirst residue	whitesecond residue
I_r, p (constant)	$[I_r]$, $[p]$	0
aI_4	0	$[a'(\theta)I_4] = [I_4]$
$\langle b \rangle$	$[\langle b(\theta) \rangle] = [\langle -1 \rangle]$	0

⬇ CSV

Table without a number, in the text of §5 Length n and $n+1$

whitevalue ν	whitebefore	white$m' = m_g(\nu)$	whiteafter
$\nu = 1$	$e = 0$	m or $m+1$ (the free bit)	$e = m' - m$
interior, m even	e	m (as $m \pm 1$ is odd)	e
interior, m odd	$e = 0$	$m+1$ (as $m-1$ would give $e = -1$)	1
interior, m odd	$e = 1$	$m-1$ (as $m+1$ would give $e = 2$)	0
$\nu = -1$	e	$m+1-e$ (degree $n+1$)	1

⬇ CSV

Table without a number, in the text of §6 One interior eigenvalue

d	at such a v	at the other places
$0, 2$	excluded, as $d \geq d_{\mathbb{Q}}(H) = 4$	excluded
4	fails: the complement is a hyperbolic plane, with $w_v = +1 \neq w_v(q)$	the signs can be met
6	fails: $w_v(q \perp I_6) = -1$, while five hyperbolic planes have $+1$	–

Colour: red = no / fails; blue shade = the number's size within its column.

⬇ CSV

Table 2. Real excess, defect and rational excess. In this family the defect, the excess rank of a rational Gram matrix, never exceeds 2; the length depends on how the residual form sits in a sum of squares.

white$n$	white3	white4	white5	white6	white7	white8	white9	white10	white11	white12	white13
$\ell_{\mathbb{R}}(H_n) - n$	0	1	0	1	0	1	0	1	0	1	0
$d_{\mathbb{Q}}(H_n)$	0	1	2	1	2	1	0	1	0	1	2
$\ell_{\mathbb{Q}}(H_n) - n$	0	1	3	1	5	2	0	2	0	3	3

Colour: blue shade = the number's size within its column.

p. 20 in the PDF ⬇ CSV not cited in the text

Table without a number, in the text of §11 Formal verification and certificates

whiteResult	whiteStatus
Prop. 2.1, (1)⇔(2) over $\mathbb{R}$	Isabelle: `represents_iff`
$\ell_{\mathbb{R}} = n \Rightarrow \det M$ square	Isabelle: `det_pencil_square`
Identities for cycle and path, all n	Isabelle
Path determinant not a square	Isabelle: `geometric_not_square`
Prop. 3.2 and paths	Isabelle: `chain_needs_more_than_n_squares`
Weighted identity	Isabelle: `weighted_ring_identity`
Thm. 8.1, degree bound	Isabelle: `integer_representation_degree`
Thm. 3.1, paired levels give n squares	Isabelle: `blocks_orthogonal`, `blocks_symmetric_part`
Prop. 7.4	Isabelle: `bailey_craigen`
Thm. 7.1, witnesses for H_5, H_7	Isabelle: `witness_H5`, `witness_H7`
Thm. 7.1, plane determinants in I_2, I_4	Isabelle: `plane_in_four_squares`
Facts (F3), quaternion embedding	Isabelle: `two_squares_over_L`, `quaternion_pure_norm`
$c \equiv 7 \pmod 8$ is no sum of three rational squares	Isabelle: `seven_mod_8_rat`
Prop. 4.4, 12 squares	Isabelle: `witness_G`
3 is no sum of two rational squares	Isabelle: `three_not_two_rational_squares`
Thm. 8.1, attained maximum of $\operatorname{nnz} T$, for unions of cycles and paths given as a list	Isabelle: `integer_length`
Thm. 6.9, Ex. 6.10, Prop. 6.11	exact procedure on the explicit H of orders 6 and 7; criterion against the procedure in 8008 cases; order 5 sampled
Thm. 3.1, the bordered matrix with the chosen μ	exact, 600 cases including eigenvalues near ± 1, with failing controls
Thm. 8.1, exact formula	exhaustive for graphs with $\Delta \le 2$, up to 6 vertices
Thm. 7.1, case of length n	local criterion checked for odd $n \le 401$
Witnesses for $n = 3, 9, 11, 83$	exact rational, independent checker
Thm. 7.1, upper bounds, $3 \le n \le 17$	exact witnesses, same rows and defect as stated

Thm. 9.1, four real squares	Lean: `Franja.real_four_squares`
Thm. 9.1, no four rational squares, also with weights	Lean: `Franja.not_rational_four_squares`
Thm. 9.1, exactly four real solutions	exact Gröbner computation
Rem. 9.2, the form is the strip (18) of [Leb]	exact computation
Prop. 4.4, witnesses and 2-adic data	exact computation
Thm. 6.7 on H_n, $3 \le n \le 66$, and Thm. 6.15, 275 cases	exact local search against the closed formulas, with failing controls
Lemma 6.4, planes in I_3 (Lagrange); Thm. 6.15, $\delta I_4 \cong I_4$; Prop. 6.5 for $d \le 3$	Isabelle: `lagrange_three`, `quaternion_columns`, `skew_two`, `skew_three`
Lemma 6.14: $s(L) = 1$ iff $a = 1$, $s(L) = 2$ for $a \neq 1$, $a \not\equiv 7 \pmod 8$, $3 \le s(L) \le 4$ for $a \equiv 7 \pmod 8$	Isabelle: `level_one`, `level_two`, `level_ge3_le4`
Lemma 6.14: $s(L) = 4$ for $a \equiv 7 \pmod 8$	Isabelle: `level_four`, assuming Pfister's theorem that a level is never 3
Prop. 10.1(1), the dilation $\frac{3}{4}$ in I_4 over $\mathbb{Q}$ and over $\mathbb{R}$	Isabelle: `dilation_iff_seven`, `no_rational_dilation`, `real_dilation`
Lemma 6.6	Isabelle: `aux`, assuming the values of the Hilbert symbol, Hilbert reciprocity and Chebotarev density for an inert prime; a model shows the assumptions are consistent
Thm. 3.1(2) and Cor. 5.4	Isabelle: `real_part2`, `cor_jump`, assuming Witt cancellation over $\mathbb{Q}$
Thm. 6.2, algebraic core: $(\iota + S)^\top(\iota + S) = -\Delta$, kernel and range of Δ orthogonal and S-stable	Isabelle: `factor_transpose`, `kernel_orthogonal_range`, `range_stable`
Thm. 6.2, parity $\dim W \equiv m \pmod 2$	Isabelle: `range_dim_parity`, assuming the extraction of planes
Cor. 6.8 and Thm. 6.9 (both directions)	Isabelle: `cor_bounded`, `sharp`, assuming Thm. 6.7, Thm. 6.2 and Hilbert-symbol facts
Prop. 4.5, the upper bound $d_{\mathbb{Q}}(H) \le 6$	Isabelle: `prop_ten_defect_le_6`, by an exact certificate
Prop. 9.5, the upper bound 46	Isabelle: `forest_upper_Q`
Ex. 6.10, $W^\top W$, the spectrum of H and the local data at 2 and 23	Isabelle: `example_6_10_witness`, with an executable Hilbert symbol
Thm. 5.1, the rotation on orthogonal planes of type λ	Isabelle: `orthogonal_planes_rotation`
Prop. 7.2	Isabelle: `prop_aux`; the direction from planes is unconditional, the statement assumes the extraction of planes over L, that a representation gives a hyperbolic form, and the normalization $A = (I; 0)$ of Prop. 2.1
Thm. 6.2, 6.7, 6.15, Lemmas 6.1, 6.4, Prop. 6.5	proved here; the isometry criterion is [BF]; not formalized beyond the rows above
Thm. 3.1, 4.1, 4.2, 5.1, 5.5, 7.1	proved here; not formalized beyond the rows above; Cor. 5.4 after [HS]
Prop. 4.4 (lower bounds), 4.6, and the lower bounds of Prop. 4.5 and 9.5	proved here; not formalized

⬇ CSV

Table without a number, in the text of §12 Questions

$\ell_{\mathbb{R}}(H)$	n **if interior multiplicities are even, else** $n + 1$

$\ell_{\mathbb{Z}}(G)$	$n+p+(z \bmod 2)$, with p the paths with at least two vertices and z the isolated vertices; ∞ if $\Delta \geq 3$
$\ell_{\mathbb{Q}}(H)=n$	$h_p \otimes F(\sqrt{\lambda^2-1})$ hyperbolic for all $p \neq x \mp 1$
$\ell_{\mathbb{Q}}(H_n)$, n odd	n if n or $n-2$ a square; else $n+3$ ($n \equiv 3,5$), $n+5$ ($n \equiv 1,7$) mod 8
$\ell_{\mathbb{Q}}(H_n)$, $n \geq 4$ even	$n+\tau(s)$, $s \in \{n, n-2\}$, $4 \mid s$
$d_{\mathbb{Q}}(H_n)$	0 if $\ell_{\mathbb{Q}}(H_n)=n$; else 2 (odd n), 1 (even $n \geq 4$)
$\ell_{\mathbb{R}}=n$ and $\ell_{\mathbb{Q}} \leq n+1$	$\Rightarrow\ \ell_{\mathbb{Q}}=n$
$\ell_{\mathbb{Q}}(H)$	$\min\{r : (M_H)_F \hookrightarrow (I_r)_F\}$, $F=\mathbb{Q}(t)$
$\ell_{\mathbb{Q}}(H^{\oplus 8} \oplus K)$	$8n+\ell_{\mathbb{Q}}(K)$
$\det M$	$(1-(-t)^n)^2$; $(1+(-t)^n)^2$; $\sum_{j \leq n} t^{2j}$
$\ell_{\mathbb{R}}, \ell_{\mathbb{Q}}$ of $P_2 \sqcup K_1$	4, 5
$\ell_{\mathbb{Q}}(\lambda I_m)$, $\lambda \in \mathbb{Q} \cap (-1,1)$	$m+\min\big((-m) \bmod 2s,\ \tau(1-\lambda^2)\big)$, $s=1,2,4$ for $\tau=1$, 2 or 3, 4
$d_{\mathbb{Q}}(\lambda I_m)$	$\min(r, 2s-r)$, $r \equiv m \pmod{2s}$
$\ell_{\mathbb{Q}}(H) \leq n+h$, spectrum $\{-1,\lambda,1\}$, $\lambda \in \mathbb{Q} \cap (-1,1)$	$\exists\, p \subseteq I_h$ positive with $(q \perp p)_{\mathbb{Q}(\sqrt{-\delta})}$ hyperbolic

⬇ CSV

References

1 R. F. Bailey, R. Craigen, On orthogonal matrices with zero diagonal, Electron. J. Linear Algebra 35 (2019), 307–318. 🔎 find it

2 H. Bass, D. R. Estes, R. M. Guralnick, Eigenvalues of symmetric matrices and graphs, J. Algebra 168 (1994), 536–567. 🔎 find it

3 E. Bayer-Fluckiger, G. Berhuy, P. Chuard-Koulmann, CM-fields and skew-symmetric matrices, Manuscripta Math. 114 (2004), 351–359. 🔎 find it

4 E. Bayer-Fluckiger, Isometries of quadratic spaces, J. Eur. Math. Soc. 17 (2015), 1629–1656. 🔎 find it

5 E. Bayer-Fluckiger, Embeddings of maximal tori in orthogonal groups, Ann. Inst. Fourier 64 (2014), 113–125. 🔎 find it

6 E. Bayer-Fluckiger, T.-Y. Lee, R. Parimala, Embeddings of maximal tori in classical groups and explicit Brauer–Manin obstruction, J. Eur. Math. Soc. 20 (2018), 137–163. 🔎 find it

7 E. A. Bender, Characteristic polynomials of symmetric matrices, Pacific J. Math. 25 (1968), 433–441. 🔎 find it

8 G. Blekherman, D. Plaumann, R. Sinn, C. Vinzant, Low-rank sum-of-squares representations on varieties of minimal degree, Int. Math. Res. Not. IMRN 2019, no. 1, 33–54. 🔎 find it

9 G. Blekherman, R. Sinn, G. G. Smith, M. Velasco, Sums of squares and quadratic persistence on real projective varieties, J. Eur. Math. Soc. 24 (2022), 925–965. find it

10 J. W. S. Cassels, Rational Quadratic Forms, Academic Press, 1978. find it

11 C. Cui, L. Qi, Y. Xu, The sum of squares rank of biquadratic forms and the Zarankiewicz number, arXiv:2602.07844.

12 R. J. de la Cruz, A. T. Paras, Sums of orthogonal, symmetric, and skew-symmetric matrices, Electron. J. Linear Algebra 38 (2022), 655–660. find it

13 D. Ž. Đoković, S. Severini, F. Szöllősi, Rational orthogonal versus real orthogonal, Electron. J. Linear Algebra 18 (2009), 649–673 (arXiv:0903.2853).

14 P. Delsarte, J.-M. Goethals, J. J. Seidel, Orthogonal matrices with zero diagonal II, Canad. J. Math. 23 (1971), 816–832. find it

15 K. Fan, G. Pall, Imbedding conditions for Hermitian and normal matrices, Canad. J. Math. 9 (1957), 298–304. find it

16 J. F. Fernando, J. M. Ruiz, C. Scheiderer, Sums of squares of linear forms, Math. Res. Lett. 13 (2006), 947–956. find it

17 S. Friedland, Rational orthogonal similarity of rational symmetric matrices, Linear Algebra Appl. 192 (1993), 109–114. find it

18 L. J. Gerstein, A new proof of a theorem of Cassels and Pfister, Proc. Amer. Math. Soc. 41 (1973), 327–328. find it

19 J.-M. Goethals, J. J. Seidel, Orthogonal matrices with zero diagonal, Canad. J. Math. 19 (1967), 1001–1010. find it

20 C. Hanselka, R. Sinn, Positive semidefinite univariate matrix polynomials, Math. Z. 292 (2019), 83–101. find it

21 T. Y. Lam, Introduction to Quadratic Forms over Fields, Amer. Math. Soc., 2005. find it

22 N. Lebedev, Asymptotic equivalence and exact values for second-order Zarankiewicz numbers, arXiv:2610.05442.

23 E. Levy, O. M. Shalit, Dilation theory in finite dimensions: the possible, the impossible and the unknown, Rocky Mountain J. Math. 44 (2014), 203–221. find it

24 D. W. Lewis, A note on hermitian and quadratic forms, Bull. London Math. Soc. 11 (1979), 265–267. find it

25

J. Löfberg, L. Qi, Second order Zarankiewicz number, arXiv:2608.30555.

26 O. T. O'Meara, Introduction to Quadratic Forms, Springer, 1963. 🔎 find it

27 Y. Pourchet, Sur la représentation en somme de carrés des polynômes à une indéterminée sur un corps de nombres algébriques, Acta Arith. 19 (1971), 89–104. 🔎 find it

28 C. Marín Muñoz, Quadratic persistence of Segre varieties and a linear gap between biquadratic SOS rank and Zarankiewicz bounds, Zenodo (2026), doi:10.5281/zenodo.24036320.

29 J. Milnor, D. Husemoller, Symmetric Bilinear Forms, Springer, 1973. 🔎 find it

30 J. Milnor, Algebraic K-theory and quadratic forms, Invent. Math. 9 (1970), 318–344. 🔎 find it

31 J. Milnor, On isometries of inner product spaces, Invent. Math. 8 (1969), 83–97. 🔎 find it

32 L. Qi, C. Cui, The second-order augmented Zarankiewicz number, arXiv:2610.04448.

33 K. B. Reid, E. Brown, Doubly regular tournaments are equivalent to skew Hadamard matrices, J. Combin. Theory Ser. A 12 (1972), 332–338. 🔎 find it

34 C. Scheiderer, Sums of squares of polynomials with rational coefficients, J. Eur. Math. Soc. 18 (2016), 1495–1513. 🔎 find it

35 D. B. Shapiro, Compositions of Quadratic Forms, de Gruyter, 2000. 🔎 find it

36 Q. Tang, W. Wang, H. Zhang, Generating all regular rational orthogonal matrices, Linear Algebra Appl. 724 (2025), 12–20. 🔎 find it

37 Y. Xu, C. Cui, L. Qi, Narrowing the gap: SOS ranks of 4×3 biquadratic forms and a lower bound of 8, arXiv:2602.21570.

38 P. Yiu, Sums of squares formulae with integer coefficients, Canad. Math. Bull. 30 (1987), 318–324. 🔎 find it

39 C. Zhang, H. Zhu, The Hurwitz sum-of-squares problem depends on the base field, arXiv:2605.00590.