Also available at http://amc-journal.eu
ISSN 1855-3966 (printed edn.), ISSN 1855-3974 (electronic edn.)
ARS MATHEMATICA CONTEMPORANEA 14 (2018) 165–176

The size of algebraic integers with many real conjugates

Artūras Dubickas

Department of Mathematics and Informatics, Vilnius University, Naugarduko 24, LT-03225 Vilnius, Lithuania

Received 20 March 2017, accepted 18 April 2017, published online 10 August 2017

Abstract

In this paper we show that the relative normalised size with respect to a number field $\mathbb{K}$ of an algebraic integer $\alpha \neq -1, 0, 1$ is greater than 1 provided that the number of real embeddings s of $\mathbb{K}$ satisfies $s \geq 0.828n$, where $n = [\mathbb{K} : \mathbb{Q}]$. This can be compared with the previous much more restrictive estimate $s \geq n - 0.192\sqrt{n/\log n}$ and shows that the minimum $m(\mathbb{K})$ over the relative normalised size of nonzero algebraic integers α in such a field $\mathbb{K}$ is equal to 1 which is attained at $\alpha = \pm 1$. Stronger than previous but apparently not optimal bound for $m(\mathbb{K})$ is also obtained for the fields $\mathbb{K}$ satisfying $0.639 \leq s/n < 0.827469\ldots$. In the proof we use a lower bound for the Mahler measure of an algebraic number with many real conjugates.

Keywords: Algebraic number field, relative size, relative normalised size, Mahler measure, Schur–Siegel–Smyth trace problem.

Math. Subj. Class.: 11R04, 11R06

1 Introduction

Let $\mathbb{K}$ be a number field with signature $(s(\mathbb{K}), t(\mathbb{K})) = (s, t)$ having s real embeddings $\sigma_i : \mathbb{K} \to \mathbb{R}$, $i = 1, \ldots, s$, and t conjugate pairs of complex embeddings $\sigma_{i+j}, \overline{\sigma_{i+j}} : \mathbb{K} \to \mathbb{C}$, $j = 1, \ldots, t$. Clearly,

$$n = n(\mathbb{K}) := [\mathbb{K} : \mathbb{Q}] = s + 2t.$$

For any $\alpha \in \mathbb{K}$ we define

$$\|\alpha\|_{\mathbb{K}} := \Big(\sum_{i=1}^{s} \sigma_i(\alpha)^2 + \sum_{j=1}^{t} |\sigma_{s+j}(\alpha)|^2 \Big)^{1/2}, \tag{1.1}$$

E-mail address: arturas.dubickas@mif.vu.lt (Artūras Dubickas) and

$$m_{\mathbb{K}}(\alpha) := \frac{\|\alpha\|_{\mathbb{K}}^2}{s+t}. \tag{1.2}$$

Also, put

$$m(\mathbb{K}) := \min_{\alpha \in \mathcal{O}_{\mathbb{K}} \setminus \{0\}} m_{\mathbb{K}}(\alpha), \tag{1.3}$$

where $\mathcal{O}_{\mathbb{K}}$ is the ring of integers of $\mathbb{K}$.

For any number field $\mathbb{K}$ we have $\pm 1 \in \mathcal{O}_{\mathbb{K}}$ and $\|\pm 1\|_{\mathbb{K}} = s(\mathbb{K}) + t(\mathbb{K})$, so that $m_{\mathbb{K}}(\pm 1) = 1$ (see (1.1) and (1.2)). By (1.3), this yields $m(\mathbb{K}) \le 1$. The lower bound

$$m(\mathbb{K}) \ge \frac{1}{1+s/n},$$

where $n = [\mathbb{K} : \mathbb{Q}]$ and $s = s(\mathbb{K})$, follows from [19, Lemma 1.1(ii)]. The stronger bound

$$m(\mathbb{K}) \ge \frac{2^{s/n}}{1+s/n} \tag{1.4}$$

is given in [16, Theorem 5.11]. In particular, the inequality (1.4) implies $m(\mathbb{K}) = 1$ if $\mathbb{K}$ is a totally complex field ($s(\mathbb{K}) = 0$) or a totally real field ($t(\mathbb{K}) = 0$).

A motivation for introducing and studying the quantities $\|\alpha\|_{\mathbb{K}}$, $m_{\mathbb{K}}(\alpha)$ and $m(\mathbb{K})$ is given in [7]; see also a subsequent paper [6]. There, we call $\|\alpha\|_{\mathbb{K}}$ the *relative size* of α with respect to the number field $\mathbb{K}$ and $\sqrt{m_{\mathbb{K}}(\alpha)}$ the *relative normalised size* of α (with respect to $\mathbb{K}$ again). Briefly speaking, it is related to some earlier work on certain lattices defined by number fields, when in the ring of integers $\mathcal{O}_{\mathbb{K}}$ of a number field $\mathbb{K}$ with signature (s,t), one considers the vectors

$$(\sigma_1(\alpha), \dots, \sigma_s(\alpha), \Re(\sigma_{s+1}(\alpha)), \Im(\sigma_{s+1}(\alpha)), \dots, \Re(\sigma_{s+t}(\alpha)), \Im(\sigma_{s+t}(\alpha)))$$

in $\mathbb{R}^n$ defined for $\alpha \in \mathcal{O}_{\mathbb{K}}$ (see [2, Chapter 8, Section 7]). This can be applied to show that the class number of a number field is finite [11]. The norm defined in (1.1) has been considered by Pethő and Schmitt [13]; see also a subsequent paper [5]. A different but at the same time quite similar to (1.1) norm related to certain number field codes has been also considered in [9]; see also [3].

Since the minimum of the function $h(x) := 2^x/(1+x)$ in the interval $x \in [0,1]$ is attained at $x_0 := 1/\log 2 - 1 \notin \mathbb{Q}$ and equals $h(x_0) = (e \log 2)/2$, the inequality

$$\frac{2^{s/n}}{1+s/n} > \frac{e \log 2}{2} = 0.942084\dots$$

holds for any integers $s \le n$, where $s \ge 0$ and $n \ge 1$. Hence, by (1.4),

$$\frac{e \log 2}{2} < m(\mathbb{K}) \le 1.$$

In particular, for any number field $\mathbb{K}$ we have either $m(\mathbb{K}) = 1$ or $m(\mathbb{K}) < 1$.

A large class of fields for which $m(\mathbb{K}) = 1$ was described in [7, Theorem 3.3], where we showed that for a number field $\mathbb{K}$ with signature (s,t) we have $m(\mathbb{K}) = 1$ if

$$t \le 0.096\sqrt{s/\log s}. \tag{1.5}$$

The following theorem relaxes the bound (1.5) on t to the bound $t \le 0.086n$ with the same conclusion and so strengthens the above result considerably. (Note that in view of $n = s + 2t$ the bound (1.5) is essentially equivalent to $t \le 0.096\sqrt{n/\log n}$.)

Theorem 1.1. *For each number field $\mathbb{K}$ of degree n and signature (s,t) satisfying $t \le 0.086n$ we have $m(\mathbb{K}) = 1$.*

Observe that $t \le 0.1038s$ implies $t \le 0.086n$ which is also equivalent to $s \ge 0.828n$. On the other hand, by [7, Theorem 3.5], for each integer $s \ge 2$ there exist infinitely many number fields $\mathbb{K}$ with signature (s,s) (so that $t = s = n/3$) for which $m(\mathbb{K}) < 1$. This shows that Theorem 1.1 is best possible up to the constant. Moreover, the constant 0.086 cannot be replaced by the constant $1/3$.

Below, the bound (1.4) will also be improved for fields $\mathbb{K}$ of degree n with signature (s,t) satisfying $0.639 \le s/n < 0.828$ (see Corollary 2.4 in Section 2). Here, the constants 0.639 and 0.828 are just three decimal digit approximations from above of some presumably transcendental constants (see Proposition 2.1 below for the definition of $\lambda_0 = 0.827469\dots$).

In the next section we state Theorem 2.2 which is the main result of this paper. Section 3 contains some auxiliary results. The proofs of Proposition 2.1, Theorem 2.2 and Theorem 2.5 will be given in Sections 4, 5 and 6, respectively.

2 Main results

Throughout, we shall use the following notation for fixed $\lambda > 0$:

$$g(\lambda) := \left(2^{-1/\lambda} + \sqrt{1 + 2^{-2/\lambda}}\right)^{\lambda}, \tag{2.1}$$

$$F(\lambda, x) := xg(\lambda)^{1/x} + 2(1-x)g(\lambda)^{-1/(1-x)} - 2 + x, \tag{2.2}$$

where $0 < x \le 1$ and, by definition, $F(\lambda, 1) = g(\lambda) - 1$. Finally, the function $\varphi(\lambda)$ is defined for positive λ as follows

$$\varphi(\lambda) := \min_{0<x\le 1} F(\lambda, x). \tag{2.3}$$

Here, the minimum in (2.3) is attained, since $F(\lambda, x) \to +\infty$ as $x \to 0+$ in view of $g(\lambda) > 1$.

With this notation, we will show that

Proposition 2.1. *The function $\varphi(\lambda)$ is increasing for $\lambda \ge 0.581$ and positive for $\lambda > \lambda_0 := 0.827469\dots$. Here, $\varphi(\lambda_0) = 0$, $\varphi(0.828) = 0.000389\dots$ and $\varphi(1) = 0.176732\dots$.*

More values of the function $\varphi(\lambda)$ are given in Table 1. Here, for each $\lambda \in [0.83, 1]$ the constant $x_0(\lambda)$ is the point of absolute minimum of $F(\lambda, x)$ in the interval $0 < x \le 1$, so that $\varphi(\lambda) = F(\lambda, x_0(\lambda))$.

Now, we can state the main result of this paper.

Theorem 2.2. *Let $\mathbb{K}$ be a number field with signature $(s(\mathbb{K}), t(\mathbb{K}))$ and degree $n = s(\mathbb{K}) + 2t(\mathbb{K})$ over $\mathbb{Q}$ satisfying $s(\mathbb{K}) \ge 0.581n$, and let $\alpha \ne -1, 0, 1$ be an algebraic integer in $\mathbb{K}$. Then,*

$$m_{\mathbb{K}}(\alpha) \ge 1 + \frac{\varphi(\lambda)}{1+\lambda}, \tag{2.4}$$

where $\lambda := s(\mathbb{K})/n$ and the function $\varphi(\lambda)$ is defined in (2.1)-(2.3). In particular, the inequality $\varphi(\lambda) > 0$ holds for each $\lambda \in (\lambda_0, 1]$, that is, for $s(\mathbb{K}) > \lambda_0 n$, where $\lambda_0 = 0.827469\dots$.

λ	$g(\lambda)$	$x_0(\lambda)$	$\varphi(\lambda)$	$\frac{\varphi(\lambda)}{1+\lambda}$
0.83	1.418557	0.529769	0.001865	0.001019
0.84	1.429308	0.532299	0.009447	0.005134
0.85	1.440180	0.534841	0.017362	0.009385
0.88	1.473522	0.542547	0.043126	0.022939
0.90	1.496362	0.547749	0.061991	0.032627
0.93	1.531545	0.555648	0.092837	0.048102
0.95	1.555624	0.560980	0.115104	0.059027
0.98	1.592687	0.569077	0.151060	0.076292
0.99	1.605296	0.571802	0.163726	0.082274
1.00	1.618033	0.574542	0.176732	0.088366

Table 1: Values of $\varphi(\lambda)$ in the range $0.83 \le \lambda \le 1$

In fact, the inequalities (5.7) and (5.8) which will be proved in Section 5 can be stronger than (2.4) under some additional assumptions.

In particular, selecting (in Theorem 2.2) $\mathbb{K} := \mathbb{Q}(\alpha)$, we obtain the following:

Corollary 2.3. *Let $\alpha \neq -1, 0, 1$ be an algebraic integer of degree $d = s + 2t$ with s real conjugates α_i, $i = 1, \dots, s$, and t pairs of complex conjugates $\alpha_{s+j}, \overline{\alpha_{s+j}}$, $j = 1, \dots, t$. Then, for $\lambda = s/d > \lambda_0$ we have*

$$m_{\mathbb{Q}(\alpha)}(\alpha) = \frac{|\alpha_1|^2 + \cdots + |\alpha_{s+t}|^2}{s+t} \ge 1 + \frac{\varphi(\lambda)}{1+\lambda},$$

where $\varphi(\lambda) > 0$ is defined in (2.1)-(2.3).

By (1.3), Theorem 2.2 immediately implies Theorem 1.1 stated in Section 1. In the range $0.581 \le \lambda = s/n \le \lambda_0$ Theorem 2.2 implies the following:

Corollary 2.4. *For a number field $\mathbb{K}$ of degree n and signature (s, t) satisfying $0.581 \le \lambda = s/n \le \lambda_0$ we have*

$$m(\mathbb{K}) \ge 1 + \frac{\varphi(\lambda)}{1+\lambda}.$$

Note that for each λ satisfying $0.639 \le \lambda \le \lambda_0$ the inequality of Corollary 2.4 strengthens the bound (1.4). In particular, for $\lambda = 0.639$ we have

$$m(\mathbb{K}) \ge 1 + \frac{\varphi(\lambda)}{1+\lambda} = 0.950175\dots,$$

whereas the bound (1.4) yields the weaker inequality

$$m(\mathbb{K}) \ge \frac{2^\lambda}{1+\lambda} = 0.950121\dots.$$

For further comparison of the functions $1 + \varphi(\lambda)/(1+\lambda)$ and $2^\lambda/(1+\lambda)$ see Table 2.

If the number of complex conjugates $2t$ of an algebraic integer is very small compared to its degree d (which is large) then the constant 1.088366 corresponding to the case $\lambda = 1$

λ	$g(\lambda)$	$\frac{2^\lambda}{1+\lambda}$	$1+\frac{\varphi(\lambda)}{1+\lambda}$
0.64	1.237064	0.950200	0.950299
0.65	1.245534	0.951011	0.951621
0.70	1.289701	0.955591	0.960509
0.75	1.336871	0.961024	0.973167
0.80	1.387027	0.967278	0.989505
0.82	1.407927	0.970003	0.997042

Table 2: Values of $1+\frac{\varphi(\lambda)}{1+\lambda}$ vs $\frac{2^\lambda}{1+\lambda}$ for $0.64 \le \lambda \le 0.82$

in Corollary 2.3 (see Table 1) can be improved, by using the results on the so-called Schur–Siegel–Smyth trace problem. The problem is named after the authors of the first three estimates of the trace of a totally positive algebraic integer [15], [17], [18]. The method of auxiliary functions introduced by Smyth in [18] was used in all subsequent papers on this subject. Specifically, we shall use the result of Liang and Wu [12] (see Lemma 3.5 below). See also some recent related papers [4] and [14].

Theorem 2.5. *There exist two absolute positive constants D and δ such that if $d \ge D$ and $t < \delta d/\log d$ then for each algebraic integer α of degree $d = s+2t$ with s real conjugates α_i, $i = 1,\dots,s$, and t pairs of complex conjugates $\alpha_{s+j}, \overline{\alpha_{s+j}}$, $j = 1,\dots,t$, the inequality*

$$m_{\mathbb{Q}(\alpha)}(\alpha) = \frac{|\alpha_1|^2+\dots+|\alpha_{s+t}|^2}{s+t} > 1.79192 \tag{2.5}$$

holds.

For large d Theorem 2.5 not only gives a better bound, but also the condition $t < \delta d/\log d$ is less restrictive than the corresponding condition $t \le 0.096\sqrt{d/\log d}$ of [7, Theorem 3.3].

3 Auxiliary results

Lemma 3.1. *Let $\alpha \ne -1,0,1$ be an algebraic number of degree d over $\mathbb{Q}$ with signature (s,t), where $\lambda = s/d > 0$. Then,*

$$M(\alpha) \ge \left(2^{-1/\lambda}+\sqrt{1+2^{-2/\lambda}}\right)^{s/2}. \tag{3.1}$$

In particular, for $s \ge 0.581d$ we have

$$M(\alpha) > 1.090691^d. \tag{3.2}$$

Proof. The inequality (3.1) was proved by Garza (it is the main result in [8]). In [10], Höhn gave an alternative proof of this result.

By (2.1), (3.1), and $s = \lambda d$, we deduce that

$$M(\alpha) \ge \left(2^{-1/\lambda}+\sqrt{1+2^{-2/\lambda}}\right)^{\lambda d/2} = g(\lambda)^{d/2}. \tag{3.3}$$

Evidently, the function $g(\lambda)$ is increasing in $\lambda > 0$, so its smallest value in the interval $[0.581, 1]$ is attained at $\lambda = 0.581$. Thus, (3.3) implies (3.2) in view of $g(0.581)^{1/2} = 1.090691\dots$. □

We will also need the following inequality.

Lemma 3.2. *For any number fields $\mathbb{L} \subseteq \mathbb{K}$ with signatures $(s(\mathbb{L}), t(\mathbb{L}))$ and $(s(\mathbb{K}), t(\mathbb{K}))$, respectively, we have $s(\mathbb{K})t(\mathbb{L}) \leq s(\mathbb{L})t(\mathbb{K})$.*

Proof. By the primitive element theorem, write $\mathbb{L} = \mathbb{Q}(\alpha)$ and $\mathbb{K} = \mathbb{Q}(\beta)$. Then, $\alpha = P(\beta)$ with some $P \in \mathbb{Q}[x]$. Without restriction of generality we may assume that $\beta_1, \dots, \beta_s$ are the real conjugates of β and $\beta_{s+1}, \overline{\beta_{s+1}}, \dots, \beta_{s+t}, \overline{\beta_{s+t}}$ are the complex conjugates of β. Here, $s = s(\mathbb{K})$ and $t = t(\mathbb{K})$. Note that in the list $\sigma(P(\beta))$, where σ runs through all $s + 2t$ automorphisms of the field $\mathbb{K}$, each conjugate of α appears $[\mathbb{K} : \mathbb{L}]$ times. In particular, each of the numbers $P(\beta_i)$, where $1 \leq i \leq s$, is real, so the number of real conjugates of α is at least $s/[\mathbb{K} : \mathbb{L}]$. This yields

$$s(\mathbb{L}) \geq \frac{s}{[\mathbb{K} : \mathbb{L}]} = \frac{s[\mathbb{L} : \mathbb{Q}]}{[\mathbb{K} : \mathbb{L}][\mathbb{L} : \mathbb{Q}]} = \frac{s[\mathbb{L} : \mathbb{Q}]}{[\mathbb{K} : \mathbb{Q}]} = \frac{s(s(\mathbb{L}) + 2t(\mathbb{L}))}{s + 2t}.$$

Multiplying both sides by $s + 2t$ we obtain the required inequality. □

Lemma 3.3. *Let $k \leq d$ be two positive integers and let $S \geq 1$, ρ and $y_1 \geq \dots \geq y_k \geq 1 \geq y_{k+1} \geq \dots \geq y_d$ be real numbers such that*

$$y_1 + \dots + y_k + S(y_{k+1} + \dots + y_d) \geq S(d - k) + k + \rho.$$

Then, for any positive numbers $w_1, \dots, w_d$ satisfying

$$\max_{1 \leq i \leq d} w_i \leq S \min_{1 \leq i \leq d} w_i$$

and $w_1 + \dots + w_d = 1$ we have

$$w_1 y_1 + \dots + w_d y_d \geq 1 + \rho \min_{1 \leq i \leq d} w_i.$$

Proof. Put $z_i := y_i - 1$ for each $i = 1, \dots, d$. Then,

$$z_1 \geq \dots z_k \geq 0 \geq z_{k+1} \geq \dots \geq z_d \tag{3.4}$$

and

$$z_1 + \dots + z_k + S(z_{k+1} + \dots + z_d) \geq \rho. \tag{3.5}$$

Now, by (3.4), the bound $0 < \max_{1 \leq i \leq d} w_i \leq S \min_{1 \leq i \leq d} w_i$ and (3.5), it follows that

$$\begin{aligned}\sum_{i=1}^{d} w_i z_i = \sum_{i=1}^{k} w_i z_i + \sum_{i=k+1}^{d} w_i z_i &\geq \min_{1 \leq i \leq k} w_i \sum_{i=1}^{k} z_i + \max_{k+1 \leq i \leq d} w_i \sum_{i=k+1}^{d} z_i \\ &\geq \min_{1 \leq i \leq d} w_i \sum_{i=1}^{k} z_i + \max_{1 \leq i \leq d} w_i \sum_{i=k+1}^{d} z_i \\ &\geq (z_1 + \dots + z_k + S(z_{k+1} + \dots + z_d)) \min_{1 \leq i \leq d} w_i \\ &\geq \rho \min_{1 \leq i \leq d} w_i.\end{aligned}$$

Combined with $z_i = y_i - 1$ and $\sum_{i=1}^{d} w_i = 1$ this implies the required estimate. □

Lemma 3.4. *Let $k \leq d$ be two integers, where $k \geq 0$, $d \geq 2$, and let α be an algebraic integer of degree d with signature (s, t) satisfying $s \geq 0.581d$ whose conjugates $\alpha_1, \dots, \alpha_d$ are labeled so that*

$$|\alpha_1| \geq \cdots \geq |\alpha_k| \geq 1 \geq |\alpha_{k+1}| \geq \cdots \geq |\alpha_d|.$$

Then,

$$|\alpha_1|^2 + \cdots + |\alpha_k|^2 + 2(|\alpha_{k+1}|^2 + \cdots + |\alpha_d|^2) \geq 2d - k + d\varphi(\lambda), \tag{3.6}$$

where $\lambda = s/d$ and $\varphi(\lambda)$ defined in (2.1)*-*(2.3)*.*

Proof. Note that $k \geq 1$. Indeed $k = 0$ can only happen if all α_i, $i = 1, \dots, d$, are of modulus 1. So, by Kronecker's theorem, α must be a root of unity which is not the case. If $k = d$ then, by the arithmetic and geometric mean inequality (referred to as AM-GM below) and (3.3), the left side of (3.6) is at least

$$d|\mathrm{Norm}(\alpha)|^{2/d} = dM(\alpha)^{2/d} \geq dg(\lambda),$$

where $g(\lambda)$ is defined in (2.1). Since $g(\lambda)$ is increasing in $\lambda > 0$ and $g(0.581) = 1.189607\dots$, we find that the left side of (3.6) is at least $1.189d$. This is greater than its right side, since

$$2d - k + d\varphi(\lambda) = d + d\varphi(\lambda) \leq d + d\varphi(1) < d + 0.18d = 1.18d$$

(see Proposition 2.1 and Table 1). In all what follows we thus assume that $0 < k < d$.

By AM-GM, estimating

$$|\alpha_1|^2 + \cdots + |\alpha_k|^2 \geq kM(\alpha)^{2/k}$$

and

$$|\alpha_{k+1}|^2 + \cdots + |\alpha_d|^2 \geq (d-k)\Big(\frac{|\mathrm{Norm}(\alpha)|}{M(\alpha)}\Big)^{2/(d-k)} \geq (d-k)M(\alpha)^{-2/(d-k)}$$

we find that the left side of (3.6) is at least

$$kM(\alpha)^{2/k} + 2(d-k)M(\alpha)^{-2/(d-k)}.$$

Hence, it suffices to show that

$$\frac{kM(\alpha)^{2/k} + 2(d-k)M(\alpha)^{-2/(d-k)}}{d} - 2 + \frac{k}{d} \geq \varphi(\lambda). \tag{3.7}$$

Note that the function $ky^{2/k} + 2(d-k)y^{-2/(d-k)}$ is increasing in y in the interval $[2^{d/8}, \infty)$, since its derivative $2y^{2/k-1} - 4y^{-2/(d-k)-1}$ is positive for $y > 2^{k(d-k)/(2d)}$ and the maximum of $k(d-k)$ is attained at $k = d/2$. Also, by (3.2) and $2^{1/8} = 1.090507\dots$, the inequality $M(\alpha) > 1.090691^d > 2^{d/8}$ holds. Thus, replacing $M(\alpha)$ in (3.7) by its estimate from below as in (3.3) and setting $x := k/d$, we see that it suffices to prove the inequality

$$xg(\lambda)^{1/x} + 2(1-x)g(\lambda)^{-1/(1-x)} - 2 + x \geq \varphi(\lambda) \tag{3.8}$$

for $0 < x < 1$. However, (3.8) clearly holds, by the definition of the function $\varphi(\lambda)$ in Theorem 2.2 as the minimum of the left side of (3.8) in the interval $(0, 1]$. □

The next result is given [12].

Lemma 3.5. *There exist m (explicitly given) polynomials with integer coefficients $Q_1, \dots,$ Q_m and m (explicitly given) positive numbers $e_1, \dots, e_m$ such that the inequality*

$$y - \sum_{i=1}^{m} e_i \log |Q_i(y)| > 1.79193$$

holds for each $y > 0$ which is not a root of $Q_1 \dots Q_m$.

We remark that each improvement of the constant of this lemma leads to the corresponding improvement in Theorem 2.5. However, although the conjectural lower bound for the trace of a totally positive algebraic integer α is $(2-\varepsilon)d$, where ε is an arbitrary positive number and the degree d of α is at least $d(\varepsilon)$, Serre has shown that the method of auxiliary functions as in the above lemma cannot give a constant greater than 1.8983021 (see the appendix in [1]).

4 Proof of Proposition 2.1

Note that $y = g(\lambda) > 1$ for $\lambda > 0$. Consider the function

$$f(y) := xy^{1/x} + 2(1-x)y^{-1/(1-x)}$$

in the interval $1 < y < \infty$ (here, $0 < x < 1$). Its derivative

$$f'(y) = y^{1/x-1} - 2y^{-1/(1-x)}$$

is positive if $y^{1/x+1/(1-x)} > 2$, that is, $y > 2^{x(1-x)}$. In particular, since $x(1-x) \le 1/4$, the function $f(y)$ is increasing in the interval $2^{1/4} < y < \infty$.

Thus, by (2.3) and (2.1) (which implies that $g(\lambda)$ is increasing in λ), for every fixed x in the range $0 < x < 1$ the function

$$xg(\lambda)^{1/x} + 2(1-x)g(\lambda)^{-1/(1-x)} - 2 + x$$

in increasing (in λ) for λ satisfying $g(\lambda) > 2^{1/4}$. In particular, $\varphi(\lambda)$ is increasing in λ for λ satisfying $g(\lambda) > 2^{1/4}$. Therefore, using the fact that $g(\lambda)$ is increasing in λ for $\lambda > 0$ and the actual expression (2.1), we find that

$$g(0.581) = 1.189607\cdots > 1.189207\cdots = 2^{1/4}.$$

Consequently, the function $\varphi(\lambda)$ is increasing for $\lambda \ge 0.581$. Evaluating $\varphi(\lambda)$ at $\lambda = 0.828$ gives the positive value $\varphi(0.828) = 0.000389\dots$, so $\varphi(\lambda) > 0$ for $\lambda \ge 0.828$. This, combined with evaluation of $\varphi(1) = 0.176732\dots$ and λ_0 satisfying $\varphi(\lambda_0) = 0$ completes the proof of the proposition.

5 Proof of Theorem 2.2

Let $\alpha \in \mathbb{K}$ and $\mathbb{L} = \mathbb{Q}(\alpha)$. Assume that the signature of α is (s,t) and the signature of $\mathbb{K}$ is $(s(\mathbb{K}), t(\mathbb{K}))$. Here, $\lambda = s(\mathbb{K})/n$, where $n = s(\mathbb{K}) + 2t(\mathbb{K}) = [\mathbb{K} : \mathbb{Q}]$. Put also $\lambda_1 := s(\mathbb{L})/d = s/d$, where $d = s + 2t = [\mathbb{L} : \mathbb{Q}]$. We will show that

$$\lambda_1 \ge \lambda. \tag{5.1}$$

Observe first that $t(\mathbb{L}) = 0$ implies that $s(\mathbb{L}) = d$, so that $\lambda_1 = 1$, which yields (5.1). Also, $t(\mathbb{K}) = 0$ implies $t(\mathbb{L}) = 0$, which leads to the situation we have just considered. So assume that $t(\mathbb{K}) \neq 0$ and $t = t(\mathbb{L}) \neq 0$. Then, in view of Lemma 3.2 we have $s(\mathbb{K})/t(\mathbb{K}) \leq s/t$. Adding 2 to both sides we deduce

$$\frac{n}{t(\mathbb{K})} = \frac{s(\mathbb{K}) + 2t(\mathbb{K})}{t(\mathbb{K})} = 2 + \frac{s(\mathbb{K})}{t(\mathbb{K})} \leq 2 + \frac{s}{t} = \frac{s+2t}{t} = \frac{d}{t}.$$

Therefore, $t/d \leq t(\mathbb{K})/n$. This implies (5.1), since $t/d = (1-\lambda_1)/2$ and $t(\mathbb{K})/n = (1-\lambda)/2$.

Let $\alpha_1, \dots, \alpha_s$ be the real conjugates of α. Put

$$\mathcal{C}(\alpha) := \sum_{j=1}^{t} |\alpha_{s+j}|^2 = \frac{1}{2} \sum_{i=s+1}^{d} |\alpha_i|^2.$$

Assume that for each real α_i, $1 \leq i \leq s$, it appears u_i times under the $s(\mathbb{K})$ real embeddings of $\mathbb{K}$ and $2v_i$ times under the $2t(\mathbb{K})$ complex embeddings of $\mathbb{K}$. Here, we have $u_i + 2v_i = [\mathbb{K} : \mathbb{L}]$ for each i. Also,

$$s(\mathbb{K}) = u_1 + \ldots + u_s \quad \text{and} \quad t(\mathbb{K}) = [\mathbb{K} : \mathbb{L}]t + v_1 + \ldots + v_s. \tag{5.2}$$

So, in view of (1.2) we can write

$$(s(\mathbb{K}) + t(\mathbb{K}))m_{\mathbb{K}}(\alpha) = \sum_{i=1}^{s} (u_i + v_i)\alpha_i^2 + [\mathbb{K} : \mathbb{L}]\mathcal{C}(\alpha). \tag{5.3}$$

Here, $\mathcal{C}(\alpha) = \frac{1}{2}\sum_{i=s+1}^{d} |\alpha_i|^2$. Setting

$$w_i := \frac{u_i + v_i}{s(\mathbb{K}) + t(\mathbb{K})}$$

for $i = 1, \dots, s$ and

$$w_i := \frac{[\mathbb{K} : \mathbb{L}]}{2s(\mathbb{K}) + 2t(\mathbb{K})} \tag{5.4}$$

for $i = s+1, \dots, d$, in view of (5.2) and (5.3), we derive that

$$m_{\mathbb{K}}(\alpha) = \sum_{i=1}^{d} w_i |\alpha_i|^2,$$

where $\sum_{i=1}^{d} w_i = 1$ and

$$\frac{[\mathbb{K} : \mathbb{L}]}{2s(\mathbb{K}) + 2t(\mathbb{K})} \leq w_i \leq \frac{[\mathbb{K} : \mathbb{L}]}{s(\mathbb{K}) + t(\mathbb{K})}$$

for each $i = 1, \dots, d$. Hence, by Lemma 3.3 with $S = 2$, $\rho = d\varphi(\lambda_1)$, $y_i = |\alpha_i|^2$ for $i = 1, \dots, d$, and Lemma 3.4 (with $\lambda_1 = s/d$ instead of λ), it follows that

$$m_{\mathbb{K}}(\alpha) = \sum_{i=1}^{d} w_i |\alpha_i|^2 \geq 1 + d\varphi(\lambda_1) \min_{1 \leq i \leq d} w_i.$$

Now, in case $s = d$ we have $\lambda_1 = 1$, so $\varphi(\lambda_1)$ is positive and using

$$\min_{1\le i\le d} w_i \ge \frac{[\mathbb{K} : \mathbb{L}]}{2s(\mathbb{K}) + 2t(\mathbb{K})} \tag{5.5}$$

we derive that

$$m_{\mathbb{K}}(\alpha) \ge 1 + \frac{d[\mathbb{K} : \mathbb{L}]\varphi(\lambda_1)}{2s(\mathbb{K}) + 2t(\mathbb{K})}. \tag{5.6}$$

Otherwise, when $s < n$, in view of (5.4) we have equality in (5.5). Thus, (5.6) also holds (even if $\varphi(\lambda_1)$ is negative).

Now, since $d[\mathbb{K} : \mathbb{L}] = [\mathbb{L} : \mathbb{Q}][\mathbb{K} : \mathbb{L}] = [\mathbb{K} : \mathbb{Q}] = n$ and

$$\frac{n}{2s(\mathbb{K}) + 2t(\mathbb{K})} = \frac{n}{n + s(\mathbb{K})} = \frac{1}{1+\lambda},$$

from (5.6) we further deduce that

$$m_{\mathbb{K}}(\alpha) \ge 1 + \frac{\varphi(\lambda_1)}{1+\lambda}. \tag{5.7}$$

Here, we have $\varphi(\lambda_1) \ge \varphi(\lambda)$, by Proposition 2.1 and the inequality (5.1). Also, by the same inequality, $1/(1+\lambda) \ge 1/(1+\lambda_1)$. So, in particular, (5.7) yields

$$m_{\mathbb{K}}(\alpha) \ge 1 + \max\left\{\frac{\varphi(\lambda)}{1+\lambda}, \frac{\varphi(\lambda_1)}{1+\lambda_1}\right\} \tag{5.8}$$

which implies the required bound.

6 Proof of Theorem 2.5

Let α be an algebraic integer with degree d greater than

$$E := 2 \max_{1\le i\le m} \deg Q_i,$$

where $Q_i \in \mathbb{Z}[x]$ are given in Lemma 3.5. Applying this lemma to $y := \alpha_j^2$, where $j = 1, \dots, s$, and summing up over j we find that

$$\sum_{j=1}^{s} \alpha_j^2 > 1.79193s + \sum_{j=1}^{s}\sum_{i=1}^{m} e_i \log|Q_i(\alpha_j^2)|. \tag{6.1}$$

Note that there is nothing to prove if at least one conjugate of α is greater than $\sqrt{2d}$, because then the right side of (2.5) is greater than $2d/(s+t) \ge 2$ which is better than required. So, in all what follows without restriction of generality we may assume that $|\alpha_{s+j}| \le \sqrt{2d}$ for $j = 1, \dots, t$.

Clearly,

$$|Q_i(\alpha_{s+j}^2)| \le (D_i + 1)H_i(2d)^{D_i},$$

where D_i and H_i are the degree and the height of the polynomial Q_i, respectively. Similarly, $|Q_i(\overline{\alpha_{s+j}}^2)| \le (D_i + 1)H_i(2d)^{D_i}$. Note that the degree of α^2 is either d or $d/2$, so it is greater than any $D_i = \deg Q_i$ provided that $d \geq D > E$. Hence, $Q_i(\alpha_j^2) \neq 0$ for each $i = 1, \dots, m$ and each $j = 1, \dots, d$. Consequently,

$$\begin{aligned}1 \leq \prod_{j=1}^{d} |Q_i(\alpha_j^2)| &= \prod_{j=1}^{s} |Q_i(\alpha_j^2)| \prod_{j=1}^{t} |Q_i(\alpha_{s+j}^2)||Q_i(\overline{\alpha_{s+j}}^2)| \\ &\leq (2d)^{2tD_i} U_i^{2t} \prod_{j=1}^{s} |Q_i(\alpha_j^2)|,\end{aligned}$$

where $U_i := (D_i + 1)H_i$, which yields

$$\sum_{j=1}^{s} \log |Q_i(\alpha_j^2)| \geq -2tD_i \log(2d) - 2t \log U_i.$$

Summing these inequalities with weights e_i over $i = 1, \dots, m$ we derive that

$$\begin{aligned}\sum_{j=1}^{s} \sum_{i=1}^{m} e_i |\log Q_i(\alpha_j^2)| &= \sum_{i=1}^{m} \sum_{j=1}^{s} e_i |\log Q_i(\alpha_j^2)| \\ &\geq -\sum_{i=1}^{m} (2tD_i e_i \log(2d) + 2te_i \log U_i) \\ &\geq -At \log(Bd),\end{aligned}$$

where the constants $A, B > 2$ depend on the constants $e_1, \dots, e_m$ and the polynomials $Q_1, \dots, Q_m$ only. Combining this inequality with (6.1) we get

$$\sum_{j=1}^{s} \alpha_j^2 > 1.79193s - At \log(Bd).$$

To complete the proof of the theorem it suffices to show that

$$1.79193s - At \log(Bd) > 1.79192(s + t),$$

which is equivalent to

$$10^{-5}s > At \log(Bd) + 1.79192t.$$

Multiplying both sides of this inequality by 10^5 and adding $2t$ we obtain the following equivalent inequality:

$$d = s + 2t > 10^5 At \log(Bd) + 179192t + 2t = 10^5 At \log(Bd) + 179194t.$$

We will show that the stronger inequality

$$d > 10^5(A + 2)t \log(Bd) \tag{6.2}$$

holds with the constants

$$\delta := \frac{1}{10^5(2A + 4)} \quad \text{and} \quad D := \max\{B, E + 1\}$$

depending on $e_1, \dots, e_m$ and $Q_1, \dots, Q_m$ only.

Indeed, in view of the upper bound on t, namely, $t < \delta d/\log d$, the first lower bound on d, namely, $d \ge D \ge B$, and the choice of δ the right side of (6.2) is less than

$$10^5(A+2)\frac{\delta d}{\log d}\log(Bd) \le 10^5(A+2)\frac{\delta d}{\log d}\log(d^2) = \delta 10^5(2A+4)d = d.$$

This completes the proof of (6.2) and the proof the theorem.

References

[1] J. Aguirre and J. C. Peral, The trace problem for totally positive algebraic integers. With an appendix by Jean-Pierre Serre, in: Number Theory and Polynomials, London Math. Soc. Lecture Note Ser., vol. 352, Cambridge Univ. Press, Cambridge, 2008, 1–19.

[2] J. H. Conway and N. J. A. Sloane, *Sphere packings, lattices and groups*, third ed., Grundlehren der Mathematischen Wissenschaften **290**, Springer-Verlag, New York, 1999.

[3] N. Coxon, List decoding of number field codes, *Des. Codes Cryptogr.* **72** (2014), 687–711.

[4] X. Dong and Q. Wu, The absolute trace of totally positive reciprocal algebraic integers, *J. Number Theory* **170** (2017), 66–74.

[5] J. R. Doyle and D. Krumm, Computing algebraic numbers of bounded height, *Math. Comp.* **84** (2015), 2867–2891.

[6] A. Dubickas, Algebraic integers with small absolute size, *Quaest. Math.*, to appear.

[7] A. Dubickas, M. Sha and I. E. Shparlinski, On distances in lattices from algebraic number fields, *Moscow Math. J.* **17** (2017), 239–268.

[8] J. Garza, On the height of algebraic numbers with real conjugates, *Acta Arith.* **128** (2007), 385–389.

[9] V. Guruswami, Constructions of codes from number fields, *IEEE Trans. Inform. Theory* **49** (2003), 594–603.

[10] G. Höhn, On a theorem of Garza regarding algebraic numbers with real conjugates, *Int. J. Number Theory* **7** (2011), 943–945.

[11] S. Lang, *Algebraic number theory*, Graduate Texts in Mathematics **110**, Springer-Verlag, New York, 1994.

[12] Y. Liang and Q. Wu, The trace problem for totally real positive integers, *J. Aust. Math. Soc.* **90** (2011), 341–354.

[13] A. Pethő and S. Schmitt, Elements with bounded height in number fields, *Period. Math. Hung.* **43** (2001), 31–41.

[14] K. Pratt, G. Shakan and A. Zaharescu, A generalization of the Schur–Siegel–Smyth trace problem, *J. Math. Anal. Appl.* **436** (2016), 489–500.

[15] I. Schur, Über die Verteilung der Wurzeln bei gewissen algebraischen Gleichungen mit ganzzahligen Koeffizienten, *Math. Z.* **1** (1918), 377–402.

[16] I. E. Shparlinski, *Finite fields: Theory and computation*, Kluwer Acad. Publ., Dordrecht, 1999.

[17] C. L. Siegel, The trace of totally positive and real algebraic integers, *Ann. of Math. (2)* **46** (1945), 302–312.

[18] C. J. Smyth, Totally positive algebraic integers of small trace, *Ann. Inst. Fourier (Grenoble)* **34** (1984), 1–28.

[19] M. A. Tsfasman, Global fields codes and sphere packings, *Journ. Arithmetiques, Luminy, Astérisque*, **198–200** (1992), 373–396.