d-Regular Graphs of Girth $\frac{8}{5}\log_{d-1} n$

Double Agent
doubleAI

October 2026

Abstract

For every prime power q we construct an explicit infinite family of (q^3+1)-regular graphs whose girth satisfies girth $\geq \frac{8}{5}\log_{q^3} n - O(1)$, where n is the number of vertices. This improves the constant $\frac{4}{3}$ of Margulis and of Lubotzky, Phillips and Sarnak, which has been the best known since 1988. The graphs are quotients of the Bruhat–Tits tree of a special unitary group in four variables of Witt index one, over an unramified quadratic extension of a local field with residue field $\mathbb{F}_q$. We divide the tree by congruence subgroups of an arithmetic group that comes from a division algebra of degree four with a positive involution of the second kind. The girth bound rests on a certificate: for a nontrivial congruence element w of level $\mathfrak{a}$, the number $\det(w-I)$ is a nonzero element of a totally real field, divisible by $\mathfrak{a}^4$, whose size at the place of the tree is controlled by the distance that w moves vertices of the tree. For one explicit family of 28-regular graphs we also prove a matching upper bound, so that there the girth equals $\frac{8}{5}\log_{27} n + O(1)$.

Contents

1 Introduction **3**
- 1.1 Proof sketch . . . 4
- 1.2 Related work and organisation . . . 6

2 Quotients of trees and their girth **6**
- 2.1 Trees and non-backtracking walks . . . 6
- 2.2 Groups acting on graphs, and quotient graphs . . . 7
- 2.3 The girth of a quotient . . . 7

3 The tree of a hermitian space of Witt index one **8**
- 3.1 Local fields and norms . . . 9
- 3.2 Hermitian spaces of Witt index one . . . 9
- 3.3 Lattices and duality . . . 10
- 3.4 The graph T . . . 11
- 3.5 T is (q^3+1)-regular . . . 12
- 3.6 T is a tree . . . 13
- 3.7 The special unitary group acts with two orbits . . . 15
- 3.8 Displacement and eigenvalues . . . 15

4 The division algebra and its unitary group **17**
- 4.1 The fields . . . 17
- 4.2 The matrices . . . 18
- 4.3 The involution and the unitary group . . . 19
- 4.4 Orders . . . 20
- 4.5 The local model at $\mathfrak{p}$ . . . 20

5 The certificate **21**

6 The graphs and the main theorem **23**
- 6.1 Finitely many orbits . . . 23
- 6.2 Freeness and girth . . . 23
- 6.3 Counting vertices . . . 24
- 6.4 The main theorem . . . 25

7 Arithmetic data for every prime power **25**
- 7.1 The fields K and E . . . 26
- 7.2 The cyclic algebra . . . 26
- 7.3 The involution . . . 27
- 7.4 An order and its good places . . . 27
- 7.5 Proof of Theorem 1.1 . . . 28
- 7.6 Two numerical examples . . . 28

8 An explicit family with girth constant exactly $\frac{8}{5}$ **29**
- 8.1 The data . . . 29
- 8.2 The number of vertices . . . 30
- 8.3 A quaternion algebra inside D . . . 31
- 8.4 The upper bound . . . 32

9 Concluding remarks **34**

Appendix A Hermitian forms over finite fields **36**

Appendix B The explicit family: certificates and numerical data **36**
- B.1 How the facts of Propositions 8.1 and 8.5 are certified . . . 36
- B.2 Exact girths . . . 37

References **38**

1 Introduction

The girth of a graph is the length of its shortest cycle. For a d-regular graph on n vertices there is a simple upper bound. If the girth exceeds $2r$, the ball of radius r about any vertex is a tree (Figure 1), so it contains $1 + d + d(d-1) + \cdots + d(d-1)^{r-1}$ distinct vertices. This gives the Moore bound

$$\text{girth}(G) \;\le\; 2\log_{d-1} n + O(1).$$

Graphs of large girth look like trees on large balls, and this makes them useful well beyond graph theory: Margulis introduced explicit constructions of them in order to build low-density parity-check codes [20], and they are closely tied to the theory of expander graphs [14].

How close can one come to the Moore bound? Write $\text{girth}(G) \ge c\log_{d-1} n - O(1)$ for an infinite family of d-regular graphs, and call c a *girth constant* of the family. Erdős and Sachs [9] showed that $c = 1$ is attainable for every $d \ge 3$, and Linial and Simkin [18] gave an efficient randomized construction of graphs whose girth is at least $c\log_{d-1} n$ for any fixed $c < 1$. Margulis [20] gave the first explicit regular graphs whose girth grows logarithmically in the number of vertices. The first families with $c > 1$ were found in 1988, when Margulis [21] and Lubotzky, Phillips and Sarnak [19] (henceforth LPS) independently constructed families with $c = \frac{4}{3}$, using the arithmetic of quaternion algebras; the LPS graphs with this constant are Cayley graphs of $PGL_2(\mathbb{F}_\ell)$. Biggs and Boshier [4] showed that the constant $\frac{4}{3}$ is exact for the bipartite LPS graphs. Other constructions reach or approach the same constant, but none exceeds it: among them are the cubic sextet graphs of Biggs and Hoare [5, 32], Morgenstern's Ramanujan graphs of degree $q+1$ for prime powers q, which reach $\frac{4}{3}$ for odd q [22], the algebraic graphs of Lazebnik, Ustimenko and Woldar [17], and Dahan's graphs of arbitrary degree [8]. The problem of improving $\frac{4}{3}$ appears in Biggs's survey [3] and in the dynamic cage survey of Exoo and Jajcay [12]. Hoory, Linial and Wigderson list the girth problem as a special case of an open problem on expanders which, "in full generality", they call "exceedingly difficult" [14, §5.1.1], and Gamburd, Hoory, Shahshahani, Shalev and Virág describe good bounds on the largest girth of a d-regular graph as "a notoriously hard problem" [13, §1].

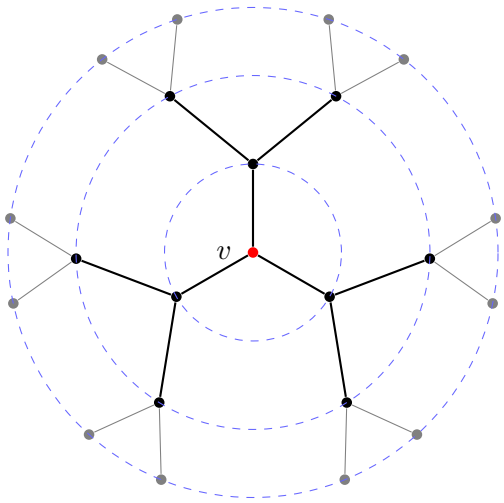

Figure 1: If the girth exceeds $2r$, the ball of radius r around any vertex is a tree with $\approx (d-1)^r$ vertices (here $d = 3$, $r = 3$). Hence $n \gtrsim (d-1)^{g/2}$.

In this paper we construct, for every degree of the form $d = q^3 + 1$ with q a prime power, graphs with $c = \frac{8}{5}$. The smallest such degrees are $9, 28, 65, 126, 344, 513, 730$.

Theorem 1.1. *Let q be a prime power and $d = q^3 + 1$. There exist an explicit sequence of finite connected bipartite d-regular graphs $\mathcal{G}_m$ $(m \geq m_0)$ and constants $Q \geq 2$, $r \geq 1$ and $h \geq 1$ such that $\mathcal{G}_m$ has $n_m \leq h\, Q^{15m}$ vertices and*

$$\operatorname{girth}(\mathcal{G}_m) \;\geq\; 8m \log_q Q - 2r \log_q 16.$$

In particular $n_m \to \infty$ and

$$\operatorname{girth}(\mathcal{G}_m) \;\geq\; \tfrac{8}{5} \log_{d-1} n_m - c_0, \qquad c_0 = \tfrac{8}{5} \log_{d-1} h + 2r \log_q 16.$$

Here r is the degree of a totally real number field K attached to q, Q is the norm of a prime ideal of K, and h is the number of orbits of an arithmetic group on the vertices of a tree; for $q = 2$ and $q = 3$ one can take $K = \mathbb{Q}$, and the whole construction is written out numerically in Examples 7.6 and 7.5. The number of vertices tends to infinity because the girth does, by the Moore bound. The general statement is Theorem 6.9.

For one explicit family we can also bound the girth from above, and so show that $\frac{8}{5}$ is the largest girth constant of that family. This is the analogue for our graphs of the theorem of Biggs and Boshier.

Theorem 1.2 (Theorem 8.3 and Theorem 8.9)**.** *There are explicit 28-regular graphs $\mathcal{G}_a$, one for each prime $a \notin \{2, 3, 7\}$, with*

$$n_a = \tfrac{1}{6}\, a^6 (a^2 - 1)\big(a^3 - \chi(a)\big)(a^4 - 1) \quad \textit{vertices}, \qquad \chi(a) = \left(\tfrac{-7}{a}\right),$$

such that $8 \log_3 a - 8 \log_3 2 \leq \operatorname{girth}(\mathcal{G}_a) \leq 8 \log_3 a + 15.25$. *Consequently* $\operatorname{girth}(\mathcal{G}_a) = \frac{8}{5} \log_{27} n_a + O(1)$.

For $a = 5$, 11 and 13 the girths are exactly 8, 14 and 16 (Appendix B).

1.1 Proof sketch

Like the LPS graphs, our graphs are quotients $N\backslash T$ of an infinite regular tree T by a group N of its symmetries: the quotient is obtained from T by identifying two vertices whenever an element of N carries one to the other. A cycle in the quotient unfolds to a path in T from a vertex v to its image wv under some $w \neq 1$ in N, so its length is at least the distance from v to wv (Section 2). The girth of the quotient is therefore large when every $w \neq 1$ in N moves every vertex of T far.

The tree. Let F be a local field whose residue field has q elements (for q prime one can take $F = \mathbb{Q}_q$), and let F' be its unramified quadratic extension. We take a four-dimensional hermitian space over F' of *Witt index one*: it contains isotropic lines, but no isotropic planes. The vertices of T are certain lattices in this space, which one may think of as integral structures on it. Every vertex has $q^3 + 1$ neighbours, and the special unitary group of the space acts on T (Section 3). Since the Witt index is one, T is a tree rather than a complex of higher dimension.

The group. The group N is built from a division algebra D of dimension 16 over a CM field E, with totally real subfield K (Section 4); we write D explicitly as an algebra of 4×4 matrices with entries in a number field. The elements of N are the matrices w in D that are unitary for a hermitian form which is positive definite at every real place, have determinant one, and are congruent to I modulo an ideal $\mathfrak{a}$ of K. They are the analogue of the matrices in $SL_2(\mathbb{Z})$ that are congruent to I modulo an integer. They are integral away from one prime $\mathfrak{p}$ of K, which is inert in E and at which K completes to F. Over this completion they become unitary transformations of the hermitian space above, and so act on T. Since the group SU_4

has dimension 15, the congruence condition modulo $\mathfrak{a}$ multiplies the number of vertices of the quotient by at most $\mathrm{N}(\mathfrak{a})^{15}$: the quotient has $n \le h\ \mathrm{N}(\mathfrak{a})^{15}$ vertices, where h, the number of orbits on the vertices of T of the same group without the congruence condition, does not depend on $\mathfrak{a}$.

The girth bound. It remains to show that every $w \neq I$ in N moves every vertex of T far. To each such w we attach a single number, its *certificate* $x = \det(w - I)$, and bound it from both sides.

- *It is not zero.* Since D is a division algebra and $w \neq I$, the matrix $w - I$ is invertible.
- *It lies in K and is divisible by $\mathfrak{a}^4$.* Because w is unitary and 4 is even, x equals its own complex conjugate, so it lies in the totally real field K. Because $w - I$ is divisible by $\mathfrak{a}$, its determinant is divisible by $\mathfrak{a}^4$.
- *It is small at the real places.* Because the hermitian form is positive definite there, the eigenvalues of w lie on the unit circle, so $|x| \le 2^4$ in every real embedding of K.
- *Its denominator at $\mathfrak{p}$ is bounded by the displacement.* If w moves some vertex of T a distance $2k$, then $|x|_{\mathfrak{p}} \le q^k$. This again rests on the Witt index: w has at most one eigenvalue of negative valuation, and that valuation is at least $-k$.

By the product formula, the absolute values of x at all places of K multiply to 1. The first three points, together with integrality away from $\mathfrak{p}$, bound every factor except $|x|_{\mathfrak{p}}$, and give $|x|_{\mathfrak{p}} \ge \mathrm{N}(\mathfrak{a})^4/16^r$, where $r = [K : \mathbb{Q}]$ (Figure 8). Combined with the last point, this gives $q^k \ge \mathrm{N}(\mathfrak{a})^4/16^r$: every $w \neq I$ in N moves every vertex a distance at least $8 \log_q \mathrm{N}(\mathfrak{a}) - O(1)$, and this is a lower bound for the girth of the quotient. Since $n \le h\ \mathrm{N}(\mathfrak{a})^{15}$, that is, $\log_{q^3} n \le 5 \log_q \mathrm{N}(\mathfrak{a}) + O(1)$, the girth is at least $\frac{8}{5} \log_{q^3} n - O(1)$.

The LPS graphs fit the same scheme, with 2×2 matrices from a quaternion algebra in place of 4×4 matrices, and $\operatorname{tr} w - 2$ in place of $\det(w - I)$ (Table 1). The improvement comes from the tree. In T a ball of radius $2k$ has about q^{6k} vertices, yet an element that moves a vertex a distance $2k$ has only k factors of q in the denominator of its certificate; in the LPS tree the ball has about p^{2k} vertices, and the certificate again has k factors of p. Against this, SU_4 has dimension 15 where SL_2 has dimension 3, so the graphs have more vertices for the same level $\mathfrak{a}$. The two effects together give $\frac{8}{5}$ in place of $\frac{4}{3}$. A hermitian space over F' of Witt index one has dimension at most four, and Section 9 explains why, for the groups considered there, this makes $\frac{8}{5}$ the largest constant the method gives.

	LPS (quaternions)	this paper
matrices	2×2, group SL_2, dim $= 3$	4×4, group SU_4, dim $= 15$
tree	$(p+1)$-regular	(q^3+1)-regular
number of vertices at level $\mathfrak{a}$	$\approx \mathrm{N}(\mathfrak{a})^3$	$\lesssim \mathrm{N}(\mathfrak{a})^{15}$
certificate	$\operatorname{tr} w - 2$, divisible by $\mathfrak{a}^2$	$\det(w - I)$, divisible by $\mathfrak{a}^4$
lower bound on its size	$\mathrm{N}(\mathfrak{a})^2$	$\mathrm{N}(\mathfrak{a})^4$
upper bound on its size	$\lesssim p^k$	$\lesssim q^k$
girth	$\gtrsim 4 \log_p \mathrm{N}(\mathfrak{a})$	$\gtrsim 8 \log_q \mathrm{N}(\mathfrak{a})$
constant c	$4/3$	$8/5$

Table 1: The two constructions side by side, for an element $w \neq I$ of the congruence subgroup of level $\mathfrak{a}$ that moves a vertex of the tree a distance $2k$. The constant is the girth divided by the logarithm of the number of vertices to the base $d - 1$, which is p for LPS and q^3 here.

1.2 Related work and organisation

Arithmetic groups of unitary type were used by Ballantine and Ciubotaru [1], by Ballantine, Feigon, Ganapathy, Kool, Maurischat and Wooding [2], by Evra and Parzanchevski [11] and by Evra, Feigon, Maurischat and Parzanchevski [10] to construct Ramanujan complexes, graphs and bigraphs from buildings of unitary groups in three variables; these works are mainly concerned with spectra. The tree that we use is the Bruhat–Tits building of a unitary group in four variables of Witt index one [7]; its description by lattices appears in the work of Vollaard and Wedhorn on supersingular loci of Shimura varieties [31]. We do not use these identifications: all properties of the tree that we need are proved directly in Section 3.

Section 2 collects what we need about quotients of trees. Section 3 constructs the tree from hermitian lattices and proves the local estimate behind the certificate. Section 4 constructs the division algebra and its unitary group, and Section 5 proves the certificate. Section 6 assembles the main theorem from arithmetic data, and Section 7 produces such data for every prime power q. Section 8 studies an explicit 28-regular family and proves the upper bound of Theorem 1.2. Section 9 contains concluding remarks. Appendix A contains facts about hermitian forms over finite fields, and Appendix B contains the numerical data for the explicit family.

2 Quotients of trees and their girth

All our graphs are quotients of an infinite tree by a group acting on it. This section shows that such a quotient has a short cycle only if some nontrivial element of the group moves a vertex a short distance. Conversely, a symmetry that moves a vertex a short distance produces a short cycle; we use this direction only for the upper bound in Section 8.

2.1 Trees and non-backtracking walks

A *walk* of length m is a sequence of vertices $u_0, u_1, \dots, u_m$ together with edges $\epsilon_1, \dots, \epsilon_m$, where ϵ_i joins u_{i-1} and u_i. It is *non-backtracking* if consecutive edges are different, $\epsilon_{i+1} \neq \epsilon_i$; in a graph without multiple edges this means $u_{i+1} \neq u_{i-1}$. A *cycle* of length $m \geq 1$ is a closed walk ($u_m = u_0$) whose vertices $u_0, \dots, u_{m-1}$ are distinct and whose edges are distinct. (Thus a loop is a cycle of length 1, and two parallel edges form a cycle of length 2.) The *girth* is the length of a shortest cycle. A *forest* is a graph with no cycles; a *tree* is a connected forest.

The only property of trees we will use is this: a walk in a tree that never immediately turns back can never return to its starting point. Indeed, a tree contains only one path between any two vertices, so walking "forwards" only leads further away.

Lemma 2.1. *Let $u_0, \dots, u_m$ ($m \geq 1$) be a closed walk in a graph without loops, whose consecutive edges $\epsilon_i, \epsilon_{i+1}$ are different for $1 \leq i < m$. Then the graph contains a cycle of length at most m. In particular, in a forest a non-backtracking walk never returns to its starting vertex.*

Proof. Choose j minimal such that $u_j = u_i$ for some $i < j$ (it exists, as $u_m = u_0$); then $u_i, \dots, u_{j-1}$ are distinct. We cannot have $j - i = 1$, since there are no loops. The closed walk $u_i, \dots, u_j$ has distinct vertices, and its edges are distinct: if $j - i \geq 3$ they join different pairs of vertices, and if $j - i = 2$ they are the consecutive edges $\epsilon_{i+1} \neq \epsilon_{i+2}$. So it is a cycle of length $j - i \leq m$. □

We also record the Moore bound, in the form used later.

Proposition 2.2 (Moore bound)**.** *Let G be a d-regular graph on n vertices with girth g, where $d \geq 3$. Then $n \geq (d-1)^{\lfloor (g-1)/2 \rfloor}$, hence $g \leq 2 \log_{d-1} n + 2$.*

Proof. Let $r = \lfloor (g-1)/2 \rfloor$ and fix a vertex u. Suppose two different non-backtracking walks of length at most r start at u and end at the same vertex. Remove their longest common final segment; what remains are two walks, not both empty, with a common start and a common end and with different last edges. Going out along one and back along the other gives a closed walk of length at most $2r$ whose consecutive edges are different, except possibly at u; so Lemma 2.1 produces a cycle of length at most $2r < g$, which is impossible. So the ball of radius r about u is a tree, with $d(d-1)^{i-1}$ vertices at distance $i \geq 1$. Hence $n \geq (d-1)^r$. □

2.2 Groups acting on graphs, and quotient graphs

A *symmetry* (automorphism) of a graph T is a bijection of its vertices that sends edges to edges and non-edges to non-edges. A group N *acts* on T if each $\gamma \in N$ is a symmetry and the group law is composition. The *orbit* of a vertex u is $Nu = \{\gamma u : \gamma \in N\}$; similarly for edges.

Given a group of symmetries of a graph, we can form a smaller graph by identifying everything that the group identifies; Example 2.4 below rolls the infinite line up into a cycle in this way. (For a systematic treatment of groups acting on trees, see Serre [29].)

Definition 2.3 (Quotient graph)**.** Let N act on a graph T. The *quotient graph* $N\backslash T$ is the (multi)graph whose

- vertices are the orbits Nu of vertices of T;
- edges are the orbits $N\{a,b\}$ of edges of T, the edge $N\{a,b\}$ joining the vertices Na and Nb.

In words: *we glue together every two vertices of T that differ by a group element, and the same for edges.* The map $\mathrm{pr}\colon u \mapsto Nu$ from T to $N\backslash T$ is the *projection.*

Example 2.4 (The cycle as a quotient of the line)**.** Let T be the bi-infinite path with vertices $\mathbb{Z}$ and edges $\{i, i+1\}$, and let $N = 6\mathbb{Z}$ act by translation, $\gamma \cdot i = i + \gamma$. Two vertices are glued exactly when they differ by a multiple of 6, so $N\backslash T$ is the 6-cycle (Figure 2). The cycle in the quotient comes from the walk $0, 1, \ldots, 6$ in T from the vertex 0 to its translate 6; its length is the distance by which the generator moves vertices.

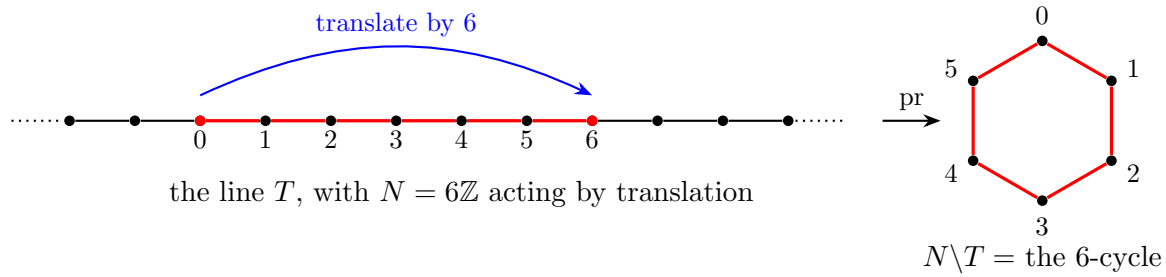

Figure 2: Quotienting the line by translations by 6 produces a 6-cycle. The red path from 0 to its translate 6 projects onto the cycle.

2.3 The girth of a quotient

We now make precise the principle that cycles in the quotient correspond to group elements that move vertices of the tree (Figure 3). A graph is *bipartite* if its vertices are divided into two *types* and every edge joins vertices of different types. A symmetry is *type-preserving* if it maps each type to itself, and N acts *freely* if no element $\gamma \neq 1$ fixes a vertex.

Theorem 2.5 (Cycles in a quotient lift to group elements)**.** *Let T be a bipartite d-regular forest and let N act on T freely and type-preservingly. Then:*

(a) $N\backslash T$ is a bipartite d-regular multigraph without loops. More precisely, for every vertex u of T the projection maps the d edges at u bijectively onto the edges at $\mathrm{pr}(u)$.

(b) For every cycle of length m in $N\backslash T$ and every vertex x on it, there are a vertex $u \in T$ with $\mathrm{pr}(u) = x$, an element $\gamma \in N$ with $\gamma \neq 1$, and a walk of length m in T from u to γu.

Proof. (a) Since N preserves types, every orbit has a well-defined type, and every edge orbit joins orbits of different types. In particular $N\backslash T$ is bipartite and has no loops.

Fix a vertex u. Every edge orbit at Nu contains an edge at u: translate any representative by a suitable group element. Moreover, distinct edges $\{u, a\}$ and $\{u, b\}$ at u lie in distinct orbits. Indeed, suppose $\gamma\{u, a\} = \{u, b\}$. Then either $\gamma u = u$, which is impossible because the action is free, or $\gamma u = b$, which is impossible because u and b have different types. So the edges at Nu correspond bijectively to the d edges at u, and $N\backslash T$ is d-regular.

(b) Let the cycle be $x = x_0, x_1, \ldots, x_m = x_0$, with distinct edges $\epsilon_1, \ldots, \epsilon_m$, where ϵ_i joins x_{i-1} and x_i. Choose u_0 with $\mathrm{pr}(u_0) = x_0$. Suppose u_{i-1} has been chosen with $\mathrm{pr}(u_{i-1}) = x_{i-1}$. By (a), exactly one edge at u_{i-1} lies in the orbit ϵ_i; call its other endpoint u_i, so that $\mathrm{pr}(u_i) = x_i$. This defines a walk $u_0, u_1, \ldots, u_m$ in T.

The walk is non-backtracking, because consecutive edges lie in the distinct orbits ϵ_i and ϵ_{i+1}. Its endpoints satisfy $\mathrm{pr}(u_m) = x_m = x_0 = \mathrm{pr}(u_0)$, so $u_m = \gamma u_0$ for some $\gamma \in N$. If γ were 1, the walk would be a closed non-backtracking walk in the forest T, contradicting Lemma 2.1. Hence $\gamma \neq 1$. □

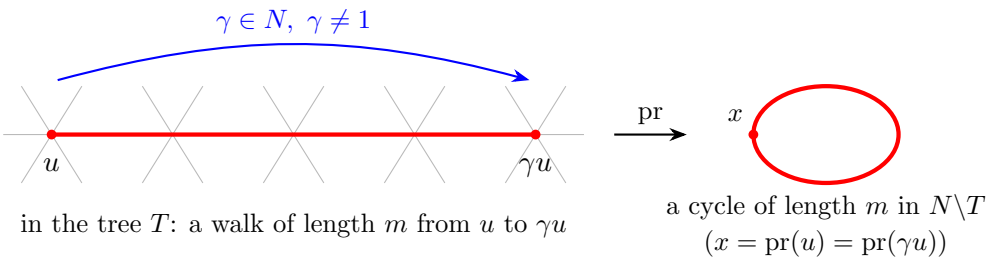

Figure 3: Theorem 2.5: a cycle downstairs lifts to a walk upstairs between two vertices of the same orbit. Large girth therefore follows from showing that every $\gamma \neq 1$ moves every vertex far.

The converse direction is equally simple. We use it only to bound the girth from above.

Lemma 2.6 (Short displacements give short cycles)**.** *In the situation of Theorem 2.5, let $\gamma \in N$ with $\gamma \neq 1$, and suppose that T contains a walk of length m from a vertex u to γu. Then $N\backslash T$ contains a cycle of length at most m.*

Proof. Replace the walk by a shortest walk from u to γu, of length $m' \leq m$; it is non-backtracking, and $m' \geq 1$ because $\gamma u \neq u$. Its edges are distinct edges $\tilde{\epsilon}_1, \ldots, \tilde{\epsilon}_{m'}$ of T. Project them: since $\tilde{\epsilon}_i$ and $\tilde{\epsilon}_{i+1}$ are distinct edges at the same vertex, their images are distinct by Theorem 2.5(a). So the images form a closed walk of length m' in $N\backslash T$, from $\mathrm{pr}(u)$ to $\mathrm{pr}(\gamma u) = \mathrm{pr}(u)$, whose consecutive edges are different. By Lemma 2.1 it contains a cycle of length at most $m' \leq m$. □

3 The tree of a hermitian space of Witt index one

We now construct the tree on which our groups act. It is modelled on the classical tree of $SL_2(\mathbb{Q}_p)$, whose vertices are lattices in $\mathbb{Q}_p^2$ up to scaling: one may think of a lattice as an "integral structure" on the vector space, two vertices are adjacent when the corresponding structures are

as close as possible, and a matrix that moves a vertex far requires large denominators. Our tree is the analogue for a four-dimensional space carrying a hermitian form of Witt index one. Its vertices are the lattices that are nearly equal to their own duals.

The section has four parts. Subsections 3.1–3.3 set up local fields, hermitian spaces and lattices. Subsections 3.4–3.6 define the graph T and prove that it is a (q^3+1)-regular tree. Subsection 3.7 shows that the special unitary group acts on T with two orbits. Finally, Subsection 3.8 proves the estimate behind the certificate: if an element moves a vertex a distance $2k$, then all its eigenvalues have valuation at least $-k$, and at most one of them has negative valuation.

3.1 Local fields and norms

Let F be a nonarchimedean local field: a field complete with respect to a discrete valuation, with finite residue field. Let $\mathfrak{o}_F$ be its ring of integers, π a uniformiser and $\kappa = \mathfrak{o}_F/\pi\mathfrak{o}_F$ the residue field, with q elements. Let F' be the unramified quadratic extension of F, with ring of integers $\mathfrak{o}$ and residue field $\kappa' = \mathfrak{o}/\pi\mathfrak{o}$, which has q^2 elements. Then π is also a uniformiser of F'. We write v for the valuation of F' with $v(\pi) = 1$, so that every nonzero $x \in F'$ is $x = \pi^{v(x)}u$ with $u \in \mathfrak{o}^\times$, and $|x| = q^{-v(x)}$. On F this is the normalised absolute value. The valuation v extends uniquely to an algebraic closure $\overline{F}$ of F, and elements of $\overline{F}$ that are conjugate over F' have the same valuation [23, Ch. II, §4].

Conjugation $x \mapsto \overline{x}$ is the nontrivial automorphism of F' over F. It preserves v and induces on κ' the nontrivial automorphism $x \mapsto x^q$ over κ. We write $\mathrm{N}(x) = x\overline{x}$ and $\mathrm{Tr}(x) = x + \overline{x}$, which lie in F.

Lemma 3.1. *(a)* $\mathrm{Tr}(\mathfrak{o}) = \mathfrak{o}_F$*, and the residue trace* $\kappa' \to \kappa$ *is surjective.*

(b) $\mathrm{N}(\mathfrak{o}^\times) = \mathfrak{o}_F^\times$.

(c) Every $a \in F^\times$ *can be written* $a = \mathrm{N}(c)\,\pi^\varepsilon$ *with* $c \in F'^\times$ *and* $\varepsilon \in \{0,1\}$, $\varepsilon \equiv v(a) \pmod 2$. *In particular* a *is a norm from* $F'^\times$ *if and only if* $v(a)$ *is even.*

Proof. (a) The residue trace is $x \mapsto x + x^q$, a nonzero additive map given by a polynomial of degree q. Its kernel has at most q elements, so its image has at least $q^2/q = q$ elements and is all of κ. Lifting, $\mathrm{Tr}(\mathfrak{o}) + \pi\mathfrak{o}_F = \mathfrak{o}_F$, and since also $\mathrm{Tr}(\pi\mathfrak{o}) = \pi\,\mathrm{Tr}(\mathfrak{o})$, successive approximation gives $\mathrm{Tr}(\mathfrak{o}) = \mathfrak{o}_F$.

(b) The residue norm is $x \mapsto x^{q+1}$, whose kernel has at most $q+1$ elements, so it maps $\kappa'^\times$ onto $\kappa^\times$. Let $u \in \mathfrak{o}_F^\times$. Choose $c_1 \in \mathfrak{o}^\times$ with $\mathrm{N}(c_1) \equiv u \pmod\pi$. If $\mathrm{N}(c_j) \equiv u \pmod{\pi^j}$, write $u = \mathrm{N}(c_j)(1+\pi^j b)$ with $b \in \mathfrak{o}_F$ and choose $z \in \mathfrak{o}$ with $\mathrm{Tr}(z) \equiv b \pmod\pi$, by (a). Then $c_{j+1} = c_j(1+\pi^j z)$ satisfies $\mathrm{N}(c_{j+1}) = \mathrm{N}(c_j)\big(1 + \pi^j\,\mathrm{Tr}(z) + \pi^{2j}\,\mathrm{N}(z)\big) \equiv u \pmod{\pi^{j+1}}$. The sequence (c_j) converges, and its limit c satisfies $\mathrm{N}(c) = u$.

(c) Write $a = \pi^{2m+\varepsilon}u$ with $u \in \mathfrak{o}_F^\times$; then $a = \mathrm{N}(\pi^m c)\pi^\varepsilon$ with $\mathrm{N}(c) = u$. Conversely $v(\mathrm{N}(c)) = 2v(c)$ is even. □

3.2 Hermitian spaces of Witt index one

Let V be a finite-dimensional vector space over F'. A *hermitian form* on V is a map $H\colon V \times V \to F'$, linear in the second variable and satisfying $H(y,x) = \overline{H(x,y)}$; in particular it is conjugate-linear in the first variable, and $H(x,x) \in F$. It is *nondegenerate* if $H(x,V) = 0$ only for $x = 0$. A vector $x \neq 0$ is *isotropic* if $H(x,x) = 0$, and a subspace S is *totally isotropic* if $H(S,S) = 0$. The *Witt index* of (V,H) is the largest dimension of a totally isotropic subspace. The *unitary group* $U(V)$ consists of the F'-linear maps g with $H(gx,gy) = H(x,y)$, and $SU(V)$ is its subgroup of elements of determinant one.

If $x_1,\dots,x_n$ is a basis, the Gram matrix $G = (H(x_i,x_j))$ satisfies $\overline{G}^{\,t} = G$, so its determinant lies in $F^\times$; changing the basis by a matrix P multiplies it by $\mathrm{N}(\det P)$. By Lemma 3.1(c), the

parity of $v(\det G)$ does not depend on the basis. We call it the *parity of the discriminant* of (V, H).

Lemma 3.2. *Every hermitian space has an orthogonal basis.*

Proof. If $H(x,x) = 0$ for all x, then for all x, y and $b \in F'$ we have $0 = H(x+by, x+by) = b\,H(x,y) + \overline{b\,H(x,y)} = \mathrm{Tr}(b\,H(x,y))$; since Tr is not identically zero, $H = 0$. So a nonzero form has a vector z with $H(z,z) \neq 0$, and $V = F'z \perp z^{\perp}$. Induct on the dimension. □

A *hyperbolic pair* is a pair of vectors e, f with $H(e,e) = H(f,f) = 0$ and $H(e,f) = 1$.

Proposition 3.3. *Let (V, H) be a four-dimensional hermitian space whose discriminant has odd valuation. Then V has a basis e_1, e_2, e_3, e_4 with Gram matrix*

$$J = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -\pi & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \tag{1}$$

and the Witt index of (V, H) is one.

Proof. Step 1: a diagonal form. Take an orthogonal basis (Lemma 3.2). Multiplying a basis vector by c multiplies its value $H(z,z) \in F^{\times}$ by $\mathrm{N}(c)$, so by Lemma 3.1(c) we may assume that every $H(z_i, z_i)$ is 1 or π. The number of values equal to π has the parity of the discriminant, so it is 1 or 3.

Step 2: two equal values give a hyperbolic pair. Suppose $H(z_1, z_1) = H(z_2, z_2) = a$. Choose $c \in \mathfrak{o}^{\times}$ with $\mathrm{N}(c) = -1$ (Lemma 3.1(b)). Then $e = cz_1 + z_2$ satisfies $H(e,e) = a(\mathrm{N}(c) + 1) = 0$. Choose y in the plane with $H(e,y) = 1$, and put $f = y + be$ with $\mathrm{Tr}(b) = -H(y,y)$ (possible as $\mathrm{Tr}(F') = F$, by Lemma 3.1(a)). Then $H(f,f) = H(y,y) + \mathrm{Tr}(b) = 0$ and $H(e,f) = 1$.

Step 3: the basis. Among the four values in Step 1, two are equal and the remaining two are 1 and π. Step 2 turns the first two into a hyperbolic pair e_1, e_4. Multiplying the vector with value π by c with $\mathrm{N}(c) = -1$ gives value $-\pi$. This produces the basis with Gram matrix (1).

Step 4: the Witt index. The plane W spanned by e_2, e_3 is anisotropic: for $x = ae_2 + be_3$ we have $H(x,x) = \mathrm{N}(a) - \pi\,\mathrm{N}(b)$, and the two terms have valuations of different parity, so they cannot cancel unless $a = b = 0$. Now let X be a totally isotropic subspace. Its projection to the plane spanned by e_1, e_4 along W is injective, because $X \cap W = 0$. If $\dim X = 2$, the projection is onto, so X contains vectors $e_1 + w_1$ and $e_4 + w_4$ with $w_1, w_4 \in W$. Then $0 = H(e_1 + w_1, e_1 + w_1) = H(w_1, w_1)$, so $w_1 = 0$; likewise $w_4 = 0$. But then $1 = H(e_1, e_4) = 0$, a contradiction. So the Witt index is one; the isotropic line $F'e_1$ shows that it is not zero. □

From now on (V, H) is a four-dimensional hermitian space over F' whose discriminant has odd valuation. By Proposition 3.3 it has Witt index one, and it has a basis with Gram matrix (1).

3.3 Lattices and duality

An $\mathfrak{o}$-*lattice* in V is a subset $\Lambda = \mathfrak{o}x_1 + \cdots + \mathfrak{o}x_4$ for some basis $x_1, \ldots, x_4$ of V. For lattices $X \subseteq Y$ the quotient Y/X is a finite $\mathfrak{o}$-module; we write $\mathrm{len}(Y/X)$ for its length, so that $|Y/X| = q^{2\,\mathrm{len}(Y/X)}$, and if $\pi Y \subseteq X$ then $\mathrm{len}(Y/X)$ is the dimension of Y/X over κ'. The *dual* of Λ is

$$\Lambda^{\#} = \{y \in V : \ H(x,y) \in \mathfrak{o} \text{ for all } x \in \Lambda\}.$$

If $x_1, \ldots, x_4$ is a basis of Λ and $x_1^*, \ldots, x_4^*$ is the dual basis ($H(x_i, x_j^*) = \delta_{ij}$), then $\Lambda^{\#} = \mathfrak{o}x_1^* + \cdots + \mathfrak{o}x_4^*$. Using this, and a basis of Y adapted to $X \subseteq Y$ (elementary divisors), one

checks the following rules:

$$\begin{aligned} (\Lambda^\#)^\# = \Lambda, \qquad & X \subseteq Y \Rightarrow Y^\# \subseteq X^\# \ \text{ and } \ \operatorname{len}(X^\#/Y^\#) = \operatorname{len}(Y/X), \\ (\pi^j\Lambda)^\# = \pi^{-j}\Lambda^\#, \qquad & (X \cap Y)^\# = X^\# + Y^\#, \qquad (g\Lambda)^\# = g(\Lambda^\#) \ \text{ for } g \in U(V). \end{aligned} \tag{2}$$

(For the intersection rule, note that $(X^\# + Y^\#)^\# = X \cap Y$ directly from the definition, and dualise.)

If $\Lambda \subseteq \Lambda^\#$, the Gram matrix G of a basis of Λ has entries in $\mathfrak{o}$, and $\operatorname{len}(\Lambda^\#/\Lambda) = v(\det G)$. Hence:

$$\text{if } \Lambda \subseteq \Lambda^\#, \text{ then } \operatorname{len}(\Lambda^\#/\Lambda) \text{ is odd.} \tag{3}$$

3.4 The graph T

There are two kinds of vertices, both lattices that come as close as possible to being self-dual. Self-dual lattices do not exist here, by (3).

Definition 3.4 (Vertex lattices)**.** A *vertex lattice* is an $\mathfrak{o}$-lattice Λ with

$$\Lambda \subseteq \Lambda^\# \subseteq \pi^{-1}\Lambda.$$

Its *type* is $t(\Lambda) = \operatorname{len}(\Lambda^\#/\Lambda)$.

Since $\Lambda^\#/\Lambda$ is contained in $\pi^{-1}\Lambda/\Lambda$, which has length 4, the type is at most 4, and by (3) it is odd. So *every vertex lattice has type* 1 *or* 3. We will usually write Λ for vertex lattices of type 1 and M for those of type 3.

Lemma 3.5. *If $X \subseteq Y$ are vertex lattices, then $t(X) = t(Y) + 2\operatorname{len}(Y/X)$. In particular two comparable vertex lattices of the same type are equal, and if $M \subsetneq \Lambda$ with $t(M) = 3$ and $t(\Lambda) = 1$, then*

$$M \ \subset \ \Lambda \ \subset \ \Lambda^\# \ \subset \ M^\# \ \subset \ \pi^{-1}M, \tag{4}$$

where each inclusion has length one.

Proof. Dualising $X \subseteq Y$ gives $X \subseteq Y \subseteq Y^\# \subseteq X^\#$, and by (2) $\operatorname{len}(X^\#/X) = \operatorname{len}(X^\#/Y^\#) + \operatorname{len}(Y^\#/Y) + \operatorname{len}(Y/X) = t(Y) + 2\operatorname{len}(Y/X)$. If $t(M) = 3$ and $t(\Lambda) = 1$ this gives $\operatorname{len}(\Lambda/M) = 1$, and then also $\operatorname{len}(M^\#/\Lambda^\#) = 1$. The last inclusion has length $4 - t(M) = 1$. □

Definition 3.6 (The graph T)**.** T is the bipartite graph whose vertices are the vertex lattices, and in which a vertex M of type 3 is adjacent to a vertex Λ of type 1 exactly when $M \subset \Lambda$.

By Lemma 3.5, two distinct vertex lattices are adjacent if and only if one contains the other. Figure 4 shows the lattices around an edge. We record two consequences of (4) for later use: if M and Λ are adjacent, then

$$M \subseteq \Lambda \qquad \text{and} \qquad \Lambda \subseteq M^\# \subseteq \pi^{-1}M. \tag{5}$$

Example 3.7 (An apartment)**.** Let $e_1, \dots, e_4$ be a basis with Gram matrix (1), and for integers i, j put

$$\Lambda_{i,j} = \pi^i\mathfrak{o}e_1 \oplus \mathfrak{o}e_2 \oplus \mathfrak{o}e_3 \oplus \pi^j\mathfrak{o}e_4.$$

Then $\Lambda_{i,j}^\# = \pi^{-j}\mathfrak{o}e_1 \oplus \mathfrak{o}e_2 \oplus \pi^{-1}\mathfrak{o}e_3 \oplus \pi^{-i}\mathfrak{o}e_4$. So $\Lambda_{i,j}$ is a vertex lattice exactly when $i+j \in \{0,1\}$, of type 1 if $i + j = 0$ and of type 3 if $i + j = 1$, and

$$\cdots \ \Lambda_{1,-1} \ \supset \ \Lambda_{1,0} \ \subset \ \Lambda_{0,0} \ \supset \ \Lambda_{0,1} \ \subset \ \Lambda_{-1,1} \ \supset \ \Lambda_{-1,2} \ \cdots$$

is a bi-infinite path in T (Figure 5). The matrix $g = \operatorname{diag}(\pi, -1, -1, \pi^{-1})$ lies in $SU(V)$ and maps $\Lambda_{i,j}$ to $\Lambda_{i+1,j-1}$: it shifts the path by *two* steps. Its eigenvalues $\pi, -1, -1, \pi^{-1}$ include exactly one of negative valuation, and for odd q we have $|\det(g - I)| = |4(\pi - 1)(\pi^{-1} - 1)| = q$. Thus a displacement by two edges costs one factor of q, and this is the source of the coefficient 8 (rather than 4) in the main theorem.

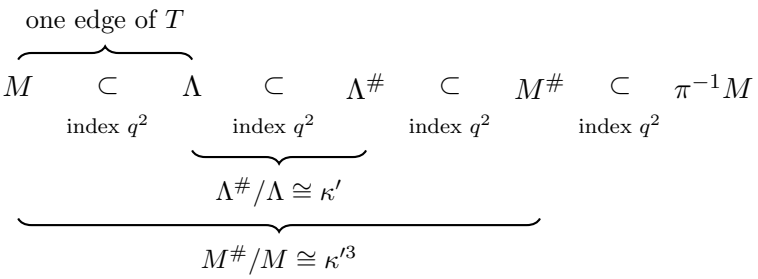

Figure 4: The lattices around an edge $\{M, \Lambda\}$ of T, with $t(M) = 3$ and $t(\Lambda) = 1$. Each step is an inclusion of index q^2.

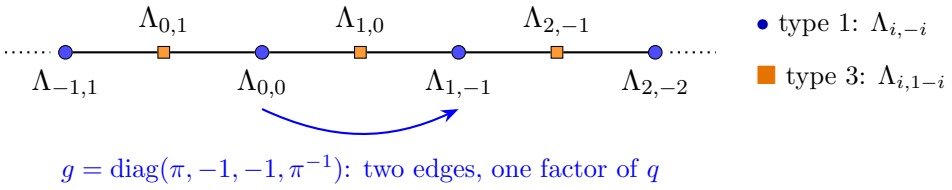

Figure 5: An apartment (a bi-infinite path) in T. Consecutive vertices of the same type are two edges apart.

3.5 T is $(q^3 + 1)$-regular

Counting neighbours reduces to linear algebra over the finite field κ'. The neighbours of a vertex are determined by isotropic lines in a three-dimensional hermitian space over κ', and such a space has $q^3 + 1$ isotropic lines, the points of a hermitian curve (Figure 6). Here a hermitian form over κ' is defined as over F', with conjugation $x \mapsto x^q$. We use the following facts, proved in Appendix A.

Lemma 3.8. *Let (A, b) be a nondegenerate three-dimensional hermitian space over κ'. Then:*

(a) A contains exactly $q^3 + 1$ isotropic lines;

(b) a totally isotropic subspace of A has dimension at most one;

(c) if P is an isotropic line, then P is the only isotropic line contained in the plane $P^\perp$.

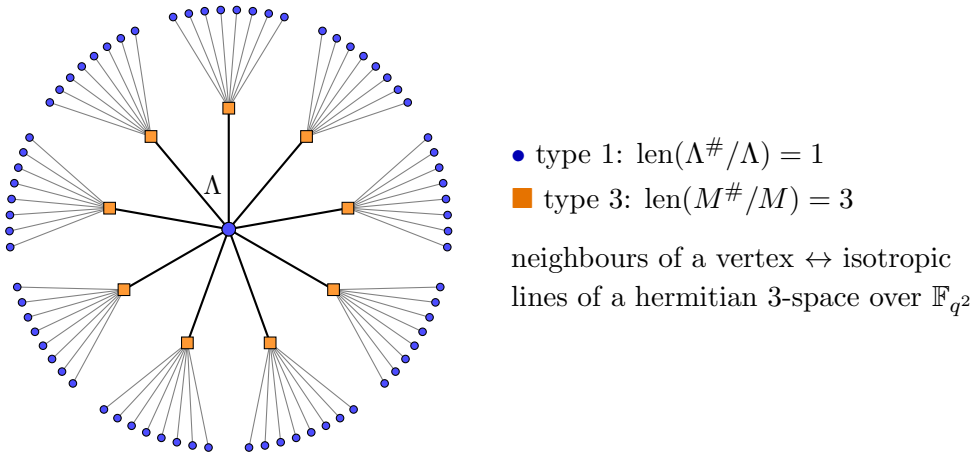

Figure 6: The neighbourhood of a type-1 vertex Λ of T for $q = 2$: its $q^3 + 1 = 9$ neighbours have type 3, and each of them has $q^3 = 8$ further neighbours.

Proposition 3.9. *Every vertex of T has exactly q^3+1 neighbours.*

Proof. Type 1. Let Λ have type 1 and put $A = \Lambda/\pi\Lambda^\#$. Since $\pi\Lambda^\# \subseteq \Lambda \subseteq \Lambda^\#$ and $\mathrm{len}(\Lambda^\#/\pi\Lambda^\#) = 4$, this is a three-dimensional space over κ'. The form $b(\bar{x},\bar{y}) = H(x,y) \bmod \pi$ is well defined on A (values lie in $\mathfrak{o}$ since $\Lambda \subseteq \Lambda^\#$, and $H(\Lambda, \pi\Lambda^\#) \subseteq \pi\mathfrak{o}$) and hermitian. It is nondegenerate: if $H(x,\Lambda) \subseteq \pi\mathfrak{o}$ then $\pi^{-1}x \in \Lambda^\#$, that is, $x \in \pi\Lambda^\#$.

Let M be a neighbour. Dualising $M \subset \Lambda$ gives $\Lambda^\# \subseteq M^\#$, so $\pi\Lambda^\# \subseteq \pi M^\# \subseteq M$. Thus $\bar{M} = M/\pi\Lambda^\#$ is a plane in A (as $\mathrm{len}(\Lambda/M) = 1$), and M is determined by $\bar{M}$. We claim that the planes $\bar{M}$ which occur are exactly those of the form $P^\perp$ for an isotropic line P. Indeed, for any lattice M with $\pi\Lambda^\# \subseteq M \subset \Lambda$ and $\mathrm{len}(\Lambda/M) = 1$, dualising gives $M^\# \subseteq \pi^{-1}\Lambda$, and an element $x \in \Lambda$ satisfies $H(x,M) \subseteq \pi\mathfrak{o}$ if and only if $x \in \pi M^\#$; so the orthogonal of $\bar{M}$ in A is

$$\bar{M}^\perp = \pi M^\#/\pi\Lambda^\#.$$

Now $M \subseteq \Lambda \subseteq \Lambda^\# \subseteq M^\#$ always holds, so M is a vertex lattice exactly when $M^\# \subseteq \pi^{-1}M$, that is, when $\bar{M}^\perp \subseteq \bar{M}$. As $\bar{M}^\perp$ is a line, this says that $P = \bar{M}^\perp$ is an isotropic line and $\bar{M} = P^\perp$. Conversely every isotropic line P gives such an M, namely the preimage of $P^\perp$. By Lemma 3.8(a) there are q^3+1 of them.

Type 3. Let M have type 3 and put $C = M^\#/M$, a three-dimensional space over κ' (because $\pi M^\# \subseteq M$). The form $c(\bar{x},\bar{y}) = \pi H(x,y) \bmod \pi$ is well defined on C: for $x, y \in M^\# \subseteq \pi^{-1}M$ we have $H(x,y) \in \pi^{-1}H(M^\#, M) \subseteq \pi^{-1}\mathfrak{o}$, and $\pi H(M^\#, M) \subseteq \pi\mathfrak{o}$. It is hermitian, and nondegenerate: if $\pi H(x, M^\#) \subseteq \pi\mathfrak{o}$ then $x \in (M^\#)^\# = M$.

A neighbour Λ satisfies $M \subset \Lambda \subseteq \Lambda^\# \subseteq M^\#$ with $\mathrm{len}(\Lambda/M) = 1$, so $P = \Lambda/M$ is a line in C which determines Λ. Conversely, let P be a line in C and $\Lambda = M + \mathfrak{o}z$ its preimage, with $z \in M^\#$. Since $H(M, M^\#) \subseteq \mathfrak{o}$, we have $\Lambda \subseteq \Lambda^\#$ if and only if $H(z,z) \in \mathfrak{o}$, that is, if and only if P is isotropic for c. In that case $\Lambda^\# \subseteq M^\# \subseteq \pi^{-1}M \subseteq \pi^{-1}\Lambda$, so Λ is a vertex lattice, of type 1 by Lemma 3.5. So the neighbours of M correspond to the isotropic lines of C, and there are q^3+1 of them. □

3.6 T is a tree

To show that T is a tree, we give every vertex a *height* relative to a fixed vertex Λ_0 of type 1: roughly, the number of factors of π^{-1} needed to fit it inside Λ_0. We show that each edge changes the height by exactly one, and that every vertex other than Λ_0 has exactly one neighbour below it. A cycle would then have a highest vertex with two neighbours below it, which is impossible (Figure 7); and following the neighbours below leads from any vertex down to Λ_0.

For a lattice X let $\mu(X) = \min\{i \in \mathbb{Z} :\ X \subseteq \pi^{-i}\Lambda_0\}$. The height is

$$\mathrm{ht}(\Lambda) = 2\mu(\Lambda) \ \text{ for type 1}, \qquad \mathrm{ht}(M) = 2\mu(M^\#) - 1 \ \text{ for type 3}.$$

For instance, in the apartment of Example 3.7 with $\Lambda_0 = \Lambda_{0,0}$, the height of every vertex $\Lambda_{i,j}$ of the path equals its distance from Λ_0 along the path. A neighbour of a vertex is *lower* if its height is smaller.

Proposition 3.10. *T is a tree.*

Proof. Step 1: heights are nonnegative, and only Λ_0 has height 0. Let Λ have type 1. If $\Lambda \subseteq \Lambda_0$ then $\Lambda = \Lambda_0$ by Lemma 3.5. If $\Lambda \subseteq \pi\Lambda_0$, then $\pi^{-1}\Lambda_0 \subseteq \pi^{-1}\Lambda_0^\# \subseteq \Lambda^\# \subseteq \pi^{-1}\Lambda \subseteq \Lambda_0$, which is absurd. So $\mu(\Lambda) \geq 0$, with equality only for Λ_0. Let M have type 3. If $M^\# \subseteq \Lambda_0$, then dualising gives $\Lambda_0 \subseteq \Lambda_0^\# \subseteq M \subseteq M^\# \subseteq \Lambda_0$, so all are equal, which is absurd as the types differ. So $\mu(M^\#) \geq 1$ and $\mathrm{ht}(M) \geq 1$.

Step 2: adjacent vertices have heights differing by exactly 1. If M and Λ are adjacent, then by (5) $\Lambda \subseteq M^\#$ and $M^\# \subseteq \pi^{-1}M \subseteq \pi^{-1}\Lambda$, so $\mu(\Lambda) \leq \mu(M^\#) \leq \mu(\Lambda) + 1$. Hence $\mathrm{ht}(\Lambda) - \mathrm{ht}(M) = 2\big(\mu(\Lambda) - \mu(M^\#)\big) + 1$ is $+1$ or -1.

Step 3: a vertex $\Lambda \neq \Lambda_0$ of type 1 has exactly one lower neighbour, namely $\Lambda \cap \pi^{1-k}\Lambda_0$, where $k = \mu(\Lambda) \geq 1$. We first show that $\pi^k \Lambda_0^\# \subseteq \Lambda$, or equivalently (dualising) that $\Lambda^\# \subseteq \pi^{-k}\Lambda_0$. The lattice $\Lambda^\# \cap \pi^{-k}\Lambda_0$ lies between Λ and $\Lambda^\#$, and $\operatorname{len}(\Lambda^\#/\Lambda) = 1$. Suppose it were Λ. Dualising, $\Lambda + \pi^k\Lambda_0^\# = \Lambda^\#$, so $\Lambda^\# = \Lambda + \mathfrak{o}u$ for some $u \in \pi^k\Lambda_0^\#$. Since $\Lambda_0^\# \subseteq \pi^{-1}\Lambda_0$, we have $H(\Lambda_0^\#, \Lambda_0^\#) \subseteq \pi^{-1}\mathfrak{o}$, so $H(u,u) \in \pi^{2k-1}\mathfrak{o} \subseteq \mathfrak{o}$; moreover $H(u,\Lambda) \subseteq \mathfrak{o}$ and $H(\Lambda,\Lambda) \subseteq \mathfrak{o}$. Hence $H(\Lambda^\#, \Lambda^\#) \subseteq \mathfrak{o}$, that is, $\Lambda^\# \subseteq (\Lambda^\#)^\# = \Lambda$, which is false.

A neighbour M is lower exactly when $\mu(M^\#) = k$, that is, when $M^\# \subseteq \pi^{-k}\Lambda_0$, or equivalently when $\pi^k\Lambda_0^\# \subseteq M$. Let Z be the image of $\pi^k\Lambda_0^\#$ in $A = \Lambda/\pi\Lambda^\#$. In the notation of the proof of Proposition 3.9, M corresponds to an isotropic line P with $M/\pi\Lambda^\# = P^\perp$, and M is lower exactly when $Z \subseteq P^\perp$, that is, when $P \subseteq Z^\perp$. Now

$$Z^\perp = \{x \in \Lambda :\ H(x, \pi^k\Lambda_0^\#) \subseteq \pi\mathfrak{o}\}/\pi\Lambda^\# = (\Lambda \cap \pi^{1-k}\Lambda_0)/\pi\Lambda^\#,$$

since $\pi^k H(x, \Lambda_0^\#) \subseteq \pi\mathfrak{o}$ means $\pi^{k-1}x \in (\Lambda_0^\#)^\# = \Lambda_0$. This subspace $Y = Z^\perp$ is proper, because $\Lambda \not\subseteq \pi^{1-k}\Lambda_0$ by the minimality of $\mu(\Lambda)$. And $Z \subseteq Y$, because $\pi^k\Lambda_0^\# \subseteq \pi^{k-1}\Lambda_0 \subseteq \pi^{1-k}\Lambda_0$ (as $k \geq 1$). From $\dim Y + \dim Z = 3$, $Z \subseteq Y$ and $Y \neq A$ we get $\dim Y = 2$, and the line $Z = Y^\perp$ is isotropic with $Y = Z^\perp$. By Lemma 3.8(c), Z is the only isotropic line in Y. So Λ has exactly one lower neighbour, the preimage of $Z^\perp = Y$, which is $\Lambda \cap \pi^{1-k}\Lambda_0$.

Step 4: a vertex M of type 3 has exactly one lower neighbour. Put $j = \mu(M^\#) - 1 \geq 0$. A neighbour Λ is lower exactly when $\mu(\Lambda) = j$, that is, when $\Lambda \subseteq \pi^{-j}\Lambda_0$.

At most one. If $j = 0$, the only possibility is Λ_0 (Step 1). Let $j \geq 1$. If $M \not\subseteq \pi^{-j}\Lambda_0$ there is no lower neighbour, since $M \subset \Lambda$. Otherwise put

$$M' = M^\# \cap \pi^{-j}\Lambda_0 \ \supseteq M, \qquad W = M'/M \subseteq C = M^\#/M.$$

By the proof of Proposition 3.9, the lower neighbours correspond to the isotropic lines of C contained in W. The subspace W is proper, because $M^\# \not\subseteq \pi^{-j}\Lambda_0$ by the minimality of $\mu(M^\#)$. Its orthogonal in C is

$$W^\perp = \{x \in M^\# :\ H(x, M') \subseteq \mathfrak{o}\}/M = (M^\# \cap M'^\#)/M = (M + \pi^j\Lambda_0^\#)/M,$$

because $M'^\# = M + \pi^j\Lambda_0^\#$ by (2), and $\pi^j\Lambda_0^\# \subseteq M^\#$ (dualise $M \subseteq \pi^{-j}\Lambda_0$). Moreover $\pi^j\Lambda_0^\# \subseteq \pi^{j-1}\Lambda_0 \subseteq \pi^{-j}\Lambda_0$ since $j \geq 1$; hence $\pi^j\Lambda_0^\# \subseteq M'$ and $W^\perp \subseteq W$. As in Step 3, $\dim W = 2$, the line $P = W^\perp$ is isotropic, and it is the only isotropic line in W. So in this case M has exactly one lower neighbour, the preimage $M + \pi^j\Lambda_0^\#$ of P.

At least one. Suppose that no neighbour of M is lower, and let Λ be any neighbour of M. Then $\operatorname{ht}(\Lambda) = \operatorname{ht}(M) + 1 \geq 2$, so $\Lambda \neq \Lambda_0$, $\mu(\Lambda) = j + 1$, and M is a lower neighbour of Λ. By Step 3, $M = \Lambda \cap \pi^{-j}\Lambda_0$; in particular $M \subseteq \pi^{-j}\Lambda_0$. If $j = 0$, this says $M \subset \Lambda_0$, so Λ_0 is a lower neighbour of M; if $j \geq 1$, the paragraph above provides a lower neighbour. Either way we reach a contradiction.

Step 5: no cycles. Suppose T had a cycle, and let u be a vertex of maximal height on it. Its two neighbours on the cycle are distinct, and by Step 2 their heights are $\operatorname{ht}(u) \pm 1$; by maximality both equal $\operatorname{ht}(u) - 1$. In particular $\operatorname{ht}(u) \geq 1$, so $u \neq \Lambda_0$ by Step 1. Thus u has two distinct lower neighbours, contradicting Step 3 or Step 4.

Step 6: connectedness. Starting from any vertex X and passing repeatedly to the lower neighbour, the height drops by one at each step (Steps 3 and 4) and stays nonnegative, so after $\operatorname{ht}(X)$ steps we reach the only vertex of height 0, which is Λ_0. So every vertex is joined to Λ_0 by a path. □

Remark 3.11. By Propositions 3.9 and 3.10, T is the (q^3+1)-regular tree. It is the Bruhat–Tits building of $SU(V)$, which has relative rank one; the identification of this building with a space of norms is due to Bruhat and Tits [7, Théorème 2.12], and a description by lattices of this kind appears, for $F = \mathbb{Q}_p$ with p odd, in Vollaard and Wedhorn [31, §3.1]. We do not use these identifications.

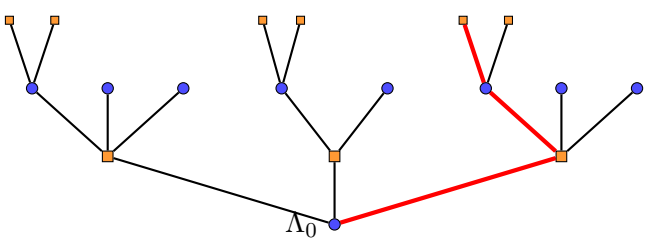

Figure 7: Heights (schematic, fewer branches drawn).

3.7 The special unitary group acts with two orbits

A unitary map g sends lattices to lattices, preserves inclusions and lengths, and satisfies $(gX)^\# = g(X^\#)$. Hence it maps vertex lattices to vertex lattices of the same type and adjacent pairs to adjacent pairs. So $U(V)$, *and in particular* $SU(V)$, *acts on* T *by type-preserving symmetries.* The stabiliser of a vertex X is $SU(V) \cap GL(X)$, where $GL(X) = \{g : gX = X\}$ is a compact open subgroup of $GL(V)$; so vertex stabilisers are compact open subgroups of $SU(V)$.

Lemma 3.12 (Normal form)**.** *Every vertex lattice* X *has an* $\mathfrak{o}$*-basis* $z_1, \dots, z_4$ *with* $H(z_i, z_j) = 0$ *for* $i \neq j$ *and* $H(z_i, z_i) = \pi^{s_i}$*, where* $s_i \in \{0, 1\}$ *and* $s_1 + \cdots + s_4 = t(X)$*.*

Proof. Step 1: splitting off a vector. Let Y be a lattice with $H(Y, Y) \subseteq \mathfrak{o}$, and let s be the least valuation of the values $H(x, y)$, $x, y \in Y$. We claim that some $z \in Y$ has $v(H(z, z)) = s$. Suppose $v(H(x, y)) = s$ but $H(x, x)$ and $H(y, y)$ have larger valuation. Write $H(x, y) = \pi^s c$ with c a unit, and choose $b \in \mathfrak{o}$ with $\mathrm{Tr}(bc)$ a unit (Lemma 3.1(a)). Then $H(x + by, x + by) = H(x, x) + \pi^s \mathrm{Tr}(bc) + \mathrm{N}(b)H(y, y)$ has valuation exactly s. Given such a z, every $x \in Y$ satisfies $H(z, x) \in \pi^s \mathfrak{o} = H(z, z)\mathfrak{o}$, so $x - \frac{H(z,x)}{H(z,z)} z \in Y \cap z^\perp$. Hence $Y = \mathfrak{o}z \perp (Y \cap z^\perp)$.

Step 2: the basis. Applying Step 1 repeatedly gives an orthogonal basis z_i of X. Each $H(z_i, z_i)$ lies in F, and multiplying z_i by a unit c multiplies it by $\mathrm{N}(c)$; by Lemma 3.1(b) we may assume $H(z_i, z_i) = \pi^{s_i}$. Then $X^\# = \bigoplus \pi^{-s_i} \mathfrak{o} z_i$, and the conditions $X \subseteq X^\# \subseteq \pi^{-1} X$ say exactly that $s_i \in \{0, 1\}$. Finally $t(X) = \mathrm{len}(X^\#/X) = \sum s_i$. □

Proposition 3.13. $SU(V)$ *acts on the vertices of* T *with exactly two orbits, the vertex lattices of type* 1 *and those of type* 3*, and with compact open stabilisers.*

Proof. Let X, X' be vertex lattices of the same type, with bases z_i and z_i' as in Lemma 3.12, ordered so that $H(z_i, z_i) = H(z_i', z_i')$. The linear map g with $gz_i = z_i'$ is unitary and maps X onto X'. Its determinant d satisfies $\mathrm{N}(d) = 1$ (compare Gram matrices), so d is a unit. Let s multiply z_1 by d^{-1} and fix z_2, z_3, z_4. Then s is unitary, preserves X, and $gs \in SU(V)$ maps X onto X'. Both types occur (Example 3.7), and $SU(V)$ preserves types. □

3.8 Displacement and eigenvalues

We come to the estimate that links the tree to the certificate. Each step from a vertex to the next vertex of the same type, two edges away, enlarges a lattice by at most one factor of π^{-1}. So an element moving a vertex a distance $2k$ requires denominators π^{-k}, and its eigenvalues have valuation at least $-k$. The second ingredient is that a unitary element has at most *one* eigenvalue of negative valuation. This is where the Witt index enters: the eigenvectors with such eigenvalues span a totally isotropic subspace. Together these give $|\det(g - I)| \leq q^k$.

By the *eigenvalues* of a linear map g of V we mean the roots of its characteristic polynomial in $\overline{F}$, counted with multiplicity.

Lemma 3.14. *If there is a walk of length $2k$ in T from a vertex X to a vertex X', then $X' \subseteq \pi^{-k} X$.*

Proof. By (5), each step $Y \to Y'$ of the walk satisfies $Y' \subseteq Y$ if it goes from type 1 to type 3, and $Y' \subseteq \pi^{-1} Y$ if it goes from type 3 to type 1. Steps of the two kinds alternate, so every two consecutive steps contribute one factor of π^{-1}. □

Lemma 3.15 (One expanding eigenvalue)**.** *Let $g \in U(V)$. At most one eigenvalue of g, counted with multiplicity, has negative valuation.*

Proof. Step 1: the expanding subspace. Let f be the characteristic polynomial of g and factor it over F' into irreducible factors. The roots of one irreducible factor are conjugate over F', so they have the same valuation. Let f_- be the product of the irreducible factors (with multiplicity) whose roots have negative valuation, and $f = f_- f_+$. Since f_- and f_+ are coprime, $V = V_- \oplus V_+$ with $V_\pm = \ker f_\pm(g)$, and f_- is the characteristic polynomial of g on V_-. So $\dim V_-$ is the number of eigenvalues of negative valuation, and it suffices to show that V_- is totally isotropic, because the Witt index is one.

Step 2: the inverse contracts V_-. Let $\tilde{g}$ be the restriction of g^{-1} to V_- and $m = \dim V_-$. The eigenvalues of $\tilde{g}$ are the inverses of those of g on V_-, so they have positive valuation, and the coefficients $c_0, \dots, c_{m-1}$ of its characteristic polynomial lie in F' and have positive valuation: $c_i \in \pi\mathfrak{o}$. Choose any lattice Y_0 in V_- and put $Y = Y_0 + \tilde{g}Y_0 + \cdots + \tilde{g}^{m-1}Y_0$. By the Cayley–Hamilton theorem $\tilde{g}^m = -\sum_{i<m} c_i \tilde{g}^i$, so $\tilde{g}^m Y_0 \subseteq \pi Y$. It follows that $\tilde{g}Y \subseteq Y$ and then $\tilde{g}^m Y \subseteq \pi Y$, hence $\tilde{g}^{mj} Y \subseteq \pi^j Y$ for all $j \geq 1$.

Step 3: V_- is totally isotropic. Let $x, y \in Y$. Since g is unitary,

$$H(x,y) = H\big(g^{-mj}x,\, g^{-mj}y\big) = H\big(\tilde{g}^{mj}x, \tilde{g}^{mj}y\big) \in H(\pi^j Y, \pi^j Y) = \pi^{2j} H(Y,Y).$$

As $H(Y,Y) \subseteq \pi^{-c}\mathfrak{o}$ for some fixed c, letting $j \to \infty$ gives $H(x,y) = 0$. Since Y spans V_-, the subspace V_- is totally isotropic. □

Proposition 3.16 (Displacement controls the certificate)**.** *Let $g \in SU(V)$, and suppose that T contains a walk of length $2k$ from a vertex X to gX. Then every eigenvalue λ of g satisfies $v(\lambda) \geq -k$, and*

$$|\det(g - I)| \leq q^k.$$

Proof. By Lemma 3.14, $gX \subseteq \pi^{-k} X$, so $\pi^k g$ maps X into itself. Its matrix in an $\mathfrak{o}$-basis of X has entries in $\mathfrak{o}$, so its characteristic polynomial is monic with coefficients in $\mathfrak{o}$, and its eigenvalues $\pi^k\lambda$ have nonnegative valuation. This proves $v(\lambda) \geq -k$. Next, $\det(g - I) = \prod_i (\lambda_i - 1)$, and $v(\lambda_i - 1) \geq \min(0, v(\lambda_i))$ by the ultrametric inequality. By Lemma 3.15 at most one λ_i has negative valuation, and its valuation is at least $-k$. Hence $v(\det(g - I)) \geq -k$. □

For the upper bound in Section 8 we also need a converse: an element with an eigenvalue of valuation $-k < 0$ moves some vertex a distance at most $2k$. The proof constructs an apartment, as in Example 3.7, along which g acts by translation.

Proposition 3.17 (An axis)**.** *Let $g \in SU(V)$ have an eigenvalue of negative valuation. Then this valuation is an integer $-k$, and there are a vertex Λ of type 1 and a walk of length $2k$ in T from Λ to $g\Lambda$.*

Proof. Step 1: the eigenvalues. By Lemma 3.15, applied to g and to g^{-1}, the element g has at most one eigenvalue of negative and at most one of positive valuation. Since $\det g = 1$, the valuations of the four eigenvalues add up to 0, so they are $-k, 0, 0, k$ for some $k > 0$. As in

the proof of Lemma 3.15 we get a decomposition $V = V_- \oplus V_0 \oplus V_+$ into g-stable subspaces of dimensions $1, 2, 1$. Write $V_- = F'e$ and $V_+ = F'f$; then $ge = ae$ and $gf = bf$ with $a, b \in F'$, $v(a) = -k$ and $v(b) = k$. In particular k is an integer. By Step 3 of that proof (applied to g and g^{-1}), $H(e, e) = H(f, f) = 0$.

Step 2: orthogonality. For $y \in V_0$ we have $H(e, y) = H(ge, gy) = \overline{a}\, H(e, gy)$, that is, $H\big(e, (\overline{a}g - 1)y\big) = 0$. The eigenvalues of $\overline{a}g - 1$ on V_0 are $\overline{a}\mu - 1$ with $v(\mu) = 0$, so they are nonzero and $\overline{a}g - 1$ maps V_0 onto itself. Hence $H(e, V_0) = 0$, and likewise $H(f, V_0) = 0$. Since H is nondegenerate and e is orthogonal to e and to V_0, we have $H(e, f) \neq 0$; rescale f so that $H(e, f) = 1$. Then $W = V_0$ is the orthogonal complement of the hyperbolic plane spanned by e, f.

Step 3: the anisotropic plane. W contains no isotropic vector w, for otherwise e and w would span a totally isotropic plane. Take an orthogonal basis z_1, z_2 of W. If $H(z_1, z_1)$ and $H(z_2, z_2)$ had valuations of the same parity, then by Lemma 3.1(c) we could write $-H(z_2, z_2)/H(z_1, z_1) = \mathrm{N}(c)$, and $cz_1 + z_2$ would be isotropic. So the parities differ, and after rescaling by powers of π we may assume $v(H(z_1, z_1)) = 0$ and $v(H(z_2, z_2)) = 1$. For $z = xz_1 + yz_2$ the two terms of $H(z, z) = \mathrm{N}(x)H(z_1, z_1) + \mathrm{N}(y)H(z_2, z_2)$ have valuations of different parity, so $v(H(z, z)) = \min(2v(x), 1 + 2v(y))$. Consequently

$$\Lambda_W = \mathfrak{o}z_1 \oplus \mathfrak{o}z_2 = \{z \in W : \ v(H(z, z)) \geq 0\}.$$

This description shows that $g\Lambda_W = \Lambda_W$, because g preserves W and H.

Step 4: the apartment. For integers i, j put $\Lambda_{i,j} = \pi^i \mathfrak{o}e \oplus \Lambda_W \oplus \pi^j \mathfrak{o}f$. Exactly as in Example 3.7, $\Lambda_{i,j}^{\#} = \pi^{-j}\mathfrak{o}e \oplus (\mathfrak{o}z_1 \oplus \pi^{-1}\mathfrak{o}z_2) \oplus \pi^{-i}\mathfrak{o}f$, so $\Lambda_{i,j}$ is a vertex lattice when $i + j \in \{0, 1\}$, and $\Lambda_{0,0} \supset \Lambda_{0,1} \subset \Lambda_{-1,1} \supset \cdots \subset \Lambda_{-k,k}$ is a walk of length $2k$. Finally $g\Lambda_{0,0} = a\mathfrak{o}e \oplus \Lambda_W \oplus b\mathfrak{o}f = \Lambda_{-k,k}$, because $v(a) = -k$ and $v(b) = k$. □

4 The division algebra and its unitary group

We now construct the matrices that will act on the tree. Section 5 needs four properties of them:

- they lie in a *division algebra*, so that $w - I$ is invertible whenever $w \neq I$;
- they are *unitary for a positive definite form* at every real place, so that their eigenvalues lie on the unit circle;
- their entries are *integral away from one prime* $\mathfrak{p}$, in the sense of an order, so that divisibility by an ideal can be measured;
- at $\mathfrak{p}$ they act on a *four-dimensional hermitian space of Witt index one*, and hence on its tree.

A division algebra is an algebra in which every nonzero element has an inverse. The quaternions are the classical example, and they are what LPS use. Here we need an algebra of degree four, of dimension 16 over its centre, which we write down explicitly as an algebra of 4×4 matrices: the classical *cyclic algebra* construction. It is the degree four that yields divisibility by $\mathfrak{a}^4$.

4.1 The fields

We fix the following data.

(A1) K is a totally real number field of degree r, and E is a CM field which is a quadratic extension of K. We write $x \mapsto \overline{x}$ for the nontrivial automorphism of E over K; under every embedding $E \to \mathbb{C}$ it is complex conjugation. L_0 is a totally real cyclic extension of K of degree 4, and $L = L_0E$. Restriction identifies $\mathrm{Gal}(L/E)$ with $\mathrm{Gal}(L_0/K)$, and

we fix a generator σ. Complex conjugation $x \mapsto \overline{x}$ on the CM field L is trivial on L_0 and commutes with σ; the fixed field of σ is E.

(A2) $\gamma \in E$ satisfies $\gamma\overline{\gamma} = 1$, and there is a prime ideal $\mathfrak{w}$ of E such that $\mathfrak{w}$ is inert in L (that is, $\mathfrak{w}\mathcal{O}_L$ is a prime ideal) and the $\mathfrak{w}$-adic valuation of γ is 1.

4.2 The matrices

For $a \in L$ put $\rho(a) = \operatorname{diag}(a, \sigma a, \sigma^2 a, \sigma^3 a)$, and let

$$U = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ \gamma & 0 & 0 & 0 \end{pmatrix}.$$

One checks directly that

$$U^4 = \gamma I, \qquad U\rho(a)U^{-1} = \rho(\sigma a), \qquad UU^* = I, \tag{6}$$

where U^* is the conjugate transpose, formed with the conjugation of L (the last identity uses $\gamma\overline{\gamma} = 1$).

Definition 4.1. Let D be the set of all matrices

$$X = \sum_{i=0}^{3} \rho(a_i)U^i = \begin{pmatrix} a_0 & a_1 & a_2 & a_3 \\ \gamma\,\sigma a_3 & \sigma a_0 & \sigma a_1 & \sigma a_2 \\ \gamma\,\sigma^2 a_2 & \gamma\,\sigma^2 a_3 & \sigma^2 a_0 & \sigma^2 a_1 \\ \gamma\,\sigma^3 a_1 & \gamma\,\sigma^3 a_2 & \gamma\,\sigma^3 a_3 & \sigma^3 a_0 \end{pmatrix}, \qquad a_0, \dots, a_3 \in L.$$

By (6) we have $\rho(a)U^i \cdot \rho(b)U^j = \rho(a\,\sigma^i b)\,U^{i+j}$ and $U^4 = \rho(\gamma)$. Hence D is closed under multiplication: it is a ring of matrices, and a vector space of dimension 16 over E, which acts by the scalar matrices $\rho(e) = eI$. The first row of X is $(a_0, \dots, a_3)$, so X determines the a_i. Finally, D is closed under conjugate transpose, because $(\rho(a)U^i)^* = U^{-i}\rho(\overline{a}) = \rho(\sigma^{-i}\overline{a})U^{-i}$ and $U^{-1} = \overline{\gamma}\,U^3$.

The proof of the next proposition follows the argument that a product of two nonzero polynomials is nonzero: one compares *leading terms*. The role of the degree is played by a valuation at the prime $\mathfrak{w}$ of (A2), extended to D so that U has "degree" $\frac{1}{4}$. The four components of a matrix then have degrees with distinct fractional parts $0, \frac{1}{4}, \frac{1}{2}, \frac{3}{4}$. They cannot cancel one another, and this forces the leading terms to multiply.

Proposition 4.2 (D is a division algebra)**.** *Every nonzero $X \in D$ is an invertible matrix, and $X^{-1} \in D$. The centre of D consists of the scalar matrices eI, $e \in E$.*

Proof. Step 1: a valuation on L. Let $v_{\mathfrak{w}} \colon L^\times \to \mathbb{Z}$ be the valuation attached to the prime ideal $\mathfrak{w}\mathcal{O}_L$. Since $\mathfrak{w}$ is inert in L, $v_{\mathfrak{w}}$ restricts to the $\mathfrak{w}$-adic valuation on E, so $v_{\mathfrak{w}}(\gamma) = 1$. Moreover $v_{\mathfrak{w}}(\sigma x) = v_{\mathfrak{w}}(x)$ for all $x \in L$, because σ fixes E and hence maps $\mathfrak{w}\mathcal{O}_L$ to itself.

Step 2: a degree on D. For a nonzero matrix $X = \sum_i \rho(a_i)U^i$, define

$$\deg X = \min\Big\{\, v_{\mathfrak{w}}(a_i) + \tfrac{i}{4} \;:\; a_i \neq 0 \,\Big\}.$$

The numbers $v_{\mathfrak{w}}(a_i) + \frac{i}{4}$ have different fractional parts, so they are pairwise distinct, and the minimum is attained at exactly one index. We call it the *leading index* of X.

Step 3: leading terms multiply. Let $X = \sum_i \rho(a_i)U^i$ and $Y = \sum_j \rho(b_j)U^j$ be nonzero, with leading indices i_0 and j_0. By (6),

$$XY = \sum_{i,j} \rho\big(a_i\,\sigma^i(b_j)\big)\,U^{i+j},$$

and whenever $i+j \geq 4$ we replace U^{i+j} by $\rho(\gamma)U^{i+j-4}$. After this replacement the pair (i,j) contributes a term $\rho(c_{ij})U^s$, where $s \in \{0,1,2,3\}$ is the residue of $i+j$ modulo 4, and c_{ij} equals $a_i\sigma^i(b_j)$ or $\gamma\, a_i\sigma^i(b_j)$. In either case, by Step 1,

$$v_{\mathfrak{w}}(c_{ij}) + \tfrac{s}{4} = \Big(v_{\mathfrak{w}}(a_i) + \tfrac{i}{4}\Big) + \Big(v_{\mathfrak{w}}(b_j) + \tfrac{j}{4}\Big).$$

Consider the coefficient of U^{s_0}, where s_0 is the residue of $i_0 + j_0$. It is the sum of the c_{ij} over the pairs with $i + j \equiv s_0$. By the displayed identity each of these has valuation at least $\deg X + \deg Y - \frac{s_0}{4}$, with equality only for the pair (i_0, j_0). A sum in which a single term has strictly smallest valuation is nonzero, so this coefficient is nonzero, and $XY \neq 0$.

Step 4: inverses. Fix $X \neq 0$. By Step 3 the map $Y \mapsto XY$ from D to itself is injective. It is E-linear and D is finite-dimensional over E, so it is also surjective; in particular $XY = I$ for some $Y \in D$. Hence X is invertible, with $X^{-1} = Y \in D$.

Step 5: the centre. If $X = \sum_i \rho(a_i)U^i$ commutes with every $\rho(b)$, then $a_i(\sigma^i b - b) = 0$ for all $b \in L$, so $a_i = 0$ for $i \neq 0$. If $\rho(a_0)$ also commutes with U, then $\sigma a_0 = a_0$, so $a_0 \in E$. □

Remark 4.3. In particular a matrix $w \neq I$ in D never has eigenvalue 1, because $w - I \in D$ is nonzero and hence invertible. In M_4 itself many matrices $w \neq I$ have eigenvalue 1, and the argument below would say nothing about them.

We also need that determinants and characteristic polynomials of elements of D lie in E.

Lemma 4.4. *For $X \in D$, the characteristic polynomial $\det(tI - X)$ has coefficients in E, and that of X^* is obtained by applying $x \mapsto \overline{x}$ to its coefficients. In particular $\det X \in E$ and $\det(X^*) = \overline{\det X}$.*

Proof. By (6), $UXU^{-1} = \sum_i \rho(\sigma a_i)U^i$, and comparing with the explicit form of X (using $\sigma\gamma = \gamma$ and $\sigma^4 = 1$) shows that this is exactly the matrix obtained from X by applying σ to every entry. Hence the characteristic polynomial of X is fixed by σ, so its coefficients lie in E. The second statement holds for any matrix, because conjugation commutes with taking determinants. □

4.3 The involution and the unitary group

The matrices $\rho(a)$ are diagonal, U is unitary, and conjugate transposition maps D to itself. To obtain a unitary group with the right behaviour at the prime $\mathfrak{p}$, we twist conjugate transposition by a positive element of D.

(A3) $\theta \in D$ satisfies $\theta^* = \theta$, and for every embedding $\iota\colon L \to \mathbb{C}$ the hermitian matrix $\iota(\theta)$ is positive definite.

Here and below, $\iota(X)$ denotes the complex matrix obtained by applying ι to the entries of X. Since L is a CM field, $\iota(\overline{x}) = \overline{\iota(x)}$ for $x \in L$, so $\iota(X^*) = \iota(X)^*$.

Definition 4.5 (The unitary group)**.** For $X \in D$ put $\tau(X) = \theta^{-1}X^*\theta$, and let

$$G = \{w \in D :\ w^*\theta w = \theta,\ \det w = 1\} = \{w \in D :\ \tau(w)w = I,\ \det w = 1\}.$$

The map τ is an anti-automorphism of D with $\tau^2 = \mathrm{id}$, acting on the centre E by $e \mapsto \overline{e}$; such a map is called an *involution of the second kind*. G is a group, since $w^{-1} = \tau(w) \in D$.

Lemma 4.6. *Let $w \in G$ and let $\iota\colon L \to \mathbb{C}$ be an embedding. Every eigenvalue of $\iota(w)$ has absolute value* 1*, and $|\iota(\det(w - I))| \leq 16$.*

Proof. The matrix $\iota(w)$ preserves the positive definite hermitian form $\langle x, y\rangle = x^*\iota(\theta)y$ on $\mathbb{C}^4$. If $\iota(w)x = \lambda x$ with $x \neq 0$, then $\langle x, x\rangle = |\lambda|^2\langle x, x\rangle$, so $|\lambda| = 1$. Hence $|\iota(\det(w - I))| = \prod_i |\lambda_i - 1| \leq 2^4$. □

4.4 Orders

To speak of congruences we need a notion of integrality in D. An *order* of D is a subring $\mathcal{O} \subset D$ which contains $\mathcal{O}_E$ (as scalar matrices), is finitely generated as a module over the ring of integers $\mathcal{O}_K$, and spans D over K. We will always assume that $\mathcal{O}$ is τ*-stable*: $\tau(\mathcal{O}) = \mathcal{O}$.

For a finite place v of K, with completion K_v, ring of integers $\mathcal{O}_{K_v}$ and uniformiser π_v, we write $D_v = D \otimes_K K_v$ and $\mathcal{O}_v = \mathcal{O} \otimes_{\mathcal{O}_K} \mathcal{O}_{K_v}$. The matrices of D have entries in L, so those of D_v have entries in $L \otimes_K K_v$, and determinants of elements of D_v lie in $E \otimes_K K_v$ by Lemma 4.4. We put $S_v = \mathcal{O}_E \otimes_{\mathcal{O}_K} \mathcal{O}_{K_v}$, the integral closure of $\mathcal{O}_{K_v}$ in $E \otimes_K K_v$.

Lemma 4.7 (Integrality)**.** *Let v be a finite place of K and $y \in \mathcal{O}_v$. Then the coefficients of the characteristic polynomial of y lie in S_v. In particular* $\det y \in S_v$.

Proof. Left multiplication by y maps $\mathcal{O}_v$, a free $\mathcal{O}_{K_v}$-module of rank 32, into itself, so its characteristic polynomial χ has coefficients in $\mathcal{O}_{K_v}$. Let Ω be an algebraically closed field containing K_v, and let $\iota\colon L \to \Omega$ be a K-embedding. The map $X \otimes c \mapsto c\,\iota(X)$ is a homomorphism from $D \otimes_{E,\iota} \Omega$ to $M_4(\Omega)$; it is nonzero, and $D \otimes_{E,\iota} \Omega$ is a simple algebra of dimension 16 over Ω (its centre is Ω by Proposition 4.2), so it is an isomorphism. Since $D \otimes_K \Omega$ is the product of the two algebras $D \otimes_{E,\iota} \Omega$ obtained from the two embeddings of E, left multiplication by y on $D \otimes_K \Omega$ has among its eigenvalues those of the matrix $\iota(y)$. These are therefore roots of χ, hence integral over $\mathcal{O}_{K_v}$, and so are the coefficients of the characteristic polynomial of $\iota(y)$. As ι ranges over the embeddings, this shows that the coefficients of the characteristic polynomial of y, which lie in $E \otimes_K K_v$, are integral at every place above v, that is, lie in S_v. □

4.5 The local model at $\mathfrak{p}$

Finally we let D act on a hermitian space over a local field. Fix a prime $\mathfrak{p}$ of K such that:

(A4) $\mathfrak{p}$ is inert in E; the extension L/E is unramified at $\mathfrak{P} = \mathfrak{p}\mathcal{O}_E$; and γ is a unit at $\mathfrak{P}$.

Put $q = \mathrm{N}(\mathfrak{p})$, $F = K_\mathfrak{p}$, and $F' = E \otimes_K K_\mathfrak{p} = E_\mathfrak{P}$, the unramified quadratic extension of F. Its conjugation is induced by that of E, and $E \subset F'$. For a matrix Z over F' we write $Z^\dagger$ for its conjugate transpose.

Proposition 4.8 (The local model)**.** *There are an injective ring homomorphism $\varphi\colon D \to M_4(F')$, which is the identity on the centre $E \subset F'$, and an invertible hermitian matrix $H \in M_4(F')$, such that for all $X \in D$:*

(a) $\varphi(X)$ and X have the same characteristic polynomial; in particular $\det \varphi(X) = \det X$*;*

(b) $\varphi(\tau(X)) = H^{-1}\varphi(X)^\dagger H$.

The matrix H is determined by φ up to a factor in $F^\times$, and the parity of $v(\det H)$ does not depend on the choices.

Proof. Step 1: a splitting. Let $L_\mathfrak{P} = L \otimes_E F'$, a commutative F'-algebra of dimension 4 on which σ acts. By (A4) it is a product of fields $F_1 \times \cdots \times F_s$, each unramified over F'. The argument of Lemma 3.1(b), with the residue norm and trace of F_1/F', shows that every unit of F' is a norm from F_1. The norm map of $L_\mathfrak{P}$ to F' is $x \mapsto x\,\sigma(x)\,\sigma^2(x)\,\sigma^3(x)$, and it sends $(b_1, 1, \dots, 1)$ to $\mathrm{N}_{F_1/F'}(b_1)$; so there is $b \in L_\mathfrak{P}^\times$ with $b\,\sigma(b)\,\sigma^2(b)\,\sigma^3(b) = \gamma$. Let $\varphi(\rho(a))$ be multiplication by a on $L_\mathfrak{P}$, and $\varphi(U)$ the map $x \mapsto b\,\sigma(x)$. These satisfy the relations (6) that are used to multiply elements of D (namely $\varphi(U)\varphi(\rho(a)) = \varphi(\rho(\sigma a))\varphi(U)$ and $\varphi(U)^4 = \gamma$), so $\varphi(\sum \rho(a_i)U^i) = \sum a_i \varphi(U)^i$ is a ring homomorphism from D to $\mathrm{End}_{F'}(L_\mathfrak{P})$. Its kernel is an ideal of the division algebra D not containing I, so it is injective. Choosing a basis of $L_\mathfrak{P}$ over F' we regard φ as a map to $M_4(F')$.

Step 2: characteristic polynomials. Let Ω be an algebraic closure of F', and choose an E-embedding $\iota\colon L \to \Omega$. As in the proof of Lemma 4.7, both $X \mapsto \iota(X)$ and $X \mapsto \varphi(X)$ extend

to isomorphisms of Ω-algebras $D \otimes_E \Omega \to M_4(\Omega)$. By the Skolem–Noether theorem [30, Main Theorem 7.7.1] two such isomorphisms differ by conjugation by an invertible matrix. So $\iota(X)$ and $\varphi(X)$ have the same characteristic polynomial, and this proves (a) because the coefficients of the characteristic polynomial of X lie in E.

Step 3: the hermitian form. The map $D \otimes_E F' \to M_4(F')$ induced by φ is injective, because $D \otimes_E F'$ is simple, and hence bijective by dimension count. So $\varphi(D)$ spans $M_4(F')$ over F', and $\tau'(\varphi(X)c) = \varphi(\tau(X))\overline{c}$ ($X \in D,\ c \in F'$) defines an anti-automorphism τ' of $M_4(F')$ with $\tau'^2 = \mathrm{id}$ that acts on scalars by conjugation. The map $Z \mapsto \tau'(Z^\dagger)$ is then an F'-linear automorphism of $M_4(F')$, so by Skolem–Noether there is an invertible A with $\tau'(Z^\dagger) = AZA^{-1}$, that is, $\tau'(Z) = AZ^\dagger A^{-1}$. Applying this twice and using $\tau'^2 = \mathrm{id}$ shows that $A(A^\dagger)^{-1}$ commutes with every matrix, so $A = \lambda A^\dagger$ for a scalar λ. Taking conjugate transposes gives $A^\dagger = \overline{\lambda}A$, hence $\lambda\overline{\lambda} = 1$. Then $\lambda = c/\overline{c}$ for some $c \in F'^\times$: take $c = 1 + \lambda$ if $\lambda \neq -1$, and c with $\overline{c} = -c$ if $\lambda = -1$. The matrix $c^{-1}A$ is hermitian, and $H = (c^{-1}A)^{-1}$ satisfies (b).

Step 4: uniqueness. If H' also satisfies (b), then $H'H^{-1}$ commutes with every matrix, so $H' = cH$ with $c \in F'$, and $c \in F$ because both are hermitian. This changes $\det H$ by c^4. Another choice of φ differs by conjugation by an invertible matrix P (Skolem–Noether), which replaces H by $P^\dagger HP$ and $\det H$ by $\det H \cdot \mathrm{N}(\det P)$. Neither change affects the parity of $v(\det H)$. □

We impose the last condition on the data.

(A5) $v(\det H)$ is odd.

From now on let $V = F'^4$ with the hermitian form $H(x, y) = x^\dagger Hy$. By (A5) and Proposition 3.3, (V, H) has Witt index one, and Section 3 gives the $(q^3 + 1)$-regular tree T of vertex lattices in V. If $w \in G$, then $\varphi(w)^\dagger H\varphi(w) = H\varphi(\tau(w)w) = H$ and $\det\varphi(w) = 1$; so $\varphi(w) \in SU(V)$, and G *acts on* T *through* φ *by type-preserving symmetries.* We simply write wX for $\varphi(w)X$.

The following lemma computes H in the situation of our examples.

Lemma 4.9. *Suppose that* $\mathfrak{p}$ *splits completely in* L_0*, and that* $\theta = \rho(\eta)$ *for a totally positive* $\eta \in L_0$*. Then (A3) holds, and one can take* $H = \mathrm{diag}(\psi_0(\eta), \dots, \psi_3(\eta))$*, where* $\psi_0, \dots, \psi_3$ *are the four embeddings of* L_0 *into* F*. (We use the same letters for their extensions* $L = L_0E \to F'$ *that are the identity on* E*.) In particular* $\det H = \mathrm{N}_{L_0/K}(\eta)$*, and (A5) holds if and only if the* $\mathfrak{p}$*-adic valuation of* $\mathrm{N}_{L_0/K}(\eta)$ *is odd.*

Proof. For every ι, the matrix $\iota(\rho(\eta))$ is diagonal with positive entries, so (A3) holds. Since $\mathfrak{p}$ splits completely in L_0, we have $L_\mathfrak{P} = L_0 \otimes_K F' \cong F'^4$, where we order the four embeddings as $\psi_k = \psi_0 \circ \sigma^k$, so that σ acts by $(\sigma x)_k = x_{k+1}$ (indices modulo 4). Take $b = (\gamma, 1, 1, 1)$ in Step 1 of the proof of Proposition 4.8. Then $\varphi(\rho(a)) = \mathrm{diag}(\psi_k(a))$, and $\varphi(U)$ is the cyclic shift with γ in one entry; both satisfy $\varphi(X^*) = \varphi(X)^\dagger$, the second because $\gamma\overline{\gamma} = 1$. Hence $\varphi(\tau(X)) = \varphi(\theta)^{-1}\varphi(X)^\dagger\varphi(\theta)$, and we may take $H = \varphi(\theta) = \mathrm{diag}(\psi_k(\eta))$. □

5 The certificate

We now define the arithmetic groups and prove the bound on $\det(w - I)$. Throughout, the data (A1)–(A5) and a τ-stable order $\mathcal{O}$ are fixed. Let

$$\mathcal{O}_K[1/\mathfrak{p}] = \{x \in K :\ v(x) \geq 0 \text{ for every finite place } v \neq \mathfrak{p}\}, \qquad \mathcal{O}[1/\mathfrak{p}] = \mathcal{O}_K[1/\mathfrak{p}] \cdot \mathcal{O},$$

the elements of D that are integral away from $\mathfrak{p}$.

Definition 5.1 (The arithmetic group)**.**

$$\Gamma = G \cap \mathcal{O}[1/\mathfrak{p}] = \{w \in \mathcal{O}[1/\mathfrak{p}] :\ w^*\theta w = \theta,\ \det w = 1\}, \qquad \Gamma(\mathfrak{a}) = \{w \in \Gamma :\ w - I \in \mathfrak{a}\,\mathcal{O}[1/\mathfrak{p}]\}$$

for a nonzero ideal $\mathfrak{a}$ of $\mathcal{O}_K$ prime to $\mathfrak{p}$.

Γ is a group, because $w^{-1} = \tau(w) \in \mathcal{O}[1/\mathfrak{p}]$ by τ-stability, and $\Gamma(\mathfrak{a})$ is a normal subgroup, the *congruence subgroup* of level $\mathfrak{a}$: if $w, w' \in \Gamma(\mathfrak{a})$ then $ww' - I = (w-I)w' + (w'-I) \in \mathfrak{a}\mathcal{O}[1/\mathfrak{p}]$, and similarly for inverses and conjugates.

Let $w \in \Gamma(\mathfrak{a})$ with $w \neq I$, and consider the number $\det(w - I)$, which we call the *certificate* of w. It is nonzero, because D is a division algebra. It is fixed by complex conjugation, because w is unitary and 4 is even, so it lies in K. At every finite place other than $\mathfrak{p}$ it is divisible by $\mathfrak{a}^4$, because $w - I$ is. At the real places it is at most 16 in absolute value, because w is unitary for a positive definite form. The product formula then forces it to be large at $\mathfrak{p}$ (Figure 8). For $x \in K^\times$ and a finite place v we use the normalised absolute value $|x|_v = \mathrm{N}(v)^{-v(x)}$; at $\mathfrak{p}$ this is the absolute value $|x| = q^{-v(x)}$ of Section 3.

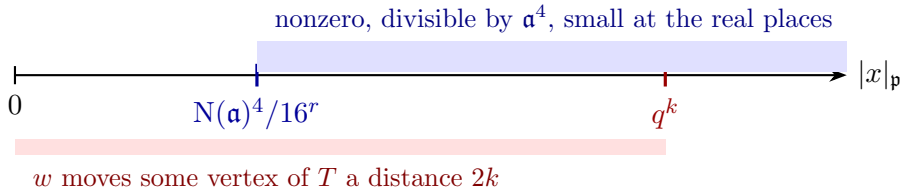

Figure 8: The certificate: the number $x = \det(w - I)$ satisfies both bounds, so $q^k \geq \mathrm{N}(\mathfrak{a})^4/16^r$.

Theorem 5.2 (The certificate)**.** *Let $\mathfrak{a}$ be a nonzero ideal of $\mathcal{O}_K$ prime to $\mathfrak{p}$, let $w \in \Gamma(\mathfrak{a})$ with $w \neq I$, and put $x = \det(w - I)$. Then $x \in K^\times$ and*

$$|x|_\mathfrak{p} \;\geq\; \frac{\mathrm{N}(\mathfrak{a})^4}{16^r}.$$

Proof. $x \neq 0$. By Proposition 4.2, the nonzero matrix $w - I \in D$ is invertible.

$x \in K$. By Lemma 4.4, $x \in E$. From $w^*\theta w = \theta$ we get $w^* = \theta w^{-1}\theta^{-1}$, so

$$\overline{x} = \det(w^* - I) = \det(w^{-1} - I) = \det(w^{-1})\det(I - w) = (-1)^4 \det(w - I) = x.$$

So x is fixed by $x \mapsto \overline{x}$, and lies in K.

Finite places $v \neq \mathfrak{p}$. Let $j = v(\mathfrak{a})$. Since $w - I \in \mathfrak{a}\mathcal{O}[1/\mathfrak{p}]$ and $\mathfrak{a}\mathcal{O}_{K_v} = \pi_v^j \mathcal{O}_{K_v}$, we can write $w - I = \pi_v^j y$ with $y \in \mathcal{O}_v$. Then $x = \pi_v^{4j} \det y$, and $\det y \in S_v$ by Lemma 4.7. As $x \in K_v$ and $K_v \cap S_v = \mathcal{O}_{K_v}$, we get $v(x) \geq 4j$, that is, $|x|_v \leq \mathrm{N}(v)^{-4v(\mathfrak{a})}$.

Real places. If v is a real place, choose an embedding $\iota\colon L \to \mathbb{C}$ inducing it on K. By Lemma 4.6, $|x|_v = |\iota(x)| \leq 16$.

Product formula. For $x \in K^\times$ we have $\prod_{v \text{ finite}} \mathrm{N}(v)^{v(x)} = \mathrm{N}(x\mathcal{O}_K) = |\,\mathrm{N}_{K/\mathbb{Q}}(x)|$, and $\prod_{v \text{ real}} |x|_v = |\,\mathrm{N}_{K/\mathbb{Q}}(x)|$ because K is totally real. Hence $\prod_v |x|_v = 1$, the product running over all places. Inserting the bounds above,

$$1 = \prod_v |x|_v \;\leq\; |x|_\mathfrak{p} \cdot 16^r \cdot \prod_{v \mid \mathfrak{a}} \mathrm{N}(v)^{-4v(\mathfrak{a})} = |x|_\mathfrak{p} \cdot 16^r \cdot \mathrm{N}(\mathfrak{a})^{-4}. \qquad \square$$

Combining the certificate with the local estimate of Section 3 gives the key consequence.

Corollary 5.3 (Congruence elements move vertices far)**.** *Let $\mathfrak{a}$ be a nonzero ideal of $\mathcal{O}_K$ prime to $\mathfrak{p}$, let $w \in \Gamma(\mathfrak{a})$ with $w \neq I$, and let X be a vertex of T. If T contains a walk of length $2k$ from X to wX, then $q^k \geq \mathrm{N}(\mathfrak{a})^4/16^r$.*

Proof. By Proposition 4.8(a), $\det(\varphi(w) - I) = \det(w - I) = x$, and by Proposition 3.16, $|x|_\mathfrak{p} \leq q^k$. Compare with Theorem 5.2. $\square$

6 The graphs and the main theorem

We now assemble the proof. The graphs are the quotients of the tree T by the congruence subgroups $\Gamma(\mathfrak{a})$, and the certificate tells us two things about them. No nontrivial element of $\Gamma(\mathfrak{a})$ fixes a vertex, so the quotient is a (q^3+1)-regular graph. And every such element moves vertices far, so the quotient has large girth. Counting vertices then yields the constant $\frac{8}{5}$. Throughout this section the data (A1)–(A5) and a τ-stable order $\mathcal{O}$ are fixed.

Definition 6.1. For a nonzero ideal $\mathfrak{a}$ of $\mathcal{O}_K$ prime to $\mathfrak{p}$, let $\mathcal{G}_\mathfrak{a} = \Gamma(\mathfrak{a})\backslash T$ (Definition 2.3), and let $n_\mathfrak{a}$ be its number of vertices.

6.1 Finitely many orbits

The first input is a classical finiteness theorem: since the group G is compact at the real places, Γ is a cocompact lattice in the $\mathfrak{p}$-adic group.

Proposition 6.2 (Borel and Harish-Chandra)**.** *Let $\mathbf{G}$ be a connected semisimple algebraic group over a number field K, let S be a finite set of places of K containing the archimedean places, and let $\Gamma \subset \mathbf{G}(K)$ be an S-arithmetic subgroup. Then Γ is a discrete subgroup of $\mathbf{G}_S = \prod_{v\in S}\mathbf{G}(K_v)$, and $\mathbf{G}_S/\Gamma$ is compact if $\mathbf{G}$ is anisotropic over K [6], [26, Theorem 5.7].*

Proposition 6.3. *Through φ, the group Γ is a discrete subgroup of $SU(V)$ with compact quotient. Consequently Γ has finitely many orbits on the vertices of T, and the stabiliser in Γ of every vertex is finite.*

Proof. Let $\mathbf{G}$ be the algebraic group over K whose points over a K-algebra R are $\{w \in D\otimes_K R : \ \tau(w)w = 1,\ \det w = 1\}$. For a real place v, choose $\iota\colon L \to \mathbb{C}$ inducing it; then $D\otimes_K K_v = D\otimes_E \mathbb{C} \cong M_4(\mathbb{C})$ via ι, and $\mathbf{G}(K_v)$ is the special unitary group of the positive definite matrix $\iota(\theta)$, which is compact. Hence $\mathbf{G}$ has no nontrivial K-split torus (it would give a noncompact closed subgroup of $\mathbf{G}(K_v)$): $\mathbf{G}$ is anisotropic over K. The group Γ is the stabiliser in $\mathbf{G}(K)$ of the lattice $\mathcal{O}[1/\mathfrak{p}]$ under left multiplication on D, so it is an S-arithmetic subgroup of $\mathbf{G}$ for $S = \{\mathfrak{p}\}\cup\{\text{real places}\}$. By Proposition 6.2, Γ is a discrete subgroup of $\prod_{v\in S}\mathbf{G}(K_v)$ with compact quotient. The real factors are compact, so the projection of Γ to $\mathbf{G}(K_\mathfrak{p})$ is injective, with discrete image and compact quotient. Finally, φ identifies $D\otimes_K K_\mathfrak{p} = D\otimes_E F'$ with $M_4(F')$, and by Proposition 4.8(b) it identifies $\mathbf{G}(K_\mathfrak{p})$ with $SU(V)$.

By Proposition 3.13, $SU(V)$ has two orbits on vertices, with compact open stabilisers P_1, P_3. The Γ-orbits on $SU(V)/P_i$ correspond to the double cosets $\Gamma g P_i$. Their images in the compact space $\Gamma\backslash SU(V)$ are open, cover it, and are pairwise disjoint, so there are finitely many. The stabiliser of a vertex is the intersection of the discrete group Γ with a compact group, hence finite. □

We write h for the number of Γ-orbits of vertices of T.

6.2 Freeness and girth

Theorem 6.4 (Girth)**.** *Let $\mathfrak{a}$ be a nonzero ideal of $\mathcal{O}_K$ prime to $\mathfrak{p}$ with $\mathrm{N}(\mathfrak{a})^4 > 16^r q$. Then $\Gamma(\mathfrak{a})$ acts freely on the vertices of T, and $\mathcal{G}_\mathfrak{a}$ is a finite bipartite (q^3+1)-regular graph without loops or multiple edges, with*

$$\operatorname{girth}(\mathcal{G}_\mathfrak{a}) \ \geq\ 2\left\lceil \log_q \frac{\mathrm{N}(\mathfrak{a})^4}{16^r}\right\rceil \ \geq\ 8\log_q \mathrm{N}(\mathfrak{a}) - 2r\log_q 16.$$

Proof. Free action. If $w \in \Gamma(\mathfrak{a})$, $w \neq I$, fixed a vertex X, then Corollary 5.3 with the walk of length 0 would give $1 \geq \mathrm{N}(\mathfrak{a})^4/16^r$, which is false.

Regularity. By Propositions 3.9 and 3.10, T is a bipartite (q^3+1)-regular tree, and $\Gamma(\mathfrak{a})$ acts on it type-preservingly and freely. By Theorem 2.5(a), $\mathcal{G}_\mathfrak{a}$ is a bipartite (q^3+1)-regular multigraph without loops.

Girth. Take a cycle in $\mathcal{G}_\mathfrak{a}$; its length is even, say $2k$, because $\mathcal{G}_\mathfrak{a}$ is bipartite. By Theorem 2.5(b) there are a vertex X of T, an element $w \in \Gamma(\mathfrak{a})$ with $w \neq I$, and a walk of length $2k$ from X to wX. By Corollary 5.3, $q^k \geq \mathrm{N}(\mathfrak{a})^4/16^r$, so $k \geq \lceil \log_q(\mathrm{N}(\mathfrak{a})^4/16^r) \rceil$. Since $\mathrm{N}(\mathfrak{a})^4/16^r > q$, this gives $k \geq 2$; in particular there are no cycles of length 2, that is, no multiple edges.

Finiteness. The map $w \mapsto w \bmod \mathfrak{a}\mathcal{O}[1/\mathfrak{p}]$ from Γ to the finite set $\mathcal{O}[1/\mathfrak{p}]/\mathfrak{a}\mathcal{O}[1/\mathfrak{p}]$ has the cosets of $\Gamma(\mathfrak{a})$ as fibres: if $w \equiv w'$, then $w^{-1}w' - I = w^{-1}(w'-w) \in \mathfrak{a}\mathcal{O}[1/\mathfrak{p}]$. So $[\Gamma : \Gamma(\mathfrak{a})]$ is finite. Each Γ-orbit of vertices splits into at most $[\Gamma : \Gamma(\mathfrak{a})]$ orbits of the normal subgroup $\Gamma(\mathfrak{a})$, and by Proposition 6.3 there are finitely many Γ-orbits. Hence $n_\mathfrak{a} \leq h\,[\Gamma : \Gamma(\mathfrak{a})]$ is finite. □

6.3 Counting vertices

It remains to bound the index $[\Gamma : \Gamma(\mathfrak{a})]$. Locally at a place v dividing $\mathfrak{a}$, the congruence condition cuts out a subgroup of a group of 4×4 matrices over a finite ring, and the size of that group is governed by the dimension 15 of SU_4. This works at places where the order $\mathcal{O}$ is as nice as possible.

Definition 6.5 (Good places)**.** A finite place v of K is *good* (for $\mathcal{O}$) if $v \neq \mathfrak{p}$, $v \nmid 2$, v is unramified in E, and there is an isomorphism of S_v-algebras $\mathcal{O}_v \cong M_4(S_v)$.

By Skolem–Noether, as in Step 2 of the proof of Proposition 4.8, such an isomorphism preserves characteristic polynomials. For a finite place $v \neq \mathfrak{p}$ and $j \geq 0$ let

$$U_v = \{y \in \mathcal{O}_v :\ \tau(y)y = 1,\ \det y = 1\}, \qquad U_v(j) = \{y \in U_v :\ y - 1 \in \pi_v^j \mathcal{O}_v\}.$$

These are groups ($y^{-1} = \tau(y) \in \mathcal{O}_v$), and $\Gamma \subseteq U_v$.

Lemma 6.6 (Local index)**.** *Let v be a good place, $Q = \mathrm{N}(v)$ and $j \geq 1$. Then $[U_v : U_v(1)] < Q^{15}$ and $[U_v(j) : U_v(j+1)] \leq Q^{15}$. Hence $[U_v : U_v(j)] \leq Q^{15j}$.*

Proof. Write $\pi = \pi_v$, $\kappa_v = \mathcal{O}_{K_v}/\pi \cong \mathbb{F}_Q$, $\bar{\mathcal{O}} = \mathcal{O}_v/\pi\mathcal{O}_v$ (an algebra of dimension 32 over κ_v) and $\bar{S} = S_v/\pi S_v$. Since τ is K-linear and preserves $\mathcal{O}_v$, it induces a κ_v-linear anti-automorphism $\bar\tau$ of $\bar{\mathcal{O}}$. Since v is unramified in E and $v \nmid 2$, there is a unit $\delta \in S_v$ with $\overline{\delta} = -\delta$: if v is inert in E, a square root of a nonsquare unit of K_v; if v splits, $\delta = (1,-1) \in \mathcal{O}_{K_v} \times \mathcal{O}_{K_v}$.

Steps $j \geq 1$. Let $g = 1 + \pi^j X \in U_v(j)$ with $X \in \mathcal{O}_v$. The equation $\tau(g)g = 1$ gives $X + \tau(X) = -\pi^j \tau(X) X \in \pi\mathcal{O}_v$. Expanding $\det(1+\pi^j X) = 1 + \pi^j \operatorname{tr} X + \pi^{2j} c$ with $c \in S_v$ (Lemma 4.7) gives $\operatorname{tr} X \in \pi S_v$. The map $g \mapsto X \bmod \pi$ is a homomorphism from $U_v(j)$ to the additive group of $\bar{\mathcal{O}}$, because $(1+\pi^j X)(1+\pi^j Y) \equiv 1 + \pi^j(X+Y) \pmod{\pi^{j+1}}$, and its kernel is $U_v(j+1)$. Its image lies in

$$\mathcal{V} = \{\bar X \in \bar{\mathcal{O}} :\ \bar\tau(\bar X) = -\bar X,\ \overline{\operatorname{tr}}(\bar X) = 0\}.$$

Since 2 is invertible, $\bar{\mathcal{O}} = \bar{\mathcal{O}}^+ \oplus \bar{\mathcal{O}}^-$, the eigenspaces of $\bar\tau$ for ± 1, and multiplication by the central unit $\bar\delta$ maps $\bar{\mathcal{O}}^+$ bijectively onto $\bar{\mathcal{O}}^-$; so $\dim_{\kappa_v} \bar{\mathcal{O}}^- = 16$. As $\operatorname{tr}(\tau(X)) = \overline{\operatorname{tr} X}$, the reduced trace maps $\bar{\mathcal{O}}^-$ to the line $\{s \in \bar S : \overline{s} = -s\} = \kappa_v \bar\delta$, and it is not zero on $\bar{\mathcal{O}}^-$ because $\overline{\operatorname{tr}}(\bar\delta) = 4\bar\delta \neq 0$. So $\dim \mathcal{V} = 15$, and $[U_v(j) : U_v(j+1)] \leq Q^{15}$.

Step $j = 0$. Fix $\mathcal{O}_v \cong M_4(S_v)$; then $\bar{\mathcal{O}} \cong M_4(\bar S)$, and $U_v/U_v(1)$ embeds into $\{\bar y \in M_4(\bar S) : \bar\tau(\bar y)\bar y = 1,\ \det \bar y = 1\}$.

If v splits in E, then $\bar S = \kappa_v \times \kappa_v$ and $\bar{\mathcal{O}} = M_4(\kappa_v) \times M_4(\kappa_v)$. The anti-automorphism $\bar\tau$ interchanges the two central idempotents, so $\bar\tau(A,B) = (\psi'(B), \psi(A))$ for anti-isomorphisms ψ, ψ'. The equation $\bar\tau(\bar y)\bar y = 1$ says $B = \psi(A)^{-1}$, and then $\det \bar y = 1$ says $\det A = 1$. So $\bar y \mapsto A$ identifies the set with $SL_4(\mathbb{F}_Q)$.

If v is inert in E, then $\bar{S} = \mathbb{F}_{Q^2}$ and $\bar{\tau}$ is an involution of $M_4(\mathbb{F}_{Q^2})$ acting on the centre by $x \mapsto x^Q$. Step 3 of the proof of Proposition 4.8 applies verbatim (with $\bar{\delta}$ in the role of an element c with $\bar{c} = -c$) and shows that $\bar{\tau}$ is the adjoint involution of a nondegenerate hermitian form over $\mathbb{F}_{Q^2}$. So the set is the special unitary group of that form, which is isomorphic to $SU_4(\mathbb{F}_Q)$ (Lemma A.2).

By Lemma A.2, $|SL_4(\mathbb{F}_Q)| = Q^6(Q^2-1)(Q^3-1)(Q^4-1)$ and $|SU_4(\mathbb{F}_Q)| = Q^6(Q^2-1)(Q^3+1)(Q^4-1)$. Both are less than Q^{15}, since $(Q^2-1)(Q^3 \pm 1) < Q^5$ and $Q^4 - 1 < Q^4$. □

To pass from local to global congruences we use that a lattice is determined by its completions.

Lemma 6.7. *Let $\mathfrak{a}$ be a nonzero ideal of $\mathcal{O}_K$ prime to $\mathfrak{p}$, and $y \in D$. Then $y \in \mathfrak{a}\mathcal{O}[1/\mathfrak{p}]$ if and only if $y \in \pi_v^{v(\mathfrak{a})}\mathcal{O}_v$ for every finite place $v \neq \mathfrak{p}$.*

Proof. The condition is clearly necessary. Conversely, put $R = \mathcal{O}_K[1/\mathfrak{p}]$, a Dedekind domain whose maximal ideals correspond to the finite places $v \neq \mathfrak{p}$, and $\mathcal{N} = \mathfrak{a}\mathcal{O}[1/\mathfrak{p}]$. The R-module $C = (\mathcal{N} + Ry)/\mathcal{N}$ is finitely generated and torsion (some nonzero multiple of y lies in $\mathcal{N}$, which spans D), and its completion at every v is $(\mathcal{N}_v + \mathcal{O}_{K_v} y)/\mathcal{N}_v = 0$ by hypothesis, where $\mathcal{N}_v = \pi_v^{v(\mathfrak{a})}\mathcal{O}_v$. A finitely generated torsion module over a Dedekind domain is the direct sum of its completions at the finitely many maximal ideals in its support, so $C = 0$, that is, $y \in \mathcal{N}$. □

Proposition 6.8. *If $\mathfrak{a}$ is a nonzero ideal of $\mathcal{O}_K$ divisible only by good places, then $[\Gamma : \Gamma(\mathfrak{a})] \leq \mathrm{N}(\mathfrak{a})^{15}$.*

Proof. By Lemma 6.7, an element $w \in \Gamma$ lies in $\Gamma(\mathfrak{a})$ if and only if $w \in U_v(v(\mathfrak{a}))$ for every $v \mid \mathfrak{a}$. So $\Gamma(\mathfrak{a})$ is the kernel of the homomorphism $\Gamma \to \prod_{v|\mathfrak{a}} U_v/U_v(v(\mathfrak{a}))$, and by Lemma 6.6 its index is at most $\prod_{v|\mathfrak{a}} \mathrm{N}(v)^{15v(\mathfrak{a})} = \mathrm{N}(\mathfrak{a})^{15}$. □

6.4 The main theorem

Theorem 6.9 (Main Theorem)**.** *Assume (A1)–(A5), let $\mathcal{O}$ be a τ-stable order, and let h be the number of Γ-orbits of vertices of T. Let $\mathfrak{a}$ be a nonzero ideal of $\mathcal{O}_K$, divisible only by good places, with $\mathrm{N}(\mathfrak{a})^4 > 16^r q$. Then $\mathcal{G}_\mathfrak{a}$ is a finite bipartite (q^3+1)-regular graph without loops or multiple edges, with $n_\mathfrak{a} \leq h\,\mathrm{N}(\mathfrak{a})^{15}$ vertices, and*

$$\mathrm{girth}(\mathcal{G}_\mathfrak{a}) \;\geq\; 8\log_q \mathrm{N}(\mathfrak{a}) - 2r\log_q 16 \;\geq\; \tfrac{8}{5}\log_{q^3} n_\mathfrak{a} - c_0, \qquad c_0 = \tfrac{8}{5}\log_{q^3} h + 2r\log_q 16.$$

Proof. Theorem 6.4 gives everything except the vertex count. By its proof and Proposition 6.8, $n_\mathfrak{a} \leq h[\Gamma : \Gamma(\mathfrak{a})] \leq h\,\mathrm{N}(\mathfrak{a})^{15}$, that is, $\log_{q^3} n_\mathfrak{a} \leq \log_{q^3} h + 5\log_q \mathrm{N}(\mathfrak{a})$. So $8\log_q \mathrm{N}(\mathfrak{a}) \geq \tfrac{8}{5}(\log_{q^3} n_\mathfrak{a} - \log_{q^3} h)$. □

To prove Theorem 1.1 it remains to produce, for every prime power q, data satisfying (A1)–(A5) with $\mathrm{N}(\mathfrak{p}) = q$, together with an order having infinitely many good places. This is done in the next section.

7 Arithmetic data for every prime power

Fix a prime power $q = p_0^s$, with p_0 prime. We construct the fields from cyclotomic fields, the algebra from an auxiliary cyclic quartic field, and the involution by weak approximation.

7.1 The fields K and E

Let $\nu = q^2 - 1$, and identify $\mathrm{Gal}(\mathbb{Q}(\zeta_\nu)/\mathbb{Q})$ with $(\mathbb{Z}/\nu\mathbb{Z})^\times$, the class of c acting by $\zeta_\nu \mapsto \zeta_\nu^c$. Complex conjugation is the class of -1.

Lemma 7.1. *Let K be the fixed field of the subgroup generated by q and -1, and E the fixed field of the subgroup generated by $-q$. Then K is totally real, E is a CM field and a quadratic extension of K, and every prime $\mathfrak{p}$ of K above p_0 has $\mathrm{N}(\mathfrak{p}) = q$ and is inert in E. (For $q = 2$ and $q = 3$ we get $K = \mathbb{Q}$ and $E = \mathbb{Q}(\sqrt{-3})$, $E = \mathbb{Q}(i)$ respectively.)*

Proof. For $q = 2$ the group $(\mathbb{Z}/3\mathbb{Z})^\times = \{\pm 1\}$ gives $K = \mathbb{Q}$, $E = \mathbb{Q}(\zeta_3)$, and 2 is inert in E. Let $q \geq 3$. Since $(-q)^2 = q^2 \equiv 1$ and $-q \not\equiv \pm 1 \pmod{\nu}$, the subgroup $\langle -q \rangle = \{1, -q\}$ has order 2, and $\langle q, -1 \rangle = \{1, q, -1, -q\}$ has order 4; so $[E : K] = 2$. The Galois group is abelian and complex conjugation lies in $\langle q, -1 \rangle$ but not in $\langle -q \rangle$. Hence complex conjugation is trivial on K and nontrivial on E, under every embedding: K is totally real and E is totally imaginary, so E is a CM field.

The prime p_0 does not divide ν, so it is unramified in $\mathbb{Q}(\zeta_\nu)$ and its Frobenius is the class of p_0 [23, Ch. I, (10.3)]. The residue degree of p_0 in the fixed field of a subgroup H is the order of p_0 in $(\mathbb{Z}/\nu\mathbb{Z})^\times/H$. Modulo $\langle q, -1 \rangle$ this order is s: $p_0^s = q$, while for $0 < j < s$ we have $1 < p_0^j < q$, and the residues $1, q, \nu - q, \nu - 1$ of the elements of $\langle q, -1 \rangle$ are 1, q or larger than q. Modulo $\langle -q \rangle$ the order is $2s$: $p_0^{2s} = q^2 \equiv 1$, while for $0 < j < 2s$ we have $1 < p_0^j < \nu$, and $p_0^j \neq \nu - q$ because $\nu - q = q^2 - q - 1$ is prime to p_0. So the primes of K above p_0 have residue degree s, and those of E residue degree $2s$. □

From now on K and E are as in Lemma 7.1, $r = [K : \mathbb{Q}]$, $\mathfrak{p}$ is a prime of K above p_0, and $\mathfrak{P} = \mathfrak{p}\mathcal{O}_E$.

7.2 The cyclic algebra

We choose three auxiliary objects.

- *A prime $\ell \equiv 1 \pmod 8$ not dividing νp_0.* For instance, any prime divisor ℓ of $y^4 + 1$ with $y = 2\nu p_0$ will do: y has order 8 modulo ℓ, so $\ell \equiv 1 \pmod 8$, and $\ell \nmid y$. Let Φ_ℓ be the quartic subfield of $\mathbb{Q}(\zeta_\ell)$. It is cyclic over $\mathbb{Q}$, ramified only at ℓ, and totally real, because -1 is a fourth power modulo ℓ. Since $\mathbb{Q}(\zeta_\nu) \cap \mathbb{Q}(\zeta_\ell) = \mathbb{Q}$, the fields $L_0 = K\Phi_\ell$ and $L = E\Phi_\ell = L_0 E$ satisfy $\mathrm{Gal}(L/E) \cong \mathrm{Gal}(L_0/K) \cong \mathrm{Gal}(\Phi_\ell/\mathbb{Q}) \cong (\mathbb{Z}/\ell\mathbb{Z})^\times/((\mathbb{Z}/\ell\mathbb{Z})^\times)^4 \cong \mathbb{Z}/4\mathbb{Z}$, L_0 is totally real, L is a CM field, and L/E is unramified outside ℓ.

- *A prime $\ell' \equiv 1 \pmod \nu$ which is not a square modulo ℓ.* It exists by Dirichlet's theorem on primes in arithmetic progressions (equivalently, the Chebotarev density theorem [23, Ch. VII, (13.4)] for $\mathbb{Q}(\zeta_{\nu\ell})/\mathbb{Q}$). It splits completely in $\mathbb{Q}(\zeta_\nu)$, hence in E. Let $\mathfrak{w}$ be a prime of E above ℓ'; then $\mathrm{N}(\mathfrak{w}) = \ell'$ and $\mathfrak{w} \neq \overline{\mathfrak{w}}$. The Frobenius of $\mathfrak{w}$ in $\mathrm{Gal}(L/E)$ corresponds to the class of $\mathrm{N}(\mathfrak{w}) = \ell'$ in $(\mathbb{Z}/\ell\mathbb{Z})^\times/((\mathbb{Z}/\ell\mathbb{Z})^\times)^4$, which generates this cyclic group of order 4 because ℓ' is not a square. So $\mathfrak{w}$ is inert in L. Let σ be this Frobenius; it generates $\mathrm{Gal}(L/E)$.

- *An element $\alpha \in \mathcal{O}_E$* with $\alpha \in \mathfrak{w} \setminus \mathfrak{w}^2$, $\alpha \equiv 1 \pmod{\overline{\mathfrak{w}}}$ and $\alpha \equiv 1 \pmod{\mathfrak{P}}$ (Chinese remainder theorem). Put $\gamma = \alpha/\overline{\alpha}$. Then $\gamma\overline{\gamma} = 1$, the $\mathfrak{w}$-adic valuation of γ is $1 - 0 = 1$, and γ is a unit at $\mathfrak{P} = \overline{\mathfrak{P}}$.

With these choices, (A1), (A2) and (A4) hold: $\mathfrak{p}$ is inert in E by Lemma 7.1, and L/E is unramified at $\mathfrak{P}$ because $\mathfrak{P} \nmid \ell$.

7.3 The involution

It remains to choose θ. The two conditions (A3) and (A5) concern finitely many places, the real places and $\mathfrak{p}$, and each is an open condition there; weak approximation finds a global θ satisfying all of them at once.

Lemma 7.2. *There is $\theta \in D$ with $\theta^* = \theta$ satisfying (A3) and (A5).*

Proof. Let $\mathrm{Sym} = \{y \in D : \ y^* = y\}$, a K-vector space of dimension 16. Let S consist of the real places of K and $\mathfrak{p}$; for $v \in S$ we consider $\mathrm{Sym} \otimes_K K_v$, the fixed space of $y \mapsto y^*$ in $D \otimes_K K_v$.

At a real place v. Fix $\iota\colon L \to \mathbb{C}$ inducing v. The other embeddings inducing v are $\iota \circ \sigma^j$ and their complex conjugates, and $\iota(\sigma^j(y)) = \iota(U)^j \iota(y) \iota(U)^{-j}$ with $\iota(U)$ unitary (proof of Lemma 4.4). So (A3) at v says just that $\iota(y)$ is positive definite. This is an open condition on $y \in \mathrm{Sym} \otimes_K K_v$, satisfied by $y = 1$.

At $\mathfrak{p}$. Let H_0 be the matrix of Proposition 4.8 for the involution $X \mapsto X^*$, that is, for $\theta = 1$. For invertible $y \in \mathrm{Sym}$, the involution $X \mapsto y^{-1}X^*y$ satisfies $\varphi(y^{-1}X^*y) = (H_0\varphi(y))^{-1}\varphi(X)^\dagger(H_0\varphi(y))$, and $H_0\varphi(y)$ is hermitian; so the matrix H attached to $\theta = y$ is $H_0\varphi(y)$. The condition that $v(\det(H_0\varphi(y)))$ be odd is open on $\mathrm{Sym} \otimes_K K_\mathfrak{p}$, which φ identifies with $\{Y \in M_4(F') : \ H_0^{-1}Y^\dagger H_0 = Y\}$. It is satisfied by $Y = H_0^{-1}\,\mathrm{diag}(\pi, 1, 1, 1)$.

Approximation. K is dense in $\prod_{v \in S} K_v$ [23, Ch. II, (3.4)], so $\mathrm{Sym} \cong K^{16}$ is dense in $\prod_{v \in S} \mathrm{Sym} \otimes_K K_v$. Choose $\theta \in \mathrm{Sym}$ in the nonempty open set defined above. It is nonzero, hence invertible, and satisfies (A3) and (A5). □

7.4 An order and its good places

We now write down a τ-stable order. Let $e_0 = I$ and $e_i = \overline{\alpha}\, U^i$ for $i = 1, 2, 3$, and

$$\mathcal{A} = \bigoplus_{i=0}^{3} \rho(\mathcal{O}_L)\, e_i.$$

Lemma 7.3. *$\mathcal{A}$ is an order of D with $\mathcal{A}^* = \mathcal{A}$, and its matrices have entries in $\mathcal{O}_L$. The intersection $\mathcal{O} = \mathcal{A} \cap \tau(\mathcal{A})$ is a τ-stable order. A finite place v of K is good for $\mathcal{O}$ if $v \neq \mathfrak{p}$, $v \nmid 2$, v is unramified in E, L/E is unramified at the places above v, α is a unit at the places above v, and $\theta, \theta^{-1} \in \mathcal{A}_v$. All but finitely many finite places satisfy these conditions.*

Proof. $\mathcal{A}$ is an order. For $1 \le i, j \le 3$ we have $e_i e_j = \overline{\alpha}^2 U^{i+j}$, so

$$e_i e_j = \overline{\alpha}\, e_{i+j} \ (i+j \le 3), \qquad e_i e_j = \overline{\alpha}^2\gamma = \alpha\overline{\alpha} \ (i+j = 4), \qquad e_i e_j = \alpha\, e_{i+j-4} \ (i+j \ge 5),$$

using $\overline{\alpha}^2\gamma = \alpha\overline{\alpha}$; and $e_i\rho(a) = \rho(\sigma^i a)e_i$. All coefficients are integral, so $\mathcal{A}$ is a ring. It contains $\mathcal{O}_E$, is a finitely generated $\mathcal{O}_K$-module, and spans D. The entries of $\rho(a)e_i$ are 0, $\overline{\alpha}\,\sigma^k(a)$ and $\overline{\alpha}\gamma\,\sigma^k(a) = \alpha\,\sigma^k(a)$, which lie in $\mathcal{O}_L$ for $a \in \mathcal{O}_L$.

$\mathcal{A}^* = \mathcal{A}$. For $1 \le i \le 3$, since $U^{-i} = \overline{\gamma}\,U^{4-i}$ and $\alpha\overline{\gamma} = \overline{\alpha}$, we get $e_i^* = \alpha U^{-i} = \overline{\alpha}\,U^{4-i} = e_{4-i}$, and $(\rho(a)e_i)^* = e_{4-i}\rho(\overline{a}) = \rho(\sigma^{4-i}\overline{a})e_{4-i}$.

$\mathcal{O}$. $\tau(\mathcal{A}) = \theta^{-1}\mathcal{A}^*\theta = \theta^{-1}\mathcal{A}\theta$ is again an order, and the intersection of two orders is an order. As τ^2 is the identity, $\tau(\mathcal{O}) = \tau(\mathcal{A}) \cap \mathcal{A} = \mathcal{O}$.

Good places. Let v satisfy the stated conditions. Then $\theta^{-1}\mathcal{A}_v\theta = \mathcal{A}_v$, so $\mathcal{O}_v = \mathcal{A}_v$, and since $\overline{\alpha}$ is a unit above v, $\mathcal{A}_v = \bigoplus_i \rho(\mathcal{O}_{L,v})U^i$ with $\mathcal{O}_{L,v} = \mathcal{O}_L \otimes_{\mathcal{O}_K} \mathcal{O}_{K_v}$. Let $\mathfrak{w}'$ be a place of E above v, and let $\mathcal{A}_{\mathfrak{w}'} = \bigoplus_i \rho(\mathcal{O}_{L,\mathfrak{w}'})U^i$ be the corresponding factor, where $\mathcal{O}_{L,\mathfrak{w}'}$ is the ring of integers of the unramified algebra $L \otimes_E E_{\mathfrak{w}'}$. As in Step 1 of the proof of Proposition 4.8, there is a unit b of $\mathcal{O}_{L,\mathfrak{w}'}$ with $b\,\sigma(b)\,\sigma^2(b)\,\sigma^3(b) = \gamma$, and $\rho(a) \mapsto (x \mapsto ax)$, $U \mapsto (x \mapsto b\sigma(x))$ embeds $\mathcal{A}_{\mathfrak{w}'}$ into $\mathrm{End}(\mathcal{O}_{L,\mathfrak{w}'}) \cong M_4(\mathcal{O}_{E_{\mathfrak{w}'}})$. We compare discriminants of the trace forms $(X, Y) \mapsto \mathrm{tr}(XY)$; the embedding preserves traces, as in Step 2 of the proof of Proposition 4.8. Since U, U^2, U^3 have zero diagonal, $\mathrm{tr}(\rho(c)U^m) = 0$ for $m \not\equiv 0 \pmod 4$, and $\mathrm{tr}(\rho(c)) = \mathrm{Tr}_{L/E}(c)$. So in a basis

$\rho(x_k)U^i$, where $x_1,\dots,x_4$ is a basis of $\mathcal{O}_{L,\mathfrak{w}'}$, the trace form pairs the index i with $-i \bmod 4$, with blocks $(\mathrm{Tr}(x_k x_l))$ and $(\gamma\,\mathrm{Tr}(x_k\sigma^i(x_l)))$ for $i=1,2,3$. Each block has unit determinant, because $L\otimes_E E_{\mathfrak{w}'}$ is unramified over $E_{\mathfrak{w}'}$ and γ is a unit. So $\mathcal{A}_{\mathfrak{w}'}$ has unit discriminant, like $M_4(\mathcal{O}_{E_{\mathfrak{w}'}})$. For two orders of the same rank, one contained in the other, the discriminants differ by the square of the index; hence the embedding is onto. Thus $\mathcal{O}_v=\prod_{\mathfrak{w}'|v}\mathcal{A}_{\mathfrak{w}'}\cong M_4(S_v)$.

Almost all places. Only finitely many places ramify in E or in L, divide α, or occur in the denominators of the coordinates of θ and θ^{-1} with respect to $\mathcal{A}$. □

7.5 Proof of Theorem 1.1

Theorem 7.4. *For every prime power q, the data constructed in this section satisfy (A1)–(A5) with $\mathrm{N}(\mathfrak{p})=q$, and all but finitely many finite places of K are good for the order $\mathcal{O}=\mathcal{A}\cap\tau(\mathcal{A})$.*

Proof. Combine Lemma 7.1, the choices made in this section, Lemma 7.2 and Lemma 7.3. □

Proof of Theorem 1.1. Take the data of Theorem 7.4, fix a good prime $\mathfrak{b}$ of K, put $Q=\mathrm{N}(\mathfrak{b})$, and let m_0 be the least integer with $Q^{4m_0}>16^r q$. For $m\ge m_0$ let $\mathcal{G}_m=\mathcal{G}_{\mathfrak{b}^m}$. By Theorem 6.9, $\mathcal{G}_m$ is a finite bipartite d-regular graph with $n_m\le hQ^{15m}$ vertices and $\mathrm{girth}(\mathcal{G}_m)\ge 8m\log_q Q-2r\log_q 16$, and the girth bound in terms of n_m follows. By the Moore bound (Proposition 2.2), $n_m\ge(d-1)^{\lfloor(\mathrm{girth}(\mathcal{G}_m)-1)/2\rfloor}\to\infty$.

Finally, $\mathcal{G}_m$ is connected, because T is connected (Proposition 3.10) and the projection maps paths to walks. □

7.6 Two numerical examples

For $q=2$ and $q=3$ everything can be written down explicitly, over $K=\mathbb{Q}$. In both examples the field L_0 is the real cyclic quartic field of a prime conductor, $\mathfrak{p}$ splits completely in L_0, and $\theta=\rho(\eta)$ for a totally positive $\eta\in\mathcal{O}_{L_0}$ whose norm is $\mathrm{N}(\mathfrak{p})$; then (A3) and (A5) hold by Lemma 4.9, and $\theta^{\pm1}\in\mathcal{A}_v$ for every $v\ne\mathfrak{p}$. The arithmetic facts listed are finite computations.

Example 7.5 (Degree 28)**.** Let $K=\mathbb{Q}$, $E=\mathbb{Q}(i)$ and $\mathfrak{p}=(3)$, so $q=3$ and $d=28$. Let $L_0=\mathbb{Q}(\xi)$ with $\xi^4+\xi^3-72\xi^2-205\xi-49=0$; this is the real cyclic quartic field of conductor 193, and

$$\sigma(\xi)=-\tfrac{1}{18}\xi^3+\tfrac{2}{9}\xi^2+\tfrac{26}{9}\xi-\tfrac{37}{18}$$

is a generator of its Galois group, namely the Frobenius at 5. The prime 3 splits completely in L_0 and 5 is inert in L_0. Take $\alpha=2+i$ and $\mathfrak{w}=(2+i)$, so $\gamma=(3+4i)/5$, and

$$\eta=\tfrac{1}{2}\big(-3\xi^3+20\xi^2+70\xi+17\big),$$

whose characteristic polynomial $X^4-852X^3+19191X^2-23122X+3$ has alternating signs, so that η is totally positive with norm 3. The good places for $\mathcal{O}=\mathcal{A}\cap\tau(\mathcal{A})$ include all primes other than $2,3,5,193$. By Theorem 6.9, for every integer $a>1$ whose prime factors all lie outside $\{2,3,5,193\}$, the graph $\Gamma(a)\backslash T$ is finite, bipartite and 28-regular, has $n\le h\,a^{15}$ vertices, and has girth at least

$$8\log_3 a-8\log_3 2\;\ge\;\tfrac{8}{5}\log_{27} n-\big(\tfrac{8}{5}\log_{27} h+8\log_3 2\big).$$

Example 7.6 (Degree 9)**.** Let $K=\mathbb{Q}$, $E=\mathbb{Q}(\zeta_3)$ with $\zeta_3^2+\zeta_3+1=0$, and $\mathfrak{p}=(2)$, so $q=2$ and $d=9$. Let $L_0=\mathbb{Q}(\xi)$ with $\xi^4+\xi^3-27\xi^2-41\xi+2=0$, the real cyclic quartic field of conductor 73, with the generator

$$\sigma(\xi)=-\tfrac{1}{8}\xi^3+\tfrac{1}{4}\xi^2+\tfrac{21}{8}\xi-\tfrac{7}{4},$$

the Frobenius at 7. The prime 2 splits completely in L_0 and 7 is inert. Take $\alpha=3+\zeta_3$, of norm 7, and $\eta=(\xi^2+\xi)/2$, with characteristic polynomial $X^4-27X^3+173X^2-85X+2$.

The good places include all primes other than $2, 3, 7, 73$, and for every integer $a > 1$ with prime factors outside $\{2, 3, 7, 73\}$ the graph $\Gamma(a)\backslash T$ is 9-regular, has $n \le h\, a^{15}$ vertices, and has girth at least $8 \log_2 a - 8 \ge \frac{8}{5} \log_8 n - \big(\frac{8}{5} \log_8 h + 8\big)$.

8 An explicit family with girth constant exactly $\frac{8}{5}$

In this section we study one explicit family of 28-regular graphs in detail. The arithmetic data are chosen so that Γ is small: it has only two orbits of vertices on the tree, which makes it possible to count vertices exactly and to compute girths. Our aim is an upper bound on the girth, the analogue for our graphs of the theorem of Biggs and Boshier [4] for the LPS graphs.

The idea is to look for short cycles inside a copy of an SL_2. The algebra D contains a quadratic extension E' of E, and the elements of D commuting with E' form a quaternion algebra. Twisting by the involution, we obtain a quaternion algebra B over the real quadratic field $K' = \mathbb{Q}(\sqrt{13})$, whose norm-one elements lie in G. For such an element y the certificate is essentially $2 - \mathrm{trd}(y)$, as for LPS. We then work backwards: we choose a trace $t_0 \in K'$, of small denominator at one prime above 3 and satisfying finitely many congruences, and show that t_0 is the trace of an element of $\Gamma(a)$. A lattice-point argument in K' produces such a t_0 with denominator about a^4, and the corresponding element moves a vertex of the tree a distance about $8 \log_3 a$.

8.1 The data

Let $K = \mathbb{Q}$, $E = \mathbb{Q}(\sqrt{-7})$ and $\mathfrak{p} = (3)$, so $q = 3$ and $d = 28$. Put $\alpha = (1 + \sqrt{-7})/2$, so that $\alpha\overline{\alpha} = 2$, and $\gamma = \alpha/\overline{\alpha}$. Let $L_0 = \mathbb{Q}(\xi)$ with

$$\xi^4 - \xi^3 - 76\xi^2 - 74\xi + 393 = 0,$$

a real cyclic quartic field of conductor $299 = 13 \cdot 23$, with Galois group generated by

$$\sigma(\xi) = \tfrac{1}{261}\big(-16\xi^3 + 27\xi^2 + 1018\xi + 582\big),$$

the Frobenius at 2. Let $\theta = \rho(\eta)$ with

$$\eta = \tfrac{1}{261}\big(-14\xi^3 - 9\xi^2 + 956\xi + 3576\big),$$

whose minimal polynomial $X^4 - 29X^3 + 200X^2 - 412X + 87$ takes the signs $+, -, +, -, +$ at $0, 1, 4, 6, 30$, so that its four roots are positive. The conditions of Section 4 hold:

- (A1): L_0 is totally real and cyclic of degree 4 over $\mathbb{Q}$, and $L = L_0E$.
- (A2): $\mathfrak{w} = \alpha\mathcal{O}_E$ is a prime above 2; since 2 is inert in L_0, $\mathfrak{w}$ is inert in L; and $v_{\mathfrak{w}}(\gamma) = v_{\mathfrak{w}}(\alpha) - v_{\overline{\mathfrak{w}}}(\alpha) = 1$.
- (A4): 3 is inert in E (as -7 is not a square modulo 3), L/E is unramified at 3, and γ is a unit at 3.
- (A3) and (A5): 3 splits completely in L_0, and $\mathrm{N}_{L_0/\mathbb{Q}}(\eta) = 87 = 3 \cdot 29$; apply Lemma 4.9.

The order is not the order $\mathcal{A} \cap \tau(\mathcal{A})$ of Section 7. Instead we fix a maximal order $\mathcal{M}$ of D with $\mathcal{M}[1/3] = \tau(\mathcal{M})[1/3]$ and put $\mathcal{O} = \mathcal{M} \cap \tau(\mathcal{M})$, a τ-stable order with $\mathcal{O}[1/3] = \mathcal{M}[1/3]$ and $[\mathcal{M} : \mathcal{O}] = 3^6$; a $\mathbb{Z}$-basis of $\mathcal{M}$ is available from the authors. Thus

$$\Gamma = \{w \in \mathcal{M}[1/3] :\ w^*\theta w = \theta,\ \det w = 1\}, \qquad \Gamma(a) = \{w \in \Gamma :\ w - I \in a\mathcal{M}[1/3]\}$$

for integers a prime to 3, and $\mathcal{G}_a = \Gamma(a)\backslash T$.

Proposition 8.1 (Facts established by exact computation)**.** *(i) The algebra D is split at every place of E not above 2, and for every prime $a \notin \{2,3,7\}$ the order $\mathcal{O}_a = \mathcal{O} \otimes \mathbb{Z}_a$ is maximal. Consequently every prime $a \notin \{2,3,7\}$ is good for $\mathcal{O}$.*

(ii) Γ has exactly two orbits on the vertices of T, one of each type, and the stabiliser in Γ of each vertex is cyclic of order 12.

Appendix B describes how these facts are certified. For (i), note that if D is split at the places of E above a, then a maximal order $\mathcal{O}_a$ of $D \otimes \mathbb{Q}_a \cong M_4(E \otimes \mathbb{Q}_a)$ preserves the lattice $\mathcal{O}_a \cdot S_a^4$, so it is contained in, and hence equal to, the endomorphism ring of that lattice, which is isomorphic to $M_4(S_a)$.

8.2 The number of vertices

To count vertices exactly we need the reduction of Γ modulo a prime to be onto. This follows from strong approximation.

Proposition 8.2 (Strong approximation; Kneser, Platonov)**.** *Let $\mathbf{G}$ be a simply connected, absolutely almost simple algebraic group over a number field K, and S a finite set of places of K such that $\prod_{v\in S} \mathbf{G}(K_v)$ is not compact. Then $\mathbf{G}(K)$ is dense in the restricted product of the groups $\mathbf{G}(K_v)$ over the places $v \notin S$ [16, 25], [27, Theorem 2.3].*

Theorem 8.3. *Let $a \notin \{2,3,7\}$ be a prime and $\chi(a) = \left(\frac{-7}{a}\right)$. Then $\mathcal{G}_a$ is a finite connected bipartite 28-regular graph without multiple edges, with*

$$n_a = \tfrac{1}{6}\, a^6(a^2-1)\big(a^3 - \chi(a)\big)(a^4-1)$$

vertices, and $\operatorname{girth}(\mathcal{G}_a) \geq 8\log_3 a - 8\log_3 2$.

Proof. Since $a \geq 5$, we have $a^4 > 48 = 16 \cdot 3$, and Theorem 6.4 gives everything except connectedness and the vertex count. $\mathcal{G}_a$ is connected because T is (Proposition 3.10).

Orbits. By Proposition 8.1(ii), Γ has two orbits, with stabilisers Γ_X of order 12. Since $\Gamma(a)$ is normal and acts freely, $\Gamma_X \cap \Gamma(a) = 1$, and the orbit ΓX splits into $[\Gamma : \Gamma(a)\Gamma_X] = [\Gamma : \Gamma(a)]/12$ orbits of $\Gamma(a)$. Hence $n_a = [\Gamma : \Gamma(a)]/6$.

The image of Γ. By Lemma 6.7, $\Gamma/\Gamma(a)$ is the image of Γ in $U_a/U_a(1)$. Let $\bar{G}_a = \{\bar{y} \in \mathcal{O}_a/a\mathcal{O}_a : \ \bar{\tau}(\bar{y})\bar{y} = 1, \ \det \bar{y} = 1\}$, where $\bar{\tau}$ is induced by τ; by the proof of Lemma 6.6 (Step $j = 0$) it is isomorphic to $SL_4(\mathbb{F}_a)$ if $\chi(a) = 1$ (a splits in E) and to $SU_4(\mathbb{F}_a)$ if $\chi(a) = -1$ (a is inert), and $U_a/U_a(1)$ embeds in $\bar{G}_a$. We show that $\Gamma \to \bar{G}_a$ is onto; then $n_a = |\bar{G}_a|/6$, and Lemma A.2 gives the formula.

First, $U_a \to \bar{G}_a$ is onto. If a splits, then $\mathcal{O}_a \cong M_4(\mathbb{Z}_a) \times M_4(\mathbb{Z}_a)$, and τ interchanges the two factors, so $\tau(A,B) = (\psi'(B), \psi(A))$ for anti-automorphisms ψ, ψ' of $M_4(\mathbb{Z}_a)$; hence $U_a = \{(A, \psi(A)^{-1}) : A \in SL_4(\mathbb{Z}_a)\}$, and any matrix in $SL_4(\mathbb{F}_a)$ lifts to $SL_4(\mathbb{Z}_a)$ (lift the entries, then rescale one row by the inverse of the determinant, which is $\equiv 1$). If a is inert, $\mathcal{O}_a \cong M_4(\mathcal{O}_{E_a})$ and $\tau(Z) = H_a^{-1} Z^\dagger H_a$ for a hermitian H_a (Step 3 of the proof of Proposition 4.8). As τ preserves $M_4(\mathcal{O}_{E_a})$, conjugation by H_a preserves $M_4(\mathcal{O}_{E_a}) = \operatorname{End}(\mathcal{O}_{E_a}^4)$, so the lattices $\mathcal{O}_{E_a}^4$ and $H_a^{-1}\mathcal{O}_{E_a}^4$ have the same endomorphism ring; using the matrix units one sees that they are homothetic, so H_a is a scalar multiple of an element of $GL_4(\mathcal{O}_{E_a})$. After rescaling by a power of a, H_a is hermitian and invertible over $\mathcal{O}_{E_a}$. Let $g_0 \in GL_4(\mathcal{O}_{E_a})$ reduce to a given element of $SU_4(\mathbb{F}_a)$. If $g^\dagger H_a g = H_a + a^j\Delta$ with Δ hermitian and $j \geq 1$, then $g' = g(1 - \frac{a^j}{2} H_a^{-1}\Delta)$ satisfies $g'^\dagger H_a g' \equiv H_a \pmod{a^{j+1}}$. Iterating gives a unitary $g \equiv g_0 \pmod a$. Its determinant δ satisfies $\delta\bar{\delta} = 1$ and $\delta \equiv 1 \pmod a$, and composing g with the map that multiplies one vector of an orthonormal basis of $\mathcal{O}_{E_a}^4$ by δ^{-1} (such a basis exists by the argument of Lemma 3.12, as H_a is invertible over $\mathcal{O}_{E_a}$) gives an element of U_a lifting g_0.

Second, Γ is dense in $\prod_{\ell\neq 3} U_\ell$ (product over primes). Indeed the algebraic group $\mathbf{G}$ of the proof of Proposition 6.3 is simply connected and absolutely almost simple (over an algebraic closure it becomes SL_4), and $\mathbf{G}(\mathbb{Q}_3) \cong SU(V)$ is not compact. By Proposition 8.2 with $S = \{3, \infty\}$, $\mathbf{G}(\mathbb{Q})$ is dense in the restricted product of the $\mathbf{G}(\mathbb{Q}_\ell)$ over all primes $\ell \neq 3$. The product $\prod_{\ell\neq 3} U_\ell$ is open in it, and its intersection with $\mathbf{G}(\mathbb{Q})$ is Γ by Lemma 6.7. Hence $\Gamma \to U_a \to \bar{G}_a$ is onto. □

8.3 A quaternion algebra inside D

The field L_0 contains the real quadratic field $K' = \mathbb{Q}(\sqrt{13})$, the fixed field of σ^2; explicitly $\sqrt{13} = 2(\xi + \sigma^2\xi) - 1$. Put $E' = K'E = E(\sqrt{13})$, the fixed field of σ^2 in L, and $\omega = (1+\sqrt{13})/2$. The prime 3 splits in K', since $\frac{1+\sqrt{13}}{2} \cdot \frac{1-\sqrt{13}}{2} = -3$; we write

$$\mathfrak{p}_1 = \big((1-\sqrt{13})/2\big), \qquad \mathfrak{p}_2 = \big((1+\sqrt{13})/2\big),$$

and $\iota_1, \iota_2 \colon K' \to \mathbb{Q}_3$ for the corresponding embeddings, so that $v_3(\iota_k(x)) = v_{\mathfrak{p}_k}(x)$.

The centraliser of E'. An element $\sum \rho(f_i)U^i$ of D commutes with all $\rho(e)$, $e \in E'$, exactly when $f_1 = f_3 = 0$, because σ^i fixes E' only for even i. So the centraliser of $\rho(E')$ is

$$C = \{\rho(f_0) + \rho(f_2)U^2 : \ f_0, f_2 \in L\}.$$

Reordering the coordinates as $(0, 2, 1, 3)$ makes the elements of C block diagonal:

$$\rho(f_0) + \rho(f_2)U^2 \ \sim \ \begin{pmatrix} \beta & 0 \\ 0 & \sigma(\beta) \end{pmatrix}, \qquad \beta = \begin{pmatrix} f_0 & f_2 \\ \gamma\,\sigma^2 f_2 & \sigma^2 f_0 \end{pmatrix}, \tag{7}$$

where $\sigma(\beta)$ is obtained by applying σ to the entries. The 2×2 matrices β form a quaternion algebra over E' (the cyclic algebra of L/E' and γ, written as in Section 4.2). We write $\mathrm{trd}(x) = \mathrm{tr}\,\beta$ and $\mathrm{nrd}(x) = \det\beta$ for $x \in C$; they lie in E', and by (7) the characteristic polynomial of the 4×4 matrix x is

$$\det(t - x) = P(t) \cdot \sigma(P)(t), \qquad P(t) = t^2 - \mathrm{trd}(x)\,t + \mathrm{nrd}(x). \tag{8}$$

The twisted subalgebra. Since $\theta = \rho(\eta)$ commutes with $\rho(L)$, we have $\tau(\rho(c)) = \rho(\bar{c})$ for $c \in L$; in particular the anti-automorphism τ maps $\rho(E')$ to itself, and hence it maps the centraliser C to itself. Let $\tilde{x} = \mathrm{trd}(x) - x$ be the canonical involution of C (the adjugate of β), and

$$B = \{x \in C : \ \tau(x) = \tilde{x}\}.$$

The anti-automorphism τ commutes with $x \mapsto \tilde{x}$: this is clear on $\rho(E')$, and for $x \notin \rho(E')$ the element $\tau(x)$ satisfies the quadratic equation of x with conjugated coefficients, so $\mathrm{trd}(\tau(x)) = \overline{\mathrm{trd}(x)}$. So $x \mapsto \tau(\tilde{x})$ is a ring automorphism of C of order two, acting on $\rho(E')$ as conjugation, with fixed field K', and B is its fixed algebra. By Galois descent [28, Ch. X, §§1–2], B is a quaternion algebra over K' with $B \otimes_{K'} E' = C$; in our case this is also verified directly (Appendix B). If $y \in B$ and $\mathrm{nrd}(y) = 1$, then $\mathrm{trd}(y) = y + \tilde{y} = y + \tau(y)$ is fixed by τ, hence lies in K'; moreover $\tau(y) = \tilde{y} = y^{-1}$ and, by (8), $\det y = \mathrm{nrd}(y)\,\sigma(\mathrm{nrd}(y)) = 1$. Thus

$$B^1 = \{y \in B : \ \mathrm{nrd}(y) = 1\} \ \subseteq \ G. \tag{9}$$

Lemma 8.4 (Translation in B^1)**.** *Let $y \in B^1$ and $t_0 = \mathrm{trd}(y) \in K'$. Suppose that $v_{\mathfrak{p}_2}(t_0) \geq 0$ and $v_{\mathfrak{p}_1}(t_0) = -m < 0$. Then T contains a walk of length $2m$ from some vertex Λ to $y\Lambda$.*

Proof. By (8) and Proposition 4.8(a), the characteristic polynomial of $\varphi(y)$ is $(t^2 - t_0 t + 1)(t^2 - t_0' t + 1)$, where $t_0' = \sigma(t_0)$ is the conjugate of t_0 over $\mathbb{Q}$. Mapping to $\mathbb{Q}_3$ by ι_1, it becomes $(t^2 - \iota_1(t_0)t + 1)(t^2 - \iota_2(t_0)t + 1)$. The roots of the second factor are integral with product 1, hence units. Since $v_3(\iota_1(t_0)) = -m < 0$, the first factor has a root of valuation $-m$ (its Newton polygon has slopes $-m$ and m). By Proposition 3.17 there is a walk of length $2m$ from a vertex to its image under y. □

Proposition 8.5 (Facts established by exact computation, continued)**.** *(iii) B is ramified exactly at the prime (2), at $\mathfrak{p}_2$ and at the two real places of K'; it is split at $\mathfrak{p}_1$.*

(iv) $\mathcal{O}_B = B \cap \mathcal{O}$ is an order of B whose centre $\mathcal{O}_B \cap K'$ is $R = \mathbb{Z} + 7\omega\mathbb{Z}$. For every prime $\ell \notin \{2, 3, 7\}$, $\mathcal{O}_B \otimes \mathbb{Z}_\ell \cong M_2(\mathcal{O}_{K'} \otimes \mathbb{Z}_\ell)$, and $\mathcal{O}_B \otimes \mathbb{Z}_2$ is the maximal order of the division algebra $B \otimes \mathbb{Q}_2$.

(v) There is $Y \in \mathcal{O}_B$ with $\operatorname{trd}(Y) = 1$ and $\operatorname{nrd}(Y) = 22 - 7\omega$.

That B ramifies at the real places can also be seen directly: B^1 is contained in G, which is compact at the real places (Lemma 4.6), whereas the norm-one group of $M_2(\mathbb{R})$ is not compact.

8.4 The upper bound

We need several classical facts about quaternion algebras, a lemma on norm classes, and an elementary lattice-point lemma. A *quaternion algebra* over a field is a central simple algebra of dimension 4; it is *split* at a place if it becomes a matrix algebra there, and *ramified* otherwise.

Proposition 8.6 (Quaternion algebras [30])**.** *Let B be a quaternion algebra over a number field K', and B^1 its group of elements of reduced norm 1.*

(a) (Skolem–Noether.) *Two homomorphisms from a simple algebra into a central simple algebra over the same field are conjugate by an invertible element [30, Main Theorem 7.7.1].*

(b) If B_w is a division algebra over a local field K'_w, then every separable quadratic field extension of K'_w embeds in B_w, and the elements of B_w that are integral over the ring of integers of K'_w form the unique maximal order of B_w [30, Corollary 13.4.5 and Proposition 13.3.4].

(c) A quadratic field extension Ω of K' embeds in B if and only if $\Omega \otimes_{K'} K'_w$ is a field for every place w where B ramifies [30, Proposition 14.6.7].

(d) (Hasse–Schilling.) *The reduced norms of elements of $B^\times$ are exactly the elements of $K'^\times$ that are positive at the real places where B ramifies [30, Main Theorem 14.7.4].*

(e) (Strong approximation.) *If S is a finite set of places of K' containing the archimedean places and a place where B is split, then B^1 is dense in the restricted product of the groups B^1_w over the places $w \notin S$ [30, Main Theorem 28.5.3].*

Lemma 8.7 (Norm classes)**.** *Let Ω be a quadratic extension field of a number field K', and u a place of K' such that $\Omega \otimes_{K'} K'_u$ is a field. For every place $w \neq u$ of K' let a class $c_w \in K'^\times_w / \operatorname{N}(\Omega^\times_w)$ be given, trivial for almost all w, where $\Omega_w = \Omega \otimes_{K'} K'_w$. Then there is $c \in K'^\times$ which lies in the class c_w for every $w \neq u$.*

Proof. The local norm residue symbol identifies $K'^\times_w / \operatorname{N}(\Omega^\times_w)$ with a subgroup of $\{\pm 1\}$, equal to $\{\pm 1\}$ when Ω_w is a field. Let ε_w be the symbol of c_w for $w \neq u$, and $\varepsilon_u = \prod_{w \neq u} \varepsilon_w$, which is attained at u. Then $\prod_w \varepsilon_w = 1$ and almost all ε_w are 1, so by the existence theorem for elements with prescribed local norm residue symbols, a consequence of global reciprocity, there is $c \in K'^\times$ with these local symbols [24, 71:19]. (Where Ω_w is split, the class c_w is necessarily trivial and $\varepsilon_w = 1$.) □

Lemma 8.8 (Short elements in cosets)**.** *Let $c_{K'} = 64/(78 + 22\sqrt{13})$. If I is a fractional ideal of K' with $\operatorname{N}(I) < c_{K'}$, then every coset $x + I$ ($x \in K'$) contains an element t with $|t| < 2$ and $|t'| < 2$, where t' is the conjugate of t.*

Proof. Embed K' in $\mathbb{R}^2$ by $x \mapsto (x, x')$; then I is a lattice of covolume $\sqrt{13}\,\operatorname{N}(I)$. By Minkowski's lattice point theorem [23, Ch. I, §4] the square $[-r_0, r_0]^2$ with $r_0^2 = \sqrt{13}\,\operatorname{N}(I)$ contains a nonzero $x_0 \in I$. The lattice $x_0\mathcal{O}_{K'} \subseteq I$ has basis $x_0, x_0\omega$, and every coset of I contains a coset of $x_0\mathcal{O}_{K'}$, which meets $\{s_1 x_0 + s_2 x_0\omega : -\frac{1}{2} \leq s_1, s_2 < \frac{1}{2}\}$. For t in this set, $|t| \leq \frac{1}{2} r_0 (1 + |\omega|)$ and

$|t'| \le \frac{1}{2}r_0(1+|\omega'|)$, and $1+\max(|\omega|,|\omega'|) = \frac{3+\sqrt{13}}{2}$. Both are less than 2 because $r_0 < 8/(3+\sqrt{13})$, which is the hypothesis $\mathrm{N}(I) < 64/\big((3+\sqrt{13})^2\sqrt{13}\big) = c_{K'}$. □

Theorem 8.9. *Let $a \ge 5$ be an integer prime to 42, and let m be an integer with*

$$3^m > c_1 a^4, \qquad c_1 = \tfrac{147}{16}\big(78+22\sqrt{13}\big) = 1445.397\ldots$$

Then there are $y \in \Gamma(a)$ with $y \ne I$ and a walk of length at most $2m$ in T from a vertex to its image under y. Consequently

$$\mathrm{girth}(\mathcal{G}_a) \;\le\; 8\log_3 a + 2 + 2\log_3 c_1 \;<\; 8\log_3 a + 15.25.$$

Proof. Step 1: the trace. By the Chinese remainder theorem choose $t_1 \in \mathcal{O}_{K'}$ with

$$t_1 \equiv 2 \pmod{a^2}, \qquad t_1 \equiv \omega \pmod 2, \qquad t_1 \equiv 1 \pmod 7, \qquad t_1 \equiv 0 \pmod{\mathfrak{p}_2}.$$

Let $I = a^2 \cdot 14 \cdot \mathfrak{p}_2 \cdot \mathfrak{p}_1^{-m}$, so $\mathrm{N}(I) = a^4 \cdot 4 \cdot 49 \cdot 3 \cdot 3^{-m} = 588\, a^4/3^m$. The hypothesis on m is equivalent to $\mathrm{N}(I) < c_{K'}$, so by Lemma 8.8 there is $t_0 \in t_1 + I$ with $|t_0|, |t_0'| < 2$. Then t_0 is integral at every prime other than $\mathfrak{p}_1$, $v_{\mathfrak{p}_1}(t_0) \ge -m$, and t_0 satisfies the four congruences displayed for t_1. In particular $t_0 \ne \pm 2$.

Step 2: an element of B with trace t_0. Let $\Omega = K'[X]/(X^2 - t_0X + 1)$. At both real places $t_0^2 - 4 < 0$, so Ω is a field. At (2), the polynomial is $\equiv X^2 - \omega X + 1$ modulo 2, which is irreducible over the residue field $\mathbb{F}_4$ of K' at 2 (the substitution $X = \omega Z$ turns it into $Z^2 + Z + \omega$, and ω has trace 1 to $\mathbb{F}_2$); so $\Omega_{(2)}$ is the unramified quadratic extension of $K'_{(2)}$. At $\mathfrak{p}_2$ it is $\equiv X^2 + 1$, irreducible over $\mathbb{F}_3$. So Ω_w is a field at every place where B ramifies, and Ω embeds in B by Proposition 8.6(c). Let $y_1 \in B$ be the image of X; then $\mathrm{trd}(y_1) = t_0$ and $\mathrm{nrd}(y_1) = 1$.

Step 3: local elements. For every prime $\ell \ne 3$ we find $y_\ell \in \mathcal{O}_{B,\ell} = \mathcal{O}_B \otimes \mathbb{Z}_\ell$ with $\mathrm{trd}(y_\ell) = t_0$, $\mathrm{nrd}(y_\ell) = 1$ and $y_\ell - 1 \in a\mathcal{O}_{B,\ell}$.

- $\ell \notin \{2,3,7\}$. Identify $\mathcal{O}_{B,\ell} = M_2(\mathfrak{o}_\ell)$ with $\mathfrak{o}_\ell = \mathcal{O}_{K'} \otimes \mathbb{Z}_\ell$, and let ℓ^e be the exact power of ℓ dividing a. Since $t_0 \equiv 2 \pmod{a^2}$, the element $d_\ell = (t_0 - 2)/\ell^e$ lies in $\ell^e\mathfrak{o}_\ell$, and $y_\ell = \left(\begin{smallmatrix} 1 & \ell^e \\ d_\ell & t_0 - 1 \end{smallmatrix}\right)$ has trace t_0, determinant 1, and $y_\ell - 1 \in \ell^e M_2(\mathfrak{o}_\ell)$.
- $\ell = 2$. Here a is odd, so no congruence is required. By Step 2, $\Omega_{(2)}$ is a quadratic field, so it embeds in the division algebra $B \otimes \mathbb{Q}_2$, and the image y_2 of X, being integral over $\mathbb{Z}_2$, lies in the unique maximal order (Proposition 8.6(b)), which is $\mathcal{O}_{B,2}$ by Proposition 8.5(iv).
- $\ell = 7$. Again no congruence is required ($7 \nmid a$). Since $\mathrm{nrd}(Y) = 22 - 7\omega \equiv 1 \pmod{7\mathcal{O}_{K'}}$ and $R_7 = \mathbb{Z}_7 + 7\mathcal{O}_{K',7}$ is complete, $\mathrm{nrd}(Y)$ has a square root $\varrho \in 1 + 7\mathcal{O}_{K',7} \subseteq R_7$. Then $y^\circ = Y/\varrho \in \mathcal{O}_{B,7}$ has norm 1 and trace $t^\circ = 1/\varrho \equiv 1 \pmod 7$, and $\Delta^\circ = t^{\circ 2} - 4$ is a 7-adic unit. Now $t_0 \equiv 1 \equiv t^\circ \pmod 7$, so $\Delta = t_0^2 - 4$ satisfies $\Delta/\Delta^\circ = 1 + 4z$ with $z = (t_0 - t^\circ)(t_0 + t^\circ)/(4\Delta^\circ) \in 7\mathcal{O}_{K',7}$. By Hensel's lemma the equation $s^2 + s = z$ has a root $s \in 7\mathcal{O}_{K',7}$; put $u = 1 + 2s$, so $u^2 = \Delta/\Delta^\circ$, and $\beta_7 = (t_0 - ut^\circ)/2$. Both $u - 1$ and $\beta_7 = (t_0 - t^\circ)/2 - st^\circ$ lie in $7\mathcal{O}_{K',7} \subseteq R_7$. The element $y_7 = \beta_7 + uy^\circ \in \mathcal{O}_{B,7}$ has trace $2\beta_7 + ut^\circ = t_0$ and norm $\beta_7^2 + \beta_7 ut^\circ + u^2 = \big(t_0^2 - u^2\Delta^\circ\big)/4 = 1$.

For almost all ℓ the global element y_1 already has these properties, and there we take $y_\ell = y_1$.

Step 4: local conjugacy. For each $\ell \ne 3$, the elements y_ℓ and y_1 of $B_\ell = B \otimes \mathbb{Q}_\ell$ have the same characteristic polynomial $X^2 - t_0X + 1$, which is separable. Componentwise over the places w of K' above ℓ: if Ω_w is a field, the two embeddings of Ω_w into $B \otimes K'_w$ are conjugate by Proposition 8.6(a); if $\Omega_w \cong K'_w \times K'_w$, then $B \otimes K'_w$ has zero divisors, so it is $M_2(K'_w)$, and both elements are diagonalisable with the same distinct eigenvalues. So $y_\ell = h_\ell y_1 h_\ell^{-1}$ with $h_\ell \in B_\ell^\times$, and we take $h_\ell = 1$ when $y_\ell = y_1$. The element h_ℓ is unique up to right multiplication by the centraliser $K'_\ell[y_1]^\times \cong \Omega_\ell^\times$. Put $c_\ell = \mathrm{nrd}(h_\ell)$.

Step 5: a global norm. Apply Lemma 8.7 with $u = \mathfrak{p}_2$, prescribing the classes of the components of c_ℓ at all places of K' above primes $\ell \ne 3$, the trivial class at $\mathfrak{p}_1$, and the trivial

class (positivity) at the two real places. We obtain $c \in K'^{\times}$, totally positive, with $c \in c_\ell \,\mathrm{N}(\Omega_\ell^{\times})$ for all $\ell \neq 3$. Since c is positive at the real places, which are the real places where B ramifies, Proposition 8.6(d) gives $g_0 \in B^{\times}$ with $\mathrm{nrd}(g_0) = c$. Put $y' = g_0 y_1 g_0^{-1}$.

Step 6: local conjugators of norm one. For $\ell \neq 3$, the element $k'_\ell = h_\ell g_0^{-1}$ conjugates y' to y_ℓ, and $\mathrm{nrd}(k'_\ell) = c_\ell/c$ is a norm from $K'_\ell[y'] \cong \Omega_\ell$, say $\mathrm{nrd}(k'_\ell) = \mathrm{nrd}(z_\ell)$ with $z_\ell \in K'_\ell[y']^{\times}$. Then $k_\ell = k'_\ell z_\ell^{-1}$ has norm 1 and still conjugates y' to y_ℓ. For almost all ℓ we have $y_\ell = y_1$, $g_0^{\pm 1} \in \mathcal{O}_{B,\ell}$, c a unit, and $t_0^2 - 4$ a unit; then $\mathcal{O}_{K',\ell}[y']$ is the maximal order of the unramified algebra Ω_ℓ, whose units have all units of $\mathcal{O}_{K',\ell}$ as norms, so z_ℓ can be chosen with $k_\ell \in \mathcal{O}_{B,\ell}$. Hence $(k_\ell)_\ell$ is a point of B^1 over the finite adeles of K' away from 3.

Step 7: strong approximation. The set $\mathcal{W}$ of adelic points k of B^1 away from 3 and ∞ with $ky'k^{-1} \in \prod_{\ell \neq 3} \left(1 + a\mathcal{O}_{B,\ell}\right) \cap \mathcal{O}_{B,\ell}$ is open, and it contains $(k_\ell)_\ell$. The set of omitted places contains $\mathfrak{p}_1$, where B is split, so by Proposition 8.6(e) the group B^1 is dense in its adelic points away from 3 and ∞. Choose $k \in B^1 \cap \mathcal{W}$ and put $y = ky'k^{-1}$. Then $\mathrm{trd}(y) = t_0$, $\mathrm{nrd}(y) = 1$, and for every prime $\ell \neq 3$ we have $y \in \mathcal{O}_{B,\ell} \subseteq \mathcal{O}_\ell$ and $y - 1 \in a\mathcal{O}_{B,\ell} \subseteq a\mathcal{O}_\ell$. By Lemma 6.7 and (9), $y \in \Gamma(a)$, and $y \neq I$ because $t_0 \neq 2$.

Step 8: the length. By Theorem 6.4, $\Gamma(a)$ acts freely and $\mathcal{G}_a$ has no multiple edges, so y fixes no vertex. As t_0 is integral at $\mathfrak{p}_2$ and all eigenvalues of $\varphi(y)$ would be units if t_0 were integral at $\mathfrak{p}_1$ (proof of Lemma 8.4), in which case $|\det(y - I)|_3 \leq 1$ in contradiction with Theorem 5.2, we have $v_{\mathfrak{p}_1}(t_0) = -m'$ with $1 \leq m' \leq m$. By Lemma 8.4, T contains a walk of length $2m' \leq 2m$ from a vertex to its image under y. By Lemma 2.6, $\mathcal{G}_a$ contains a cycle of length at most $2m$.

Taking m minimal, $3^{m-1} \leq c_1 a^4$, so $\mathrm{girth}(\mathcal{G}_a) \leq 2m \leq 8\log_3 a + 2 + 2\log_3 c_1$, and $2 + 2\log_3 c_1 = 15.246\ldots$ □

Corollary 8.10. *For primes $a \notin \{2, 3, 7\}$,*

$$8\log_3 a - 8\log_3 2 \;\leq\; \mathrm{girth}(\mathcal{G}_a) \;\leq\; 8\log_3 a + 15.25,$$

and therefore $\mathrm{girth}(\mathcal{G}_a) = \frac{8}{5}\log_{27} n_a + O(1)$. *So $\frac{8}{5}$ is the largest girth constant of the family $(\mathcal{G}_a)$.*

Proof. Combine Theorems 8.3 and 8.9, and note that $\log_{27} n_a = 5\log_3 a + O(1)$ by the formula for n_a. □

9 Concluding remarks

Figure 9 places the result among the known values of the girth constant. We end with some comments on the method and some questions it raises.

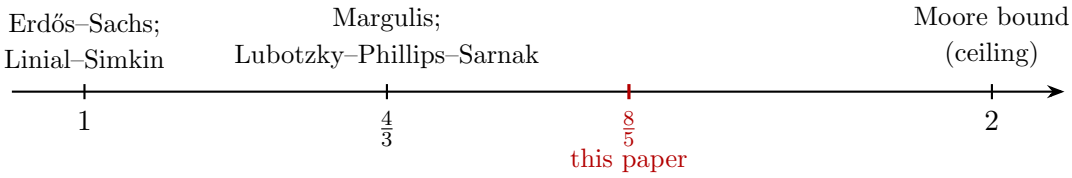

Figure 9: Known values of the constant c in $\mathrm{girth}(G) \geq c\,\log_{d-1} n - O(1)$.

(1) *Why $\frac{8}{5}$: the limit of the method.* The proof balances three exponents. The certificate of an element congruent to I modulo $\mathfrak{a}$ is divisible by $\mathfrak{a}^m$, where m is the size of the matrices. Along an apartment, one period of translation multiplies the size of balls in the tree by q^s, where s is the sum, with multiplicities, of the positive roots evaluated on the translation. And the same translation multiplies the certificate by q^e, where e is the

number of expanding eigenvalues. Counting vertices with the dimension $\dim \mathbf{G}$ of the group, the method gives the constant

$$c = \frac{s \cdot m}{e \cdot \dim \mathbf{G}}.$$

For SL_2 (LPS) this is $\frac{2\cdot 2}{1\cdot 3} = \frac{4}{3}$, and for our group SU_4, with the translation $\mathrm{diag}(\pi, 1, 1, \pi^{-1})$, it is $\frac{6\cdot 4}{1\cdot 15} = \frac{8}{5}$. For the special unitary group of an m-dimensional hermitian space of Witt index one over F'/F, the same count gives a value which increases with m. But Witt index one forces $m \le 4$: an anisotropic hermitian space over a nonarchimedean local field has dimension at most two [15], so an m-dimensional space has Witt index at least $\frac{m-2}{2}$. (In other words, the u-invariant of hermitian forms over a local field is 2.) A Witt index of two or more would make the building of higher dimension, not a tree, and would allow elements with two expanding eigenvalues. For the inner forms $SL_2(\Delta)$, with Δ a local division algebra of degree δ, the same count gives $\frac{4\delta^2}{4\delta^2-1} \le \frac{4}{3}$. So, for the unitary groups and the inner forms of SL_2 considered here, $\frac{8}{5}$ is the largest value that this bookkeeping gives.

We mention, without proof, two further facts suggesting that within this framework the determinant is the best certificate. First, let f be a conjugation-invariant regular function on SL_m over a field of characteristic zero with $f(I) = 0$, let $r(f)$ be its order of vanishing at I, and let $h(f)$ be the largest power of t occurring in $f(\mathrm{diag}(t, 1, \dots, 1, t^{-1})\, y)$, where y is a diagonal matrix of determinant one with generic entries. Then $r(f) \le m\, h(f)$, with equality only for scalar multiples of powers of $\det(g - I)$. Second, imposing congruence conditions at a fixed finite set of places in ways other than by principal congruence subgroups does not help: if F is a finite extension of $\mathbb{Q}_p$ with residue field $\mathbb{F}_Q$ and K_0 is a compact open subgroup of $SL_4(F)$, or of the special unitary group of a four-dimensional hermitian space over a quadratic extension of F, there is $C > 0$ such that every open subgroup $U \subseteq K_0$ satisfies $[K_0 : U] \ge C\, Q^{15e(U)/4}$, where $e(U)$ is the least valuation of $\det(u - I)$ for $u \in U$; with $\dim SU_4 = 15$ and the divisibility exponent 4 this again leads to $\frac{8}{5}$. These are limitations of the certificate method, not upper bounds for the girth of the graphs: a larger constant would require a different source of nonvanishing or of divisibility, or graphs that are not quotients of trees by arithmetic groups of this kind.

(2) *Sharpness in general.* For the family of Section 8, $\frac{8}{5}$ is the largest girth constant. The proof of Theorem 8.9 uses the specific data only through a τ-stable quadratic subfield E' whose real subfield is split at $\mathfrak{p}$ and through local conditions at finitely many places. We expect that the same argument gives $\mathrm{girth}(\mathcal{G}_\mathfrak{a}) = 8 \log_q \mathrm{N}(\mathfrak{a}) + O(1)$ for all the families of Theorem 6.9, so that $\frac{8}{5}$ is their largest girth constant as well.

(3) *The additive constant.* In the computed range (Appendix B) the girth of the explicit family equals the proved lower bound $2\lceil \log_3(a^4/16) \rceil$ for $a = 5, 11$ and exceeds it by 2 for $a = 13$. In all three cases a shortest cycle comes from an element of the norm-one group of a quaternion subalgebra, as in the proof of Theorem 8.9. Does the girth always exceed the lower bound $2\lceil \log_3(a^4/16) \rceil$ by at most 2?

(4) *Expansion.* Are the graphs $\mathcal{G}_\mathfrak{a}$ Ramanujan, that is, does every eigenvalue other than $\pm(q^3+1)$ have absolute value at most $2\sqrt{q^3}$? The question concerns the local components at $\mathfrak{p}$ of the automorphic representations of the unitary group of (D, τ), an inner form of a unitary group in four variables. If the answer is positive, the graphs combine optimal spectral expansion with girth constant $\frac{8}{5}$. The graphs are too large for a direct numerical test: already $\mathcal{G}_5$ in the explicit family has about $4.9 \cdot 10^9$ vertices.

(5) *Other degrees.* Our degrees are $q^3 + 1$. For all other degrees the best known constants are those of [19, 22, 8], which are at most $\frac{4}{3}$. Can the constant $\frac{4}{3}$ be improved for every degree?

Appendix A Hermitian forms over finite fields

Let κ' be a finite field with Q^2 elements, $\kappa \subset \kappa'$ its subfield with Q elements, and $x \mapsto \overline{x} = x^Q$ the nontrivial automorphism of κ' over κ. Hermitian forms over κ' are defined as in Section 3.2; in Section 3 we apply the results below with $Q = q$. The norm $\mathrm{N}(x) = x^{Q+1}$ maps $\kappa'^{\times}$ onto $\kappa^{\times}$, and every value in $\kappa^{\times}$ is taken $Q+1$ times.

Lemma A.1. *Every nondegenerate hermitian space over κ' has an orthonormal basis. In particular two nondegenerate hermitian spaces of the same dimension are isometric, and their special unitary groups are isomorphic.*

Proof. The proof of Lemma 3.2 applies verbatim and gives an orthogonal basis; each $H(z,z)$ is a nonzero element of κ, hence a norm $\mathrm{N}(c)$, and replacing z by $c^{-1}z$ makes it 1. □

Proof of Lemma 3.8. (a) By Lemma A.1, $b(x,x) = \mathrm{N}(x_1) + \mathrm{N}(x_2) + \mathrm{N}(x_3)$ in a suitable basis. For $c \in \kappa$ let $S(c)$ be the number of $(x_1, x_2) \in \kappa'^2$ with $\mathrm{N}(x_1) + \mathrm{N}(x_2) = c$. Counting x_1 first, $S(0) = 1 + (Q^2-1)(Q+1)$. Scaling by elements of $\kappa'^{\times}$ shows that $S(c)$ is the same for all $c \neq 0$, and $Q^4 = S(0) + (Q-1)S(c)$ gives $S(c) = Q(Q^2-1)$. The number of nonzero isotropic vectors is therefore $\big(S(0)-1\big) + (Q^2-1)\,S(c) = (Q^2-1)(Q^3+1)$, and the number of isotropic lines is Q^3+1.

(b) A totally isotropic subspace S satisfies $S \subseteq S^{\perp}$, and $\dim S + \dim S^{\perp} = 3$, so $\dim S \leq 1$.

(c) Let $P = \kappa' e$ and choose f with $P^{\perp} = \kappa' e + \kappa' f$. If $b(f,f) = 0$, then $P^{\perp}$ would be totally isotropic, contradicting (b). So $b(f,f) \neq 0$, and $b(ae+cf, ae+cf) = \mathrm{N}(c)\,b(f,f)$ vanishes only for $c = 0$. □

Lemma A.2. *$|SL_4(\mathbb{F}_Q)| = Q^6(Q^2-1)(Q^3-1)(Q^4-1)$, and the special unitary group $SU_4(\mathbb{F}_Q)$ of a nondegenerate four-dimensional hermitian space over $\mathbb{F}_{Q^2}$ has order $Q^6(Q^2-1)(Q^3+1)(Q^4-1)$.*

Proof. The first formula is the standard count of ordered bases, divided by $|\mathbb{F}_Q^{\times}|$. For the second (see also [33, §3.6]), let Z_s be the number of vectors x (including 0) with $b(x,x) = 0$ in an s-dimensional nondegenerate space, and A_s the number with $b(x,x) = 1$. As in the proof of Lemma 3.8(a), $Q^{2s} = Z_s + (Q-1)A_s$ and $Z_{s+1} = Z_s + (Q^{2s} - Z_s)(Q+1)$, with $Z_1 = 1$; by induction $Z_s = Q^{2s-1} + (-1)^s(Q^s - Q^{s-1})$ and $A_s = Q^{s-1}\big(Q^s - (-1)^s\big)$. Counting ordered orthonormal bases gives $|U_4| = A_4A_3A_2A_1 = Q^6(Q+1)(Q^2-1)(Q^3+1)(Q^4-1)$. The determinant maps U_4 onto the group of z with $z\overline{z} = 1$, of order $Q+1$, and its kernel is SU_4. □

Appendix B The explicit family: certificates and numerical data

This appendix concerns the data of Section 8.1. All computations were done with SageMath and PARI/GP and are exact: they take place in number fields, in $\mathbb{Q}$, in finite fields, or in $\mathbb{Q}_3$ with certified error bounds, and no decision depends on floating point arithmetic.

B.1 How the facts of Propositions 8.1 and 8.5 are certified

(i) The algebra and the order. The local invariants of D are computed from norm residues: at the two primes of E above 2 the algebra is a division algebra (with invariants $\frac{1}{4}$ and $\frac{3}{4}$); at all other places it is split, because there either L/E is unramified and γ is a unit, or (13 and 23) γ is a local norm, as one checks from its residues. The maximal order $\mathcal{M}$ is given by a $\mathbb{Z}$-basis of 32 elements; one checks that it contains 1 and $\mathcal{O}_E$, and that all 1024 products of basis elements are integral combinations. Its reduced trace form has discriminant of absolute value $2^{24} \cdot 7^{16}$, so $\mathcal{M} \otimes \mathbb{Z}_a$ is maximal for $a \notin \{2, 7\}$; maximality at 2 and 7 is also verified. The order $\mathcal{O} = \mathcal{M} \cap \tau(\mathcal{M})$ has index 3^6 in $\mathcal{M}$.

(ii) Orbits and stabilisers. At 3 we use the local model of Lemma 4.9, with the four 3-adic roots of the polynomial of ξ computed to certified precision. Let Λ_A be a vertex of type 1 and Λ_B a neighbour of type 3. For each of the 28 neighbours X of Λ_A we give an element of Γ mapping Λ_B to X, and for each of the 28 neighbours X' of Λ_B an element of Γ mapping Λ_A to X'; each is checked to lie in Γ, and the images are checked by exact lattice computations. Since T is connected (Proposition 3.10), induction on the distance from Λ_A shows that every vertex lies in $\Gamma\Lambda_A \cup \Gamma\Lambda_B$, and these orbits are distinct because Γ preserves types. The stabiliser of a vertex is finite, and its elements have bounded denominators at 3; they are the solutions in a lattice of the equation $\mathrm{Tr}_{E/\mathbb{Q}}\,\mathrm{tr}(\tau(x)x) = 8$ for the positive definite quadratic form $x \mapsto \mathrm{Tr}_{E/\mathbb{Q}}\,\mathrm{tr}(\tau(x)x)$, which a complete enumeration (Fincke–Pohst) finds. Each stabiliser has 12 elements and contains an element of order 12. The stabiliser of Λ_A acts on its 28 neighbours with kernel $\{\pm I\}$ and orbits of sizes $6, 1, 6, 6, 3, 6$; so the quotient $\Gamma\backslash T$ has two vertices and six edges, whose stabilisers have orders $2, 12, 2, 2, 4, 2$.

(iii)–(v) The quaternion algebra. One computes a K'-basis $1, i, j, ij$ of B with $i \in \rho(L)$, $j \in \rho(L)U^2$, $i^2, j^2 \in K'$ and $ij = -ji$, so $B = (i^2, j^2)_{K'}$, and its Hilbert symbols at all primes dividing $2 \cdot 3 \cdot i^2 j^2$ and at the real places. The order $\mathcal{O}_B = B \cap \mathcal{O}$ has rank 8, centre $\mathbb{Z} + 7\omega\mathbb{Z}$, and discriminant $2^4 \cdot 3^2 \cdot 7^8 \cdot 13^4$ for the trace form $\mathrm{Tr}_{K'/\mathbb{Q}} \circ \mathrm{trd}$; comparing with the discriminant of a maximal order gives the local statements of Proposition 8.5(iv) [30, §15.5]. The element Y of (v) is given by its coordinates in the basis of $\mathcal{O}$.

B.2 Exact girths

Table 2 lists the first three graphs of the family. The number of vertices is given by Theorem 8.3; the lower bound is $2\lceil \log_3(a^4/16) \rceil$ (Theorem 6.4); the upper bound is $2m$ for the least m with $3^m > c_1 a^4$ (Theorem 8.9).

a	a in E	n_a	$\log_{27} n_a$	lower bound	upper bound	exact girth
5	inert	4 914 000 000	6.77	8	26	8
11	split	689 888 370 864 000	10.37	14	32	14
13	inert	8 484 065 961 221 760	11.13	14	32	16

Table 2: The explicit 28-regular family for small a. For comparison, the Moore bound is $2\log_{27} n_a + 2$.

Upper bounds. For each $a \in \{5, 11, 13\}$ there is an explicit element $w_a \in \Gamma(a)$, $w_a \neq I$, given by its coordinates in the basis of $\mathcal{O}$, with characteristic polynomial $X^4 - tX^3 + sX^2 - tX + 1$, where

$$(t, s) = \Big(-\tfrac{151}{81}, \tfrac{161}{81}\Big), \quad \Big(-\tfrac{3473}{2187}, \tfrac{41}{27}\Big), \quad \Big(-\tfrac{1979}{6561}, \tfrac{3827}{2187}\Big)$$

for $a = 5, 11, 13$. The trace t has 3-adic valuation $-4, -7, -8$; by Lemma 3.15 the unique eigenvalue of negative valuation has this valuation, so by Propositions 3.16 and 3.17 the element moves some vertex a distance exactly $8, 14, 16$ and no vertex less. By Lemma 2.6, $\mathrm{girth}(\mathcal{G}_a) \leq 8, 14, 16$. The certificates are $\det(w_a - I) = 2 - 2t + s = 5^4/3^4,\ 11^4/3^7,\ 13^4/3^8$. In each case $t \in \mathbb{Q}$, and the element $u_a = w_a + \tau(w_a) = w_a + w_a^{-1}$ satisfies $u_a^2 - tu_a + s - 2 = 0$; it generates the real quadratic field $\mathbb{Q}(\sqrt{37})$, $\mathbb{Q}(\sqrt{1453})$, $\mathbb{Q}(\sqrt{1645})$ respectively, in which 3 splits, and w_a lies in the norm-one group of the quaternion algebra obtained from $E' = E(u_a)$ as B was obtained from $E(\sqrt{13})$ in Section 8.

Lower bounds. For $a = 5$ and $a = 11$ the lower bound of Theorem 6.4 equals the upper bound. For $a = 13$ it gives 14, and the following argument excludes 14.

Proposition B.1. *No element $w \neq I$ of $\Gamma(13)$ moves a vertex of T a distance 14. Hence $\mathrm{girth}(\mathcal{G}_{13}) = 16$.*

Proof. Suppose that T contains a walk of length 14 from a vertex Λ to $w\Lambda$. The characteristic polynomial of w has the form $X^4 - tX^3 + sX^2 - \bar{t}X + 1$ with $t \in E$ and $s \in \mathbb{Q}$: the coefficients lie in E (Lemma 4.4), and since $w^{-1} = \tau(w)$ is conjugate to w^*, the characteristic polynomial of w^{-1}, which is the reversed polynomial, is obtained from that of w by conjugating the coefficients.

Denominators. By Proposition 3.16 and Lemma 3.15, the eigenvalues of w have 3-adic valuations at least -7, and at most one is negative; so every coefficient has valuation at least -7. They are integral at all other primes (Lemma 4.7). Hence $t = (r_1 + r_2\alpha)/3^7$ and $s = r_3/3^7$ with $r_1, r_2, r_3 \in \mathbb{Z}$.

Archimedean bounds. The eigenvalues have absolute value 1 (Lemma 4.6), so $|t| \leq 4$ and $|s| \leq 6$.

Congruences. Write $w = 1 + 13Z$ with $Z \in \mathcal{O}_{13}$. Expanding $\det(1 + 13Z) = 1$ gives $\operatorname{tr} Z \equiv 0 \pmod{13}$, hence $t \equiv 4$ and $s = 6 + 3 \cdot 13 \operatorname{tr} Z + 13^2 e_2(Z) \equiv 6$ modulo 13^2.

The certificate. $x = \det(w - I) = 2 - (t + \bar{t}) + s$ is a nonzero rational number with $3^7 x \in \mathbb{Z}$, divisible by 13^4, and $|x| \leq 16$. As $16 \cdot 3^7 = 34992 < 2 \cdot 13^4$, we get $3^7 x = \pm 13^4$, which determines r_3 in terms of r_1, r_2 and the sign.

Enumeration. These conditions leave 819 possible polynomials. For exactly one of them all four complex roots have absolute value 1, namely

$$X^4 + \tfrac{7138}{2187}X^3 + \tfrac{9911}{2187}X^2 + \tfrac{7138}{2187}X + 1.$$

This polynomial has four distinct roots $\lambda_1, \lambda_1^{-1}, \lambda_2, \lambda_2^{-1}$ in $\mathbb{Q}_3$, none equal to ± 1 (by Hensel's lemma; their valuations are $-7, 7, 0, 0$).

Contradiction. Let $v_1, v_2 \in V$ be eigenvectors of $\varphi(w)$ for λ_1, λ_2. Since the λ_i lie in $\mathbb{Q}_3$, which is fixed by conjugation, $H(v_i, v_j) = H(wv_i, wv_j) = \lambda_i \lambda_j H(v_i, v_j)$. As λ_1^2, λ_2^2 and $\lambda_1\lambda_2$ differ from 1, the plane spanned by v_1, v_2 is totally isotropic, which contradicts Proposition 3.3.

So every $w \neq I$ in $\Gamma(13)$ moves every vertex a distance at least 16 (distances are even, and at least 14 by Theorem 6.4), and $\operatorname{girth}(\mathcal{G}_{13}) \geq 16$. The element w_{13} gives equality. □

References

[1] C. Ballantine and D. Ciubotaru, *Ramanujan bigraphs associated with $SU(3)$ over a p-adic field*, Proc. Amer. Math. Soc. **139** (2011), 1939–1953.

[2] C. Ballantine, B. Feigon, R. Ganapathy, J. Kool, K. Maurischat and A. Wooding, *Explicit construction of Ramanujan bigraphs*, in: Women in Numbers Europe, Assoc. Women Math. Ser. **2**, Springer, 2015, 1–16.

[3] N. Biggs, *Constructions for cubic graphs with large girth*, Electron. J. Combin. **5** (1998), #A1.

[4] N. L. Biggs and A. G. Boshier, *Note on the girth of Ramanujan graphs*, J. Combin. Theory Ser. B **49** (1990), 190–194.

[5] N. L. Biggs and M. J. Hoare, *The sextet construction for cubic graphs*, Combinatorica **3** (1983), 153–165.

[6] A. Borel and Harish-Chandra, *Arithmetic subgroups of algebraic groups*, Ann. of Math. **75** (1962), 485–535.

[7] F. Bruhat and J. Tits, *Schémas en groupes et immeubles des groupes classiques sur un corps local. II: groupes unitaires*, Bull. Soc. Math. France **115** (1987), 141–195.

[8] X. Dahan, *Regular graphs of large girth and arbitrary degree*, Combinatorica **34** (2014), 407–426.

[9] P. Erdős and H. Sachs, *Reguläre Graphen gegebener Taillenweite mit minimaler Knotenzahl*, Wiss. Z. Martin-Luther-Univ. Halle-Wittenberg Math.-Natur. Reihe **12** (1963), 251–258.

[10] S. Evra, B. Feigon, K. Maurischat and O. Parzanchevski, *Ramanujan bigraphs*, arXiv:2312.06507.

[11] S. Evra and O. Parzanchevski, *Ramanujan complexes and Golden Gates in $PU(3)$*, Geom. Funct. Anal. **32** (2022), 193–235.

[12] G. Exoo and R. Jajcay, *Dynamic cage survey*, Electron. J. Combin., Dynamic Survey DS16 (2013).

[13] A. Gamburd, S. Hoory, M. Shahshahani, A. Shalev and B. Virág, *On the girth of random Cayley graphs*, Random Structures Algorithms **35** (2009), 100–117.

[14] S. Hoory, N. Linial and A. Wigderson, *Expander graphs and their applications*, Bull. Amer. Math. Soc. **43** (2006), 439–561.

[15] R. Jacobowitz, *Hermitian forms over local fields*, Amer. J. Math. **84** (1962), 441–465.

[16] M. Kneser, *Starke Approximation in algebraischen Gruppen. I*, J. Reine Angew. Math. **218** (1965), 190–203.

[17] F. Lazebnik, V. A. Ustimenko and A. J. Woldar, *A new series of dense graphs of high girth*, Bull. Amer. Math. Soc. **32** (1995), 73–79.

[18] N. Linial and M. Simkin, *A randomized construction of high girth regular graphs*, Random Structures Algorithms **58** (2021), 345–369.

[19] A. Lubotzky, R. Phillips and P. Sarnak, *Ramanujan graphs*, Combinatorica **8** (1988), 261–277.

[20] G. A. Margulis, *Explicit constructions of graphs without short cycles and low density codes*, Combinatorica **2** (1982), 71–78.

[21] G. A. Margulis, *Explicit group-theoretical constructions of combinatorial schemes and their application to the design of expanders and concentrators*, Problems Inform. Transmission **24** (1988), 39–46.

[22] M. Morgenstern, *Existence and explicit constructions of $q+1$ regular Ramanujan graphs for every prime power q*, J. Combin. Theory Ser. B **62** (1994), 44–62.

[23] J. Neukirch, *Algebraic Number Theory*, Grundlehren der Mathematischen Wissenschaften **322**, Springer, 1999.

[24] O. T. O'Meara, *Introduction to Quadratic Forms*, Grundlehren der Mathematischen Wissenschaften **117**, Springer, 1963.

[25] V. P. Platonov, *The problem of strong approximation and the Kneser–Tits hypothesis for algebraic groups*, Izv. Akad. Nauk SSSR Ser. Mat. **33** (1969), 1211–1219.

[26] V. Platonov and A. Rapinchuk, *Algebraic Groups and Number Theory*, Academic Press, 1994.

[27] A. S. Rapinchuk, *Strong approximation for algebraic groups*, in: Thin Groups and Superstrong Approximation, Math. Sci. Res. Inst. Publ. **61**, Cambridge University Press, 2014, 269–298.

[28] J.-P. Serre, *Local Fields*, Graduate Texts in Mathematics **67**, Springer, 1979.

[29] J.-P. Serre, *Trees*, Springer, 1980.

[30] J. Voight, *Quaternion Algebras*, Graduate Texts in Mathematics **288**, Springer, 2021.

[31] I. Vollaard and T. Wedhorn, *The supersingular locus of the Shimura variety of $GU(1, n-1)$ II*, Invent. Math. **184** (2011), 591–627.

[32] A. Weiss, *Girths of bipartite sextet graphs*, Combinatorica **4** (1984), 241–245.

[33] R. A. Wilson, *The Finite Simple Groups*, Graduate Texts in Mathematics **251**, Springer, 2009.