Eigenvalues of hyperbolic elements in Kleinian groups

D. D. Long* & A. W. Reid†

November 4, 2008

1 Introduction

Let $\Gamma$ be a torsion-free Kleinian group, so that $M = \mathbb{H}^3/\Gamma$ is an orientable hyperbolic 3-manifold. The non-trivial elements of $\Gamma$ are classified as either parabolic or hyperbolic. If $\gamma \in \Gamma$ is hyperbolic, then $\gamma$ has an axis in $\mathbb{H}^3$ which projects to a closed geodesic $g_\gamma$ in $M$ (which depends only on the conjugacy class of $\gamma$ in $\Gamma$). The element $\gamma$ acts on its axis by translating and possibly rotating around the axis. In terms of eigenvalues, if $\gamma \in \Gamma$ is hyperbolic, we let

$$\lambda = \lambda_\gamma = r_\gamma e^{i\theta_\gamma}$$

be the eigenvalue of $\gamma$ (more accurately of a pre-image of $\gamma$ in $\text{SL}(2, \mathbb{C})$) for which $|\lambda| > 1$. The angle $\theta_\gamma$ takes values in $[0, 2\pi)$, and is the rotation angle mentioned above. We will usually suppress the subscripts. A hyperbolic element is called purely hyperbolic if and only if $\theta = 0$, or equivalently, if $\text{tr}(\gamma) \in \mathbb{R}$.

The length of the closed geodesic $g_\gamma$ is given by $2 \ln |\lambda|$ and the collections of these lengths counted with multiplicities is a well-known important geometric invariant of the manifold $M$ (see [2] and [3] and the references therein). On the other hand, little seems known about the “angle spectrum” for hyperbolic 3-manifolds. If $\Gamma$ is not Fuchsian, then there must be hyperbolic elements that are not purely hyperbolic, however, the following question naturally arises as a first step beyond this.

Question 1: Let $M = \mathbb{H}^3/\Gamma$ be a finite volume orientable hyperbolic 3-manifold, does $\Gamma$ contain infinitely many conjugacy classes of hyperbolic elements, no power of which is purely hyperbolic?

It is implicit in [2] (see the discussion in §4.1 below) that Question 1 has an affirmative answer for arithmetic Kleinian groups. The purpose of this note is to establish that this holds more generally. Namely we prove:

Theorem 1.1 Let $M = \mathbb{H}^3/\Gamma$ be as in Question 1. Then $\Gamma$ contains infinitely many primitive hyperbolic elements with the property that they have no power which is purely hyperbolic.

Indeed, Theorem 1.1 is a consequence of a more general result.

Theorem 1.2 Let $\Gamma$ be a finitely generated Zariski dense Kleinian group whose trace-field is a finite extension of $\mathbb{Q}$. Then $\Gamma$ contains infinitely many primitive hyperbolic elements with the property that they have no power which is purely hyperbolic.

*supported in part by the NSF
†supported in part by the NSF
The Zariski density condition ensures that the group $\Gamma$ is non-elementary and does not contain a Fuchsian group of finite index. Clearly for any Kleinian group that is virtually a Fuchsian group, all hyperbolic elements have a power that is purely hyperbolic.

Theorem 1.1 follows immediately from Theorem 1.2 by the well-known consequence of Mostow Rigidity that the trace-field of a finite co-volume Kleinian group is a number field (see [7] for example). The proof of Theorem 1.2 is given in §3. The proof proceeds by first establishing the existence of one primitive hyperbolic element for which no power is purely hyperbolic. The extension to infinite can be made either by an algebraic argument or a geometric argument, and we include both.

There is an obvious generalization of the previous discussion to arbitrary dimensions, and in §5 we provide a proof of the following result.

**Theorem 1.3** Let $M = \mathbb{H}^n / \Gamma$ be an orientable hyperbolic $n$-manifold of finite volume. Then $\Gamma$ contains infinitely many primitive hyperbolic elements with the property that they have no power which is purely hyperbolic.

As in the proof of Theorem 1.2, the proof of Theorem 1.3 proceeds by first establishing the existence of one primitive hyperbolic element for which no power is purely hyperbolic. However, the method of proof is different to that given for dimension 3. Indeed, the proof in the higher dimensional case does not work in dimension 3, and so it is natural to separate the case of dimension 3. Amusingly, the issue is related to whether there are infinitely many Mersenne primes (see §5).

**Acknowledgments:** We thank Mahan Mj for email correspondence on the “angle spectrum” that prompted us to write this down carefully, and Chris Leininger for correspondence that helped to clarify the statement of Theorem 1.2. We also wish to thank Ted Chinburg and Emily Hamilton for many interesting conversations on matters related to this arising from [2]. The second author wishes to thank the Institute for Advanced Study for its hospitality whilst this paper was written.

# 2 Some preliminaries for the proof of Theorems 1.1 and 1.2

## 2.1

By a number field $k$ we will mean a finite extension of $\mathbb{Q}$. The ring of integers of $k$ will be denoted $\mathcal{O}_k$. A place $\nu$ of $k$ will be one of the canonical absolute values of $k$. The finite places of $k$ correspond bijectively to the prime ideals of $\mathcal{O}_k$. We denote by $k_\nu$ the completion of of $k$ at a place $\nu$. In the case of finite places we sometimes abuse notation and write the prime $\mathfrak{p}$ rather than the associated place $\nu$ when referring to the completions.

If $\mathfrak{a}$ is an ideal of $\mathcal{O}_k$, the norm of $\mathfrak{a}$ is the cardinality of the quotient ring $\mathcal{O}_k / \mathfrak{a}$ and is denoted by $N(\mathfrak{a})$. When $\mathfrak{a}$ is a prime ideal, then $N(\mathfrak{a}) = p^t$ for some rational prime $p$, and $\mathcal{O}_k / \mathfrak{a}$ is a finite field of characteristic $p$. We will denote this finite field by $\mathbb{F}_{\mathfrak{a}}$.

## 2.2

For convenience we record two well-known results about extensions of number fields. We refer the reader to [4] for example for more details.

The first of these follows from the fact that if $\zeta = e^{2\pi i / n}$ is a primitive $n$-th root of unity, then $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \phi(n)$ (where $\phi$ denotes the Euler $\phi$-function) and $\phi(n)$ is well-known to go to infinity with $n$.

**Proposition 2.1** There are only finitely many roots of unity $\zeta$ for which $\mathbb{Q}(\zeta)$ has bounded degree over $\mathbb{Q}$.
The second result we need requires some additional notation. Let \( k \) be a number field and \( L \) a proper subfield. Suppose that \( p \) is a rational prime and \( P \) (resp. \( \mathcal{P} \)) is an \( L \)-prime (resp. \( k \)-prime) divisor of \( p \). Then we get extensions of local fields,

\[
\mathbb{Q}_p \subset L_P \subset k_P,
\]

and extensions of finite fields (the so-called residue class fields)

\[
\mathbb{F}_p \subset \mathbb{F}_P \subset \mathbb{F}_{\mathcal{P}}.
\]

Note that, even though \( L \) is a proper subfield of \( k \), the field extensions shown above may all be equalities. With this we have the following standard consequence of the Cebotarev Density theorem. We sketch a proof for convenience.

**Proposition 2.2** In the notation above, there exist infinitely many rational primes \( p \) for which the field extension \( \mathbb{F}_P/\mathbb{F}_P \) has degree at least 2.

**Proof:** Let \( K \) denote the Galois closure of \( k \). Since \( L \) is a proper subfield of \( k \) there exists a Galois automorphism \( \sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/L) \) such that \( \sigma \) is trivial on \( L \) and non-trivial on \( k \). The Cebotarev density theorem provides a positive density set of primes of \( \mathbb{Q} \) in \( K \) for which the induced Galois automorphism \( \sigma \) of the Galois extension \( \overline{\mathbb{Q}}/\mathbb{F}_P \) has order \( |\sigma| \). In particular \( \sigma \) is trivial on \( \mathbb{F}_P \) but not on \( \mathbb{F}_P \); i.e. \( \mathbb{F}_P \) is a proper extension of \( \mathbb{F}_P \) as required. 

\[\square\]

**2.3**

We will also make use of the classification of elements in \( \mathrm{PSL}(2, \mathbb{F}) \) where \( \mathbb{F} \) is a finite field. The following is easily deduced from [11] §6.23. We will exclude the prime 2 from all considerations and henceforth any prime \( p \) that is mentioned is odd.

**Proposition 2.3** Suppose that \( \mathbb{F} \) is a finite field of order \( p^t \), and \( x \in \mathrm{PSL}(2, \mathbb{F}) \) a non-trivial element. Then either \( x \) is unipotent and has order \( p \), or the order of \( x \) is a divisor of \( (p^t \pm 1)/2 \). Moreover, for each divisor \( m \) of \( (p^t \pm 1)/2 \), there is an element of \( \mathrm{PSL}(2, \mathbb{F}) \) of order \( m \).

**3 Proof of Theorem 1.2**

Before commencing with the proof we introduce some notation and make some preliminary comments. There is no loss in generality in assuming that \( \Gamma \) is torsion-free. Let \( k \) denote the trace-field of \( \Gamma \). This is not a subfield of \( \mathbb{R} \), since if so, then \( \Gamma \) is conjugate into \( \mathrm{PSL}(2, \mathbb{R}) \) and this contradicts Zariski density.

As remarked in §1, since \( \Gamma \) is a non-elementary Kleinian group, there are infinitely many hyperbolic elements that have no common fixed point. Since the trace of a purely hyperbolic element is real, such a trace will generate a real subfield of \( k \), and by the remarks above, this is a proper subfield of \( k \). We will denote by \( k_\mathbb{R} \) the maximal real subfield of \( k \). Clearly, this contains all the fields \( \mathbb{Q}(\mathrm{tr}(\gamma)) \) where \( \gamma \) is a purely hyperbolic element of \( \Gamma \).

As is well-known, and is discussed in [5] for example, for all but a finite number of \( k \)-primes \( \nu \), there are natural reduction homomorphisms

\[
\pi_\nu : \Gamma \to \mathrm{PSL}(2, \mathbb{F}_\nu).
\]

Zariski density ensures that Strong Approximation can be applied (see [8], [13] or [5] for a more elementary approach for \( \mathrm{SL}(2) \)), showing that for all but a finite number of such \( \nu \), \( \pi_\nu \) is surjective.
Applying Proposition 2.2 to the field extension $k/k_R$, we can find infinitely many rational primes $p$ such that if $\nu$ and $\omega$ denote a $k$-prime and $k_R$ prime dividing $p$, then the extension of residue class fields $F_\nu/F_\omega$ has degree at least 2. We will denote by $S$ the set of such primes of $k$ for which, in addition, Strong Approximation guarantees that $\pi_\nu$ is onto.

**Proof of Theorem 1.2:**

We will first establish the following claim.

**Claim 1:** There exists a primitive hyperbolic element in $\Gamma$ with the property that no power is purely hyperbolic.

**Proof of Claim 1:** We begin by noting that if $\gamma \in \Gamma$ is a hyperbolic element for which some power is purely hyperbolic, then $\lambda = re^{i\theta}$ and $e^{i\theta}$ is a root of unity. Given this, we have the following simple lemma.

**Lemma 3.1** Let $\Gamma$ be as above. Then there is a positive integer $N$ so that if $re^{i\theta}$ is an eigenvalue of a hyperbolic element of $\Gamma$ with $e^{i\theta}$ a root of unity, then $e^{iN\theta} = 1$.

**Proof:** By assumption, $k$ is a number field, so has finite degree, say $d$. Hence the eigenvalue $\lambda = re^{i\theta}$ has degree at most $2d$ over $Q$. Let $K = k(\lambda)$. The complex conjugate field $\overline{K}$ has the same degree, so that the smallest field containing $K$ and $\overline{K}$ has degree at most $(2d)^2$. This field contains $\lambda/\overline{\lambda} = e^{2i\theta}$.

If now $e^{i\theta}$ is a root of unity, then the above paragraph shows that it lies in a field of degree at most $2(2d)^2$ over $Q$, thus bounding the degree of the root of unity. Proposition 2.1 now shows there are only finitely many such roots of unity, and this provides the required $N$. $\square$

Thus to establish Claim 1, we need only show that there is a hyperbolic element that has not become purely hyperbolic for powers $\leq N$ (where $N$ is as in Lemma 3.1). To achieve this we argue as follows.

With $N$ as in Lemma 3.1, we fix $\nu \in S$ with $\nu/p$ and assume that $p >> N$. Proposition 2.3 shows that the orders of the elements in $PSL(2, F_\nu)$ are either $p$, or divisors of $(|F_\nu| \pm 1)/2$, and in the latter case, the maximal possible order is attained. Denote this maximal order by $R$, and let $\delta \in PSL(2, F_\nu)$ be an element of order $R$. Note that $\delta$ is not unipotent. Using Proposition 2.3, observe that $R$ is roughly at least on the order of $p$ times greater than the order of an element whose trace lies $F_\omega$. Now if $\gamma \in \Gamma$ is purely hyperbolic, then $tr(\pi_\nu(\gamma)) \in F_\omega$. In particular any element $\gamma \in \Gamma$ which maps under $\pi_\nu$ to $\delta$ cannot have had real trace before it has been raised to a power which is approximately at least $p$, else its total order would be too small. By choice of $p >> N$, this provides an element no power of which is purely hyperbolic. Given such an element $\gamma$, then a primitive element in the cyclic subgroup containing $\gamma$ finishes the proof of Claim 1. $\square$

**Remark:** This argument shows that all the elements $\gamma$ in $\pi_\nu^{-1}(\delta)$ are hyperbolic and no power is purely hyperbolic.

We now complete the proof of the existence of infinitely many, giving both an algebraic argument and a geometric one.

**Algebraic argument:** We argue as follows. Let $\alpha_1$ be a primitive hyperbolic element that is produced in the proof of Claim 1. Let $\Gamma_2 = \ker(\pi_\nu)$. Now we can choose a different prime $\nu' \in S$ (with residue class field $F_{\nu'}$) so that the reduction homomorphism

$$\pi_{\nu'} : \Gamma \rightarrow PSL(2, F_{\nu'})$$

4
restricted to \( \Gamma_2 \) is onto. Moreover, an easy argument now shows that the homomorphism

\[ \Gamma \longrightarrow \text{PSL}(2, F_{\nu}) \times \text{PSL}(2, F_{\nu'}) \]

is also onto. Choose a \( \gamma_2 \in \Gamma \) with the property that in the second coordinate it maps to an element of maximal order and in the first coordinate it maps to a unipotent element \( \xi \). Notice that \( \xi \) has order precisely \( p \) and Proposition 2.3 shows that \( < \xi > \) is a maximal cyclic subgroup of \( \text{PSL}(2, F_{\nu}) \).

Now choose the primitive element in \( \Gamma \) associated to the element \( \gamma_2 \), and denote this element by \( \alpha_2 \). As above, consideration of the image of \( \alpha_2 \) in the second factor shows that no power is pure hyperbolic. We claim that no power of \( \alpha_1 \) is conjugate to any power of \( \alpha_2 \). The reason is this. Hyperbolic elements with this property must simultaneously conjugate into a single cyclic subgroup of \( \Gamma \). Since the elements \( \alpha_1 \) and \( \alpha_2 \) are primitive in \( \Gamma \), they must both be generators of this cyclic group, and this implies that they are conjugate (up to inverting one of them) before taking powers. However, \( \alpha_2 \) has order \( p \) in the first factor and \( \alpha_1 \) has maximal order in the first factor, and in particular much larger than \( p \). Hence, these elements can never be conjugate.

The theorem is proved by repeating this argument making use of the infinitude of primes in the set \( S \) applied to a nested descending chain of kernels. \( \square \)

**Geometric argument:** We begin by fixing some notation needed in the proof. For a Kleinian group \( \Gamma \), \( \Lambda_F \) will denote the limit set of \( \Gamma \), and \( C(\Lambda_F) \) the convex hull of the limit set.

As in the previous setting, we fix one primitive element provided by the proof of Claim 1, \( \alpha = \alpha_1 \) say, so that \( \pi_\nu^{-1}(\delta) = \alpha \ker(\pi_\nu) \).

Now by construction, everything in this coset maps to an element of order \( R \), and therefore all the primitive elements associated to such elements map to elements of maximal order too. Hence, as remarked above, they are all hyperbolic elements with no power being purely hyperbolic. To construct infinitely many non-conjugate primitive elements in this case we argue as follows. We will use \( \ell \) to denote the hyperbolic length in the hyperbolic 3-manifold \( M = \mathbb{H}^3/\Gamma \).

Fix a number \( K > 10\ell(g_0) \) say, and let \( g \subset M \) be a closed geodesic with length \( \ell(g) > K \). Now choose a point \( p \) on \( g \) and some small compact ball \( B_1 \subset M = \mathbb{H}^3/\Gamma \) centered at \( p \) which is disjoint from all the primitive closed geodesics in \( M \) which have length at most \( K \). Fix some lift of \( B_1 \) (still denoted \( B_1 \)) and a lift of \( g \) (still denoted \( g \)) in \( \mathbb{H}^3 \) which passes through \( B_1 \). We next choose very small open neighbourhoods \( N_+, N_- \) of the endpoints of \( g \), so that any geodesic in \( C(\Lambda_F) \) with one endpoint in \( N_+ \) and one endpoint in \( N_- \) must run through \( B_1 \).

Now \( \ker(\pi_\nu) \) is normal in \( \Gamma \), and so has the same limit set as \( \Gamma \). Since the limit set is perfect, there exists an element \( \beta \in \ker(\pi_\nu) \) with one fixed point in \( N_+ \) and one in \( N_- \), and so by standard arguments, for \( k \) sufficiently large, the element \( \beta^k \alpha_1 \beta^k \) also has fixed points in those neighbourhoods. Let \( \alpha_2 \) be the primitive hyperbolic element in the cyclic group containing \( \beta^k \alpha_1 \beta^k \). By construction, \( g_{\alpha_2} \) runs through the ball \( B_1 \) in \( M \), so that by choice of \( B_1 \) it has length \( > K > 10\ell(\alpha) \) and in particular, \( \alpha_2 \) is not conjugate to \( \alpha \). However \( \alpha_2 \) is conjugate to \( \alpha \beta^k \) which lies in \( \pi^{-1}(\delta) \), so that it has no power which is purely hyperbolic.

Now repeat this argument by choosing a small ball \( B_2 \) missing all geodesics of length at most \( K_2 > 10\ell(\alpha_2) \). It is clear that repeating this construction provides infinitely many distinct primitive elements (up to conjugacy). \( \square \)

# 4 Comments on the case of arithmetic Kleinian groups

## 4.1

We begin by discussing the proof of Theorem 1.1 for arithmetic hyperbolic 3-manifolds that is implicit in [2]. It is convenient to work with arithmetic Kleinian groups derived from a quaternion
algebra (i.e., those for which the invariant trace-field coincides with the trace-field). We refer the reader to [2] and [7] for more details. In the notation of §3, if \( k \) denotes the trace-field and \( k_R \) the maximal real subfield, then the analysis in [2] breaks into two cases: either \( |k : k_R| > 2 \) or \( |k : k_R| = 2 \).

The former case is straightforward to handle, since there are no purely hyperbolic elements in this case (see [7] Theorem 5.3.1).

The latter case is handled using Lemmas 4.3 and 5.2 of [2]. Briefly, Lemma 5.2 of [2] provides infinitely many hyperbolic elements for which the eigenvalue \( \lambda \) generates a field \( \mathbb{Q}(\lambda) \) which is distinct from \( \mathbb{Q}(\overline{\lambda}) \). However, if \( \lambda \) is the eigenvalue of a hyperbolic element for which some power is purely hyperbolic, it can be shown that \( \mathbb{Q}(\lambda) = \mathbb{Q}(\overline{\lambda}) \), and hence a contradiction.

4.2

More is implicit in [2] as we now discuss, and that we are unable to establish in general.

If \( \lambda = r e^{i\theta} \) is the eigenvalue for a hyperbolic element for which no power is purely hyperbolic, then \( e^{i\theta} \) is an algebraic number that is not a root of unity. A stronger version of Question 1 to ask is:

**Question 2:** For those eigenvalues associated to hyperbolic elements no power of which is purely hyperbolic, is the collection of fields \( \mathbb{Q}(e^{i\theta}) \) infinite?

**Claim 2:** Question 2 has an affirmative answer in the arithmetic case.

**Proof:** As in §4.1, is convenient to work with arithmetic Kleinian groups derived from a quaternion algebra. Suppose that there are only finitely many such fields. Then there are only finitely many fields \( \mathbb{Q}(e^{2i\theta}) = \mathbb{Q}(\lambda/\overline{\lambda}) \). Now it is shown in [2] (see Lemma 5.2 and Proposition 4.4), that we can find infinitely many hyperbolic elements (no power of which is purely hyperbolic) such that the Galois Closure \( \mathbb{Q}(\lambda)^{\text{cl}} \) of \( \mathbb{Q}(\lambda) \) over \( \mathbb{Q} \) coincides with \( \mathbb{Q}(\lambda/\overline{\lambda})^{\text{cl}} \) (the Galois closure of \( \mathbb{Q}(\lambda/\overline{\lambda}) \) over \( \mathbb{Q} \)). Now for these \( \lambda \), it can be shown that \( \mathbb{Q}(\lambda/\overline{\lambda})^{\text{cl}} = \mathbb{Q}(\lambda/\overline{\lambda})^{\text{cl}} \) (the Galois closure of \( \mathbb{Q}(\lambda/\overline{\lambda}) \) over \( \mathbb{Q} \)). Hence \( \mathbb{Q}(\lambda)^{\text{cl}} = \mathbb{Q}(\lambda/\overline{\lambda})^{\text{cl}} \).

Consequently, if there are only finitely many fields \( \mathbb{Q}(\lambda/\overline{\lambda}) \), there are only finitely many fields arising as \( \mathbb{Q}(\lambda)^{\text{cl}} \), and this implies that there are in fact only finitely many possibilities for \( \lambda \), which is a contradiction. \( \square \)

5 The higher dimensional setting

Throughout this section, we shall always assume that \( n \geq 4 \). We begin with some preliminary discussion.

5.1

A hyperbolic element \( \gamma \in \text{SO}_0(n,1) \) is conjugate in \( \text{SO}_0(n,1) \) to an element of the form

\[
\begin{pmatrix}
\alpha & 0 \\
0 & T
\end{pmatrix},
\]

where \( \alpha \) has real eigenvalues \( \lambda \) and \( 1/\lambda \) with \( |\lambda| > 1 \), and \( T \in O(n-1) \). In this case, a hyperbolic element is called purely hyperbolic if \( T = 1 \). If \( \gamma \) is a hyperbolic element that powers to be purely hyperbolic, then \( T \) must have finite order.
Let $M = \mathbb{H}^n / \Gamma$ be orientable and finite volume. As is well-known (see [9]), $\Gamma$ can be conjugated in $O_0(n, 1)$ to have entries in a (real) number field. Furthermore, Vinberg [12] showed that there is a minimal field of definition for this number field. We will denote this by $k$ in what follows. Using this number field, an argument similar to that used in Lemma 3.1 proves the following lemma.

**Lemma 5.1** Let $\Gamma$ be as above. Then there is a positive integer $N$ such that if $\gamma \in \Gamma$ powers to be purely hyperbolic, then $T_{\gamma}^N = 1$.

**Remark:** As is well-known there are infinitely rational primes that split completely in $k$ (see [4]). We will denote by $\mathcal{V}$ be the collection of such primes. As in the case of dimension 3, for convenience, we will exclude any prime from $\mathcal{V}$ for which the residue class field has characteristic 2.

### 5.2

We will use some facts about the simple groups of orthogonal type (see [11] or [1] for more details).

Let $f$ be an $m$-dimensional quadratic form over the finite field $F$ of cardinality $q$, where to simplify some of the discussion we assume $q$ is an odd prime. In the case when $m$ is also odd, there is a unique orthogonal group $O(m, q)$ up to isomorphism, and when $m$ is even there are two $O_\pm(m, q)$ (see [11] p 377 Theorem 5.8). Let $SO(m, q)$ and $SO_\pm(m, q)$ denote the special orthogonal groups in these cases, and let $\Omega(m, q) = [O(m, q), O(m, q)]$ when $m$ is odd (resp. $\Omega_\pm(m, q) = [O_\pm(m, q), O_\pm(m, q)]$ when $m$ is even) where $[G, G]$ denotes the commutator subgroup of a group $G$. When $m$ is even $\Omega_\pm(m, q)$ has index 2 in $SO_\pm(m, q)$ and has a center of order 1 or 2. Let $P\Omega_\pm(m, q)$ be the central quotient group.

We summarize the important facts for us in the following theorem (see [11] loc. cit. or [1] pp. 6-7 for a discussion):

**Theorem 5.2**

1. $\Omega(2m+1, q)$ is a simple subgroup of $O(2m+1, q)$ of index 4 and has order $\frac{1}{2} q^{m^2} \prod_{i=1}^{m} (q^{2i} - 1)$.

2. $\Omega(2m, q)$ is a subgroup of $O(2m, q)$ of index 4 and the central quotient groups $P\Omega_\pm(2m, q)$ are simple groups whenever $m \geq 3$. These groups have orders

$$\frac{1}{d} q^{m(m-1)} (q^m - 1) \prod_{i=1}^{m-1} (q^{2i} - 1), \text{ where } d = (4, q^m - 1), \text{ (in the case of +)}$$

and

$$\frac{1}{d} q^{m(m-1)} (q^m + 1) \prod_{i=1}^{m-1} (q^{2i} - 1), \text{ where } d = (4, q^m + 1), \text{ (in the case of -)}.$$

**Remark:** The cases of $\pm$ are distinguished by the discriminant of the quadratic form. When the discriminant is a square in $F_q$, we are in the case of $+$, and the non-square case corresponds to $-$. As in §3 (using the minimal field of definition $k$), we will consider reduction homomorphisms

$$\pi_\nu : \Gamma \to SO(n, 1; q),$$

for $\nu \in \mathcal{V}$.

Strong Approximation in this case gives ([8], [13] or [6] for a discussion of the proof of the version stated below):
**Theorem 5.3** In the notation above, for all but a finite number of primes \( \nu \in \mathcal{V} \), we have

1. \( \Omega(n + 1, q) \leq \pi_\nu(\Gamma) \leq \text{SO}(n + 1; q) \), when \( n + 1 \) is odd.

2. \( P\Omega_{\pm}(n + 1, q) \leq P\pi_\nu(\Gamma) \leq P\text{SO}_{\pm}(n + 1; q) \), when \( n + 1 \) is even (where the notation indicates that only the correct sign is chosen in the subscript).

It is necessary for us to sharpen this discussion a little so as to better suit our needs. In particular we will pass to an infinite subset of primes \( \mathcal{V}_0 \subset \mathcal{V} \) that have some additional constraints. (Actually we need only that \( \mathcal{V}_0 \) is nonempty.) Firstly, Lemma 5.1 provides an integer \( N \) such that if \( \beta \in \Gamma \) is a hyperbolic element that has some power that is purely hyperbolic, then \( T^N_{\beta} = 1 \). Thus the eigenvalues of \( T_{\beta} \) are \( N \)-th roots of unity. Secondly, in the case when \( (n + 1) \) is even, we wish to restrict to those primes so as to ensure that \(-1\) is a square in \( \mathbb{F}_q \), and so the form of signature \((n, 1)\) determines a form over \( \mathbb{F}_q \) whose discriminant is a square (recall the Remark after Theorem 5.2).

Given the remarks of the previous paragraph, henceforth, we will restrict attention to those reduction homomorphisms arising from the (infinite) subset of primes \( \mathcal{V}_0 \subset \mathcal{V} \) that divide rational primes that split completely in the field \( K \) obtained by adjoining to \( k \) the \( N \)-th roots of unity together with a square root of \(-1\). That \( \mathcal{V}_0 \) is still infinite is a well-known consequence of Cebatorev Density theorem. In particular, we have arranged that when \( n + 1 \) is even, we are in the case of + in Theorems 5.2 and 5.3.

We prove the following rather general lemma:

**Lemma 5.4** Suppose in the notation established above, that \( T_{\beta} \) is the rotational part of some element of \( \Gamma \) which has finite order \( r_{\beta} \) (in particular, this order divides \( N \)).

Then for any \( \nu \in \mathcal{V}_0 \) lying over a rational prime \( q \), \( r_{\beta} \) divides \( |O(n - 1; q)| \).

**Proof:** Note that it suffices to construct any element of order \( r_{\beta} \) in \( O(n - 1; q) \).

Since by construction \( K \) contains all the relevant \( N \)-th roots of unity, it contains \( c = \cos(2\pi/r_{\beta}) \) and \( s = \sin(2\pi/r_{\beta}) \). Note that \( c, s \in K \) differ from an algebraic integer only at primes dividing 2. Then consider the element

\[
\begin{pmatrix}
c & s & 0 \\
-s & c & 0 \\
0 & 0 & 1
\end{pmatrix} \in O(n - 1; K),
\]

where the orthogonal group is that of the standard positive definite quadratic form over \( \mathbb{R} \) of signature \((n - 1, 0)\) with coefficients in \( K \). Observe that for the primes \( q \) under consideration, the appropriate reduction homomorphism carries this element into \( O(n - 1; q) \).

The proof of the lemma is completed with the observation that the image of this element has order \( r_{\beta} \) in \( O(n - 1; q) \). The reason for this is the following. A theorem of Minkowski implies that (typically) the kernels of these reduction homomorphisms are torsion-free. The exceptions arise only for \( \ell \)-torsion where \( \ell \) is the characteristic of the residue class field involved (see Lemma 2.4 of [6] for example). Since a rational prime \( t|N \) will be ramified in \( \mathbb{Q}(\zeta_N) \), and we consider only those primes splitting completely in \( K \), such primes cannot give rise to any of these exceptions. \( \square \)

**5.3 Proof of Theorem 1.3.**

We need one more ingredient before embarking on the proof of Theorem 1.3. As in the proof of Theorem 1.2, we need control on the orders of certain elements in the finite simple groups given in Theorem 5.2. To that end, for convenience we recall Zsigmondy’s Theorem [14] (see also [10] for a short proof of this and some related results).
Theorem 5.5 Let \( a \) and \( n \) be integers greater than 1. Exclude the cases
(1) \( a = 2^r - 1, \ r \geq 2 \) and \( n = 2 \); and (2) \( a = 2 \) and \( n = 6 \).

Then there exists a prime \( s \) such that \( s \mid (a^n - 1) \), but for each \( j < n \), \( s \) does not divide \( a^j - 1 \).

A prime divisor as in the conclusion of Theorem 5.5 is called a primitive prime divisor (or sometimes a Zsigmondy prime).

We now complete the proof of Theorem 1.3 by arguing as follows. Since the property of being a hyperbolic element having no power that is purely hyperbolic is preserved by passage to subgroups of finite index, we will assume that the reduction homomorphisms \( \pi_\nu \) surject \( \Gamma \) onto the finite simple groups as given in Theorem 5.3. Since \( n \geq 4 \) is fixed, for convenience of notation, we will simply denote any of these finite simple groups by \( \Omega_q \).

Fix some such prime \( \nu \in \mathcal{V}_0 \) lying over the rational prime \( q \), and let \( p \) be a primitive prime divisor of \( q^{2m} - 1 \) (when \( n = 2m \), ie \( n + 1 \) is odd) or a primitive prime divisor of \( q^{2(m-1)} - 1 \) (when \( n = 2m - 1 \), ie \( n + 1 \) is even). Note that since we are always assuming \( n \geq 4 \), and \( q \) is odd we can apply Theorem 5.5. By Cauchy’s theorem, there is an element \( \delta \in \Omega_q \) of order \( p \). Pick some \( \gamma \in \Gamma \), with \( \pi_\nu(\gamma) = \delta \). Then the proof is completed by the following claim.

Claim 3: No power of \( \gamma \) is purely hyperbolic.

Proof of Claim 3: To begin with, suppose that \( \beta \in \Gamma \) is a hyperbolic element for which some power is purely hyperbolic. Then applying Lemma 5.4, we see that if we raise \( \beta \) to the power \( |\text{O}(n-1; q)| \), it becomes purely hyperbolic. Now since such any pure hyperbolic element is conjugate in \( \text{SO}_q(n, 1) \) to an element with rotational part being the identity, it follows that the image under the reduction homomorphism \( \pi_\nu \) is an element whose order divides \( q(q^2 - 1)/2 \) (recall Proposition 2.3). Putting these two observations together we see that the image of the given \( \beta \) under \( \pi_\nu \) is an element whose order divides \( q(q^2 - 1)/\text{O}(n-1; q)/2 \).

We next claim that \( p \) does not divide \( \text{O}(n-1; q) \). The reason is this: the order of \( \text{O}(n-1; q) \) differs from the order of the corresponding finite simple group of that orthogonal type by a factor of most 4 (cf. Theorems 5.2 and 5.3). As remarked above, we have arranged that when \( n \) is odd (by choice of \( q \)) that the finite simple group which arises is of + type. Now when one computes the order from Theorem 5.2, one finds that the property that \( p \) is a primitive prime divisor ensures it cannot divide the order of \( \text{O}(n-1; q) \).

Finally, recall that we chose \( \gamma \in \Gamma \) so that \( \pi_\nu(\gamma) = \delta \), an element of order \( p \). We claim that no power of \( \gamma \) is purely hyperbolic. The argument is that the above discussion shows that if it were, its order would divide \( q(q^2 - 1)/\text{O}(n-1; q)/2 \). However note that \( p \) being a primitive prime divisor and the exponent of \( q \) being at least 4, means that \( p \) does not divide \( q^2 - 1 \) and we have already argued that \( p \) does not divide \( |\text{O}(n-1; q)| \). This contradiction finishes the proof of Claim 3.

The proof of Theorem 1.3 is completed using the geometric argument provided in §3. Briefly, notice that the argument to produce one element given above, shows that any element \( \gamma \) in \( \pi_\nu^{-1}(\delta) \) is hyperbolic and no power is purely hyperbolic. The argument now proceeds as before. \( \square \)

Remarks:(1) Notice that, for \( n = 3 \), the proof of Theorem 1.3 (conjecturally at least) does not apply. The reason is that, in this case, we have (in the notation above) \( m = 2 \), so the exponent is 2. Now the excluded values in Theorem 5.5(1) would be primes \( q \) of the form \( 2^r - 1 \); i.e. Mersenne primes. It is still an open problem as to whether there are infinitely many Mersenne primes.

(2) There is also a version of Theorem 1.2 in the higher dimensional setting. Namely, the methods
of §5 and the geometric proof show:

**Theorem 5.6** Let $\Gamma$ be a finitely generated Zariski dense subgroup of $\text{SO}_0(n,1)$ which is contained in $\text{SO}_0(n,1;k)$ for some (real) number field $k$. Then $\Gamma$ contains infinitely many primitive hyperbolic elements with the property that they have no power which is purely hyperbolic.

**References**


Department of Mathematics, University of California Santa Barbara, CA 93106, USA. Email: long@math.ucsb.edu

Department of Mathematics, University of Texas Austin, TX 78712, USA. Email: areid@math.utexas.edu