Finding all cospectral mates over a number field

Alexander Van Werde

Abstract. We investigate a notion of cospectrality for integer matrices that is parameterized by algebraic number fields. Given a number field and a symmetric integer matrix, we wonder when conjugating the integer matrix by an orthogonal matrix with entries in the given field can produce new integer matrices.

Our results concern sufficient conditions for the associated notion of spectral determination, and we give constraints on the orthogonal matrices when the conditions are not applicable. The results use the discriminant of the characteristic polynomial and properties of Krylov subspaces. We leverage the theory to develop an algorithm to find all cospectral mates over a given (small) field. An implementation of the algorithm is made available.

MSC2020 subject classifications: 05C50, 15B36, 11C20, 11R04, 05C60

Keywords: Integer matrix, Dedekind domain, discriminant, sufficient condition, Krylov subspace, computational algebraic number theory, spectral graph theory

Contents

1. Introduction 2
2. Results 5
2.1. General framework 5
2.2. Results over Dedekind domains 6
2.3. Algebraic number fields 8
3. Matrices over a Dedekind domain — Proofs for Section 2.2 11
3.1. Preliminaries 12
3.2. Discriminant and characteristic polynomial 12
3.3. Krylov spaces — Proof of Theorems 2.8 and 2.9 14
3.4. Divisibility by $\mathcal{P}^2$ — Proof of Theorem 2.1 15
4. Matrices over number fields — Proofs for Section 2.3 17
4.1. Sufficient conditions — Proof of Corollaries 2.11 and 2.12 17
4.2. Orthogonal matrices with a given level — Proof of Proposition 2.13 17
5. Algorithmic search for cospectral mates 18
5.1. Algorithm outline 18
5.2. Detailed description 19
5.3. Proof of algorithmic properties 24
6. Numerical experiments 26
References 29
Appendix A. Matrices with discriminant ±1 — Proof of Proposition 2.15 32
Appendix B. Numerical data for signed graphs and graphs with loops 33

University of Münster, Germany
E-mail address: a.van.werde@uni-muenster.de.

1. Introduction

Eigenvalues of symmetric integer matrices frequently reveal rich combinatorial information. For example, spectral methods are often applied in the study of graphs and their signed or weighted variants [2, 5, 12, 26]. A classical question in this area asks when the spectrum gives complete information.

More precisely, consider a symmetric integer matrix $\mathbf{X} \in \mathbb{Z}^{n\times n}$ and let $\phi_{\mathbf{X}}(x) \coloneqq \det(x\mathbf{I} - \mathbf{X})$ be its characteristic polynomial. Then, a symmetric matrix $\mathbf{Y} \in \mathbb{Z}^{n\times n}$ is a *cospectral mate* of $\mathbf{X}$ if $\phi_{\mathbf{X}} = \phi_{\mathbf{Y}}$. We say that $\mathbf{X}$ is *determined by its spectrum* if the only cospectral mates are the trivial ones $\mathbf{Y} = \mathbf{S}^\top\mathbf{X}\mathbf{S}$ following from conjugation of $\mathbf{X}$ by a signed permutation $\mathbf{S}$. Here, a *signed permutation* is a matrix with a single nonzero entry ± 1 in every row and column.

If $\mathbf{X}$ and $\mathbf{Y}$ are adjacency matrices of graphs and thus have nonnegative entries, then the signs may be removed and one recovers the notion of graph isomorphism. For signed graphs, conjugation by signed permutation corresponds to *switching equivalence* [2]. Questions concerning adjacency cospectrality of graphs date back to the 1956 work of Günthard and Primas on quantum chemistry [14]. The topic can also be viewed as a discrete variant on the question "Can one hear the shape of a drum?" that was popularized by Kac in 1966 [22].

There is unfortunately no known general method to decide whether a matrix is determined by spectrum, or to find its cospectral mates. (That is, aside from exhaustive enumeration which quickly becomes intractable [4, 16].) In many cases, however, an improved understanding has been achieved through the analysis of more restrictive notions such as cospectrality through small *switching methods* [1, 11, 32] or *generalized cospectrality* [21, 31, 42, 45, 48]. Note that $\mathbf{X}$ and $\mathbf{Y}$ are cospectral mates if and only if there exists an orthogonal matrix $\mathbf{Q}$ with $\mathbf{Q}^\top\mathbf{X}\mathbf{Q} = \mathbf{Y}$. The restricted notions can be interpreted as putting additional constraints on the orthogonal matrix.

Switching methods restrict to orthogonal matrices of the form $\operatorname{diag}(\mathbf{Q}_m, \mathbf{I}_{n-m})$ with a small nontrivial block of size $m \ll n$; see the unified framework of Abiad, Van de Berg, and Simoens [1, Definition 1]. Restricting the block size m can be interpreted as focusing on local obstructions for spectral characterization. Classical examples are *Godsil–McKay switching* [11] and *Schwenk switching* [32]. An efficient algorithmic implementation of switching methods will appear in a forthcoming work of Simoens and Van Overberghe [33].

Generalized cospectrality restricts the orthogonal matrix $\mathbf{Q}$ to satisfy $\mathbf{Q}\zeta = \eta$ for given integer vectors $\zeta, \eta \in \mathbb{Z}^n$; see Wang et al. [31, 42, 45, 48]. Notably, sufficient conditions that can certify that a matrix is determined by its generalized spectrum have been established [31, 42, 45, 48]. Such conditions are conjectured to apply with non-vanishing frequency to high-dimensional matrices [24, 42].

Moreover, algorithms to find all generalized cospectral mates have recently been developed by Wang and Wang [44]. They concern the case when the orthogonal matrix has to fix the all-ones vector. That is, $\mathbf{Q}e = e$ with $e = (1, \ldots, 1)^\top$. This notion has particular significance, as there are a number of equivalent formulations dating back to the 1980 work of Johnson and Newman [21].

Generalized cospectrality has the pleasing feature that it does not require any a-priori bound on the size of obstructions to spectral characterization. However, while switching methods naturally give a hierarchy of relaxations with $m = n$ recovering the classical notion of cospectrality, generalized cospectrality is a legitimately restricted notion that does not necessarily recover the classical variant.

The idea of the present paper is as follows: while it may not always be possible to relate cospectral $\mathbf{X}$ and $\mathbf{Y}$ by an orthogonal matrix $\mathbf{Q}$ satisfying $\mathbf{Q}\zeta = \eta$ for given integer vectors $\zeta, \eta \in \mathbb{Z}^n$, we can certainly assume that the entries of $\mathbf{Q}$ come from an algebraic number field. Indeed, the latter can be verified by using the orthogonal matrices from the eigendecomposition. This motivates studying the notion that arises by constraining the field:

Definition 1.1. Fix some number field K. Two symmetric integer matrices $\mathbf{X}, \mathbf{Y} \in \mathbb{Z}^{n\times n}$ are *cospectral mates over* K if there exists some $\mathbf{Q} \in K^{n\times n}$ that is orthogonal $\mathbf{Q}^\top\mathbf{Q} = \mathbf{I}$ and satisfies $\mathbf{Q}^\top\mathbf{X}\mathbf{Q} = \mathbf{Y}$.

The simplest case of $K = \mathbb{Q}$ is already of significant interest. Indeed, this case essentially recovers generalized cospectrality, as the constraint $\mathbf{Q}\zeta = \eta$ for integer $\zeta, \eta \in \mathbb{Z}^n$ implies that $\mathbf{Q}$ has rational entries under mild conditions that are necessary to make the theory a useful relaxation; see e.g., [45, Lemma 2.4], [31, Lemma 2.1], [48, Theorem 1.3]. Cospectrality over the rationals as an extension of generalized cospectrality was notably emphasized in a 2016 preprint of Wang and Yu [47] who proved sufficient conditions. See also Bhargava, Gross, and Wang [3, Proposition 35] for related conditions with pairs of p-adic matrices.

Section 2 presents our results. We give a condition to rule out cospectrality over an arbitrary number field K, and establish constraints on the potential orthogonal matrices $\mathbf{Q} \in K^{n\times n}$ when the condition is not applicable. Moreover, we leverage the results to develop an algorithm that can find all cospectral mates of $\mathbf{X}$ over K. The sufficient condition recovers [47, Theorem 1.4] when $K = \mathbb{Q}$. To our knowledge, the constraints on the orthogonal matrices were not previously known for $K = \mathbb{Q}$, nor were algorithms known without further restrictions.

The only assumption that is strictly required for our theory is that $\mathbf{X}$ should not have repeated eigenvalues. In particular, this assumption is applicable with high probability to the adjacency matrix of an Erdős–Rényi random graph with constant edge probability [34]. For practical applications of the algorithms, some additional assumptions are necessary to make computations tractable; see Section 2.3.2. Most crucially, we require that the field K is not too large. This requirement makes Definition 1.1 into a meaningful relaxation.

We have implemented the algorithm building on methods from `PARI` [30] and `SageMath` [35] for computational algebraic number theory. The source code is distributed in a repository named COSPECTRAL:

https://github.com/Alexander-Van-Werde/cospectral

Section 6 presents numerical results applying the algorithm to random integer matrices in dimension ≤ 100. We find that $K = \mathbb{Q}$ is a frequent source of cospectral mates, and a nontrivial fraction of additional mates arise over larger fields like the quadratic fields $K = \mathbb{Q}(\sqrt{d})$.

The idea to parametrize cospectrality by number fields arose from recent work of the author on the probability that the conjugation action of a fixed orthogonal matrix on a random integral matrix again yields an integral matrix; see Van Werde [39]. The probabilistic theory in [39] worked equally well over the rings of integers of number fields as over $\mathbb{Z}$, raising the question whether sufficient conditions could also be extended.

Some special cases of number fields have also appeared in sufficient conditions for generalized spectral characterization of *mixed graphs* [20, 43]. That is, graphs with both directed and undirected edges. The relevance of the number fields was there mainly to indicate edge directions. For instance, Wang, Qiu and Qian [43] considered a *Hermitian adjacency matrix* with entries from $\{0, 1, i, -i\}$ with $i = \sqrt{-1}$. They studied a notion of cospectrality that effectively restricts attention to conjugation by unitary matrices $\mathbf{U}$ with entries in the Gaussian rationals $\mathbb{Q}(i)$ satisfying $\mathbf{U}e = e$ with e the all-ones vector [43, Theorem 10].

We conclude this introduction with a few illustrative examples for Definition 1.1, and by outlining the structure of the remainder of the paper.

Example 1.2. A minimal example of a pair of adjacency cospectral graphs with loops is visualized in Figure 1. The characteristic polynomial is $x^4 - 2x^3 - x^2 + 2x$ which splits over $\mathbb{Q}$ with roots 2, ± 1, and 0. However, it turns out that these graphs are *not* adjacency cospectral over the rationals.

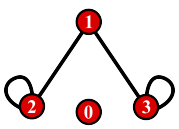
To explain this, note that normalizing eigenvectors here requires a field extension. For instance, the eigenvectors of $\mathbf{A}_1$ include $(0, 1, 1, 1)^\top$ and $(0, 0, -1, 1)^\top$. Normalizing thus requires dividing by $\sqrt{3}$ and $\sqrt{2}$. In fact, one can check that all eigenvectors of $\mathbf{A}_1$ and $\mathbf{A}_2$ can be normalized over $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, so the graphs are certainly cospectral over the latter field. Indeed, one can then find $\mathbf{Q}_1, \mathbf{Q}_2$ with

$$\mathbf{Q}_1^\top \mathbf{A}_1 \mathbf{Q}_1 = \operatorname{diag}(2, 1, -1, 0) = \mathbf{Q}_2^\top \mathbf{A}_2 \mathbf{Q}_2, \tag{1.1}$$

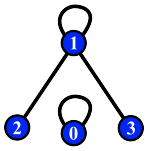
and hence $\mathbf{Q}^\top \mathbf{A}_1 \mathbf{Q} = \mathbf{A}_2$ with $\mathbf{Q} \coloneqq \mathbf{Q}_1 \mathbf{Q}_2^\top$. Actually, the matrices are already cospectral over $\mathbb{Q}(\sqrt{2})$:

$$\mathbf{Q}^\top \mathbf{A}_1 \mathbf{Q} = \mathbf{A}_2 \quad \text{with} \quad \mathbf{Q} = \frac{1}{\sqrt{2}} \begin{pmatrix} 0 & 0 & 1 & -1 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ -1 & 1 & 0 & 0 \end{pmatrix} \tag{1.2}$$

In this example, cancellations lead to cospectrality over a smaller field than is necessary to define the normalized eigenvectors of the individual matrices.



$$\mathbf{A}_1 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$$



$$\mathbf{A}_2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

FIGURE 1. Two cospectral graphs and their adjacency matrices.

Example 1.3. The theory and algorithms are particularly relevant for matrices with large entries or high dimensionality, since exhaustive enumeration of candidate cospectral mates then becomes infeasible.

In high dimensional settings, *Haemers' conjecture* proposes that the probability of cospectrality of dense Erdős–Rényi random graphs should tend to zero as the number of nodes grows large [17, 36]. In fixed dimensionality, on the other hand, a random symmetric matrix with entries uniform from $\{1, \dots, M\}$ is cospectral with probability bounded away from zero as $M \to \infty$. (See, e.g., [39].) It is not necessarily easy to guess whether the following matrix will be cospectral:

$$\mathbf{X} = \begin{pmatrix} 57 & 21 & 80 & 57 & 19 \\ 21 & 56 & 14 & 5 & 78 \\ 80 & 14 & 82 & 71 & 43 \\ 57 & 5 & 71 & 17 & 46 \\ 19 & 78 & 43 & 46 & 14 \end{pmatrix}. \tag{1.3}$$

Our algorithm reveals that $\mathbf{X}$ is cospectral over $\mathbb{Q}$. We have $\mathbf{Q}^\top \mathbf{X} \mathbf{Q} = \mathbf{Y}$ with

$$\mathbf{Y} = \begin{pmatrix} 33 & 1 & 115 & 49 & 6 \\ 1 & -7 & 23 & 12 & -9 \\ 115 & 23 & 136 & 14 & 30 \\ 49 & 12 & 14 & 90 & 29 \\ 6 & -9 & 30 & 29 & -26 \end{pmatrix}, \quad \mathbf{Q} = \frac{1}{31} \begin{pmatrix} 19 & -20 & 10 & -6 & 8 \\ -6 & -10 & 5 & 28 & 4 \\ -4 & 14 & 24 & -2 & 13 \\ 8 & 3 & 14 & 4 & -26 \\ 22 & 16 & -8 & 11 & 6 \end{pmatrix}. \tag{1.4}$$

Note that $\mathbf{Q}e \neq e$ with e the all-ones vector. This cospectral pair is not generalized cospectral in the sense of [44]. We refer to Section 6 for statistics on cospectrality probabilities for random integer matrices of varying dimensionality.

Outline. We present the results in Section 2. We give proofs in Sections 3 and 4. The algorithm is given in Section 5. We conclude with numerical experiments in Section 6.

2. Results

A key fact in our arguments is that the ring of integers in a number field is a Dedekind domain, so we present our results in this setting. A relevant example to keep in mind is $\mathbb{Z}[\sqrt{10}] \subseteq \mathbb{Q}(\sqrt{10})$, which is not a principal ideal domain. Other examples where the framework is applicable are the coordinate rings of non-singular curves such as $\mathbb{F}_p[x]$ and $\mathbb{R}[x, y]/(x^2 + y^2 - 1)\mathbb{R}[x, y]$.

We introduce the framework in Section 2.1, present our general results in Section 2.2, and specialize to algebraic number fields in Section 2.3.

2.1. General framework.

All rings in this paper are commutative and unital. A Noetherian integral domain R is a *Dedekind domain* if every nonzero proper ideal $\mathcal{I} \neq R$ admits a prime factorization, i.e., there exist distinct nonzero prime ideals $\mathcal{P}_1, \dots, \mathcal{P}_m \subseteq R$ and integers $e_1, \dots, e_m \geq 1$ with

$$\mathcal{I} = \mathcal{P}_1^{e_1} \mathcal{P}_2^{e_2} \cdots \mathcal{P}_m^{e_m}. \tag{2.1}$$

The prime ideals $\mathcal{P}_i$ and integers e_i in (2.1) are unique up to reordering.

Let K be the fraction field of R. We fix a symmetric matrix $\mathbf{X} \in R^{n\times n}$ and assume that there exist $\mathbf{Y} \in R^{n\times n}$ and some nonzero $\mathbf{Q} \in K^{n\times n}$ with

$$\mathbf{XQ} = \mathbf{QY} \quad \text{and} \quad \mathbf{Q}^\top\mathbf{Q} \in R^{n\times n}. \tag{2.2}$$

In particular, $\mathbf{Q}^\top\mathbf{Q} \in R^{n\times n}$ holds if $\mathbf{Q}$ is orthogonal in the strict sense $\mathbf{Q}^\top\mathbf{Q} = \mathbf{I}$, in which case the first condition states that $\mathbf{Q}^\top\mathbf{XQ} = \mathbf{Y}$. Some of our results however do not require the full strength of orthogonality. We will in general hence only assume (2.2) and explicitly state it when we impose stronger assumptions.

We measure how far $\mathbf{Q}$ is from being a matrix over R by considering the denominator of its entries. The *level* of $\mathbf{Q}$ is the ideal $\mathcal{L} \subseteq R$ defined by

$$\mathcal{L} \coloneqq \left\{r \in R : r\mathbf{Q} \in R^{n\times n}\right\}. \tag{2.3}$$

Note that $\mathcal{L} = R$ if and only if $\mathbf{Q} \in R^{n\times n}$.

If $R = \mathbb{Z}$, then $\mathbf{Q}$ has entries in the rational numbers and $\mathcal{L} \subseteq \mathbb{Z}$ is a principal ideal with generator given by the least common denominator of the entries of $\mathbf{Q}$. In this case, (2.3) recovers the definition of the level of a rational matrix used in previous sufficient conditions [31, 38, 45, 47, 48]. In such previous works, controlling the prime factorization over $\mathbb{Z}$ has been a key aim. The natural analogy for Dedekind domains is the prime factorization of ideals (2.1). An ideal $\mathcal{A} \subseteq R$ is said to be *divisible* by an ideal $\mathcal{B} \subseteq R$ if there exists an ideal $\mathcal{C} \subseteq R$ with $\mathcal{BC} = \mathcal{A}$. In this case, we write $\mathcal{B} \mid \mathcal{A}$. We write $\mathcal{B} \nmid \mathcal{A}$ otherwise.

Our initial goal will be to control the prime divisors of the level $\mathcal{L}$. If the level is nontrivial, then we further study the R-submodule of R^n defined by

$$\mathrm{Im}_R(\mathcal{L}\mathbf{Q}) \coloneqq \left\{\sum_{i=1}^{m} \ell_i\mathbf{Q}v_i : \ell_i \in \mathcal{L},\ v_i \in R^n\right\}. \tag{2.4}$$

The study of this module will enable constraints on the potential columns of $\mathbf{Q}$.

2.2. **Results over Dedekind domains.**

2.2.1. *Sufficient condition.* Recall that $\phi_{\mathbf{X}}(x) = \det(x\mathbf{I} - \mathbf{X})$ is the characteristic polynomial. We define the *discriminant* using the formal derivative $\phi'_{\mathbf{X}}$ as

$$\Delta_{\mathbf{X}} \coloneqq \det\big(\phi'_{\mathbf{X}}(\mathbf{X})\big). \tag{2.5}$$

Note that $\Delta_{\mathbf{X}} \in R$, so we can consider the ideal $\Delta_{\mathbf{X}}R \subseteq R$. The following Theorem 2.1 and Corollary 2.2 generalize [47] from $R = \mathbb{Z}$ to Dedekind domains:

Theorem 2.1. *If $\mathcal{P} \mid \mathcal{L}$ for some non-zero prime ideal $\mathcal{P} \subseteq R$ then $\mathcal{P}^2 \mid \Delta_{\mathbf{X}}R$.*

Corollary 2.2. *Suppose that $\Delta_{\mathbf{X}} \neq 0$ and that in the ideal prime factorization $\Delta_{\mathbf{X}}R = \prod_i \mathcal{P}_i^{e_i}$ every exponent satisfies $e_i \leq 1$. Then, $\mathcal{L} = R$.*

It is conjectured that the discriminant is square-free over $\mathbb{Z}$ with non-vanishing frequency for random symmetric integer matrices, such as those arising as the adjacency matrices of random graphs with loops; see Lvov and Van Werde [24, Conjecture 1.7]. Let us note however that $\Delta_{\mathbf{X}}$ being a square-free integer does not necessarily imply that $\Delta_{\mathbf{X}}R$ is a square-free ideal when R is the ring of integers of a number field; see Section 2.3.

Remark 2.3. In general, the *discriminant of a monic polynomial* $f \in R[x]$ can be defined using roots of f in the algebraic closure $\lambda_1, \ldots, \lambda_n \in \overline{K}$ as $\Delta_f := \prod_{i<j}(\lambda_i - \lambda_j)^2$. A direct calculation using Jordan decomposition verifies that we then have $\Delta_{\mathbf{X}} = \pm\Delta_{\phi_{\mathbf{X}}}$. This alternative definition may be useful when comparing to related literature, but we shall see that (2.5) is the natural definition for our proofs. I thank Nikita Lvov for bringing (2.5) as well as other formulations to my attention in our recent collaboration [24, Remark 3.11].

Remark 2.4. If $\mathbf{X}$ is the adjacency matrix of a simple graph on n nodes, then it always holds that $4 \mid \Delta_{\mathbf{X}}$ [46, 47]. Thus, different from graphs with loops, the discriminant is never square-free for simple graphs. The subsequent results are still applicable to simple graphs, although the algorithm's efficiency will be reduced when the dimensionality is large.

2.2.2. *Constraints on the matrix* $\mathbf{Q}$. We next constrain the possibilities for $\mathbf{Q}$ and $\mathcal{L}$ when $\Delta_{\mathbf{X}}R$ fails to be square-free. We first set up some notation.

Nonzero prime ideals in a Dedekind domain are maximal, so the quotient $\mathbb{F}_{\mathcal{P}} := R/\mathcal{P}$ is a field. Consider the factorization of $\phi_{\mathbf{X}}$ mod $\mathcal{P}$ into powers of irreducible monic polynomials $\gamma_1, \ldots, \gamma_m \in \mathbb{F}_{\mathcal{P}}[x]$:

$$\phi_{\mathbf{X}} \equiv \prod_{i=1}^{m} \gamma_i^{d_i} \bmod \mathcal{P}, \tag{2.6}$$

with $d_1, \ldots, d_m \geq 1$. Define an (approximate) square-root $\Gamma \in \mathbb{F}_{\mathcal{P}}[x]$ by

$$\Gamma := \prod_{i=1}^{m} \gamma_i^{\lfloor d_i/2 \rfloor}, \tag{2.7}$$

where $\lfloor\cdot\rfloor$ is the floor function.

Definition 2.5. Fix some $e \geq 1$. A R-submodule $\mathscr{M} \subseteq R^n$ is Γ-*contractive up to level* $\mathcal{P}^e$ if for every $k \leq e-1$ and $q \in \mathscr{M} \cap (\mathcal{P}^k)^n$ it holds that

$$\Gamma(\mathbf{X})q \equiv 0 \bmod \mathcal{P}^{k+1}. \tag{2.8}$$

Definition 2.6. Fix some $e \geq 1$. A R-submodule $\mathscr{M} \subseteq R^n$ is said to be *isotropic up to level* $\mathcal{P}^e$ if $q_1^\top q_2 \equiv 0 \bmod \mathcal{P}^e$ for every $q_1, q_2 \in \mathscr{M}$.

Isotropy has recently also played a role in sufficient conditions for generalized cospectrality by Guo and Wang [15].

Definition 2.7. The *Krylov space* of a set of vectors $w_1, \ldots, w_m \in R^n$ is given by

$$\mathscr{K}_{\mathbf{X}}(w_1, \ldots, w_m) := \left\{ \sum_{j=1}^{m} \sum_{i=0}^{n-1} c_{i,j} \mathbf{X}^i w_j : c_{i,j} \in R \right\}. \tag{2.9}$$

The Krylov space is sometimes also referred to as *control space* [9, 29] and relates to the *walk matrix* considered in some sufficient conditions for generalized spectral characterization [38, 41, 48] through the image of that matrix.

It would be equivalent to let the powers i run up to integers greater than $n-1$ in (2.9). Indeed, it follows from the Cayley–Hamilton theorem that $\mathbf{X}^n$ can be expressed as a R-linear combination of the $\mathbf{X}^i$ with $i < n$. Thus, the Krylov subspace can also be interpreted as the $R[x]$-module span of the vectors $w_1, \ldots, w_m$ when one

equips R^n with the action of $\mathbf{X}$. The latter perspective has also played a role in recent probabilistic results [24, 37].

The contraposition of the following Theorem 2.8 can be used to prove upper bounds on the greatest power of $\mathcal{P}$ that divides the level $\mathcal{L}$.

Theorem 2.8. *Assume that $\mathcal{P}^e \mid \mathcal{L}$ for some non-zero prime ideal $\mathcal{P} \subseteq R$ and $e \geq 1$. Then, there exists $w \in R^n$ with $w \not\equiv 0 \bmod \mathcal{P}$ for which the Krylov space $\mathscr{K}_{\mathbf{X}}(w)$ is Γ-contractive up to level $\mathcal{P}^e$ and isotropic up to level $\mathcal{P}^{2e}$.*

It can occur that the bound resulting from contraposition of Theorem 2.8 degenerates to infinity if a vector w with the claimed properties exists for every $e \geq 1$. For instance, this is (necessarily) so if $\mathbf{X} = \mathbf{I}$. We however prove in Lemma 5.10 that the bound is finite when R is the ring of integers of a number field and $\mathbf{X} \in \mathbb{Z}^{n\times n}$ satisfies $\Delta_{\mathbf{X}} \neq 0$. That is, if all eigenvalues of $\mathbf{X}$ are distinct.

We can also restrict the columns of $\mathbf{Q}$. Recall the definition of $\mathrm{Im}_R(\mathcal{L}\mathbf{Q})$ from (2.4). This module corresponds to a contractive and isotropic Krylov space:

Theorem 2.9. *Let $e \geq 1$ be an integer such that $\mathcal{P}^e \mid \mathcal{L}$. Then, there exist $m \geq 1$ vectors $w_1, \ldots, w_m \in R^n$, not all zero modulo $\mathcal{P}$, whose Krylov space $\mathscr{K}_{\mathbf{X}}(w_1, \ldots, w_m)$ is Γ-contractive up to level $\mathcal{P}^e$ and isotropic up to level $\mathcal{P}^{2e}$ and such that*

$$\mathrm{Im}_R(\mathcal{L}\mathbf{Q}) = \mathscr{K}_{\mathbf{X}}(w_1, \ldots, w_m). \tag{2.10}$$

2.3. **Algebraic number fields.** Recall that an *algebraic number field* is a field K of characteristic zero that is finite-dimensional as a $\mathbb{Q}$-vector space. Further, recall that the *ring of integers* $\mathcal{O}_K$ consists of the roots of monic integer polynomials:

$$\mathcal{O}_K := \left\{ k \in K : \exists m \geq 1,\ \exists c_i \in \mathbb{Z},\ k^m + c_{m-1}k^{m-1} + \cdots + c_0 = 0 \right\}. \tag{2.11}$$

The ring of integers of a number field is a Dedekind domain [28, C1, §3]. We next apply the results of the preceding Section 2.2 with $R = \mathcal{O}_K$. There, K denoted the fraction field of the Dedekind domain R. This is consistent with the current notation since the field K is indeed the fraction field of its ring of integers [28, C1, §2].

2.3.1. *Sufficient condition.* Consider an integer symmetric matrix $\mathbf{X} \in \mathbb{Z}^{n\times n}$. Then, the discriminant is also an integer $\Delta_{\mathbf{X}} \in \mathbb{Z}$. If the discriminant is further nonzero, then it admits a unique factorization:

$$\Delta_{\mathbf{X}} = \pm p_1^{h_1} p_2^{h_2} \cdots p_m^{h_m}, \tag{2.12}$$

for integers $h_i \geq 1$ and distinct prime numbers $p_i \in \mathbb{Z}_{\geq 2}$. Hence, as ideals,

$$\Delta_{\mathbf{X}}\mathcal{O}_K = \left(p_1\mathcal{O}_K\right)^{h_1} \left(p_2\mathcal{O}_K\right)^{h_2} \cdots \left(p_m\mathcal{O}_K\right)^{h_m}. \tag{2.13}$$

It would however be premature to conclude that Corollary 2.2 may be used if $h_i \leq 1$ for every i. Indeed, the ideals $p_i\mathcal{O}_K$ are not necessarily prime. Moreover, the ideals are not even necessarily square-free:

Definition 2.10. A prime number $p \in \mathbb{Z}_{\geq 2}$ is said to be *ramified* in the algebraic number field K if there exists a nonzero prime ideal $\mathcal{P} \subseteq \mathcal{O}_K$ with $\mathcal{P}^2 \mid p\mathcal{O}_K$.

Ramified primes always exist if $K \neq \mathbb{Q}$, but there are only finitely many [28, p.207]. For nonzero prime $\mathcal{P} \subseteq \mathcal{O}_K$, the ideal $\mathcal{P} \cap \mathbb{Z} \subseteq \mathbb{Z}$ is again prime and nonzero [25, C3, p44-45]. If p is the prime with $\mathcal{P} \cap \mathbb{Z} = p\mathbb{Z}$ then $\mathcal{P}$ is said to *lie above* p.

Consider a symmetric integer matrix $\mathbf{X} \in \mathbb{Z}^{n\times n}$ and suppose that we are given some matrix $\mathbf{Q} \in K^{n\times n}$ which satisfies (2.2) over $R = \mathcal{O}_K$. That is, $\mathbf{Q}^\top\mathbf{Q} \in \mathcal{O}_K^{n\times n}$ and there exists $\mathbf{Y} \in \mathcal{O}_K^{n\times n}$ with $\mathbf{XQ} = \mathbf{QY}$. Recall the definition of $\mathcal{L}$ from (2.3). The following results then follow from Theorem 2.1 and Corollary 2.2:

Corollary 2.11. *If $\mathcal{P} \mid \mathcal{L}$ for a non-zero prime ideal $\mathcal{P} \subseteq \mathcal{O}_K$, then $\mathcal{P}$ lies above a prime $p \in \mathbb{Z}_{\geq 2}$ with $p \mid \Delta_\mathbf{X}$. Moreover, if $p^2 \nmid \Delta_\mathbf{X}$ then the prime p is ramified in K and it holds that $\mathcal{P}^2 \mid p\mathcal{O}_K$.*

Corollary 2.12. *Assume that $\Delta_\mathbf{X} \neq 0$ and that none of the primes in the factorization (2.12) is ramified in K. Further, assume that all h_i in (2.12) satisfy $h_i \leq 1$. Then, $\mathcal{L} = \mathcal{O}_K$.*

The foregoing results all concerned the general setting of (2.2). Our main motivation however comes from matrices that are orthogonal in the strict sense that $\mathbf{Q}^\top\mathbf{Q} = \mathbf{I}$. Under an additional assumption on the number field, this allows us to deduce more restrictive constraints on the matrix $\mathbf{Q}$.

The number field K is said to be *totally real* if every field embedding $\sigma : K \to \mathbb{C}$ satisfies $\sigma(K) \subseteq \mathbb{R}$. In particular, this is the case for the splitting field of a polynomial $f \in \mathbb{Q}[x]$ if all roots of f are real.

Proposition 2.13. *Consider a totally real number field K. Then, for any fixed ideal $\mathcal{L} \subseteq \mathcal{O}_K$, there are only finitely many matrices $\mathbf{Q} \in K^{n\times n}$ with $\mathbf{Q}^\top\mathbf{Q} = \mathbf{I}$ and level ideal $\mathcal{L}$. Moreover, the only such matrices with $\mathcal{L} = \mathcal{O}_K$ are signed permutations.*

Combining Corollary 2.12 and Proposition 2.13 over some totally real algebraic number field K gives a sufficient condition to rule out nontrivial cospectral mates over K in the sense of Definition 1.1.

Example 2.14. Consider a positive square-free integer $d \geq 2$. Then $K = \mathbb{Q}(\sqrt{d})$ is totally real. The ramified primes are the prime divisors of d, and also $p = 2$ if $d \not\equiv 1 \bmod 4$ (see, e.g., , [28, C1, p.15], [28, C3, p.199, Theorem 2.6]):

$$\mathscr{P}_d = \begin{cases} \{\text{prime } p : p \mid d\} & \text{if } d \equiv 1 \bmod 4, \\ \{2\} \cup \{\text{prime } p : p \mid d\} & \text{if } d \not\equiv 1 \bmod 4. \end{cases} \tag{2.14}$$

Corollary 2.12 and Proposition 2.13 now yield a sufficient condition applicable to symmetric matrices $\mathbf{X} \in \mathbb{Z}^{n\times n}$ with square-free discriminant $\Delta_\mathbf{X}$ whose prime divisors $p \mid \Delta_\mathbf{X}$ satisfy $p \notin \mathscr{P}_d$. When applicable, we may conclude that the only orthogonal matrices $\mathbf{Q} \in K^{n\times n}$ with $\mathbf{Q}^\top\mathbf{XQ} \in \mathcal{O}_K^{n\times n}$ are signed permutations.

One notable example of a totally real number field is the field found by adjoining a root of the characteristic polynomial $\phi_\mathbf{X}$. Let us note however that the assumptions of Corollary 2.12 are essentially never applicable in that setting. In particular, if $\Delta_\mathbf{X}$ is square-free, then every prime divisor $p \mid \Delta_\mathbf{X}$ ramifies in the latter field if $\phi_\mathbf{X}$ is irreducible [25, p.79, Theorem 34] (see also the proof of Lemma A.1), and the assumption becomes $\Delta_\mathbf{X} = \pm 1$. Matrices with discriminant ± 1 are exceptional:

Proposition 2.15. *A symmetric matrix $\mathbf{X} \in \mathbb{Z}^{n\times n}$ with $n > 1$ satisfies $|\Delta_\mathbf{X}| = 1$ if and only if $n = 2$ and it is a diagonal matrix of the following form for some $a \in \mathbb{Z}$:*

$$\mathbf{X} = \begin{pmatrix} a & 0 \\ 0 & a \pm 1 \end{pmatrix}. \tag{2.15}$$

A proof is given in Appendix A. That the sufficient condition fails when the field is chosen depending on the matrix is not surprising. Indeed, if one considers the field K that arises from the splitting field after the tower of quadratic extensions necessary to normalize the eigenvectors into the unit vectors, then $\mathbf{X}$ can be related through an orthogonal matrix with entries in K to the diagonal matrix of eigenvalues, which has entries in $\mathcal{O}_K$.

2.3.2. *Algorithmic search for cospectral mates.* If Corollary 2.12 is not applicable in some given setting, then it may be possible to use our other results to constrain the potential orthogonal matrices to a finite set. This can be used to find all cospectral mates over K of a given matrix $\mathbf{X} \in \mathbb{Z}^{n\times n}$ with $\Delta_{\mathbf{X}} \neq 0$. We here describe when the resulting algorithm is reasonably efficient.

Let us note from the start that it will be important that the field K is not too large. This is because we have to solve problems in computational algebraic number theory that are otherwise prohibitively expensive.

Assumption 2.16. The number field K is totally real and is such that we can practically run algorithms over $\mathcal{O}_K$. (e.g., computing the list of ramified primes, determining the prime ideals $\mathcal{P} \subseteq \mathcal{O}_K$ with $\mathcal{P}^2 \mid p\mathcal{O}_K$ for some given $p \in \mathbb{Z}$,...)

Even if the number field is small, like $K = \mathbb{Q}$, we will have to determine all primes p that satisfy $p^2 \mid \Delta_{\mathbf{X}}$. To our knowledge, there is no way to do this that is significantly more efficient than factorizing the discriminant. Prime factorization is tractable for some moderate-sized matrices, such as those in Example 1.3, but prohibitively expensive for large matrices.

Probabilistic heuristics however suggest the relevant primes should typically all be small. Indeed, modeling $\Delta_{\mathbf{X}}$ as a random integer gives a probability of order $1/p^2$ for divisibility by p^2, which is summable. (See also [24, Conjecture 1.7] for refined predictions.) We assume knowledge of an a-priori bound:

Assumption 2.17. We are given an integer $M \geq 1$ such that every prime number p with $p^2 \mid \Delta_{\mathbf{X}}$ satisfies that $p \leq M$.

In practice, if a rigorous upper bound is unknown, then one can simply substitute a large value of M for a heuristic algorithm. We can then not guarantee the completeness of the set of cospectral mates, only that we find all orthogonal matrices whose level only contains ideals lying above primes $p \leq M$.

The efficiency of the algorithm also depends on the approximate square root Γ defined in (2.7):

Assumption 2.18. It holds for every prime ideal $\mathcal{P} \subseteq \mathcal{O}_K$ with $\mathcal{P}^2 \mid \Delta_{\mathbf{X}}\mathcal{O}_K$ that the polynomial $\Gamma \in \mathbb{F}_{\mathcal{P}}[x]$ has low degree.

Different from Assumption 2.17, the degree of Γ does not have to be known from the start.

Subject to the foregoing assumptions, Algorithm 1 in Section 5 enables finding all cospectral mates of $\mathbf{X}$ over K. This is done essentially by bounding the level and next searching through the finitely many orthogonal matrices that remain possible, although implementing this idea requires developing additional theory. At any rate, we have the following guarantee:

Theorem 2.19. *Consider an integer symmetric matrix* $\mathbf{X} \in \mathbb{Z}^{n\times n}$ *with* $\Delta_{\mathbf{X}} \neq 0$ *and a totally real number field* K*. Then, Algorithm 1 terminates in finite time and outputs all matrices* $\mathbf{Q} \in K^{n\times n}$ *with* $\mathbf{Q}^\top\mathbf{Q} = \mathbf{I}$ *and* $\mathbf{Q}^\top\mathbf{X}\mathbf{Q} \in \mathcal{O}_K^{n\times n}$*.*

This guarantee does not require the foregoing assumptions, but they are nonetheless crucial for the interpretation. In particular, the subroutines involved are reasonably tractable only if the assumptions are applicable.

For comparison, it could also be shown by more elementary means that there are only finitely many symmetric matrices $\mathbf{Y} \in \mathbb{Z}^{n\times n}$ that are cospectral to $\mathbf{X}$. Indeed, since the trace of a matrix is the sum of the eigenvalues,

$$\sum_{i,j=1}^{n} \mathbf{X}_{i,j}^2 = \mathrm{Tr}(\mathbf{X}^2) = \mathrm{Tr}(\mathbf{Y}^2) = \sum_{i,j=1}^{n} \mathbf{Y}_{i,j}^2. \tag{2.16}$$

In principle, this also enables finding all such matrices $\mathbf{Y}$ by brute force in finite time. The usability of such an exhaustive method is however limited due to the number of candidate matrices exploding as a function of $\sum_{i,j} \mathbf{X}_{i,j}^2$.

Even if one restricts $\mathbf{X}$ and $\mathbf{Y}$ to have entries in $\{0, 1\}$, the number of candidate matrices to compare with in (2.16) grows exponentially in n^2. It took a non-trivial effort when Brouwer and Spence determined the fraction of cospectral graphs on $n \leq 12$ nodes through exhaustive enumeration [4], extending earlier work by Godsil and McKay [10] for $n \leq 9$ and by Haemers and Spence for $n \leq 11$ [16].

Algorithm 1 can be applied to to integer matrices that simultaneously have large entries and high dimensionality. In fact, due to phenomena related to Remark 2.4, such applications with general symmetric integer matrices will typically run somewhat faster than applications to simple graphs. Numerical data is given in Section 6.

Remark 2.20. One can not guarantee that there are only finitely many orthogonal matrices $\mathbf{Q} \in K^{n\times n}$ with $\mathbf{Q}^\top\mathbf{X}\mathbf{Q} \in \mathcal{O}_K^{n\times n}$ if $\Delta_{\mathbf{X}} = 0$. For example, consider $\mathbf{X} = \mathbf{I}$. In fact, infinitely many orthogonal matrices with $\mathbf{Q}^\top\mathbf{X}\mathbf{Q} \in \mathcal{O}_K^{n\times n}$ appears to be the typical behavior when $\Delta_{\mathbf{X}} = 0$, at least when K is sufficiently large, since one can act by rotation on an eigenspace with repeated eigenvalue. Thus, the assumption in Theorem 2.19 is necessary to guarantee a finite output.

On the other hand, these examples arise from the fact that there are infinitely many orthogonal matrices with $\mathbf{X} = \mathbf{Q}^\top\mathbf{X}\mathbf{Q}$ and do not actually give rise to an infinitude of cospectral mates. (Indeed, there can only be finitely many cospectral mates due to (2.16).) Theory and algorithms for matrices with repeated eigenvalues remain an interesting question for future work.

3. Matrices over a Dedekind domain — Proofs for Section 2.2

Throughout this section, we adopt the general framework from Section 2.1. Thus, let $\mathbf{X}, \mathbf{Y} \in R^{n\times n}$ be matrices over a Dedekind domain with $\mathbf{X}$ symmetric, and consider a matrix $\mathbf{Q} \in K^{n\times n}$ over the fraction field such that (2.2) is satisfied.

We set up some general preliminaries in Section 3.1 that are repeatedly used in the subsequent arguments. The arguments for Theorems 2.1, 2.8, and 2.9 are subsequently given in Sections 3.2 to 3.4.

3.1. **Preliminaries.**

3.1.1. *Structure of the image module.* Recall the definitions of $\mathcal{L}$ and $\mathrm{Im}_R(\mathcal{L}\mathbf{Q})$ from (2.3) and (2.4), respectively. The following two results show how the assumption (2.2) is reflected in the structure of $\mathrm{Im}_R(\mathcal{L}\mathbf{Q})$.

Lemma 3.1. *The matrix* $\mathbf{X}$ *restricts to a* R*-linear map on* $\mathrm{Im}_R(\mathcal{L}\mathbf{Q})$*,*

$$\mathbf{X}\,|_{\mathrm{Im}_R(\mathcal{L}\mathbf{Q})}\colon \mathrm{Im}_R(\mathcal{L}\mathbf{Q}) \to \mathrm{Im}_R(\mathcal{L}\mathbf{Q}) : v \mapsto \mathbf{X}v. \tag{3.1}$$

Proof. By (2.2), there exists $\mathbf{Y} \in R^{n\times n}$ with $\mathbf{X}(\ell\mathbf{Q}) = (\ell\mathbf{Q})\mathbf{Y}$ for every $\ell \in \mathcal{L}$. Recall from the definition (2.4) that every vector in $\mathrm{Im}_R(\mathcal{L}\mathbf{Q})$ is a R-linear combination of vectors of the form $(\ell\mathbf{Q})v$ with $v \in R^n$ and $\ell \in \mathcal{L}$. It hence follows that $\mathbf{X}(\mathrm{Im}_R(\mathcal{L}\mathbf{Q})) \subseteq \mathrm{Im}_R(\mathcal{L}\mathbf{Q})$, as desired. □

Lemma 3.2. *It holds for every* $q_1, q_2 \in \mathrm{Im}_R(\mathcal{L}\mathbf{Q})$ *that* $q_1^\top q_2 \equiv 0 \bmod \mathcal{L}^2$*.*

Proof. By (2.2), we have $v_1^\top\mathbf{Q}^\top\mathbf{Q}v_2 \in R$ for all $v_1, v_2 \in R^n$. Hence, $(\ell_1 v_1)^\top\mathbf{Q}^\top\mathbf{Q}(\ell_2 v_2) \in \mathcal{L}^2$ for every $\ell_1, \ell_2 \in \mathcal{L}$. The claim is hence immediate from the definition (2.4). □

3.1.2. *Ideal arithmetic.* We will rely on the ideal arithmetic of Dedekind domains and hence recall the properties for easy reference. Recall that a *fractional ideal* is a R-submodule $\mathcal{F} \subseteq K$ of the fraction field K such that $r\mathcal{F} \subseteq R$ for some non-zero $r \in R$. Recall that $\mathcal{F}^{-1} \coloneqq \{k \in K : k\mathcal{F} \subseteq R\}$.

Proposition 3.3. *Every nonzero fractional ideal* $\mathcal{F} \subseteq K$ *admits a factorization* $\mathcal{F} = \mathcal{P}_1^{f_1}\cdots\mathcal{P}_m^{f_m}$ *with* $f_j \in \mathbb{Z}$ *and distinct prime ideals* $\mathcal{P}_j \subseteq R$*, which is unique up to reordering of the factors. If* $\mathcal{G} = \mathcal{P}_1^{g_1}\cdots\mathcal{P}_m^{g_m}$ *is another fractional ideal, then*

$$\mathcal{F}+\mathcal{G} = \textstyle\prod_{j=1}^m \mathcal{P}_j^{\min\{f_j,g_j\}},\ \ \mathcal{F}\cap\mathcal{G} = \prod_{j=1}^m \mathcal{P}_j^{\max\{f_j,g_j\}},\ \ \mathcal{F}\mathcal{G} = \prod_{j=1}^m \mathcal{P}_j^{f_j+g_j} \tag{3.2}$$

In particular, $\mathcal{F} \subseteq \mathcal{G}$ *if and only if* $f_j \geq g_j$ *for every* j*.*

Proof. See [50, Chapter 5, Theorem 11], [25, Chapter 3], or [8, Chapter 16]. □

Lemma 3.4. *Suppose that* $\mathcal{L} \neq R$ *and consider a nonzero prime divisor* $\mathcal{P} \mid \mathcal{L}$*. Then, there exists at least one* $\ell \in \mathcal{L}$ *with* $\ell\mathbf{Q} \not\equiv 0 \bmod \mathcal{P}$*.*

Proof. Consider the prime factorization $\mathcal{L} = \prod_{j=1}^m \mathcal{P}_j^{e_j}$ and suppose to the contrary that $\mathcal{L}\times(\sum_{v,w=1}^n \mathbf{Q}_{v,w}R) \subseteq \mathcal{P}_i R$ for some $\mathcal{P}_i$ with $e_i \geq 1$. Then, by the inclusion and multiplication properties of fractional ideals,

$$(\mathcal{P}_i^{e_i-1}\textstyle\prod_{j\neq i}\mathcal{P}_j^{e_j})\times(\sum_{v,w=1}^n \mathbf{Q}_{v,w}R) \subseteq R. \tag{3.3}$$

This would however contradict that $\mathcal{L}$ is the maximal (non-fractional) ideal satisfying $\mathcal{L}\times(\sum_{v,w=1}^n \mathbf{Q}_{v,w}R) \subseteq R$; recall the definition (2.3). □

3.2. **Discriminant and characteristic polynomial.** Among other things, we here prove a first step towards Theorem 2.1 by establishing that $\mathcal{P} \mid \mathcal{L}$ implies that $\mathcal{P} \mid \Delta_{\mathbf{X}}R$. (The strengthening to $\mathcal{P}^2 \mid \Delta_{\mathbf{X}}R$ is proved in Section 3.4.) We rely on the following classical property of the discriminant:

Lemma 3.5. *Let* $\mathbb{F}$ *be a field. Then,* $g^2 \mid \phi_{\mathbf{M}}$ *for* $g \in \mathbb{F}[x]$ *with* $\deg(g) \geq 1$ *implies that* $\Delta_{\mathbf{M}} = 0$ *in* $\mathbb{F}$*. Moreover, the converse also holds if* $\mathbb{F}$ *is a perfect field.*

Proof. Consider the factorization of the characteristic polynomial, i.e., $\phi_{\mathbf{M}} = \prod_j g_j^{d_j}$ with $g_j \in \mathbb{F}[x]$ coprime, monic, and irreducible. Then,

$$\phi'_{\mathbf{M}} = \sum_j d_j g_j^{d_j - 1} g'_j \prod_{i \neq j} g_i^{d_i}. \tag{3.4}$$

Note that $f \in \mathbb{F}[x]$ satisfies $\det(f(\mathbf{M})) = 0$ if and only if f has shared roots with $\phi_{\mathbf{M}}$ in the latter's splitting field. Shared roots are implied by shared irreducible divisor and this is an equivalence if $\mathbb{F}$ is perfect. The result hence follows from the definition $\Delta_{\mathbf{M}} = \det(\phi'_{\mathbf{M}}(\mathbf{M}))$ since (3.4) yields that $\phi'_{\mathbf{M}} \equiv 0 \bmod g_j$ if and only if $d_j \geq 2$. □

Let us assume that $\mathcal{L} \neq R$. Motivated by Lemma 3.5, our goal in the subsequent results is to study the characteristic polynomial of $\mathbf{X}$ over $\mathbb{F}_{\mathcal{P}} = R/\mathcal{P}$ for a prime ideal $\mathcal{P} \mid \mathcal{L}$. We rely on the properties of $\mathrm{Im}_R(\mathcal{L}\mathbf{Q})$ from Section 3.1.1.

Let $\mathcal{Q}_0 \subseteq \mathbb{F}_{\mathcal{P}}^n$ be the subspace found as the reduction of $\mathrm{Im}_R(\mathcal{L}\mathbf{Q})$ modulo $\mathcal{P}$. Further, for every $k \geq 1$ let $\mathcal{Q}_k \subseteq \mathbb{F}_{\mathcal{P}}^n$ be the reduction modulo $\mathcal{P}$ of $\{q \in R^n : \forall r \in \mathcal{P}^k,\ rq \in \mathrm{Im}_R(\mathcal{L}\mathbf{Q}) + (\mathcal{P}^{k+1})^n\}$. This defines a nested sequence of subspaces:

$$\mathcal{Q}_0 \subseteq \mathcal{Q}_1 \subseteq \mathcal{Q}_2 \subseteq \cdots \tag{3.5}$$

Informally, the vectors in the difference $\mathcal{Q}_k \setminus \mathcal{Q}_{k-1}$ can be interpreted as the new directions that are observed when going from the reduction of $\mathrm{Im}_R(\mathcal{L}\mathbf{Q})$ modulo $\mathcal{P}^k$ to the reduction modulo $\mathcal{P}^{k+1}$.

Lemma 3.6. *Assume that $\mathcal{P} \mid \mathcal{L}$. Then, $\mathcal{Q}_k \neq 0$ for all $k \geq 0$.*

Proof. Due to the inclusions (3.5), it suffices to consider $k = 0$. The latter case follows from Lemma 3.4 since $\ell\mathbf{Q} \not\equiv 0 \bmod \mathcal{P}$ for some $\ell \in \mathcal{L}$ implies that $\mathrm{Im}_R(\mathcal{L}\mathbf{Q})$ contains at least one vector with nonzero reduction modulo $\mathcal{P}$. □

Given a subspace $V \subseteq \mathbb{F}_{\mathcal{P}}^n$, the *orthogonal dual* is the subspace defined by $V^\perp := \{w \in \mathbb{F}_{\mathcal{P}}^n : \forall v \in V,\ w^\top v = 0\}$. A subspace with $V \subseteq V^\perp$ is called *isotropic*. Such subspaces are precisely the reductions modulo $\mathcal{P}$ of submodules of R^n that are isotropic modulo $\mathcal{P}$ in the sense of Definition 2.6.

Lemma 3.7. *Assume that $\mathcal{P}^e \mid \mathcal{L}$. Then, $\mathcal{Q}_k$ is isotropic for every $k \leq e - 1$.*

Proof. Let $q_1, q_2 \in \{q \in R^n : \forall r \in \mathcal{P}^k,\ rq \in \mathrm{Im}_R(\mathcal{L}\mathbf{Q}) + (\mathcal{P}^{k+1})^n\}$. Then, by definition of $\mathcal{Q}_k$, it suffices to show that $q_1^\top q_2 \equiv 0 \bmod \mathcal{P}$.

Using Lemma 3.2, it holds for all $r_1, r_2 \in \mathcal{P}^k$ that the vectors $v_i := r_i q_i$ satisfy $v_1^\top v_2 \equiv 0 \bmod \mathcal{P}^{2k+1}$. Thus, we have an ideal inclusion $\mathcal{P}^{2k}(q_1^\top q_2 R) \subseteq \mathcal{P}^{2k+1}$. The ideal arithmetic from Proposition 3.3 then yields that $q_1^\top q_2 R \subseteq \mathcal{P}$, as desired. □

Given a polynomial $g \in \mathbb{F}_{\mathcal{P}}[x]$, let $\mathcal{V}_g \subseteq \mathbb{F}_{\mathcal{P}}^n$ denote the primary subspace:

$$\mathcal{V}_g := \left\{v \in \mathbb{F}_{\mathcal{P}}^n : \exists j \geq 1,\ g(\mathbf{X})^j v = 0\right\}. \tag{3.6}$$

Let it be understood that $\dim_{\mathcal{P}}(\cdot)$, $\mathrm{Im}_{\mathcal{P}}(\cdot)$, and $\ker_{\mathcal{P}}(\cdot)$ refer to the respective operations over the field $\mathbb{F}_{\mathcal{P}}$. So, for instance, $\ker_{\mathcal{P}}(\mathbf{M}) \subseteq \mathbb{F}_{\mathcal{P}}^n$ for a matrix $\mathbf{M} \in R^{n \times n}$ refers to the kernel over $\mathbb{F}_{\mathcal{P}}$ of the matrix $\mathbf{M}$ mod $\mathcal{P}$.

Lemma 3.8. *Assume that $\mathcal{P}^e \mid \mathcal{L}$. Then, for every $k \leq e - 1$ and $g \in \mathbb{F}_{\mathcal{P}}[x]$,*

$$\dim_{\mathcal{P}}(\mathcal{V}_g) \geq 2 \dim_{\mathcal{P}}(\mathcal{Q}_k \cap \mathcal{V}_g). \tag{3.7}$$

Proof. Note that $v \notin \mathscr{V}_g$ implies that $g(\mathbf{X})^j v \notin \mathscr{V}_g$ for every j. In other words, a vector $v \in \mathbb{F}_{\mathcal{P}}^n$ can only satisfy $g(\mathbf{X})^j v \in \mathscr{V}_g$ if $v \in \mathscr{V}_g$. Fix some sufficiently large $j \geq 1$ with $\ker_{\mathcal{P}}(g(\mathbf{X})^j) = \mathscr{V}_g$ and note that we then have $\mathrm{Im}_{\mathcal{P}}(g(\mathbf{X})^j) \cap \mathscr{V}_g = 0$. In particular,

$$\mathrm{Im}_{\mathcal{P}}(g(\mathbf{X})^j) \cap (\mathscr{Q}_k \cap \mathscr{V}_g) = 0. \tag{3.8}$$

Recall from Lemma 3.7 that $\mathscr{Q}_k \subseteq \mathscr{Q}_k^{\perp}$. In particular, $\mathscr{Q}_k \cap \mathscr{V}_g \subseteq (\mathscr{Q}_k \cap \mathscr{V}_g)^{\perp}$. Further, using that $\mathbf{X}$ is symmetric and that $g(\mathbf{X})^j$ annihilates every vector in $\mathscr{V}_g$ by definition of j, we have $q^{\top} g(\mathbf{X})^j v = 0$ for every $q \in \mathscr{V}_g$ and $v \in \mathbb{F}_{\mathcal{P}}^n$. Thus, $\mathrm{Im}_{\mathcal{P}}(g(\mathbf{X})^j) \subseteq \mathscr{V}_g^{\perp}$. In particular, we also have that $\mathrm{Im}_{\mathcal{P}}(g(\mathbf{X})^j) \subseteq (\mathscr{Q}_k \cap \mathscr{V}_g)^{\perp}$.

We have proved that $\mathscr{Q}_k \cap \mathscr{V}_g$ and $\mathrm{Im}_{\mathcal{P}}(g(\mathbf{X})^j)$ are both subspaces of $(\mathscr{Q}_k \cap \mathscr{V}_g)^{\perp}$, and these subspaces are independent by (3.8). Hence,

$$\dim_{\mathcal{P}}\big(\mathscr{Q}_k \cap \mathscr{V}_g\big) + \dim_{\mathcal{P}}\big(\mathrm{Im}_{\mathcal{P}}(g(\mathbf{X})^j)\big) \leq \dim_{\mathcal{P}}\big((\mathscr{Q}_k \cap \mathscr{V}_g)^{\perp}\big). \tag{3.9}$$

Note that $\dim_{\mathcal{P}}(\mathrm{Im}_{\mathcal{P}}(g(\mathbf{X})^j)) = n - \dim_{\mathcal{P}}(\ker_{\mathcal{P}}(g(\mathbf{X})^j)) = n - \dim_{\mathcal{P}}(\mathscr{V}_g)$ and that $\dim_{\mathcal{P}}((\mathscr{Q}_k \cap \mathscr{V}_g)^{\perp}) = n - \dim_{\mathcal{P}}(\mathscr{Q}_k \cap \mathscr{V}_g)$ to find (3.7). □

The well-definedness of the restriction of $\mathbf{X}$ to $\mathrm{Im}_R(\mathcal{L}\mathbf{Q})$ from Lemma 3.1 implies that $\mathbf{X}$ mod $\mathcal{P}$ restricts to $\mathscr{Q}_k$ for every k. Let $\psi_k(x) \in \mathbb{F}_{\mathcal{P}}[x]$ denote the characteristic polynomial of this restriction $\mathbf{X}|_{\mathscr{Q}_k}$. Note that $\deg(\psi_k) \geq 1$ by Lemma 3.6.

Lemma 3.9. *Assume that $\mathcal{P}^e \mid \mathcal{L}$ and consider some $k \leq e-1$. Then, $\psi_k^2 \mid \phi_{\mathbf{X}}$ as polynomials over $\mathbb{F}_{\mathcal{P}}$.*

Proof. Consider some irreducible factor $g \in \mathbb{F}_{\mathcal{P}}[x]$ of ψ_k and let $h \geq 1$ be maximal with $g^h \mid \psi_k$. It then suffices to show that $g^{2h} \mid \phi_{\mathbf{X}}$.

By the primary decomposition theorem [19, C6, Thm.12; C7, Thm.4], the power of g in the characteristic polynomial is proportional to the dimension of the primary subspace:

$$\sup\{d \geq 0 : g^d \mid \phi_{\mathbf{X}}\} = \dim_{\mathcal{P}}(\mathscr{V}_g)/\deg(g). \tag{3.10}$$

The exact same argument applies with $\phi_{\mathbf{X}}$ replaced by ψ_k, as the latter is the characteristic polynomial of the restriction of $\mathbf{X}$ to $\mathscr{Q}_k$:

$$h = \dim_{\mathcal{P}}(\mathscr{Q}_k \cap \mathscr{V}_g)/\deg(g). \tag{3.11}$$

It now follows from Lemma 3.8 that $g^{2h} \mid \phi_{\mathbf{X}}$, as desired. □

Corollary 3.10. *Assume that $\mathcal{P} \mid \mathcal{L}$. Then, $\mathcal{P} \mid \Delta_{\mathbf{X}} R$.*

Proof. Combine Lemmas 3.5 and 3.9 and note that $\mathcal{P} \mid \Delta_{\mathbf{X}} R$ if and only if $\Delta_{\mathbf{X}}$ vanishes in $\mathbb{F}_{\mathcal{P}}$. □

3.3. **Krylov spaces — Proof of Theorems 2.8 and 2.9.** Note that it holds for every $w_1, \ldots, w_m \in R^n$ and $i \leq m$ that $\mathscr{K}_{\mathbf{X}}(w_i) \subseteq \mathscr{K}_{\mathbf{X}}(w_1, \ldots, w_m)$. Hence, considering that Γ-contractivity and isotropy are inherited by subspaces, it suffices to prove Theorem 2.9 since the latter implies Theorem 2.8.

Proof of Theorem 2.9. By definition, Dedekind domains are Noetherian. Hence, every submodule of R^n is finitely generated. Let $w_1, \ldots, w_m \in \mathrm{Im}_R(\mathcal{L}\mathbf{Q})$ be a set of generators for $\mathrm{Im}_R(\mathcal{L}\mathbf{Q}) \subseteq R^n$.

That the w_i generate $\mathrm{Im}_R(\mathcal{LQ})$ implies that $\mathrm{Im}_R(\mathcal{LQ}) \subseteq \mathscr{K}_{\mathbf{X}}(w_1, \ldots, w_m)$. On the other hand, recall from Lemma 3.1 that the action of $\mathbf{X}$ restricts to $\mathrm{Im}_R(\mathcal{LQ})$. Thus, recalling Definition 2.7, it follows from $w_1, \ldots, w_m \in \mathrm{Im}_R(\mathcal{LQ})$ that $\mathscr{K}_{\mathbf{X}}(w_1, \ldots, w_m) \subseteq \mathrm{Im}_R(\mathcal{LQ})$. This proves the equality (2.10).

It remains to prove that $\mathcal{P}^e \mid \mathcal{L}$ implies that $\mathrm{Im}_R(\mathcal{LQ})$ is Γ-contractive up to level $\mathcal{P}^e$ and isotropic up to level $\mathcal{P}^{2e}$. Isotropy is immediate from Lemma 3.2, so only contractivity remains. Pick some arbitrary $v \in \mathrm{Im}_R(\mathcal{LQ})$ with $v \equiv 0 \bmod \mathcal{P}^k$ for some $k \leq e-1$. Then, recalling the definition of contractivity from Definition 2.5, it has to be shown that $\Gamma(\mathbf{X})v \equiv 0 \bmod \mathcal{P}^{k+1}$.

Recall that any nontrivial quotient of a Dedekind domain is a principal ideal ring [50, p.278]. Let $r \in \mathcal{P}^k$ be an element that reduces to a generator of the ideal $\mathcal{P}^k/\mathcal{P}^{k+1}$ in $R/\mathcal{P}^{k+1}$. Then, every vector in $(\mathcal{P}^k)^n$ is congruent to a multiple of r modulo $\mathcal{P}^{k+1}$. In particular, $v \equiv rw \bmod \mathcal{P}^{k+1}$ for this $r \in \mathcal{P}^k$ and $w \in R^n$.

Note that $w \bmod \mathcal{P}$ is an element of $\mathcal{Q}_k$, by definition of $\mathcal{Q}_k$. Here, by Lemma 3.9, the characteristic polynomial ψ_k of $\mathbf{X}$ on $\mathcal{Q}_k$ satisfies $\psi_k^2 \mid \phi_{\mathbf{X}}$ over $\mathbb{F}_{\mathcal{P}}$. By the definition (2.7) of Γ we hence have $\psi_k \mid \Gamma$. Using that $\psi_k(\mathbf{X})w \equiv 0 \bmod \mathcal{P}$ by the Cayley–Hamilton theorem, it follows that $\Gamma(\mathbf{X})w \equiv 0 \bmod \mathcal{P}$. Thus, using that $v \equiv rw \bmod \mathcal{P}^{k+1}$ with $r \in \mathcal{P}^k$, we have $\Gamma(\mathbf{X})v \equiv 0 \bmod \mathcal{P}^{k+1}$, as desired. □

3.4. **Divisibility by $\mathcal{P}^2$ — Proof of Theorem 2.1.** We exploit the representation $\Delta_{\mathbf{X}} = \det(\phi'_{\mathbf{X}}(\mathbf{X}))$ and that the determinant of a matrix vanishes modulo $\mathcal{P}^k$ if and only if the matrix is sufficiently degenerate, in the following sense:

Lemma 3.11. *Consider a matrix $\mathbf{M} \in R^{n\times n}$ and an integer $k \geq 1$. Then,* $\det(\mathbf{M}) \equiv 0 \bmod \mathcal{P}^k$ *if and only if there exist vectors $v_1, \ldots, v_i \in R^n$ whose reductions modulo $\mathcal{P}$ are linearly independent over $\mathbb{F}_{\mathcal{P}}$ and integers $\lambda_1, \ldots, \lambda_i \geq 1$ such that*

$$\textstyle\sum_{j=1}^{i} \lambda_j \geq k \quad \text{and} \quad \mathbf{M}v_j \equiv 0 \bmod \mathcal{P}^{\lambda_j} \text{ for all } j \leq i. \tag{3.12}$$

Proof. Every nontrivial quotient of a Dedekind domain is a principal ideal ring [50, p.278]. In particular, matrices over $R/\mathcal{P}^k$ hence admit a Smith normal form [6, Theorem 15.24]. That is, there exist $d_1, \ldots, d_n \in R$ and invertible $\mathbf{V}, \mathbf{U} \in \mathrm{GL}_n(R/\mathcal{P}^k)$ such that $\mathbf{M} \bmod \mathcal{P}^k$ can be reduced to diagonal form:

$$\mathbf{M} \equiv \mathbf{UDV} \bmod \mathcal{P}^k \quad \text{with} \quad \mathbf{D} = \mathrm{diag}(d_1, \ldots, d_n). \tag{3.13}$$

Multiplication by $\mathrm{GL}_n(R/\mathcal{P}^k)$ preserves both the event where $\det(\mathbf{M}) \equiv 0 \bmod \mathcal{P}^k$ and the event where there exists a system satisfying (3.12). Consequently, it suffices to prove Lemma 3.11 when $\mathbf{M}$ is replaced by the diagonal matrix $\mathbf{D}$.

The case with diagonal matrices is elementary. Indeed, for every j, let $\lambda_j \geq 0$ be the power of $\mathcal{P}$ in the factorization of the ideal d_jR. Then, the arithmetic for inclusion and product of ideals in Proposition 3.3 yields that $\det(\mathbf{D}) \equiv 0 \bmod \mathcal{P}^k$ if and only if $\sum_{j=1}^{n} \lambda_j \geq k$. Let $e_1, \ldots, e_n \in R^n$ be the standard basis vectors. Taking $v_j = e_{r_j}$ with r_j the jth index with $\lambda_{r_j} \geq 1$ then proves that (3.12) follows from $\det(\mathbf{D}) \equiv 0 \bmod \mathcal{P}^k$. The other direction follows similarly. □

Lemma 3.12. *Assume that $\mathcal{P}^e \mid \mathcal{L}$. Consider some polynomial $f \in R[x]$, not necessarily monic, such that*

$$\ker_{\mathcal{P}}\big(f(\mathbf{X})\big) \subseteq \mathcal{Q}_e. \tag{3.14}$$

Then, it holds for every $v \in \mathcal{Q}_{e-1}$ with $f(\mathbf{X})v \equiv 0 \bmod \mathcal{P}$ that there exists $w \in R^n$ with $w \equiv v \bmod \mathcal{P}$ and $f(\mathbf{X})w \equiv 0 \bmod \mathcal{P}^2$.

Proof. Recall that nontrivial quotients of a Dedekind domain are principal ideal rings [50, p.278]. Let $\pi \in \mathcal{P} \setminus \mathcal{P}^2$. Then, π is a generator for the ideal $\mathcal{P}/\mathcal{P}^{2e}$ in $R/\mathcal{P}^{2e}$.

By definition of $\mathcal{Q}_{e-1}$, every vector in $\mathcal{Q}_{e-1} \subseteq \mathbb{F}_{\mathcal{P}}^n$ is the reduction of some $v \in R^n$ with $\pi^{e-1}v \in \mathrm{Im}_R(\mathcal{L}\mathbf{Q}) + (\mathcal{P}^e)^n$. In fact, using that $\mathcal{P}^e/\mathcal{P}^{2e}$ is generated by π^e, we may assume without loss of generality that $\pi^{e-1}v \in \mathrm{Im}_R(\mathcal{L}\mathbf{Q}) + (\mathcal{P}^{2e})^n$ by replacing v with $v - \pi\varepsilon$ for some suitable error term $\varepsilon \in R^n$.

Note that $f(\mathbf{X})v \equiv 0 \bmod \mathcal{P}$ implies that there exists $y \in R^n$ with

$$f(\mathbf{X})v \equiv \pi y \bmod \mathcal{P}^{2e}. \tag{3.15}$$

By Lemma 3.1, we have that $f(\mathbf{X})(\pi^{e-1}v) \in \mathrm{Im}_R(\mathcal{L}\mathbf{Q}) + (\mathcal{P}^{2e})^n$. Hence, $\pi^e y \in \mathrm{Im}_R(\mathcal{L}\mathbf{Q}) + (\mathcal{P}^{2e})^n$. In particular, Lemma 3.2 hence implies that

$$\pi^e(q^\top y) \equiv 0 \bmod \mathcal{P}^{2e} \quad \text{for every} \quad q \in \mathrm{Im}_R(\mathcal{L}\mathbf{Q}) + (\mathcal{P}^e)^n. \tag{3.16}$$

By definition of π and the ideal arithmetic in Proposition 3.3, it holds that $\pi^e r \in \mathcal{P}^{2e}$ for $r \in R$ if and only if $r \in \mathcal{P}^e$. Using this twice in (3.16) yields that $\tilde{q}^\top y \equiv 0 \bmod \mathcal{P}$ for every $\tilde{q} \in R^n$ with $\pi^{e-1}\tilde{q} \in \mathrm{Im}_R(\mathcal{L}\mathbf{Q}) + (\mathcal{P}^e)^n$. Hence, by definition of $\mathcal{Q}_{e-1}$,

$$\tilde{q}^\top y \equiv 0 \bmod \mathcal{P} \quad \text{for every} \quad \tilde{q} \in \mathcal{Q}_{e-1}. \tag{3.17}$$

In particular, using the assumption (3.14), we may conclude that

$$y \in \ker_{\mathcal{P}}(f(\mathbf{X}))^\perp. \tag{3.18}$$

Using that $\mathbf{X}$ is symmetric, we have that $\ker_{\mathcal{P}}(f(\mathbf{X}))^\perp = \mathrm{Im}_{\mathcal{P}}(f(\mathbf{X}))$. It hence follows from (3.18) that there exists $\gamma \in R^n$ with $y \equiv f(\mathbf{X})\gamma \bmod \mathcal{P}$. Let $w := v - \pi\gamma$ and note that we then have $f(\mathbf{X})w \equiv 0 \bmod \mathcal{P}^2$ due to (3.15). □

Corollary 3.13. *Assume that $\mathcal{P}^e \mid \mathcal{L}$. Then, $\mathcal{P}^{\dim_{\mathcal{P}}(\mathcal{Q}_k)+1} \mid \Delta_{\mathbf{X}}R$ for every $k \leq e-1$.*

Proof. Recall that ψ_k denotes the characteristic polynomial of the action of $\mathbf{X}$ on $\mathcal{Q}_k$. Recall from Lemma 3.9 that $\psi_k^2 \mid \phi_{\mathbf{X}}$. Consequently, $\psi_k \mid \phi'_{\mathbf{X}}$ and hence

$$\ker_{\mathcal{P}}\big(\psi_k(\mathbf{X})\big) \subseteq \ker_{\mathcal{P}}\big(\phi'_{\mathbf{X}}(\mathbf{X})\big). \tag{3.19}$$

Note that it follows from ψ_k being the characteristic polynomial for $\mathcal{Q}_k$ that $\ker_{\mathcal{P}}(\psi_k(\mathbf{X}))$ has dimension no less than $\dim_{\mathcal{P}}(\mathcal{Q}_k)$.

If the inclusion (3.19) is strict or if $\ker_{\mathcal{P}}(\psi_k(\mathbf{X}))$ has dimension strictly greater than $\dim_{\mathcal{P}}(\mathcal{Q}_k)$, then it follows that $\ker_{\mathcal{P}}(\phi'_{\mathbf{X}}(\mathbf{X}))$ has dimension greater than or equal to $\dim_{\mathcal{P}}(\mathcal{Q}_k) + 1$. Hence, by applying Lemma 3.11 to a basis of $\ker_{\mathcal{P}}(\phi'_{\mathbf{X}}(\mathbf{X}))$, we indeed have $\mathcal{P}^{\dim_{\mathcal{P}}(\mathcal{Q}_k)+1} \mid \Delta_{\mathbf{X}}R$ in this case.

Now suppose that $\ker_{\mathcal{P}}(\psi_k(\mathbf{X})) = \ker_{\mathcal{P}}(\phi'_{\mathbf{X}}(\mathbf{X}))$ and that this vector space has dimension $\dim_{\mathcal{P}}(\mathcal{Q}_k)$. Then, considering that $\mathcal{Q}_k \subseteq \ker_{\mathcal{P}}(\psi_k(\mathbf{X}))$, we have that $\ker_{\mathcal{P}}(\phi'_{\mathbf{X}}(\mathbf{X})) = \mathcal{Q}_k$. Using that $\mathcal{P}^{k+1} \mid \mathcal{L}$, Lemma 3.12 now allows lifting a basis of $\ker_{\mathcal{P}}(\phi'_{\mathbf{X}}(\mathbf{X}))$ to a system of independent solutions to $\phi'_{\mathbf{X}}(\mathbf{X})w \equiv 0 \bmod \mathcal{P}^2$. Hence, $\mathcal{P}^{2\dim_{\mathcal{P}}(\mathcal{Q}_k)} \mid \Delta_{\mathbf{X}}R$ by Lemma 3.11. In particular, $\mathcal{P}^{\dim_{\mathcal{P}}(\mathcal{Q}_k)+1} \mid \Delta_{\mathbf{X}}R$. □

Proof of Theorem 2.1. Immediate from Corollary 3.13 with $e = 1$. (Recall from Lemma 3.6 that $\mathcal{Q}_0 \neq 0$.) □

4. Matrices over number fields — Proofs for Section 2.3

We here adopt the setting of Section 2.3. Thus, K is a number field with ring of integers $\mathcal{O}_K$, and we consider some symmetric $\mathbf{X} \in \mathbb{Z}^{n\times n}$.

4.1. Sufficient conditions — Proof of Corollaries 2.11 and 2.12.

It suffices to establish Corollary 2.11, since Corollary 2.12 is a direct consequence.

Proof of Corollary 2.11. We trivially have $p^2 \mid \Delta_{\mathbf{X}}$ for every prime if $\Delta_{\mathbf{X}} = 0$, so suppose that $\Delta_{\mathbf{X}} \neq 0$. Let $\Delta_{\mathbf{X}} = \pm \prod_{i=1}^{m} p_i^{h_i}$ be the prime factorization.

Consider a nonzero prime ideal $\mathcal{P} \subseteq \mathcal{O}_K$ with $\mathcal{P} \mid \mathcal{L}$. Then, $\mathcal{P}^2 \mid \Delta_{\mathbf{X}} R$ by Theorem 2.1. The inclusion rules from Proposition 3.3 imply that $\mathcal{P} \mid p\mathcal{O}_K$ for a prime p if and only if $p \in \mathcal{P}$. Thus, there is a unique prime number with $\mathcal{P} \mid p\mathcal{O}_K$, this being the prime above which $\mathcal{P}$ lies.

Using that $\mathcal{P}^2 \mid \Delta_{\mathbf{X}}\mathcal{O}_K$ and the multiplication rules for ideal arithmetic in Proposition 3.3 now yield $\mathcal{P}^2 \mid (p_i\mathcal{O}_K)^{h_i}$ for some p_i in the prime factorization. Then, $\mathcal{P}^2 \mid p_i\mathcal{O}_K$ or $h_i \geq 2$. □

4.2. Orthogonal matrices with a given level — Proof of Proposition 2.13.

Lemma 4.1. *Assume that K is totally real. Then, every matrix $\mathbf{Q} \in \mathcal{O}_K^{n\times n}$ with $\mathbf{Q}^\top\mathbf{Q} = \mathbf{I}$ is a signed permutation.*

Proof. Recall that the *norm* of $k \in K$ is $\mathcal{N}_{K/\mathbb{Q}}(k) \coloneqq \prod_\sigma \sigma(k)$ where the product runs over all embeddings $\sigma : K \to \mathbb{C}$. It is classical that $\mathcal{N}_{K/\mathbb{Q}}(r) \in \mathbb{Z}$ for every algebraic integer $r \in \mathcal{O}_K$ [25, Chapter 2].

Every row $q = (q_1, \ldots, q_n)$ of $\mathbf{Q}$ satisfies $\sum_{i=1}^n q_i^2 = 1$. Hence, using that K is totally real, we have $0 \leq \sigma(q_i)^2 \leq 1$ for every embedding σ. Then, $\mathcal{N}_{K/\mathbb{Q}}(q_i) \in \mathbb{Z}$ implies that $|\sigma(q_i)| = 1$ if $q_i \neq 0$. A theorem by Kronecker [13] however states that the only algebraic integers $\alpha \in \mathcal{O}_K$ with $|\sigma(\alpha)| = 1$ for all embeddings $\sigma : K \to \mathbb{C}$ are roots of unity. Here, since $K \subseteq \mathbb{R}$, the only roots of unity are ± 1.

We conclude that every row q of $\mathbf{Q}$ has exactly one nonzero entry ± 1. The orthogonality of the rows now yields that $\mathbf{Q}$ is a signed permutation. □

Lemma 4.2. *Assume that K is totally real. Then, for every nonzero ideal $\mathcal{L} \subseteq \mathcal{O}_K$, there are finitely many matrices $\mathbf{Q} \in K^{n\times n}$ with $\mathbf{Q}^\top\mathbf{Q} = \mathbf{I}$ and $\ell\mathbf{Q} \in \mathcal{O}_K^{n\times n}$ for every $\ell \in \mathcal{L}$.*

Proof. Fix some arbitrary nonzero $\ell \in \mathcal{L}$ and let $\mathbf{G} = \ell\mathbf{Q}$. Then, every column $g = (g_1, \ldots, g_n)$ of $\mathbf{G}$ satisfies $\sum_{i=1}^n g_i^2 = \ell^2$. Hence, using that K is totally real, there exists some $C > 0$ depending only on ℓ with $|\sigma(g_i)| \leq C$ for every g_i.

Recall that the *Minkowski embedding* $j : K \to \mathbb{R}^r$ of K into Euclidean space sends every $k \in K$ to the vector $(\sigma(k))_\sigma$ [28, C1,§5]. Further, recall that this embedding sends $\mathcal{O}_K$ into a lattice [28, Proposition 5.2]. In particular, $j(\mathcal{O}_K)$ has a finite intersection with the compact box $\prod_\sigma [-C, C]$. This proves that there are only finitely many options for the entries of $\mathbf{G}$, and hence also for $\mathbf{Q} = \mathbf{G}/\ell$. □

Proof of Proposition 2.13. Combine Lemmas 4.1 and 4.2. □

5. Algorithmic search for cospectral mates

Throughout this section, we assume that $\mathbf{X} \in \mathbb{Z}^{n\times n}$ is a symmetric matrix over the (rational) integers and that K is a totally real algebraic number field. We think of $\mathbf{X}$ as being potentially high-dimensional while K is small and fixed.

5.1. **Algorithm outline.** The main steps of the method are as follows; see also Algorithm 1 for pseudocode. Details are given in the following Section 5.2.

Step 1. Determine potential ideal divisors: Compute the discriminant and all primes in the prime factorization $\Delta_{\mathbf{X}} = \pm p_1^{h_1} p_2^{h_2} \cdots p_m^{h_m}$ for which $h_i \geq 2$ or that ramify in K and have $h_i \geq 1$. Subsequently, determine all prime ideals $\mathcal{P} \subseteq \mathcal{O}_K$ lying above the p_i subject to the additional constraint that $\mathcal{P}^2 \mid p_i\mathcal{O}_K$ if $h_i = 1$. By Theorem 2.1, all prime ideals dividing the level $\mathcal{L} \subseteq \mathcal{O}_K$ of any orthogonal matrix $\mathbf{Q} \in K^{n\times n}$ with $\mathbf{Q}^\top\mathbf{X}\mathbf{Q} \in \mathcal{O}_K^{n\times n}$ are of this form.

Step 2. Upper-bound exponents: For every prime ideal $\mathcal{P}$ from the previous step, we determine some $E_\mathcal{P} \geq 0$ with $\mathcal{P}^e \nmid \mathcal{L}$ for every $e > E_\mathcal{P}$ as follows:

Step 2a. Compute square root Γ: The (approximate) square root polynomial $\Gamma \in \mathbb{F}_\mathcal{P}[x]$ from (2.7) can be computed without having to factorize $\phi_{\mathbf{X}}$ mod $\mathcal{P}$ into irreducible factors by using a square-free factorization instead.

Step 2b. Determine contractive and isotropic Krylov spaces: Let $\mathscr{W}_\mathcal{P}(e)$ be the set of all $w \in (\mathcal{O}_K/\mathcal{P}^e)^n$ with $w \not\equiv 0 \bmod \mathcal{P}$ that are representatives of a vector in $\mathcal{O}_K^n$ for which $\mathscr{K}_{\mathbf{X}}(w)$ is Γ-contractive and isotropic up to the level $\mathcal{P}^e$. (We do not track representatives in $\mathcal{O}_K/\mathcal{P}^{2e}$ and isotropy of level $\mathcal{P}^{2e}$ here for algorithmic reasons.) We give a method to lift vectors from $\mathscr{W}_\mathcal{P}(e)$ to vectors in $\mathscr{W}_\mathcal{P}(e+1)$ by solving linear equations. Initialization exploits that w mod $\mathcal{P}$ lies in $\ker_\mathcal{P}(\Gamma(\mathbf{X}))$, which is low-dimensional.

Step 2c. Additional isotropy checks: The previous step did not enforce the constraint of isotropy up to level $\mathcal{P}^{2e}$ from Theorem 2.8, only up to level $\mathcal{P}^e$. We enforce an additional linear condition and determine the subset $\mathbb{W}_\mathcal{P}(e) \subseteq \mathscr{W}_\mathcal{P}(e)$ of those vectors that admit a lift that is isotropic up to level $\mathcal{P}^{2e}$.

Theorem 2.8 now implies that $E_\mathcal{P} := \inf\{e \geq 0 : \mathbb{W}_\mathcal{P}(e+1) = \emptyset\}$ has the desired property that $\mathcal{P}^e \nmid \mathcal{L}$ for every $e > E_\mathcal{P}$.

Step 3. Construct orthogonal matrices: We determine all orthogonal matrices $\mathbf{Q} \in K^{n\times n}$ with $\mathbf{Q}^\top\mathbf{X}\mathbf{Q} \in \mathcal{O}_K^{n\times n}$ as follows:

Step 3a. Candidate residues for column vectors: Each column q of $\mathbf{Q}$ has level ideal $\mathcal{L}(q) := \{r \in \mathcal{O}_K : rq \in \mathcal{O}_K^n\}$ of the form $\mathcal{L}(q) = \prod_\mathcal{P} \mathcal{P}^{e_\mathcal{P}}$ for $e_\mathcal{P} \leq E_\mathcal{P}$. We iterate over the possible $e_\mathcal{P}$ and pick some element $\ell \in \mathcal{L}(q)$ such the exponent of $\mathcal{P}^{e_\mathcal{P}}$ is preserved in $\ell\mathcal{O}_K$. The sets $\mathbb{W}_\mathcal{P}(e_\mathcal{P})$ then allow us to determine a finite number of possible residue classes for ℓq mod $\ell\mathcal{O}_K$.

Step 3b. Lift candidate vectors: For every fixed residue class W there are only finitely many vectors $V \in \mathcal{O}_K^n$ with $V \equiv W$ mod $\prod_\mathcal{P} \mathcal{P}^{e_\mathcal{P}}$ and $V^\top V = \ell^2$. We construct all these vectors V by exploiting that the solutions typically require many coordinates of V to be zero. Considering V/ℓ then yields a finite set $\mathcal{Q}$ of possible column vectors for $\mathbf{Q}$.

Step 3c. Orthogonal matrix: We construct $\mathbf{Q}$ by picking a subset $\{q_1, \ldots, q_n\} \subseteq \mathcal{Q}$ subject to orthogonality $q_i^\top q_j = \mathbb{1}\{i = j\}$ and $\mathbf{Q}^\top\mathbf{X}\mathbf{Q} \in \mathcal{O}_K^{n\times n}$.

If it terminates, then the algorithm determines the complete set of orthogonal matrices $\mathbf{Q} \in K^{n\times n}$ with $\mathbf{Q}^\top \mathbf{X}\mathbf{Q} \in \mathcal{O}_K^{n\times n}$. Every signed permutation of the columns of $\mathbf{Q}$ again gives a valid orthogonal matrix, so we leave this implicit to reduce the size of the output by a factor $2^n n!$.

Regarding termination in finite time: it may be clear from the preceding description that the main potential problem lies in the computation of $E_{\mathcal{P}}$, as this number could potentially be infinite. All other tasks are finite problems. We prove in Section 5.3.1 that $E_{\mathcal{P}}$ is finite whenever $\Delta_X \neq 0$.

Algorithm 1

Input: Symmetric integer matrix $\mathbf{X} \in \mathbb{Z}^{n\times n}$, totally real algebraic number field K, integer $M \geq 1$ with $p^2 \nmid \Delta_X$ for all $p > M$.
Output: All orthogonal matrices $\mathbf{Q} \in K^{n\times n}$ with $\mathbf{Q}^\top \mathbf{X}\mathbf{Q} \in \mathcal{O}_K^{n\times n}$.

Determine all $\mathcal{P} \subseteq \mathcal{O}_K$ with $\mathcal{P}^2 \mid \Delta_X \mathcal{O}_K$.
for each $\mathcal{P}$ with $\mathcal{P}^2 \mid \Delta_X \mathcal{O}_K$ **do**
  Compute approximate square root Γ for $\phi_X \bmod \mathcal{P}$.
  $\mathscr{W}(1) \leftarrow \left\{w \in \ker_{\mathcal{P}}(\Gamma(\mathbf{X})) \setminus \{0\} : \forall j \leq n-1, w^\top \mathbf{X}^j w \equiv 0 \bmod \mathcal{P}\right\}$
  $\mathbb{W}(1) \leftarrow \left\{w \in \mathscr{W}(1) : \exists W \equiv w \bmod \mathcal{P}^2,\ \mathscr{K}_X(W) \text{ isotropic up to level } \mathcal{P}^2\right\}$
  $e \leftarrow 1$
  while $\mathbb{W}(e) \neq \emptyset$ **do**
    $e \leftarrow e+1$
    $\mathbb{W}(e) \leftarrow \left\{w \in (\mathcal{O}_K/\mathcal{P}^e)^n : \exists W \equiv w \bmod \mathcal{P}^e, \mathscr{K}_X(W) \text{ is } \Gamma\text{-contractive up to level } \mathcal{P}^e \text{ and isotropic up to level } \mathcal{P}^{2e}\right\}$
  end while
  $E_{\mathcal{P}} \leftarrow \inf\{e \geq 0 : \mathbb{W}_{\mathcal{P}}(e+1) = \emptyset\}$
end for
$\mathcal{Q} \leftarrow \emptyset$
for each exponent sequence $\{e_{\mathcal{P}} \leq E_{\mathcal{P}} : \mathcal{P}^2 \mid \Delta_X \mathcal{O}_K\}$ **do**
  Find $\ell \in \prod_{\mathcal{P}} \mathcal{P}^{e_{\mathcal{P}}}$ with $\mathcal{P}^{e_{\mathcal{P}}+1} \nmid \ell \mathcal{O}_K$ for all $\mathcal{P}$ with $\mathcal{P}^2 \mid \Delta_X \mathcal{O}_K$
  Determine vectors $V \in \mathcal{O}_K^n$ with $V \bmod \mathcal{P}^{e_{\mathcal{P}}}$ in $\mathbb{W}_{\mathcal{P}}(e_{\mathcal{P}})$ and $V^\top V = \ell^2$
  Add the vectors $V/\ell \in K^n$ to $\mathcal{Q}$
end for
Construct matrices $\mathbf{Q}$ with columns $q_1, \ldots, q_n \in \mathcal{Q}$ subject to $q_i^\top q_j = \mathbb{1}\{i = j\}$
Check if $\mathbf{Q}^\top \mathbf{X}\mathbf{Q} \in \mathcal{O}_K^{n\times n}$

5.2. **Detailed description.**

5.2.1. *Details for Step 1 — Prime ideal divisors.* The primes $p \in \mathbb{Z}_{\geq 2}$ that ramify in K are the prime divisors of the discriminant of the number field $\mathrm{disc}(\mathcal{O}_K)$ [25, C3, Thm.24 & C4, Thm.34]. Computing the number field discriminant is a classical task, although computing it and determining the prime divisors may be prohibitively expensive for large number fields. This is one of the many times when Assumption 2.16 is used.

Considering the prime ideals above prime divisors $p \mid \Delta_X$ that are ramified or have $p^2 \mid \Delta_X$ then allows us to find all $\mathcal{P} \subseteq \mathcal{O}_K$ with $\mathcal{P}^2 \mid \Delta_X \mathcal{O}_K$.

5.2.2. *Details for Step 2a — Computing the square root.* If no prime ideals $\mathcal{P} \subseteq \mathcal{O}_K$ with $\mathcal{P}^2 \mid \Delta_{\mathbf{X}}\mathcal{O}_K$ exist, then Corollary 2.12 is applicable and we may conclude that the only orthogonal matrices $\mathbf{Q} \in K^{n\times n}$ with $\mathbf{Q}^\top\mathbf{X}\mathbf{Q} \in \mathcal{O}_K^{n\times n}$ are signed permutations. Now assume that we are given some $\mathcal{P}$ with $\mathcal{P}^2 \mid \Delta_{\mathbf{X}}\mathcal{O}_K$.

Recall that the polynomial $\Gamma \in \mathbb{F}_{\mathcal{P}}[x]$ was defined in (2.7) using the irreducible factorization of $\phi_{\mathbf{X}}$ mod $\mathcal{P}$. For computational purposes, it is more efficient to consider the *square–free factorization* [27, 49]:

$$\phi_{\mathbf{X}}(x) \equiv \textstyle\prod_i g_i(x)^i \bmod \mathcal{P}, \tag{5.1}$$

where $g_1, g_2, \ldots \in \mathbb{F}_{\mathcal{P}}[x]$ are coprime monic polynomials. Then,

$$\Gamma(x) = \textstyle\prod_i g_i(x)^{\lfloor i/2 \rfloor}. \tag{5.2}$$

By Lemma 3.5 and the assumption that $\mathcal{P}^2 \mid \Delta_{\mathbf{X}}\mathcal{O}_K$, we know that $\deg(\Gamma) \geq 1$. (This application of Lemma 3.5 uses that $\mathbb{F}_{\mathcal{P}}$ is a finite field and hence perfect.)

Note that the embedding $\mathbb{Z} \to \mathcal{O}_K$ induces an inclusion of finite fields $\mathbb{Z}/p\mathbb{Z} \to \mathbb{F}_{\mathcal{P}}$. Using that an extension of finite fields is separable, it hence suffices to compute Γ over $\mathbb{Z}/p\mathbb{Z}$. The polynomial over $\mathbb{F}_{\mathcal{P}}$ then follows using the field inclusion.

5.2.3. *Details for Step 2b — Krylov spaces.* Recall that $\mathscr{W}_{\mathcal{P}}(e) \subseteq (\mathcal{O}_K/\mathcal{P}^e)^n$ consists of the vectors that are representative of some $w \in \mathcal{O}_K^n$ with $w \not\equiv 0$ mod $\mathcal{P}$ and such that $\mathscr{K}_{\mathbf{X}}(w)$ is a Γ-contractive and isotropic subspace up to level $\mathcal{P}^e$.

We have $w \in \mathscr{W}_{\mathcal{P}}(1)$ if and only if $\Gamma(\mathbf{X})w \equiv 0$ mod $\mathcal{P}$ and $w^\top\mathbf{X}^j w \equiv 0$ mod $\mathcal{P}$ for every $j \leq n-1$. A linear-algebraic computation over $\mathbb{Z}/p\mathbb{Z}$ yields a basis $k_1, \ldots, k_d \in \ker_{\mathcal{P}}(\Gamma(\mathbf{X}))$. Let $\mathbf{K} = [k_1, \ldots, k_d]$ be the $n \times d$ matrix with these columns. Then, $\Gamma(\mathbf{X})w \equiv 0$ mod $\mathcal{P}$ if and only if $w \equiv \mathbf{K}v$ mod $\mathcal{P}$ for some $v \in \mathbb{F}_{\mathcal{P}}^d$, and $w^\top\mathbf{X}^j w \equiv 0$ mod $\mathcal{P}$ for all $j \leq n-1$ if and only if

$$v^\top(\mathbf{K}^\top\mathbf{X}^j\mathbf{K})v = 0, \quad \forall j \leq \deg(\Gamma) - 1. \tag{5.3}$$

We here used that $\mathbf{K}v \in \ker_{\mathcal{P}}(\Gamma(\mathbf{X}))$ to restrict the powers to $j \leq \deg(\Gamma) - 1$.

Note that (5.3) is an intersection of $\deg(\Gamma)$ quadrics. The general problem of solving an intersection of multivariate quadrics is known as the *MQ problem* in cryptography and is expensive in large problems [7, §2.3.1]. We are however concerned with cases where $\deg(\Gamma)$ is small; recall Assumption 2.18. Thus, solving (5.3) enables us to determine the following set:

$$\mathscr{W}_{\mathcal{P}}(1) = \{w \in \ker_{\mathcal{P}}(\Gamma(\mathbf{X})) \setminus \{0\} : \forall j \leq n-1,\ w^\top\mathbf{X}^j w = 0\}. \tag{5.4}$$

Remark 5.1. If $\mathcal{P}$ lies above $p = 2$, then $\mathbb{F}_{\mathcal{P}}$ has characteristic 2 and hence

$$v^\top(\mathbf{K}^\top\mathbf{X}^j\mathbf{K})v \equiv \textstyle\sum_{i=1}^d D_i^{(j)} v_i^2 \equiv \left(\sum_{i=1}^d D_i^{(j)} v_i\right)^2 \bmod \mathcal{P}, \tag{5.5}$$

where $D_i^{(j)}$ is the i-th diagonal entry of $\mathbf{K}^\top\mathbf{X}^j\mathbf{K}$ and we used that $D_i^{(j)} = (D_i^{(j)})^2$ since this is an element of the subfield $\mathbb{Z}/2\mathbb{Z} \subseteq \mathbb{F}_{\mathcal{P}}$. Thus, the quadratic constraints (5.3) could be replaced linear ones in this case.

Now suppose that we are given some $w \in \mathscr{W}_{\mathcal{P}}(e)$ for $e \geq 1$. Our task is to find the lifts to $\mathscr{W}_{\mathcal{P}}(e+1)$, or to show that no such lifts exist.

Fix some arbitrary $\tilde{w} \in (\mathcal{O}_K/\mathcal{P}^{e+1})^n$ with $\tilde{w} \equiv w$ mod $\mathcal{P}^e$, and consider some $\pi \in \mathcal{P}$ with $\pi \notin \mathcal{P}^2$. Then, $\mathcal{O}_K/\mathcal{P}^{e+1}$ is a principal ideal ring with ideals given by the

reductions of $\{\mathcal{P}^j : j \le e\}$ and $\mathcal{P}/\mathcal{P}^{e+1}$ is generated by $\pi \bmod \mathcal{P}^{e+1}$. Hence, every $\omega \in (\mathcal{O}_K/\mathcal{P}^{e+1})^n$ with $\omega \equiv w \bmod \mathcal{P}^e$ can be uniquely represented as

$$\omega \equiv \tilde{w} + \pi^e \delta \bmod \mathcal{P}^{e+1}, \tag{5.6}$$

for $\delta \in \mathbb{F}_{\mathcal{P}}^n$. We next determine when the Krylov space is Γ-contractive and isotropic.

Let $Q_e(x) \in (\mathcal{O}_K/\mathcal{P}^e)[x]$ be a polynomial of minimal degree with

$$Q_e(\mathbf{X})w \equiv 0 \bmod \mathcal{P}^e. \tag{5.7}$$

Such a polynomial can be computed by linear-algebraic computations expressing that $\mathbf{X}^d w$ is in the span of $\{\mathbf{X}^j w : j < d\}$ over $\mathcal{O}_K/\mathcal{P}^e$. Let $\tilde{Q}_e \in \mathcal{O}_K[x]$ be an arbitrary monic lift of Q_e and consider the unique vector $r \in \mathbb{F}_{\mathcal{P}}^n$ with

$$\tilde{Q}_e(\mathbf{X})\tilde{w} \equiv \pi^e r \bmod \mathcal{P}^{e+1}. \tag{5.8}$$

The following Lemmas 5.2 and 5.3 turn the constraints of Γ-contractivity and isotropy into a system of linear equations.

Lemma 5.2. *With notation and assumptions as above, $\omega = \tilde{w} + \pi^e\delta$ satisfies that $\mathcal{K}_{\mathbf{X}}(\omega)$ is Γ-contractive up to level $\mathcal{P}^{e+1}$ if and only if*

$$\Gamma(\mathbf{X})Q_e(\mathbf{X})\delta \equiv -\Gamma(\mathbf{X})r \bmod \mathcal{P}. \tag{5.9}$$

Lemma 5.3. *Let $c_j \in \mathbb{F}_{\mathcal{P}}$ be the unique scalars with $\tilde{w}^\top \mathbf{X}^j \tilde{w} \equiv \pi^e c_j$ for every $j \le n-1$. Then, $\omega = \tilde{w} + \pi^e\delta$ satisfies that $\mathcal{K}_{\mathbf{X}}(\omega)$ is isotropic up to level $\mathcal{P}^{e+1}$ if and only if δ satisfies the following linear equations over $\mathbb{F}_{\mathcal{P}}$:*

$$2w^\top \mathbf{X}^j \delta \equiv -c_j \bmod \mathcal{P} \quad \text{for} \quad j = 0, 1, \ldots, \deg(Q_e) + \deg(Q_1) - 1. \tag{5.10}$$

The proofs of Lemmas 5.2 and 5.3 are given in Sections 5.3.2 and 5.3.3, respectively. By solving the linear equations (5.9) and (5.10), we can determine all vectors in $\mathscr{W}_{\mathcal{P}}(e+1)$ that are lifts of some given $w \in \mathscr{W}_{\mathcal{P}}(e)$, or conclude that no such lifts exists.

Remark 5.4. Note that $w \in \mathscr{W}_{\mathcal{P}}(e)$ if and only if $rw \in \mathscr{W}_{\mathcal{P}}(e)$ for every $r \in \mathcal{O}_K/\mathcal{P}^e$ with $r \not\equiv 0 \bmod \mathcal{P}$. This means that r reduces to a unit. It hence suffices to determine a single representative in $(\mathcal{O}_K/\mathcal{P}^e)^n$ up to scalar multiplication. Our implementation exploits this to reduce repeated computations by tracking only the vector with $w_{i_*} \equiv 1 \bmod \mathcal{P}^e$ for the smallest index $i_* \le n$ with $w_{i_*} \not\equiv 0 \bmod \mathcal{P}$. At the end of Step 2, we finally consider all scalar multiples of the found vectors.

Remark 5.5. If two prime ideals $\mathcal{P}_1, \mathcal{P}_2 \subseteq \mathcal{O}_K$ are in the same orbit of the Galois group, i.e., there exists $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ with $\sigma(\mathcal{P}_1) = \mathcal{P}_2$, then naturally $\sigma(\mathscr{W}_{\mathcal{P}_1}(e)) = \mathscr{W}_{\mathcal{P}_2}(e)$. This could be used to reduce redundant computations, as it implies that it suffices to do the computations only once for each orbit. In particular, if K is the splitting field of a polynomial (i.e., a Galois extension), then there is only a single orbit [28, C1,§9].

5.2.4. *Details for Step 2c — Additional isotropy checks.* Recall that Theorem 2.9 involves isotropy up to level $\mathcal{P}^{2e}$, not only up to level $\mathcal{P}^e$. The reason why we nonetheless only tracked representatives over $\mathcal{O}_K/\mathcal{P}^e$ is due to the combinatorial explosion in the number vectors over $\mathcal{O}_K/\mathcal{P}^{2e}$ relative to $\mathcal{O}_K/\mathcal{P}^e$ when n is large.

The following variant on Lemma 5.3 allows us to filter out the subset $\mathbb{W}_{\mathcal{P}}(e) \subseteq \mathscr{W}_{\mathcal{P}}(e)$ consisting of those vectors that admit a lift that is isotropic up to level $\mathcal{P}^{2e}$. Crucially, we avoid computing these lifts explicitly. Recall that $\pi \in \mathcal{P} \setminus \mathcal{P}^2$.

Lemma 5.6. *Consider some $w \in \mathscr{W}_{\mathcal{P}}(e)$. Pick some lift $W \in (\mathcal{O}_K/\mathcal{P}^{2e})^n$ with $W \equiv w \bmod \mathcal{P}^e$ and let $C_j \in \mathcal{O}_K/\mathcal{P}^e$ be the scalars with $W^\top \mathbf{X}^j W \equiv \pi^e C_j \bmod \mathcal{P}^{2e}$. Then, there exists $\Omega \in \mathcal{O}_K^n$ with $\Omega \equiv w \bmod \mathcal{P}^e$ and $\mathscr{K}_{\mathbf{X}}(\Omega)$ isotropic up to level $\mathcal{P}^{2e}$ if and only if the following system admits a solution $\delta \in (\mathcal{O}_K/\mathcal{P}^e)^n$:*

$$2w^\top \mathbf{X}^j \delta \equiv -C_j \bmod \mathcal{P}^e \quad \text{for} \quad j = 0, 1, \ldots, 2\deg(Q_e) - 1. \tag{5.11}$$

5.2.5. *Step 3a. — Candidate residues for column vectors.* Recall we associate a level ideal $\mathcal{L}(q) = \{r \in \mathcal{O}_K : rq \in \mathcal{O}_K^n\}$ to every column vector $q \in K^n$ of the potential orthogonal matrix $\mathbf{Q}$. This ideal has the following form:

$$\mathcal{L}(q) = \textstyle\prod_{\mathcal{P}} \mathcal{P}^{e_{\mathcal{P}}} \text{ for certain } e_{\mathcal{P}} \le E_{\mathcal{P}}. \tag{5.12}$$

Here, $E_{\mathcal{P}} = \inf\{e \ge 0 : \mathbb{W}_{\mathcal{P}}(e+1) = \emptyset\}$. We iterate over the possible exponents $e_{\mathcal{P}}$, and our goal is to determine the corresponding possibilities for q.

If all exponents are zero, then q must be a vector with a single nonzero entry ± 1; recall the proof of Lemma 4.1. We next consider the nontrivial case with $e_{\mathcal{P}} \ge 1$ for some $e_{\mathcal{P}}$. Then, by the Chinese remainder theorem over $\mathcal{O}_K/\prod_{\mathcal{P}} \mathcal{P}^{e_{\mathcal{P}}+1}$, there exists some $\ell \in \mathcal{L}(q)$ with

$$\ell \in \mathcal{P}^{e_{\mathcal{P}}} \setminus \mathcal{P}^{e_{\mathcal{P}}+1} \text{ for all } \mathcal{P} \text{ with } e_{\mathcal{P}} \ge 1. \tag{5.13}$$

This element is not unique and the efficiency of subsequent steps will depend on the choice. Our implementation picks ℓ such that it has minimal absolute norm [28, p.8] subject to (5.13). In any case, $\ell \in \mathcal{L}(q)$ implies that its ideal can be factorized as

$$\ell \mathcal{O}_K = \mathcal{L}(q)\mathcal{J}. \tag{5.14}$$

The ideal $\mathcal{J} \subseteq \mathcal{O}_K$ will be nontrivial if $\mathcal{L}(q)$ was not principal.

It follows from (5.13) and the ideal arithmetic of Proposition 3.3 that $\ell q \not\equiv 0 \bmod \mathcal{P}$ whenever $e_{\mathcal{P}} \ge 1$. It can here be deduced from Theorem 2.9 that $\ell q \bmod \mathcal{P}^{e_{\mathcal{P}}}$ lies in $\mathbb{W}_{\mathcal{P}}(e_{\mathcal{P}})$. Further, the condition that q has level ideal $\mathcal{L}(q)$ implies that $\ell q \equiv 0 \bmod \mathcal{J}$. We can hence determine a set of vectors $W \in (\mathcal{O}_K/\ell\mathcal{O}_K)^n$ that could plausibly satisfy $W \equiv \ell q \bmod \ell\mathcal{O}_K$ by using the Chinese remainder theorem:

$$\begin{cases} W \equiv w_{\mathcal{P}} \bmod \mathcal{P}^{e_{\mathcal{P}}} \text{ with } w_{\mathcal{P}} \in \mathbb{W}_{\mathcal{P}}(e_{\mathcal{P}}) \text{ whenever } e_{\mathcal{P}} \ge 1, \\ W \equiv 0 \bmod \mathcal{J}. \end{cases} \tag{5.15}$$

The set of vectors that arises from this system should typically be small relative to $(\mathcal{O}_K/\ell\mathcal{O}_K)^n$ and $(\mathcal{O}_K/\mathcal{L}(q))^n$, which are also finite but grow exponentially in n.

5.2.6. *Details for Step 3b — Lift candidate vectors.* If q is a column of an orthogonal matrix, then $(\ell q)^\top(\ell q) = \ell^2(q^\top q) = \ell^2$. Given some $W \in (\mathcal{O}_K/\ell\mathcal{O}_K)^n$ arising from (5.15) we hence wish to determine all vectors $V \in \mathcal{O}_K^n$ with

$$V \equiv W \bmod \ell\mathcal{O}_K \text{ and } V^T V = \ell^2. \tag{5.16}$$

We start by considering a constraint that often quickly shows that W is such that no solutions to (5.16) exist, or restricts the search space otherwise.

Let $\sigma_1, \ldots, \sigma_r : K \to \mathbb{R}$ be the field embeddings of our totally real number field. Let us define a *ℓ-twisted trace* $T_\ell : K \to \mathbb{R}$ and norm $\|\cdot\|_\ell$ by

$$T_\ell(x) := \textstyle\sum_m \sigma_m(x/\ell^2) \quad \text{and} \quad \|x\|_\ell := \sqrt{T_\ell(x^2)}. \tag{5.17}$$

For every $w \in \mathcal{O}_K$ representing a residue class in $\mathcal{O}_K/\ell\mathcal{O}_K$, we then compute

$$\tau_\ell(w) := \min_{x \in \ell\mathcal{O}_K} T_\ell\big((w-x)^2\big) = \min_{y \in \mathcal{O}_K} T_1\big((w/\ell - y)^2\big), \tag{5.18}$$

and we store a value $x(w) \in \ell\mathcal{O}_K$ achieving the minimum. This is a *closest vector problem* for the lattice $\mathcal{O}_K$ and its tractability uses Assumption 2.16.

It follows from $V^\top V = \ell^2$ and linearity that $\sum_i T_\ell(v_i^2) = r$. Thus, the existence of a solution to (5.16) necessitates that

$$\sum_{i=1}^{n} \tau_\ell(w_i) \le r. \tag{5.19}$$

If (5.19) is violated, then (5.16) does not admit solutions. Now suppose that (5.19) holds. Heuristically, for large n, this should imply that W has only a few nonzero coordinates. The coordinates that are 0 mod $\ell\mathcal{O}_K$ yield algebraic integer entries in V/ℓ and could hence only be 0 or ± 1 by V/ℓ being a unit vector; recall the proof of Lemma 4.1. In fact, these lifts have to be zero due to W also having nonzero coordinates.

It hence remains to lift the nonzero coordinates, which we do by picking values one-by-one. Suppose that the v_j with $j < i$ have been assigned a value. Then, we restrict the search space for v_i using that completion to a full vector requires satisfaction of the following *lookahead constraint*:

$$T_\ell\big(v_i^2\big) \le r - \textstyle\sum_{j<i} T_\ell\big(v_j^2\big) - \sum_{j>i} \tau_\ell(w_j). \tag{5.20}$$

In particular, if we write $v_i = w_i - x(w_i) + \delta_i$ with $x(w_i)$ the minimizer for (5.18) and $\delta_i \in \ell\mathcal{O}_K$, then the triangle inequality and (5.20) yield that

$$\|\delta_i\|_\ell \le \sqrt{\tau_\ell(w_i)} + \sqrt{r - \sum_{j<i} T_\ell\big(v_j^2\big) - \sum_{j>i} \tau_\ell(w_j)}. \tag{5.21}$$

We compute all δ_i satisfying (5.21) and additionally filter the choices using that v_i must satisfy the following *spent budget constraints*:

$$\sigma_m\big(v_i\big)^2 \le \sigma_m\big(\ell^2\big) - \textstyle\sum_{j<i} \sigma_m\big(v_j^2\big) \text{ for every } m \le r. \tag{5.22}$$

Once a full vector is composed, we finally check if equality holds in $V^\top V = \ell^2$.

5.2.7. *Details for Step 3c — Orthogonal matrix.* Considering the vectors V/ℓ with V satisfying (5.16), and the standard basis vectors $\pm e_i$ corresponding to $\mathcal{L}(q) = \mathcal{O}_K$, yields a finite set $\mathcal{Q} \subseteq K^n$ of potential column vectors.

It remains to determine orthogonal subsets of size n. We do this by exploiting that an orthogonal set of vectors $\{q_i : i = 1, \dots, m\}$ can be completed to an orthogonal basis by adding standard basis vectors if and only if the number of active coordinates is exactly m. Here, $j \in \{1, \dots, n\}$ is *active* if there exists some q_i whose jth entry is nonzero. Recursively selecting such subsets based on the vectors V/ℓ turns out to run sufficiently quickly in practice.

Given an orthogonal set of vectors $\{q_i : i = 1, \dots, n\}$ we then finally check if the associated orthogonal matrix $\mathbf{Q} \in K^{n\times n}$ indeed satisfies $\mathbf{Q}^\top \mathbf{X} \mathbf{Q} \in \mathcal{O}_K^{n\times n}$. The algorithm returns all orthogonal matrices over K with the latter property, up to signed permutation of the columns.

5.3. **Proof of algorithmic properties.**

5.3.1. *Termination in finite time — Proof of Theorem 2.19.* Let $q_k \in \mathbb{Z}[w_1, \dots, w_n]$ be the polynomial defined by the quadratic form associated to $\mathbf{X}^k$:

$$q_k(w_1, \dots, w_n) = w^\top \mathbf{X}^k w \quad \text{with} \quad w = (w_1, \dots, w_n)^\top. \tag{5.23}$$

Lemma 5.7. *Assume that $\Delta_{\mathbf{X}} \neq 0$. Then, the only $w \in \mathbb{C}^n$ satisfying the equations $q_k(w) = 0$ for all $k \leq n-1$ is the trivial solution $w = 0$.*

Proof. Let $\lambda_1, \dots, \lambda_n \in \mathbb{R}$ be the eigenvalues of the symmetric matrix $\mathbf{X} \in \mathbb{Z}^{n \times n}$ and consider an associated orthonormal basis of eigenvectors $U_1, \dots, U_n \in \mathbb{R}^n$, so that $\mathbf{X} = \sum_i \lambda_i U_i U_i^\top$. Write $w = \sum_{i=1}^n c_i U_i$ for arbitrary coefficients $c_i \in \mathbb{C}$. Then,

$$q_k(w) = 0 \quad \Longleftrightarrow \quad \sum_{i=1}^n c_i^2 \lambda_i^k = 0. \tag{5.24}$$

The system of equations $\{\sum_i x_i \lambda_i^k = 0 : k \leq n-1\}$ is specified by a Vandermonde matrix with determinant $\prod_{i<j}(\lambda_j - \lambda_i) = \sqrt{|\Delta_{\mathbf{X}}|}$. Hence, using that $\Delta_{\mathbf{X}} \neq 0$, the system only has the trivial solution. Thus, $c_i^2 = 0$ for all i and hence $w = 0$. □

Lemma 5.8. *Assume that $\Delta_{\mathbf{X}} \neq 0$. Then, for every $i \leq n$ there exist $h_i \geq 0$ and $n_i \in \mathbb{Z} \setminus \{0\}$ such that the monomial $n_i w_i^{h_i}$ can be expressed as a $\mathbb{Z}[w_1, \dots, w_n]$-linear combination of the q_k. That is,*

$$n_i w_i^{h_i} = \textstyle\sum_{k=0}^{n-1} s_k^{(i)}(w_1, \dots, w_n) q_k(w_1, \dots, w_n), \tag{5.25}$$

for certain polynomials $s_0^{(i)}, \dots, s_{n-1}^{(i)} \in \mathbb{Z}[w_1, \dots, w_n]$.

Proof. Using Lemma 5.7 and Hilbert's Nullstellensatz [18, p.4] yields that w_i is an element of the radical of the ideal generated by the polynomials q_k over $\mathbb{C}$. That is, there exists $h_i \geq 0$ and polynomials $\tilde{s}_k^{(i)} \in \mathbb{C}[w_1, \dots, w_n]$ with

$$w_i^{h_i} = \textstyle\sum_{k=0}^{n-1} \tilde{s}_k^{(i)}(w_1, \dots, w_n) q_k(w_1, \dots, w_n). \tag{5.26}$$

Moreover, it follows from the fact that $w_i^{h_i}$ and $q_k(w_1, \dots, w_n)$ are polynomials over $\mathbb{Q}$ that the $\tilde{s}_k^{(i)}$ can also be taken to have coefficients over $\mathbb{Q}$. Indeed, one can view (5.26) as a system of linear equations for the coefficients of the $\tilde{s}_k^{(i)}$, and use that a system of linear equations has a solution over a field extension if and only if it has one in the original field. Clearing denominators now yields (5.25). □

The following Lemmas 5.9 and 5.10 do not require K to be totally real.

Lemma 5.9. *Assume that $\Delta_{\mathbf{X}} \neq 0$ and consider a nonzero prime ideal $\mathcal{P} \subseteq \mathcal{O}_K$. Then, there exists some $e \geq 0$ such that every $w \in \mathcal{O}_K^n$ with $w^\top \mathbf{X}^k w \equiv 0 \bmod \mathcal{P}^e$ for every $k \leq n-1$ satisfies that $w \equiv 0 \bmod \mathcal{P}$.*

Proof. Let $e \geq 0$ be sufficiently large so that the integers n_i in (5.25) satisfy that $n_i \notin \mathcal{P}^e$ for every i. Note that (5.25) implies that $n_i w_i^{h_i} \equiv 0 \bmod \mathcal{P}^e$ whenever $w^\top \mathbf{X}^k w \equiv 0 \bmod \mathcal{P}^e$ for every $k \leq n-1$. By definition of e and the ideal arithmetic Proposition 3.3, it is only possible to have $n_i w_i^{h_i} \in \mathcal{P}^e$ if $w_i \in \mathcal{P}$. □

Lemma 5.10. *Assume that $\Delta_{\mathbf{X}} \neq 0$ and consider a nonzero prime ideal $\mathcal{P} \subseteq \mathcal{O}_K$. Then, there exists $e \geq 0$ depending on $\mathbf{X}$ such that there does not exist any $w \in \mathcal{O}_K^n$ with $w \not\equiv 0 \bmod \mathcal{P}$ for which $\mathscr{K}_{\mathbf{X}}(w)$ is isotropic up to level $\mathcal{P}^e$.*

Proof. This is immediate from Lemma 5.9 since $\mathscr{K}_{\mathbf{X}}(w)$ being isotropic up to level $\mathcal{P}^e$ necessitates that $w^\top \mathbf{X}^k w \equiv 0 \bmod \mathcal{P}^e$. □

Corollary 5.11. *Assume that $\Delta_{\mathbf{X}} \neq 0$. Then, Algorithm 1 terminates in finite time.*

Proof. The only potential problem was whether the number $E_{\mathcal{P}} = \inf\{e \geq 0 : \mathbb{W}_{\mathcal{P}}(e+1) = \emptyset\}$ is finite. Lemma 5.10 implies that this is indeed the case since $\mathscr{W}_{\mathcal{P}}(e) = \emptyset$ implies that $\mathbb{W}_{\mathcal{P}}(e) = \emptyset$. □

Remark 5.12. Note that the Γ-contractivity was not used to prove termination in finite time. Its relevance is only for the efficiency of the algorithm.

5.3.2. *Linear rephrasing for contractivity of lifts — Proof of Lemma 5.2.* Recall from (5.7) that $\tilde{Q}_e \in \mathcal{O}_K[x]$ is a monic polynomial of minimal degree with $\tilde{Q}_e(\mathbf{X})w \equiv 0 \bmod \mathcal{P}^e$. Further, recall that we fix some $\pi \in \mathcal{P}$ with $\pi \notin \mathcal{P}^2$.

Lemma 5.13. *Fix some $w \in \mathcal{O}_K^n$ and $e \geq 1$. Then, for every $q \in \mathcal{O}_K[x]$ with $q(\mathbf{X})w \equiv 0 \bmod \mathcal{P}^e$ there exist polynomials $d(x), r(x) \in \mathcal{O}_K[x]$ with*

$$q(x) \equiv d(x)\tilde{Q}_e(x) + \pi r(x) \bmod \mathcal{P}^{e+1}. \tag{5.27}$$

Proof. Subtracting a multiple of $\tilde{Q}_e$ from q ensures that $\deg(q) < \deg(\tilde{Q}_e)$. Then, the leading coefficient must be a multiple of π in $\mathcal{O}_K/\mathcal{P}^{e+1}$, as we could otherwise invert it to get a monic polynomial, contradicting the degree minimality of $\tilde{Q}_e$.

In this case, subtracting multiples of πQ_1 ensures that $q(x) = \pi\gamma(x)Q_1(x)+\rho(x)$ for some $\gamma(x), \rho(x) \in \mathcal{O}_K[x]$ with $\deg(\rho) < \deg(Q_1)$. However, we then have $\rho(\mathbf{X})w \equiv 0 \bmod \mathcal{P}$ so that the degree minimality of Q_1 implies that $\rho \equiv 0 \bmod \mathcal{P}$. Then, $\rho = \pi\rho' \bmod \mathcal{P}^{e+1}$. The claim then follows with $r(x) = \gamma(x)Q_1(x) + \rho'(x)$. □

Lemma 5.14. *Fix some $w \in \mathcal{O}_K^n$ for which $\mathscr{K}_{\mathbf{X}}(w)$ is Γ-contractive up to level $\mathcal{P}^e$ for $e \geq 1$. Consider some $\tilde{w} \in \mathcal{O}_K^n$ with $\tilde{w} \equiv w \bmod \mathcal{P}^e$. Then, $\mathscr{K}_{\mathbf{X}}(\tilde{w})$ is Γ-contractive up to level $\mathcal{P}^{e+1}$ if and only if $\Gamma(\mathbf{X})\tilde{Q}_e(\mathbf{X})\tilde{w} \equiv 0 \bmod \mathcal{P}^{e+1}$.*

Proof. By Definition 2.7 and the Cayley–Hamilton theorem, $\mathscr{K}_{\mathbf{X}}(\tilde{w})$ consists exactly of the vectors of the form $q(\mathbf{X})\tilde{w}$ for $q \in \mathcal{O}_K[x]$. In particular, $\tilde{Q}_e(\mathbf{X})\tilde{w} \in \mathscr{K}_{\mathbf{X}}(\tilde{w}) \cap \mathcal{P}^e$ by definition of $\tilde{Q}_e$. Thus, by Definition 2.5, the Krylov space being contractive up to level $\mathcal{P}^{e+1}$ certainly implies that $\Gamma(\mathbf{X})\tilde{Q}_e(\mathbf{X})\tilde{w} \equiv 0 \bmod \mathcal{P}^{e+1}$.

It remains to show that $\Gamma(\mathbf{X})\tilde{Q}_e(\mathbf{X})\tilde{w} \equiv 0 \bmod \mathcal{P}^{e+1}$ implies that $\Gamma(\mathbf{X})q(\mathbf{X})\tilde{w} \equiv 0 \bmod \mathcal{P}^{e+1}$ whenever $q(x) \in \mathcal{O}_K[x]$ is a polynomial with $q(\mathbf{X})\tilde{w} \equiv 0 \bmod \mathcal{P}^e$. By Lemma 5.13 we can then write $q(x) \equiv d(x)\tilde{Q}_e(x) + \pi r(x) \bmod \mathcal{P}^{e+1}$. It then follows from $q(\mathbf{X})\tilde{w} \equiv 0 \bmod \mathcal{P}^e$ that $r(\mathbf{X})\tilde{w} \equiv 0 \bmod \mathcal{P}^{e-1}$. That $\mathscr{K}_{\mathbf{X}}(w)$ is Γ-contractive up to level $\mathcal{P}^e$ then yields that $\Gamma(\mathbf{X})r(\mathbf{X})\tilde{w} \equiv 0 \bmod \mathcal{P}^e$. Hence,

$$\Gamma(\mathbf{X})q(\mathbf{X})\tilde{w} \equiv d(\mathbf{X})\Gamma(\mathbf{X})\tilde{Q}_e(\mathbf{X})\tilde{w} + \pi\Gamma(\mathbf{X})r(\mathbf{X})\tilde{w} \equiv 0 \bmod \mathcal{P}^{e+1}, \tag{5.28}$$

as desired. □

Proof of Lemma 5.2. This is immediate from Lemma 5.14, since the linear equality (5.9) is equivalent to having $\Gamma(\mathbf{X})\tilde{Q}_e(\mathbf{X})\omega \equiv 0 \bmod \mathcal{P}^{e+1}$ for $\omega = \tilde{w} + \pi^e\delta$. □

5.3.3. *Linear rephrasing for isotropy of lifts — Proofs of Lemmas 5.3 and 5.6.* The following result covers both of the desired results as a special case:

Lemma 5.15. *Consider some $w \in \mathcal{O}_K^n$ whose Krylov space $\mathscr{K}_{\mathbf{X}}(w)$ is isotropic up to level $\mathcal{P}^e$ for $e \geq 1$. Fix some $k \in \{1, \dots, e\}$ and $\pi \in \mathcal{P} \setminus \mathcal{P}^2$.*

Pick an arbitrary lift $\tilde{w} \in (\mathcal{O}_K/\mathcal{P}^{e+k})^n$ with $\tilde{w} \equiv w \bmod \mathcal{P}^e$ and let $C_j \in \mathcal{O}_K/\mathcal{P}^k$ satisfy $\tilde{w}^\top \mathbf{X}^j \tilde{w} \equiv \pi^e C_j \bmod \mathcal{P}^{e+k}$. Consider $\omega \in \mathcal{O}_K^n$ and $\delta \in (\mathcal{O}_K/\mathcal{P}^k)^n$ with

$$\omega \equiv \tilde{w} + \pi^e \delta \bmod \mathcal{P}^{e+k}. \tag{5.29}$$

Then, $\mathscr{K}_{\mathbf{X}}(\omega)$ is isotropic up to level $\mathcal{P}^{e+k}$ if and only if δ satisfies the following equations:

$$2w^\top \mathbf{X}^j \delta \equiv -C_j \bmod \mathcal{P}^k \quad \text{for} \quad j = 0, 1, \dots, \deg(Q_e) + \deg(Q_k) - 1. \tag{5.30}$$

Proof. Note that $\mathscr{K}_{\mathbf{X}}(\omega)$ is isotropic up to level $\mathcal{P}^{e+k}$ if and only if $\omega^\top \mathbf{X}^j \omega \equiv 0 \bmod \mathcal{P}^{e+k}$ for all j. Here, expanding (5.29) using the symmetry of $\mathbf{X}$,

$$\omega^\top \mathbf{X}^j \omega = \tilde{w}^\top \mathbf{X}^j \tilde{w} + \pi^e 2\tilde{w}^\top \mathbf{X}^j \delta + \pi^{2e} \delta^\top \mathbf{X}^j \delta \equiv \pi^e \Big(C_j + 2w^\top \mathbf{X}^j \delta \Big) \bmod \mathcal{P}^{e+k}, \tag{5.31}$$

where we used that $\tilde{w} \equiv w \bmod \mathcal{P}^e$, the assumption that $\mathscr{K}_{\mathbf{X}}(w)$ is isotropic up to level $\mathcal{P}^e$, and that $e \geq k$. We may conclude that $\mathscr{K}_{\mathbf{X}}(\omega)$ is isotropic up to level $\mathcal{P}^{e+k}$ if and only if $2w^\top \mathbf{X}^j \delta \equiv -C_j \bmod \mathcal{P}^k$ for all $j \leq n-1$.

It remains to show that every δ with $2w^\top \mathbf{X}^j \delta \equiv -C_j \bmod \mathcal{P}^k$ for $j \leq \deg(Q_e) + \deg(Q_k) - 1$ satisfies the constraints for all larger values of j. We proceed by induction on j. Consider some $j \geq \deg(Q_e)$ with $2w^\top \mathbf{X}^{j'} \delta \equiv -C_{j'} \bmod \mathcal{P}^k$ for all $j' < j$.

Recall that Q_e is monic with $Q_e(\mathbf{X})w \equiv 0 \bmod \mathcal{P}^e$. It follows that there exist coefficients $q_i^{(e)} \in \mathcal{O}_K$ with

$$\mathbf{X}^{\deg(Q_e)} \tilde{w} \equiv \textstyle\sum_{i < \deg(Q_e)} q_i^{(e)} \mathbf{X}^i \tilde{w} + \pi^e r \bmod \mathcal{P}^{e+k}. \tag{5.32}$$

Hence, for every $j \geq \deg(Q_e)$, using the definition $\tilde{w}^\top \mathbf{X}^j \tilde{w} = \pi^e C_j$,

$$C_j \equiv \textstyle\sum_{i < \deg(Q_e)} q_i^{(e)} C_{j - \deg(Q_e) + i} + w^\top \mathbf{X}^{j - \deg(Q_e)} r \bmod \mathcal{P}^k. \tag{5.33}$$

Similarly, reducing (5.32) modulo $\mathcal{P}^k$ and using the induction hypothesis,

$$\begin{aligned} 2w^\top \mathbf{X}^j \delta &\equiv \textstyle\sum_{i < \deg(Q_e)} 2q_i^{(e)} w^\top \mathbf{X}^{j - \deg(Q_e) + i} \delta \bmod \mathcal{P}^k \\ &\equiv - \textstyle\sum_{i < \deg(Q_e)} q_i^{(e)} C_{j - \deg(Q_e) + i} \bmod \mathcal{P}^k. \end{aligned} \tag{5.34}$$

Thus, $2w^\top \mathbf{X}^j \delta \equiv -C_j \bmod \mathcal{P}^k$ for $j \geq \deg(Q_e)$ if and only if $w^\top \mathbf{X}^{j - \deg(Q_e)} r \equiv 0 \bmod \mathcal{P}^k$. It follows from Q_k being monic with $Q_k(\mathbf{X})w \equiv 0 \bmod \mathcal{P}^k$ that it is equivalent to impose the latter constraint only for $j \leq \deg(Q_e) + \deg(Q_k) - 1$. □

6. Numerical experiments

We finally apply Algorithm 1 to random integer matrices with entries uniform on $[-100, 100] \cap \mathbb{Z}$. To our knowledge, no numerical data is available in such settings in previous literature, due to the difficulty of exhaustive approaches. Our experiments below use $M = 10^4$ as the prime cutoff for Assumption 2.17.

Table 1 concerns cospectrality over $\mathbb{Q}$ in varying dimensionality $n \leq 100$. We observe that the probability of rational cospectrality peaks at approximately 40% near $n \approx 7$. This finding gives numerical evidence in favor of a conjecture by the author [39, Conjecture 1.9] that posits that the probability of rational cospectrality should be bounded away from one for integer matrices in fixed dimension.

Rational cospectrality appears to be less frequent in high dimensions. For example, no rationally cospectral mates were found in dimension $n = 100$. This is suggestive of an integer matrix variant of Haemers' conjecture concerning the spectral determinacy of high-dimensional random graphs [17, 36].

We can also study the orthogonal matrix realizing cospectrality. The *block size* $|\mathbf{Q}|$ is the number of columns with strictly more than one nonzero entry. We identify the level ideal $\mathcal{L} \subseteq \mathbb{Z}$ from (2.3) with the positive integer $\ell \in \mathbb{Z}_{\geq 1}$ satisfying $\mathcal{L} = \ell\mathbb{Z}$. Table 1 shows that the blocksize and level may both be relatively large when n is small, but that it is typical to have small values for large n. Most rational cospectral mates for $n \geq 15$ had the smallest possible level $\ell = 2$ and a small blocksize ≈ 4. That small blocksizes are typical is partially explained by our proofs; recall (5.19).

n	#Cospectral in $\mathbb{Z}$ over $\mathbb{Q}$	Avg. block size $\lvert\mathbf{Q}\rvert$	Avg. level ℓ	Timeout
2	74	2.000	9.350	0
3	246	2.838	16.269	0
4	315	3.594	8.933	0
5	360	4.120	9.904	0
6	383	4.878	11.790	0
7	407	5.492	103.945	0
8	379	6.167	18.131	0
9	389	6.265	12.765	0
10	343	6.507	9.222	0
11	253	6.492	20.571	0
12	182	6.113	5.028	0
13	132	5.705	3.496	0
14	84	4.869	2.768	0
15	54	4.817	2.413	2
16	23	4.580	2.540	1
17	20	4.286	2.048	0
18	6	4.000	2.000	1
19	14	4.235	2.000	1
20	4	4.286	2.143	1
25	0	N/A	N/A	0
50	0	N/A	N/A	2
100	0	N/A	N/A	0

TABLE 1. The number of integer matrices among 1000 random samples where Algorithm 1 with $M = 10^4$ and $K = \mathbb{Q}$ finds a cospectral mate, as well as average the blocksizes and levels of the rational orthogonal matrices realizing the cospectrality. Computations that were inconclusive due to exceeding a time limit are reported under "Timeout".

We finally consider cospectrality over the quadratic fields $K \in \{\mathbb{Q}(\sqrt{d}) : d = 2, 3, 5, 6, 7\}$. Table 2 provides data on the number of matrices that admit a nontrivial cospectral mate in $R^{n\times n}$ strictly over K for $R \in \{\mathbb{Z}, \mathcal{O}_K\}$. Here, *strictly* means that we consider only those mates that arise through conjugation with an orthogonal matrix over K for which not all entries lie in the proper subfield $\mathbb{Q}$.

We observe in Table 2 that the quadratic fields produce a nontrivial number of additional cospectral mates, both in $\mathcal{O}_K$ and $\mathbb{Z}$. Notably, the probability for $\mathbb{Z}$ depends sensitively on the dimensionality n. For example, we find a substantial number of integer cospectral mates strictly over $\mathbb{Q}(\sqrt{2})$ only in even dimensions. A similar phenomenon of sensitive dependence on the dimensionality is observed for $\mathbb{Q}(\sqrt{d})$ with $d > 2$, but is not simply based on divisibility of n by d.

Dimension n	2	3	4	5	6	7	8	9	10
$\#\mathbb{Z}$ over $\mathbb{Q}(\sqrt{2})$	495	0	330	0	166	0	78	0	14
$\#\mathbb{Z}[\sqrt{2}]$ over $\mathbb{Q}(\sqrt{2})$	508	645	640	580	504	437	333	213	131
Timeout	0	2	2	0	6	4	15	19	29
$\#\mathbb{Z}$ over $\mathbb{Q}(\sqrt{3})$	0	0	240	0	0	0	23	0	0
$\#\mathbb{Z}[\sqrt{3}]$ over $\mathbb{Q}(\sqrt{3})$	147	279	379	239	128	50	37	6	0
Timeout	0	3	1	1	6	4	21	15	24
$\#\mathbb{Z}$ over $\mathbb{Q}(\sqrt{5})$	347	0	94	0	12	0	1	0	0
$\#\mathbb{Z}[\frac{\sqrt{5}+1}{2}]$ over $\mathbb{Q}(\sqrt{5})$	358	236	291	227	177	95	53	5	4
Timeout	0	0	1	0	9	5	24	17	23
$\#\mathbb{Z}$ over $\mathbb{Q}(\sqrt{6})$	0	0	67	0	0	0	3	0	0
$\#\mathbb{Z}[\sqrt{6}]$ over $\mathbb{Q}(\sqrt{6})$	36	103	108	27	7	0	3	0	0
Timeout	0	1	2	2	3	5	17	16	26
$\#\mathbb{Z}$ over $\mathbb{Q}(\sqrt{7})$	0	0	47	0	0	0	0	0	0
$\#\mathbb{Z}[\sqrt{7}]$ over $\mathbb{Q}(\sqrt{7})$	39	35	59	15	0	0	0	0	0
Timeout	0	1	3	2	4	2	11	13	27

TABLE 2. The number of integer matrices in 1000 samples where Algorithm 1 with $M = 10^4$ finds a cospectral mate with entries in $R \in \{\mathbb{Z}, \mathcal{O}_K\}$ strictly over $K = \mathbb{Q}(\sqrt{d})$. Computations that were inconclusive due to exceeding a time limit are reported under "Timeout".

Let us finally note that Algorithm 1 is also applicable to simple graphs. However, phenomena related to Remark 2.4 make it less efficient in high dimensions ($n \gg 20$). Potential refinements of the algorithm to simple graphs are an interesting problem, which we intend to pursue in future work. We refer to [40, 44] for numerical data on generalized cospectrality in simple graphs. Numerical data for graphs with loops and signed graphs is given in Appendix B.

Acknowledgements. I thank Nikita Lvov and Nils Van de Berg for discussions related to the topic of this paper.

Funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany's Excellence Strategy EXC 2044/2 –390685587, Mathematics Münster: Dynamics–Geometry–Structure.

Tool and computational resource disclosure. The author developed the main mathematical content and the writing. In the preparation of this manuscript, large language models (LLMs) were used as a supporting tool for language refinement or idea exploration, never to autonomously generate text. For the codebase, LLMs were used to optimize the implementation, as discussed below.

The initial implementation (v0.0.1 on GitHub) was written manually, with LLM use (Google Gemini Pro 3.1) being restricted to `SageMath` syntax searches and local code fragment suggestions. The initial implementation was however relatively slow, which we suspect to be primarily due to reliance on a generic `SageMath` quotient ring constructor whose arithmetic is not optimized for the special case of (quotients of) rings of integers. There were also some bugs.

Iterations to improve the code efficiency and quality were hereafter done with more intensive LLM use, mostly with Anthropic Claude Opus 4.8. To ensure that the code remained maintainable and understood, a two-stage process was used. First, a LLM was used to aid in drafting design specifications that addressed issues in the code, which the author then edited. Next, the specifications were implemented using a separate LLM instance.

The resulting code was reviewed by the author and tested on exhaustively generated examples, including all cospectral 3×3 matrices with $\sum_{i \le j} \mathbf{X}_{i,j}^2 \le 25$. The algorithm was run over the field K required to realize the cospectrality, which was determined using the orthogonal matrices from the pair's eigendecomposition. The degree of the required extension $K/\mathbb{Q}$ ranged from 1 to 4.

The experiments in Section 6 used version 0.0.3 of the implementation. The source code is available at https://github.com/Alexander-Van-Werde/cospectral.

References

[1] A. Abiad, N. Van de Berg, and R. Simoens. Counting cospectral graphs obtained via switching. *Discrete Mathematics*, 2026. doi: 10.1016/j.disc.2025.114775.

[2] F. Belardo, S. M. Cioabă, J. H. Koolen, and J. Wang. Open problems in the spectral theory of signed graphs. *arXiv preprint arXiv:1907.04349*, 2019. doi: 10.48550/arXiv.1907.04349.

[3] M. Bhargava, B. Gross, and X. Wang. A positive proportion of locally soluble hyperelliptic curves over $\mathbb{Q}$ have no point over any odd degree extension. *Journal of the American Mathematical Society*, 2017. doi: 10.1090/jams/863.

[4] A. Brouwer and E. Spence. Cospectral graphs on 12 vertices. *The Electronic Journal of Combinatorics*, 2009. doi: 10.37236/258.

[5] A. E. Brouwer and W. H. Haemers. *Spectra of graphs*. Springer Science & Business Media, 2011. doi: 10.1007/978-1-4614-1939-6.

[6] W. Brown. *Matrices over Commutative Rings*. Monographs and Textbooks in Pure and Applied Mathematics. Marcel Dekker, 1992.
[7] J. Ding, J. Gower, and D. Schmidt. *Multivariate public key cryptosystems*. Springer, 2006. doi: 10.1007/978-1-0716-0987-3.
[8] D. Dummit and R. Foote. *Abstract Algebra*. John Wiley & Sons, third edition, 2004.
[9] C. Godsil. Controllable subsets in graphs. *Annals of Combinatorics*, 2012. doi: 10.1007/s00026-012-0156-3.
[10] C. Godsil and B. McKay. Some computational results on the spectra of graphs. In *Combinatorial Mathematics IV: Proceedings of the Fourth Australian Conference Held at the University of Adelaide*, pages 73–92. Springer, 1976. doi: 10.1007/BF b0097370.
[11] C. Godsil and B. McKay. Constructing cospectral graphs. *Aequationes Mathematicae*, 1982. doi: 10.1007/BF02189621.
[12] C. Godsil and G. Royle. *Algebraic graph theory*. Springer Science & Business Media, 2013. doi: 10.1007/978-1-4613-0163-9.
[13] G. Greiter. A simple proof for a theorem of Kronecker. *The American Mathematical Monthly*, 1978. doi: 10.1080/00029890.1978.11994694.
[14] H. Günthard and H. Primas. Zusammenhang von Graphentheorie und MO-theorie von Molekeln mit Systemen konjugierter Bindungen. *Helvetica Chimica Acta*, 1956. doi: 10.1002/hlca.19560390623.
[15] S. Guo and W. Wang. Primary decomposition theorem and generalized spectral characterization of graphs. *Advances in Applied Mathematics*, 2025. doi: 10.101 6/j.aam.2025.102927.
[16] W. Haemers and E. Spence. Enumeration of cospectral graphs. *European Journal of Combinatorics*, 2004. doi: 10.1016/S0195-6698(03)00100-8.
[17] W. H. Haemers. Are almost all graphs determined by their spectrum? *Notices of the South African Mathematical Society*, 2016.
[18] R. Hartshorne. *Algebraic geometry*. Springer Science & Business Media, 1997. doi: 10.1007/978-1-4757-3849-0.
[19] K. Hoffmann and R. Kunze. *Linear algebra*. Prentice-Hall New Jersey, second edition, 1971.
[20] Y. Ji, W. Wang, and H. Zhang. Mixed graphs determined by their generalized Hermitian adjacency spectrum based on Eisenstein integers. *The Electronic Journal of Combinatorics*, 2025. doi: 10.37236/13156.
[21] C. Johnson and M. Newman. A note on cospectral graphs. *Journal of Combinatorial Theory, Series B*, 1980. doi: 10.1016/0095-8956(80)90058-1.
[22] M. Kac. Can one hear the shape of a drum? *The American Mathematical Monthly*, 1966. doi: 10.1080/00029890.1966.11970915.
[23] S. Lang. *Algebra*. Springer Science & Business Media, revised third edition, 2012. doi: 10.1007/978-1-4613-0041-0.
[24] N. Lvov and A. Van Werde. On the satisfaction frequency of spectral characterization conditions. *arXiv preprint arXiv:2603.26932*, 2026. doi: 10.48550/arXiv.2 603.26932.

[25] D. Marcus and E. Sacco. *Number fields*. Springer, second edition, 1977. doi: 10.1007/978-3-319-90233-3.

[26] B. Mohar and S. Poljak. Eigenvalues in combinatorial optimization. In *Combinatorial and graph-theoretical problems in linear algebra*. Springer, 1993. doi: 10.1007/978-1-4613-8354-3_5.

[27] D. Musser. Algorithms for polynomial factorization. Technical report, University of Wisconsin-Madison Department of Computer Sciences, 1971. http://digital.library.wisc.edu/1793/57716.

[28] J. Neukirch. *Algebraic number theory*. Springer Science & Business Media, first edition, 1999. doi: 10.1007/978-3-662-03983-0.

[29] S. O'Rourke and B. Touri. On a conjecture of Godsil concerning controllable random graphs. *SIAM Journal on Control and Optimization*, 2016. doi: 10.1137/15M1049622.

[30] The PARI Group, Univ. Bordeaux. *PARI/GP version 2.15.4*, 2023. http://pari.math.u-bordeaux.fr/.

[31] L. Qiu, Y. Ji, L. Mao, and W. Wang. Generalized spectral characterizations of regular graphs based on graph-vectors. *Linear Algebra and its Applications*, 2023. doi: 10.1016/j.laa.2023.01.006.

[32] A. Schwenk. Almost all trees are cospectral. *New directions in the theory of graphs*, 1973.

[33] R. Simoens and S. Van Overberghe. An algorithm to find cospectral mates. Announced at the 2026 Discrete Mathematics Days: https://damnetwork.github.io/dmd2026/submissions.html.

[34] T. Tao and V. Vu. Random matrices have simple spectrum. *Combinatorica*, 2017. doi: 10.1007/s00493-016-3363-4.

[35] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 10.9)*, 2026. https://www.sagemath.org.

[36] E. Van Dam and W. Haemers. Which graphs are determined by their spectrum? *Linear Algebra and its Applications*, 2003. doi: 10.1016/S0024-3795(03)00483-X.

[37] A. Van Werde. Cokernel statistics for walk matrices of directed and weighted random graphs. *Combinatorics, Probability and Computing*, 2025. doi: 10.1017/S0963548324000312.

[38] A. Van Werde. A sufficient condition for generalized spectral characterization of graphs with loops. *arXiv preprint arXiv:2511.19625*, 2025. doi: 10.48550/arXiv.2511.19625.

[39] A. Van Werde. Exact cospectrality probabilities for uniform random matrices. *arXiv preprint arXiv:2602.00233*, 2026. doi: 10.48550/arXiv.2602.00233.

[40] A. Van Werde. Exact cospectrality probabilities for uniform random matrices. *arXiv preprint arXiv:2602.00233*, 2026. doi: 10.48550/arXiv.2602.00233.

[41] W. Wang. Generalized spectral characterization of graphs: revisited. *The Electronic Journal of Combinatorics*, 2013. doi: 10.37236/3748.

[42] W. Wang. A simple arithmetic criterion for graphs being determined by their generalized spectra. *Journal of Combinatorial Theory, Series B*, 2017. doi: 10.1016/j.jctb.2016.07.004.

[43] W. Wang, L. Qiu, and J. Qian. Generalized spectral characterization of mixed graphs. *The Electronic Journal of Combinatorics*, 2020. doi: 10.37236/9588.
[44] W. Wang and W. Wang. Haemers' conjecture: an algorithmic perspective. *Experimental Mathematics*, 2025. doi: 10.1080/10586458.2024.2337229.
[45] W. Wang and C.-X. Xu. A sufficient condition for a family of graphs being determined by their generalized spectra. *European Journal of Combinatorics*, 2006. doi: 10.1016/j.ejc.2005.05.004.
[46] W. Wang, J. Yang, and H. Zhang. Rational orthogonal matrices and isomorphism of graphs. *Discrete Mathematics*, 2024. doi: 10.1016/j.disc.2024.114002.
[47] W. Wang and T. Yu. Square-free discriminants of matrices and the generalized spectral characterizations of graphs. *arXiv preprint arXiv:1608.01144*, 2016. doi: 10.48550/arXiv.1608.01144.
[48] W. Wang and D. Zhao. Graph isomorphism and multivariate graph spectrum. *Advances in Applied Mathematics*, 2026. doi: 10.1016/j.aam.2025.102994.
[49] D. Yun. On square-free decomposition algorithms. In *Proceedings of the third ACM symposium on Symbolic and algebraic computation*, pages 26–35, 1976. doi: 10.1145/800205.806320.
[50] O. Zariski and P. Samuel. *Commutative algebra: Volume I.* Springer Science & Business Media, 1958. https://archive.org/details/commutativealgeb0001zari.

Appendix A. Matrices with discriminant ±1 — Proof of Proposition 2.15

Recall from Remark 2.3 that the discriminant of a monic polynomial $f \in \mathbb{Z}[x]$ with roots $\lambda_1, \ldots, \lambda_n \in \mathbb{C}$ is given by $\Delta_f = \prod_{i<j}(\lambda_i - \lambda_j)^2$.

Lemma A.1. *Let $f \in \mathbb{Z}[x]$ be a monic polynomial with $\Delta_f = \pm 1$. Then, all irreducible factors of f over $\mathbb{Z}[x]$ have degree one.*

Proof. Suppose to the contrary that $f(x) = a(x)b(x)$ for some monic irreducible $a(x) \in \mathbb{Z}[x]$ with $\deg(a) \geq 2$. Then, $\Delta_f = \Delta_a \Delta_b R(a,b)^2$ with $R(a,b) = \prod_i \prod_j (\alpha_i - \beta_j)$ for α_i (resp. β_j) running over the roots of $a(x)$ (resp. $b(x)$). Here, $R(a,b)$ is the *resultant* of a, b is again an integer; see e.g., [23, Chapter IV, Section 8]. It hence remains to show that $|\Delta_a| \geq 2$.

Let $\alpha \in \mathbb{C}$ be an arbitrary root of a, let $K := \mathbb{Q}(\alpha)$, and denote $k := \deg(a)$. Recall that the *discriminant* of $k_1, \ldots, k_m \in K$ is $\operatorname{disc}(k_1, \ldots, k_k) := \det([\sigma_i(k_j)])^2$ with $\sigma_i : K \to \mathbb{C}$ the field embeddings [25, p.18]. Recall the classical fact that,

$$\operatorname{disc}(1, \alpha, \ldots, \alpha^{k-1}) = \prod_{i<j} \big(\sigma_i(\alpha) - \sigma_j(\alpha)\big)^2 = \pm \Delta_a, \tag{A.1}$$

which can be proved by considering a Vandermonde determinant [25, p.19]. Let $\operatorname{disc}(\mathcal{O}_K)$ be the discriminant of an arbitrary $\mathbb{Z}$-module basis $\gamma_1, \ldots, \gamma_k \in \mathcal{O}_K$. Then, $(1, \alpha, \ldots, \alpha^{k-1})^\top = \mathbf{M}(\gamma_1, \ldots, \gamma_k)^\top$ for some $\mathbf{M} \in \mathbb{Z}^{k \times k}$ and hence,

$$\operatorname{disc}(1, \alpha, \ldots, \alpha^{k-1}) = \det(\mathbf{M})^2 \operatorname{disc}(\mathcal{O}_K). \tag{A.2}$$

Note that $K \neq \mathbb{Q}$ since a is monic and irreducible over $\mathbb{Z}[x]$ and hence also over $\mathbb{Q}$ by Gauss's lemma [25, Theorem 1, p.10]. It however holds that $|\operatorname{disc}(\mathcal{O}_K)| \geq 2$ for any non-trivial number field $K \neq \mathbb{Q}$ [25, p.96]. The result hence follows from (A.1) and (A.2) since $\det(\mathbf{M}) \in \mathbb{Z}$ and $\Delta_a \neq 0$. □

Lemma A.2. *Let $f \in \mathbb{Z}[x]$ be a monic polynomial for which all roots are real and* $\deg(f) > 1$. *Then,* $\Delta_f = \pm 1$ *implies that* $\deg(f) = 2$.

Proof. Lemma A.1 implies that f factors in linear factors, and the formula $\Delta_f = \prod_{i<j}(\lambda_i - \lambda_j)^2$ implies that all roots of f have to satisfy $|\lambda_i - \lambda_j| = 1$. By the structure of the real line, this is impossible if $n \geq 3$. □

Proof of Proposition 2.15. It follows from Lemma A.2 that $|\Delta_{\mathbf{X}}| = 1$ for a symmetric integer matrix $\mathbf{X} \in \mathbb{Z}^{n\times n}$ with $n > 1$ implies then $n = 2$. In this case,

$$\mathbf{X} = \begin{pmatrix} a & b \\ b & c \end{pmatrix}. \tag{A.3}$$

Then, $\phi_{\mathbf{X}}(x) = x^2 - (a+c)x - b^2 + ac$ and $|\Delta_{\mathbf{X}}| = (a-c)^2 + 4b^2$. Hence, $|\Delta_{\mathbf{X}}| = 1$ if and only if $|a - c| = 1$ and $b = 0$. □

Appendix B. Numerical data for signed graphs and graphs with loops

We here repeat the experiments concerning rational cospectrality in Table 1, but now consider the adjacency matrices of graphs with loops and signed graphs.

B.1. **Signed graphs.** We consider a random symmetric matrix with the entries $\{\mathbf{X}_{i,j} : i \leq j\}$ uniform and independent from $\{-1, 0, 1\}$. Table 3 reports on the number of samples where Algorithm 1 finds a cospectral mate with entries in $\mathbb{Z}$, while Table 6 restricts to cospectral mates that again have entries in $\{-1, 0, 1\}$.

n	#Cospectral in $\mathbb{Z}$ over $\mathbb{Q}$	Avg. block size $\lvert\mathbf{Q}\rvert$	Avg. level ℓ	Inconclusive
5	150	4.205	4.586	51
6	270	4.914	7.694	32
7	369	5.690	22.416	16
8	400	6.807	35.120	2
9	404	6.396	37.608	1
10	322	6.730	36.746	0
11	268	6.014	6.378	1
12	219	6.084	7.675	0
13	135	5.825	3.666	1
14	94	5.588	2.748	1
15	58	4.558	2.274	1
16	31	4.407	2.169	0
17	28	4.654	2.231	0
18	19	4.171	2.086	1
19	7	4.308	2.154	0
20	10	4.211	2.158	3
25	0	N/A	N/A	1
50	0	N/A	N/A	2

Table 3. The number of signed graphs among 1000 random samples where Algorithm 1 with $M = 10^4$ and $K = \mathbb{Q}$ finds an integer cospectral mate to the adjacency matrix, and orthogonal matrix statistics. Computations that exceeding a time limit or could not be initiated due to a vanishing discriminant are reported under "Inconclusive".

n	#Cospectral in $\{-1,0,1\}$ over $\mathbb{Q}$	Avg. block size $\lvert\mathbf{Q}\rvert$	Avg. level ℓ	Inconclusive
5	47	3.718	3.254	51
6	125	4.677	8.463	32
7	164	5.183	24.342	16
8	149	5.676	25.091	2
9	116	5.322	33.441	1
10	54	4.957	19.565	0
11	47	4.231	2.750	1
12	25	4.531	2.156	0
13	8	4.750	2.375	1
14	8	4.600	2.100	1
15	4	3.750	2.250	1
16	3	4.000	2.000	0
17	2	4.000	2.000	0
18	0	N/A	N/A	1
19	0	N/A	N/A	0
20	0	N/A	N/A	3
25	0	N/A	N/A	1
50	0	N/A	N/A	2

TABLE 4. The number of signed graphs among 1000 random samples where Algorithm 1 finds a $\{-1,0,1\}^{n\times n}$-valued cospectral mate. The remainder of the setup is as in the caption of Table 3.

B.2. **Unsigned graphs (possibly with loops).** We consider a random symmetric matrix with the entries $\{\mathbf{X}_{i,j} : i \le j\}$ uniform and independent from $\{0,1\}$. Table 5 reports on the number of samples where Algorithm 1 finds a cospectral mate with entries in $\mathbb{Z}$.

n	#Cospectral in $\mathbb{Z}$ over $\mathbb{Q}$	Avg. block size $\lvert\mathbf{Q}\rvert$	Avg. level ℓ	Inconclusive
5	53	4.344	3.958	211
6	149	4.920	5.243	155
7	205	5.669	11.850	102
8	259	6.045	11.853	67
9	279	6.732	137.320	47
10	266	6.499	317.561	28
11	235	6.676	62.949	13
12	157	6.735	31.331	9
13	124	6.307	52.952	3
14	75	7.265	78.273	4
15	56	4.850	4.009	3
16	29	4.724	3.931	1
17	22	4.238	2.119	1
18	10	5.000	12.353	2
19	6	4.000	2.000	1
20	3	4.000	2.000	2
25	1	4.000	2.000	0
50	0	N/A	N/A	2

TABLE 5. The number of graphs (possibly with loops) among 1000 random samples where Algorithm 1 finds an integer cospectral mate. The remainder of the setup is as in the caption of Table 3.

Table 6 restricts to cospectral mates in that again correspond to unsigned graphs (possibly with loops). Finally, Table 7 considers cospectrality to signed graphs.

n	#Cospectral in $\{0,1\}$ over $\mathbb{Q}$	Avg. block size $\lvert\mathbf{Q}\rvert$	Avg. level ℓ	Inconclusive
5	10	4.286	3.143	211
6	50	4.494	4.071	155
7	76	5.170	14.717	102
8	123	5.560	11.632	67
9	142	5.567	93.372	47
10	145	5.931	22.121	28
11	149	5.886	57.270	13
12	97	5.725	11.775	9
13	83	5.443	6.402	3
14	59	6.656	77.021	4
15	48	4.909	5.255	3
16	24	4.480	4.120	1
17	22	4.435	2.217	1
18	8	5.889	21.556	2
19	6	4.000	2.000	1
20	3	4.000	2.000	2
25	1	4.000	2.000	0
50	0	N/A	N/A	2

TABLE 6. The number of graphs (possibly with loops) among 1000 random samples where Algorithm 1 finds a $\{0,1\}^{n\times n}$-valued cospectral mate. The remainder of the setup is as in the caption of Table 3.

n	#Cospectral in $\{-1,0,1\}$ over $\mathbb{Q}$	Avg. block size $\lvert\mathbf{Q}\rvert$	Avg. level ℓ	Inconclusive
5	13	4.278	3.111	211
6	61	4.565	6.037	155
7	91	5.329	13.193	102
8	133	5.714	12.028	67
9	154	5.765	73.085	47
10	153	6.033	19.811	28
11	160	5.966	60.461	13
12	104	5.840	11.165	9
13	87	5.435	7.344	3
14	61	7.256	79.288	4
15	48	4.847	5.034	3
16	25	4.500	3.929	1
17	22	4.417	2.208	1
18	8	5.889	21.556	2
19	6	4.000	2.000	1
20	3	4.000	2.000	2
25	1	4.000	2.000	0
50	0	N/A	N/A	2

TABLE 7. The number of graphs (possibly with loops) among 1000 random samples where Algorithm 1 finds a $\{-1,0,1\}^{n\times n}$-valued cospectral mate. The remainder of the setup is as in the caption of Table 3.