INTEGER SYMMETRIC MATRICES: COUNTEREXAMPLES TO ESTES–GURALNICK'S CONJECTURE

Pavlo Yatsyna

Royal Holloway,
University of London

Thesis submitted to

The University of London

for the degree of

Doctor of Philosophy

2016.

Declaration of Authorship

I, Pavlo Yatsyna, hereby declare that this thesis and the work presented in it is entirely my own. Where I have consulted the work of others, this is always clearly stated.

Signature:

Date:

Abstract

The aim of this thesis is to study which polynomials appear as minimal polynomials of integer symmetric matrices. It has been known for a long time that to be the minimal polynomial of a rational symmetric matrix it is necessary and sufficient that the polynomial is monic, separable and has only real roots. It was conjectured by Estes and Guralnick that the equivalent conditions should hold for integer symmetric matrices.

We present counterexamples to Estes–Guralnick's conjecture for every degree strictly larger than five. In the process, we construct Salem numbers of trace -2 for every even degree strictly larger than 22. Furthermore, we settle the Schur–Siegel–Smyth trace problem for polynomials that appear as minimal polynomials of integer symmetric matrices or integer oscillatory matrices.

Acknowledgements

I would like to thank my supervisor, Professor James McKee, for his endless support, guidance and patience. It was a great pleasure and honour to be supervised by him.

I am thankful to the members of the mathematics department in Royal Holloway. My thanks go to Andrew, Caroline, Christian, Conrad, Dale, Dean, Eugenio, Ged, George, Joachim, Konstantinos, Matteo, Marcelo, Sam, Thalia, Victor and Wangpen for their friendship and all the good times that we have shared together. A special thanks to Dr Alexey Koloydenko for many stimulating conversations, and to Dr Martin Widmer for always finding time to discuss mathematics and patiently explain to me many interesting concepts in number theory.

I am grateful to Dr Gary Greaves for his advice over the past four years.

To my family, thank you for everything.

Contents

Notation

We fix the following notation:

$$
\begin{aligned}
\mathbb{C} &= \text{complex numbers} \\
\mathbb{R} &= \text{real numbers} \\
\mathbb{R}_+ &= \text{positive real numbers} \\
\mathbb{Q} &= \text{rational numbers} \\
\mathbb{Z} &= \text{rational integers} \\
\mathbb{Z}_+ &= \text{positive rational integers} \\
\mathcal{O} &= \text{a commutative ring} \\
\mathrm{Mat}(\mathcal{O}) &= \text{the set of square matrices over } \mathcal{O} \\
\mathrm{Mat}(n, \mathcal{O}) &= \text{the set of } n \times n \text{ matrices over } \mathcal{O} \\
\mathrm{Sym}(\mathcal{O}) &= \text{the set of symmetric matrices over } \mathcal{O} \\
\mathrm{Sym}(n, \mathcal{O}) &= \text{the set of } n \times n \text{ symmetric matrices over } \mathcal{O} \\
I_n &= \text{the identity matrix of order } n \\
O &= \text{the zero matrix} \\
\mathrm{Tr}(A) &= \text{the trace of a matrix } A \\
A^t &= \text{the transpose of a matrix } A \\
\chi_A(x) &= \text{the characteristic polynomial of a matrix } A \\
\mathrm{diag}(\cdots) &= \text{a diagonal matrix} \\
\deg(f(x)) &= \text{the degree of a polynomial } f(x) \\
\upharpoonright &= \text{the restriction of a function} \\
|X| &= \text{the cardinality of a set } X.
\end{aligned}
$$

Chapter 1

Introduction

1.1 An overview

Our starting point is an old question (1933) of Lehmer:

Question 1.1.1. [68] Let $\epsilon > 0$. Does there exist a monic $f \in \mathbb{Z}[x]$ such that the absolute value of the product of the roots of f that lie outside of the unit circle, lies between 1 and $1 + \epsilon$?

This question was motivated by the search for large prime numbers. In particular, Lehmer was interested in primes dividing the function

$$\Delta_n(f) = \prod_{i=1}^{r} (\alpha_i^n - 1),$$

where $f \in \mathbb{Z}[x]$ is an irreducible monic polynomial of degree r, with roots $\alpha_1, \ldots, \alpha_r$. By picking $f = x - 2$, we observe that this method generalises the search of Mersenne primes.

Definition 1.1.2. *Let $f = a_0 \prod_{i=1}^{n} (x - \alpha_i) \in \mathbb{Z}[x]$. Then the **Mahler measure** of f is defined as $\mathrm{M}(f) := |a_0| \prod_{i=1}^{n} \max(1, |\alpha_i|)$.*

Notice that the Mahler measure respects multiplication, i.e. $\mathrm{M}(fg) = \mathrm{M}(f)\mathrm{M}(g)$ for $f, g \in \mathbb{Z}[x]$. A cyclotomic polynomial is a monic integer polynomial such that all its roots are roots of unity (see Chapter 4). The following is a well known result of Kronecker:

Theorem 1.1.3. [65] *Let $f \in \mathbb{Z}[x]$ and $f \neq 0$. Then $\mathrm{M}(f) = 1$ if and only if f is a cyclotomic polynomial.*

Thus in the light of Lehmer's question there exists the following conjecture:

Conjecture 1.1.4 (Lehmer's conjecture)**.** There exists $\epsilon > 0$ such that for all $f \in \mathbb{Z}[x]$ if $\mathrm{M}(f) < 1 + \epsilon$ then $\mathrm{M}(f) = 1$.

Over the past 70 years some progress has been achieved in the pursuit of settling this conjecture. Many special cases of Lehmer's conjecture have been proved [101]. One of the best general bounds for the Mahler measure of a polynomial was given by Dobrowolski:

Theorem 1.1.5. [30] *Let $f \in \mathbb{Z}[x]$ be a nonzero monic polynomial of degree n. If*

$$\mathrm{M}(f) \leq 1 + \frac{1}{1200}\left(\frac{\log\log n}{\log n}\right)^3$$

then $\mathrm{M}(f) = 1$.

The smallest known Mahler measure of a monic integer polynomial is $\lambda_0 = \mathrm{M}(L) = 1.17628\ldots$, where

$$L(x) = x^{10} + x^9 - x^7 - x^6 - x^5 - x^4 - x^3 + x + 1,$$

which sometimes is known as **Lehmer's polynomial**. All but two roots of this polynomial are on the unit circle. For any such polynomial we can define the polynomial $g \in \mathbb{Z}[x]$ such that $f(x) = x^{\deg(g)} g\left(x + \frac{1}{x}\right)$ (see Proposition 4.1.5). We say that f is the **associated reciprocal polynomial** of g. All roots of the polynomial g are real; moreover all but one is in the interval $[-2, 2]$. For example, Lehmer's polynomial is the associated reciprocal polynomial of

$$x^5 + x^4 - 5x^3 - 5x^2 + 4x + 3.$$

Accordingly we shall depart from the general statement of Lehmer's conjecture and focus our attention to the monic integer polynomials with all real roots and their corresponding associated reciprocal polynomials. The central result motivating this deviation is the following theorem due to McKee and Smyth:

Theorem 1.1.6. [80] *Let S be an integer symmetric matrix. Then the Mahler measure of the associated reciprocal polynomial of the characteristic polynomial of S is either one or at least λ_0.*

Hence understanding which polynomials appear as characteristic polynomials of integer symmetric matrices is paramount in this case of Lehmer's conjecture.

Symmetric matrices play an important role in many areas of mathematics. In graph theory the adjacency matrix of a simple graph is a $(0, 1)$-symmetric matrix, and in number theory quadratic forms have a representation as symmetric matrices. Much of what follows will rely on the findings and notions in these two areas of research.

The question of which polynomials appear as characteristic polynomials of integer symmetric matrices was studied quite extensively, and yet it is far from being answered. Much has been contributed by the wide outreach of work of Taussky [106], Faddeev [35, 36, 37, 38], Bender [10, 11, 12, 13, 14], Shapiro [92, 93, 94], and many others [15, 16, 41, 89, 90, 110]. A real symmetric matrix has only real eigenvalues. By considering diagonal matrices, it is clear that every real number can appear as an eigenvalue of a real symmetric matrix. If we restrict to rational symmetric matrices, then linear polynomials are characteristic polynomials of integer symmetric matrices, under the necessary and sufficient condition that the given polynomial is monic. But even for quadratic polynomials, it is not sufficient any more to be monic and have real roots.

Example 1.1.7. Let $P(x) := x^2 - p$, where p is a prime number. A 2×2 symmetric matrix

$$\begin{pmatrix} a & b \\ b & c \end{pmatrix}$$

has the characteristic polynomial $x^2 - (a+c)x + (ac - b^2)$, where $a, b, c \in \mathbb{Q}$. This polynomial is equal to $P(x)$ if and only if $a = -c$ and $p = a^2 + b^2$. But it is well known that a prime number can be represented as a sum of two squares of rational numbers if and only if p is 2 or $p \equiv 1 \pmod 4$. Therefore, there exist infinitely many monic rational polynomials that have all real roots, but are not characteristic polynomials of rational symmetric matrices. For example, $x^2 - 3$ is not the characteristic polynomial of a rational symmetric matrix.

However, $x^2 - 3$ is the minimal polynomial of rational symmetric matrix

$$\begin{pmatrix} -1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & -1 \\ 0 & 1 & -1 & -1 \end{pmatrix}.$$

Thus it is pertinent to revise our investigation to consideration of minimal polynomials of integer symmetric matrices. Given that we are working over fields of characteristic zero, the question of which polynomials appear as minimal polynomials of symmetric matrices, requires an extra condition of separability, i.e. that all the roots of the polynomial are distinct. We pose the following conjecture:

Conjecture 1.1.8. Let S be an integer symmetric matrix. Then the Mahler measure of the associated reciprocal polynomial of the minimal polynomial of S is either one or at least λ_0.

For rational symmetric matrices it was proved that:

Theorem 1.1.9. [11, 13, 64] *Let $f \in \mathbb{Q}[x]$ be a monic polynomial of degree n such that all its roots are real and distinct. Then f is the minimal polynomial of a $4n \times 4n$ rational symmetric matrix. Furthermore, if n is odd, then f is the characteristic polynomial of a rational symmetric matrix.*

Bender complemented the above result for polynomials of even degree, by showing that an appropriate polynomial of degree $2n$ divides the characteristic polynomial of a $2n+1 \times 2n+1$ rational symmetric matrix [11].

It is natural to ask which of the theorems above hold for integer symmetric matrices. Obviously, the necessary conditions over the field remain necessary over the ring. Estes and Guralnick, in their paper [34], conjectured that those conditions are sufficient:

Conjecture 1.1.10 (Estes–Guralnick's conjecture)**.** An integer polynomial is the minimal polynomial of an integer symmetric matrix if and only if it is monic, separable and all its roots are real.

Furthermore, they showed that every monic separable polynomial with all real roots and of degree $n \leq 4$, is the minimal polynomial of a $2n \times 2n$ integer symmetric matrix. We shall expand on this in the next chapter.

Estes–Guralnick's conjecture was proved to be wrong. The first counterexamples were due to Dobrowolski [31] based on the discriminant bound. He showed that there exists an infinite family of counterexamples, with the smallest being of degree 2880. Not much later McKee [76] found counterexamples by studying polynomials with a small span (separation between the largest and smallest roots), the smallest such counterexample being of degree six. The lowest degree for which Estes–Guralnick's conjecture is unknown is five. Given that Estes–Guralnick's conjecture is false, it is worthwhile to propose a "weaker" form of Question 5.1 in [34] as a conjecture:

Conjecture 1.1.11 (Weak Estes–Guralnick's conjecture)**.** If an integer polynomial of degree n is the minimal polynomial of an integer symmetric matrix, then it is the minimal polynomial of a $2n \times 2n$ integer symmetric matrix.

An affirmative answer to this conjecture would give us an effective way of determining whether a given polynomial is the minimal polynomial of an integer symmetric matrix. This follows from the fact that to check that a given polynomial is the characteristic polynomial of an integer symmetric matrix is a finite search (see Chapter 3).

The following chapters are divided into two parts. The first part presents the general overview of Estes and Guralnick's approach and the case for Estes–Guralnick's conjecture. The second part focuses on the array of previously unknown methods of finding counterexamples to the conjecture. We show that:

Theorem 3.2.1. Let $A \in \mathrm{Sym}(n, \mathbb{Z})$ be a connected and positive definite matrix. Then $\mathrm{Tr}(A) \geq 2n - 1$.

Therefore, for a monic irreducible polynomial $f \in \mathbb{Z}[x]$ such that all its n roots are real and positive, to be the minimal polynomial of an integer symmetric matrix it is necessary that the sum of the roots of f is strictly larger than $2n - 2$. By constructing infinite families of Salem numbers we show that:

Proposition 4.1.25. There are Salem numbers of trace -2 of degree $2d$ for all $d \geq 12$.

As a consequence, we show that for each degree strictly larger than five there exists a counterexample to Estes–Guralnick's conjecture (see Corollary 4.1.26). In addition we show that if n is squarefree, not a prime number or twice a prime number, and $\phi(n) > 8$, then the minimal polynomial of $\zeta_n + \zeta_n^{-1}$ is noninterlacing and thus is a counterexample to Estes–Guralnick's conjecture (Corollary 4.2.42). Finally, we prove that there do not exist noninterlacing monic irreducible integer polynomials of degree n such that all their roots are real and $n = 1, 2, 3, 4, 5$ or 7 (Corollary 4.2.51).

Throughout the work, all the computation were performed by PARI/GP.

Part I

Estes–Guralnick's conjecture

Chapter 2

Minimal polynomials of integer symmetric matrices

This chapter presents the main body of Estes and Guralnick's method of constructing positive definite odd unimodular lattices that have a self-adjoint operator acting on them. This will entail us proving a version of Theorem 1.1.9. Consequently we shall be able to show that every totally real algebraic integer is an eigenvalue of an integer symmetric matrix, and is in the spectrum of adjacency matrices of simple graphs. Much of this chapter is an expansion of the proof in the paper of Estes and Guralnick [34], but the subsection at the end about quintic polynomials is new.

2.1 Preliminaries

We begin by introducing all the necessary definitions and notations that we shall employ in the forthcoming sections. We used [57, 58] as the main reference for commutative algebra, [84, 86] for quadratic forms, and [67, 85] for algebraic number theory. Throughout the chapter by a ring we should always mean a commutative domain with an identity and of characteristic zero.

2.1.1 Modules

First let us remind ourselves about modules.

Definition 2.1.1. *Let $\mathcal{O}$ be a ring. An $\mathcal{O}$-**module** is an abelian group A on which $\mathcal{O}$ acts linearly. Thus for $1, \alpha, \beta \in \mathcal{O}$ and $v, w \in A$ we have*

(i) $\alpha(v + w) = \alpha v + \alpha w$;

(ii) $(\alpha + \beta)v = \alpha v + \beta v$;

(iii) $(\alpha\beta)v = \alpha(\beta v)$;

(iv) $1 \cdot v = v$,

where αv (or $\alpha \cdot v$) is the action of $\mathcal{O}$ on A.

We say that an $\mathcal{O}$-module A is a **left** (**right**) $\mathcal{O}$-module if $\mathcal{O}$ acts on the left (right) of A. Evidently a module is a generalisation of a vector space over an arbitrary ring.

Definition 2.1.2. *Let A and B be two $\mathcal{O}$-modules. Define an $\mathcal{O}$-**homomorphism** to be a mapping*

$$f : A \longrightarrow B,$$

such that

(i) $f(v + w) = f(v) + f(w)$;

(ii) $f(\alpha v) = \alpha \cdot f(v)$,

for $\alpha \in \mathcal{O}$, $v, w \in A$.

Note that the map is $\mathcal{O}$-linear. The set of all such $\mathcal{O}$-homomorphisms forms an $\mathcal{O}$-module, i.e. given

$$f, g : A \longrightarrow B,$$

we define $f + g$ and $\alpha \cdot f$ for $\alpha \in \mathcal{O}$ and $v \in A$ by

$(f + g)(v) = f(v) + g(v)$;

$(\alpha \cdot f)(v) = \alpha \cdot f(v)$.

This $\mathcal{O}$-module is denoted $\mathrm{Hom}_{\mathcal{O}}(A, B)$. We shall drop $\mathcal{O}$ from the notation (i.e. leaving us with $\mathrm{Hom}(A, B)$) if the underlying ring is obvious from the context. In the case when $B = A$ we obtain an **endomorphism ring**, denoted $\mathrm{End}(A) := \mathrm{Hom}(A, A)$.

Definition 2.1.3. *Let $\mathcal{O}$ be a ring and X be a nonempty set. A **free** $\mathcal{O}$-module $\bigoplus_{x\in X} A_x$ is a direct product of copies of $\mathcal{O}$ indexed by X, where $A_x \cong \mathcal{O}$ for each x. We say that $|X|$ is the **rank** of $\bigoplus_{x\in X} A_x$.*

To work with lattices we will need the following generalisation of a free module.

Definition 2.1.4. *A module M is a **projective** module if given modules N and P and an epimorphism*

$$g : P \longrightarrow N,$$

then any homomorphism

$$h : M \longrightarrow N$$

can be factored as $h = gf$, where

$$f : M \longrightarrow P.$$

Note that the epimorphism in our context is a surjective homomorphism.

2.1.2 Lattices

Definition 2.1.5. *Let $\mathcal{O}$ be a ring. We say that $\boldsymbol{F} := \{\alpha\beta^{-1} \mid \alpha, \beta \in \mathcal{O}, \beta \neq 0\}$ is the **quotient field** of $\mathcal{O}$.*

Let $\mathrm{Sq}(\mathcal{O})$ denote the set of all the elements of $\mathcal{O}$ that can be represented as a sum of squares in $\mathcal{O}$, i.e.

$$\mathrm{Sq}(\mathcal{O}) := \left\{ r \in \mathcal{O} \mid r = \sum_{i=1}^{m} x_i^2, \text{ for some } m \in \mathbb{N}, \text{ and } x_i \in \mathcal{O} \right\}.$$

Let $\mathrm{Sq}_n(\mathcal{O}) \subset \mathrm{Sq}(\mathcal{O})$ be the subset of all those elements of $\mathcal{O}$ that can be represented as a sum of n squares, i.e.

$$\mathrm{Sq}_n(\mathcal{O}) := \left\{ r \in \mathcal{O} \mid r = \sum_{i=1}^{n} x_i^2, \text{ for some } x_i \in \mathcal{O} \right\}.$$

Example 2.1.6. *(i)* $\mathrm{Sq}(\mathbb{Z}) = \mathbb{N} \cup \{0\}$;

(ii) $\mathrm{Sq}_2(\mathbb{Z}) = \{n \in \mathbb{N} \mid \text{if for each prime } p = 4m+3,\ p^k \| n, \text{ then } k \text{ is even}\} \cup \{0\}$;

(iii) $\mathrm{Sq}_3(\mathbb{Z}) = \{n \in \mathbb{N} \mid n \neq 4^k(8m+7),\ k \in \mathbb{N} \cup \{0\}\} \cup \{0\}$;

(iv) $\mathrm{Sq}_4(\mathbb{Z}) = \mathbb{N} \cup \{0\}$.

By $p^k || n$ we convey that $p^k | n$ but $p^{k+1} \not| \, n$.

Let $\mathcal{O}^\times$ denote the group of units of $\mathcal{O}$, i.e.

$$\mathcal{O}^\times := \{r \in \mathcal{O} | r^{-1} \in \mathcal{O}\}.$$

Example 2.1.7. *(i)* $\mathbb{Z}^\times = \{1, -1\}$;

(ii) $\mathrm{Mat}(n, \mathcal{O})^\times = \mathrm{GL}(n, \mathcal{O})$;

(iii) $\mathbb{Z}[i]^\times = \{-1, 1, -i, i\}$.

Definition 2.1.8. *Let A be a left $\mathcal{O}$-module. Define a* ***bilinear form*** *on A to be a map*

$$\beta : A \times A \longrightarrow \mathcal{O},$$

such that

$$\beta(\gamma v_1 + \delta v_2, w_1) = \gamma\beta(v_1, w_1) + \delta\beta(v_2, w_1),$$
$$\beta(v_1, \gamma w_1 + \delta w_2) = \gamma\beta(v_1, w_1) + \delta\beta(v_1, w_2),$$

for $v_1, v_2, w_1, w_2 \in A$ and $\gamma, \delta \in \mathcal{O}$.

Definition 2.1.9. *We say that a bilinear form β on A is* ***symmetric*** *if*

$$\beta(v, w) = \beta(w, v)$$

for all $v, w \in A$.

We assume that all bilinear forms in this work are symmetric.

By putting $Q(v) := \beta(v, v)$ we obtain a **quadratic form** over $\mathcal{O}$, i.e. a homogeneous polynomial of degree two in $\mathcal{O}[v_1, \ldots, v_m]$ such that:

(i) $Q(\alpha v) = \alpha^2 Q(v)$;

(ii) $Q(v + w) = Q(v) + Q(w) + 2\beta(v, w)$,

where $v, w \in A$ and $\alpha \in \mathcal{O}$.

Let $\mathbf{F}$ be the quotient field of $\mathcal{O}$, and let V be a finite dimensional vector space on $\mathbf{F}$, i.e. V is an $\mathbf{F}$-space. If there exists a quadratic form Q on V with the corresponding symmetric bilinear form β, then we say that (V, β) is a **quadratic space**.

Definition 2.1.10. *An* ***$\mathcal{O}$-lattice*** *is a pair (L, β) where L is a finitely generated projective and torsion-free $\mathcal{O}$-module and β is a symmetric $\mathcal{O}$-bilinear form on L,*

$$\beta : L \times L \longrightarrow \mathcal{O}.$$

A module L is **torsion-free** if there does not exist an element $v \in L$, $r \in \mathcal{O}$, $v \neq 0$, such that r is not a zero divisor and $rv = 0$. The **rank** of a lattice L, denoted rank(L), is the rank of the corresponding module. If L has $\mathcal{O}$-basis and if $\mathcal{O}$ is a commutative domain with the quotient field $\mathbf{F}$, then (L, β) is contained in the quadratic space (V, β), where $V = \mathbf{F}L$. We can say that L is a lattice on V.

Definition 2.1.11. *Let (V, β) be a quadratic space. Then (V, β) is a* ***nonsingular*** *quadratic space if and only if: $\beta(v, w) = 0$ for all $w \in V$ implies that $v = 0$.*

All the quadratic spaces that we shall consider in the next few chapters will be nonsingular, unless stated otherwise.

Definition 2.1.12. *Let (L, β) be an $\mathcal{O}$-lattice. We say that (L, β) is* ***even*** *if and only if $\beta(v, v) \in 2\mathcal{O}$ for all $v \in L$. Otherwise, the lattice is said to be* ***odd****.*

Definition 2.1.13. *Let (L, β) be an $\mathcal{O}$-lattice. We define the* ***dual*** *of L to be $L^\vee := Hom(L, \mathcal{O})$. Specifically, for $v \in L$, let $\phi_v \in L^\vee$ be the map*

$$\begin{aligned} \phi_v : L &\longrightarrow \mathcal{O} \\ w &\mapsto \beta(v, w). \end{aligned}$$

Definition 2.1.14. *Let (L, β) be an $\mathcal{O}$-lattice. We say that (L, β) is* ***unimodular*** *if $L \cong L^\vee$. In particular, the map*

$$\begin{aligned} L &\longrightarrow L^\vee \\ v &\mapsto \phi_v \end{aligned}$$

is an isomorphism between L and $L^\vee$.

Let (L, β) be an $\mathcal{O}$-lattice and (V, β) be a nonsingular quadratic space.

Proposition 2.1.15. *Let (L, β) be an $\mathcal{O}$-lattice and (V, β) be its nonsingular quadratic space. Then $L^\vee = \{v \in V \mid \beta(v, L) \subseteq \mathcal{O}\}$.*

Proof. Let $v_1, v_2 \in V$. If $\phi_{v_1} = \phi_{v_2}$ then $\beta(v_1, w) = \beta(v_2, w)$ for all $w \in V$. Therefore $\beta(v_1 - v_2, w) = 0$ for all $w \in V$. Given that V is a nonsingular quadratic space implies that $v_1 = v_2$. Therefore $v \mapsto \phi_v$ is an injection from L to $L^\vee$.

Let $\phi \in L^\vee$. We can extend ϕ to an element of $V^\vee = \mathrm{Hom}(V, \mathbf{F})$, where $\mathbf{F}$ is the quotient field of $\mathcal{O}$. The map $v \mapsto \phi_v$ defines a bijection from V to $V^\vee$, as $v \mapsto \phi_v$ clearly is an injection and $\dim V = \dim V^\vee$. Therefore there exists $v \in V$ such that $\phi = \phi_v$. Since $\phi \restriction_L \in L^\vee$ implies that $\phi_v(L) \subseteq \mathcal{O}$. Hence $v \mapsto \phi_v$ defines a bijection and therefore $L^\vee = \{v \in V \mid \beta(v, L) \subseteq \mathcal{O}\}$. □

If L is a free $\mathcal{O}$-module of rank n then by choosing a basis $\{\omega_1, \dots, \omega_n\}$ we can associate L with a matrix $X = (X_{ij}) \in \mathrm{Sym}(n, \mathcal{O})$ defined by $X_{ij} = \beta(\omega_i, \omega_j)$. We denote by I_n the **sum of squares** lattice, i.e. the lattice with the corresponding matrix being the identity matrix of order n. Note that if an $\mathcal{O}$-lattice is unimodular then the corresponding matrix is invertible over $\mathcal{O}$.

Definition 2.1.16. *Let $\boldsymbol{F}$ be a number field. We say that $\boldsymbol{F}$ is a **totally real number field** if all embeddings $\sigma : \boldsymbol{F} \hookrightarrow \mathbb{C}$ satisfy $\sigma(\boldsymbol{F}) \subset \mathbb{R}$. An element α in a totally real field $\boldsymbol{F}$ is **totally positive**, denoted $\alpha \gg 0$, if $\sigma(\alpha) > 0$ for all embeddings σ of $\boldsymbol{F}$ in $\mathbb{R}$.*

We denote by $\mathbf{F}_+$ the set of all the totally positive elements in $\mathbf{F}$.

Definition 2.1.17. *Let $\mathcal{O}$ be a ring with the quotient field $\boldsymbol{F}$, where $\boldsymbol{F}$ is a totally real number field. Let (L, β) be an $\mathcal{O}$-lattice. We say that (L, β) is a **positive definite** lattice if and only if $\beta(v, v) \gg 0$ for all $v \in L$, $v \neq 0$.*

To distinguish among the various elements we shall choose to use bold script for vectors.

Example 2.1.18. (*i*) Let (L, β) be an $\mathbb{Z}$-lattice such that $L = \mathbb{Z}^2$ has the standard basis $\{\mathbf{e}_1, \mathbf{e}_2\}$. Let β be given by a matrix X,

$$X = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}.$$

Thus $\beta(\mathbf{v}, \mathbf{v}) = 2v_1^2 + v_2^2$. It follows that (L, β) is an odd and positive definite lattice.

Let $\mathbf{v} = (v_1, v_2)^t$, then

$$\begin{aligned} \phi_{\mathbf{v}}(\mathbf{e}_1) &= \beta(\mathbf{v}, \mathbf{e}_1) \\ &= \begin{pmatrix} v_1 & v_2 \end{pmatrix} \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ &= 2v_1, \end{aligned}$$

and

$$\begin{aligned}\phi_{\mathbf{v}}(\mathbf{e}_2) &= \beta(\mathbf{v}, \mathbf{e}_2) \\ &= \begin{pmatrix} v_1 & v_2 \end{pmatrix} \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} \\ &= v_2.\end{aligned}$$

Therefore the corresponding matrix for the dual space of L with respect to the standard basis is

$$\begin{pmatrix} 1/2 & 0 \\ 0 & 1 \end{pmatrix}.$$

(ii) A $\mathbb{Z}[\sqrt{2}]$-lattice with the corresponding matrix

$$\begin{pmatrix} 2-\sqrt{2} & 1 \\ 1 & 2+\sqrt{2} \end{pmatrix}$$

is a positive definite lattice.

(iii) A $\mathbb{Z}[\sqrt{2}]$-lattice with the corresponding matrix

$$\begin{pmatrix} 3\sqrt{2} & 2 \\ 2 & \sqrt{2} \end{pmatrix}$$

is a **definite** lattice, as the above matrix is a positive definite matrix, while its conjugate is a negative definite matrix.

(iv) A $\mathbb{Z}[\sqrt{3}]$-lattice with the corresponding matrix

$$\begin{pmatrix} \sqrt{3} & 2 \\ 2 & 2+\sqrt{3} \end{pmatrix}$$

is an **indefinite** lattice, i.e. it is not definite.

Definition 2.1.19. *We say that $A \in \mathrm{End}(L)$ is a **self-adjoint** operator on a lattice (L, β) if and only if $\beta(Au, v) = \beta(u, Av)$ for all u, $v \in L$.*

Example 2.1.20. *(i)* Trivial examples of self-adjoint operators are the identity and the zero maps.

(*ii*) Let (L, β) be an $\mathbb{Z}$-lattice with the corresponding matrix

$$S = \begin{pmatrix} 2 & 1 \\ 1 & 6 \end{pmatrix}.$$

Let $A = \begin{pmatrix} 0 & 3 \\ 1 & 0 \end{pmatrix}$. Now $\beta(\mathbf{v}, \mathbf{w}) = \mathbf{v}^t S \mathbf{w}$ and given that $A^t S = SA$ implies that

$$\begin{aligned} \beta(A\mathbf{v}, \mathbf{w}) &= (A\mathbf{v})^t S \mathbf{w} \\ &= \mathbf{v}^t A^t S \mathbf{w} \\ &= \mathbf{v}^t S A \mathbf{w} \\ &= \beta(\mathbf{v}, A\mathbf{w}), \end{aligned}$$

for all $\mathbf{v}, \mathbf{w} \in \mathbb{Z}^2$. Thus A is a self-adjoint operator on L.

Remark. Let $A, B \in \mathrm{Mat}(n, \mathbb{Z})$. We say that A is **similar** (over $\mathcal{O}$) to B if there exists $X \in \mathrm{GL}(n, \mathcal{O})$ such that $A = XBX^{-1}$. It is an equivalence relation. Define the **class** of A to be the set $\{XAX^{-1} \mid X \in \mathrm{GL}(n, \mathbb{Z})\}$. If in the class of A there exists a symmetric matrix XAX^{-1} then

$$\begin{aligned} XAX^{-1} &= (XAX^{-1})^t \\ &= (X^t)^{-1} A^t X^t, \end{aligned}$$

therefore

$$X^t X A = A^t X^t X.$$

Notice that $S = X^t X$ is a symmetric positive definite matrix; in particular $S \in \mathrm{SL}(n, \mathbb{Z})$. Therefore we can think of A as a self-adjoint operator on a unimodular positive definite lattice, as $SA = A^t S$. This is a necessary condition for the existence of a symmetric matrix in the class of A.

Proposition 2.1.21. *Let (L, β) be a lattice with an orthonormal basis. Then A is a self-adjoint operator on L if and only if the matrix of A with respect to the orthonormal basis is symmetric.*

Proof. Let $\{\mathbf{e}_1, \dots, \mathbf{e}_n\}$ be the orthonormal basis for (L, β). Thus $\beta(\mathbf{e}_i, \mathbf{e}_j) = \delta_{ij}$, and therefore the matrix corresponding to the lattice L over this basis is I_n. So $AI_n = I_n A^t$ if and only if $A = A^t$, as was required to show. □

Definition 2.1.22. *We say that matrices $A, B \in \mathrm{Mat}(n, \mathcal{O})$ are **equivalent** over $\mathcal{O}$, denoted $A \sim_{\mathcal{O}} B$, if there exists $X \in \mathrm{GL}(n, \mathcal{O})$ such that $XAX^t = B$.*

We say that two lattices are equivalent (or **isometric**) if their corresponding matrices are equivalent [82:1, 86]. In particular, if $\mathcal{O}$-lattices (L, β) and (M, γ) are isometric then we will write $(L, \beta) \sim_{\mathcal{O}} (M, \gamma)$ or $L \sim_{\mathcal{O}} M$.

Definition 2.1.23. *Let (L, β) be a lattice in a quadratic space V. The **scale** of L, denoted $\mathfrak{s}L$, is an $\mathcal{O}$-module generated by $\beta(L, L)$, i.e.*

$$\mathfrak{s}L := \left\{ \sum_{i,j}^{k} \beta(v_i, w_j) \mid v_i, w_j \in L,\ k \in \mathbb{N} \right\}.$$

*Similarly, the **norm** of L is*

$$\mathfrak{n}L := \left\{ \sum_{i}^{k} \beta(v_i, v_i) \mid v_i \in L,\ k \in \mathbb{N} \right\}.$$

Definition 2.1.24. *Let (L, β) be an $\mathcal{O}$-lattice. We say that the lattice L is **proper** if $\mathfrak{n}L = \mathcal{O}$.*

Trace forms

We introduce an algebraic construction of quadratic forms which play a prominent role throughout this work.

Definition 2.1.25. *Let $\boldsymbol{K}$ be a finite field extension of a number field $\boldsymbol{F}$. For $x \in \boldsymbol{K}$ we define an endomorphism*

$$T_x : \boldsymbol{K} \longrightarrow \boldsymbol{K}$$
$$\alpha \mapsto x\alpha.$$

We let the ***trace*** *map be the trace of this endomorphism, i.e.* $\mathrm{tr}_{\boldsymbol{K}/\boldsymbol{F}}(x) := \mathrm{Tr}(T_x)$*. Furthermore, we define the* ***trace form*** *to be the nonsingular bilinear form*

$$\boldsymbol{K} \times \boldsymbol{K} \longrightarrow \boldsymbol{F}$$
$$(x, y) \mapsto \mathrm{tr}(xy).$$

Note that tr is nonsingular as there exists an element $y \in \mathbf{K}^\times$ such that $\mathrm{tr}(y) \neq 0$. Thus if we assume that $x \neq 0$ and $\mathrm{tr}(xz) = 0$ for all $z \in \mathbf{K}$, then letting $z = x^{-1}y$ we get $\mathrm{tr}(xz) = \mathrm{tr}(y) = 0$, a contradiction.

Definition 2.1.26. *Let* (L, tr) *be a bilinear form. Then for* $\alpha \in \boldsymbol{K}^\times$ *we define another bilinear form* t_α *by*

$$t_\alpha : L \times L \longrightarrow \boldsymbol{K}$$
$$(v, w) \mapsto \mathrm{tr}(\alpha v w).$$

Example 2.1.27. $t_1(u, v) = \mathrm{tr}(uv)$.

Let $\mathbf{K}$ be a finite field extension of $\mathbf{F}$. For each $\alpha \in \mathbf{K}$, t_α is a symmetric bilinear form. Furthermore $(\mathbf{K}, t_\alpha)$ is a quadratic space. Let $\mathcal{O}_\mathbf{K}$ denote the ring of integers of $\mathbf{K}$, and let $\mathcal{O}_\mathbf{K}^\vee$ denote an $\mathcal{O}_\mathbf{F}$-dual of $(\mathcal{O}_\mathbf{K}, \mathrm{tr})$, i.e. $\mathcal{O}_\mathbf{K}^\vee = \{u \in \mathbf{K} \mid \mathrm{tr}(u, \mathcal{O}_\mathbf{K}) \subseteq \mathcal{O}_\mathbf{F}\}$.

Definition 2.1.28. *A symmetric bilinear form*

$$\beta : A \times A \longrightarrow B$$

is said to be ***associative*** *if* $\beta(ab, c) = \beta(a, bc)$ *for all* $a, b, c \in A$*. We say that a lattice* (L, β) *is an* ***associative*** *lattice if* β *is associative symmetric bilinear form.*

Remark. The above definition only make sense if the multiplication of the elements of the lattice is defined.

Example 2.1.29. Let $\mathbf{K}$ be a number field and let $\delta \in \mathbf{K}$. Then

$$\begin{aligned} t_\delta(s, tu) &= \mathrm{tr}(\delta s(tu)) \\ &= \mathrm{tr}(\delta(st)u) \\ &= t_\delta(st, u), \end{aligned}$$

and therefore t_δ is an associative form.

2.1.3 Semilocal rings

We refer to [3] as a reference for quadratic forms over semilocal rings.

Definition 2.1.30. *We define the* ***Jacobson radical*** $\mathfrak{J}$ *of a ring* $\mathcal{O}$ *to be the intersection of all the maximal ideals of* $\mathcal{O}$*, i.e.*

$$\mathfrak{J} := \bigcap \mathfrak{m}_i, \tag{2.1.1}$$

where the $\mathfrak{m}_i$ *run over all the maximal ideals of* $\mathcal{O}$*.*

Proposition 2.1.31. [Prop. 1.9, 2] *Let* $\mathcal{O}$ *be a ring and* $\mathfrak{J}$ *be its Jacobson radical. Then* $x \in \mathfrak{J}$ *if and only if* $u - xy \in \mathcal{O}^\times$ *for all* $u \in \mathcal{O}^\times$ *and for all* $y \in \mathcal{O}$*.*

Proof. Let $u \in \mathcal{O}^\times$. If $x \in \mathfrak{J}$ and $u - xy$ is not a unit then there exists some maximal ideal $\mathfrak{m}$ such that $u - xy \in \mathfrak{m}$. However $xy \in \mathfrak{m}$ and consequently $u \in \mathfrak{J}$, a contradiction.

On the other hand let $x \in \mathcal{O}$. Let us assume that there exists a maximal ideal $\mathfrak{m}$ such that $x \notin \mathfrak{m}$ (and therefore $x \notin \mathfrak{J}$). Then the ideal generated by x and $\mathfrak{m}$ is the whole ring $\mathcal{O}$. In particular, there exists some $\alpha \in \mathfrak{m}$ such that $\alpha + xy = u \in \mathcal{O}^\times$. Therefore $u - xy = \alpha \in \mathfrak{m}$, and α is not a unit. □

Proposition 2.1.32. [Ch. II, §3.5, 20] *Let* $\mathcal{O}$ *be a ring and* $\mathfrak{J}$ *be its Jacobson radical. The following are equivalent:*

(*i*) $\mathcal{O}$ *has a finite number of maximal ideals.*

(*ii*) *$\mathcal{O}/\mathfrak{J}$ is isomorphic to a finite product of fields.*

Proof. Let $\mathfrak{J}$ be the Jacobson radical of $\mathcal{O}$. Assume that (*ii*) holds, so that $\mathcal{O}/\mathfrak{J}$ is a product of a finite number of fields. Therefore $\mathcal{O}/\mathfrak{J}$ has finitely many ideals and maximal ideals. Given that $\mathfrak{J}$ is contained in each maximal ideal of $\mathcal{O}$, there is one-to-one correspondence between the maximal ideals of $\mathcal{O}$ and $\mathcal{O}/\mathfrak{J}$. Thus (*i*) follows.

Assume now that (*i*) holds and we have that $\{\mathfrak{m}_1, \ldots, \mathfrak{m}_k\}$ is the complete set of maximal ideals of $\mathcal{O}$. For each maximal ideal $\mathfrak{m}_i$ the quotient $\mathcal{O}/\mathfrak{m}_i$ is a field. Consider the following map

$$\mathcal{O} \longrightarrow \prod_{i=1}^{k} \mathcal{O}/\mathfrak{m}_i.$$

As maximal ideals are coprime, by the Chinese Remainder Theorem [Ch. I, Thm. (3.6), 85] we have that the map above is surjective and its kernel is exactly $\mathfrak{J}$. Therefore $\mathcal{O}/\mathfrak{J} \cong \prod_{i=1}^{k} \mathcal{O}/\mathfrak{m}_i$. □

Definition 2.1.33. *We say that a ring is* ***semilocal*** *if it satisfies* (*i*) *and* (*ii*) *of Proposition 2.1.32.*

Given a finite set S of maximal ideals of $\mathcal{O}$ we define a **semilocalisation** of $\mathcal{O}$ at S to be

$$\mathcal{O}_S := \{as^{-1} \mid a \in \mathcal{O}, s \notin S\}.$$

In particular $\mathcal{O}_S$ is a semilocal ring.

Example 2.1.34. $\mathbb{Z}_{\{2\}} = \{ab^{-1} \mid a, b \in \mathbb{Z},\ b \not\equiv 0 \pmod 2\}$.

2.2 Estes–Guralnick's theorem

The recurring themes in this area of research is its reliance on the classification of positive definite unimodular lattices over the rational integers. Noteworthy is the lack of equivalence classes for the low rank lattices.

Theorem 2.2.1. [106:13, 86] *Positive definite, odd and unimodular $\mathbb{Z}$-lattices over n-ary quadratic space are equivalent to I_n for $1 \leq n \leq 8$.* □

In dimension 8 there exists an even unimodular positive definite lattice E_8 (Gosset's roots lattice [26]) and therefore for ranks strictly larger than 8, along with I_n, there also exists an odd unimodular lattice $E_8 \oplus I_{n-8}$. The number of distinct classes of unimodular lattices grows fast. For instance, in dimension 32 there are at least 80,000,000 different classes of even unimodular lattices [Ch. 2, 26].

Estes and Guralnick proved the following theorem in their paper.

Theorem 2.2.2. [Thm. A, 34] *Let $f \in \mathbb{Z}[x]$ be a monic polynomial of degree n such that all its roots are real and distinct. Then there exists an odd unimodular positive definite lattice of rank $2n$ with a self-adjoint operator A such that the minimal polynomial of A is f.* □

In the light of the classification of positive definite unimodular lattices and Proposition 2.1.21, Estes and Guralnick concluded that:

Corollary 2.2.3. *Let $f \in \mathbb{Z}[x]$ be a monic polynomial of degree n such that all its roots are real and distinct, $1 \leq n \leq 4$. Then f is the minimal polynomial of an integer symmetric matrix of order $2n$.* □

We shall describe a local version of Estes–Guralnick's theorem. Furthermore we present some of the machinery from the global case. In particular, we shall see that finding a unimodular positive definite lattice with a self-adjoint operator is equivalent to finding a unimodular lattice over a ring of algebraic integers.

2.2.1 Lattices over semilocal rings

Let us assume that $\mathcal{O}$ is a commutative domain with a quotient field $\mathbf{F}$. Let $f \in \mathcal{O}[x]$ be a monic separable polynomial of degree n. We define $\mathcal{O}_{\mathbf{K}} :=$

$\mathcal{O}[x]/(f)$ and let $\mathbf{K}$ be its quotient field. Note that $\mathcal{O}_{\mathbf{K}}$ is not to be confused with the ring of integers in $\mathbf{K}$; $\mathcal{O}_{\mathbf{K}}$ is an order in $\mathbf{K}$ which may or may not be the full ring of integers (see [Ch.I, §12, 85]).

Definition 2.2.4. *Let $\boldsymbol{K}$ be a number field of degree n. Then $\mathcal{O}_{\boldsymbol{K}}$ is an **order** of $\boldsymbol{K}$ if $\mathcal{O}_{\boldsymbol{K}}$ is a subring of the rings of integers of $\boldsymbol{K}$ such that $\mathcal{O}_{\boldsymbol{K}}$ contains a basis of length n, i.e. $\mathbb{Q}\mathcal{O}_{\boldsymbol{K}} = \boldsymbol{K}$.*

Our aim shall be to show the following result.

Theorem 2.2.5. *Let $\mathcal{O}$ be a semilocalisation of $\mathbb{Z}$ and $f \in \mathcal{O}[x]$ be a monic polynomial of degree n such that all its roots are real and distinct. Then there exists $\delta \in \boldsymbol{K}$ such that for an $\mathcal{O}$-lattice $(\mathcal{O}_{\boldsymbol{K}}, t_\delta)$ we have $\mathcal{O}_{\boldsymbol{K}}^4 \sim_{\mathcal{O}} I_{4n}$.*

We understand $\mathcal{O}_{\mathbf{K}}^4$ to be an orthogonal sum of four copies of lattice $\mathcal{O}_{\mathbf{K}}$. Consequently we have the following.

Corollary 2.2.6. *Let $\mathcal{O}$ be a semilocalisation of $\mathbb{Z}$ and let $f \in \mathcal{O}[x]$ be a monic polynomial of degree n such that all its roots are real and distinct. Then f is the minimal polynomial of an $\mathcal{O}$-symmetric matrix of order $4n$.* □

We observe that as a semilocal ring of rational integers is contained in the rational field, we recoup Theorem 1.1.9 of Krakowski and Bender. However given that the proof is over semilocal rings we achieve more.

Spectra of simple graphs

Definition 2.2.7. *Let $\mathcal{E}(\mathbb{Z}) \subset \mathbb{R}$ denote the set of all the algebraic integers that appear as eigenvalues of integer symmetric matrices.*

Proposition 2.2.8. *$\mathcal{E}(\mathbb{Z})$ is a ring.*

Proof. Let λ, $\mu \in \mathcal{E}(\mathbb{Z})$ be eigenvalues of matrices $A \in \mathrm{Sym}(n, \mathbb{Z})$ and $B \in \mathrm{Sym}(m, \mathbb{Z})$, respectively. Then $\lambda\mu$ is an eigenvalue of the Kronecker product $A \otimes B$, and $\lambda - \mu$ is an eigenvalue of $A \otimes I_m - I_n \otimes B$. Thus $\mathcal{E}(\mathbb{Z})$ is a ring. □

Corollary 2.2.9. *Every totally real algebraic integer is an eigenvalue of an integer symmetric matrix.*

Proof. Let λ be an algebraic integer and let $m_\lambda \in \mathbb{Z}[x]$ be the minimal polynomial of λ. By the corollary to Theorem 2.2.5 there exists a symmetric matrix A over $\mathbb{Z}_{\{2\}}$ (see Example 2.1.34) that has m_λ as its minimal polynomial. Let $p_1, \ldots, p_k$ be a complete list of primes that divide the denominators of the entries in this matrix. Let h be the least common multiple of all those denominators. Thus $hA \in \mathrm{Sym}(\mathbb{Z})$ and hence $h\lambda \in \mathcal{E}(\mathbb{Z})$. There also exists a symmetric matrix over $\mathbb{Z}_{\{p_1,\ldots,p_k\}}$ with the minimal polynomial m_λ. Due to the analogous argument as before we have that there exists $j \in \mathbb{Z}$ such that $j\lambda \in \mathcal{E}(\mathbb{Z})$ and $\gcd(h, j) = 1$. The latter statement follows from the fact that we semilocalised at all the primes that divide h. By Bézout's identity and the fact that $\mathcal{E}(\mathbb{Z})$ is a ring, we have that $\lambda \in \mathcal{E}(\mathbb{Z})$. □

This corollary was first proved in [33] and was further generalised in [4]. It was conjectured by Alan J. Hoffman [55], motivated by the following result in [56], which was proved for nonnegative matrices.

Proposition 2.2.10. *Let $\alpha \in \mathbb{R}$ be a totally real algebraic integer. Then α is an eigenvalue of the adjacency matrix of a simple graph if and only if $\alpha \in \mathcal{E}(\mathbb{Z})$.*

Proof. The adjacency matrix of a graph is a $(0, 1)$-symmetric matrix with a zero trace. Therefore one direction of the proposition is obvious. Assume now that $\alpha \in \mathcal{E}(\mathbb{Z})$ and let $A \in \mathrm{Sym}(n, \mathbb{Z})$ be a matrix such that α appears as an eigenvalue of A. Let $A = \sum_{i=1}^{k} A_i$ where $A_i \in \mathrm{Sym}(n, \{0, \pm 1\})$ (note that such decomposition is not unique). Let $\overline{A}$ be a block circulant matrix with blocks

A_i, i.e.

$$\overline{A} := \begin{pmatrix} A_1 & A_2 & \ddots & A_k \\ A_2 & A_3 & \ddots & A_1 \\ \vdots & \vdots & \ddots & \vdots \\ A_k & A_1 & \cdots & A_{k-1} \end{pmatrix}.$$

We have that $\overline{A} \in \mathrm{Sym}(kn, \{0, \pm 1\})$ as each matrix A_i is symmetric. We claim that α is an eigenvalue of $\overline{A}$. Let $\mathbf{v}$ be an eigenvector of A with the corresponding eigenvalue α, i.e. $A\mathbf{v} = \alpha\mathbf{v}$. We construct a vector $\overline{\mathbf{v}} = \begin{pmatrix} \mathbf{v} \\ \vdots \\ \mathbf{v} \end{pmatrix} \in$ $\mathrm{Mat}(kn, 1, \mathbb{R})$. Then

$$\begin{aligned} (\overline{A}\overline{\mathbf{v}})_j &= \sum_{i=1}^{k} A_i \mathbf{v} \\ &= A\mathbf{v} \\ &= \alpha\mathbf{v}, \end{aligned}$$

where by $(\overline{A}\overline{\mathbf{v}})_j$ we mean the product of the j-th column of $n \times n$ blocks of $\overline{A}$ and $\overline{\mathbf{v}}$. Therefore $\overline{A}\overline{\mathbf{v}} = \alpha\overline{\mathbf{v}}$, and hence the claim follows. Let us represent $\overline{A}$ as $\overline{A} = A^+ - A^-$, where $A^+, A^- \in \mathrm{Sym}(kn, \{0, 1\})$. Then $A' = \begin{pmatrix} A^+ & A^- \\ A^- & A^+ \end{pmatrix} \in$ $\mathrm{Sym}(2kn, \{0, 1\})$ is a symmetric matrix also. Let $\mathbf{v}' = \begin{pmatrix} \overline{\mathbf{v}} \\ -\overline{\mathbf{v}} \end{pmatrix}$, then $A'\mathbf{v}' = \alpha\mathbf{v}'$. Finally, if there exists a nonzero value on the diagonal of A' we can extend A' further to $\begin{pmatrix} 0 & A' \\ A' & 0 \end{pmatrix}$ to give us the desired symmetric matrix with the eigenvalue α and its corresponding eigenvector $\begin{pmatrix} \mathbf{v}' \\ \mathbf{v}' \end{pmatrix}$. □

Corollary 2.2.11. [33] *Every totally real algebraic integer is an eigenvalue of the adjacency matrix of a simple graph.* □

Recently this corollary was extended (by a completely different method) to show that every totally real algebraic integer is an eigenvalue of a tree [91].

Bass, Estes and Guralnick were first to show that for a given totally real algebraic integer of degree n, the integer symmetric matrix for which it appears as an eigenvalue is at most of order $(n+\epsilon)(n+2)$, where ϵ is 1 or 0, depending on whether n is even or odd [4]. Recently, Mario Kummer improved this bound to $9n$ [66]. An affirmative answer to the weak Estes–Guralnick's conjecture would give us a bound of $2n$ for all those algebraic integers whose minimal polynomial is the minimal polynomial of an integer symmetric matrix. Recall that this bound is n or $n+1$ for rational symmetric matrices. It is not known whether the bound for integer symmetric matrices should be analogous to the rational case.

Proof of Theorem 2.2.5

We need the following results.

Proposition 2.2.12. [Ch. I, Prop. 3.5, 3] *Let $\mathcal{O}$ be a semilocal ring and let (L, β) be an $\mathcal{O}$-lattice such that L is proper. Then L has an orthonormal basis over $\mathcal{O}$.* □

The next lemma is attributed to Euler.

Lemma 2.2.13. [Ch. III, §1, 67] *An $\mathcal{O}$-lattice $(\mathcal{O}_{\boldsymbol{K}}, t_\delta)$ is unimodular for some $\delta \in \boldsymbol{K}^\times$.*

Proof. Let $f \in \mathbb{Z}[x]$ be an irreducible monic polynomial, $\mathcal{O}_{\mathbf{K}} = \mathbb{Z}[x]/(f)$ and $\mathbf{K}$ be the quotient field of $\mathcal{O}_{\mathbf{K}}$. Let $\delta = 1/f' \in \mathbf{K}^\times$, where f' is the derivative of f. Given that $\mathcal{O}_{\mathbf{K}}^{\vee\vee} = \mathcal{O}_{\mathbf{K}}$ (see [p. 231, 86]), it suffices to show that $\mathcal{O}_{\mathbf{K}}^{\vee} = \delta\mathcal{O}_{\mathbf{K}}$, for if $\mathcal{O}_{\mathbf{K}}^{\vee} = \delta\mathcal{O}_{\mathbf{K}}$ then

$$\begin{aligned}(\mathcal{O}_{\mathbf{K}}, t_\delta)^\vee &= \{\alpha \in \mathbf{K} \mid t_\delta(\alpha\mathcal{O}_{\mathbf{K}}) \subseteq \mathbb{Z}\}\\ &= \{\alpha \in \mathbf{K} \mid \operatorname{tr}(\alpha\delta\mathcal{O}_{\mathbf{K}}) \subseteq \mathbb{Z}\}\\ &= \{\alpha \in \mathbf{K} \mid \operatorname{tr}(\alpha\mathcal{O}_{\mathbf{K}}^{\vee}) \subseteq \mathbb{Z}\}\\ &= \mathcal{O}_{\mathbf{K}}.\end{aligned}$$

Let us consider the following equation

$$\frac{f(X)}{X-\alpha_1} = \prod_{j=2}^{n}(X-\alpha_j)$$

$$= b_0 + b_1X + \ldots + b_{n-1}X^{n-1}, \tag{2.2.1}$$

where $\alpha_1 \ldots, \alpha_n$ are the roots of f, $b_i \in \mathbf{K}$ and $b_{n-1} = 1$. We claim that

$$\sum_{i=1}^{n} \frac{f(X)}{X-\alpha_i}\frac{\alpha_i^j}{f'(\alpha_i)} = X^j.$$

Let

$$g_j(X) := \sum_{i=1}^{n} \frac{f(X)}{X-\alpha_i}\frac{\alpha_i^j}{f'(\alpha_i)} - X^j.$$

Now

$$f'(X) = \sum_{i=1}^{n}\prod_{\substack{j=1\\ j\neq i}}^{n}(X-\alpha_j),$$

which implies that $f'(\alpha_i) = \prod_{\substack{j=1\\ j\neq i}}^{n}(\alpha_i - \alpha_j)$. Therefore $\alpha_1, \ldots, \alpha_n$ are the roots of $g_j(X)$ for each $0 \leq j \leq n-1$. As degree of $g_j(X) \leq n-1$ we conclude that the $g_j(X)$ are the zero polynomials. Therefore

$$\operatorname{tr}\left(\frac{f(X)}{X-\alpha_1}\frac{\alpha_1^j}{f'(\alpha_1)}\right) = X^j,$$

where $\operatorname{tr} = \operatorname{tr}_{\mathbf{K}/\mathbf{F}}$ applied to each coefficient of the polynomial. From equation (2.2.1) and the additive property of the $\operatorname{tr}(\cdot)$ it follows that $\operatorname{tr}\left(\alpha_1^j \frac{b_i}{f'(\alpha_1)}\right) = \delta_{ij}$. Now $\left\{1, \alpha_1, \ldots, \alpha_1^{n-1}\right\}$ is a basis of $\mathcal{O}_{\mathbf{K}}$, and the above computation shows that $\{b_0\delta, \ldots, b_{n-1}\delta\}$ is the dual basis for $\mathcal{O}_{\mathbf{K}}^{\vee}$. Therefore, $\mathcal{O}_{\mathbf{K}}^{\vee} \subseteq \delta\mathcal{O}_{\mathbf{K}}$. And since $b_{n-1} = 1$ we have $\delta \in \mathcal{O}_{\mathbf{K}}^{\vee}$, and hence $\delta\mathcal{O}_{\mathbf{K}} \subseteq \mathcal{O}_{\mathbf{K}}^{\vee}$. Thus $\delta\mathcal{O}_{\mathbf{K}} = \mathcal{O}_{\mathbf{K}}^{\vee}$. □

Lemma 2.2.14. *Let S be a finite set of maximal ideals of $\mathcal{O}$. Let β be an associative symmetric bilinear $\mathcal{O}$-form on $\mathcal{O}_{\boldsymbol{K}}$ such that $(\mathcal{O}_{\boldsymbol{K}}, \beta)$ is a unimodular lattice. Then there exist $u, v \in \mathcal{O}_{\boldsymbol{K}}$ such that $u\beta(uv, v) \in \mathcal{O}_{\boldsymbol{K},S}^{\times}$.*

Proof. We want to show that for $u \in \mathcal{O}_{\mathbf{K},S}^{\times}$ and $v \in \mathcal{O}_{\mathbf{K}}$ we have $\beta(uv, v) \in \mathcal{O}_S^{\times}$, which will suffice for the proof of the lemma as $\mathcal{O}_{\mathbf{K},S}^{\times} \supset \mathcal{O}_S^{\times}$. Given that there exists a correspondence between the ideals in S and the maximal ideals of $\mathcal{O}_S$ [Ch. I, Prop. 11.1, 85], we can find elements satisfying conditions of the lemma over each maximal ideal and then with Chinese Remainder Theorem lift it over the whole ring. Thus without loss of generality we can assume that $\mathcal{O}$ is a local ring. Let $\mathfrak{m}$ be the maximal ideal of $\mathcal{O}$.

$$\mathcal{O}_{\mathbf{K}}/\mathfrak{m}\mathcal{O}_{\mathbf{K}} \cong \mathcal{O}_{\mathbf{K}}^{(1)} \times \ldots \times \mathcal{O}_{\mathbf{K}}^{(m)},$$

where each $\mathcal{O}_{\mathbf{K}}^{(i)}$ is a local ring. The quadratic form β induces an associative form,

$$\begin{aligned} \beta : \mathcal{O}_{\mathbf{K}}/\mathfrak{m}\mathcal{O}_{\mathbf{K}} \times \mathcal{O}_{\mathbf{K}}/\mathfrak{m}\mathcal{O}_{\mathbf{K}} &\longrightarrow \mathcal{O}/\mathfrak{m} \\ (b_1 + \mathfrak{m}\mathcal{O}_{\mathbf{K}}, b_2 + \mathfrak{m}\mathcal{O}_{\mathbf{K}}) &\mapsto \beta(b_1, b_2) + \mathfrak{m} \end{aligned}$$

Let X be the matrix of β with respect to a basis $\{1, \omega, \ldots, \omega^{n-1}\}$. As $(\mathcal{O}_{\mathbf{K}}, \beta)$ is a unimodular lattice, $\det(X)$ is a unit in $\mathcal{O}$, so $\det(X) \notin \mathfrak{m}$. Since

$$\beta : \mathcal{O}_{\mathbf{K}}/\mathfrak{m}\mathcal{O}_{\mathbf{K}} \times \mathcal{O}_{\mathbf{K}}/\mathfrak{m}\mathcal{O}_{\mathbf{K}} \longrightarrow \mathcal{O}/\mathfrak{m}$$

has the same matrix as $X \pmod{\mathfrak{m}}$ with respect to $\{1, \omega, \ldots, \omega^{n-1}\}$, and we have that $\det(X) \neq 0$, therefore $(\mathcal{O}_{\mathbf{K}}/\mathfrak{m}\mathcal{O}_{\mathbf{K}}, \beta)$ is a unimodular lattice.

Let $\mathbf{e}_i \in \mathcal{O}_{\mathbf{K}}/\mathfrak{m}\mathcal{O}_{\mathbf{K}}$ correspond to 1 in $\mathcal{O}_{\mathbf{K}}^{(i)}$ and 0 in all other $\mathcal{O}_{\mathbf{K}}^{(j)}$, i.e. $\mathbf{e}_i = (0, \ldots, 0, 1, 0, \ldots, 0)^t$. Let $u \in \mathcal{O}_{\mathbf{K}}^{(i)}$ and $v \in \mathcal{O}_{\mathbf{K}}^{(j)}$ for $i \neq j$. We have

$$\begin{aligned} \beta(u, v) &= \beta(u\mathbf{e}_i, v) \\ &= \beta(u, \mathbf{e}_i v) \\ &= \beta(u, 0) \\ &= 0. \end{aligned}$$

The bases for $\mathcal{O}_{\mathbf{K}}^{(1)}, \ldots, \mathcal{O}_{\mathbf{K}}^{(m)}$ give a basis for $\mathcal{O}_{\mathbf{K}}/\mathfrak{m}\mathcal{O}_{\mathbf{K}}$. The matrix of

$$\beta : \mathcal{O}_{\mathbf{K}}/\mathfrak{m}\mathcal{O}_{\mathbf{K}} \times \mathcal{O}_{\mathbf{K}}/\mathfrak{m}\mathcal{O}_{\mathbf{K}} \longrightarrow \mathcal{O}/\mathfrak{m}$$

with respect to this basis has a block diagonal form, with blocks giving the matrix of β restricted to the $\mathcal{O}_{\mathbf{K}}^{(i)}$. Since $(\mathcal{O}_{\mathbf{K}}/\mathfrak{m}\mathcal{O}_{\mathbf{K}}, \beta)$ is a unimodular lattice, the determinant of the matrix is invertible, hence so is the determinant of each block. Therefore, β restricted to each $\mathcal{O}_{\mathbf{K}}^{(i)}$ is unimodular.

We claim that there exists $u_1 \in \mathcal{O}_{\mathbf{K}}^{(1),\times}$, with $\beta(u_1, 1) \neq 0$. Since $(\mathcal{O}_{\mathbf{K}}, \beta)$ is unimodular, there exists $v_1 \in \mathcal{O}_{\mathbf{K}}^{(1)}$ with $\beta(v_1, 1) = 1$. If v_1 is a unit then put $v_1 = u_1$ and we are done. Else, if $\beta(1, 1) \neq 0$ put $u_1 = 1$. Otherwise, $\beta(1+v_1, 1) = \beta(1, 1) + \beta(v_1, 1)$ and put $u_1 = 1 + v_1$, which is a unit, since $\mathcal{O}_{\mathbf{K}}^{(1)}$ is a local ring.

Let $\overline{\mathbf{u}} = (u, 1, \ldots, 1)^t \in \mathcal{O}_{\mathbf{K}}/\mathfrak{m}\mathcal{O}_{\mathbf{K}}$ and $\overline{\mathbf{v}} = (1, 0, \ldots, 0)^t$. Then $\beta(\overline{\mathbf{u}\mathbf{v}}, \overline{\mathbf{v}}) \neq 0$ in $\mathcal{O}/\mathfrak{m}$. Let $u, v \in \mathcal{O}_{\mathbf{K}}$ such that $u + \mathfrak{m}\mathcal{O}_{\mathbf{K}} = \overline{\mathbf{u}}$, $v + \mathfrak{m}\mathcal{O}_{\mathbf{K}} = \overline{\mathbf{v}}$. As $\mathcal{O}$ is a local ring and $\beta(uv, v) \notin \mathfrak{m}$, we have that $\beta(uv, v) \in \mathcal{O}^\times$. □

Proposition 2.2.15. *Let $\mathcal{O}$ be a semilocalisation of $\mathbb{Z}$. Then there exists $\delta \in \boldsymbol{K}$ such that $(\mathcal{O}_{\boldsymbol{K}}, t_\delta)$ is proper and positive definite over $\mathbb{Q}$.*

Proof. From Lemma 2.2.13 we know that we can find $\delta \in \mathbf{K}^\times$ making our lattice unimodular. Our form is totally positive if $t_\delta(x, x) > 0$ for all $x \in \mathcal{O}_{\mathbf{K}}$. We can modify δ so that $\delta \in \mathrm{Sq}(\mathbf{K})$. As $\delta \in \mathbf{K}^\times$ there exists $\lambda \in \mathcal{O}_{\mathbf{K}}$ such that $\delta\lambda = q \in \mathbb{Q}$. Let $j \in \mathfrak{J}$, where $\mathfrak{J}$ is the Jacobson radical of $\mathcal{O}_{\mathbf{K}}$, and jq is large enough. By Proposition 2.1.31 we have $1 + j\lambda \in \mathcal{O}_{\mathbf{K}}^\times$ and $\delta(1+j\lambda) = \delta + jq > 0$ is a unit. Let $\delta' = \delta(1 + j\lambda)$. As δ' can be represented as a sum of squares it follows that $\mathrm{tr}(\delta' x^2) > 0$ for all $x \in \mathcal{O}_{\mathbf{K}}$.

To show that our form is proper it suffices to find $x \in \mathcal{O}_{\mathbf{K}}$ such that $t_\delta(x, x)$ is a unit in $\mathcal{O}$, and by definition the ideal generated by such element is the entire ring. By Lemma 2.2.14 adjusting δ by $u \in \mathcal{O}_{\mathbf{K}}^\times$ we achieve precisely the element we are looking for, thus $(\mathcal{O}_{\mathbf{K}}, t_\delta)$ is a proper lattice. □

Lemma 2.2.16. *Let $n \in \mathbb{Q}$, $n \geq 0$. Then there exists $A \in \mathrm{Mat}(4, \mathbb{Q})$ such that $AA^t = nI_4$.*

Proof. Given that n is a positive number, we can represent it as a sum of four squares. In particular $n = a^2 + b^2 + c^2 + d^2$, where $a, b, c, d \in \mathbb{Q}$. We define the following matrix

$$A = \begin{pmatrix} a & b & c & -d \\ b & -a & d & c \\ c & -d & -a & -b \\ d & c & -b & a \end{pmatrix}.$$

Clearly $AA^t = nI_4$. □

Notice that the matrix in the lemma above is almost always not invertible over the integers, as $\det(AA^t) = \det(A)^2 = n^4$.

Proof of Theorem 2.2.5. Let $f \in \mathcal{O}[x]$ satisfy the hypothesis of the theorem. Then by Proposition 2.2.15 we can find a lattice, say (L, β), such that it is unimodular, proper and positive definite over the $\mathbb{Q}$, and so by Proposition 2.2.12 such lattice has an orthogonal basis. In particular it implies that there exists a basis $\{\omega_1, \ldots, \omega_n\}$ such that $\beta(\omega_i, \omega_j) = A_{ij}\delta_{ij}$, where by positive definiteness we have that $A_{ii} > 0$ for $1 \leq i \leq n$. The corresponding matrix is $A := \operatorname{diag}(A_{11}, \ldots, A_{nn})$. Construct a matrix $A^* := A \oplus A \oplus A \oplus A$ (by a direct sum we mean a block diagonal matrix with blocks of A). We can permute the matrix so that $A^* = A_1 \oplus A_2 \oplus \ldots \oplus A_n$, where each $A_i := \operatorname{diag}(A_{ii}, \ldots, A_{ii}) \in \operatorname{Mat}(4, \mathcal{O})$. By Lemma 2.2.16 there exists a matrix M_i such that $M_i M_i^t = A_i$, therefore $A_i \sim_{\mathcal{O}} I_4$. So we can construct a block diagonal matrix $M := \operatorname{diag}(M_1, \ldots, M_n)$ such that $MM^t = A^*$, thus $A^* \sim_{\mathcal{O}} I_{4n}$ and the theorem follows. □

2.2.2 Lattices over global rings

In this section we demonstrate that the existence of an odd positive definite unimodular lattice over the rational integers with a self-adjoint operator acting on it is equivalent to the existence of a unimodular definite lattice over the integers of a totally real field. Let $\mathcal{O}$ be a commutative integral domain, let $\mathbf{F}$ be the quotient field of $\mathcal{O}$. Let $\mathcal{O}_{\mathbf{K}}$ be a commutative domain that contains $\mathcal{O}$ and let $\mathbf{K}$ be its quotient field. Let $\operatorname{tr} : \mathcal{O}_{\mathbf{K}} \longrightarrow \mathcal{O}$ be the trace map and

(V, β) be a nonsingular $\mathbf{K}$-space. Let L be an $\mathcal{O}_{\mathbf{K}}$-lattice. We will need the following result.

Theorem 2.2.17. [Thm. 11.3, 74] *Let $\mathcal{O}_{\boldsymbol{K}}$ be an integral domain, and $\mathfrak{a}$ be a fractional ideal of $\mathcal{O}_{\boldsymbol{K}}$. The following are equivalent:*

(i) *$\mathfrak{a}$ is an invertible ideal;*

(ii) *$\mathfrak{a}$ is a projective ideal;*

(iii) *$\mathfrak{a}$ is a finitely generated $\mathcal{O}_{\boldsymbol{K}}$ ideal and for every prime $\mathfrak{p}$ in $\mathcal{O}_{\boldsymbol{K}}$, $\mathfrak{a}\mathcal{O}_{\boldsymbol{K},\mathfrak{p}}$ is a principal ideal in $\mathcal{O}_{\boldsymbol{K},\mathfrak{p}}$.* □

By a projective ideal $\mathfrak{a}$ we understand $\mathfrak{a}$ as an $\mathcal{O}$-module that is projective.

Lemma 2.2.18. *Let $\mathfrak{a}$ be an invertible fractional ideal of $\mathcal{O}_{\boldsymbol{K}}$ and $(\mathfrak{a}, t_\delta)$ be a unimodular $\mathcal{O}$-lattice. Then the $\mathcal{O}$-lattice $(\mathfrak{a}L, t_\delta \circ \beta)$ is unimodular if and only if (L, β) is a unimodular $\mathcal{O}_{\boldsymbol{K}}$-lattice.*

Proof. First, note that from the theorem above we have that $\mathfrak{a}_{\mathfrak{p}} = \mathfrak{a}\mathcal{O}_{\mathbf{K},\mathfrak{p}}$ is a principal ideal in $\mathcal{O}_{\mathbf{K},\mathfrak{p}}$ for every maximal ideal $\mathfrak{p}$ in $\mathcal{O}_{\mathbf{K}}$. Given that the lattice is unimodular over $\mathcal{O}_{\mathbf{K}}$ if and only if it is unimodular over $\mathcal{O}_{\mathbf{K},\mathfrak{p}}$, for every maximal ideal $\mathfrak{p}$, it will suffice to prove the lemma locally. Let $\mathfrak{p}$ be any maximal ideal in $\mathcal{O}_{\mathbf{K}}$, then $\mathfrak{a}_{\mathfrak{p}} = \alpha\mathcal{O}_{\mathbf{K},\mathfrak{p}}$, $(\mathfrak{a}_{\mathfrak{p}}, t_\delta)$ is isometric to $(\mathcal{O}_{\mathbf{K},\mathfrak{p}}, t_\delta)$ and $(\mathfrak{a}_{\mathfrak{p}}L_{\mathfrak{p}}, t_\delta \circ \beta)$ is isometric to $(L_{\mathfrak{p}}, t_\delta \circ \beta)$ (considering the facts that $\mathcal{O}_{\mathbf{K},\mathfrak{p}}L_{\mathfrak{p}} = L_{\mathfrak{p}}$ and the existence of the isometry $\sigma_\alpha : \mathfrak{a}_{\mathfrak{p}}L_{\mathfrak{p}} \longrightarrow L_{\mathfrak{p}}$ that "forgets" α, i.e. $\sigma(\alpha bm) = bm$, for all $b \in \mathcal{O}_{\mathbf{K},\mathfrak{p}}$ and $m \in L_{\mathfrak{p}}$). In particular we can assume that $\mathfrak{a}_{\mathfrak{p}} = \mathcal{O}_{\mathbf{K},\mathfrak{p}}$. Therefore $(L_{\mathfrak{p}}, \beta)^\vee = (L_{\mathfrak{p}}, t_\delta \circ \beta)^\vee$, as

$$\begin{aligned}(L_{\mathfrak{p}}, t_\delta \circ \beta)^\vee &= \{x \in \mathbf{K} \mid t_\delta \circ \beta(xL_{\mathfrak{p}}) \subset \mathcal{O}_{\mathfrak{p}}\} \\ &= \{x \in \mathbf{K} \mid \beta(xL_{\mathfrak{p}}) \subset \mathcal{O}_{\mathbf{K},\mathfrak{p}}\} \\ &= (L_{\mathfrak{p}}, \beta)^\vee.\end{aligned}$$

□

Parts of the above result can be traced back to J. Milnor and to M. Knebusch and W. Scharlau [Lemma 3.4, 63].

Lemma 2.2.19. *Let* $\boldsymbol{K}$ *be a totally real field extension of* $\boldsymbol{F}$*. Then* (V, β) *is totally positive definite over* $\boldsymbol{K}$ *if and only if* $(V, \mathrm{tr} \circ \beta)$ *is totally positive definite over* $\boldsymbol{F}$*.*

Proof. Let V be a $\mathbf{K}$-space. If β is a positive definite bilinear form over V then clearly $\mathrm{tr} \circ \beta$ is positive definite too, as $\beta(x,x) \gg 0$ for all $x \in V$ and the trace of a totally positive element is positive by definition. Given that $\mathbf{K}$ has characteristic zero we can find an orthogonal basis for (V, β). Thus we can assume that $\mathrm{tr} \circ \beta$ is of dimension one, i.e. $\beta(x,x) = \alpha x^2$ and thus $\mathrm{tr} \circ \beta = t_\alpha$, where $\alpha \in \mathbf{K}$. The bilinear form β is positive definite if and only if $\alpha \gg 0$. Let $\{\omega_1, \ldots, \omega_n\}$ be a basis of $\mathbf{K}$ over $\mathbf{F}$. Let $x = \sum_{i=1}^n \gamma_i \omega_i$, $\gamma_i \in \mathbf{F}$. Then

$$\begin{aligned} \mathrm{tr}\alpha x^2 &= \mathrm{tr}\alpha \left(\sum_{i=1}^n \gamma_i \omega_i \right)^2 \\ &= \boldsymbol{\gamma}^t B^t \mathrm{diag}(\alpha_1, \ldots, \alpha_n) B \boldsymbol{\gamma}, \end{aligned}$$

where $\boldsymbol{\gamma} \in \mathbf{F}^n$, $\sigma_i : \mathbf{K} \hookrightarrow \mathbb{R}$ is an $\mathbf{F}$-embedding, $B \in \mathrm{Mat}(n, \mathbf{K})$ such that $B_{ij} = \sigma_i(\omega_j)$, and $\alpha_i = \sigma_i(\alpha)$. As a basis is linearly independent, B is invertible over $\mathbf{K}$. We have that $\mathrm{tr} \circ \beta$ is equivalent to $\mathrm{diag}(\alpha_1, \ldots, \alpha_n)$ and thus $\mathrm{tr} \circ \beta$ is positive definite if and only if $\mathrm{diag}(\alpha_1, \ldots, \alpha_n)$ is positive definite. The latter is valid if and only if each $\alpha_i > 0$. Therefore $\alpha \gg 0$ and β is a positive definite bilinear form as was required to show. □

Definition 2.2.20. *Let* $f = x^n + a_1 x^{n-1} + \ldots + a_n \in \mathcal{O}[x]$*. We define the* ***companion matrix*** *of* f *to be* $C_f \in \mathrm{Mat}(n, \mathcal{O})$*, such that*

$$C_f := \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_n \\ 1 & 0 & \cdots & 0 & -a_{n-1} \\ 0 & 1 & \cdots & 0 & -a_{n-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_1 \end{pmatrix}$$

and $\chi_{C_f} = f$*.*

Lemma 2.2.21. *Let f be a monic polynomial of degree n and let C_f be its companion matrix. Then for every $n \times n$ matrix X that satisfies $XC_f = C_f^t X$ we have that $X_i = X_1 C_f^{i-1}$, where X_j is the j-th row of X, and $i = 1, \ldots, n$.*

Proof. Let $X \in \mathrm{Mat}(n, \mathbf{F})$ such that $XC_f = C_f^t X$, where C_f is the companion matrix of polynomial $f = x^n + a_1 x^{n-1} + \ldots + a_n$, represented in the form

$$C_f = \left(\begin{array}{c|c} \mathbf{0}^t & \\ \hline I_{n-1} & \mathbf{f} \end{array} \right),$$

where $\mathbf{0}$ is an n dimensional zero vector and $\mathbf{f} = (-a_n, \ldots, -a_1)^t \in \mathbf{F}^n$. Let

$$X = \left(\begin{array}{c} \mathbf{v}^t \\ \hline X' \end{array} \right), \tag{2.2.2}$$

where $\mathbf{v} \in \mathbf{F}^n$ and $X' \in \mathrm{Mat}(n-1, n, \mathbf{F})$. Then

$$\begin{aligned} XC_f &= \left(\begin{array}{c} \mathbf{v}^t C_f \\ \hline X' C_f \end{array} \right) \qquad (2.2.3) \\ &= C_f^t X \\ &= \left(\begin{array}{c} X' \\ \hline \mathbf{f}^t X \end{array} \right). \qquad (2.2.4) \end{aligned}$$

Therefore

$$\begin{aligned} X_1' &= (XC_f)_1 \\ &= X_1 C_f. \qquad (2.2.5) \end{aligned}$$

From equation (2.2.3) we have that $X_i C_f = X_{i-1}' C_f$ for $i = 2, \ldots, n$, while from equation (2.2.4) we have that $X_i C_f = X_i'$ for $i = 1, \ldots, n-1$. Given equation (2.2.2) we conclude that

$$\begin{aligned} X_{i+1} &= X_i' \\ &= X_{i-1}' C_f \\ &= X_1 C_f^i \end{aligned}$$

for $i = 2, \ldots, n-1$. Therefore in the light of equation (2.2.5) the lemma follows. □

Although the consequences of the lemma above is well known, we believe that the explicit construction is new.

Corollary 2.2.22. *Let $\boldsymbol{K}$ be a finite separable extension of a field $\boldsymbol{F}$ such that $[\boldsymbol{K} : \boldsymbol{F}] = n$. Let V be a finite dimensional vector space over $\boldsymbol{K}$. If an $\boldsymbol{F}$-lattice (V, γ) is such that $\boldsymbol{K}$ acts on (V, γ) as self-adjoint operators, then there exists a symmetric bilinear $\boldsymbol{K}$-form β such that $\gamma = \operatorname{tr} \circ \beta$.*

Proof. Let $\mathbf{K} = \mathbf{F}[\alpha]$ and let $f = x^n + a_1 x^{n-1} + \ldots + a_n \in \mathbf{F}[x]$ be the minimal polynomial of α. Let C_f be the companion matrix of f. Consider the space of $\mathbf{F}$-bilinear forms of rank r on which $\mathbf{K}$ acts as self-adjoint operators,

$$\{A \in \operatorname{Sym}(rn, \mathbf{F}) \mid A\overline{C_f} = \overline{C_f}^t A\}, \tag{2.2.6}$$

where $\overline{C_f} = \operatorname{diag}(C_f, \ldots, C_f)$ is a block diagonal matrix with r blocks of matrix C_f. We claim that this space has dimension $\dfrac{nr(r+1)}{2}$ over $\mathbf{F}$. First, by the previous lemma we have that the space of matrices X that satisfies $XC_f = C_f^t X$ is n dimensional, as for a given matrix C_f we can only freely choose the first row in X. Second, every matrix in the set (2.2.6) can be written as $\dfrac{r(r+1)}{2}$ blocks of matrices Y that satisfy $YC_f = C_f^t Y$. Thus this is a space of dimension $\dfrac{nr(r+1)}{2}$ over $\mathbf{F}$, as was claimed.

Clearly $\mathbf{K}$ acts on $(V, \operatorname{tr} \circ \beta)$ as self-adjoint operators, as V is a $\mathbf{K}$-space. Thus,

$$(V, \operatorname{tr} \circ \beta) \subset \{A \in \operatorname{Sym}(rn, \mathbf{F}) \mid A\overline{C} = \overline{C}^t A\}.$$

Given that the $\mathbf{F}$-dimension of this space is $\dfrac{nr(r+1)}{2}$, the corollary follows. □

Proposition 2.2.23. [Lemma 3.1, 34] *Let $r \in \mathbb{N}$, $\mathcal{O}_{\boldsymbol{K}}$ be a ring of integer of a finite field extension $\boldsymbol{K}$ of $\boldsymbol{F}$. The following are equivalent:*

(i) There exists a positive definite unimodular $\boldsymbol{F}$-lattice (L, β) of rank nr such that $\mathcal{O}_{\boldsymbol{K}}$ acts as self-adjoint operators on L.

(ii) There exists a unimodular $\mathcal{O}_{\boldsymbol{K}}$-lattice (M, α) of rank r such that $(\boldsymbol{K}M, \delta\alpha)$ is a totally positive definite lattice, for some $\delta \in \boldsymbol{K}$.

Proof. Let us assume that (i) holds. Then by Corollary 2.2.22 it follows that there exists a $\mathbf{K}$-bilinear form γ such that $(L, \beta) = (L, \operatorname{tr} \circ \gamma)$. Let $\mathfrak{a}$ be an invertible fractional ideal of $\mathcal{O}_{\mathbf{K}}$ and let $\delta \in \mathbf{K}$ such that $(\mathfrak{a}, t_\delta)$ is a unimodular $\mathcal{O}$-lattice. We know that such δ exists from Lemma 2.2.13. Let us define $M = \mathfrak{a}^{-1}L$. Then by Lemma 2.2.18 if $(\mathfrak{a}M, t_\delta \circ \delta^{-1}\gamma)$ is unimodular then so is $(M, \delta^{-1}\gamma)$. Lemma 2.2.19 implies that $(\mathbf{K}M, \gamma)$ is a positive definite lattice, thus letting $\alpha = \delta^{-1}\gamma$ it follows that $(\mathbf{K}M, \delta\alpha)$ is a positive definite lattice, thus (ii) follows.

Now let us assume that (ii) holds. Let $\mathfrak{a}$ be an invertible fractional $\mathcal{O}_{\mathbf{K}}$-ideal such that $(\mathfrak{a}, t_\delta)$ is a unimodular lattice. Then by Lemma 2.2.18 it follows that $(\mathfrak{a}M, t_\delta \circ \alpha)$ is a positive definite unimodular $\mathcal{O}$-lattice. Obviously, $\mathcal{O}_{\mathbf{K}}$ acts on it as self-adjoint operators. Thus (ii) implies (i). □

Quintic polynomials

In this final section we list some of the conditions under which a given quintic polynomial is the minimal polynomial of an integer symmetric matrix.

Conjecture 2.2.24. Estes–Guralnick's conjecture holds true for quintic polynomials.

We computed all the 5×5 positive definite integer symmetric matrices of traces 9, 10 and 11. Then we compared the irreducible quintic polynomials that appeared as characteristic polynomials of those matrices with the complete list of minimal polynomials of totally real algebraic integers up to trace 11 (those polynomials can be found in [103]). Those polynomials that did not appear as characteristic polynomials of integer symmetric matrices, were found to be minimal polynomial of 10×10 integer symmetric matrices, by applying either construction that can be found in Estes and Guralnick's paper, or the one described below. Therefore we confirmed the above conjecture for all the quintic polynomials with only positive roots up to trace 11. This may not constitute as a strong evidence, however all the known counterexamples of Estes–Guralnick's conjecture can be categorised as either polynomials with small trace, small discriminant or small span of roots.

Definition 2.2.25. *Let (L, β) be a positive definite lattice. We denote by*

$$\min(L, \beta) := \min\{\beta(v, v) \mid 0 \neq v \in L\}$$

*the **minimum** of (L, β), and by*

$$\mathcal{M}(L, \beta) := \{v \in L \mid \beta(v, v) = \min(L, \beta)\}$$

the set of the minimal vectors of L.

We will write $\min(L)$ and $\mathcal{M}(L)$ if the quadratic form β is clear from the context. Given that $\beta(v, v)$ is a quadratic form, if $v \in L$ is in $\mathcal{M}(L)$ then $-v \in \mathcal{M}(L)$ too, and therefore $|\mathcal{M}(L)| \equiv 0 \pmod 2$. For example $|\mathcal{M}(I_n)| = 2n$.

Let (L, β) be a unimodular binary quadratic lattice over $\mathcal{O}_{\mathbf{K}}$. Let $\mathbf{K}$ be the quotient field of $\mathcal{O}_{\mathbf{K}}$ and $(\mathbf{K}L, \delta\beta)$ be a totally positive definite for some $\delta \in \mathbf{K}$. Then by Proposition 2.2.23 we know that $\mathcal{O}_{\mathbf{K}}$ acts as self-adjoint operators on $(L, t_\delta \circ \beta)$. From the classifications of positive definite unimodular lattices we gather that L is either I_{10} or $I_2 \oplus E_8$, where E_8 is an even unimodular lattice of rank 8. Now, $|\mathcal{M}(I_2 \oplus E_8)| = 4$, thus if we can show that our lattice has $|\mathcal{M}(L)| > 4$ then necessarily $L \sim_{\mathbb{Z}} I_{10}$. More generally we have:

Lemma 2.2.26. *Let $\boldsymbol{K}$ be a totally real number field of degree n and let $\mathcal{O}_{\boldsymbol{K}}$ be a ring of integers in $\boldsymbol{K}$. Let (L, β) be a unimodular $\mathcal{O}_{\boldsymbol{K}}$-lattice of rank r such that $(\boldsymbol{K}L, \delta\beta)$ is a totally positive definite for some $\delta \in \boldsymbol{K}$. If $\min(L, t_\delta \circ \beta) = 1$ and $\frac{1}{2}|\mathcal{M}(L, t_\delta \circ \beta)| > nr - 8$ then $L \sim_{\mathbb{Z}} I_{rn}$.*

Proof. Given that $\frac{1}{2}|\mathcal{M}(L, t_\delta \circ \beta)| > nr - 8$ implies that $L \sim_{\mathbb{Z}} I_{nr-7} \oplus M$ where M is a positive definite unimodular lattice of rank 7. In particular, M is odd, and therefore by Theorem 2.2.1 we have that $M \sim_{\mathbb{Z}} I_7$, thus $L \sim_{\mathbb{Z}} I_{rn}$, as was required to show. □

Let $f \in \mathbb{Z}[x]$ be an irreducible monic polynomial such that all its roots are real, $\mathcal{O}_{\mathbf{K}} = \mathbb{Z}[x]/(f)$ and $\mathbf{K}$ is the quotient field of $\mathcal{O}_{\mathbf{K}}$. Let $\delta = 1/f' \in \mathbf{K}^\times$, where f' is the derivative of f. Let $A \in \mathrm{Sym}(r, \mathcal{O}_{\mathbf{K}})$. We shall write $A^\aleph$ if $A \in \mathrm{GL}(r, \mathcal{O}_{\mathbf{K}})$ and δA is a positive definite matrix. Let $\gamma_m \subset \mathcal{O}_{\mathbf{K}}$ be the set of elements $\alpha \in \mathcal{O}$ such that $\delta\alpha \gg 0$ and $\frac{1}{2}|\mathcal{M}(\mathcal{O}, t_{\delta\alpha})| \geq m$, where $m \in \mathbb{N}$. We denote by

$$\begin{pmatrix} \gamma_x & * & \cdots & * \\ * & * & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ * & * & \cdots & * \end{pmatrix} \subset \mathrm{Sym}(n, \mathcal{O}_{\mathbf{K}})$$

a set of $n \times n$ matrices such that the top diagonal entry comes from the set γ_x. Now if we write

$$\begin{pmatrix} \gamma_x & * & \cdots & * \\ * & * & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ * & * & \cdots & * \end{pmatrix}^\aleph$$

then we state that there exists

$$A \in \begin{pmatrix} \gamma_x & * & \cdots & * \\ * & * & \cdots & * \\ \vdots & \vdots & \ddots & \vdots \\ * & * & \cdots & * \end{pmatrix}$$

such that $A^\aleph$.

Example 2.2.27. (*i*) Let $f = x^2 - 3$ and $\mathbb{Z}[x]/(f) \cong \mathbb{Z}[\sqrt{3}]$. Then $\delta = \dfrac{1}{2\sqrt{3}}$ and $\gamma_1 = \{\sqrt{3} - 1, \sqrt{3}, \sqrt{3} + 1\}$. Consider the matrix

$$M = \begin{pmatrix} \sqrt{3} + 1 & 1 \\ 1 & \sqrt{3} - 1 \end{pmatrix}.$$

As $\det(M) = 1$ we have that $M \in \mathrm{GL}(2, \mathbb{Z}[\sqrt{3}])$. Furthermore, $\delta M \gg 0$, therefore $\begin{pmatrix} \gamma_1 & * \\ * & \gamma_1 \end{pmatrix}^{\aleph}$ is not empty over $\mathbb{Z}[\sqrt{3}]$. Let (L, α) be a $\mathbb{Z}[\sqrt{3}]$-lattice such that the corresponding matrix of α is M, i.e (L, α) is a unimodular lattice of rank 2 such that $(\mathbb{Q}(\sqrt{3})L, \delta\alpha)$ is a totally positive definite lattice. By Proposition 2.2.23 we deduce that there exists a positive definite unimodular $\mathbb{Z}$-lattice (L, β) of rank 4 such that $\mathbb{Z}[\sqrt{3}]$ acts on it as self-adjoint operators. Now $\frac{1}{2}|\mathcal{M}(L, \beta)| \geq 2$ as $\beta = t_\delta \circ \alpha$ and $t_\delta \circ \alpha((1, 0)^t, (1, 0)^t) = 1$ (the same holds for vector $(0, 1)^t$). From Lemma 2.2.26 it follows that $L \sim_{\mathbb{Z}} I_4$ (actually the minimal vector data is redundant in this case, as the rank of the lattice is low enough to achieve the same result directly from the classification of unimodular lattice). And therefore we show again that $x^2 - 3$ is the minimal polynomial of an integer symmetric matrix.

(ii) Let $f = x^5 - 10x^4 + 32x^3 - 37x^2 + 12x - 1$, f is an irreducible polynomial with only real roots. Let $\alpha \in \mathbb{R}$ be one of the roots of f and $\mathbb{Z}[x]/(f) \cong \mathbb{Z}[\alpha]$. We denote by $\mathbf{K}$ the quotient field of $\mathbb{Z}[\alpha]$, and let $\delta = \dfrac{1}{f'(\alpha)}$. We have that $\mathrm{tr}_{\mathbf{K}/\mathbb{Q}}(\alpha^i) = 10, 36, 151$ and 680 for $i = 1, \ldots, 4$, respectively. We can check that $\{\alpha^4 - 7\alpha^3 + 14\alpha^2 - 9\alpha + 1, \alpha^4 - 7\alpha^3 + 14\alpha^2 - 7\alpha + 1, \alpha^4 - 7\alpha^3 + 16\alpha^2 - 13\alpha + 2\} \subset \gamma_3$. Let

$$M = \begin{pmatrix} \alpha^4 - 7\alpha^3 + 14\alpha^2 - 7\alpha + 1 & \alpha^3 - 3\alpha^2 + \alpha \\ \alpha^3 - 3\alpha^2 + \alpha & \alpha^4 - 7\alpha^3 + 14\alpha^2 - 8\alpha + 1 \end{pmatrix}.$$

Given that $M \in \mathrm{GL}(2, \mathbb{Z}[\alpha])$ and $\delta M \gg 0$ implies that $\begin{pmatrix} \gamma_3 & * \\ * & * \end{pmatrix}^{\aleph}$ is not empty over $\mathbb{Z}[\alpha]$. Let (L, β) be a $\mathbb{Z}[\alpha]$-lattice such that the corresponding matrix for β is M. In the light of the lemma above, $(L, t_\delta \circ \beta) \sim_{\mathbb{Z}} I_{10}$, thus f is the minimal polynomial of an integer symmetric matrix.

Proposition 2.2.28. *Let $f \in \mathbb{Z}[x]$ be an irreducible quintic monic polynomial such that the roots of f are all real. Let $\mathcal{O} = \mathbb{Z}[x]/(f)$. If there exists*

$\gamma_1, \gamma_2, \gamma_3, \gamma_4$ *or* $\gamma_5 \subset \mathcal{O}$ *such that at least one of*

$$\begin{pmatrix}\gamma_5\end{pmatrix}, \begin{pmatrix}\gamma_3 & * \\ * & *\end{pmatrix}^{\aleph}, \begin{pmatrix}\gamma_2 & * \\ * & \gamma_2\end{pmatrix}^{\aleph}, \begin{pmatrix}\gamma_4 & * & * \\ * & \gamma_4 & * \\ * & * & *\end{pmatrix}^{\aleph}, \begin{pmatrix}\gamma_4 & * & * \\ * & \gamma_3 & * \\ * & * & \gamma_1\end{pmatrix}^{\aleph}, \begin{pmatrix}\gamma_3 & * & * \\ * & \gamma_3 & * \\ * & * & \gamma_2\end{pmatrix}^{\aleph},$$

$$\begin{pmatrix}\gamma_4 & * & * & * \\ * & \gamma_4 & * & * \\ * & * & \gamma_4 & * \\ * & * & * & \gamma_1\end{pmatrix}^{\aleph}, \begin{pmatrix}\gamma_4 & * & * & * \\ * & \gamma_4 & * & * \\ * & * & \gamma_3 & * \\ * & * & * & \gamma_2\end{pmatrix}^{\aleph}, \begin{pmatrix}\gamma_4 & * & * & * \\ * & \gamma_3 & * & * \\ * & * & \gamma_3 & * \\ * & * & * & \gamma_3\end{pmatrix}^{\aleph},$$

$$\begin{pmatrix}\gamma_4 & * & * & * & * \\ * & \gamma_4 & * & * & * \\ * & * & \gamma_4 & * & * \\ * & * & * & \gamma_4 & * \\ * & * & * & * & \gamma_2\end{pmatrix}^{\aleph}, \begin{pmatrix}\gamma_4 & * & * & * & * \\ * & \gamma_4 & * & * & * \\ * & * & \gamma_4 & * & * \\ * & * & * & \gamma_3 & * \\ * & * & * & * & \gamma_3\end{pmatrix}^{\aleph}, \begin{pmatrix}\gamma_4 & * & * & * & * & * \\ * & \gamma_4 & * & * & * & * \\ * & * & \gamma_4 & * & * & * \\ * & * & * & \gamma_4 & * & * \\ * & * & * & * & \gamma_4 & * \\ * & * & * & * & * & \gamma_3\end{pmatrix}^{\aleph},$$

$$\begin{pmatrix}\gamma_4 & * & * & * & * & * & * \\ * & \gamma_4 & * & * & * & * & * \\ * & * & \gamma_4 & * & * & * & * \\ * & * & * & \gamma_4 & * & * & * \\ * & * & * & * & \gamma_4 & * & * \\ * & * & * & * & * & \gamma_4 & * \\ * & * & * & * & * & * & \gamma_4\end{pmatrix}^{\aleph}$$

is not empty over $\mathcal{O}$*, then* f *is the minimal polynomial of an integer symmetric matrix.*

Proof. Let $f \in \mathbb{Z}[x]$ be an irreducible quintic monic polynomial such that the roots of f are all real. Let $\mathcal{O} = \mathbb{Z}[x]/(f)$. By Proposition 2.2.23 we have that if any of the above sets is not empty then there exist a matrix in $\mathrm{Sym}(r, \mathcal{O}) \subset \mathrm{GL}(r, \mathcal{O})$, and thus a positive definite $\mathbb{Z}$-lattice (L, β) of rank $5r$, such that $\mathcal{O}$ act on it as self-adjoint operators. Furthermore, due to the restrictions of the possible elements on the diagonal of such matrices, we will have that for each of such lattice $\frac{1}{2}|\mathcal{M}(L, \beta)| > nr - 8$. Therefore, by Lemma 2.2.26 the proposition follows. □

Part II

Counterexamples

Chapter 3

Linear algebraic études

In this chapter we introduce some necessary conditions for the existence of an integer symmetric matrix with a given minimal polynomial. These conditions derive almost exclusively from the linear algebraic considerations. The main new result of this chapter is Theorem 3.2.1, which appeared in [82]. As a corollary we will find counterexamples to Estes–Guralnick's conjecture, some previously unknown. Moreover we are able to settle the Schur–Siegel–Smyth trace problem for polynomials that are minimal polynomials of integer symmetric matrices. In the end of this chapter we will take a little detour in introducing a new class of matrices, totally nonnegative matrices, for which we can pose an analogous problem to Estes–Guralnick's conjecture and the Schur–Siegel–Smyth trace problem. Throughout the chapter there will be sporadic references to graph theory; we consulted [46] for everything graph-related that we required.

3.1 Elementary methods

The following theorem will play a crucial role throughout the chapter.

Theorem 3.1.1 (Cauchy Interlacing Theorem)**.** [Thm. 9.1.1, 46] *Let* $A \in \mathrm{Sym}(n, \mathbb{R})$ *have eigenvalues* $\lambda_1 \geq \ldots \geq \lambda_n$ *and let* $A' \in \mathrm{Sym}(n-1, \mathbb{R})$ *be a principal submatrix of* A*, where* $\mu_1 \geq \ldots \geq \mu_{n-1}$ *are the eigenvalues of* A'*.*

Then the eigenvalues of A and A' interlace, i.e.

$$\lambda_1 \geq \mu_1 \geq \lambda_2 \geq \ldots \geq \mu_{n-1} \geq \lambda_n. \qquad \square$$

It will be useful to associate to a given $A \in \mathrm{Sym}(n, \mathbb{Z})$ a simple graph on n vertices labelled $1, \ldots, n$, defined as follows: the vertices of the graph, i and j, are connected by an edge if and only if $A_{ij} \neq 0$. Note that we ignore the values on the diagonal of the matrix.

Definition 3.1.2. *Let $A \in \mathrm{Sym}(n, \mathbb{Z})$. We say that A is **indecomposable** (or **connected**) if for all permutation matrices P, PAP^t is not a block diagonal matrix with more than one block.*

Remark. By a permutation matrix P we mean a square (0,1)-matrix such that in each row and column there exists a single entry of one, and zeros elsewhere. It is well known that $\det(P) = \pm 1$ and $PP^t = I_n$.

If a symmetric matrix A is indecomposable then in each row and column of A there exists at least one nonzero off-diagonal entry. The name connected is coined from graph theory, as an indecomposable symmetric matrix will correspond to a connected simple graph. More can be said if a give matrix is also nonnegative (see [p.178, 46]). Given a not connected (or **decomposable**) symmetric matrix A, we can permute its basis so that we gain a block diagonal matrix with more than one block, i.e. there exists a permutation matrix P such that

$$PAP^t = A_1 \oplus \ldots \oplus A_k.$$

The characteristic polynomial of such matrix A is reducible, as

$$\chi_A = \prod_{i=1}^{k} \chi_{A_i}.$$

Thus a necessary condition for a matrix to have an irreducible characteristic polynomial is to be indecomposable. However it is not sufficient; see for example

$$\begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}.$$

This matrix is connected but its characteristic polynomial is $(x-3)(x-1)$.

We will need the following proposition.

Proposition 3.1.3 (Maclaurin's inequality)**.** [27] *Let* $\alpha_1, \ldots, \alpha_n \in \mathbb{R}_+$ *and* $n \in \mathbb{N}$. *Then*

$$M_1 \geq \sqrt[2]{M_2} \geq \ldots \geq \sqrt[n]{M_n},$$

where

$$M_k := \frac{\sum_{1 \leq i_1 < \ldots < i_k \leq n} \alpha_{i_1} \ldots \alpha_{i_k}}{\binom{n}{k}}. \qquad \square$$

Let us recall the Leibniz formula for determinants ([p. 95, 57]). For $A \in \mathrm{Mat}(n, \mathbb{Z})$ we have

$$\det(A) = \sum_{\sigma \in S_n} \mathrm{sign}(\sigma) \prod_{i=1}^{n} A_{\sigma(i)i},$$

where S_n is the symmetric group on n elements, and $\mathrm{sign}(\cdot)$ is the sign function, i.e.

$$\mathrm{sign} : S_n \longrightarrow \{\pm 1\},$$

such that for $\sigma \in S_n$ the $\mathrm{sign}(\sigma) = 1$ if and only if σ is an even permutation. We are interested in the characteristic polynomial of a symmetric matrix A, i.e.

$$\begin{aligned} \chi_A :&= \det(xI_n - A) \\ &= x^n - a_1 x^{n-1} + \ldots + (-1)^n a_n, \end{aligned}$$

where $a_1 = \mathrm{Tr}(A)$ and $a_n = \det(A)$.

Example 3.1.4. Consider a coefficient a_2 of x^{n-2} in χ_A. We claim that

$$a_2 = \sum_{1 \leq i < j \leq n} A_{ii} A_{jj} - \sum_{1 \leq i < j \leq n} A_{ij} A_{ji}.$$

From the Leibniz formula it follows that

$$\begin{aligned}\chi_A &= \det(xI_n - A)\\ &= \sum_{\sigma\in S_n} \operatorname{sign}(\sigma)\prod_{i=1}^{n}(xI_n - A)_{\sigma(i)i}.\end{aligned}$$

For $1 \in S_n$ we have a contribution of

$$\prod_{i=1}^{n}(x - A_{ii}) = x^n - \sum_{i=1}^{n} A_{ii}x^{n-1} + \sum_{1\leq i<j\leq n} A_{ii}A_{jj}x^{n-2} - \ldots,$$

and thus $\sum_{1\leq i<j\leq n} A_{ii}A_{jj}$ will contribute to the coefficient a_2. Next, notice that the product

$$\prod_{i=1}^{n}(xI_n - A)_{\sigma(i)i}$$

will contribute to the coefficient of an indeterminate of degree $n-2$ if a permutation $\sigma \in S_n$ fixes $n-2$ points and swaps the other 2, i.e. σ is a transposition. Thus for a given σ, that swaps j and k, we have: $\operatorname{sign}(\sigma) = -1$ and furthermore

$$A_{jk}A_{kj}\prod_{j\neq i\neq k}^{n}(x - A_{ii}).$$

Given that

$$\prod_{j\neq i\neq k}^{n}(x - A_{ii})$$

is a monic polynomial of degree $n-2$, the claim follows.

For a polynomial $f = \prod_{i=1}^{n}(x-\alpha_i)$ we shall write $a_i := \sum_{1\leq j_1<\ldots<j_i\leq n} \alpha_{j_1}\ldots\alpha_{j_i}$.

We are ready to present the first bound.

Proposition 3.1.5. *Let $f \in \mathbb{Z}[x]$ be a monic irreducible polynomial such that all its roots are real and positive. If*

$$\frac{(n-1)}{2n}a_1^2 - n < a_2, \tag{3.1.1}$$

then f is the minimal polynomial of an integer symmetric matrix if and only if there exists $A \in \operatorname{Sym}(ln, \mathbb{Z})$ for which f is the minimal polynomial and $l \in \{1, \ldots, k\}$, where

$$k \leq \left(a_2 + n - \frac{(n-1)}{2n}a_1^2\right)^{-1}. \tag{3.1.2}$$

Proof. Let $f \in \mathbb{Z}[x]$ be a monic irreducible polynomial of degree n such that all its roots are real and positive. Obviously f is the minimal polynomial of an integer symmetric matrix if and only if there exists $A \in \mathrm{Sym}(kn, \mathbb{Z})$ such that f annihilates it. Let us assume that A is the smallest such matrix, i.e. k is minimal. Given that f is irreducible and k is minimal it follows that A is an indecomposable matrix. We note the following

$$f^k = x^{kn} - b_1 x^{kn-1} + b_2 x^{kn-2} + \dots,$$

where by a simple counting one sees that $b_1 = ka_1$ and $b_2 = \binom{k}{2} a_1^2 + ka_2$. From the example above examining the determinant of $kn \times kn$ integer symmetric matrix we see that

$$b_2 = \sum_{1 \le i < j \le kn} A_{ii} A_{jj} - \sum_{1 \le i < j \le kn} A_{ij}^2. \tag{3.1.3}$$

By the Maclaurin's inequality it follows

$$\sum_{1 \le i < j \le kn} A_{ii} A_{jj} \le \frac{(kn-1)}{2kn} (ka_1)^2 = \frac{k(kn-1)}{2n} a_1^2.$$

Combining the above facts together gives us

$$\begin{aligned}
\binom{k}{2} a_1^2 + ka_2 &= \sum_{1 \le i < j \le kn} A_{ii} A_{jj} - \sum_{1 \le i < j \le kn} A_{ij}^2 \\
\binom{k}{2} a_1^2 + ka_2 + \sum_{1 \le i < j \le kn} A_{ij}^2 &= \sum_{1 \le i < j \le kn} A_{ii} A_{jj} \\
\binom{k}{2} a_1^2 + ka_2 + \sum_{1 \le i < j \le kn} A_{ij}^2 &\le \frac{k(kn-1)}{2n} a_1^2 \\
k(k-1)na_1^2 + 2nka_2 + 2n \sum_{1 \le i < j \le kn} A_{ij}^2 &\le k(kn-1)a_1^2 \\
k(1-n)a_1^2 + 2nka_2 + 2n \sum_{1 \le i < j \le kn} A_{ij}^2 &\le 0 \\
k\left((1-n)a_1^2 + 2na_2\right) + 2n \sum_{1 \le i < j \le kn} A_{ij}^2 &\le 0.
\end{aligned}$$

Given that A is indecomposable implies that

$$\sum_{1 \le i < j \le kn} A_{ij}^2 \ge kn - 1,$$

And thus

$$((1-n)a_1^2 + 2na_2 + 2n^2)k - 2n \leq 0.$$

In particular we will have an effective bound if the coefficient of k is strictly positive, i.e. $(1-n)a_1^2 + 2na_2 + 2n^2 > 0$. This is equivalent to

$$\frac{(n-1)}{2n}a_1^2 - n < a_2.$$

as was required to show. □

Corollary 3.1.6. *There exist counterexamples to Estes–Guralnick's conjecture for degrees* 8 *and* 9*.*

Proof. Consider the following irreducible polynomials

$$x^9 - 21x^8 + 188x^7 - 937x^6 + 2848x^5 - 5434x^4 + 6447x^3 - 4528x^2 + 1676x - 241$$

and

$$x^8 - 20x^7 + 168x^6 - 770x^5 + 2092x^4 - 3420x^3 + 3247x^2 - 1610x + 311.$$

We claim that neither of them can be the minimal polynomial of an integer symmetric matrix. In each case the polynomial satisfies the condition of Proposition 3.1.5, thus based on bound (3.1.2) it suffices to examine whether the polynomial can appear as the characteristic polynomial of an integer symmetric matrix.

Consider the degree 8 polynomial. We can avoid computation of all possible symmetric matrices by noting that if $A \in \mathrm{Sym}(8, \mathbb{Z})$ is the corresponding integer symmetric matrix then

$$\begin{aligned}\sum_{1\leq i<j\leq 8} A_{ii}A_{jj} =& \frac{\mathrm{Tr}(A)^2 - \sum_{i=1}^{8} A_{ii}^2}{2} \\ =& \frac{20^2 - \sum_{i=1}^{8} A_{ii}^2}{2}.\end{aligned}$$

To maximise this sum we have to minimise $\sum_{i=1}^{8} A_{ii}^2$. The matrix A is connected, thus $\sum_{1\le i<j\le 8} A_{ij}^2 \ge 7$. From equation (3.1.3) we have that

$$\begin{aligned} 168 &= \sum_{1\le i<j\le 8} A_{ii}A_{jj} - \sum_{1\le i<j\le 8} A_{ij}^2 \\ &\le \sum_{1\le i<j\le 8} A_{ii}A_{jj} - 7 \end{aligned}$$

and hence

$$\begin{aligned} 175 &\le \sum_{1\le i<j\le 8} A_{ii}A_{jj} \\ 175 &\le \frac{20^2 - \sum_{i=1}^{8} A_{ii}^2}{2} \\ 350 &\le 20^2 - \sum_{i=1}^{8} A_{ii}^2 \\ 50 &\ge \sum_{i=1}^{8} A_{ii}^2. \end{aligned}$$

Given that

$$\begin{aligned} \frac{1}{8}\sum_{i=1}^{8} A_{ii}^2 &\ge \left(\frac{\sum_{i=1}^{8} A_{ii}}{8}\right)^2 \\ &\ge \frac{25}{4}, \end{aligned}$$

with equality only if all A_{ii} are equal, i.e. $A_{ii} = \frac{5}{2}$. As $A_{ii} \in \mathbb{Z}_+$ we conclude that such matrix does not exist. The analogous method covers the polynomial of degree 9 too. Thus the corollary follows. □

Note that the two polynomials in the proof above are not small-span, and thus were previously unknown to be counterexamples to Estes–Guralnick's conjecture.

Definition 3.1.7. *Let $f \in \mathbb{Z}[x]$ be a monic polynomial such that all its roots are real and positive. Then f has* ***minimal trace*** *(or is of minimal trace) if at least one of its roots is less than one.*

It is sometimes convenient to regard monic polynomials f and $g \in \mathbb{Z}[x]$ as equivalent if there exists $m \in \mathbb{Z}$ such that $f(x) = g(x+m)$. Any such polynomial with only real roots is equivalent to the unique one of minimal trace.

Proposition 3.1.8. *Let $n \in \mathbb{N}$ and $B \geq 0$ be given. Then there are only finitely many monic irreducible polynomials $f \in \mathbb{Z}[x]$ of degree n such that:*

- *f has all roots real and positive, and is of minimal trace;*
- $a_2 > \dfrac{(n-1)}{2n} a_1^2 - B.$

Proof. Let f be of minimal trace, then by definition, there exists $\gamma \in (0,1)$ such that $f(\gamma) = 0$. Let $\gamma, \alpha_1, \ldots, \alpha_{n-1} \in \mathbb{R}_+$ be the roots of f. Then by Maclaurin's inequality (Proposition 3.1.3) we have

$$\frac{(n-2)}{2(n-1)}(a_1 - \gamma)^2 \geq a_2', \tag{3.1.4}$$

where

$$a_2' := \sum_{1 \leq i < j \leq n-1} \alpha_i \alpha_j.$$

Note that

$$\begin{aligned} a_2 &= a_2' + (a_1 - \gamma)\gamma \\ &< a_2' + a_1 - \gamma \\ &< a_2' + a_1. \end{aligned}$$

Combining this and inequality (3.1.4) we have

$$\begin{aligned} \frac{(n-2)}{2(n-1)}(a_1 - \gamma)^2 + a_1 &> a_2 \\ \frac{(n-2)}{2(n-1)}(a_1^2 - 2\gamma a_1 + \gamma^2) + a_1 &> a_2 \\ \frac{(n-2)}{2(n-1)}a_1^2 + (1 - \frac{(n-2)}{(n-1)}\gamma)a_1 + \frac{(n-2)}{2(n-1)}\gamma^2 &> a_2 \\ \frac{(n-2)}{2(n-1)}a_1^2 + a_1 + 1 &> a_2. \end{aligned}$$

Let $B \in \mathbb{R}_+$. By hypothesis of the proposition we have that

$$\begin{aligned} a_2 &> \frac{(n-1)}{2n} a_1^2 - B \\ n(n-2)a_1^2 + 2(n-1)na_1 + 2(n-1)n &> (n-1)^2 a_1^2 - 2(n-1)B \\ 2(n-1)na_1 + 2(n-1)n &> a_1^2 - 2(n-1)B \\ a_1^2 + 2n(1-n)a_1 + 2n(1-n)(B+1) &< 0. \qquad (3.1.5) \end{aligned}$$

There are only finitely many $a_1 \in \mathbb{Z}_+$ for a given n satisfying the bound. Thus the proposition follows from Proposition 3.1.3 again. □

We note that using inequality (3.1.5) one can effectively compute the bound for a_1.

Corollary 3.1.9. *Let $f \in \mathbb{Z}[x]$ be a monic irreducible polynomial of degree n such that the roots of f are real and positive. If*

$$\frac{(n-1)}{2n} a_1^2 - n + 1 < a_2$$

then f is not the minimal polynomial of an integer symmetric matrix, and for a given degree n there can be only finitely many such polynomials of minimal trace.

Proof. We begin by noticing that such polynomials would satisfy condition (3.1.1) and letting

$$\frac{(n-1)}{2n} a_1^2 - n + 1 < a_2$$

we see that inequality (3.1.2) gives us

$$k < 1$$

and so f is not the minimal polynomial of an integer symmetric matrix. The finiteness of examples follows from the previous proposition. □

Example 3.1.10. Consider the polynomial

$$x^{20} - 60x^{19} + 1692x^{18} - 29808x^{17} + 367793x^{16} - 3377328x^{15} + 23938743x^{14}$$

$$- 134063334x^{13} + 602208104x^{12} - 2190171816x^{11} + 6481403363x^{10}$$
$$- 15626636538x^9 + 30625401686x^8 - 48496762272x^7 + 61411191934x^6$$
$$- 61191470268x^5 + 46823870156x^4 - 26500746624x^3 + 10428844368x^2$$
$$- 2542580352x + 288610561.$$

It is irreducible and has all real and positive roots. From the bound above we see that $\frac{60^2 \times 19}{40} - 19 = 1691 < 1692$, thus this polynomial is not the minimal polynomial of an integer symmetric matrix.

Lemma 3.1.11. [Lemma 6.1.6, 88] *Let $f \in \mathbb{Z}[x]$ be a monic polynomial with roots $\alpha_1, \ldots, \alpha_n \in \mathbb{R}_+$, where $n > 1$. Let $\alpha_1^{(k)}, \ldots, \alpha_{n-k}^{(k)}$ be roots of the k-th derivative of f. Then*

$$\frac{1}{n^2(n-1)} \sum_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2 = \frac{1}{(n-k)^2(n-k-1)} \sum_{1 \le i < j \le n-k} (\alpha_i^{(k)} - \alpha_j^{(k)})^2. \quad \square$$

Corollary 3.1.12. *Let $f \in \mathbb{Z}[x]$ be a monic polynomial as above. Then $\frac{(n-1)}{2n} a_1^2 = a_2 + B$, where $B \ge \frac{n-1}{4}$.*

Proof. Let $f \in \mathbb{Z}[x]$, such that $\alpha_1, \ldots, \alpha_n \in \mathbb{R}_+$ are the roots of f. Let

$$f^{(n-2)} := \frac{n!}{2} x^2 - (n-1)! a_1 x + (n-2)! a_2$$

be its $n-2$-th derivative. Thus by the previous lemma we have that

$$\frac{1}{n^2(n-1)} \sum_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2 = \frac{1}{4} \left(\alpha_1^{(n-2)} - \alpha_2^{(n-2)} \right)^2,$$

where

$$\alpha_i^{(n-2)} := \frac{a_1}{n} \pm \sqrt{\frac{a_1^2}{n^2} - \frac{2a_2}{n(n-1)}}.$$

Therefore,

$$\frac{1}{n^2(n-1)} \sum_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2 = \left(\frac{a_1^2}{n^2} - \frac{2a_2}{n(n-1)} \right)$$
$$\frac{2}{n(n-1)} \sum_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2 = 2 \left(\frac{a_1^2}{n} - \frac{2a_2}{(n-1)} \right)$$

$$= \frac{2}{n}\left(a_1^2 - \frac{2na_2}{(n-1)}\right).$$

Let $B \in \mathbb{Q}$ be such that $\frac{2n}{n-1}a_2 = a_1^2 - \frac{2n}{n-1}B$. Let the discriminant of our polynomial be

$$\Delta_f := \prod_{1\le i<j\le n} (\alpha_i - \alpha_j)^2.$$

We have

$$\frac{2}{n(n-1)} \sum_{1\le i<j\le n} (\alpha_i - \alpha_j)^2 = \frac{2}{n}\left(a_1^2 - a_1^2 + \frac{2n}{n-1}B\right)$$
$$= \frac{4B}{n-1}.$$

And finally by the arithmetic mean–geometric mean inequality it follows

$$1 \le \Delta_f \le \left(\frac{2}{n(n-1)} \sum_{1\le i<j\le n} (\alpha_i - \alpha_j)^2\right)^{\frac{n(n-1)}{2}} = \left(\frac{4B}{n-1}\right)^{\frac{n(n-1)}{2}}.$$

Therefore $B \ge \frac{n-1}{4}$ as was claimed. □

3.2 A trace bound for positive definite integer symmetric matrices

Some of the new results of this section appeared in the paper [82]. We present a lower bound for the trace of connected and positive definite integer symmetric matrices. This bound will play a key role in showing that a given polynomial cannot be the minimal polynomial of an integer symmetric matrix.

Theorem 3.2.1. [Thm. 1, 82] *Let $A \in \mathrm{Sym}(n, \mathbb{Z})$ be a connected and positive definite matrix. Then* $\mathrm{Tr}(A) \ge 2n - 1$.

Proof. Let $A \in \mathrm{Sym}(n, \mathbb{Z})$ be a matrix satisfying conditions of the theorem. We prove by induction on n that $\mathrm{Tr}(A) \ge 2n - 1$. It clearly true for $n = 1$, as (0) is not a positive definite matrix. Assume that the theorem holds for $n - 1$, where $n > 1$. If it fails for n then there exists $A \in \mathrm{Sym}(n, \mathbb{Z})$ such that A is a positive definite, connected matrix and $\mathrm{Tr}(A) \leq 2n-2$. Let us assume that A is such matrix with the smallest possible trace. Let $\{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$ be the basis for $\mathbb{R}^n$ such that A represents a symmetric bilinear form β, i.e. $\beta(\mathbf{e}_i, \mathbf{e}_j) = A_{ij}$. Given that A is a positive definite matrix, $\beta(\mathbf{x}, \mathbf{x}) > 0$ for all $\mathbf{x} \in \mathbb{R}^n$, $\mathbf{x} \neq \mathbf{0}$, implies that $A_{ii} > 0$ for all $i \in \{1, \ldots, n\}$. By assumption that $\mathrm{Tr}(A) \leq 2n-2$ we have that at least two entries on the diagonal are equal to one.

Without loss of generality assume that $A_{11} = 1$. Our matrix is connected and so in each row and column there exists at least one off-diagonal nonzero entry. Therefore there exists j such that $A_{1j} \neq 0$; assume that $j = 2$. Let $\mathbf{e}'_2 := \mathbf{e}_2 - A_{12}\mathbf{e}_1$, and define a new basis $\{\mathbf{e}_1, \mathbf{e}'_2, \ldots, \mathbf{e}_n\}$ for $\mathbb{R}^n$, and a new matrix A' such that $\beta(\mathbf{e}'_i, \mathbf{e}'_j) = A'_{ij}$ (where $\mathbf{e}'_j = \mathbf{e}_j$ when $j \neq 2$). The matrix A' is symmetric and positive definite. We have

$$\begin{aligned}\beta(\mathbf{e}'_2, \mathbf{e}_j) &= \beta(\mathbf{e}_2, \mathbf{e}_j) - A_{12}\beta(\mathbf{e}_1, \mathbf{e}_j) \\ &= A_{2j} - A_{12}A_{1j}. \end{aligned} \tag{3.2.1}$$

Specifically if $j = 1$, then $A'_{12} = 0$. Furthermore

$$\begin{aligned}\beta(\mathbf{e}'_2, \mathbf{e}'_2) &= \beta(\mathbf{e}_2, \mathbf{e}_2) - 2A_{12}\beta(\mathbf{e}_1, \mathbf{e}_2) + A_{12}^2\beta(\mathbf{e}_1, \mathbf{e}_1) \\ &= A_{22} - A_{12}^2.\end{aligned}$$

Given that $A'_{ii} = A_{ii}$ for $i \neq 2$, we have conclude that $\mathrm{Tr}(A') < \mathrm{Tr}(A)$. From the minimality assumption on the trace of A we can conclude that A' is decomposable. We claim that A' splits exactly into two connected components; moreover one of these components contains A'_{11} and the other contains A'_{22}.

We define a **path** in a matrix to represent a chain of nonrepeating off-diagonal entries of the matrix, such that consecutive entries in a chain share a common index, i.e. for A' an example of a chain is $A'_{x_1x_2}A'_{x_2x_3}A'_{x_3x_4}\ldots A'_{x_{l-1}x_l}$ where each $A'_{x_ix_j} \neq 0$. One notices that two entries are in the same path only if they are in the same connected component. So given any $j \in \{3, \ldots, n\}$, if

A'_{j*} cannot be in any path with A'_{2*} then we claim that there exists a path with A'_{1*} such that A'_{j*} is there. This would prove our claim. From the assumption that A is connected, and A' differs from A only in the entries of the second row and column, if there does not exist a path from A'_{2*} to A'_{j*} then either the existent path in A was through A_{21} or A_{2j}, both of which got annihilated through the change of basis (see 3.2.1). In either case, this implies that A'_{1*} is in the path with A'_{j*} as we wanted to show.

Therefore we have that A' is subdivided into two connected components, say B_1 and B_2 of size $m_1 \times m_1$ and $m_2 \times m_2$, respectively. Thus $A' = B_1 \oplus B_2$ and $m_1 + m_2 = n$. Now

$$\operatorname{Tr}(A') = \operatorname{Tr}(B_1) + \operatorname{Tr}(B_2) < \operatorname{Tr}(A) \leq 2n - 1.$$

In particular, both of B_i are positive definite and connected but at least one has $\operatorname{Tr}(B_i) \leq 2m_i - 2$, contradicting the inductive hypothesis. □

Remark. This theorem does not hold for matrices over $\mathbb{Q}$ as it fails in the base case, i.e. there does not exist a smallest positive rational number. And furthermore, if for a given connected and positive definite matrix $A \in \operatorname{Sym}(n, \mathbb{Q})$ there exists $B \in \mathbb{R}$ such that $\operatorname{Tr}(A) \geq 2n - B$, then for any $k \in \mathbb{N}$ we construct an another matrix $\frac{1}{k}A \in \operatorname{Sym}(n, \mathbb{Q})$ which is still a positive definite and connected matrix, but its trace is smaller.

One could try to restrict to $A \in \operatorname{Sym}(n, \mathbb{Q})$ such that $\chi_A \in \mathbb{Z}[x]$, but when we change the basis and find two submatrices, it is not always true that either would have an integer characteristic polynomial. For example $\begin{pmatrix} \frac{7}{2} & -\frac{3}{2} & 1 \\ -\frac{3}{2} & \frac{3}{2} & -1 \\ 1 & -1 & 2 \end{pmatrix}$ has integer characteristic polynomial $x^3 - 7x^2 + 11x - 4$, but the characteristic polynomial of submatrix $\begin{pmatrix} \frac{7}{2} & 1 \\ 1 & 2 \end{pmatrix}$ is $x^2 - \frac{11}{2}x + \frac{17}{2}$. It is known that for $\chi_A \in \mathbb{Z}[x]$ such that $\chi_A(0) = \pm 1$ and $A \in \operatorname{Sym}(\mathbb{Q})$ there exists $k \in \mathbb{N}$ such that $A^k \in \operatorname{Sym}(\mathbb{Z})$ (see [28]).

It is rather easy to see that Theorem 3.2.1 also holds for negative definite matrix (the bound would be $\mathrm{Tr}(A) \leq -2n+1$). Further generalisations can be made to hermitian matrices over the ring of integers of totally imaginary quadratic fields. Denoting by

$$\bar{\cdot} : \mathbb{C} \longrightarrow \mathbb{C}$$

the ordinary complex conjugation, we say that the matrix H is **hermitian** if $H^t = \overline{H}$. And by a totally imaginary quadratic field $\mathbf{F}$ we mean a quadratic extension of $\mathbb{Q}$ such that there are no embeddings of $\mathbf{F}$ into $\mathbb{R}$. We shall return to the topic of symmetric matrices over ring of algebraic integers in the last chapter.

Corollary 3.2.2. *Let $f \in \mathbb{Z}[x]$ be a monic irreducible polynomial of degree n such that all its roots are real and positive. If the trace of f is less than $2n-1$, then f is not the minimal polynomial of an integer symmetric matrix.*

Proof. Let f satisfy the hypothesis of the corollary, and let us write $\mathrm{tr}(f)$ for the sum of roots of f. Thus the degree of f is n and $\mathrm{tr}(f) < 2n-1$. Then the corollary follows from the following identity:

$$\mathrm{tr}(f^k) = k\mathrm{tr}(f)$$

for $k \in \mathbb{N}$. Therefore $\mathrm{tr}(f^k) < 2nk-k$ and f cannot be the minimal polynomial of any integer symmetric matrix, as any such matrix $A \in \mathrm{Sym}(nk, \mathbb{Z})$, would be positive definite, connected (assuming minimality of k) and have $\mathrm{Tr}(A) < 2nk-k$. □

Example 3.2.3. (*i*) Let $A_n = (A_{ij}) \in \mathrm{Sym}(n, \mathbb{Z})$ be defined as follows:

$$A_{ij} = \begin{cases} 2 & \text{if } i = j > 1 \\ 1 & \text{if } i = j = 1 \\ 1 & \text{if } |i-j| = 1 \\ 0 & \text{otherwise.} \end{cases}$$

Then $\mathrm{Tr}(A_n) = 2n-1$, A_n is connected and positive definite, thus the trace bound of Theorem 3.2.1 is sharp. It was shown in [Table 1, 79] that

$$x^n \chi_{A_n}\left(x + \frac{1}{x} + 2\right) = \frac{x^{2n+1}-1}{x-1}.$$

From [76] we know that

$$f = x^6 - 13x^5 + 64x^4 - 146x^3 + 148x^2 - 48x + 1$$

is not the minimal polynomial of an integer symmetric matrix. The polynomial $x^6 f\left(x + \frac{1}{x} + 2\right)$ divides $\frac{x^{21}-1}{x-1}$. Thus $f \mid \chi_{A_{10}}$.

(ii) Let $B_n = (B_{ij}) \in \mathrm{Sym}(n, \mathbb{Z})$ be defined as follows:

$$B_{ij} = \begin{cases} n & \text{if } i = j = 1 \\ 1 & \text{if } i = j > 1 \\ 1 & \text{if } i = 1 \text{ or } j = 1 \\ 0 & \text{otherwise.} \end{cases}$$

Then $\mathrm{Tr}(B_n) = 2n-1$, B_n is connected and positive definite and its characteristic polynomial is $(x-1)^{n-2}(x^2 - (n+1)x + 1)$. Therefore eigenvalues of B_n are all in $\left(0, \frac{n+1+\sqrt{n^2+2n-3}}{2}\right]$.

Definition 3.2.4. *Let $f \in \mathbb{Z}$ be an irreducible polynomial of degree n with only real and positive roots. We define the **absolute trace** to be the average of its roots.*

There exists an old conjecture stating that:

Conjecture 3.2.5 (Schur–Siegel–Smyth trace problem)**.** [1, 19, 96, 98] For any $\epsilon > 0$ there exists only finitely many monic irreducible $f \in \mathbb{Z}$ with all its roots being real and positive, and such that the absolute trace of f is smaller than $(2 - \epsilon)$.

It could be read as a question of whether 2 is the smallest limit point of absolute traces of totally real and positive algebraic integers. There exists an infinite family of "cosine" polynomials, i.e. the minimal polynomials of $4\cos^2\left(\frac{\pi}{n}\right)$. In case n is an odd prime, then such polynomial is irreducible of degree $\frac{1}{2}(n-1)$ and trace $n-2$ [1]. Therefore, 2 is a limit point. It was proven that there are only finitely many polynomials of absolute trace ≤ 1.79193 [69], which is an improvement of initial bound given by Schur of $\exp(1/2)$ in [96].

Corollary 3.2.6. *The Schur–Siegel–Smyth trace problem holds true for polynomials that are minimal polynomials of integer symmetric matrices.*

Proof. Assume to contradiction that there exists $\epsilon > 0$ such that there are infinitely many irreducible polynomials $f \in \mathbb{Z}[x]$ such that all its roots are real and positive, and their absolute trace is less than $(2-\epsilon)$. Knowing that for a given trace and degree there can be only finitely many totally positive polynomials, implies that we can find f as above of an arbitrarily high degree. Let $n \in \mathbb{N}$ such that $n\epsilon > 1$. Let $A \in \mathrm{Sym}(m, \mathbb{Z})$ be a connected and positive definite matrix, $m \geq n$, such that f is its minimal polynomial, i.e. $f(A)$ is a zero matrix. Clearly then $\mathrm{Tr}(A) \leq (2-\epsilon)n < 2n-1$, contradicting Theorem 3.2.1. □

Corollary 3.2.7. *There exist counterexamples to Estes–Guralnick's conjecture for degrees 10 and 12.*

Proof. This follows from the existence of irreducible polynomials ([1])

$$\begin{aligned}&x^{10} - 18x^9 + 134x^8 - 538x^7 + 1273x^6 - 1822x^5 + 1560x^4 - 766x^3\\&+ 200x^2 - 24x + 1\end{aligned}$$

and

$$\begin{aligned}&x^{12} - 22x^{11} + 207x^{10} - 1092x^9 + 3561x^8 - 7897x^7 + 11086x^6\\&- 10061x^5 + 5726x^4 - 1941x^3 + 361x^2 - 32x + 1.\end{aligned}$$

□

Corollary 3.2.8. *Let $A \in \mathrm{Sym}(n, \mathbb{Z})$ be a connected positive definite matrix. Let*

$$\lambda_1 \geq \ldots \geq \lambda_n$$

be eigenvalues of A. Then

$$\lambda_1 \geq \frac{\mathrm{Tr}(A) - 1}{n} + 1.$$

Proof. Let A be a positive definite symmetric matrix. Let $K = \lceil \lambda_1 \rceil$. Then $A - KI_n$ is negative definite, and by Theorem 3.2.1 we have

$$\begin{aligned} \mathrm{Tr}(A - KI_n) &\leq -2n + 1 \\ \mathrm{Tr}(A) - Kn &\leq -2n + 1 \\ \frac{\mathrm{Tr}(A) - 1}{n} + 2 &\leq K. \end{aligned} \tag{3.2.2}$$

Given that K is a ceiling of λ_1 implies that $K - 1 \leq \lambda_1 \leq K$, thus the corollary holds. □

Corollary 3.2.9. *Let $f = \prod_{i=1}^{n}(x - \alpha_i) \in \mathbb{Z}[x]$ be an irreducible polynomial of degree $n > 1$ such that all α_i are real and*

$$\alpha_1 > \ldots > \alpha_n > 0.$$

If

$$\lfloor \alpha_1 \rfloor < \frac{\sum_{i=1}^{n} \alpha_i}{n} + 1,$$

then there exists $K \in \mathbb{N}$ such that f is the minimal polynomial of an integer symmetric matrix if and only if there exists $A \in \mathrm{Sym}(ln, \mathbb{Z})$ for $l \in \{1, \ldots, K\}$ which f annihilates.

Proof. Let $f \in \mathbb{Z}[x]$ be an irreducible polynomial of degree n such that all of its roots are real and positive. Let f be the minimal polynomial of a matrix $A \in \mathrm{Sym}(ln, \mathbb{Z})$; assume A is indecomposable. From inequality (3.2.2) in Proposition 3.2.8 we have

$$\lfloor \alpha_1 \rfloor \geq \frac{\mathrm{Tr}(A) - 1}{ln} + 1$$

$$\begin{aligned}&\geq \frac{\mathrm{Tr}(A)}{ln} - \frac{1}{ln} + 1\\ &\geq \frac{\sum_{i=1}^{n} \alpha_i}{n} - \frac{1}{ln} + 1.\end{aligned}$$

If

$$\lfloor \alpha_1 \rfloor < \frac{\sum_{i=1}^{n} \alpha_i}{n} + 1,$$

then there exists $K \in \mathbb{N}$ such that for $l > K$

$$\lfloor \alpha_1 \rfloor < \frac{\sum_{i=1}^{n} \alpha_i}{n} - \frac{1}{ln} + 1.$$

Therefore the corollary holds. □

If the absolute trace of a polynomial is small, we get a stronger bound.

Corollary 3.2.10. *Let $f = \prod_{i=1}^{n}(x - \alpha_i) \in \mathbb{Z}[x]$ be an irreducible polynomial such that all $\alpha_i \in \mathbb{R}_+$ and $\sum_{i=1}^{n} \alpha_i < 2n$. Then f is the minimal polynomial of an integer symmetric matrix if and only if it is the characteristic polynomial of an integer symmetric matrix.*

Proof. Assume that f is the minimal polynomial of a matrix $A \in \mathrm{Sym}(kn, \mathbb{Z})$ and assume that k is minimal. Given that $\sum_{i=1}^{n} \alpha_i < 2n$, we have that $\sum_{i=1}^{n} \alpha_i \leq 2n - 1$ and thus $\mathrm{Tr}(A) \leq 2kn - k$. From the minimality assumption of k we know that the matrix is indecomposable, and by Theorem 3.2.1 we have that $\mathrm{Tr}(A) \geq 2kn - 1$, therefore $k = 1$ as was required to show. □

Proposition 3.2.11. *The smallest limit point of the absolute trace of irreducible monic integer polynomials is equal to the smallest limit point of the absolute trace of separable monic integer polynomials.*

Proof. Let $\mathcal{L}_s$ be the smallest limit point of separable polynomials and $\mathcal{L}_i$ be the smallest limit point of irreducible polynomials. It is clear that $\mathcal{L}_i \geq \mathcal{L}_s$, thus it will suffice to show that $\mathcal{L}_s \geq \mathcal{L}_i$. Let $t(f) := \dfrac{\mathrm{tr}(f)}{\deg(f)}$. Let $\epsilon > 0$. Given that $\mathcal{L}_i$ is the smallest point of irreducible polynomials implies that there exists

$\delta > 0$ such that for an irreducible polynomial f with $t(f) > \mathcal{L}_i - \epsilon$ we have $t(f) \geq \mathcal{L}_i - \epsilon + \delta$. Let f be a separable polynomial such that $t(f) < \mathcal{L}_i - \epsilon$. We have that $f = gh$ where all irreducible factors p that divide g have $t(p) < \mathcal{L}_i$ and all the irreducible factors q that divide h have $t(q) > \mathcal{L}_i$ (h could be a unit).

There are finitely many irreducible factors of g, and given that g is separable, these factors cannot repeat, thus there are finitely many possibilities for g. Let d denote the largest degree of the irreducible factor of g. Each irreducible factor of h has absolute trace $\geq \mathcal{L}_i - \epsilon + \delta$, thus $t(h) \geq \mathcal{L}_i - \epsilon + \delta$. This gives us

$$\begin{aligned} \mathcal{L}_i - \epsilon \geq t(f) &= t(gh) \\ &= \frac{\operatorname{tr}(g) + \operatorname{tr}(h)}{\deg(g) + \deg(h)} \\ &\geq \frac{\operatorname{tr}(h)}{d + \deg(h)} \\ &\geq \frac{(\mathcal{L}_i - \epsilon + \delta)\deg(h)}{d + \deg(h)}. \end{aligned}$$

Therefore,

$$\deg(h) \leq \frac{(\mathcal{L}_i - \epsilon)d}{\delta}.$$

Thus the degree of h is dependent on ϵ and therefore is bounded. Similarly, $\operatorname{tr}(h)$ is bounded by $(d + \deg(h))(\mathcal{L}_i - \epsilon)$, consequently there are finitely many choices for h too, thus $\mathcal{L}_s \geq \mathcal{L}_i$. □

In the light of the above proposition, we can alter the condition of the "speculative" section of [77] to include separable polynomials.

Corollary 3.2.12. *Let $f \in \mathbb{Z}[x]$ such that f is a separable polynomial of absolute trace less than 2, and such that $|f(0)| \geq 2$, and between all consecutive roots of f there exists $x \in \mathbb{R}$ such that $|f(x)| \geq 2$. Then the Schur–Siegel–Smyth trace problem is false.*

Proof. Let f be a polynomial which satisfies the hypothesis of the corollary. Let $\alpha = \zeta_p + \frac{1}{\zeta_p}$, where ζ_p is a p-th root of unity. Let $\alpha_1, \ldots, \alpha_n$ be the conjugate set of α; note that all $\alpha_i \in (-2, 2)$. We can construct a new polynomial $F(x) = \prod_{i=1}^{n}(f(x) - \alpha_i)$. Given the hypothesis of the corollary, such polynomial still has all roots real, moreover it is separable and its absolute trace is equal to the absolute trace of f. Given that there are infinitely many prime numbers, the corollary follows. □

3.3 Totally nonnegative matrices

The following section is composed of a brief digression from the integer symmetric matrices into the study of totally nonnegative matrices, and more specifically oscillatory matrices. The first systemic study of oscillatory matrices can be found in [44]; there are beautiful links between the totally nonnegative matrices and various combinatorial objects [43], and recently there was a renewed interest in totally nonnegative matrices associated with cluster algebras [42]. We will show that the Schur–Siegel–Smyth trace problem is true for the class of polynomials arising as characteristic polynomials of integer oscillatory matrices. We shall use [39] and [87] as main references for everything that is widely known about the totally nonnegative matrices.

Definition 3.3.1. *We say that $A \in \mathrm{Mat}(m, n, \mathbb{R})$ is a* ***totally nonnegative*** *(or* ***totally positive****) matrix if every minor of A is nonnegative (or positive), where $m, n \in \mathbb{N}$.*

Example 3.3.2. (*i*) Any 1×1 matrix (a) such that $a \geq 0$ is a totally nonnegative matrix.

(*ii*) A matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{Mat}(2, \mathbb{R})$ is a totally nonnegative if and only if

$$a, b, c, d, ad - bc \geq 0.$$

Naïvely, for a matrix $A \in \mathrm{Mat}(n, \mathbb{R})$ one has to check $\binom{2n}{n} - 1$ minors before one can be sure that the matrix is totally nonnegative. This can be improved (see [43]), although the exact bound is not known.

We restrict our focus to square matrices, and specifically to the following class of totally nonnegative matrices:

Definition 3.3.3. *Let $A \in \mathrm{Mat}(n, \mathbb{R})$ be a totally nonnegative matrix. Then A is* ***oscillatory*** *if A^k is totally positive for some $k \in \mathbb{N}$.*

Example 3.3.4. The matrix $\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$ is an oscillatory matrix. On the other hand, the matrix $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$ is totally nonnegative, but it is not oscillatory as $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}^k = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & k \\ 0 & 0 & 1 \end{pmatrix}$ for all $k \in \mathbb{N}$, and thus never is totally positive.

Notice that a totally nonnegative matrix being oscillatory is an “analogue” of connectivity in symmetric matrices. In particular, any totally nonnegative symmetric matrix is oscillatory if and only if it is connected. We are interested in oscillatory matrices due to their spectral properties. For example, for totally nonnegative matrices there exists a variant of Cauchy Interlacing Theorem (see Chapter 5 in [87]). Furthermore:

Theorem 3.3.5. [Thm. 5.2, 39] *Let $A \in \mathrm{Mat}(n, \mathbb{R})$ be an oscillatory matrix. Then all the eigenvalues of A are real, positive and simple. In particular, A^{n-1} is totally positive.* □

We will need the following theorems.

Theorem 3.3.6. [Thm. 1.3, 43] *An invertible totally nonnegative matrix X is an oscillatory matrix if and only if $X_{i,i+1}X_{i+1,i} \geq 0$.* □

Remark that every principal submatrix of an oscillatory matrix is an oscillatory matrix.

Let $a_i, b_j \in \mathbb{R}$, we define **elementary Jacobi matrices** $L_i(a_i) := I_n + a_i E_{i,i-1}$ and $U_j(b_j) := I_n + b_j E_{j,j+1}$, where $E_{lk} = (e_{ij}) \in \mathrm{Mat}(n, \mathbb{R})$ is defined by

$$e_{ij} = \begin{cases} 1 & \text{if } i = l \text{ and } j = k \\ 0 & \text{otherwise.} \end{cases}$$

We shall refer to such a_i and b_j as weights of a given elementary Jacobi matrix.

Theorem 3.3.7. [Thm. 2.3.2, 39, 45] *A matrix X is totally nonnegative if and only if $X = \prod L_i(a_i) D \prod U_j(b_j)$, where $D = \mathrm{diag}(d_1, \ldots, d_n)$ and $a_i, b_j, d_k \in \mathbb{R}_{\geq 0}$.* □

Note that for an invertible nonnegative matrix over $\mathbb{Z}$ we have $\prod_{i=1}^{n} d_i = 1$. There exists a refinement of the theorem above for oscillatory matrices:

Theorem 3.3.8. [Thm. 2.6.4, 39, 45] *An invertible totally nonnegative matrix $X \in \mathrm{Mat}(n, \mathbb{R})$ is oscillatory if and only if*

$$X = \prod L_i(a_i) D \prod U_j(b_j),$$

where at least one of a_i for each $L_2(a_2), \ldots, L_n(a_n)$, and at least one of b_j for each $U_1(b_1), \ldots, U_{n-1}(b_{n-1})$ are strictly positive. □

Note that $L_i(a_i)L_j(a_j) = L_j(a_j)L_i(a_i)$ for $|i - j| > 1$ and $L_i(a_i)L_i(a_i') = L_i(a_i + a_i')$. Same holds for the matrices $U_i(b_i)$. Clearly $L_i(a_i)^t = U_{i-1}(a_i)$. The decomposition from the theorem above can be represented rather neatly with planar weighted networks (see for example [39]). Unfortunately, integer oscillatory matrices do not necessarily decompose as a product of elementary Jacobi matrices with integer weights.

Example 3.3.9. Let $M = \begin{pmatrix} 2 & 2 \\ 1 & 2 \end{pmatrix}$. M is an oscillatory matrix. Assume we can write it as a product of elementary Jacobi matrices with integer weights. Let $d_1, d_2, l, u \in \mathbb{Z}$, then

$$\begin{pmatrix} 1 & 0 \\ l & 1 \end{pmatrix} \begin{pmatrix} d_1 & 0 \\ 0 & d_2 \end{pmatrix} \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} d_1 & d_1 u \\ d_1 l & d_1 l u + d_2 \end{pmatrix}$$

$$= \begin{pmatrix} 2 & 2 \\ 1 & 2 \end{pmatrix}$$

thus $d_1 = 2$, however $d_1 l = 1$, a contradiction.

The question we are interested in is the following:

Question 3.3.10. Which irreducible polynomials appear as minimal polynomials of integer totally nonnegative matrices?

This is an integer totally nonnegative analogue of Estes–Guralnick's question. From the theorem above we can infer that given two oscillatory matrices $A, B \in \mathrm{Mat}(n, \mathbb{R})$, then AB is oscillatory too. However, unlike symmetric matrices, totally nonnegative matrices are not closed under addition, or conjugation by permutation matrices. For example matrix

$$\begin{pmatrix} 1 & 2 & 1 \\ 1 & 4 & 2 \\ 0 & 1 & 1 \end{pmatrix}$$

is a totally nonnegative matrix (also an oscillatory matrix), but

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 1 \\ 1 & 4 & 2 \\ 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 4 & 1 & 2 \\ 2 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}$$

is not, as $\det \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix} < 0$. Similarly we have that the matrices $\begin{pmatrix} 3 & 8 \\ 1 & 3 \end{pmatrix}$ and $\begin{pmatrix} 3 & 1 \\ 8 & 3 \end{pmatrix}$ are both oscillatory, but their sum $\begin{pmatrix} 6 & 9 \\ 9 & 6 \end{pmatrix}$ is not even totally nonnegative. Another question of interest is the following:

Question 3.3.11. If an irreducible polynomial is the minimal polynomial of an integer totally nonnegative matrix is it then the minimal polynomial of an integer oscillatory matrix too?

Given the spectral properties of the oscillatory matrices, the affirmative answer to the question above would imply that if an irreducible polynomial is the minimal polynomial of an integer totally nonnegative matrix, then necessarily it is the characteristic polynomial of some integer totally nonnegative matrix too. We have that this is the case for some low degree polynomials:

Theorem 3.3.12. *Every separable monic integer polynomial with only real and nonnegative roots and of degree one or two is the characteristic polynomial of an integer totally nonnegative matrix.*

Proof. Let $f \in \mathbb{Z}[x]$ satisfy the hypothesis of the theorem. If f is of degree one, i.e. $f = x - A$, then it suffices to consider the matrix $\begin{pmatrix} A \end{pmatrix}$. Let $f = x^2 - Ax + B$, where $A, B \in \mathbb{Z}$, $A, B \geq 0$. By considering the zero matrix, we can exclude the case when $A = 0$, thus let $A > 0$. If $A^2 - 4B = 0$ then matrix

$$\begin{pmatrix} \frac{A}{2} & 0 \\ 0 & \frac{A}{2} \end{pmatrix}$$

will suffice. Assume f has two distinct roots, therefore $A^2 - 4B > 0$. If A is even, then matrix

$$\begin{pmatrix} \frac{A}{2} & \frac{A^2}{4} - B \\ 1 & \frac{A}{2} \end{pmatrix}$$

is totally nonnegative. Else,

$$\begin{pmatrix} \frac{A-1}{2} & \frac{A^2-1}{4} - B \\ 1 & \frac{A+1}{2} \end{pmatrix}$$

is a totally nonnegative matrix with the characteristic polynomial $x^2 - Ax + B$, as was required to show. □

We propose the following question:

Question 3.3.13. Is every totally positive algebraic integer an eigenvalue of integer oscillatory matrix?

The answer for real oscillatory matrices is affirmative, but it is not known whether the same holds even for rational matrices.

The aim of what follows is to show that there exist infinitely many totally irreducible monic integer polynomials with only real and positive roots, but that are not minimal polynomials of integer oscillatory matrices. Given that we are interested in irreducible polynomials and that eigenvalues of oscillatory matrices are simple, we can restrict to the case when our polynomial is the characteristic polynomial only.

Theorem 3.3.14. *Let* $A \in \mathrm{Mat}(n, \mathbb{Z})$ *be an oscillatory matrix, then* $\mathrm{Tr}(A) \geq 2n - 1$.

Proof. We shall prove this by induction on n. For $n = 1$ and 2 it is clear from Theorem 3.3.12. Assume that the hypothesis holds for $n - 1 \geq 2$. We argue by contradiction and assume that the hypothesis fails for n and there exists $A \in \mathrm{Mat}(n, \mathbb{Z})$ such that A is oscillatory and $\mathrm{Tr}(A) \leq 2n - 2$. Assume that this is the smallest such n. We need to consider the following cases:

I. $\mathrm{Tr}(A) < 2n - 2$. In this case A has a principal submatrix $(A_{ij})_2^n$. This submatrix is an oscillatory matrix (see the remark after Theorem 3.3.6) of order $n - 1$ and it has a trace that is less than $2(n - 1) - 1$. A contradiction.

II. $\mathrm{Tr}(A) = 2n - 2$ and

   a) either A_{11} or A_{nn} not equal to 1. In this case we assume without a loss of generality that $A_{11} \neq 1$. Consider a principal submatrix $(A_{ij})_2^n$ which is an oscillatory matrix of order $n-1$ and trace less than $2(n - 1) - 1$. A contradiction.

   b) $A_{11} = 1 = A_{nn}$, and there exists j such that $A_{jj} > 2$. We consider principal submatrices $A' = (A_{ij})_{j+1}^n$ and $A'' = (A_{ij})_1^{j-1}$. Both A' and A'' are oscillatory matrices. We have that

$$\begin{aligned} \mathrm{Tr}(A') + \mathrm{Tr}(A'') &= \mathrm{Tr}(A) - A_{jj} \\ &= 2n - 2 - A_{jj} \\ &\leq 2n - 5 = 2(n - 1) - 3. \end{aligned}$$

By our hypothesis we know that $\operatorname{Tr}(A') \geq 2(n-j)-1$ and $\operatorname{Tr}(A'') \geq 2(j-1)-1$, thus

$$\operatorname{Tr}(A') + \operatorname{Tr}(A'') \geq 2(n-1)-2,$$

a contradiction.

c)

$$A_{ii} = \begin{cases} 1 & \text{if } i = 1, n \\ 2 & \text{otherwise.} \end{cases}$$

If $n = 3$ then A is a 3×3 matrix that has the following form

$$\begin{pmatrix} 1 & 1 & \alpha \\ 1 & 2 & 1 \\ \beta & 1 & 1 \end{pmatrix}.$$

The entries 1 on the off-diagonal follow from the fact that the principal minors have to be strictly positive, as matrices are oscillatory (all eigenvalues strictly positive) and Cauchy Interlacing Theorem. Now the characteristic polynomial of A is $x^3 - 4x^2 + (3-\alpha\beta)x - (\alpha+\beta-2\alpha\beta)$. Therefore we have that $\alpha + \beta - 2\alpha\beta > 0$ and $3 - \alpha\beta > 0$. But α and β both have to equal to 0, else one of the minors $\begin{vmatrix} 1 & 2 \\ \beta & 1 \end{vmatrix}$ or $\begin{vmatrix} 1 & \alpha \\ 2 & 1 \end{vmatrix}$ would be negative. Therefore the characteristic polynomial of A is $x(x^2 - 4x + 3)$, thus A is not oscillatory. Hence $n > 3$, and any such matrix has a principal 3×3 submatrix $(A_{ij})_1^3$ with diagonal entries 1, 2 and 2. By checking all the possible 3×3 oscillatory matrices, we are left with the following possibilities (up to transposition)

$$X = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 2 \\ 0 & 1 & 2 \end{pmatrix} \text{ and } Y = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 2 & 1 \\ 0 & 1 & 2 \end{pmatrix}.$$

We want to show that we can write A as

$$A = L_2(a_2) \prod_{i \neq 2} L_i(a_i) D \prod U_j(b_j),$$

so that $L_2(a_2)^{-1}A$ is a totally nonnegative matrix. Let us assume that $(A_{ij})_1^3 = X$ (similar argument holds for the submatrix Y). By

Theorem 3.3.8 we know that $A = \prod L_i(a_i) D \prod U_j(b_j)$ and for each $2 \leq i \leq n$ there exists $L_i(a_i)$ with a positive a_i. Let $L'_i(e_i)$ denote $(L_i(a_i))_1^3$. Clearly $L'_i(a_i)X = X$ for $i \geq 4$. Furthermore, we have that $L_2(a_2)\left(\prod_{i\geq 4} L_i(a_i)\right) = \left(\prod_{i\geq 4} L_i(a_i)\right) L_2(a_2)$ (by the remark after Theorem 3.3.8) so if we argue to contradiction that $A \neq L_2(a_2) \prod L_i(a_i) \prod U_j(b_j)$ then there exists $L_3(a_3)$ such that

$$A = \left(\prod_{i\geq 4} L_i(a_i)\right) L_3(a_3) \left(\prod_{i\neq 2} L_i(a_i)\right) L_2(a_2) \left(\prod L_i(a_i)\right) \left(\prod U_j(b_j)\right),$$

where some of $\prod_{i\geq 4} L_i(a_i)$ and $\prod_{i\neq 2} L_i(a_i)$ can equal to one. Thus we have that $L_3^{-1}(a_3)\left(\prod_{i\geq 4} L_i(a_i)\right)^{-1} A$ is a totally nonnegative matrix. Note that $L_i(a_i)^{-1} = L_i(-a_i)$ and so

$$L'_3(-a_3)\left(\prod_{i\geq 4} L'_i(a_i)\right)^{-1} X = L'_3(-a_3)X$$

is a totally nonnegative matrix. But

$$\begin{aligned} L'_3(-a_3)X &= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -a_3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 2 \\ 0 & 1 & 2 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 2 \\ -a_3 & 1-2a_3 & 2-2a_3 \end{pmatrix}, \end{aligned}$$

and if $a_3 > 0$ then $L'_3(-a_3)X$ is not a totally nonnegative matrix, and consequently $L_3(-a_3)A$ is not a totally nonnegative matrix, a contradiction. Hence, we can write A as $A = L_2(a_2) \prod_{i\neq 2} L_i(a_i) \prod U_j(b_j)$. Consider the following

$$\begin{aligned} L'_2(a_2)^{-1}X &= \begin{pmatrix} 1 & 0 & 0 \\ -a_2 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 2 \\ 0 & 1 & 2 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 1 & 1 \\ 1-a_2 & 2-a_2 & 2-a_2 \\ 0 & 1 & 2 \end{pmatrix}. \end{aligned}$$

We can let $a_2 = 1$,

$$L'_2(1)^{-1}X = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 1 & 2 \end{pmatrix},$$

in particular $L_2(-1)A$ is totally nonnegative matrix. The principal submatrix $A' = (A'_{ij})_2^n$ of $L_2(-1)A$ is totally positive and furthermore oscillatory. But $\mathrm{Tr}(A') = 2(n-1) - 2$, a contradiction. □

Example 3.3.15. Recall matrices $A_n \in \mathrm{Sym}(n, \mathbb{Z})$ from example (3.2.3). These matrices are totally nonnegative and furthermore, due to Theorem 3.3.6, we know that A_n is oscillatory for all n. Thus we can always find an oscillatory matrix of trace $2n-1$.

Corollary 3.3.16. *The Schur–Siegel–Smyth trace problem holds true for polynomials that are minimal polynomials of integer oscillatory matrices.* □

Given the rigid constrains of the totally nonnegative and oscillatory matrices, we are able to show that some polynomials are not characteristic polynomials of an oscillatory matrix which have arbitrary large traces. First we will need the following theorem:

Theorem 3.3.17. [Thm. 4.3, 87] *Let $A \in \mathrm{Mat}(n, \mathbb{R}_+)$ be a tridiagonal matrix. If all of the principal minors of A are nonnegative then A is a totally nonnegative matrix.* □

Proposition 3.3.18. *Let $A \in \mathrm{Mat}(n, \mathbb{R})$ be an oscillatory matrix. Then $A + dI_n$ is an oscillatory matrix for all $d \in \mathbb{R}_+$ if and only if A is a tridiagonal matrix.*

Proof. Let A be an oscillatory matrix. Let A_{ij} such that $|i-j| > 1$. Without loss of generality assume that $i > j$. Then the determinant of minor $\begin{vmatrix} A_{ik} & A_{ij} \\ A_{kk} & A_{kj} \end{vmatrix}$ is strictly positive. In a matrix $A + dI$ this minor corresponds to $\begin{vmatrix} A_{ik} & A_{ij} \\ A_{kk} + d & A_{kj} \end{vmatrix}$, and thus nonnegative for all positive d if and only if $A_{ij} = 0$. □

Corollary 3.3.19. *Let $f \in \mathbb{Z}[x]$ be a monic irreducible polynomial such that all its roots real and positive, and $|\{A \in \mathrm{Mat}(n, \mathbb{N} \cup \{0\}) \mid \chi_A = f\}| < \infty$. Then $f(x-k)$ is the characteristic polynomial of an integer oscillatory matrix for all $k \in \mathbb{N} \cup \{0\}$ if and only if there exists a tridiagonal $T \in \mathrm{Mat}(n, \mathbb{N} \cup \{0\})$ such that $\chi_T = f$.* □

Example 3.3.20. Let $f = x^3 - 6x^2 + 5x - 1$. All the roots of f are real and positive. We know that f is the characteristic polynomial of an oscillatory matrix, for example

$$\begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 2 \\ 1 & 2 & 3 \end{pmatrix}.$$

But it is not the characteristic of an integer tridiagonal oscillatory matrix. And as $|\{A \in \mathrm{Mat}(3, \mathbb{N} \cup \{0\}) \mid \chi_A = f\}| < \infty$, there exists $k \in \mathbb{N}$ such that $f(x-k)$ is not the characteristic polynomial of an integer oscillatory matrix.

Chapter 4

Interlacing polynomials

In this final chapter we endeavour an exploration of interlacing polynomials as an attempt to better understand which polynomials appear as minimal polynomials of integer symmetric matrices. Although the general answer is not within reach, and the question of quintic polynomials is still open, we are able to show that there exist counterexamples to Estes–Guralnick's conjecture for all degrees strictly larger than five.

We begin by applying an interlacing-based construction given in [75] of Salem numbers to show that there exists a Salem number of trace -2 of each even degree strictly larger than 22. Counterexamples to Estes–Guralnick's conjecture follow as a corollary thereof. This new result appeared in the paper [83].

In the latter part of this chapter we focus directly on interlacing polynomials. Given that we still would like to know which polynomials are the minimal polynomials of integer symmetric matrices, the interlacing polynomials present us with a neat way of finding new counterexamples to Estes–Guralnick's conjecture. The main result of this section is a demonstration of nonexistence of noninterlacing monic polynomials for certain low degrees. We refer to [73] for further details about discrete geometry, and to [40] for interlacing polynomials.

4.1 Salem numbers

In this section we shall construct infinite families of Salem numbers of trace -2, and thus produce counterexamples to Estes–Guralnick's conjecture in almost all degrees. Salem numbers appear to have pandemic-like properties and thus are a subject of an everlasting body of research. For more information about Salem numbers we refer to [102]. The motivational problem from our perspective is:

Conjecture 4.1.1 (Salem's conjecture)**.** [71, 102] There exists $\epsilon > 0$ such that if $\alpha_1 \in (2, 2+\epsilon)$ and $\alpha_2, \ldots, \alpha_n \in (-2, 2)$ then $\prod_{i=1}^{n}(x - \alpha_i) \notin \mathbb{Z}[x]$, where $n \in \mathbb{N}$ is strictly larger than one.

4.1.1 Palindromic polynomials

For $f(x) \in \mathbb{R}[x]$, a real polynomial evaluated at x, we shall drop x and write f if the situation allows us to do so without causing any ambiguities.

Definition 4.1.2. *Let $\alpha \in \mathbb{R}$ be an algebraic integer and let $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n$ be its conjugates. Then α is a **Salem number** if and only if $\alpha > 1$, $|\alpha_i| \leq 1$ for $2 \leq i \leq n$, and there exists α_j such that $|\alpha_j| = 1$.*

For $m \in \mathbb{Z}$, we say that a Salem number is of trace m when the sum of all its conjugates is m. Before we introduce an example of a Salem number we note that if α is a Salem number then by definition $\alpha > 1$ and at least one of its conjugates has to be on the unit circle. Thus the degree of a Salem number is at least 3. But there does not exist a Salem number of degree three, and in general we have that:

Proposition 4.1.3. *Let $f \in \mathbb{Q}[x]$ be an irreducible polynomial of degree $n > 1$ such that at least one of the roots of f is on the unit circle. Then n is an even integer and $f(x) = x^n f\left(\frac{1}{x}\right)$.*

Proof. Let f be an irreducible polynomial of degree $n > 1$ such that one of its roots, say α, is on the unit circle. Then $\alpha\overline{\alpha} = 1$, where $\overline{\alpha}$ is the complex conjugate of α. As the coefficients of f are real we have that $\overline{\alpha} = 1/\alpha$ is also a root of f. Thus $x^n f\left(\frac{1}{x}\right) = \epsilon f(x)$ for some $\epsilon \in \mathbb{Q}$. Given that $n > 1$ and f is an irreducible polynomial imply that $f(1) \neq 0$. Taking $x = 1$ we have $f(1) = \epsilon f(1)$ and thus $\epsilon = 1$. Moreover $f(-1) \neq 0$, so taking $x = -1$ implies that $(-1)^n f(-1) = f(-1)$, thus n must be even. □

Remark. If $f(x) = x^n f\left(\frac{1}{x}\right)$ then for $f(x) = \sum_{i=0}^{n} a_i x^i$ we have $a_i = a_{n-i}$. Such polynomials are called **self-reciprocal** or **palindromic** polynomials. Thus a Salem number is a root of a monic palindromic polynomial. The converse of the proposition above is not true, and given an even irreducible palindromic polynomial it is not necessary that it has a root on the unit circle (for example $x^2 + 3x + 1$). Let us note that the set of all palindromic polynomials is closed under multiplication and the sum of two palindromic polynomials of the same degree is again a palindromic polynomial. The latter is not true when we drop the degree criterion, for example $x^2 + x + 1$ and $x + 1$ are both palindromic but their sum, $x^2 + 2x + 2$, is not.

Example 4.1.4. The algebraic integer $\frac{1}{4}\left(3 + \sqrt{5} + \sqrt{2(-1 + 3\sqrt{5})}\right)$ is a root of the polynomial $x^4 - 3x^3 + 3x^2 - 3x + 1$. Its conjugates are

$$\frac{1}{4}\left(3 + \sqrt{5} - \sqrt{2(-1 + 3\sqrt{5})}\right)$$

and

$$\frac{1}{4}\left(3 - \sqrt{5} \pm i\sqrt{2(1 + 3\sqrt{5})}\right).$$

Now

$$\frac{1}{4}\left(3 + \sqrt{5} + \sqrt{2(-1 + 3\sqrt{5})}\right) > 1$$

and the absolute value of all its conjugates is less than or equal to 1, with

$$\left|\frac{1}{4}\left(3 - \sqrt{5} + i\sqrt{2(1 + 3\sqrt{5})}\right)\right| = 1.$$

Thus $\frac{1}{4}\left(3+\sqrt{5}+\sqrt{2(-1+3\sqrt{5})}\right)$ is a Salem number of trace 3.

Proposition 4.1.5. *Let $f \in \mathbb{R}[x]$ be a palindromic polynomial of degree $2n$. Then there exists a polynomial $h \in \mathbb{R}[x]$ such that $f(x) = x^n h\left(x+\frac{1}{x}\right)$.*

Proof. We prove by induction on n. For $n = 1$ let $f = a_2x^2 + a_1x + a_2$ and $h = a_2x + a_1$, then $f(x) = xh\left(x+\frac{1}{x}\right)$. Let us assume that the proposition holds for $n \geq 1$. To check the case for degree $n+1$ let $f = \sum_{i=0}^{2(n+1)} a_ix^i$. Then $\frac{1}{x}\left(f(x) - a_{2(n+1)}x^{n+1}\left(x+\frac{1}{x}\right)^{n+1}\right)$ is a palindromic polynomial of degree $\leq 2n$. By the inductive argument there exists $\tilde{h} \in \mathbb{R}[x]$ such that $f(x) - a_{2(n+1)}x^{n+1}\left(x+\frac{1}{x}\right)^{n+1} = x^n\tilde{h}\left(x+\frac{1}{x}\right)$. Letting $h\left(x+\frac{1}{x}\right) = \tilde{h}(x) + a_{2(n+1)}x^{n+1}$ we get $x^{n+1}h\left(x+\frac{1}{x}\right) = f(x)$, as was required to show. □

Remark. There exists a two-to-one map between the roots of polynomials $f = \prod_{i=1}^{n}(x-\beta_i)(x-\frac{1}{\beta_i})$ and $h = \prod_{i=1}^{n}(x-\alpha_i)$, where $x^nh\left(x+\frac{1}{x}\right) = f(x)$. In particular, if we let $\alpha_i = \beta_i + \frac{1}{\beta_i}$ then the roots of $x^2 - \alpha_ix + 1$ are the roots of f.

Example 4.1.6. For a polynomial $h = x^2 - 3x + 1$ we have $x^4h\left(x+\frac{1}{x}\right) = x^4 - 3x^3 + 3x^2 - 3x + 1$, call it f. From the previous example we know that f is palindromic, and in particular, it is the minimal polynomial of a Salem number of trace 3.

Corollary 4.1.7. *Let $f \in \mathbb{Z}[x]$ be the minimal polynomial of a Salem number of trace m and degree $2n$. Then there exists an irreducible polynomial $h \in \mathbb{Z}[x]$ of degree n such that all roots of h are real and positive and the trace of h is $2n+m$, i.e. $h = x^n - (2n+m)x^{n-1} + \dots$.*

Proof. Let $f \in \mathbb{Z}[x]$ satisfy the hypothesis of the corollary. Then by Proposition 4.1.5 there exists $\tilde{h} \in \mathbb{Z}[x]$ such that $x^n\tilde{h}\left(x+\frac{1}{x}\right) = f(x)$. Given that f is irreducible implies that $\tilde{h}$ is irreducible too. The roots of $\tilde{h}$ are all strictly larger than -2 and their sum is m. Therefore $h(x) = \tilde{h}(x-2)$ has only real and positive roots such that their sum is $2n + m$. □

Definition 4.1.8. *Let $n \in \mathbb{N}$. We say that $\Phi_n \in \mathbb{Z}[x]$ is the **n-th cyclotomic polynomial** if it is the unique irreducible polynomial divisor of $x^n - 1$, such that $\Phi_n \nmid x^k - 1$ for $1 \leq k \leq n-1$.*

Example 4.1.9. $\Phi_1 = x - 1$ and $\Phi_2 = x + 1$. We have that $\Phi_p = x^{p-1} + x^{p-2} + \ldots + x + 1$, where p is a prime number.

Remark. For a cyclotomic polynomial we have that $\deg(\Phi_n) = \phi(n)$, where $\phi(n)$ is Euler's ϕ-function; furthermore $x^n - 1 = \prod_{d|n} \Phi_d$ ([Ch. IV, 67]).

4.1.2 Interlacing polynomials

Much of what follows will be used throughout the chapter. For further details we refer to the first chapter in [40].

Definition 4.1.10. *Let f and $g \in \mathbb{R}[x]$ be such that $g = \prod_{i=1}^{n}(x - \beta_i)$, $n > 1$, all $\beta_i \in \mathbb{R}$ and $\beta_i < \beta_{i+1}$ for $1 \leq i \leq n-1$. Then f **sign interlaces** g if $\operatorname{sign}(f(\beta_i)) \neq \operatorname{sign}(f(\beta_{i\pm1}))$ for all roots of g.*

In the above definition we assume that if $\beta_i = \beta_1$ then it suffices to check that $\operatorname{sign}(f(\beta_1)) \neq \operatorname{sign}(f(\beta_2))$. Analogous assumption holds for when $i = n$. Recall that

$$\operatorname{sign}(x) = \begin{cases} 1 & \text{if } x > 0 \\ -1 & \text{if } x < 0 \\ 0 & \text{if } x = 0. \end{cases}$$

Note that if all the roots of f and g are real and their degrees differ at most by one, then f sign interlaces g implies that g sign interlaces f too.

Definition 4.1.11. *Let g be as in the definition above and let $f = \prod_{i=1}^{n}(x - \alpha_i) \in \mathbb{R}[x]$ such that all $\alpha_i \in \mathbb{R}$ and $\alpha_i < \alpha_{i+1}$ for $1 \leq i \leq n$. Then the roots of f and g **interlace** if $\alpha_1 < \beta_1 < \alpha_2 < \ldots < \beta_n$ or $\beta_1 < \alpha_1 < \ldots < \beta_n < \alpha_n$.*

The more interesting case for us will be the following:

Definition 4.1.12. *Let $g = \prod_{i=1}^{n-1}(x - \beta_i)$ and $f = \prod_{i=1}^{n}(x - \alpha_i)$ such that all $\alpha_i, \beta_j \in \mathbb{R}$, $\alpha_i < \alpha_{i+1}$ for $1 \leq i \leq n-1$ and $\beta_j < \beta_{j+1}$ for $1 \leq j \leq n-2$. Then g* ***interlaces*** *f if $\alpha_1 < \beta_1 < \alpha_2 < \ldots < \beta_{n-1} < \alpha_n$.*

Above definitions represent the strict cases of interlacing, i.e. where all the inequalities are strict. Recall Theorem 3.1.1 (Cauchy Interlacing Theorem), where it is shown that the characteristic polynomial of a symmetric matrix is interlaced by the characteristic polynomial of its principal submatrix. There we allowed for a weaker form of interlacing, where the interlacing polynomial may have a root in common with the interlaced polynomial. Given that we will be mostly interested in irreducible polynomials, the strict interlacing will suffice. Nevertheless, much of what follows, either holds or can be extended to the weaker form of interlacing.

From now on, when we say that polynomials are interlacing or that one polynomial is interlacing the other, we will implicitly assume that both polynomials are monic and have only real roots.

Lemma 4.1.13. *Let $f, g \in \mathbb{R}[x]$ such that $\deg(f) = \deg(g) + 1$. Then f sign interlaces g if and only if g interlaces f.*

Proof. Let us assume that f sign interlaces g, and $\deg(f) = n$. By the Intermediate Value Theorem we have that between two consecutive roots of f there exists a root of g. Given that degree of g is $n-1$ implies that g interlaces f. The reverse argument is clear. □

Lemma 4.1.14. *Let $f = \prod_{i=1}^{n}(x - \alpha_i)$ and consider a polynomial*

$$g = \sum_{i=1}^{n} \lambda_i \prod_{j \neq i}(x - \alpha_j) = \gamma \prod_{i=1}^{n-1}(x - \beta_i)$$

such that all $\alpha_i, \gamma, \lambda_i \in \mathbb{R}$ with $\alpha_i < \alpha_{i+1}$ and all γ_i are nonzero. Then $\alpha_1 < \beta_1 < \alpha_2 < \ldots < \beta_{n-1} \leq \alpha_n$ if and only if $\operatorname{sign}(\lambda_i) = \operatorname{sign}(\lambda_{i+1})$ for $1 \leq i \leq n-1$.

Proof. Let f and g as above. Then $\deg(f) = \deg(g)+1$ and by our assumption f has only real roots. By the previous lemma, to show that g interlaces f it suffices to show that g sign interlaces f. Note that Intermediate Value Theorem tells us that all the roots of g are real. Let us evaluate g at the roots of f. We have

$$g(\alpha_i) = \lambda_i \prod_{j \neq i} (\alpha_i - \alpha_j).$$

Now for $j > i$ we have $\text{sign}(\alpha_i - \alpha_j) = -1$ as $\alpha_j > \alpha_i$, thus

$$\begin{aligned} \text{sign}(g(\alpha_i)) &= \text{sign}(\lambda_i)\text{sign}\left(\prod_{i<j}(\alpha_i - \alpha_j)\right)\text{sign}\left(\prod_{i>j}(\alpha_i - \alpha_j)\right) \\ &= \text{sign}(\lambda_i)(-1)^{n-i}. \end{aligned}$$

Therefore $\text{sign}(g(\alpha_i)) \neq \text{sign}(g(\alpha_{i\pm1}))$ if and only if $\text{sign}(\lambda_i) = \text{sign}(\lambda_{i\pm1})$. □

Lemma 4.1.15. *Let $f = a_0 \prod_{i=1}^{n}(x - \alpha_i)$, $g = b_0 \prod_{i=1}^{n-1}(x - \beta_i) \in \mathbb{R}[x]$ such that g interlaces f, f is not a multiple of g, and $a_0, b_0 \in \mathbb{R}_+$. Then for all $\gamma \in \mathbb{R}_+ \setminus \{0\}$ we have that $h = \gamma g - f$ has only real roots. Furthermore the roots of f and h interlace, and g interlaces h, i.e. $h = \prod(x - \gamma_i)$ and $\alpha_1 < \gamma_1 < \beta_1 < \alpha_2 < \gamma_2 < \ldots < \beta_{n-1} < \alpha_n < \gamma_n$.*

Proof. Let us define a set

$$X = \bigcap_{i=1}^{n-1} \left\{ \frac{f(r)}{g(r)} \mid r \in (\alpha_i, \beta_i) \right\}.$$

We claim that X is not empty. On each interval (α_i, β_i) the function $\frac{f}{g}$ is continuous going from zero to infinity (note that it can be either negative or positive infinity). We have that the sign $\left(\frac{f(r^{(i)})}{g(r^{(i)})}\right) = \text{sign}\left(\frac{f(r^{(j)})}{g(r^{(j)})}\right)$ for $r^{(i)} \in (\alpha_i, \beta_i)$, $r^{(j)} \in (\alpha_j, \beta_j)$ where $1 \leq i, j \leq n-1$. This follows from the fact that g interlaces f and thus g sign interlaces f, i.e. $\text{sign}(f(\beta_i)) \neq \text{sign}(f(\beta_{i+1}))$. Therefore, $\text{sign}(f(r^{(i)})) \neq \text{sign}(f(r^{(i+1)}))$. Similar can be concluded for g, giving us that $\text{sign}(f(r^{(i)}))$ and $\text{sign}(g(r^{(i)}))$ are constant on (α_i, β_i) for $1 \leq$

$i \leq n-1$. Thus X is not empty. In particular, given the hypothesis that $a_0, b_0 \in \mathbb{R}_+$ implies that $\text{sign}(f(r^{(i)})) = \text{sign}(g(r^{(i)}))$ for $1 \leq i \leq n-1$, and therefore $X = (0, +\infty)$.

As X is not empty, this implies that there exists $\gamma \in X$ such that $\gamma \neq 0$ and $\dfrac{f(r^{(i)})}{g(r^{(i)})} = \gamma$ for $r^{(i)} \in (\alpha_i, \beta_i)$, $1 \leq i \leq n-1$. Let $h = \gamma g - f$, then $r^{(i)}$ are the roots of h. Our assumption that f and g are not a multiple of each other implies that h is not a constant. The polynomial h is at most of degree n and clearly $h \in \mathbb{R}[x]$ as $f, g \in \mathbb{R}[x]$ and $\gamma \in \mathbb{R}$. The n-th root of h is real too as the coefficients of h are real.

Finally, we show that we cannot have γ_n to be less than α_n. We have that $\text{sign}\left(\dfrac{f(r)}{g(r)}\right) \neq \text{sign}\left(\dfrac{f(r^{(n-1)})}{g(r^{(n-1)})}\right)$ for $r^{(n-1)} \in (\alpha_{n-1}, \beta_{n-1})$ and $r \in (\beta_{n-1}, \alpha_n)$, as for $r \in (\beta_{n-1}, \alpha_n)$ we have that $\text{sign}(f(r)) = \text{sign}(f(r^{(n-1)}))$ but $\text{sign}(g(r)) \neq \text{sign}(g(r^{(n-1)}))$. And so the remaining root of h has to be larger than α_n, or more precisely $\gamma_n \in (\alpha_n, +\infty)$. □

The following result was demonstrated by Johnson [59].

Proposition 4.1.16. *Let $f \in \mathbb{R}[x]$ with roots $\alpha_1 < \alpha_2 < \ldots < \alpha_n$ and all $\alpha_i \in \mathbb{R}$. The the set of all polynomials which interlace f forms a convex set.*

Proof. Let $f_1, f_2 \in \mathbb{R}[x]$ be two polynomials which interlace f. We want to show that $\lambda f_1 + (1-\lambda) f_2$ interlaces f, for all $\lambda \in [0,1]$. Note that $\lambda f_1 + (1-\lambda) f_2$ is a monic polynomial, as f_1 and f_2 are. The degree of $\lambda f_1 + (1-\lambda) f_2$ is $n-1$, its roots are real and $\lambda f_1 + (1-\lambda) f_2$ sign interlaces f. Therefore by Lemma 4.1.13 $\lambda f_1 + (1-\lambda) f_2$ interlaces f. □

Remark. All polynomials that interlace f (f is separable) are of the form written in Lemma 4.1.14, i.e. $\sum_{i=1}^{n} \lambda_i \prod_{j \neq i}(x - \alpha_j)$, where $\lambda_i \in \mathbb{R}_+$. The polynomials $\prod_{i \neq j}(x - \alpha_i)$ are linearly independent over $\mathbb{R}$. This follows from the fact that if there exists $\lambda_j \in \mathbb{R}$ such that $\sum_{j=1}^{n} \lambda_j \prod_{i \neq j}(x - \alpha_j)$, then evaluating at α_k we would have that $\lambda_k \prod_{i \neq j}(\alpha_k - \alpha_i) = 0$ thus $\lambda_k = 0$. Hence polynomials $\prod_{i\neq j}(x-\alpha_j)$ span the space of polynomials of degree $\leq n-1$. Restriction to the monic polynomials implies that $\sum_{i=1}^{n}\lambda_i = 1$.

Proposition 4.1.17. [Lemma 4, 78] *Let $\gamma > 0$, $\alpha_1 < \beta_1 < \alpha_2 < \ldots < \beta_{n-1} < \alpha_n \leq A$ and*

$$h = \frac{\gamma\prod_{i=1}^{n-1}(x-\beta_i)}{\prod_{i=1}^{n}(x-\alpha_i)}.$$

Then we can write h as

$$h = \sum_{i=1}^{n}\frac{\lambda_i}{x-\alpha_i}$$

where $\lambda_i \in \mathbb{R}_+$ for $1 \leq i \leq n$. Also $h(x) = 1$ has real roots $\gamma_1, \ldots, \gamma_n$ such that $\alpha_1 < \gamma_1 < \beta_1 < \alpha_2 < \gamma_2 < \ldots < \beta_{n-1} < \alpha_n < \gamma_n$, and $\gamma_n > A$ if and only if $h(A) > 1$.

Proof. Let $f = \prod_{i=1}^{n}(x-\alpha_i)$ and $g = \prod_{i=1}^{n-1}(x-\beta_i)$. Then by the argument above we know that we can write g as

$$g = \sum_{i=1}^{n}\lambda_i\prod_{j\neq i}(x-\alpha_j)$$

with all $\lambda_i \geq 0$. So we have that

$$h = \frac{\gamma g}{f} = \frac{\gamma\sum_{i=1}^{n}\lambda_i\prod_{j\neq i}(x-\alpha_j)}{\prod_{i=1}^{n}(x-\alpha_i)} = \sum_{i=1}^{n}\frac{\lambda'_i}{x-\alpha_i},$$

where $\lambda'_i = \gamma\lambda_i$. Let $h(x) = 1$, then $\dfrac{\gamma g}{f} = 1$ implies that $\gamma g - f = 0$ and by Lemma 4.1.15 it follows that $h(x) = 1$ has real roots $\gamma_1, \ldots, \gamma_n$ such that $\alpha_1 < \gamma_1 < \beta_1 < \alpha_2 < \gamma_2 < \ldots < \beta_{n-1} < \alpha_n < \gamma_n$. Finally, we have that $\dfrac{\gamma g}{f}$ goes from positive infinity to one as x goes from α_n to γ_n. Therefore if $h(A) > 1$ then $\gamma_n > A$ when $h(\gamma_n) = 1$. Likewise, if $\gamma_n > A$ then $h(A) > 1$. □

Remark. Given a polynomial of the form $f = \sum_{i=1}^{n}\dfrac{\lambda_i}{x-\alpha_i}$, where all $\lambda_i \in \mathbb{R}_+$, by the proof of the proposition above we can write f as $\dfrac{\gamma\prod_{i=1}^{n-1}(x-\beta_i)}{\prod_{i=1}^{n}(x-\alpha_i)}$, where $\prod_{i=1}^{n-1}(x-\beta_i)$ interlaces $\prod_{i=1}^{n}(x-\alpha_i)$.

Circular interlacing condition

We shall use standard notation $f(z)$ and $g(x)$ to assist us to distinguish between polynomials which may have complex roots and those that have all real roots, respectively.

Definition 4.1.18. *Let $f, g \in \mathbb{R}[z]$ be two coprime polynomials such that their leading terms are positive and such that all their roots are on the unit circle. We say that f, g satisfy the* ***circular interlacing condition*** *if their roots interlace on the unit circle.*

Remark. If polynomials f and g satisfy the circular interlacing condition then f and g are of the same degree and do not have repeating roots. Further, 1 and -1 appear as roots of fg. This follows from that fact that all the roots of f and g come in conjugate pairs. Thus the conjugate pairs nearest to the real axis need to be interlaced by -1 and 1.

Example 4.1.19. Polynomials $z-1$ and $z+1$ satisfy interlacing condition.

For more examples and details about polynomials that satisfy the circular interlacing condition we refer to [81].

Lemma 4.1.20. *Let $f, g \in \mathbb{Z}[x]$ be such that f is of degree n, g interlaces f and all roots of f are in $(-2, 2)$. Then $z^n f\left(z+\dfrac{1}{z}\right)$ and $(z^2-1)z^{n-1}g\left(z+\dfrac{1}{z}\right)$ satisfy the circular interlacing condition.*

Proof. Let $\tilde{f}(z) = z^n f\left(z+\dfrac{1}{z}\right)$ and $\tilde{g}(z) = (z^2-1)z^{n-1}g\left(z+\dfrac{1}{z}\right)$. First note that $\tilde{f}(z)$ and $\tilde{g}(z)$ are both of degree $2n$ and ± 1 are roots of $\tilde{f}(z)\tilde{g}(z)$. Given that the roots of $f(x)$, and therefore of $g(x)$, are all in $(-2, 2)$ implies that the roots of $\tilde{f}(z)$ and $\tilde{g}(z)$ are all on the unit circle. This follows from the fact that if we have $f(x) = \prod_{j=1}^{n}(x-\alpha_j)$, $\alpha_j \leq \alpha_{j+1}$ then all the roots of $\tilde{f}(z)$ are the roots of $z^2 - \alpha_j z + 1$ for some j. So $\tilde{f}(z) = \prod_{j=1}^{n}(z-\gamma_j)(z-\gamma_{n+j})$, where $\gamma_{j,n+j} = \dfrac{\alpha_j \pm i\sqrt{4-\alpha_j^2}}{2}$. Similarly we have $g(x) = \prod_{j=1}^{n-1}(x-\beta_j)$, $\beta_j \leq \beta_{j+1}$, and $\tilde{g}(z) = (z^2 - 1)\prod_{j=1}^{n-1}(z - \delta_j)(z - \delta_{n-1+j})$ where $\delta_{j,n-1+j} = \dfrac{\beta_j \pm i\sqrt{4 - \beta_j^2}}{2}$. The fact that these two polynomials interlace on the unit circle is clear. □

Proposition 4.1.21. [Prop. 5, 78] *Let $f, g \in \mathbb{Z}[z]$ be polynomials satisfying the circular interlacing condition. Then $(z^2 - 1)f - zg$ is the minimal polynomial of a Salem number, possibly multiplied by a cyclotomic polynomial or a Pisot number.*

Remark. For a polynomial $f \in \mathbb{R}[z]$ such that its roots are all on the unit circle and $f(\pm 1) \neq 0$, by Proposition 4.1.5 there exists a polynomial $\tilde{f}$ such that $f(z) = z^m \tilde{f}\left(z + \frac{1}{z}\right)$, where all the roots of $\tilde{f}$ are in $[-2, 2]$. If $\tilde{f}$ has all roots in $[-2, 2]$, then $z^m \tilde{f}\left(z + \frac{1}{z}\right)$ has all its roots on the unit circle. Therefore we will show that for a polynomial $h = (z^2 - 1)f - zg$ we can find a polynomial $\tilde{h}$ such that $h(z) = z^m \tilde{h}\left(z + \frac{1}{z}\right)$ and the roots of $\tilde{h}$ are all but one in $[-2, 2]$. A real algebraic integer $\alpha > 1$ is a **Pisot** number if all its conjugates have an absolute value strictly less than 1.

In this proposition it will be possible that instead of the minimal polynomial of a Salem number, $(z^2 - 1)f - zg$ will be the minimal polynomial of a quadratic Pisot number multiplied by a cyclotomic polynomial.

Proof. Let $f(z)$ and $g(z)$ satisfy the condition of the proposition and let γ be the leading coefficient of $g(z)$. Set $x = z + \frac{1}{z}$. We examine the following polynomial

$$\frac{z}{z^2 - 1}\frac{g(z)}{f(z)}.$$

We need to consider three separate cases:

(i) If $f(z)$ and $g(z)$ are of degree $2n$ and $(z^2 - 1)$ divides $g(z)$ then let $g(z) = (z^2 - 1)\overline{g}(z)$, $\overline{g}(z) \in \mathbb{Z}[z]$. There exist polynomials $\tilde{g}(x), \tilde{f}(x) \in \mathbb{Z}[x]$ such that $\overline{g}(z) = z^{n-1}\tilde{g}(x)$ and $f(z) = z^n \tilde{f}(x)$, then

$$\frac{z}{z^2 - 1}\frac{g(z)}{f(z)} = \frac{z}{z^2 - 1}\frac{z^{n-1}(z^2 - 1)\tilde{g}(x)}{z^n \tilde{f}(x)}$$

$$\begin{aligned}&= \frac{\tilde{g}(x)}{\tilde{f}(x)}\\&= \frac{\prod_{i=1}^{n-1}(x-\beta_i)}{\prod_{i=1}^{n}(x-\alpha_i)},\end{aligned}$$

where α_is are the roots of $\tilde{f}(x)$ and β_is are the roots of $\tilde{g}(x)$. Following the remark above we know that these roots are totally real and are contained in the interval $[-2, 2]$, i.e. $-2 < \alpha_1 < \beta_1 < \alpha_2 < \ldots < \beta_{n-1} < \alpha_n < 2$. We apply Proposition 4.1.17. Thus

$$\frac{\prod_{i=1}^{n-1}(x-\beta_i)}{\prod_{i=1}^{n}(x-\alpha_i)} = \sum_{i=1}^{n} \frac{\lambda_i}{x-\alpha_i},$$

and so $\sum_{i=1}^{n} \dfrac{\lambda_i}{x-\alpha_i} = 1$ has real roots γ_i such that $-2 < \alpha_1 < \gamma_1 < \beta_1 < \alpha_2 < \gamma_2 < \ldots < \beta_{n-1} < \alpha_n < \gamma_n$. For the polynomial $(z^2-1)f(z)-zg(z)$ to be the minimal polynomial of a Salem number it is necessary for $\gamma_n > 2$. This will be addressed in the end of this proof.

(ii) Assume now that $f(z), g(z)$ are of even degree and z^2-1 divides $f(z)$. Then $f(z) = (z^2-1)\overline{f}(z)$, and there exist polynomials $\tilde{f}(x), \tilde{g}(x)$ such that $\overline{g}(z) = z^n\tilde{g}(x), \overline{f}(z) \in \mathbb{Z}[z]$ and $\overline{f}(z) = z^{n-1}\tilde{f}(x)$. Observe that $\left(z - \dfrac{1}{z}\right)^2 = x^2-4$, then

$$\begin{aligned}\frac{z}{z^2-1}\frac{g(z)}{f(z)} &= \frac{z}{z^2-1}\frac{z^n\tilde{g}(x)}{z^{n-1}(z^2-1)\tilde{f}(x)}\\&= \frac{z^2}{(z^2-1)^2}\frac{\tilde{g}(x)}{\tilde{f}(x)}\\&= \frac{1}{\left(z-\dfrac{1}{z}\right)^2}\frac{\tilde{g}(x)}{\tilde{f}(x)}\\&= \frac{\prod_{i=1}^{n}(x-\beta_i)}{(x^2-4)\prod_{i=1}^{n-1}(x-\alpha_i)}.\end{aligned}$$

Similarly to the case before, we apply Proposition 4.1.17 and see that $-2 < \beta_1 < \alpha_1 < \ldots < \beta_n < 2$. It is clear here that the root γ_n of $h(z) = 1$ is a Salem number, as $\gamma_n > 2$. However it is still possible that

$(z^2-1)f(z) - zg(z)$ may be reducible, but any non-Salem factor has to be cyclotomic.

(*iii*) The last two cases to be consider are when $f(z), g(z)$ have an odd degree $2n+1$, $z+\epsilon$ divides $f(z)$ and $z-\epsilon$ divides $g(z)$, where $\epsilon = \pm 1$. Then $f(z) = (z+\epsilon)\overline{f}(z)$ and $g(z) = (z-\epsilon)\overline{g}(z), \overline{f}(z), \overline{g}(z) \in \mathbb{Z}[z]$ and there exist $\tilde{f}, \tilde{g} \in \mathbb{Z}[x]$ such that $\overline{g}(z) = z^n\tilde{g}(x)$ and $\overline{f}(z) = z^n\tilde{f}(x)$, then

$$\begin{aligned}\frac{z}{z^2-1}\frac{g(z)}{f(z)} &= \frac{z}{z^2-1}\frac{z^n(z-\epsilon)\tilde{g}(x)}{z^n(z+\epsilon)\tilde{f}(x)} \\ &= \frac{z}{(z+\epsilon)(z-\epsilon)}\frac{(z-\epsilon)\tilde{g}(x)}{(z+\epsilon)\tilde{f}(x)} \\ &= \frac{z}{z^2+2\epsilon z+\epsilon^2}\frac{\tilde{g}(x)}{\tilde{f}(x)} \\ &= \frac{1}{z+\dfrac{1}{z}+2\epsilon}\frac{\tilde{g}(x)}{\tilde{f}(x)} \\ &= \frac{\prod_{i=1}^n (x-\beta_i)}{(x+2\epsilon)\prod_{i=1}^n (x-\alpha_i)}.\end{aligned}$$

From Proposition 4.1.17 we have that $-2 < \beta_1 < \alpha_1 < \ldots < \beta_n < \alpha_n < 2$ if $\epsilon = 1$ and $-2 < \alpha_1 < \beta_1 < \alpha_2 < \ldots < \beta_n < 2$ if $\epsilon = -1$.

It remains to show that we have that $\gamma_n > 2$ in all the cases. We have to use the latter part of Proposition 4.1.17, in particular we claim that at $x = 2$ $\left(\text{that is } z = 1, \text{ as } x = z + \dfrac{1}{z}\right)$ we have $\tilde{h}(2) > 1$. This follows from the fact that one of $f(1)$ or $g(1)$ is zero and the other one is positive, as these polynomials have a positive leading term and all the roots are less than or equal to one. □

Proposition 4.1.22. [Prop. 6, 78] *Let $f_i, g_i \in \mathbb{R}[z]$ be pairs of polynomials satisfying the circular interlacing condition for $i = 1, \ldots, n$. Then $\sum_{i=1}^n \dfrac{g_i}{f_i} = \dfrac{g}{f}$ where f and g also satisfy the circular interlacing condition.*

Proof. Let $f_i, g_i \in \mathbb{R}[z]$ be of degree n_i. Then by the previous proposition for each i we have that

$$\frac{z}{z^2-1}\frac{g_i}{f_i} = \sum_{j=1}^{n_i} \frac{\lambda_j^{(i)}}{x-\alpha_j^{(i)}},$$

such that $x = z + \frac{1}{z}$, $\lambda_i \in \mathbb{R}_+$ and $\alpha_i \in [-2, 2]$. Summing over i we get

$$\begin{aligned}\sum_{i=1}^{n} \frac{z}{z^2-1}\frac{g_i}{f_i} &= \sum_{i=1}^{n}\sum_{j=1}^{n_i} \frac{\lambda_j^{(i)}}{x-\alpha_j^{(i)}} \\ &= \sum_{k=1}^{m} \frac{\lambda_k}{x-\alpha_k},\end{aligned}$$

where $m \leq \sum_{i=1}^{n} n_i$. By Proposition 4.1.17 this sum is equal to $\frac{\prod(x-\beta_j)}{\prod(x-\alpha_i)}$, where $-2 \leq \alpha_1 < \beta_1 < \ldots < \alpha_d \leq 2$. On the substitution of $x = z + \frac{1}{z}$, and considering different cases the results follows. □

Proposition 4.1.23. [Lemma 1, (ii), 17] *Let ζ be a root of unity. Then at least one of $-\zeta, \zeta^2, -\zeta^2$ is a conjugate of ζ.*

Proof. Let $\zeta = \exp\left(\frac{2\pi i k}{n}\right)$ such that $\gcd(k, n) = 1$. It is known that for all l such that $\gcd(l, n) = 1$, we have that ζ^l is conjugate of ζ. We partition integers into the following three types:

(i) Let $n = 2m$, where m is odd, and put $l = m + 2$. Then $\gcd(l, n) = 1$, k is odd and

$$\begin{aligned}\zeta^l &= \exp\left(\frac{2\pi i k(m+2)}{2m}\right) \\ &= \exp(\pi i k)\exp\left(\frac{(2\pi i k)2}{2m}\right) \\ &= (-1)^k \zeta^2 \\ &= -\zeta^2.\end{aligned}$$

(ii) Let $n = 4m$ and put $l = 2m + 1$. Then $\gcd(l, n) = 1$, k is odd and

$$\zeta^l = \exp\left(\frac{2\pi i k(2m+1)}{4m}\right)$$

$$
\begin{aligned}
&= \exp(\pi i k)\exp\left(\frac{2\pi i k}{4m}\right) \\
&= -\zeta.
\end{aligned}
$$

(iii) Let $n = 2m+1$ and $l = 2$. Then $\gcd(l, n) = 1$ and $\zeta^l = \zeta^2$ is a conjugate of ζ. □

4.1.3 Salem numbers of trace -2

The following findings first appeared in [83].

Lemma 4.1.24. *Let $p, q \in \mathbb{Z}[z]$ be a pair of coprime polynomials such that*

$$
\frac{q}{p} = \frac{z^{p_1+p_2}-1}{(z^{p_1}-1)(z^{p_2}-1)} + \frac{z^{p_3+p_4}-1}{(z^{p_3}-1)(z^{p_4}-1)} + \frac{z^{p_5+n}-1}{(z^{p_5}-1)(z^{n}-1)}, \qquad (4.1.1)
$$

where p_1, p_2, p_3, p_4, p_5 are distinct prime numbers, and $n \geq 5$ such that n is coprime with all p_i. Let $(p_1, p_2, p_3, p_4, p_5)$ be one of the following 5-tuples:

$$
\begin{array}{ccc}
(2,3,5,7,11), & (2,3,5,7,13), & (2,3,5,11,13), \\
(2,3,5,11,19), & (2,3,5,13,17), & (2,3,5,13,19), \\
(2,3,5,17,19), & (2,3,7,11,13), & (2,3,7,11,17), \\
(2,3,7,11,19), & (2,3,7,13,17), & (2,3,7,13,19), \\
(2,3,11,13,19), & (2,3,11,17,19), & (2,3,13,17,19).
\end{array}
$$

Then the polynomial $(z^2-1)p - zq$ is the minimal polynomial of a Salem number of trace -2 and degree $n + p_1 + p_2 + p_3 + p_4 + p_5 - 3$.

Proof. Let us write equation (4.1.1) over a common denominator to give us

$$
\frac{q(z)}{p(z)} = \frac{\Phi_{p_3}\Phi_{p_4}\Phi_{p_5}\prod_{\substack{d|p_1+p_2\\ d\neq 1}}\Phi_d \prod_{\substack{d'|n\\ d'\neq 1}}\Phi_{d'} + \Phi_{p_1}\Phi_{p_2}\Phi_{p_5}\prod_{\substack{d|p_3+p_4\\ d\neq 1}}\Phi_d \prod_{\substack{d'|n\\ d'\neq 1}}\Phi_{d'} + \Phi_{p_1}\Phi_{p_2}\Phi_{p_3}\Phi_{p_4}\prod_{\substack{d|p_5+n\\ d\neq 1}}\Phi_d}{\Phi_{p_1}\Phi_{p_2}\Phi_{p_3}\Phi_{p_4}\Phi_{p_5}\prod_{d|n}\Phi_d},
$$

and from the coprimality hypothesis we deduce that

$$
\begin{aligned}
p(z) &= \Phi_{p_1}\Phi_{p_2}\Phi_{p_3}\Phi_{p_4}\Phi_{p_5}\prod_{d|n}\Phi_d \\
&= z^{p_1+p_2+p_3+p_4+p_5+n-5} + 5z^{p_1+p_2+p_3+p_4+p_5+n-6} + \dots,
\end{aligned}
$$

and

$$
q(z) = \Phi_{p_3}\Phi_{p_4}\Phi_{p_5}\prod_{\substack{d|p_1+p_2\\ d\neq 1}}\Phi_d \prod_{\substack{d'|n\\ d'\neq 1}}\Phi_{d'} + \Phi_{p_1}\Phi_{p_2}\Phi_{p_5}\prod_{\substack{d|p_3+p_4\\ d\neq 1}}\Phi_d \prod_{\substack{d'|n\\ d'\neq 1}}\Phi_{d'} + \Phi_{p_1}\Phi_{p_2}\Phi_{p_3}\Phi_{p_4}\prod_{\substack{d|p_5+n\\ d\neq 1}}\Phi_d
$$

$$= 3z^{p_1+p_2+p_3+p_4+p_5+n-5} + \dots .$$

Thus $(z^2-1)p-zq$ is of degree $n+\sum_{i=1}^{5} p_i-3$ and of trace -2. By Proposition 4.1.21 we know that equation (4.1.1) satisfies the circular interlacing condition, and by Proposition 4.1.22 we have that $(z^2-1)p-zq$ is the minimal polynomial of a Salem number, with a possibility that $(z^2-1)p-zq$ is not irreducible and is divisible by a cyclotomic polynomial or a reciprocal quadratic polynomial of a Pisot number. Thus to prove this proposition it remains to show that for each 5-tuple and a coprime n we get an irreducible polynomial.

Let us define

$$\frac{Q(y,z)}{P(y,z)} = \frac{z^{p_1+p_2}-1}{(z^{p_1}-1)(z^{p_2}-1)} + \frac{z^{p_3+p_4}-1}{(z^{p_3}-1)(z^{p_4}-1)} + \frac{yz^{p_5}-1}{(z^{p_5}-1)(y-1)},$$

and consider the curve defined by $C(y,z) : (z^2-1)P(y,z) - zQ(y,z) = 0$. Note that $C(z^n,z) : (z^2-1)p - zq = 0$. By Proposition 4.1.23 we know that if ζ is a root of unity then it is a conjugate to one of $-\zeta, \zeta^2$ or $-\zeta^2$. Thus if $(z^2-1)p-zq$ is divisible by a cyclotomic polynomial then there exist at least two cyclotomic points on $C(y,z)$ — (y,z) and $(-y,-z)$, (y^2,z^2) or $(-y^2,-z^2)$. In particular, (y,z) is a cyclotomic point on both $C(y,z)$ and either $C_1(y,z)$: $(z^2-1)P(-y,-z)+zQ(-y,-z)$, $C_2(y,z) : (z^4-1)P(y^2,z^2)-z^2Q(y^2,z^2)$ or $C_3(y,z) : (z^4-1)P(-y^2,-z^2)+z^2Q(-y^2,-z^2)$. For each of the three 2-tuples (C,C_1), (C,C_2) and (C,C_3) we can eliminate for y or z to get a single variable polynomial which has only a finite set of solutions. We now proceed discussing four possible arising cases:

I. If we eliminate for z in (C,C_1) and get a nonmonic irreducible polynomial, then such curves cannot have any cyclotomic points in common. Take for example $(p_1,p_2,p_3,p_4,p_5) = (2,3,5,7,13)$.

II. For (p_1,p_2,p_3,p_4,p_5), if we eliminate for y in (C,C_2) and find cyclotomic factors $\Phi_{p_1}, \Phi_{p_2}, \Phi_{p_3}, \Phi_{p_4}$, and Φ_{p_5}, then given that these are the precise factors of p, and the fact that $\gcd(p,g)=1$, implies that none of these points can correspond to a cyclotomic point on C. Take for example $(p_1, p_2, p_3, p_4, p_5) = (2, 3, 5, 7, 11)$.

III. Consider a case $(2, 3, p_3, p_4, p_5)$, where if we eliminate y for (C, C_3), then we find a cyclotomic factor of $\Phi_{12}(z) = z^4 - z^2 + 1$ with roots $\exp\left(\frac{2\pi ik}{12}\right)$, where $\gcd(k, 12) = 1$. Moreover, if we eliminate the same curves for z, then we find a factor of $\Phi_4(y) = y^2 + 1$. If (y, z) is a cyclotomic points on both curves, then $y = z^n$ and $\exp\left(\frac{2\pi i}{4}\right) = \exp\left(\frac{2\pi ikn}{12}\right)$. As $\gcd(k, 12) = 1$, this implies that $3 \mid n$, contradicting our assumption of coprimality of n and 3. See for example $(p_1, p_2, p_3, p_4, p_5) = (2, 3, 5, 7, 11)$.

IV. Consider a tuple $(2, 5, p_3, p_4, p_5)$, such that if we eliminate y for (C, C_1), we find a cyclotomic factor of $\Phi_{20}(z) = z^8 - z^6 + z^4 - 1$ (its roots are $\exp\left(\frac{2\pi ik}{20}\right)$, where $\gcd(k, 20) = 1$). Furthermore, assume that if we eliminate the same curves for z, then we find a factor of $\Phi_4(y) = y^2 + 1$. And so if (y, z) is a cyclotomic point on both curves, then $y = z^n$ and $\exp\left(\frac{2\pi i}{4}\right) = \exp\left(\frac{2\pi ikn}{20}\right)$. As $\gcd(k, 20) = 1$, this implies that $5 \mid n$, contradicting our assumption of coprimality of n and 5. See for example $(p_1, p_2, p_3, p_4, p_5) = (2, 3, 5, 17, 19)$.

Table 4.1 summaries how cyclotomic points were eliminated for each of the fifteen 5-tuples $(p_1, p_2, p_3, p_4, p_5)$. □

Notice that in the list we omitted a 5-tuple $(2, 3, 5, 11, 17)$. If we eliminate y on (C, C_2) among the cyclotomic factors as in case II. we also get an additional cyclotomic factor $\Phi_{13}(z)$ which we cannot eliminate, and if we consider $C(z^{103}, z)$, we will find that it is divisible by $\Phi_{13}(z)$.

Proposition 4.1.25. *There are Salem numbers of trace -2 of degree $2d$ for all $d \geq 12$.*

Proof. For $d = 19$ and for all $d \geq 21$ it is sufficient to check that all even residues modulo $2 \times 3 \times 5 \times 7 \times 11 \times 13 \times 17 \times 19 = 9699690$ are covered by the 15

Table 4.1: Cases

$(p_1, p_2, p_3, p_4, p_5)$	(C, C_1)	(C, C_2)	(C, C_3)
(2,3,5,7,11)	III.	II.	III.
(2,3,5,7,13)	I.	II.	I.
(2,3,5,11,13)	I.	II.	I.
(2,3,5,11,19)	III.	II.	III.
(2,3,5,13,17)	I.	II.	I.
(2,3,5,13,19)	I.	II.	I.
(2,3,5,17,19)	IV.	II.	IV.
(2,3,7,11,13)	I.	II.	I.
(2,3,7,11,17)	III.	II.	III.
(2,3,7,11,19)	I.	II.	I.
(2,3,7,13,17)	I.	II.	I.
(2,3,7,13,19)	I.	II.	I.
(2,3,11,13,19)	I.	II.	I.
(2,3,11,17,19)	III.	II.	III.
(2,3,13,17,19)	I.	II.	I.

infinite families of 5-tuples, which they are. For $d \in \{12, 13, 14, 15, 16, 17, 18, 20\}$ we have the following polynomials:

$$x^{24} + 2x^{23} - 4x^{22} - 28x^{21} - 72x^{20} - 116x^{19} - 116x^{18} - 27x^{17} + 166x^{16}$$
$$+431x^{15} + 701x^{14} + 900x^{13} + 973x^{12} + \ldots + 1,$$

$$x^{26} + 2x^{25} + x^{24} - 3x^{23} - 9x^{22} - 16x^{21} - 23x^{20} - 30x^{19} - 36x^{18} - 40x^{17}$$
$$- 42x^{16} - 44x^{15} - 46x^{14} - 47x^{13} - \ldots + 1,$$

$$x^{28} + 2x^{27} + x^{26} - 3x^{25} - 9x^{24} - 16x^{23} - 23x^{22} - 30x^{21} - 36x^{20} - 40x^{19}$$
$$-42x^{18} - 43x^{17} - 43x^{16} - 43x^{15} - 43x^{14} - \ldots + 1,$$

$$x^{30} + 2x^{29} - 3x^{28} - 19x^{27} - 39x^{26} - 51x^{25} - 53x^{24} - 53x^{23} - 55x^{22} - 56x^{21}$$
$$- 51x^{20} - 41x^{19} - 34x^{18} - 38x^{17} - 49x^{16} - 55x^{15} - \ldots + 1,$$

$$x^{32}+2x^{31}+x^{30}-3x^{29}-9x^{28}-16x^{27}-23x^{26}-29x^{25}-33x^{24}-35x^{23}$$
$$-36x^{22}-38x^{21}-41x^{20}-45x^{19}-49x^{18}-52x^{17}-53x^{16}-\ldots+1,$$

$$x^{34}+2x^{33}+x^{32}-3x^{31}-8x^{30}-12x^{29}-14x^{28}-15x^{27}-15x^{26}-14x^{25}$$
$$-13x^{24}-13x^{23}-13x^{22}-12x^{21}-9x^{20}-4x^{19}+x^{18}+3x^{17}+\ldots+1,$$

$$x^{36}+2x^{35}+x^{34}-3x^{33}-8x^{32}-12x^{31}-13x^{30}-11x^{29}-8x^{28}-7x^{27}-9x^{26}$$
$$-13x^{25}-17x^{24}-20x^{23}-21x^{22}-19x^{21}-15x^{20}-12x^{19}-11x^{18}-\ldots+1,$$

$$x^{40}+2x^{39}+x^{38}-3x^{37}-9x^{36}-16x^{35}-23x^{34}-29x^{33}-33x^{32}-35x^{31}$$
$$-36x^{30}-37x^{29}-38x^{28}-40x^{27}-43x^{26}-46x^{25}-48x^{24}-49x^{23}-49x^{22}$$
$$-49x^{21}-49x^{20}-\ldots+1.$$ □

Corollary 4.1.26. *There exist counterexamples to Estes–Guralnick's conjecture for every degree strictly larger than 5.*

Proof. From the proposition above we know of existence of Salem numbers of trace -2 for degrees $2d$ where $d \geq 12$. Corollary 4.1.7 implies that there exist monic integer irreducible polynomials of degree d with all real and positive roots and trace $2d-2$ for all $d \geq 12$. By Corollary 3.2.2 each such polynomial is a counterexample to the Estes–Guralnick conjecture. Counterexamples to Estes–Guralnick's conjecture for degrees $6, 7, 8, 9, 10, 11$ come from the small-span method, and can be found in [76]. □

Corollary 4.1.27. *For each degree n strictly larger than 11 there exists polynomial $f \in \mathbb{Z}[x]$ such that f is a monic irreducible polynomial of degree n, all roots of f are real and positive, and f is not the characteristic polynomial of an integer oscillatory matrix.* □

In the proof of Proposition 4.1.25, the case $d = 15$ first appeared in [32] while the remaining polynomials are from [83]. Chris Smyth showed that there exist Salem numbers of trace -1 for all even degrees larger than 6 [100], and James McKee and Chris Smyth showed that there exist Salem numbers of every trace [78]. We conjecture the following.

Conjecture 4.1.28. For all $m \in \mathbb{N}$ there exists $N = \mathrm{N}(m)$ such that for all $d \geq N$ there exists a Salem number of trace $-m$ and degree $2d$.

4.2 Convex sets

This section focuses on the geometry of numbers approach to the problem of Estes and Guralnick. Let us introduced some basic concepts from discrete geometry. We shall use [73] as the main reference.

Definition 4.2.1. *The set $C \subset \mathbb{R}^n$ is a **convex set** if for each $x, y \in C$ and for every $0 \leq \lambda \leq 1$, we have $\lambda x + (1-\lambda)y \in C$.*

Definition 4.2.2. *Let $X \subset \mathbb{R}^n$ and $|X| < \infty$. The **convex hull** of X is defined as*

$$\mathrm{conv}(X) := \left\{ \sum_{i=1}^{|X|} \lambda_i \boldsymbol{x}_i | \boldsymbol{x}_i \in X,\ \lambda_i \in \mathbb{R}_+,\ \sum_{i=1}^{|X|} \lambda_i = 1 \right\}.$$

Definition 4.2.3. *Let $X \subset \mathbb{R}^n$. Then $x \in X$ is a **vertex** of $\mathrm{conv}(X)$ if and only if $x \notin \mathrm{conv}(X \setminus \{x\})$.*

Definition 4.2.4. *A **simplex** $C \subset \mathbb{R}^d$ is a convex set with $d+1$ distinct vertices.*

Note that the above definition is equivalent to an existence of $\mathbf{v}_1, \ldots, \mathbf{v}_{d+1} \in C$ such that $\{\mathbf{v}_1 - \mathbf{v}_{d+1}, \ldots, \mathbf{v}_d - \mathbf{v}_{d+1}\}$ is linearly independent and $C = \mathrm{conv}(\mathbf{v}_1, \ldots, \mathbf{v}_{d+1})$.

Definition 4.2.5. *Let $f \in \mathbb{Z}[x]$ be a monic separable polynomial such that all its roots are real, i.e. $f = \prod_{i=1}^{n}(x - \alpha_i)$ where $\alpha_i \in \mathbb{R}$. Then we say that f is* ***interlaced*** *(over $\mathbb{Z}$) if there exists a monic polynomial $g \in \mathbb{Z}[x]$ such that g interlaces f.*

Proposition 4.2.6. [59] *Let $f = \prod_{i=1}^{n}(x - \alpha_i) \in \mathbb{Z}[x]$ be a monic separable polynomial such that all its roots are real. Let $C \subset \mathbb{R}[x]$ be the set of all monic polynomials that interlace f. Then $C = \operatorname{conv}(\{f_i | i = 1, \dots, n\})$, where C is a simplex and*

$$f_i := \prod_{j \neq i}^{n-1}(x - \alpha_j) = x^{n-1} + b_1^{(i)} x^{n-2} + \ldots + b_{n-1}^{(i)}.$$

Proof. Let f and f_i be as above. Let $g \in C$ be any monic real polynomial that interlaces f. To prove the proposition it suffices to show that there exist $\lambda_i \in \mathbb{R}_+$ such that $\sum_{i=1}^{n} \lambda_i = 1$ and $g = \sum_{i=1}^{n} \lambda_i f_i$.

Let f' be the derivative of f, then $f'(\alpha_i)g(\alpha_i) > 0$ for all α_i. Let $\lambda_i \in \mathbb{R}_+$ such that $g(\alpha_i) = \lambda_i f'(\alpha_i)$. We note that $f'(\alpha_i) = f_i(\alpha_i)$, and thus $g(\alpha_i) = \lambda_i f_i(\alpha_i)$. Let us define a polynomial $F(x) = g(x) - \sum_{i=1}^{n} \lambda_i f_i(x)$, which is of degree less than or equal to $n - 1$, and $F(\alpha_i) = 0$ for all α_i. Thus $F = 0$ and therefore $g = \sum_{i=1}^{n} \lambda_i f_i$. Given that g and f_i are monic implies that $\sum_{i=1}^{n} \lambda_i = 1$, the proposition follows. □

It is important to note that the existence of an integer polynomial in this convex set will imply that the polynomial f is interlaced.

Let $\mathbb{R}[x]_M^{n-1}$ be the set of all monic real polynomials of degree $n - 1$, i.e. polynomials $x^{n-1} + g$ where g is in the span of $\{1, x, \dots, x^{n-2}\}$ over $\mathbb{R}$. Let us consider the map

$$\begin{aligned} \phi_{n-1} : \mathbb{R}[x]_M^{n-1} &\longrightarrow \mathbb{R}^{n-1} \\ x^{n-1} + \sum_{i=1}^{n-1} a_i x^{n-1-i} &\mapsto (a_1, \dots, a_{n-1})^t, \end{aligned}$$

mapping real monic polynomials of degree $n-1$ into $\mathbb{R}^{n-1}$, i.e. mapping x^{n-k-1} to $\mathbf{e}_k$ for $k = 1, \ldots, n-1$, where $\mathbf{e}_k$ is a vector of a standard basis. For our polynomial $f \in \mathbb{Z}[x]$ let us define

$$\mathcal{K}(f) := \{\phi_{n-1}(g) | g \in \operatorname{conv}(\{f_i | i = 1, \ldots, n\})\}$$

(we shall write $\mathcal{K}$ when it is clear what polynomial we imply). It is easy to see that $\mathcal{K}$ is a convex set too. Points $\mathbf{v}_i := \phi_n(f_i)$ are the vertices of $\mathcal{K}$. If $\operatorname{int}(\mathcal{K}) \cap \mathbb{Z}^{n-1} \neq \emptyset$ then the polynomial f is interlaced, where $\operatorname{int}(\mathcal{K})$ is the interior of $\mathcal{K}$. Note that if we do not restrict to the interior of $\mathcal{K}$ then the integral points may correspond to polynomials whose roots interlace not in a strict sense.

To our simplex $\mathcal{K}$ we can associate a real matrix $A(\mathcal{K}) := A \in \operatorname{Mat}(n-1, n, \mathbb{R})$, where the vertices of $\mathcal{K}$ correspond to the columns of A. Thus we have $A_{ij} := \sum_{\substack{1 \leq m_1 < \ldots < m_i \leq n \\ m_k \neq j}} (-1)^i \alpha_{m_1} \ldots \alpha_{m_i}$.

Proposition 4.2.7. *Let*

$$\prod_{i=1}^{n} (x - \alpha_i) = \sum_{i=0}^{n} (-1)^i a_i x^{n-i},$$

where $a_0 = 1$. Then

$$\sum_{\substack{1 \leq m_1 < \ldots < m_k \leq n \\ m_l \neq i}} \alpha_{m_1} \ldots \alpha_{m_k} = \sum_{j=0}^{k} (-1)^j \alpha_i^j a_{k-j}.$$

Remark. Coefficients a_i are elementary symmetric polynomials in $\alpha_1, \ldots, \alpha_n$, i.e. $a_i = \sum_{1 \leq m_1 < \ldots < m_i \leq n} \alpha_{m_1} \ldots \alpha_{m_i}$.

Proof. We prove the proposition by induction on k. For $k = 1$ we have

$$\sum_{\substack{j=1 \\ j \neq i}}^{n} \alpha_j = a_1 - \alpha_i.$$

Assume now that the proposition holds for k, then for $k+1$ we have

$$\sum_{\substack{1 \leq m_1 < \ldots < m_{k+1} \leq n \\ m_l \neq i}} \alpha_{m_1} \ldots \alpha_{m_{k+1}} = a_{k+1} - \sum_{\substack{1 \leq m_1 < \ldots < m_k \leq n \\ m_l \neq i}} \alpha_i \alpha_{m_1} \ldots \alpha_{m_k}$$

$$\begin{aligned}
&= a_{k+1} - \alpha_i \sum_{\substack{1\le m_1<\ldots<m_k\le n \\ m_l\ne i}} \alpha_{m_1}\ldots\alpha_{m_k} \\
&= a_{k+1} - \alpha_i \sum_{j=0}^{k} (-1)^j \alpha_i^j a_{k-j} \\
&= (-1)^0 \alpha_i^0 a_{k+1} + \sum_{j=0}^{k} (-1)^{j+1} \alpha_i^{j+1} a_{k-j} \\
&= \sum_{j=0}^{k+1} (-1)^j \alpha_i^j a_{k+1-j}. \qquad \square
\end{aligned}$$

The proposition above implies that $A_{ij} = \sum_{k=0}^{i} (-1)^k \alpha_j^k a_{i-k}$. Let

$$A'_{ij} = \begin{cases} 1 & \text{if } i = 1 \\ a_{i-1} - \alpha_j A'_{i-1,j} & \text{otherwise.} \end{cases} \tag{4.2.1}$$

Note that A' is just A with an adjoint row of ones as the first row.

Proposition 4.2.8. *Let $f = \prod_{i=1}^{n}(x - \alpha_i)$ be a separable polynomial and $A' \in \mathrm{Mat}(n, \mathbb{R})$ be defined as above. Then the inverse B of A' is defined as $B_{ij} = \dfrac{\alpha_i^{n-j}}{f'(\alpha_i)}$.*

Proof. Let $B'_{ik} = f'(\alpha_i)B_{ik}$. By direct computation we have

$$\begin{aligned}
(BA)_{ij} &= \sum_{k=1}^{n} B_{ik} A'_{kj} \\
&= \frac{1}{f'(\alpha_i)} \sum_{k=1}^{n} B'_{ik} A'_{kj} \\
&= \frac{1}{f'(\alpha_i)} \sum_{k=1}^{n} \alpha_i^{n-k} \sum_{\substack{1\le m_1<\ldots<m_{k-1}\le n \\ m_l\ne j}} (-1)^{k-1} \alpha_{m_1}\ldots\alpha_{m_{k-1}} \\
&= \frac{1}{f'(\alpha_i)} \prod_{k\ne j} (\alpha_i - \alpha_k).
\end{aligned}$$

Therefore if $i = j$ then $(BA')_{ij} = 1$, else 0. Therefore $(BA')_{ij} = \delta_{ij}$. □

Let $\mathcal{K} \subset \mathbb{R}^{n-1}$ be a simplex. Let us denote

$$\Lambda(\mathcal{K}) := \{\boldsymbol{\lambda} \in \mathbb{R}_+^n | A(\mathcal{K})\boldsymbol{\lambda} \in \mathbb{Z}^{n-1}, \ \sum_{i=1}^{n} \lambda_i = 1\}.$$

Corollary 4.2.9. *Let $\mathcal{K} \subset \mathbb{R}^{n-1}$ be a simplex. Then $C \cap \mathbb{Z}^{n-1} \neq \emptyset$ if and only if $\Lambda(\mathcal{K}) \neq \emptyset$.* □

Let $C \subset \mathbb{R}^d$ be a convex set. We denote by $G(C) := |\{\mathbf{r} \in \mathbb{Z}^d \mid \mathbf{r} \in C\}|$.

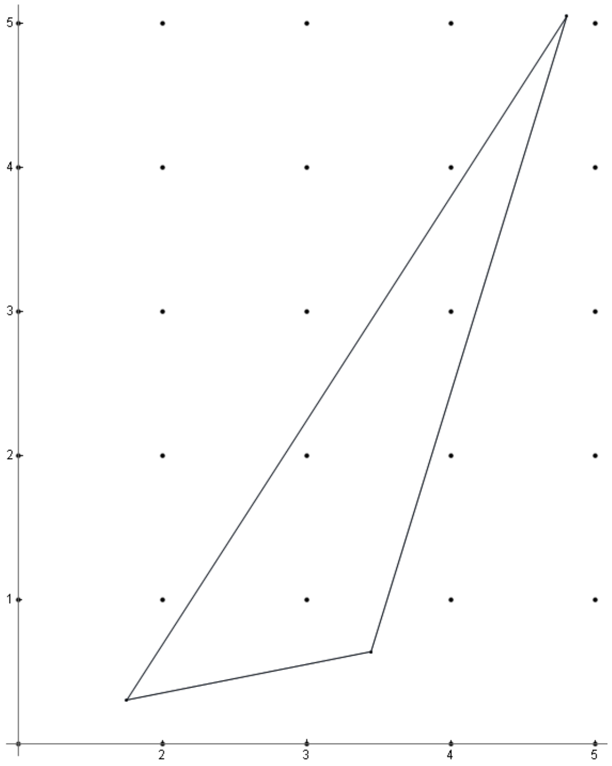
Example 4.2.10. (*i*) Let $f = x^2 - d$, where $d \in \mathbb{N}$, then

$$\begin{aligned}\mathcal{K}(f) &= \{\lambda\sqrt{d} - (1-\lambda)\sqrt{d} \mid \lambda \in [0,1]\} \\ &= \{(2\lambda - 1)\sqrt{d} \mid \lambda \in [0,1]\} \\ &= \{\lambda'\sqrt{d} \mid \lambda' \in [-1,1]\}.\end{aligned}$$

Therefore all the integer points in $\mathcal{K}(f)$ correspond to the integers in the interval $[-\sqrt{d}, \sqrt{d}]$. In particular $G(\mathcal{K}(f)) = 2\lfloor\sqrt{d}\rfloor + 1$. For each $m \in \mathcal{K} \cap \mathbb{Z}$ we have the corresponding interlacing polynomial $x + m$. Lastly,

$$\Lambda(\mathcal{K}(f)) = \{(1/2 - md^{-\frac{1}{2}}, 1/2 + md^{-\frac{1}{2}})^t \mid m \in [-\sqrt{d}, \sqrt{d}] \cap \mathbb{Z}\}.$$

(*ii*) Let $f = x^3 + 5x^2 + 6x + 1$. Then the boundary of $\mathcal{K}(f)$ corresponds to a triangle in $\mathbb{R}^2$:



Thus every lattice point inside the simplex $\mathcal{K}(f)$ corresponds to an interlacing polynomial of f. In particular, $\mathcal{K}(f) \cap \mathbb{Z}^2 = \{(3,1)^t, (3,2)^t, (4,3)^t\}$, and thus f is interlaced by x^2+3x+1, x^2+3x+2 and x^2+4x+3.

Corollary 4.2.11. *Let $f \in \mathbb{Z}[x]$ be a monic separable polynomial such that all its roots are real. Let $\mathcal{K} \subset \mathbb{R}^d$ be the affiliated convex set. Then $G(\mathcal{K})$ is finite.* □

Definition 4.2.12. *Let $f = a_0 \prod_{i=1}^n (x-\alpha_i), g = b_0 \prod_{i=1}^m (x-\beta_i) \in \mathbb{R}[x]$, $a_0, b_0 \in \mathbb{R}$. Then we define the* ***resultant*** *of f and g to be*

$$\mathrm{Res}(f,g) := a_0^m b_0^n \prod_{i=1}^{n} \prod_{j=1}^{m} (\alpha_i - \beta_j).$$

We observe the following two identities, $\mathrm{Res}(f,g) = b_0^n \prod_{i=1}^m f(\beta_i)$ and $\mathrm{Res}(g,f) = (-1)^{mn}\mathrm{Res}(f,g)$.

Let us note that for any $\boldsymbol{\lambda} \in \mathbb{R}^n_+$ such that $A'\boldsymbol{\lambda} = \mathbf{b} \in \mathbb{Z}^n$ we have $\mathbf{b} = (b_1, \dots, b_n)^t$ and $b_1 = \sum_{i=1}^n \lambda_i$. We can represent $\mathbf{b} = (b_1, \dots, b_n)^t \in \mathbb{R}^n$ in a polynomial form as $g = \sum_{i=1}^n b_i x^{n-i}$. If $\sum_{i=1}^n \lambda_i = 1$ then g is a monic polynomial and thus f is interlaced. If $\sum_{i=1}^n \lambda_i \neq 1$ then we can normalise $\boldsymbol{\lambda}$, denoting $\boldsymbol{\lambda'} = \dfrac{\boldsymbol{\lambda}}{\sum_{i=1}^n \lambda_i}$. In this case f is interlaced once more, just not necessarily over $\mathbb{Z}$.

Proposition 4.2.13. *Let $f \in \mathbb{Z}[x]$ be a monic polynomial such that all its roots are real. Let $\boldsymbol{\lambda} = (\lambda_1, \dots, \lambda_n)^t \in \Lambda(\mathcal{K})$. Then $|\prod_{i=1}^n \lambda_i| = \left|\dfrac{\operatorname{Res}(f,g)}{\Delta_f}\right|$, where g is some polynomial that interlaces f.*

Proof. Let A' be a matrix as defined in (4.2.1) corresponding to f, and let $\boldsymbol{\lambda} \in \Lambda(\mathcal{K})$. Then $A'\boldsymbol{\lambda} = \mathbf{b} \in \mathbb{Z}^n$. Let B be the inverse of matrix A'. We have $\boldsymbol{\lambda} = B\mathbf{b}$ and

$$\begin{aligned}\lambda_i &= \sum_{j=1}^n B_{ij} b_j \\ &= \frac{1}{f'(\alpha_i)} \sum_{j=1}^n \alpha_i^{n-j} b_j \\ &= \frac{g(\alpha_i)}{f'(\alpha_i)}.\end{aligned}$$

Therefore,

$$\begin{aligned}\prod_{i=1}^n \lambda_i &= \prod_{i=1}^n \frac{g(\alpha_i)}{f'(\alpha_i)} \\ \left|\prod_{i=1}^n \lambda_i\right| &= \left|\frac{\operatorname{Res}(g,f)}{\Delta_f}\right|.\end{aligned}$$

as was required to show. □

Lemma 4.2.14. *Let $\mathcal{K} \subset \mathbb{R}^{n-1}$ be a simplex affiliated with the polynomial $\prod_{i=1}^n (x - \alpha_i)$. Let $A = A(\mathcal{K}) \in \operatorname{Mat}(n-1, n, \mathbb{R})$, $\boldsymbol{\lambda} = (\lambda_1, \dots, \lambda_n)^t \in \Lambda(C)$ and $\boldsymbol{b} = (b_1, \dots, b_{n-1})^t \in \mathbb{Z}^{n-1}$ such that $A\boldsymbol{\lambda} = \boldsymbol{b}$. Then each component of $\boldsymbol{b}$ can be written as*

$$b_k := g(a_1, \dots, a_k, b_1, \dots, b_{k-1}) + (-1)^k \sum_{i=1}^n \lambda_i \alpha_i^k,$$

where $g(x_1, \dots, x_{2k-1}) \in \mathbb{Z}[x_1, \dots, x_{2k-1}]$.

Proof. We prove by induction on k. For $k = 1$ we have

$$\begin{aligned} b_1 &= \sum_{j=1}^{n} A_{1j}\lambda_j \\ &= \sum_{j=1}^{n} (a_1 - \alpha_j)\lambda_j \\ &= a_1 - \sum_{j=1}^{n} \lambda_j \alpha_j. \end{aligned}$$

This implies that $\sum_{j=1}^{n} \lambda_j \alpha_j = a_1 - b_1$, i.e. $\sum_{j=1}^{n} \lambda_j \alpha_j$ is a polynomial in a_1 and b_1. More generally, if the lemma holds for k, then $\sum_{j=0}^{n} \lambda_j \alpha_j^k$ is a polynomial in $a_1, \dots, a_k, b_1, \dots, b_k \in \mathbb{Z}$.

Assume that the lemma does hold for k, then for $k+1$ we have

$$\begin{aligned} b_{k+1} &= \sum_{j=1}^{n} A_{k+1j}\lambda_j \\ &= \sum_{j=1}^{n} \left(\sum_{l=0}^{k+1} (-1)^l \alpha_j^l a_{k+1-l} \right) \lambda_j \\ &= \sum_{j=1}^{n} \left(\sum_{l=0}^{k} (-1)^l \alpha_j^l a_{k+1-l} + (-1)^{k+1} \alpha^{k+1} \right) \lambda_j \\ &= \sum_{j=1}^{n} \left(\sum_{l=0}^{k} (-1)^l \alpha_j^l a_{k+1-l} \right) \lambda_j + \sum_{j=1}^{n} \lambda_j \alpha_j^{k+1} \\ &= \sum_{l=0}^{k} (-1)^l a_{k+1-l} \left(\sum_{j=1}^{n} \lambda_j \alpha_j^l \right) + \sum_{j=1}^{n} \lambda_j \alpha_j^{k+1} \\ &= \sum_{l=0}^{k} (-1)^l a_{k+1-l} g_l(a_1, \dots, a_l, b_1, \dots, b_l) + \sum_{j=1}^{n} \lambda_j \alpha_j^{k+1}, \end{aligned}$$

where $g_l(x_1, \dots, x_{2l}) \in \mathbb{Z}[x_1, \dots, x_{2l}]$, and where $g_0, a_0, b_0 = 1$. Therefore the lemma follows. □

Definition 4.2.15. *The curve*

$$\psi_d : \mathbb{R} \longrightarrow \mathbb{R}^d$$

$$r \mapsto (r, r^2, \ldots, r^d)$$

is called a ***moment curve*** *in dimension d.*

Definition 4.2.16. *Let $n, d \in \mathbb{N}$, and let $r_1, \ldots, r_n$ be n distinct real numbers. Then*

$$\mathcal{C} := \mathcal{C}(r_1, \cdots, r_n) = \operatorname{conv}\{\psi_d(r_i) | i = 1, \ldots, n\}$$

is a ***cyclic polytope****, i.e. a convex hull of n distinct points on the moment curve in dimension d.*

Let $f = \prod_{i=1}^n (x - \alpha_i)$ be a separable polynomial such that all its roots are real. Then we write $\mathcal{C}(f)$ for a cyclic polytope of the roots of f in dimension $n-1$, i.e. $\mathcal{C}(f) := \mathcal{C}(\alpha_1, \cdots, \alpha_n) \subset \mathbb{R}^{n-1}$. Observe that $\mathcal{C}(f)$ is a simplex.

Proposition 4.2.17. *Let $f \in \mathbb{Z}[x]$ be a monic separable polynomial and such that all its roots are real. Then $\Lambda(\mathcal{K}) = \Lambda(\mathcal{C})$.*

Proof. We show that for each vector $\boldsymbol{\lambda}$ for which $\mathcal{C}$ has an integer point, $\mathcal{K}$ has an integer point too, and vice versa. Let $A(\mathcal{C}) = (A_{ij})$ be the matrix associated to $\mathcal{C}$, where $A_{ij} = \alpha_j^i$. Let $A\boldsymbol{\lambda} = \mathbf{b}' \in \mathbb{Z}^{n-1}$. Lemma 4.2.14 implies that $b'_i = \sum_{j=1}^n \lambda_j \alpha_j^i \in \mathbb{Z}^{n-1}$ if and only if $b_i = g(a_1, \ldots, a_i, b_1, \ldots, b_{i-1}) + (-1)^i \sum_{j=1}^n \lambda_j \alpha_j^i \in \mathbb{Z}^{n-1}$ for $1 \leq i \leq n$. □

From the proposition it follows that for polynomial f it would not be incorrect to forgo the convex set and write just $\Lambda(f)$ for $\Lambda(\mathcal{C}(f))$ or $\Lambda(\mathcal{K}(f))$.

Definition 4.2.18. *Let $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$. The* ***Vandermonde*** *matrix $V := V(\alpha_1, \ldots, \alpha_n)$ of $\alpha_1, \ldots, \alpha_n$ is defined as follows $V_{ij} = \alpha_i^{j-1}$.*

Proposition 4.2.19. [p. 11, 85] *Let $\alpha_1, \ldots \alpha_n \in \mathbb{C}$. Then*

$$\det(V(\alpha_1, \ldots, \alpha_n)) = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j).$$ □

Proposition 4.2.20. *Let $\alpha_1, \dots, \alpha_n \in \mathbb{R}$ be the roots of a monic separable polynomial. If $\sum_{i=1}^{n} y_i \alpha_i^j = 0$ for $0 \leq j \leq n-1$, where $y_i \in \mathbb{R}$, then $y_i = 0$ for $1 \leq i \leq n$.*

Proof. Let V be the Vandermonde matrix of $\alpha_1, \dots, \alpha_n \in \mathbb{R}$. Then the statement of the proposition can be rewritten as $\mathbf{y}^t V = \mathbf{0}^t$, where $\mathbf{y} = (y_1, \dots, y_n)^t \in \mathbb{R}^n$. In particular, as the polynomial with roots α_i is assumed to be separable implies that $\det(V) \neq 0$, following from Proposition 4.2.19. Thus the result follows. □

Recall that $G(C)$ denotes the number of lattice points in a convex set C.

Corollary 4.2.21. *Let $f \in \mathbb{Z}[x]$ be a separable polynomial of degree n such that all its roots are real. Then $|\Lambda(\mathcal{C})| = G(\mathcal{C})$.*

Proof. Assume there exists $\boldsymbol{\lambda}, \boldsymbol{\mu} \in \Lambda(\mathcal{C})$ such that $A(\mathcal{C})\boldsymbol{\lambda} = A(\mathcal{C})\boldsymbol{\mu}$. This implies that

$$\sum_{i=1}^{n} \lambda_i \alpha^j = \sum_{i=1}^{n} \mu_i \alpha_i^j$$

$$\sum_{i=1}^{n} (\lambda_i - \mu_i) \alpha_i^j = 0,$$

and by previous proposition we have that all $\lambda_i = \mu_i$. □

Corollary 4.2.22. *Let $f \in \mathbb{Z}[x]$ be a monic polynomial such that all its roots are real. Then $\mathcal{C} \cap \mathbb{Z}^{n-1} \neq \emptyset$ if and only if $\mathcal{K} \cap \mathbb{Z}^{n-1} \neq \emptyset$. Moreover, if f is separable then $G(\mathcal{C}) = G(\mathcal{K})$.* □

Definition 4.2.23. *Let $\alpha \in \mathbb{R}$ be a totally real algebraic integer, and let $f \in \mathbb{Z}[x]$ be its minimal polynomial. We say that α is* ***interlaced*** *if and only if f is interlaced.*

Proposition 4.2.24. *Let $f \in \mathbb{Z}[x]$ be a monic irreducible polynomial such that all its roots are real. Let $\alpha \in \mathbb{R}$ such that $f(\alpha) = 0$. If α is interlaced then so is every $\beta \in \mathbb{Z}[\alpha]$, such that* $\deg(\beta) = \deg(\alpha)$.

Proof. Let $f = \prod_{i=1}^{n}(x - \alpha_i)$, $\alpha_i \in \mathbb{R}$ and $\mathcal{O} = \mathbb{Z}[\alpha]$, where $f(\alpha) = 0$. If f is interlaced then according to the corollary above there exists $\boldsymbol{\lambda} \in \Lambda(f)$ such that $\sum_{i=1}^{n} \lambda_i = 1$ and $\sum_{i=1}^{n} \lambda_i \alpha_i^j \in \mathbb{Z}$ for $1 \leq j \leq n-1$. To prove this proposition it suffices to show that for each $g \in \mathbb{Z}[x]$, $\sum_{i=1}^{n} \lambda_i g(\alpha_i^j) \in \mathbb{Z}$ for $1 \leq j \leq n-1$. Let $g = \sum_{l=0}^{m} a_l x^l$, then

$$\begin{aligned}\sum_{i=1}^{n} \lambda_i g(\alpha_i^j) &= \sum_{i=1}^{n} \lambda_i \sum_{l=0}^{m} a_l (\alpha_i^j)^l \\ &= \sum_{l=0}^{m} a_l \sum_{i=1}^{n} \lambda_i \alpha_i^{jl} \in \mathbb{Z}.\end{aligned}$$

This follows from the fact that $a_l \in \mathbb{Z}$ and when $jl \leq n-1$ then it is clear, while each α_j^{jl} for $jl \geq n-1$ can be transformed into $\sum_{i=0}^{n-1} b_i \alpha_j^i$, $b_i \in \mathbb{Z}$, using the following identity $\alpha_j^n = \alpha_j^n - f(\alpha_j)$. □

Remark. If the roots of irreducible polynomial f are invertible, i.e. $f(0) = \pm 1$, then the corresponding polynomial $x^n f\left(\frac{1}{x}\right)$ will have the same number of interlacing polynomials. This follows from the fact that if $\alpha \in \mathbb{R}$ such that $f(\alpha) = 0$, then $\mathbb{Z}[\alpha] = \mathbb{Z}[\alpha^{-1}]$, as $f = \sum_{i=1}^{n} a_i x^i + (-1)^k$ and

$$\begin{aligned}f(\alpha) = \sum_{i=1}^{n} a_i \alpha^i + (-1)^k &= 0 \\ \sum_{i=1}^{n} a_i \alpha^i &= (-1)^{k+1} \\ \alpha \sum_{i=1}^{n} a_i \alpha^{i-1} &= (-1)^{k+1},\end{aligned}$$

therefore $\alpha^{-1} = (-1)^{k+1} \sum_{i=1}^{n} a_i \alpha^{i-1} \in \mathbb{Z}[\alpha]$ and thus $\mathbb{Z}[\alpha^{-1}] \subset \mathbb{Z}[\alpha]$. The reverse inclusion is analogous, thus $\mathbb{Z}[\alpha] = \mathbb{Z}[\alpha^{-1}]$. Therefore $G(\mathcal{C}(f)) = G\left(\mathcal{C}\left(x^n f(1/x)\right)\right)$.

Lemma 4.2.25. *Let $\alpha_1, \ldots, \alpha_n \in \mathbb{R}$ and $W = V(\alpha_1, \ldots, \alpha_n)^t$. Then $W^{-1} := (W'_{ij})$ where $W'_{ij} := \dfrac{\sum_{k=0}^{j}(-1)^{k+j}\alpha_i^k a_{j-k}}{f'(\alpha_i)}$, and $f = \prod_{k=1}^{n}(x - \alpha_k) = \sum_{k=0}^{n} a_k x^{n-k}$.*

Proof. We have $W^{-1}W = I_n$, it implies that

$$\begin{aligned}(W^{-1}W)_{ij} &= \sum_{k=0}^{n} W'_{ik}W_{kj}\\ &= \sum_{k=1}^{n} W'_{ik}\alpha_j^{k-1}\\ &= \delta_{ij}.\end{aligned}$$

Let $g_i = \dfrac{\prod_{k\neq i}(x-\alpha_k)}{f'(\alpha_i)} = \sum_{k=0}^{n-1} b_k^{(i)} x^{n-1-k}$. Then $g_i(\alpha_j) = \delta_{ij}$. Thus we take

$$\begin{aligned}W'_{ij} &= (-1)^j b_j^{(i)}\\ &= \frac{(-1)^j}{f'(\alpha_i)} \sum_{\substack{1\leq m_1<\ldots<m_j\leq n\\ m_k\neq i}} \alpha_{m_1}\ldots\alpha_{m_j}.\end{aligned}$$

Now apply Proposition 4.2.7. □

Definition 4.2.26. *Let $\boldsymbol{K}$ be a number field with the ring of integers $\mathcal{O}_{\boldsymbol{K}}$. The fractional ideal*

$$\mathcal{D}_{\boldsymbol{K}}^{-1} = \{x \in \boldsymbol{K} \mid \operatorname{tr}_{\boldsymbol{K}/\mathbb{Q}}(x\mathcal{O}_{\boldsymbol{K}}) \subset \mathbb{Z}\}$$

*is called the **codifferent** of $\mathcal{O}_{\boldsymbol{K}}$.*

Proposition 4.2.27. *Let f be an irreducible monic polynomial of degree n such that all its roots are real. Let $\boldsymbol{K} = \mathbb{Q}(\alpha)$ for $\alpha \in \mathbb{R}$ such that $f(\alpha) = 0$. Then $\Lambda(f) \subset \boldsymbol{K}^n$. If $\mathcal{O}_{\boldsymbol{K}} = \mathbb{Z}[\alpha]$ then there exists a bijection between $\Lambda(f)$ and $\{\gamma \in \mathcal{D}_{\boldsymbol{K}}^{-1} \mid \gamma \gg 0,\ \operatorname{tr}_{\boldsymbol{K}/\mathbb{Q}}(\gamma) = 1\}$.*

Proof. If $f \in \mathbb{Z}[x]$ satisfy the condition of the proposition, then there exist some $\boldsymbol{\lambda} \in \Lambda(f)$ such that given the Vandermonde matrix V of the roots of f, we have $V^t\boldsymbol{\lambda} \in \mathbb{Z}^n$. By Lemma 4.2.25 we have that $\lambda_i \in \mathbf{K}$, more precisely each λ_i is in $\dfrac{1}{f'(\alpha_i)}\mathbb{Z}[\alpha_i]$. Let us denote the embeddings $\sigma_i : \mathbf{K} \hookrightarrow \mathbb{R}$, where $i = 1, \ldots, n$ such that $\sigma_i\alpha = \alpha_i$. Consider the map

$$\begin{aligned}\psi : \{\gamma \in \mathcal{D}_{\mathbf{K}}^{-1} \mid \gamma \gg 0,\ \operatorname{tr}_{\mathbf{K}/\mathbb{Q}}(\gamma) = 1\} &\longrightarrow \Lambda(f)\\ \alpha &\mapsto (\alpha_1, \ldots \alpha_n)^t.\end{aligned}$$

Clearly this map is injective. In the case when $\mathcal{O}_{\mathbf{K}} = \mathbb{Z}[\alpha]$ we have that $\mathcal{D}_{\mathbf{K}}^{-1} = \dfrac{1}{f'(\alpha)}\mathbb{Z}[\alpha]$ (see Lemma 2.2.13) and therefore ψ is a bijection. □

We would like to determine the conditions under which a given polynomial is interlaced. For example, a result similar to Minkowski's First Theorem [85]. Moreover, we would like to count those integral points. A problem for us is that the associated to a polynomial convex set is not symmetric and generally it does not contain the origin. For instance, we can construct a cubic polynomial, by choosing three points on the parabola, such that the convex hull of those points is an arbitrarily large triangle in $\mathbb{R}^2$ that does not contain a point of $\mathbb{Z}^2$. However this polynomial may not have integer coefficients, and indeed later we will show that it is impossible for an irreducible cubic integer polynomial to be not interlaced. Irreducibility here is necessary.

There are different strategies to deal with asymmetric convex sets. First, we can consider the volume–surface area ratio of a simplex, as was studies in [9, 18, 51, 95]. Let $V(\mathcal{C})$ denote the volume of the simplex $\mathcal{C}$ related to a polynomial f of degree $n+1$. It is not hard to notice that (see [104])

$$V(\mathcal{C}) = \frac{1}{n!}\sqrt{|\Delta_f|}.$$

The expression for the surface area of $\mathcal{C}$, denoted $S(\mathcal{C})$, is more involved. Unlike the volume, the surface area does change as we shift the roots of f by a real number. For example, for $f = \prod_{i=1}^{3}(x-\alpha_i)$ we have $S(\mathcal{C}) = \sqrt{|\Delta_f|}\sum_{i=1}^{3}\dfrac{\sqrt{1+(\alpha_1+\alpha_2+\alpha_3-\alpha_i)^2}}{|f'(\alpha_i)|}$ (the perimeter of a triangle). Generally,

$$S(\mathcal{C}) = \frac{1}{(n-1)!}\sqrt{|\Delta_f|}\sum_{k=1}^{n+1}\frac{B_k}{|f'(\alpha_k)|},$$

where $B_k = \sqrt{\sum_{i=0}^{n-1} b_2^{(k)2}}$ and $f_i = f/(x-\alpha_i) = b_0^{(i)}x^n + b_1^{(i)}x^{n-1} + \ldots + b_n^{(i)}$. From [Thm. 1, 51] we know that if $\dfrac{V(\mathcal{C})}{S(\mathcal{C})} \geq \dfrac{r}{2}$, then $G(\mathcal{C}) \geq r$. However, using the formulas above, we get $\dfrac{V(\mathcal{C})}{S(\mathcal{C})} = \dfrac{1}{n}\dfrac{1}{\sum_{k=1}^{n+1}\dfrac{B_k}{|f'(\alpha_k)|}}$. As $B_k \geq 1$, if $|f'(\alpha_k)|$ is small then the ratio will be small too. Unlike B_k, $|f'(\alpha_k)|$ is invariant under the transformation of the roots of f by a constant.

Alternatively we can apply Khinchin's Flatness Theorem [8, 54, 60].

Definition 4.2.28. *Let (L, β) be a lattice in $\mathbb{R}^n$, and let $C \subset \mathbb{R}^n$ be a convex set. Then the **width** of C is*

$$w(C, L) := \min\{\max_{w \in C} \beta(v, w) - \min_{w \in C} \beta(v, w) \mid v \in L \setminus \{0\}\}.$$

The flatness theorem states that a convex set that does not contain a lattice point has a bounded width, which depends only on the dimension of the set. Currently the best bound known is $w(C, L) \leq cn(1 + \log(n))$ [Cor. 2.5, 8], where c is a universal constant and $C \subset \mathbb{R}^n$ is a simplex.

Let us denote by $\operatorname{span}(\alpha) := \max_{i,j} |\alpha_i - \alpha_j|$ the **span** of α, where $\alpha \in \mathbb{R}$ is a totally real algebraic integer and $\alpha = \alpha_1, \ldots, \alpha_n$ are all its conjugates. Note that $\operatorname{span}(m) = 0$ if and only if $m \in \mathbb{Q}$. And $\operatorname{span}(\alpha) = \operatorname{span}(\alpha + k)$ for all $k \in \mathbb{Z}$.

Proposition 4.2.29. *Let $f \in \mathbb{Z}[x]$ be a monic irreducible polynomial such that totally real algebraic integer α is a root of f. Then*

$$w(\mathcal{C}, \mathbb{Z}^n) = \min\{\operatorname{span}(\gamma) \mid \gamma \in \mathbb{Z}[\alpha] \setminus \mathbb{Z}\}.$$

Proof. Let $(\mathbb{Z}^n, \beta)$ be our lattice, where for $\mathbf{v}$,$\mathbf{w} \in \mathbb{R}^n$ we have $\beta(\mathbf{v}, \mathbf{w}) = \sum_{i=1}^n v_i w_i$. Let A be the associated matrix of $\mathcal{C}$. Thus every element $\boldsymbol{\gamma} \in \mathcal{C}$ may be written as $\boldsymbol{\gamma} = A\boldsymbol{\lambda}$ where $\boldsymbol{\lambda} \in \Lambda := \{\boldsymbol{\theta} \in \mathbb{R}^n_+ \mid \sum_{i=1}^n \theta_i = 1\}$. Let $\mathbf{v} \in \mathbb{Z}^n$ then

$$\max_{\mathbf{w} \in \mathcal{C}} \beta(\mathbf{v}, \mathbf{w}) = \max_{\boldsymbol{\lambda} \in \Lambda} \mathbf{v}^t A \boldsymbol{\lambda}.$$

Therefore $\mathbf{v}^t A = (\sum_{i=1}^{n-1} v_i \alpha_1^i, \ldots, \sum_{i=1}^{n-1} v_i \alpha_n^i)$ and so

$$\max_{\mathbf{w} \in \mathcal{C}} \beta(\mathbf{v}, \mathbf{w}) = \max_j \sum_{i=1}^{n-1} v_i \alpha_j^i.$$

Similarly we have that

$$\min_{\mathbf{w}\in\mathcal{C}} \beta(\mathbf{v},\mathbf{w}) = \min_{j} \sum_{i=1}^{n-1} v_i \alpha_j^i.$$

Let $g \in \mathbb{Z}[x]$ such that $g = \sum_{i=1}^{n-1} v_i x^i$, and let $\gamma = g(\alpha) \in \mathbb{Z}[\alpha]$, thus the proposition follows. □

Let $f \in \mathbb{Z}[x]$ be an irreducible polynomial such that a totally real algebraic integer α is a root of f. Then $w(\mathcal{C}, \mathbb{Z}^n) \leq \operatorname{span}(\alpha)$. This bound is strict, i.e. there exists $\mathcal{C}$ such that $w(\mathcal{C}, \mathbb{Z}^n) = \operatorname{span}(\alpha)$, although that is not always the case. For example let α be a roots of $f = x^3 - 6x^2 + 5x - 1$. Then the $\operatorname{span}(\alpha^2 - 5\alpha + 6) < \operatorname{span}(\alpha)$.

Unfortunately, for a totally real algebraic integer $\beta \in \mathbb{R}$ there can exist infinitely many (up to equivalence) totally real algebraic integers $\alpha \in \mathbb{R}$ of bounded degree, such that $\beta \in \mathbb{Z}[\alpha]$. For example if we consider the family of polynomials

$$\{x^4 - 2ax^2 + a^2 - 2 \in \mathbb{Z}[x] \mid a \geq 2\}.$$

The roots of these polynomials are $\pm\sqrt{a \pm \sqrt{2}}$. Thus for each of the corresponding simplices, the width is bounded above by $2\sqrt{2}$.

Neither of the strategies above give us an effective way of bounding the number of lattice points in a given simplex. Thus we cannot show as yet that for a given degree there is a finite number of irreducible monic polynomials with a bound on the number of interlacing polynomials.

4.2.1 Lehmer's conjecture

The following was proved by Dobrowolski for minimal polynomials of integer symmetric matrices.

Theorem 4.2.30. [Lemma 1, 31] *Let $f \in \mathbb{Z}[x]$ be a monic and irreducible polynomial of degree n such that all its roots are real. If f is interlaced then $|\Delta_f| \geq n^n$.*

Proof. Let $f = \prod_{i=1}^{n}(x - \alpha_i) \in \mathbb{Z}[x]$ be an irreducible interlaced polynomial. Then there exists at least one $g \in \mathbb{Z}[x]$ such that g is monic and it interlaces f. In particular, there exist $\boldsymbol{\lambda} \in \Lambda(f)$ such that $\sum_{i=1}^{n} \lambda_i = 1$ and $g = \sum_{i=1}^{n} \lambda_i f_i$, where f_i are defined as in Proposition 4.2.6. First we note that $f_i(\alpha_i) = f'(\alpha_i)$ and thus $g(\alpha_i) = \lambda_i f'(\alpha_i)$. Then

$$\begin{aligned} \left|\prod_{i=1}^{n} g(\alpha_i)\right| &= \left|\prod_{i=1}^{n} \lambda_i f'(\alpha_i)\right| \\ &= \prod_{i=1}^{n} \lambda_i \left|\prod_{i=1}^{n} f'(\alpha_i)\right| \\ &\leq \left(\frac{1}{n}\sum_{i=1}^{n} \lambda_i\right)^n |\Delta_f| \\ &\leq \frac{1}{n^n} |\Delta_f| \end{aligned}$$

As $|\prod_{i=1}^{n} g(\alpha_i)| = |\mathrm{Res}(f, g)|$, we conclude that $|\Delta_f| \geq n^n |\mathrm{Res}(f, g)|$ and given that $\mathrm{Res}(f, g) \in \mathbb{Z} \setminus \{0\}$ we have $|\Delta_f| \geq n^n$. □

Remark. In the theorem above the assumption that f is irreducible can be replaced with a weaker condition that f is separable and interlaced by a coprime polynomial.

The restriction that f is interlaced over $\mathbb{Z}$ can be replaced by a condition that f is interlaced by $g \in \mathbb{R}[x]$ such that $|\mathrm{Res}(f, g)| \geq 1$. If we consider the interlacing polynomial $g = \dfrac{1}{n} f'$, we will see that $\Delta_f = n^n |\mathrm{Res}(f, g)|$. Thus the penultimate inequality in the theorem above is sharp. The condition that $f \in \mathbb{Z}[x]$ has only real roots can be replaced by an existence of $g \in \mathbb{C}[x]$ and $\boldsymbol{\lambda} \in \mathbb{R}_{+}^{n}$ such that $\sum_{i=1}^{n} \lambda_i = 1$ and $g = \sum_{i=1}^{n} \lambda_i f_i$.

Recall Corollary 3.2.12 in the previous chapter. If such polynomial f of degree n exists, then $|\Delta_f| \geq 2^{n-1} n^n$.

There is an alternative proof for Theorem 4.2.30. Let $\gamma \in \mathbf{K}_{+}$, and let $\gamma' = \dfrac{\gamma}{\mathrm{tr}(\gamma)}$, thus $\mathrm{tr}(\gamma') = 1$. In the light of Proposition 4.2.13 we know that $|\mathrm{N}(\gamma')| = \left|\dfrac{\mathrm{Res}(f, g)}{\Delta_f}\right|$, where $g \in \mathbb{Q}[x]$ is the corresponding interlacing polynomial over $\mathbb{Q}[x]$, and $\mathrm{N}(\cdot)$ is the field norm. By the arithmetic mean – geometric mean inequality we know that $\dfrac{1}{n^n} \geq |\mathrm{N}(\gamma')|$, thus we have $|\Delta_f| \geq n^n \left|\mathrm{Res}(f,g)\right|$.

Theorem 4.2.31. [30, Lemma 2] *Let $f = \prod_{i=1}^n (x-\alpha_i) \in \mathbb{Z}[x]$ be a monic separable polynomial such that it does not have a cyclotomic factor. Let p be a prime number, denote $f_{(p)} := \prod_{i=1}^n (x-\alpha_i^p)$. Then $p^n \mid |\mathrm{Res}(ff_{(p)})| > 0$.* □

Recall the Mahler measure of a polynomial (see Definition 1.1.2).

Proposition 4.2.32. [31] *Let $f \in \mathbb{Z}[x]$ be a monic irreducible and interlaced polynomial of degree n. Then $\mathrm{M}\left(x^n f\left(x+\dfrac{1}{x}\right)\right) > 1.0449642$.*

Proof. Let $f = \prod_{i=1}^n (x-\alpha_i) \in \mathbb{Z}[x]$ such that f is interlaced. Let

$$\begin{aligned} g &= x^n f\left(x+\frac{1}{x}\right) \\ &= \prod_{i=1}^{2n} (x-\beta_i). \end{aligned}$$

Let $g_{(p)} = \prod_{i=1}^{2n} (x-\beta^p)$, where p is a prime number. Let us consider the polynomial $gg_{(p)}$, with discriminant $\left|\Delta_{gg_{(p)}}\right| = \left|\Delta_g \Delta_{g_{(p)}} \mathrm{Res}(g, g_{(p)})^2\right|$. Now

$$\begin{aligned} |\Delta_g| &= \left|\Delta_f^2 f_{(2)}(4)\right| \\ &\geq \left|\Delta_f^2\right|, \end{aligned}$$

where $f_{(2)} = \prod_{i=1}^n (x-\alpha_i^2)$,

$$\begin{aligned} \left|\Delta_{g_{(p)}}\right| &= \left|\prod_{1\leq i<j\leq 2n} (\beta_i^p - \beta_j^p)^2\right| \\ &= \left|\prod_{1\leq i<j\leq 2n} (\beta_i - \beta_j)^2 \left(\sum_{k=0}^{p} \beta_i^{p-k}\beta_j^k\right)^2\right| \\ &\geq |\Delta_g|. \end{aligned}$$

The last inequality follows from the fact that $\prod_{1\leq i<j\leq 2n} \left(\sum_{k=0}^p \beta_i^{p-k}\beta_j^k\right)^2 \in \mathbb{Z}\setminus\{0\}$. Applying Theorem 4.2.31 we have that $p^{2n} \mid \mathrm{Res}(g, g_{(p)})$. Finally, as

$|\Delta_f| \geq n^n$ we get

$$\begin{aligned}\left|\Delta_{gg_{(p)}}\right| &= \left|\Delta_g \Delta_{g_{(p)}} \mathrm{Res}(g, g_{(p)})^2\right| \\ &\geq \left|\Delta_g^2 p^{4n}\right| \\ &\geq \left|\Delta_f^4 p^{4n}\right| \\ &\geq n^{4n} p^{4n}.\end{aligned}$$

Let $V = V(\beta_1, \ldots, \beta_{2n}, \beta_1^p, \ldots, \beta_{2n}^p) \in \mathrm{Mat}(4n, \mathbb{R})$ be the Vandermonde matrix for the roots of $gg_{(p)}$. From Hadamard's inequality we have $|\det(V)| \leq (4n)^{2n} \mathrm{M}(g)^{(p+1)(4n-1)}$. Thus

$$\begin{aligned}(4n)^{2n} \mathrm{M}(g)^{(p+1)(4n-1)} &\geq n^{2n} p^{2n} \\ \mathrm{M}(g) &\geq \left(\frac{p}{4}\right)^{\overline{\frac{1}{2(p+1)}}}.\end{aligned}$$

For $p = 11$ we achieve the required bound. □

Remark. The identity $|\Delta_g| = \left|\Delta_f^2 f_{(2)}(4)\right|$, where $f_{(2)} = \prod_{i=1}^n (x - \alpha_i^2)$, follows from the fact that $\beta_{i,n+1} = \dfrac{\alpha_i \pm \sqrt{\alpha_i^2 - 4}}{2}$. Therefore

$$\begin{aligned}\Delta_g = &\prod_{1 \geq i > j \geq n} \left(\frac{\alpha_i \pm \sqrt{\alpha_j^2 - 4}}{2} - \frac{\alpha_j \pm \sqrt{\alpha_j^2 - 4}}{2}\right)^2 \prod_{i=1}^n \left(\frac{\alpha_i + \sqrt{\alpha_j^2 - 4}}{2} - \frac{\alpha_i - \sqrt{\alpha_j^2 - 4}}{2}\right)^2 \\ = &\prod_{1 \geq i > j \geq n} (\alpha_i - \alpha_j)^4 \prod_{i=1}^n (\alpha_i^2 - 4).\end{aligned}$$

In the proposition above most of the bounds are sharp. For example, we have that $\left|\Delta_{g_{(p)}}\right| = \left|\Delta_g \prod_{1 \leq i < j \leq 2n} \left(\sum_{k=0}^p \beta_i^{p-k} \beta_j^k\right)^2\right|$ and if we let $g = x^{10} + x^9 - x^7 - x^6 - x^5 - x^4 - x^3 + x + 1$, then for $p = 3$ we have $\left|\prod_{1 \leq i < j \leq 20} \left(\sum_{k=0}^3 \beta_i^{3-k} \beta_j^k\right)^2\right| = 1$. Using the same polynomial g, we have $\mathrm{Res}(g, g_{(2)}) = 2^{10}$. Finally for $|\Delta_g| = \left|\Delta_f^2 f_{(2)}(4)\right|$, if we let $f = x^3 - 4x + 1$, then $|f_{(2)}(4)| = 1$, and so $|\Delta_g| = \left|\Delta_f^2\right|$.

For cyclic polytopes associated to monic polynomials we have the following result:

Corollary 4.2.33. *There exists $\epsilon > 0$ such that if $\alpha_1 \in (2, 2+\epsilon)$, $\alpha_2, \dots, \alpha_n \in (-2, 2)$ and $G(\operatorname{int}(\mathcal{C}(\alpha_1, \dots, \alpha_n))) = 0$ then $\prod_{i=1}^{n}(x - \alpha_i) \notin \mathbb{Z}[x]$, where $n \in \mathbb{N}$ is strictly larger than one.* □

In the light of the remark after Theorem 4.2.30 we have the following corollary.

Corollary 4.2.34. *Let $f \in \mathbb{Z}[x]$ be an irreducible monic polynomial such that it is not divisible by any cyclotomic polynomial. If there exists $g \in \mathbb{C}[x]$ and $\lambda_1, \dots, \lambda_n \in \mathbb{R}_+$ such that $\sum_{i=1}^{n} \lambda_i = 1$, $g = \sum_{i=1}^{n} \lambda_i f_i$ and $|\operatorname{Res}(f, g)| \geq 1$, then $\mathrm{M}(f) > 1.08144$.*

Remark. We do not assume that the roots of f are all real, so perhaps $g \notin \mathbb{R}[x]$.

Proof. This proof follows analogously to the proof of the proposition above. Let f be a polynomial satisfying our hypothesis, then $\left|\Delta_{ff_{(p)}}\right| \geq n^{2n}p^{2n}$. Using Hadamard's inequality we have $\mathrm{M}(f) \geq \left(\frac{p}{2}\right)^{\overline{2(p+1)}}$ and for $p = 7$ we achieve the required bound. □

Given the strength of the bound above, one would hope that it is possible to show that if an integer monic polynomial f is not interlaced then $\mathrm{M}\left(x^n f\left(x + \frac{1}{x}\right)\right) = 1$. For example, the family of polynomials with small discriminants, cited by Dobrowolski in [31], had cyclotomic polynomials as associated reciprocal polynomials. Unfortunately it can happen that the polynomial is noninterlaced and its Mahler measure is strictly larger than one. For example, the polynomial

$$f = x^8 - 4x^7 + 14x^5 - 8x^4 - 12x^3 + 7x^2 + 2x - 1$$

is a noninterlacing polynomial and $\mathrm{M}\left(x^8 f\left(x + \frac{1}{x} + k\right)\right) > 1$ for all values of $k \in \mathbb{Z}$.

4.2.2 Ideal lattices

In this section we discuss an algebraic constructions of lattices. For more details and some of the proofs we refer to [6, 7].

Definition 4.2.35. *Let $\boldsymbol{K}$ be a number field and $\mathcal{O}_{\boldsymbol{K}}$ be its ring of integers. Let $\mathfrak{a}$ be a fractional ideal in $\mathcal{O}_{\boldsymbol{K}}$. An **ideal lattice** is a lattice $(\mathfrak{a}, \beta)$ such that*

$$\beta(\lambda x, y) = \beta(x, \overline{\lambda} y)$$

for all $x, y \in \mathfrak{a}$ and $\lambda \in \mathcal{O}_{\boldsymbol{K}}$, where $\overline{\lambda}$ is the complex conjugate of λ.

Proposition 4.2.36. [Prop. 1, 7] *Let $\mathfrak{a}$ be a fractional ideal in $\mathcal{O}_{\boldsymbol{K}}$. Then $(\mathfrak{a}, \beta)$ is an ideal lattice if and only if there exists $\alpha \in \boldsymbol{K}$ such that $\beta(x, y) = \mathrm{tr}(\alpha x \overline{y})$.* □

Note the similarity of the proposition above with Corollary 2.2.22.

Proposition 4.2.37. [Prop. 2, 7] *Let $(\mathfrak{a}, t_\alpha)$ be an ideal lattice, $\alpha \in \boldsymbol{K}$. Then $|\det(t_\alpha)| = \mathrm{N}(\mathfrak{a})^2 \mathrm{N}(\alpha) \Delta_{\boldsymbol{K}}$.* □

Definition 4.2.38. *We say that a lattice (L, β) is **integral** if for all $x, y \in L$ we have $\beta(x, y) \in \mathbb{Z}$.*

Proposition 4.2.39. [Prop. 6, 7] *An ideal lattice $(\mathfrak{a}, \beta)$, where $\beta(x, y) = \mathrm{tr}(\alpha x \overline{y})$, is integral if and only if $\alpha \mathfrak{a} \overline{\mathfrak{a}} \subset \mathcal{D}_{\boldsymbol{K}}^{-1}$.* □

Corollary 4.2.40. *Let $\boldsymbol{K}$ be a totally real number field of degree n. Then $\Delta_{\boldsymbol{K}} \geq \dfrac{n^n}{m^n}$ where $m = \min\{\mathrm{tr}(\gamma) | \gamma \in \mathcal{D}_{+}^{-1}\}$.*

Proof. Let $\gamma \in \mathcal{D}_{+}^{-1}$ such that $\mathrm{tr}(\gamma) = m$. Let us define an integral ideal lattice $(\mathcal{O}_{\mathbf{K}}, t_\gamma)$. From the arithmetic mean–geometric mean inequality it follows that $\mathrm{N}(\gamma) \leq \dfrac{m^n}{n^n}$. By Proposition 4.2.37 and the fact that $|\det(t_\gamma)| \geq 1$, as our lattice is integral, we have

$$|\det(t_\gamma)| = \mathrm{N}(\gamma) \Delta_{\mathbf{K}}$$

$$\begin{aligned} &\leq \frac{m^n}{n^n}\Delta_{\mathbf{K}} \\ 1 &\leq \frac{m^n}{n^n}\Delta_{\mathbf{K}} \\ \frac{n^n}{m^n} &\leq \Delta_{\mathbf{K}}. \end{aligned}$$ □

A similar result to the corollary above was shown by Siegel in [99].

This is a slightly different bound than the one achieved in Theorem 4.2.30. We have an identity $\Delta_f = \Delta_{\mathbf{K}} [\mathcal{O}_{\mathbf{K}} : \mathbb{Z}[\alpha]]^2$ (see [Prop. 4.4.4, 24]), and so when $[\mathcal{O}_{\mathbf{K}} : \mathbb{Z}[\alpha]] = 1$ then the two bounds could be equal.

Any integral ideal lattice in $\mathbf{K}$ will be called an $\mathcal{O}_{\mathbf{K}}$-lattice.

Proposition 4.2.41. [Cor. 2.2, 5] *Let $\boldsymbol{K} = \mathbb{Q}[\zeta_n]$ such that $n \neq p, 2p$ is square free, p is a prime number, and $\phi(n) > 8$. Then the minimum of any $\mathcal{O}_{\boldsymbol{K}}$-lattice is at least 4.* □

Corollary 4.2.42. *Let $\boldsymbol{K} = \mathbb{Q}[\zeta_n]$, where n is squarefree, $n \neq p, 2p$, and $\phi(n) > 8$. Let $\boldsymbol{F}$ be the maximal totally real subfield in $\boldsymbol{K}$, i.e. $\boldsymbol{F} = \mathbb{Q}[\zeta_n + \zeta_n^{-1}]$. Then the minimum of any $\mathcal{O}_{\boldsymbol{F}}$-lattice is at least 2.*

Proof. Let $\mathfrak{a}$ be an ideal in $\mathcal{O}_{\mathbf{F}}$, and let $\alpha \in \mathbf{F}$ such that $(\mathfrak{a}, t_\alpha)$ is an ideal lattice. Let m be the minimum of t_α and $z \in \mathfrak{a}$ be such that $t_\alpha(z^2) = m$. Let us extend this lattice to $\mathcal{O}_{\mathbf{K}}$, let $\mathfrak{a}^e := \{\sum a_i b_i | a_i \in \mathfrak{a},\ b_i \in \mathcal{O}_{\mathbf{K}}\}$, and $t'(x, y) := \mathrm{tr}_{\mathbf{K}/\mathbf{F}} \circ t_\alpha(x, y) = \mathrm{tr}_{\mathbf{K}/\mathbb{Q}} \alpha x \overline{y}$. Clearly $(\mathfrak{a}^e, t')$ is an $\mathcal{O}_{\mathbf{K}}$-lattice. Given that $z \in \mathfrak{a}^e$, we have that the minimum of t' is smaller than $t'(z^2)$. Thus

$$\begin{aligned} t'(z^2) &= \mathrm{tr}_{\mathbf{K}/\mathbf{F}} m \\ &= 2m \\ &\geq 4, \end{aligned}$$

the last inequality follows from the previous proposition, thus $m \geq 2$. □

Therefore the minimal polynomial of $\zeta_{21} + \zeta_{21}^{-1}$,

$$x^6 - x^5 - 6x^4 + 6x^3 + 8x^2 - 8x + 1,$$

is noninterlacing. This implies that it cannot be the minimal polynomial of an integer symmetric matrix. In general, the corollary above provides counterexamples to Estes–Guralnick's conjecture for all polynomials of degree $\phi(n)$, where n satisfies the necessary conditions. However when $n = p$ is a prime number strictly larger than 5, then it is known that the corresponding minimal polynomial of $\zeta_p + \zeta_p^{-1}$ is the characteristic polynomial of an integer symmetric matrix [37]. That the minimal polynomial of $\zeta_{21} + \zeta_{21}^{-1}$ is a counterexample to Estes–Guralnick's conjecture was shown with another method in [76].

It is not known whether every integer lattice can appear as an ideal lattice. Neither it is generally known what can be said about the ring of integers $\mathcal{O}_{\mathbf{K}}$ if a given lattice is an $\mathcal{O}_{\mathbf{K}}$-lattice. A special case of this question was studied in [72]. From our perspective, if $\mathbf{K}$ is a totally real number field and a positive definite $\mathcal{O}_{\mathbf{K}}$-lattice has an orthonormal basis, then the minimal polynomial of every element in $\mathcal{O}_{\mathbf{K}}$ is the characteristic polynomial of an integer symmetric matrix [Prop. 13, 7]. That in turn means that the codifferent is narrowly equivalent to a square of an ideal [Thm. 176, 53], i.e. there exists an ideal $\mathfrak{a} \subseteq \mathcal{O}_{\mathbf{K}}$ and $\gamma \in \mathbf{K}_+$ such that $\mathcal{D}_{\mathbf{K}}^{-1} = \gamma\mathfrak{a}^2$. This has consequences for the study of Hilbert modular forms [52].

Universal forms

Definition 4.2.43. *We say that a positive definite $\mathcal{O}$-lattice (L, β) is **universal** if for every $\alpha \in \mathcal{O}_+$ there exists $v \in L$ such that $\beta(v, v) = \alpha$.*

For a lattice, a condition of being universal is not equivalent to $\mathfrak{n}L = \mathcal{O}$, i.e. a lattice can be proper but not universal. For example $(\mathbb{Z}, I_1)$ is a proper rational integer lattice, as it represents one, but it is not universal as it does not represent nonsquares. On the other hand, the rational integer lattice $(\mathbb{Z}^4, I_4)$ is both universal and proper.

Siegel in [97] showed that if $\mathbf{K}$ is a totally real number field such that every totally positive algebraic integer can be represented as sums of squared integers in $\mathbf{K}$, then $\mathbf{K} = \mathbb{Q}$ or $\mathbb{Q}(\sqrt{5})$, i.e. if $\mathrm{Sq}(\mathcal{O}) = \mathcal{O}_+$ and $\mathcal{O}$ is a ring of integers of a totally real number field, then $\mathcal{O} \subset \mathbb{Q}(\sqrt{5})$. Maass showed that $\mathrm{Sq}_3(\mathcal{O}) = \mathcal{O}_+$, where $\mathcal{O}$ is the ring of integers of $\mathbb{Q}(\sqrt{5})$ [70]. A more detailed explanation of the modern advances in this research can be found in [62].

Recall the notation from Definition 2.2.25, where $\mathcal{M}(L)$ is the set of the minimal vectors of a positive definite lattice L.

Definition 4.2.44. *The* ***kissing number*** *in dimension n is $\tau_n := \max_{(L,\beta)} |\mathcal{M}(L)|$, where L runs over all integer positive definite lattices of rank n.*

Generally, the kissing number represents the maximal number of spheres that can all touch one sphere in given dimension. This relates to a classical problem of sphere packing (which recently experienced some exciting developments [25, 109]). Clearly $\tau_n \geq 2n$ given the existence of a lattice $(\mathbb{Z}^n, I_n)$. The values of τ_n are known only for small dimensions. For example, for $n = 1, 2, 3, 4$ and 5 we have $\tau_n = 2, 6, 12, 24$ and 40, respectively. Be aware that our definition of the kissing number is a restriction to the kissing numbers for lattices.

Example 4.2.45. Let $f = x^5 - 12x^4 + 43x^3 - 58x^2 + 28x - 4$ and let $\mathbf{K} = \mathbb{Q}[\alpha]$, where $f(\alpha) = 0$, and $\mathcal{O}$ be its ring of integers. The polynomial f is irreducible and has only real roots. Let

$$\delta = \frac{121868\alpha^4 - 1177502\alpha^3 + 3245038\alpha^2 - 2803155\alpha + 301764}{43795} \in \mathbf{K}_+.$$

Then the ideal lattice $(\mathcal{O}, t_\delta)$ is a positive definite lattice of rank 5 such that $\mathcal{M}(\mathcal{O}, t_\delta) = 40 = \tau_5$.

Let us denote $\mathcal{D}_+^{-1} = \mathbf{K}_+ \cap \mathcal{D}_{\mathbf{K}}^{-1}$.

Proposition 4.2.46. *Let $\boldsymbol{K}$ be a totally real algebraic number field of degree n. Let us assume that its codifferent is a principal ideal generated by $\delta \in \boldsymbol{K}$ and there exists $\epsilon \in \mathcal{O}_{\boldsymbol{K}}^\times$ such that $\epsilon\delta \gg 0$. Let $m = |\{\alpha \in \mathcal{D}_+^{-1} \mid \mathrm{tr}(\alpha) = \min_{\gamma \in \mathcal{D}_+^{-1}}(\mathcal{O}, t_\gamma)\}|$. If a positive definite $\mathcal{O}$-lattice (L, β) of rank r is universal then $\tau_{rn} \geq m$.*

Proof. Let (L, β) be a universal $\mathcal{O}$ lattice of rank r. Every element $\alpha \in \mathcal{D}_{\mathbf{K}}^{-1}$ can be written as $\alpha = \alpha'\delta$, where $\alpha' \in \mathcal{O}_{\mathbf{K}}$. Let us assume that such $\alpha \gg 0$. Then δ and α' have the same signatures, i.e. $\operatorname{sign}(\sigma\delta) = \operatorname{sign}(\sigma\alpha')$ for all embeddings $\sigma : \mathbf{K} \hookrightarrow \mathbb{R}$. In particular, as there exists $\epsilon \in \mathcal{O}_{\mathbf{K}}^{\times}$ such that $\epsilon\delta \gg 0$, we have that $\epsilon\alpha' \gg 0$ and $\epsilon^{-1}\alpha' \gg 0$. Consider an $\mathbb{Z}$-lattice $(L, t_{\epsilon\delta} \circ \beta)$ of rank rn. By the definition of universal forms, β is positive definite, and $\epsilon\delta \gg 0$, thus $(L, t_{\epsilon\delta} \circ \beta)$ is positive definite too. Given that L is universal, there exists $v \in L$ such that $\beta(v, v) = \epsilon^{-1}\alpha'$. Then

$$\begin{aligned} t_{\epsilon\delta} \circ \beta(v, v) &= t_{\epsilon\delta}(\epsilon^{-1}\alpha') \\ &= \operatorname{tr}(\delta\alpha') \\ &= \operatorname{tr}(\alpha), \end{aligned}$$

and therefore our $\mathbb{Z}$-lattice represents $\operatorname{tr}(\alpha)$ for all $\alpha \in \mathcal{D}_{+}^{-1}$. Clearly $\min(L, t_{\epsilon\delta} \circ \beta) = \min_{\gamma \in \mathcal{D}_{+}^{-1}}(\mathcal{O}, t_{\gamma})$, therefore

$$\begin{aligned} |\mathcal{M}(L, t_{\epsilon\delta} \circ \beta)| &= |\{\alpha \in \mathcal{D}_{+}^{-1} \mid \operatorname{tr}(\alpha) = \min_{\gamma \in \mathcal{D}_{+}^{-1}}(\mathcal{O}, t_{\gamma})\}| \\ &= m, \end{aligned}$$

and the proposition follows. □

Byeong Moon Kim constructed infinitely many universal octonary quadratic forms over real quadratic number fields [61]. As $\tau_{16} \leq 8313$ [p. 23, 26], if $|\{\alpha \in \mathcal{D}_{+}^{-1} \mid \operatorname{tr}(\alpha) = 1\}| > 8313$ and remaining conditions in the proposition above are met, then we conclude that a given quadratic number field cannot have octonary universal form defined over it. Quadratic number fields have a normal integral basis. Therefore we can always find a polynomial such that its root is a generator of the ring of integers. In the light of Proposition 4.2.27 and example (4.2.10), for polynomials with span large enough we will have $|\{\alpha \in \mathcal{D}_{+}^{-1} \mid \operatorname{tr}(\alpha) = 1\}| > 8313$. This accounts for almost all polynomials. Thus the existence of a unit with an appropriate signature in the proposition above is necessary.

Let us define

$$u(\mathcal{O}_{\mathbf{K}}) := \min\{\operatorname{rank}(L) \mid L \text{ is a universal } \mathcal{O}_{\mathbf{K}}\text{-lattice}\},$$

where $\mathcal{O}_{\mathbf{K}}$ is the ring of algebraic integers of a number field $\mathbf{K}$.

Conjecture 4.2.47 (Kitaoka's conjecture)**.** [61] There exist finitely many totally real number fields $\mathbf{K}$ such that $u(\mathcal{O}_{\mathbf{K}}) = 3$.

If for a given degree there exist only finitely many irreducible monic integer polynomial with a bounded number of interlacing polynomials, then Proposition 4.2.46 will give an affirmative answer to a special case of Kitaoka's conjecture.

4.2.3 The Dedekind zeta function

Let $\mathbf{K}$ be an algebraic number field, $n = [\mathbf{K} : \mathbb{Q}]$, and let $\mathcal{O}_{\mathbf{K}}$ be the ring of integers in $\mathbf{K}$. Let $\mathrm{N}_{\mathbf{K}/\mathbb{Q}}$ be an absolute norm (we shall simply write N when it is clear which algebraic number field we imply).

Definition 4.2.48. *The* ***Dedekind zeta function*** *of an algebraic number field* $\boldsymbol{K}$ *is defined by the series*

$$\zeta_{\boldsymbol{K}}(s) = \sum_{\mathfrak{a}\subset\mathcal{O}_{\boldsymbol{K}}} \frac{1}{\mathrm{N}(\mathfrak{a})^s},$$

where $s \in \mathbb{C}$*,* $\mathrm{Re}(s) > 1$*, and* $\mathfrak{a}$ *ranges through all the ideals in* $\mathcal{O}_{\boldsymbol{K}}$*.*

The Dedekind zeta function admits an analytic continuations to $\mathbb{C} \setminus \{1\}$ ([Cor. 5.11, 85]).

Let us define

$$\sigma_r(\mathfrak{a}) = \sum_{\mathfrak{b}|\mathfrak{a}} \mathrm{N}(\mathfrak{b})^r,$$

where $\mathfrak{a}$ is an ideal of $\mathcal{O}_{\mathbf{K}}$. Furthermore, let

$$s_l^{\mathbf{K}}(m) = \sum_{\substack{\gamma\in\mathcal{D}_+^{-1}\\ \mathrm{tr}(\gamma)=l}} \sigma_{m-1}((\gamma)\mathcal{D}_{\mathbf{K}}),$$

where $\mathcal{D}_{\mathbf{K}}$ is the inverse ideal of the codifferent.

Theorem 4.2.49. [99] *Let $\boldsymbol{K}$ be a totally real algebraic number field of degree $n > 1$. Let $h = 2mn$, where $m \in \mathbb{N}$. Then*

$$\zeta_{\boldsymbol{K}}(1-2m) = 2^n \sum_{l=1}^{r} b_l(h) s_l^{\boldsymbol{K}}(2m).$$

The numbers $r \geq 1, b_1(h), \ldots, b_r(h)$ are rational and they only depend on h, where

$$r = \begin{cases} \left\lfloor \dfrac{h}{12} \right\rfloor & \textit{if } h \equiv 2 \pmod{12} \\ \\ \left\lfloor \dfrac{h}{12} \right\rfloor + 1 & \textit{if } h \not\equiv 2 \pmod{12}. \end{cases}$$

□

Corollary 4.2.50. *Let $\boldsymbol{K}$ be a totally real number field. Then $\zeta_{\boldsymbol{K}}(1-2m) \in \mathbb{Q}^{\times}$ for all $m \in \mathbb{N}^{\times}$.* □

Corollary 4.2.51. *There does not exist a noninterlacing irreducible integer polynomial of degrees $1, 2, 3, 4, 5$ or 7.*

Proof. Let $f \in \mathbb{Z}[x]$ be an irreducible polynomial of degree $1, 2, 3, 4, 5$ or 7, such that all its roots are real. Let $\alpha \in \mathbb{R}$ be a root of f and $\mathbf{K} = \mathbb{Q}(\alpha)$. Let $\mathcal{O}_{\mathbf{K}}$ be the ring of integers of $\mathbf{K}$, then $\mathbb{Z}[\alpha] \subset \mathcal{O}_{\mathbf{K}}$ and $\mathbb{Z}[\alpha]^{\vee} = \{x \in \mathbf{K} \mid \mathrm{tr}_{\mathbf{K}/\mathbb{Q}}(x\mathbb{Z}[\alpha]) \subset \mathbb{Z}\}$. If there does not exist $\gamma \in \mathbb{Z}[\alpha]^{\vee}$ such that $\gamma \in \mathbf{K}_+$ and $\mathrm{tr}(\gamma) = 1$ then nor such γ can exist in $\mathcal{D}_{\mathbf{K}}^{-1}$, this follows from Proposition 4.2.27. Therefore if f is noninterlacing then there does not exist $\gamma \in \mathcal{D}_{+}^{-1}$ such that $\mathrm{tr}(\gamma) = 1$. From the theorem above it follows that $\zeta_{\mathbf{K}}(-1) = 2^n \sum_{l=1}^{r} b_l(h) \sum_{\substack{\gamma \in \mathcal{D}_+^{-1} \\ \mathrm{tr}(\gamma)=l}} \sigma_1((\gamma)\mathcal{D}_{\mathbf{K}})$ and for $n \in \{2, 3, 4, 5, 7\}$ we have $r = 1$ and $\zeta_{\mathbf{K}}(-1) = 2^n b_1(h) \sum_{\substack{\gamma \in \mathcal{D}_+^{-1} \\ \mathrm{tr}(\gamma)=1}} \sigma_1((\gamma)\mathcal{D}_{\mathbf{K}})$. By the previous corollary $\zeta_{\mathbf{K}}(-1) \neq 0$, and therefore there exists at least one $\gamma \in \mathcal{D}_{+}^{-1} \subset \mathbb{Z}[x]^{\vee}$ such that $\mathrm{tr}(\alpha) = 1$. □

The similar approaches in studying totally positive elements of codifferent via cyclic polytopes were rediscovered several times [22, 23]. Predominantly, those studies were motivated by possibility to estimate the values of the Dedekind zeta function of a totally real number field evaluated at negative odd integers.

4.3 Integer symmetric matrices

We now bring focus back to the integer symmetric matrices. First of all, let $f \in \mathbb{Z}[x]$ be a monic irreducible polynomial with all n roots being real. Let $g_1, \ldots, g_k \in \mathbb{Z}[x]$ be all the monic polynomials of degree $n-1$ that interlace f. We know that the number of such polynomials is finite. If there exists an integer symmetric matrix A such that $\chi_A = f^m$ then for any principal submatrix $A' \in \mathrm{Sym}(mn-1, \mathbb{Z})$ of A we have $\chi_{A'} = f^{m-1} g_i$ (see Theorem 3.1.1). Then $\mathrm{Tr}(A) = \mathrm{Tr}(A') + A_{ii}$ where A_{ii} is a difference between the trace of f and g_i. Thus diagonal entries of the matrix A are wholly depend on the g_is.

Example 4.3.1. Let us consider the polynomial $f = x^{10} - 18x^9 + 135x^8 - 549x^7 + 1320x^6 - 1920x^5 + 1662x^4 - 813x^3 + 206x^2 - 24x + 1$. It has only real and positive roots. This is the set of all the polynomials that interlace f:

$$\begin{gathered}
x^9 - 16x^8 + 105x^7 - 366x^6 + 734x^5 - 858x^4 + 567x^3 - 198x^2 + 33x - 2, \\
x^9 - 16x^8 + 105x^7 - 366x^6 + 735x^5 - 865x^4 + 582x^3 - 209x^2 + 35x - 2, \\
x^9 - 16x^8 + 105x^7 - 367x^6 + 742x^5 - 882x^4 + 599x^3 - 215x^2 + 35x - 2, \\
x^9 - 16x^8 + 105x^7 - 367x^6 + 743x^5 - 887x^4 + 608x^3 - 222x^2 + 37x - 2.
\end{gathered}$$

Given that every polynomial that interlaces f has trace 16 implies that if there exists a matrix $A \in \mathrm{Sym}(10k, \mathbb{Z})$ such that f is the minimal polynomial of A, then all the diagonal entries of such matrix is 2. But this is impossible as it would imply that $\mathrm{Tr}(A) = 20k$.

With a slightly more elaborate computations we can find the possible values for $\sum_{\substack{j=1 \\ j \neq i}}^{n} A_{ji}^2$ from the knowledge of all the interlacing polynomials.

The following is based on [10] and [29]. Let $f \in \mathbb{Z}[x]$ to be a monic irreducible polynomial of degree n such that all its roots are real. Let $\mathbf{K} = \mathbb{Q}(\alpha)$ such that $f(\alpha) = 0$, and $\mathcal{O}_{\mathbf{K}} = \mathbb{Z}[\alpha]$.

Definition 4.3.2. *We say that the homomorphism*

$$\rho : \mathcal{O}_{\boldsymbol{K}} \longrightarrow \operatorname{Mat}(n, \mathbb{Z})$$

is a ***representation*** *of $\mathcal{O}_{\boldsymbol{K}}$ over $\mathbb{Z}$, if for all $x \in \mathbb{Z}$ we have $\rho(x) = xI_n$. If in addition we have that*

$$\rho : \mathcal{O}_{\boldsymbol{K}} \longrightarrow \operatorname{Sym}(n, \mathbb{Z}),$$

then we say that our representation is ***symmetric****.*

Definition 4.3.3. *We say that two representations*

$$\rho, \psi : \mathcal{O}_{\boldsymbol{K}} \longrightarrow \operatorname{Mat}(n, \mathbb{Z})$$

are ***equivalent*** *if there exists $A \in \operatorname{GL}(n, \mathbb{Z})$ such that $\rho(x) = A\psi(x)A^{-1}$ for all $x \in \mathcal{O}_K$.*

It is a well known result that:

Theorem 4.3.4 (Latimer–MacDuffee–Taussky)**.** [105] *There is a one-to-one correspondence between equivalence classes of representations of $\mathcal{O}_{\boldsymbol{K}}$ over $\mathbb{Z}$ and ideal classes in $\mathcal{O}_{\boldsymbol{K}}$.* □

Example 4.3.5. Let $f \in \mathbb{Z}[x]$ be a monic polynomial of degree n and let $\alpha \in \mathbb{C}$ be a root of f. Then

$$\psi : \mathbb{Z}[\alpha] \longrightarrow \operatorname{Mat}(n, \mathbb{Z})$$
$$\alpha \mapsto C_f,$$

where C_f is the companion matrix of f. For any $\beta \in \mathbb{Z}[\alpha]$ there exists $g \in \mathbb{Z}[x]$ such that $g(\alpha) = \beta$. Therefore $\psi(g(\alpha)) = g(C_f)$ and so ψ is a representation of $\mathbb{Z}[\alpha]$.

Given that ρ is a homomorphism, and the requirement of the definition that $\rho(x) = xI$ for all $x \in \mathbb{Z}$, we conclude that there are no examples of trivial representations.

So far we assumed that the dimension of the representation, i.e. the order of matrices by which we represent the ring, and the degree of the number field are equal. Generally it does not have to be so, the only restriction is that the dimension of the representation is a multiple of the degree of the number field.

Let ρ be an integer representation of $\mathcal{O}$, where $\mathcal{O}$ is an order defined by $\alpha \in \mathbb{C}$, i.e. $\mathcal{O} = \mathbb{Z}[\alpha]$. Let $f \in \mathbb{Z}[x]$ be the minimal polynomial of α. As ρ is a homomorphism then $\rho(f(\alpha)) = f(\rho(\alpha)) = 0$, thus f is the minimal polynomial of $\rho(\alpha)$. Be aware that we implicitly assume that ρ is a homomorphism over $\mathbb{Z}$. Let g be the minimal polynomial of $\gamma \in \mathbb{C}$. If $g \notin \mathbb{Z}[x]$, but instead $g \in \mathbb{Z}[\alpha]$, then $\rho(g(\gamma)) \neq g(\rho(\gamma))$. However if we let $h \in \mathbb{Z}[x]$ be the minimal polynomial of $\rho(\gamma)$, then $g \mid h$ over $\mathbb{Z}[\alpha]$.

Let $\alpha \in \mathbb{R}$ be an algebraic integer. We say that α is **represented** over $\mathcal{O}$ if there exists a representation $\rho : \mathbb{Z}[\alpha] \longrightarrow \mathrm{Mat}(n, \mathcal{O})$. Similarly we shall say that α is **represented symmetrically** if ρ is a symmetric representation.

Proposition 4.3.6 (Bukh's observation)**.** [21] *Let $\alpha \in \mathbb{R}$ be a totally real algebraic integer, $\mathcal{O} = \mathbb{Z}[\alpha]$, and let α be represented symmetrically over $\mathbb{Z}$. Then a totally real algebraic integer $\beta \in \mathbb{R}$ is symmetrically represented over $\mathcal{O}$ if and only if it is represented symmetrically over $\mathbb{Z}$.*

Proof. Let $\alpha \in \mathbb{R}$ be represented symmetrically over $\mathbb{Z}$, and let $A \in \mathrm{Sym}(n, \mathbb{Z})$ such that the minimal polynomial of A is the minimal polynomial of α. We have a bijection

$$\psi : \mathbb{Z}[\alpha] \longrightarrow \mathbb{Z}[A].$$

Let $\beta \in \mathbb{R}$ be a totally real algebraic integer, and let $f \in \mathbb{Z}[x]$ be the minimal polynomial of β. Then β is symmetrically represented over $\mathbb{Z}[\alpha]$ if and only if there exists $B \in \mathrm{Sym}(m, \mathbb{Z}[\alpha])$ such that the minimal polynomials of B is f, i.e. $f(B) = O$. Given that ψ is a symmetric representation over $\mathbb{Z}$, we have that $\psi(B) \mapsto \mathrm{Sym}(nm, \mathbb{Z})$, and from the definition of a representation we have that

$$\begin{aligned} \psi(f(B)) &= f(\psi(B)) \\ \psi(O) &= O, \end{aligned}$$

thus the proposition follows. □

Example 4.3.7. *(i)* Let $\mathcal{O} = \mathbb{Z}[\sqrt{2}]$ and let ψ be a symmetric representation of $\mathcal{O}$ such that

$$\sqrt{2} \mapsto \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

Consider the matrix

$$M = \begin{pmatrix} \sqrt{2} & 1 \\ 1 & -\sqrt{2} \end{pmatrix}.$$

Its characteristic polynomial is $x^2 - 3$, and clearly it is represented over $\mathcal{O}$. Then

$$\begin{aligned} \psi(M) &= \psi \begin{pmatrix} \sqrt{2} & 1 \\ 1 & -\sqrt{2} \end{pmatrix} \\ &= \begin{pmatrix} \psi(\sqrt{2}) & \psi(1) \\ \psi(1) & \psi(-\sqrt{2}) \end{pmatrix} \\ &= \begin{pmatrix} -1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & -1 \\ 0 & 1 & -1 & -1 \end{pmatrix}. \end{aligned}$$

(ii) Let $\alpha \in \mathbb{R}$ be a totally real algebraic integer satisfying equation $x^3 - x^2 - 2x + 1$ and $\mathcal{O}$ be the ring of integers of $\mathbb{Q}(\alpha)$. By Estes–Guralnick's theorem, we know that α is symmetrically represented over the integers. The polynomial $x^6 - x^5 - 6x^4 + 6x^3 + 8x^2 - 8x + 1$ is not the minimal polynomial of an integer symmetric matrix (see example 3.2.3). It is divisible by $x^2 - \alpha x + (\alpha^2 - 3)$ over $\mathcal{O}$. Therefore the analogue to Estes–Guralnick's conjecture over totally real number fields would have counterexamples even for quadratic polynomials.

Generalisations of Estes–Guralnick's conjecture to hermitian matrices over the ring of integers of a number field were considered by Greaves and Taylor [47, 48, 49, 50, 107, 108].

Conjecture 4.3.8. Let $f \in \mathbb{Z}[x]$ be a monic irreducible polynomial of degree n such that all its roots are real. Then f is the minimal polynomial of an integer symmetric matrix only if there exist at least n distinct interlacing polynomials of f.

For characteristic polynomials the above is true. Let $f \in \mathbb{Z}[x]$ satisfy conditions of the conjecture. Let $\mathbf{K} = \mathbb{Q}[\alpha]$, where α is a root of f. Assume for contradiction that f is the characteristic polynomial of an integer symmetric matrix but it is interlaced only by $g_1, \ldots, g_m$, where $m < n$. Then there exists $\gamma \in \mathbf{K}_+$ such that $(\mathcal{O}_\mathbf{K}, t_\gamma) \sim_\mathbb{Z} (\mathbb{Z}^n, I_n)$. Therefore there are $\pm x_i \in \mathcal{O}_\mathbf{K}$ such that $t_\gamma(x_i^2) = 1$ for $i = 1, \ldots, n$. Now $\gamma x_i^2 \gg 0$ and $\mathrm{tr}(\gamma x_i^2) = 1$, thus γx_i^2 corresponds to an integral point in $\mathcal{C}(f)$, i.e. $\gamma x_i^2 = \delta g_k(\alpha)$, where $\delta = \dfrac{1}{f'(\alpha)}$. There are n distinct $|x_i|$s and only $m < n$ distinct g_ks. Therefore there exists g_k such that

$$\gamma x_i^2 = \delta g_k(\alpha) = \gamma x_j^2,$$

$x_i, x_j \in \mathcal{O}$ and $x_i \neq \pm x_j$, a contradiction.

Observe that a polynomial of degree n that is interlaced by n distinct polynomials is not necessarily the minimal polynomial of an integer symmetric matrix. For example $x^6 - 12x^5 + 54x^4 - 112x^3 + 105x^2 - 36x + 1$ is not the minimal polynomial of an integer symmetric matrix [76], but it is interlaced by:

$$x^5 - 10x^4 + 35x^3 - 50x^2 + 25x - 2,$$
$$x^5 - 10x^4 + 36x^3 - 55x^2 + 31x - 3,$$
$$x^5 - 10x^4 + 36x^3 - 56x^2 + 34x - 4,$$
$$x^5 - 10x^4 + 36x^3 - 56x^2 + 35x - 6,$$

$$x^5 - 10x^4 + 36x^3 - 57x^2 + 39x - 9,$$

$$x^5 - 10x^4 + 37x^3 - 62x^2 + 46x - 12.$$

Bibliography

[1] Julián Aguirre and Juan Carlos Peral. The trace problem for totally positive algebraic integers. In *Number theory and polynomials*, volume 352 of *London Math. Soc. Lecture Note Ser.*, pages 1–19. Cambridge Univ. Press, Cambridge, 2008. With an appendix by Jean-Pierre Serre.

[2] M. F. Atiyah and I. G. Macdonald. *Introduction to commutative algebra*. Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969.

[3] Ricardo Baeza. *Quadratic forms over semilocal rings*. Lecture Notes in Mathematics, Vol. 655. Springer-Verlag, Berlin, 1978.

[4] Hyman Bass, Dennis R. Estes, and Robert M. Guralnick. Eigenvalues of symmetric matrices and graphs. *J. Algebra*, 168(2):536–567, 1994.

[5] Eva Bayer-Fluckiger. Definite unimodular lattices having an automorphism of given characteristic polynomial. *Comment. Math. Helv.*, 59(4):509–538, 1984.

[6] Eva Bayer-Fluckiger. Lattices and number fields. In *Algebraic geometry: Hirzebruch 70 (Warsaw, 1998)*, volume 241 of *Contemp. Math.*, pages 69–84. Amer. Math. Soc., Providence, RI, 1999.

[7] Eva Bayer-Fluckiger. Ideal lattices. In *A panorama of number theory or the view from Baker's garden (Zürich, 1999)*, pages 168–184. Cambridge Univ. Press, Cambridge, 2002.

[8] Eva Bayer-Fluckiger, Grégory Berhuy, and Pascale Chuard-Koulmann. CM-fields and skew-symmetric matrices. *Manuscripta Math.*, 114(3):351–359, 2004.

[9] Edward A. Bender. Area-Perimeter Relations for Two-Dimensional Lattices. *Amer. Math. Monthly*, 69(8):742–744, 1962.

[10] Edward A. Bender. Classes of matrices over an integral domain. *Illinois J. Math.*, 11:697–702, 1967.

[11] Edward A. Bender. Characteristic polynomials of symmetric matrices. *Pacific J. Math.*, 25:433–441, 1968.

[12] Edward A. Bender. Classes of matrices and quadratic fields. *Linear Algebra and Appl.*, 1:195–201, 1968.

[13] Edward A. Bender. The dimensions of symmetric matrices with a given minimum polynomial. *Linear Algebra and Appl.*, 3:115–123, 1970.

[14] Edward A. Bender. Characteristic polynomials of symmetric matrices. II. Local number fields. *Linear and Multilinear Algebra*, 2:55–63, 1974.

[15] Edward A. Bender and Norman P. Herzberg. Symmetric matrices, characteristic polynomials, and Hilbert symbols over local number fields. *Bull. Amer. Math. Soc.*, 79:518–520, 1973.

[16] Edward A. Bender and Norman P. Herzberg. Characteristic polynomials of symmetric matrices. III. Some counterexamples. *Linear and Multilinear Algebra*, 2:173–178, 1974.

[17] F. Beukers and C. J. Smyth. Cyclotomic points on curves. In *Number theory for the millennium, I (Urbana, IL, 2000)*, pages 67–85. A K Peters, Natick, MA, 2002.

[18] J. Bokowski and A. M. Odlyzko. Lattice points and the volume/area ratio of convex bodies. *Geometriae Dedicata*, 2:249–254, 1973.

[19] Peter Borwein. *Computational excursions in analysis and number theory.* CMS Books in Mathematics/Ouvrages de Mathématiques de la SMC, 10. Springer-Verlag, New York, 2002.

[20] Nicolas Bourbaki. *Commutative algebra. Chapters 1–7.* Elements of Mathematics (Berlin). Springer-Verlag, Berlin, 1989. Translated from the French, Reprint of the 1972 edition.

[21] B. Bukh. Ranks of matrices with few distinct entries. *ArXiv e-prints*, August 2015.

[22] Seung Ju Cheon, Hyun Kwang Kim, and Jun Ho Lee. Evaluation of the Dedekind zeta functions of some non-normal totally real cubic fields at negative odd integers. *Manuscripta Math.*, 124(4):551–560, 2007.

[23] Henri Cohen. Variations sur un thème de Siegel-Hecke. *Publ. Math. Univ. Bordeaux Année*, (5):1–45, 1973/74.

[24] Henri Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate Texts in Mathematics.* Springer-Verlag, Berlin, 1993.

[25] H. Cohn, A. Kumar, S. D. Miller, D. Radchenko, and M. Viazovska. The sphere packing problem in dimension 24. *Ann. of Math. (2)*, to appear.

[26] J. H. Conway and N. J. A. Sloane. *Sphere packings, lattices and groups*, volume 290 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences].* Springer-Verlag, New York, third edition, 1999. With additional contributions by E. Bannai, R. E. Borcherds, J. Leech, S. P. Norton, A. M. Odlyzko, R. A. Parker, L. Queen and B. B. Venkov.

[27] Zdravko Cvetkovski. *Inequalities.* Springer, Heidelberg, 2012. Theorems, techniques and selected problems.

[28] E. C. Dade, D. W. Robinson, O. Taussky, and M. Ward. Divisors of recurrent sequences. *J. Reine Angew. Math.*, 214/215:180–183, 1964.

[29] E. C. Dade, O. Taussky, and H. Zassenhaus. On the theory of orders, in paricular on the semigroup of ideal classes and genera of an order in an algebraic number field. *Math. Ann.*, 148:31–64, 1962.

[30] E. Dobrowolski. On a question of Lehmer and the number of irreducible factors of a polynomial. *Acta Arith.*, 34(4):391–401, 1979.

[31] Edward Dobrowolski. A note on integer symmetric matrices and Mahler's measure. *Canad. Math. Bull.*, 51(1):57–59, 2008.

[32] S. El Otmani, A. Maul, G. Rhin, and J.-M. Sac-Épée. Finding degree-16 monic irreducible integer polynomials of minimal trace by optimization methods. *Exp. Math.*, 23(1):1–5, 2014.

[33] Dennis R. Estes. Eigenvalues of symmetric integer matrices. *J. Number Theory*, 42(3):292–296, 1992.

[34] Dennis R. Estes and Robert M. Guralnick. Minimal polynomials of integral symmetric matrices. *Linear Algebra and its Applications*, 192(0):83 – 99, 1993.

[35] D. K. Faddeev. On a problem of analytical geometry. *C. R. (Doklady) Acad. Sci. URSS (N.S.)*, 47:539–540, 1945.

[36] D. K. Faddeev. On the characteristic equations of rational symmetirc matrices. *Doklady Akad. Nauk SSSR (N. S.)*, 58:753–754, 1947.

[37] D. K. Faddeev. Representations of algebraic numbers by matrices. *Zap. Naučn. Sem. Leningrad. Otdel. Mat. Inst. Steklov. (LOMI)*, 46:89–91, 141, 1974. Modules and representations.

[38] D. K. Faddeyev. Construction of fields of algebraical numbers whose Galois group is a group of quaternion units. *C. R. (Doklady) Acad. Sci. URSS (N.S.)*, 47:390–392, 1945.

[39] Shaun M. Fallat and Charles R. Johnson. *Totally nonnegative matrices.* Princeton Series in Applied Mathematics. Princeton University Press, Princeton, NJ, 2011.

[40] S. Fisk. Polynomials, roots, and interlacing. *ArXiv Mathematics e-prints*, December 2006.

[41] Robert W. Fitzgerald. Characteristic polynomials of symmetric matrices. *Linear and Multilinear Algebra*, 36(4):233–237, 1994.

[42] Sergey Fomin. Total positivity and cluster algebras. In *Proceedings of the International Congress of Mathematicians. Volume II*, pages 125–145. Hindustan Book Agency, New Delhi, 2010.

[43] Sergey Fomin and Andrei Zelevinsky. Total positivity: tests and parametrizations. *Math. Intelligencer*, 22(1):23–33, 2000.

[44] F. R. Gantmaher and M. G. Kreĭn. *Oscillyacionye matricy i yadra i malye kolebaniya mehaničeskih sistem.* Gosudarstv. Isdat. Tehn.-Teor. Lit., Moscow-Leningrad, 1950. 2d ed.

[45] M. Gasca and J. M. Peña. On factorizations of totally positive matrices. In *Total positivity and its applications (Jaca, 1994)*, volume 359 of *Math. Appl.*, pages 109–130. Kluwer Acad. Publ., Dordrecht, 1996.

[46] Chris Godsil and Gordon Royle. *Algebraic graph theory*, volume 207 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, 2001.

[47] Gary Greaves. Cyclotomic matrices over real quadratic integer rings. *Linear Algebra Appl.*, 437(9):2252–2261, 2012.

[48] Gary Greaves. Cyclotomic matrices over the Eisenstein and Gaussian integers. *J. Algebra*, 372:560–583, 2012.

[49] Gary Greaves. Small-span Hermitian matrices over quadratic integer rings. *Math. Comp.*, 84(291):409–424, 2015.

[50] Gary Greaves and Graeme Taylor. Lehmer's conjecture for Hermitian matrices over the Eisenstein and Gaussian integers. *Electron. J. Combin.*, 20(1):Paper 42, 22, 2013.

[51] Joseph Hammer. Volume-surface area relations for n-dimensional lattices. *Math. Z.*, 123:219–222, 1971.

[52] William F. Hammond. The modular groups of Hilbert and Siegel. *Amer. J. Math.*, 88:497–516, 1966.

[53] Erich Hecke. *Lectures on the theory of algebraic numbers*, volume 77 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1981. Translated from the German by George U. Brauer, Jay R. Goldman and R. Kotzen.

[54] A. Ya. Hinčin. A quantitative formulation of the approximation theory of Kronecker. *Izvestiya Akad. Nauk SSSR. Ser. Mat.*, 12:113–122, 1948.

[55] A. J. Hoffman. Eigenvalues of graphs. In *Studies in graph theory, Part II*, pages 225–245. Studies in Math., Vol. 12. Math. Assoc. Amer., Washington, D. C., 1975.

[56] Alan J. Hoffman. On limit points of spectral radii of non-negative symmetric integral matrices. In *Graph theory and applications (Proc. Conf., Western Michigan Univ., Kalamazoo, Mich., 1972; dedicated to the memory of J. W. T. Youngs)*, pages 165–172. Lecture Notes in Math., Vol. 303. Springer, Berlin, 1972.

[57] Nathan Jacobson. *Basic algebra. I.* W. H. Freeman and Company, New York, second edition, 1985.

[58] Nathan Jacobson. *Basic algebra. II.* W. H. Freeman and Company, New York, second edition, 1989.

[59] Charles R. Johnson. Interlacing polynomials. *Proc. Amer. Math. Soc.*, 100(3):401–404, 1987.

[60] Ravi Kannan and László Lovász. Covering minima and lattice-point-free convex bodies. *Ann. of Math. (2)*, 128(3):577–602, 1988.

[61] Byeong Moon Kim. Universal octonary diagonal forms over some real quadratic fields. *Comment. Math. Helv.*, 75(3):410–414, 2000.

[62] Myung-Hwan Kim. Recent developments on universal forms. In *Algebraic and arithmetic theory of quadratic forms*, volume 344 of *Contemp. Math.*, pages 215–228. Amer. Math. Soc., Providence, RI, 2004.

[63] M. Knebusch and W. Scharlau. Quadratische Formen und quadratische Reziprozitätsgesetze über algebraischen Zahlkörpern. *Math. Z.*, 121:346–368, 1971.

[64] Fred Krakowski. Eigenwerte und Minimalpolynome symmetrischer Matrizen in kommutativen Körpern. *Comment. Math. Helv.*, 32:224–240, 1958.

[65] L. Kronecker. Zwei Sätze über Gleichungen mit ganzzahligen Coefficienten. *J. Reine Angew. Math.*, 53:173–175, 1857.

[66] Mario Kummer. Eigenvalues of symmetric matrices over integral domains. *Journal of Algebra*, 466:195 – 203, 2016.

[67] Serge Lang. *Algebraic number theory*, volume 110 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1994.

[68] D. H. Lehmer. Factorization of certain cyclotomic functions. *Ann. of Math. (2)*, 34(3):461–479, 1933.

[69] Yanhua Liang and Qiang Wu. The trace problem for totally positive algebraic integers. *J. Aust. Math. Soc.*, 90(3):341–354, 2011.

[70] Hans Maass. Über die Darstellung total positiver Zahlen des Körpers $R(\sqrt{5})$ als Summe von drei Quadraten. *Abh. Math. Sem. Univ. Hamburg*, 14(1):185–191, 1941.

[71] Colin Maclachlan and Alan W. Reid. *The arithmetic of hyperbolic 3-manifolds*, volume 219 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2003.

[72] Guillermo Mantilla-Soler. On number fields with equivalent integral trace forms. *Int. J. Number Theory*, 8(7):1569–1580, 2012.

[73] Jiří Matoušek. *Lectures on discrete geometry*, volume 212 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2002.

[74] Hideyuki Matsumura. *Commutative ring theory*, volume 8 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1986. Translated from the Japanese by M. Reid.

[75] J. F. McKee, P. Rowlinson, and C. J. Smyth. Salem numbers and Pisot numbers from stars. In *Number theory in progress, Vol. 1 (Zakopane-Kościelisko, 1997)*, pages 309–319. de Gruyter, Berlin, 1999.

[76] James McKee. Small-span characteristic polynomials of integer symmetric matrices. In *Algorithmic number theory*, volume 6197 of *Lecture Notes in Comput. Sci.*, pages 270–284. Springer, Berlin, 2010.

[77] James McKee and Chris Smyth. Salem numbers of trace -2 and traces of totally positive algebraic integers. In *Algorithmic number theory*, volume

3076 of *Lecture Notes in Comput. Sci.*, pages 327–337. Springer, Berlin, 2004.

[78] James McKee and Chris Smyth. There are Salem numbers of every trace. *Bull. London Math. Soc.*, 37(1):25–36, 2005.

[79] James McKee and Chris Smyth. Integer symmetric matrices having all their eigenvalues in the interval $[-2, 2]$. *J. Algebra*, 317(1):260–290, 2007.

[80] James McKee and Chris Smyth. Integer symmetric matrices of small spectral radius and small Mahler measure. *Int. Math. Res. Not. IMRN*, (1):102–136, 2012.

[81] James McKee and Chris Smyth. Single polynomials that correspond to pairs of cyclotomic polynomials with interlacing zeros. *Cent. Eur. J. Math.*, 11(5):882–899, 2013.

[82] James McKee and Pavlo Yatsyna. A trace bound for positive definite connected integer symmetric matrices. *Linear Algebra Appl.*, 444:227–230, 2014.

[83] James McKee and Pavlo Yatsyna. Salem numbers of trace -2, and a conjecture of Estes and Guralnick. *J. Number Theory*, 160:409–417, 2016.

[84] John Milnor and Dale Husemoller. *Symmetric bilinear forms.* Springer-Verlag, New York, 1973. Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 73.

[85] Jürgen Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences].* Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[86] O. T. O'Meara. *Introduction to quadratic forms.* Springer-Verlag, New York, 1971. Second printing, corrected, Die Grundlehren der mathematischen Wissenschaften, Band 117.

[87] Allan Pinkus. *Totally positive matrices*, volume 181 of *Cambridge Tracts in Mathematics.* Cambridge University Press, Cambridge, 2010.

[88] Q. I. Rahman and G. Schmeisser. *Analytic theory of polynomials*, volume 26 of *London Mathematical Society Monographs. New Series.* The Clarendon Press Oxford University Press, Oxford, 2002.

[89] L. I. Roginskiĭ. Representation of the direct sum of two quadratic fields by rational symmetric matrices. *Zap. Naučn. Sem. Leningrad. Otdel. Mat. Inst. Steklov. (LOMI)*, 67:195–200, 227, 1977. Studies in number theory (LOMI), 4.

[90] L. I. Roginskiĭ. On a problem of N. G. Čebotarëv. *Izv. Vyssh. Uchebn. Zaved. Mat.*, (9):30–31, 1980.

[91] Justin Salez. Every totally real algebraic integer is a tree eigenvalue. *J. Combin. Theory Ser. B*, 111:249–256, 2015.

[92] A. P. Šapiro. Characteristic polynomials of rational symmetric matrices of third order. *Dokl. Akad. Nauk SSSR (N.S.)*, 119:890–892, 1958.

[93] A. P. Šapiro. Characteristic polynomials of symmetric matrices. *Sibirsk. Mat. Ž.*, 3:280–291, 1962.

[94] A. P. Šapiro. Characteristic polynomials of symmetric matrices of order four over the field of p-adic numbers. *Dal′nevostoč. Gos. Univ. Učen. Zap.*, 16:114–147, 1968.

[95] Wolfgang M. Schmidt. Volume, surface area and the number of integer points covered by a convex set. *Arch. Math. (Basel)*, 23:537–543, 1972.

[96] I. Schur. Über die Verteilung der Wurzeln bei gewissen algebraischen Gleichungen mit ganzzahligen Koeffizienten. *Math. Z.*, 1(4):377–402, 1918.

[97] Carl Ludwig Siegel. Sums of mth powers of algebraic integers. *Ann. of Math. (2)*, 46:313–339, 1945.

[98] Carl Ludwig Siegel. The trace of totally positive and real algebraic integers. *Ann. of Math. (2)*, 46:302–312, 1945.

[99] Carl Ludwig Siegel. Berechnung von Zetafunktionen an ganzzahligen Stellen. *Nachr. Akad. Wiss. Göttingen Math.-Phys. Kl. II*, 1969:87–102, 1969.

[100] C. J. Smyth. Salem numbers of negative trace. *Math. Comp.*, 69(230):827–838, 2000.

[101] Chris Smyth. The Mahler measure of algebraic numbers: a survey. In *Number theory and polynomials*, volume 352 of *London Math. Soc. Lecture Note Ser.*, pages 322–349. Cambridge Univ. Press, Cambridge, 2008.

[102] Chris Smyth. Seventy years of Salem numbers. *Bull. Lond. Math. Soc.*, 47(3):379–395, 2015.

[103] Christopher Smyth. Totally positive algebraic integers of small trace. *Ann. Inst. Fourier (Grenoble)*, 34(3):1–28, 1984.

[104] P. Stein. Classroom Notes: A Note on the Volume of a Simplex. *Amer. Math. Monthly*, 73(3):299–301, 1966.

[105] Olga Taussky. On a theorem of Latimer and MacDuffee. *Canadian J. Math.*, 1:300–302, 1949.

[106] Olga Taussky. Matrices of rational integers. *Bull. Amer. Math. Soc.*, 66:327–345, 1960.

[107] Graeme Taylor. Cyclotomic matrices and graphs over the ring of integers of some imaginary quadratic fields. *J. Algebra*, 331:523–545, 2011.

[108] Graeme Taylor. Lehmer's conjecture for matrices over the ring of integers of some imaginary quadratic fields. *J. Number Theory*, 132(4):590–607, 2012.

[109] M. Viazovska. The sphere packing problem in dimension 8. *Ann. of Math. (2)*, to appear.

[110] A. Weiss. Characteristic polynomials of symmetric matrices over local fields. In *Selected topics on ternary forms and norms (Sem. Number Theory, California Inst. Tech., Pasadena, Calif., 1974/75), Paper No. 9*, page 25. California Inst. Tech., Pasadena, Calif., 1976.