

# On the satisfaction frequency of spectral characterization conditions

Nikita Lvov<sup>◇</sup>

Alexander Van Werde<sup>\*</sup>

---

**Abstract.** We give the first specific conjectures on how frequently graphs satisfy sufficient conditions for being uniquely characterized by spectral information. These conjectures arise from a theoretical framework that we developed based on abstract-algebraic random matrix statistics. Specifically, we rephrase conditions from the literature in terms of  $\mathbb{Z}[x]$ -modules associated to the adjacency matrix, and study the distribution of those modules in analytically tractable profinite random matrix ensembles. We applied this new method to two distinct conditions. The first requires square-freeness of the determinant of the walk matrix, and the second uses the discriminant of the characteristic polynomial.

*MSC2020 subject classifications:* 05C50, 05C80, 60B20, 15B52

*Keywords:* cospectral, cokernel, walk matrix, discriminant, symmetric integer matrix, profinite model

---

## 1. INTRODUCTION

It has been known since the 1950s that there exist non-isomorphic graphs whose adjacency matrices have the same characteristic polynomial, called *cospectral mates* [13]. A fundamental conjecture by Haemers however proposes that such examples should be atypical [24, 44]. That is, if one picks a graph on  $n$  nodes uniformly at random, then it is believed that the probability of cospectrality tends to zero as  $n \rightarrow \infty$ . A closely related *fingerprint conjecture* for matrices with entries  $\pm 1$  was more recently also proposed by Vu [49, 50].

Haemers' conjecture remains open. The current best lower bound on the number of graphs characterized by spectrum is by Koval and Kwan [30] who established that at least  $\exp(cn)$  graphs on  $n$  nodes are characterized by adjacency spectrum for some  $c > 0$ . This was a significant improvement on previous bounds of order  $\exp(c\sqrt{n})$ , but remains a vanishing fraction of all  $(1-o(1))2^{n(n-1)/2}/n! \geq \exp(cn^2)$  graphs. Moreover, it seems likely that an exponential bound is the limit of the constructive methods in [30] and that even bounds of order  $\exp(n^{1+\varepsilon})$  would require different methods: "...It is hard to imagine a natural argument that could reconstruct so many different graphs... Instead, it seems that non-constructive methods may be necessary..." [30, §1.1].

There indeed exist sufficient conditions that can certify that a graph is determined by spectral information without giving an algorithm to reconstruct the graph from its spectrum. Such conditions were first discovered by Wang and Xu [54] for a generalized notion where one is also given the spectrum of the complement graph, and considerable effort has since been devoted to refinements of these sufficient conditions [6, 23, 38, 47, 51, 52, 53, 55, 56, 60]. (We give examples in Section 1.1.)

Numerical investigations suggest that such sufficient conditions are applicable with non-vanishing frequency. This would be significant considering the expected limits of constructive methods. Unfortunately, the current theoretical understanding of the probabilistic behavior of the conditions is also limited. For instance, while the satisfaction frequencies of the conditions can be roughly estimated numerically, it is not known for any of them what the exact limiting values might be.

---

<sup>◇</sup> MCGILL UNIVERSITY, CANADA

<sup>\*</sup> UNIVERSITY OF MÜNSTER, GERMANY

*E-mail address:* nikita.lvov@mail.mcgill.ca, a.van.werde@uni-muenster.de.

*Date:* March 27, 2026.

The present paper takes an initial step towards a probabilistic understanding of spectral characterization condition by developing a connection to the theory of abstract-algebraic random matrix statistics. Our approach has two main steps. The first is to rephrase the considered condition in terms of an abstract-algebraic object associated to the graph's adjacency matrix, such as certain groups or a modules. The second step is to study the distribution of those algebraic objects using an analytically tractable profinite random matrix ensemble. The ensemble used in this second step incorporates the symmetry constraint on the adjacency matrix that comes from the the graph being undirected, while achieving analytical tractability by taking the entries uniform on a larger space than  $\{0, 1\}$ . In particular, the results achieved in the latter model give theoretical insight on the limiting satisfaction frequency of various conditions; see Theorems 4.11 and 4.17.

Our main results require some technical background to motivate and state, which we build up over the span of the paper. A notable and easy-to-state consequence is that we find the first specific predictions on the satisfaction frequency of spectral characterization conditions. The resulting conjectures are showcased in Section 1.1. We explain the framework that we developed in Section 1.2 and comment on universality in Section 1.3. The remainder of the paper is outlined in Section 1.4.

**1.1. Specific predictions for satisfaction frequencies.** To demonstrate the flexibility of our approach, we consider two different conditions. The first is based on the square-freeness of the determinant of the walk matrix and is the subject of Conjecture 1.4. The second uses the discriminant of the characteristic polynomial and is considered in Conjecture 1.7.

1.1.1. *Conditions based on the walk matrix.* The following definitions are due to Farrugia [18] and Qiu, Ji, Mao, and Wang [37] in a special case; see also [47, 55] for the general setting used here.

**Definition 1.1.** Consider an integer vector  $\zeta \in \mathbb{Z}^n$  and a matrix  $\mathbf{M} \in \mathbb{Z}^{n \times n}$  that is symmetric  $\mathbf{M} = \mathbf{M}^\top$ . Two such pairs  $(\mathbf{M}, \zeta)$  and  $(\mathbf{N}, \eta)$  are *isomorphic up to signed permutation* if there exists a signed permutation  $\mathbf{S}$  such that  $\mathbf{N} = \mathbf{S}\mathbf{M}\mathbf{S}^\top$  and  $\mathbf{S}\zeta = \eta$ .

Here, a *signed permutation* is a matrix of the form  $\mathbf{S} = \mathbf{P}\mathbf{D}$  with  $\mathbf{P}$  a permutation and  $\mathbf{D}$  a diagonal matrix with entries  $\pm 1$ . The signs serve to avoid trivial obstructions to spectral characterization for general integer matrices, but are irrelevant if one restricts to the adjacency matrices of a graphs as two nonnegative matrices are related by a signed permutation if and only if they are related by an unsigned permutation. Consequently, since permutations corresponds to graph isomorphism, the following notion yields a generalization of adjacency spectral characterization, with some additional information related to the vector  $\zeta$ :

**Definition 1.2.** The *bivariate characteristic polynomial* of the pair  $(\mathbf{M}, \zeta)$  is defined as

$$\Phi_{\mathbf{M}, \zeta}(\lambda, t) := \det(\lambda \mathbf{I} - \mathbf{M} - t\zeta\zeta^\top), \quad (1.1)$$

where  $\mathbf{I}$  is the identity. The pair  $(\mathbf{M}, \zeta)$  is said to be *characterized by  $\Phi$ -spectrum* if every  $(\mathbf{N}, \eta)$  with  $\Phi_{\mathbf{M}, \zeta} = \Phi_{\mathbf{N}, \eta}$  is isomorphic up to signed permutation.

The case where  $\zeta = \mathbb{1}_S$  is the indicator vector of some set  $S \subseteq \{1, \dots, n\}$  and  $\mathbf{M}$  is the adjacency matrix of a graph admits a direct graph-theoretic interpretation. Then, the differentiating information in  $\Phi_{\mathbf{M}, \zeta}$  can be shown to be equivalent to the pair consisting of the spectrum of  $\mathbf{M}$  and the spectrum of the graph on  $n + 1$  nodes found by connecting the vertices in  $S$  to a new node; see Farrugia [18]. The special case where  $\zeta = (1, \dots, 1)^\top$  is the all-ones vector is also known to be equivalent to considering the spectra of the graph and its complement, due to Johnson and Newman [27].

We consider a sufficient condition in [47, Theorem 2.12] that is a variant on one by Wang [51]. The *walk matrix* of  $(\mathbf{M}, \zeta)$  is the square matrix  $\mathbf{W} \in \mathbb{Z}^{n \times n}$  with columns  $\zeta, \mathbf{M}\zeta, \dots, \mathbf{M}^{n-1}\zeta$ . The terminology refers to the fact that if  $\zeta = \mathbb{1}_S$  is an indicator vector and  $\mathbf{M}$  is the adjacency matrix of a graph, then the  $ij$ th entry  $\mathbf{W}_{i,j}$  counts walks of length  $j - 1$  that start in vertex  $i$  and end in  $S$ . Recall that an integer  $d$  is said to be *square-free* if  $p^2 \nmid d$  for every prime  $p$ .

**Theorem 1.3** (Van Werde [47]). *Consider  $\zeta \in \mathbb{Z}^n$  and  $\mathbf{M} \in \mathbb{Z}^{n \times n}$  with  $\mathbf{M} = \mathbf{M}^\top$  and suppose that  $\det(\mathbf{W})$  is square-free. Then,  $(\mathbf{M}, \zeta)$  is characterized by  $\Phi$ -spectrum up to signed permutation.*

We would like to understand how often this condition is applicable. For instance, one natural setting would be to take  $\mathbf{M}$  as the adjacency matrix of a random graph and  $\zeta = \mathbb{1}_S$  as the indicator

of some randomly chosen set of vertices. Results by O'Rourke and Touri show that  $\det(\mathbf{W}) \neq 0$  with high probability in such settings [36, Theorems 1.5 & 3.7]; see also [32, 34] for extensions.

Unfortunately, [32, 34, 36] do not enable predictions for square-freeness. The results achieved in Section 4.3 in different random matrix ensembles lead us to the following prediction for the satisfaction frequency of the condition in Theorem 1.3 for graphs with loops:

**Conjecture 1.4.** *Suppose that  $\mathbf{M}$  is chosen uniformly at random from all symmetric  $n \times n$  matrices with  $\{0, 1\}$ -valued entries and consider an independent random vector  $\zeta$  that is uniform on  $\{0, 1\}^n$ . Then, for every prime  $p$ ,*

$$\lim_{n \rightarrow \infty} \mathbb{P}(p^2 \nmid \det(\mathbf{W})) = \left(1 - \frac{1}{p^2} - \frac{1}{p^3} + \frac{1}{p^4}\right) \prod_{k=1}^{\infty} \left(1 - \frac{1}{p^{2k}}\right) \quad (1.2)$$

Further, the limiting probability of square-freeness factorizes over the constituent primes:

$$\begin{aligned} \lim_{n \rightarrow \infty} \mathbb{P}(\det(\mathbf{W}) \text{ is square-free}) &= \prod_{p \text{ prime}} \left(1 - \frac{1}{p^2} - \frac{1}{p^3} + \frac{1}{p^4}\right) \prod_{k=1}^{\infty} \left(1 - \frac{1}{p^{2k}}\right) \\ &= 0.2943 \dots \end{aligned} \quad (1.3)$$

One can compare (1.2) with empirical probabilities in Table 1 and observe a good match up to at least the third significant digit. Let us note that such a good match does not apply for the simpler heuristic probability  $1 - 1/p^2$  that would arise if one considers the probability that  $p^2 \nmid D$  for a random integer  $D$  uniform on  $\{1, \dots, m\}$  for  $m$  large. In fact, even if one only disregards the term  $1/p^4$  in (1.2) then this would already show a discrepancy on the second significant digit since  $(1 - 1/p^2 - 1/p^3) \prod_{k \geq 1} (1 - 1/p^{2k})$  is approximately 0.430 and 0.747 for  $p = 2$  and  $p = 3$ , respectively.

$p^2 \nmid \det(\mathbf{W})$	$n = 8$	$n = 10$	$n = 12$	$n = 15$	$n = 25$	$n = 50$	$n = 100$	Conjecture 1.4
$p = 2$	0.451	0.465	0.470	0.472	0.473	0.473	0.473	0.4733695677...
$p = 3$	0.616	0.690	0.731	0.752	0.758	0.757	0.757	0.75752129361...
$p = 5$	0.689	0.801	0.867	0.905	0.914	0.914	0.914	0.91393033780...
$p = 7$	0.708	0.830	0.904	0.946	0.957	0.956	0.957	0.95674525798...
$p = 11$	0.719	0.848	0.926	0.972	0.983	0.983	0.983	0.98279431682...

TABLE 1. Estimated probability that  $p^2 \nmid \det(\mathbf{W})$  in the setting of Conjecture 1.4. These estimates used  $10^6$  samples and hence have an uncertainty of  $\pm 0.0005$  in the sense of standard deviation.

To our knowledge, (1.3) is the first well-motivated conjecture for the limiting satisfaction frequency for any sufficient condition for spectral characterization. A conceptual forerunner is our previous work that studied the walk matrix in a setting without symmetry constraint; see Van Werde [46]. That setting is substantially simpler because removing the symmetry constraint allows the entries of  $\mathbf{M}$  to all be independent which enables different methods, such as direct analysis of the stochastic process  $\zeta, \mathbf{M}\zeta, \dots, \mathbf{M}^{n-1}\zeta$  in the columns of  $\mathbf{W}$ . However, the predictions in that setting do not match observations in symmetric settings [46, Section 4] and there are no sufficient conditions for non-symmetric matrices, so that there were no implications for spectral characterization. A key technical innovation in the current work is that we can incorporate a symmetry constraint.

Moreover, the results in [46] were specific to the walk matrix. The perspective developed in the current paper is more flexible. For instance, we next illustrate in Section 1.1.2 that we also gain insight on spectral characterization conditions that are initially unrelated to the walk matrix.

**1.1.2. Conditions based on the discriminant.** Note that symmetric matrices  $\mathbf{M}, \mathbf{N}$  are cospectral if and only if there exists an orthogonal matrix  $\mathbf{Q}$  such that  $\mathbf{N} = \mathbf{Q}\mathbf{M}\mathbf{Q}^\top$ . In many examples of cospectral graphs, although certainly not all, it further holds that  $\mathbf{Q}$  can be taken to have rational entries. For instance, this holds for examples produced by *Godsil-McKay switching* [21] which exhaustive enumeration has shown to be responsible for a large fraction of cospectral graphs on  $n \leq 12$  vertices [24]. This may motivate the following relaxation of cospectrality:

**Definition 1.5.** Two symmetric matrices  $\mathbf{M}, \mathbf{N}$  are said to be *cospectral through a rational matrix* if there exists a orthogonal matrix  $\mathbf{Q}$  with entries in  $\mathbb{Q}$  such that  $\mathbf{N} = \mathbf{Q}\mathbf{M}\mathbf{Q}^\top$ .

This notion is closely related to Definition 1.2. Indeed, given a pair  $(\mathbf{M}, \zeta)$  with nonsingular walk matrix  $\det(\mathbf{W}) \neq 0$  it can be shown that  $\Phi$ -cospectrality to some other pair  $(\mathbf{N}, \eta)$  is equivalent to the existence of a rational orthogonal matrix  $\mathbf{Q}$  with  $\mathbf{N} = \mathbf{Q}\mathbf{M}\mathbf{Q}^\top$  and  $\eta = \mathbf{Q}\zeta$ ; see [47, Lemma 2.1]. Here, recall that O'Rourke and Touri proved that the walk matrix is indeed nonsingular with high probability [36]. Definition 1.5 hence provides at least as good a proxy for Haemers' conjecture as  $\Phi$ -cospectrality since the constraint that  $\mathbf{Q}$  has to be compatible with the vectors is now removed. In particular, a bound on the fraction of graphs that are cospectral through a rational matrix would imply a bound on the fraction that are  $\Phi$ -cospectral.

We consider a condition from a work of Wang and Yu [55]. The *discriminant* of a monic polynomial  $\phi \in \mathbb{Z}[x]$  is the integer  $\Delta_\phi \in \mathbb{Z}$  given by the resultant of  $\phi$  and its derivative  $\phi'$ ; see Definition 3.3 in Section 3.2.1. If  $\lambda_1, \dots, \lambda_n \in \mathbb{C}$  are the roots of  $\phi$ , then one has the following equivalent expression:

$$\Delta_\phi = \prod_{i=1}^n \prod_{j \neq i} (\lambda_i - \lambda_j). \quad (1.4)$$

Let  $\Delta_{\mathbf{M}} := \Delta_{\varphi_{\mathbf{M}}}$  denote the discriminant of the characteristic polynomial  $\varphi_{\mathbf{M}}(\lambda) := \det(\lambda\mathbf{I} - \mathbf{M})$ .

**Theorem 1.6** (Wang and Yu [55]). *Consider symmetric integer matrix  $\mathbf{M}$  and suppose that the discriminant  $\Delta_{\mathbf{M}}$  is odd and square free. Then, a symmetric integer  $\mathbf{N}$  is cospectral to  $\mathbf{M}$  through a rational matrix if and only if there exists a signed permutation  $\mathbf{S}$  with  $\mathbf{N} = \mathbf{S}\mathbf{M}\mathbf{S}^\top$ .*

Related conditions for pairs of matrices are given in work of Bhargava, Gross, and Wang [4, Proposition 35], and extensions to algebraic number fields will appear in our forthcoming [45].

Our results achieved using abstract-algebraic random matrix statistics in Section 4.4 yield the following prediction for the satisfaction frequency of the condition in Theorem 1.6:

**Conjecture 1.7.** *Suppose that  $\mathbf{M}$  is chosen uniformly at random from all symmetric  $n \times n$  matrices with  $\{0, 1\}$ -valued entries. Then, for every prime  $p$ ,*

$$\lim_{n \rightarrow \infty} \mathbb{P}(p \nmid \Delta_{\mathbf{M}}) = \left(1 - \frac{1}{p}\right) \prod_{k=1}^{\infty} \left(1 - \frac{1}{p^{2k}}\right). \quad (1.5)$$

Further, for every odd prime  $p$ ,

$$\lim_{n \rightarrow \infty} \mathbb{P}(p^2 \nmid \Delta_{\mathbf{M}}) = \left(1 - \frac{1}{p^2} \frac{3p-1}{p+1}\right) \prod_{k=1}^{\infty} \left(1 - \frac{1}{p^{2k}}\right) \quad (1.6)$$

Moreover, the limiting probability for being odd and square-free factorizes over the constituent primes:

$$\begin{aligned} \lim_{n \rightarrow \infty} \mathbb{P}(\Delta_{\mathbf{M}} \text{ is odd and square-free}) &= \frac{6}{7} \prod_{p \text{ prime}} \left(1 - \frac{1}{p^2} \frac{3p-1}{p+1}\right) \prod_{k=1}^{\infty} \left(1 - \frac{1}{p^{2k}}\right) \\ &= 0.1686\dots \end{aligned} \quad (1.7)$$

Conjecture 1.7 matches empirical evidence presented in Table 2. For comparison, let us note that a random monic polynomial  $\phi \in \mathbb{Z}[x]$  with independent and uniform random coefficients is known to satisfy that  $p^2 \nmid \Delta_\phi$  for odd  $p$  with probability  $1 - p^{-1} + (p-1)^2 p^{-2} (p+1)^{-1}$  as  $n \rightarrow \infty$ ; see e.g., [2, Section 6]. That heuristic would not match the evidence in Table 2. For instance, it would predict that  $\mathbb{P}(3^2 \nmid \Delta_\phi) \approx 0.7777\dots$  and  $\mathbb{P}(5^2 \nmid \Delta_\phi) \approx 0.9066\dots$

$q \nmid \Delta_{\mathbf{M}}$	$n = 8$	$n = 10$	$n = 12$	$n = 15$	$n = 25$	$n = 50$	$n = 100$	Conjecture 1.7
$q = 2$	0.346	0.345	0.345	0.344	0.344	0.345	0.344	0.34426876856...
$q = 3^2$	0.628	0.662	0.672	0.679	0.682	0.682	0.682	0.68176916425...
$q = 5^2$	0.780	0.821	0.850	0.865	0.868	0.869	0.869	0.86894942632...
$q = 7^2$	0.843	0.885	0.909	0.925	0.929	0.929	0.929	0.92921742127...
$q = 11^2$	0.885	0.929	0.952	0.966	0.970	0.970	0.970	0.96981231057...

TABLE 2. Estimated probability that  $q \nmid \Delta_{\mathbf{M}}$  in the setting of Conjecture 1.7 for those values of  $q$  that are relevant for the discriminant being odd and square-free. These estimates used  $10^6$  samples.

**1.2. Two-step approach based on abstract-algebraic random matrix statistics.** Let us now explain the theoretical framework that we developed and that resulted in the predicted values in Conjectures 1.4 to 1.7. The basic idea is given by the following two-step approach:

- (1) A-priori it may appear that the walk matrix and the discriminant are totally different objects whose study would require different methods, but it turns out that they can both be expressed in terms of the structure of the same abstract-algebraic object. Specifically, an integer matrix  $\mathbf{M} \in \mathbb{Z}^{n \times n}$  induces a  $\mathbb{Z}[x]$ -module structure on the  $n$ -dimensional lattice  $\mathbb{Z}^n$  specified by  $xv = \mathbf{M}v$  for every  $v \in \mathbb{Z}^n$ . As it turns out, both spectral characterization conditions can be rephrased in terms of the structure of this  $\mathbb{Z}[x]$ -module. This is done in Section 3.
- (2) The question becomes to understand the distribution of the aforementioned module. To this end, we introduce an analytically tractable random matrix ensemble that incorporates key structure from  $\mathbf{M}$  and also induces a  $\mathbb{Z}[x]$ -module. Our model here is the Haar distribution on symmetric matrices with entries in the profinite completion of  $\mathbb{Z}[x]$ . Section 4 defines this ensemble in detail and gives rigorous results on frequency with which the associated modules satisfy the constraints arising from spectral characterization conditions.

The reason why this profinite ensemble is analytically tractable is that it enjoys a strong invariance property: if  $\mathbf{M}$  is a matrix from that ensemble and  $\mathbf{G}$  is a fixed invertible matrix over the profinite completion of  $\mathbb{Z}[x]$ , then  $\mathbf{G}\mathbf{M}\mathbf{G}^\top$  is again symmetric with the same distribution as  $\mathbf{M}$ . We crucially exploit this invariance the proof of Proposition 4.5 to establish a reduction from module-theoretic events associated to the  $n \times n$  matrix  $\mathbf{M}$  to events stated using matrices of bounded size. Given that reduction, all relevant probabilities can be deduced from a finite computation.

We believe that the two-step method itself has significant potential beyond the specific results that we establish in the present paper. There are many different sufficient conditions in the literature whose satisfaction frequency remains to be theoretically understood [6, 23, 38, 47, 51, 52, 53, 55, 56, 60]. Simplified analytically tractable models are attractive in this context, as they should enable theoretical insight for many different conditions at a relatively low cost. Of course, some adjustments may be necessary. The appropriate category of abstract-algebraic objects considered in the first step may depend on the condition under consideration, and the selection of analytical tractable model in the second step also requires some care. One has to incorporate enough structure of the original random matrix ensemble that one hopes to gain insight on, but the computation will become more complicated as more structure is retained.

The first step in our approach to rephrase using abstract-algebraic objects arguably has roots dating back all the way to the proofs of the original sufficient conditions of Wang and Xu [54]. Those made use of the Smith normal form of the walk matrix in [54, Section 3], a perspective which has recently also been emphasized in work on refinements of the conditions by Qiu, Wang, and Zhang [37]. The Smith normal form of an integer matrix is equivalent to the Abelian group structure of its cokernel. However, [37, 54] mostly seem to have viewed the Smith normal form as a sequence of integers that provides more detailed information than the determinant. That the viewpoint of abstract-algebraic objects and  $\mathbb{Z}[x]$ -module structure is useful in probabilistic results stems from our previous work [46] with walk matrices for directed graphs; recall the discussion after Conjecture 1.4.

The second step of the approach is similar in spirit to the role of Gaussian ensembles in classical random matrix theory that are analytically tractable and enable detailed asymptotics for joint eigenvalue statistics, which can often be rigorously extended to other ensembles like random graphs by a universality argument; see e.g., [1, 16]. We are however concerned with arithmetical statistics such as square-freeness and random abstract-algebraic objects. Profinite ensembles with Haar distributed entries are the natural analogue for Gaussian ensembles in this arithmetical setting.

A related story can be found in the literature on *sandpile groups* of random graphs, which are the cokernels of Laplacian matrices. Motivated by experimental findings by Clancy, Leake, and Payne [12], those authors together with Kaplan and Wood [11] established rigorous results in analytically tractable  $p$ -adic random matrix models. The predictions following from those models were later shown to be correct for random graphs by universality arguments; see e.g., Wood [58], Nguyen and Wood [35], and Hodges [25]. In particular, the results in [11, 58] showed that the symmetry constraint on the Laplacian that comes from the graph being undirected has an important effect on

the distribution. As we discuss in Section 2, the profinite completion of  $\mathbb{Z}$  is closely related to the rings of  $p$ -adic integers. Hence, [11] can also be interpreted as a profinite symmetric model.

For random  $\mathbb{Z}[x]$ -modules associated to random matrices, all previous works that we are aware of have focused on settings without symmetry constraint. In particular, the module structure of the cokernel of  $P(\mathbf{M})$  when  $\mathbf{M}$  is a random matrix with independent entries and  $P \in \mathbb{Z}[x]$  is a polynomial has been considered by various authors; see e.g., [7, 8, 9, 10, 31, 43, 46]. A *linearization trick* is often used in that setting to reduce the study of the cokernel of the integer matrix  $P(\mathbf{M}) \in \mathbb{Z}^{n \times n}$  to that of the polynomial matrix  $\mathbf{M} - x\mathbf{I} \in \mathbb{Z}[x]^{n \times n}$ . We also use that trick in our arguments; see Section 2.1 as well as the discussion surrounding (3.3) and Remark 3.11.

The idea of our reduction approach exploiting invariance was sparked by proofs of Evans concerning Markovian structure in the Smith normal form of a random  $p$ -adic matrix without symmetries [17]. After using the method in the current paper, we have also found application of such invariance in cospectrality problems that are not directly related to sufficient conditions, such as the probability that  $\mathbf{Q}^\top \mathbf{M} \mathbf{Q} \in \mathbb{Z}^{n \times n}$  for a fixed rational matrix  $\mathbf{Q}$  when  $\mathbf{M}$  is a random symmetric integer matrix with sufficiently uniform entries; see Van Werde [48].

**1.3. On universality.** We believe that the considered statistics should not be too sensitive to the specific distribution of entries, so long as the key structure of the matrix is retained. Indeed, this belief is implicit in our approach, as it is what justifies passing to a different random matrix model.

Specifically, we expect that the limiting probabilities (1.2), (1.5), and (1.6) will be universal so long as the entries of the random matrix  $\mathbf{M}$  are not too concentrated on any residue class, in the sense of balanced distributions [59, Definition 1]. Such universality is known to hold in related models; see Van Werde [46, Theorem 1.3] for cokernels of walk matrices and Cheong and Yu for  $\mathbb{Z}[x]$ -module statistics [10, Theorem 1.3], both without symmetry constraint, and see Wood [58] for sandpile groups in a setting with symmetry. A sufficiently strong universality statement would make our conjectures into theorems, as our results for profinite models then identify the limiting law.

We intend to pursue such universality results in future work, but note that significant technical challenges remain to be resolved before a full proof of (1.3) and (1.7) could be expected. For instance, square-freeness depends on infinitely many primes simultaneously, which will likely necessitate separate methods to rule out large primes as certain universality techniques perform best when one only considers a finitely many primes simultaneously; see e.g., [35, Section 1.5] for discussion of such issues in the context of sandpile groups. In fact, even (1.2), (1.5), and (1.6) which only depend on a single integer prime  $p$  are deduced in our proofs by a decomposition in terms of the infinitely many maximal ideals of  $\mathbb{Z}[x]$  that contain  $p$ , and similar issues may be expected to arise. These challenges also remain open in the simpler setting of walk matrices of directed graphs; see [46, Conjecture 1.4].

Let us emphasize that the preceding discussion concerns universality with respect to the distribution of the entries. Structural changes to the random matrix, on the other hand, will often change the universality class. As was mentioned earlier, the prediction in (1.2) explicitly differs from our prior results in [46, Theorem 1.2] for walk matrices in a setting without symmetry constraint. That Conjectures 1.7 and 1.4 are stated for random graphs with self-loops is also no coincidence: the considered statistics are sensitive to the presence of a diagonal in the matrix. For instance, for graphs without self loops, it is known that the discriminant is always even [55, Section 5].

In the context of Conjecture 1.4, one may also wonder what happens if the vector  $\zeta$  is taken to be deterministic instead of random. The all-ones vector  $\zeta = (1, \dots, 1)^\top$  is particularly relevant, as this special case of  $\Phi$ -cospectrality has special historical interest. This case dates back to the 1980 work of Johnson and Newman [27], who viewed it as a natural generalization of adjacency cospectrality where the entries 0 and 1 in the adjacency matrix are replaced by formal symbols  $x, y \in \mathbb{R}$ . It is precisely this notion that was considered in the original conditions by Wang and Xu [54]. Remarkably, numerical evidence presented in Section 5 seems to suggest that the prediction in (1.2) for the probability that  $p^2$  divides the determinant is universal in terms of the vector  $\zeta$  for every deterministic  $\zeta$  whose reduction modulo  $p$  is nonzero, *except* for the all-ones vector when  $p = 2$ .

While the aforementioned exceptional phenomena surrounding the prime 2 go beyond the specific models studied here, they are not fundamentally beyond our two-step framework. We intend to pursue the relevant modifications of our framework in a future work.

1.4. **Outline.** Section 2 provides background, such as that surrounding profinite completions. Section 3 establishes equivalent phrasings of the conditions from Theorems 1.3 and 1.6 in terms of  $\mathbb{Z}[x]$ -module structure. We subsequently study the relevant  $\mathbb{Z}[x]$ -modules in a profinite random matrix ensemble in Section 4. Our main results are Theorems 4.11 and 4.17. We conclude in Section 5.

The subsections concerning the walk matrix and discriminant in Sections 3 and 4 can be read separately. While these parts are conceptually related, their logical treatment is mostly self-contained.

## 2. BACKGROUND AND NOTATION

The most natural way to state our subsequent rigorous results relies on concepts from arithmetic statistics and commutative algebra that are not so common in the areas of graph theory where the spectral characterization topic comes from. We here provide the required background.

2.1. **Definition and interpretation of cokernels.** In general, if  $R$  is a commutative ring and we are given a matrix  $X \in R^{n \times m}$  then the *cokernel* is the quotient  $R$ -module that measures to what extent  $X$  fails to be surjective as an  $R$ -module morphism onto  $R^n$ :

$$\text{coker}(X) := R^n / \text{Im}(X) \quad \text{where} \quad \text{Im}(X) := \{Xv : v \in R^m\}. \quad (2.1)$$

Given a matrix  $Z \in R^{n \times k}$  we denote  $\text{coker}(X, Z)$  for the cokernel of the  $n \times (m+k)$  rectangular matrix found by concatenating  $X$  and  $Z$ . If  $z \in R^k$  is a vector then we similarly write  $\text{coker}(X, z)$ .

Now introduce a formal symbol  $x$  and let  $R = \mathbb{Z}[x]$ . Given an integer matrix  $M \in \mathbb{Z}^{n \times n}$  it then holds that  $M - xI \in \mathbb{Z}[x]^{n \times n}$  where  $I \in \mathbb{Z}^{n \times n}$  is the identity matrix. In particular, we can consider the  $\mathbb{Z}[x]$ -module  $\text{coker}(M - xI)$ . To interpret this object, it is instructive to compare with another natural module associated to  $M$ . Consider the  $\mathbb{Z}[x]$ -module structure on  $\mathbb{Z}^n$  induced by the action of the matrix. That is, let  $Q(x)v := Q(M)v$  for every  $Q(x) \in \mathbb{Z}[x]$  and  $v \in \mathbb{Z}^n$ . One then has a natural map  $\mathbb{Z}^n \rightarrow \text{coker}(M - xI)$  found by composing the embedding  $\mathbb{Z}^n \rightarrow \mathbb{Z}[x]^n$  with the quotient map:

$$\begin{array}{ccccc} \mathbb{Z}^n & \longrightarrow & \mathbb{Z}[x]^n & \longrightarrow & \text{coker}(M - xI) \\ & & \searrow & \nearrow & \\ & & & & \end{array}$$

One can check that this composition defines a bijection and is compatible with the  $\mathbb{Z}[x]$ -module structures on  $\mathbb{Z}^n$  and  $\text{coker}(M - xI)$ . In other words, the  $\mathbb{Z}[x]$ -modules are isomorphic.

2.2. **Profinite completion and its Haar distribution.** Recall that we will take matrix entries from the uniform probability distribution on some larger space than  $\{0, 1\}$  to achieve analytical tractability. One natural idea would be to take  $\mathbb{Z}$  or  $\mathbb{Z}[x]$  as this space, but these are infinite countable sets and hence do not admit a uniform probability distribution. Finite quotients of these rings, on the other hand, do admit a uniform probability distribution and the distributions on different quotients are compatible in the sense that, for example, the uniform law on  $\mathbb{Z}/20\mathbb{Z}$  pushes forward to the uniform law on  $\mathbb{Z}/10\mathbb{Z}$  under the quotient map. This leads one to the *profinite completion*, which is an object that gathers all finite quotients and comes with a natural probability distribution.

Consider a commutative ring  $R$  and let  $\mathcal{F} := \{I \triangleleft R : \#R/I < \infty\}$  be the ideals of finite index. For any  $I, J \in \mathcal{F}$  with  $I \subseteq J$  let  $\varphi_{I,J} : R/I \rightarrow R/J$  be the quotient morphism. The *profinite completion* of  $R$  is the inverse limit of this system, which can be concretely realized defined as the subring of  $\prod_{I \in \mathcal{F}} R/I$  consisting of only those sequences that are compatible with the quotient morphisms  $\varphi_{I,J}$ :

$$\widehat{R} := \{(r_I)_{I \in \mathcal{F}} \in \prod_{I \in \mathcal{F}} R/I : \varphi_{I,J}(r_I) = r_J, \forall I \subseteq J\}. \quad (2.2)$$

We equip  $\widehat{R}$  with the subspace topology from  $\prod_{I \in \mathcal{F}} R/I$  where the latter carries the product topology of the discrete sets  $R/I$ . This makes  $(\widehat{R}, +)$  into a compact Hausdorff topological group. In particular, and this is the crucial fact for our purposes, there exists a unique Haar probability measure on  $\widehat{R}$ . The translation invariance of the latter implies that for every  $I \in \mathcal{F}$  and  $S \subseteq R/I$ ,

$$\text{Haar}(\{(r_J)_{J \in \mathcal{F}} : r_I \in S\}) = \frac{\#S}{\#R/I}. \quad (2.3)$$

In other words, the Haar measure pushes forward to the uniform law on the finite quotients of  $R/I$  under the projection. This recovers the aforementioned intuition that the profinite completion is the natural object that gathers all the finite quotients and their uniform laws. We refer to [40, 57] for additional background on profinite completions.

**Remark 2.1.** Another way to study the properties of a random elements of  $\mathbb{Z}$  is to consider the limiting behavior of the uniform probability measures  $\mu_n$  on  $[-n, n] \cap \mathbb{Z}$ . This perspectives is equivalent to considering the Haar measure on  $\widehat{\mathbb{Z}}$  for properties that only depends on the residue of the random integer modulo some fixed  $k$ , due to (2.3). What makes the profinite completion particularly convenient, however, is that its Haar distribution remains tractable for properties depending on infinitely many different residues. This is more delicate for  $\mu_n$  since the law is far from uniform on  $\mathbb{Z}/k_n\mathbb{Z}$  for large  $k_n \gg n$ . Analogous comments apply to  $\mathbb{Z}[x]$  when one considers random polynomials with sufficiently uniform coefficients and diverging degree.

2.2.1. *On the special cases  $\mathbb{Z}$  and  $\mathbb{Z}[x]$ .* Our subsequent results will concern the profinite completions of specific rings, particularly  $\mathbb{Z}[x]$ , and more concrete descriptions can be given. If one prefers, one could alternatively adopt the following equivalent formulations as the definitions and simply remember from the above why these are natural settings.

For  $R = \mathbb{Z}$ , it follows from the Chinese remainder theorem that  $\widehat{\mathbb{Z}} \cong \prod_{\text{primes } p} \mathbb{Z}_p$  where  $\mathbb{Z}_p$  is the ring of  $p$ -adic integers associated to the prime  $p$ . The  $p$ -adic integers can be identified with formal power series in the variable  $p$  with coefficients in  $\{0, \dots, p-1\}$ :

$$\mathbb{Z}_p := \left\{ \sum_{i=0}^{\infty} c_i p^i : c_i \in \{0, 1, \dots, p-1\} \right\}. \quad (2.4)$$

Addition and multiplication is done with overflow on coefficients being carried to higher powers of  $p$ . The  $p$ -adic integers admit a unique Haar probability measure that corresponds to sampling independent uniform random coefficients: it holds for  $H_p \sim \text{Haar}(\mathbb{Z}_p)$  that

$$H_p = \sum_{i=0}^{\infty} C_i p^i \quad \text{where } C_i \sim \text{Unif}\{0, 1, \dots, p-1\}. \quad (2.5)$$

Under the isomorphism  $\widehat{\mathbb{Z}} \cong \prod_p \mathbb{Z}_p$ , a Haar random element of  $\widehat{\mathbb{Z}}$  corresponds to sampling independent elements from the Haar measures on the different factors:

$$\text{Haar}(\widehat{\mathbb{Z}}) = \otimes_{\text{primes } p} \text{Haar}(\mathbb{Z}_p). \quad (2.6)$$

The reader is referred to the books [22, 29, 41] for additional background.

In greater generality, the role of the  $p$ -adic integers may be replaced by the  $\mathfrak{m}$ -adic completions<sup>1</sup> at maximal ideals  $\mathfrak{m} \subseteq R$ . (See e.g., [26, §2.1] for such a statement for arbitrary finitely generated rings.) The maximal ideals of  $\mathbb{Z}[x]$  are  $\mathfrak{m} = p\mathbb{Z}[x] + \beta(x)\mathbb{Z}[x]$  with  $p \in \mathbb{Z}$  a prime and  $\beta \in \mathbb{Z}[x]$  a monic polynomial of degree  $\geq 1$  whose reduction modulo  $p$  is irreducible in  $\mathbb{F}_p[x]$ ; see [39, p.22]. Thus, one has the following explicit description in the case of  $R = \mathbb{Z}[x]$ :

$$\widehat{R} \cong \prod_p \prod_{\beta(x)} R_{p,\beta} \quad \text{with } R_{p,\beta} := \left\{ \sum_{i=0}^{\infty} c_i \beta^i : c_i \in \mathbb{Z}_p[x] \text{ with } \deg(c_i) < \deg(\beta) \right\}, \quad (2.7)$$

where the products correspond to the distinct maximal ideals, meaning that the second product has as many factors as there are irreducible monic polynomial in  $\mathbb{F}_p[x]$ . Multiplication in  $R_{p,\beta}$  is done with overflow on the degree of the polynomial coefficients being carried to higher powers of  $\beta$ . (In other words,  $R_{p,\beta}$  is isomorphic as a ring to the quotient of  $\mathbb{Z}_p[x][[y]]$  by the ideal generated by  $y - \beta(x)$ .) A random element  $H_{p,\beta} \sim \text{Haar}(R_{p,\beta})$  can be generated using independent coefficients:

$$H_{p,\beta} = \sum_{i=0}^{\infty} c_i \beta^i \quad \text{where } c_i = \sum_{j=0}^{\deg(\beta)-1} C_{i,j} x^j \quad \text{with } C_{i,j} \sim \text{Haar}(\mathbb{Z}_p). \quad (2.8)$$

A Haar random element under the isomorphism  $\widehat{R} \cong \prod_{p,\beta(x)} R_{p,\beta}$  corresponds to sampling independent elements from the Haar measures on the different factors, similar to (2.6).

**2.3. Pieces of modules and relevant properties.** Given an Abelian group  $G$  and a  $\mathbb{Z}[x]$ -module  $\mathcal{M}$  we introduce the following notation:

$$G_p := G \otimes_{\mathbb{Z}} \mathbb{Z}_p \quad \text{and} \quad \mathcal{M}_{p,\beta} := \mathcal{M} \otimes_{\mathbb{Z}[x]} R_{p,\beta}. \quad (2.9)$$

Here,  $\otimes_{\mathbb{Z}}$  and  $\otimes_{\mathbb{Z}[x]}$  refer to tensor products of Abelian groups or  $\mathbb{Z}[x]$ -modules, respectively. The subscript  $\mathbb{Z}$  reflects that Abelian groups are exactly the same object as  $\mathbb{Z}$ -modules.

Concrete calculations for the group operation can be done using that every finitely generated Abelian group is a direct sum of cyclic groups by the classification theorem together with the following standard fact:

<sup>1</sup>Here, the  $\mathfrak{m}$ -adic completion of a ring is defined similar to (2.2) except that we now consider the inverse limit of the system  $R/\mathfrak{m}^n$ . We refer to [3, Chapter 10] and [15, Chapter 7] for additional background.

**Lemma 2.2.** *Suppose that  $G \cong \bigoplus_{i=1}^m (\mathbb{Z}/k_i\mathbb{Z})$  for  $k_1, \dots, k_m \geq 0$ . Then,  $G_p \cong \bigoplus_{i=1}^m (\mathbb{Z}/p^{e_i}\mathbb{Z})$  with  $e_i := \sup\{j \geq 0 : p^j \mid k_i\}$ . Here, it is to be understood that  $\mathbb{Z}/p^\infty\mathbb{Z} := \mathbb{Z}_p$  when  $k_i = 0$ .*

*Proof.* Note that  $(\mathbb{Z}/p^{e_i}\mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Z}_p \cong \mathbb{Z}/p^{e_i}\mathbb{Z}$ . Further, any integer  $k' \geq 1$  that is coprime with  $p$  is invertible in  $\mathbb{Z}_p$  [41, §1.5], implying that  $(\mathbb{Z}/k'\mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Z}_p = 0$  if  $k' \not\equiv 0 \pmod{p}$ . The claim now follows from the Chinese remainder theorem since tensor products distribute over direct sums.  $\square$

In particular, Lemma 2.2 implies that every finite Abelian group satisfies  $G \cong \bigoplus_{\text{primes } p} G_p$ . A related decomposition result for modules that are finitely generated as groups (but not necessarily finite) is given by the following Lemma 2.3:

**Lemma 2.3.** *Consider a  $\mathbb{Z}[x]$ -module  $\mathcal{M}$  which is finitely generated as an Abelian group. Then, it holds for every prime  $p$  that  $\mathcal{M}_p \cong \bigoplus_{\beta} \mathcal{M}_{p,\beta}$  as  $\mathbb{Z}[x]$ -modules, where the direct sum runs over representatives in  $\mathbb{Z}[x]$  of the irreducible monic polynomials in  $\mathbb{F}_p[x]$ .*

A proof for Lemma 2.3 can be found in Appendix A.

### 3. REPHRASING CONDITIONS USING THE $\mathbb{Z}[x]$ -MODULE STRUCTURE OF $\text{coker}(\mathbf{M} - x\mathbf{I})$

We now consider the first step of the approach outlined in Section 1.2 and rephrase the sufficient conditions in terms of module-theoretic data. The condition from Theorem 1.3 is rephrased in Proposition 3.2 and the condition from Theorem 1.6 is considered in Propositions 3.8 and 3.10.

Throughout this section we let  $\zeta \in \mathbb{Z}^n$  be an integer vector and we consider an integer matrix  $\mathbf{M} \in \mathbb{Z}^{n \times n}$ . The results of the current section do not require  $\mathbf{M}$  to be symmetric. The symbol  $p$  will always refer to a prime number.

**3.1. Regarding the walk matrix.** Note that the walk matrix  $\mathbf{W} = [\zeta, \mathbf{M}\zeta, \dots, \mathbf{M}^{n-1}\zeta]$  has integer entries. In particular, since  $\mathbb{Z}$ -modules are just Abelian groups, we may consider  $\text{coker}(\mathbf{W})$  as a group. A group-theoretic rephrasing of the sufficient conditions similar to the following one was also considered in [46]. Readers consulting that previous work are warned, however, that our notation  $G_p$  from (2.9) differs from the notation used in [46].

**Lemma 3.1.** *It holds that  $p^2 \nmid \det(\mathbf{W})$  if and only if  $\text{coker}(\mathbf{W})_p$  is the trivial group or  $\mathbb{Z}/p\mathbb{Z}$ .*

*Proof.* Let  $\mathbf{W} = \mathbf{U}\mathbf{D}\mathbf{V}$  be the Smith normal form. This means that  $\mathbf{U}, \mathbf{V} \in \mathbb{Z}^{n \times n}$  are integer matrices with  $\det(\mathbf{U}), \det(\mathbf{V}) \in \{-1, +1\}$  and  $\mathbf{D} = \text{diag}(d_1, \dots, d_n)$  is a diagonal matrix with integer entries  $d_i \in \mathbb{Z}$  satisfying  $d_i \mid d_{i+1}$  for every  $i \geq 1$ . Note that  $\det(\mathbf{W}) = \pm \prod_{i=1}^n d_i$ . Consequently, it holds that  $p^2 \nmid \det(\mathbf{W})$  if and only if  $p \nmid d_{n-1}$  and  $p^2 \nmid d_n$ .

The constraint on the determinant of  $\mathbf{U}$  and  $\mathbf{V}$  means that these matrices are invertible over the integers. In particular,  $\text{Im}(\mathbf{W}) = \text{Im}(\mathbf{U}\mathbf{D})$ . Now, recalling the definition of the cokernel from (2.1),

$$\text{coker}(\mathbf{W}) = \mathbb{Z}^n / \text{Im}(\mathbf{U}\mathbf{D}) \cong \text{coker}(\mathbf{D}) \cong \bigoplus_{i=1}^n \mathbb{Z}/d_i\mathbb{Z}, \quad (3.1)$$

where the isomorphism  $\mathbb{Z}^n / \text{Im}(\mathbf{U}\mathbf{D}) \cong \text{coker}(\mathbf{D})$  uses that the map  $z \mapsto \mathbf{U}^{-1}z$  on  $\mathbb{Z}^n$  sends  $\text{Im}(\mathbf{U}\mathbf{D})$  to  $\text{Im}(\mathbf{D})$ . Use Lemma 2.2 to conclude that  $p^2 \nmid \det(\mathbf{W})$  if and only if  $\text{coker}(\mathbf{W})_p \in \{0, \mathbb{Z}/p\mathbb{Z}\}$ .  $\square$

Note that if  $\mathbb{Z}^n$  is equipped with the  $\mathbb{Z}[x]$ -module structure induced by the action of  $\mathbf{M}$  as in Section 2.1 then the image of  $\mathbf{W}$  is exactly the  $\mathbb{Z}[x]$ -submodule generated by the vector  $\zeta$ :

$$\text{Im}(\mathbf{W}) = \{\mathbf{W}v : v \in \mathbb{Z}^n\} = \{\sum_{i=0}^{n-1} v_i \mathbf{M}^i \zeta : v_i \in \mathbb{Z}\} = \{Q(\mathbf{M})\zeta : Q \in \mathbb{Z}[x]\}, \quad (3.2)$$

where the final equality uses that  $\mathbf{M}^n = \sum_{i=0}^{n-1} c_i \mathbf{M}^i$  for certain  $c_i \in \mathbb{Z}$  due to the Cayley–Hamilton theorem. It follows that the quotient  $\text{coker}(\mathbf{W}) = \mathbb{Z}^n / \text{Im}(\mathbf{W})$  is not only an Abelian group but also canonically equipped with the structure of a  $\mathbb{Z}[x]$ -module. Moreover, as  $\mathbb{Z}[x]$ -modules,

$$\text{coker}(\mathbf{W}) = \frac{\mathbb{Z}^n}{\text{Im}(\mathbf{W})} \cong \frac{\mathbb{Z}[x]^n}{\text{Im}(\mathbf{M} - x\mathbf{I}) + \mathbb{Z}[x]\zeta} = \text{coker}(\mathbf{M} - x\mathbf{I}, \zeta), \quad (3.3)$$

where we consider  $[\mathbf{M} - x\mathbf{I}, \zeta]$  as a rectangular matrix over  $\mathbb{Z}[x]$  in the final equality.

To understand why (3.3) is useful, note that the entries of  $\mathbf{W}$  are nontrivial algebraic combinations of those of  $\mathbf{M}$  and  $\zeta$  which would complicate direct study of  $\text{coker}(\mathbf{W})$ . On the other hand,  $\text{coker}(\mathbf{M} - x\mathbf{I}, \zeta)$  refers directly to  $\mathbf{M}$  and  $\zeta$  in a linear way.

We can refine the group-theoretic formulation from Lemma 3.1 by considering the admissible  $\mathbb{Z}[x]$ -module structures:

**Proposition 3.2.** *It holds that  $p^2 \nmid \det(\mathbf{W})$  if and only if one of the following two events occurs:*

- (1) *It holds that  $\text{coker}(\mathbf{M} - x\mathbf{I}, \zeta)_{p,\beta} \cong 0$  for all monic  $\beta(x) \in \mathbb{Z}[x]$  with irreducible reduction in  $\mathbb{F}_p[x]$ .*
- (2) *Or, there exists  $a \in \mathbb{Z}$  such that one has an isomorphism of  $\mathbb{Z}[x]$ -modules*

$$\text{coker}(\mathbf{M} - x\mathbf{I}, \zeta)_{p,x-a} \cong \mathbb{F}_p[x]/(x-a)\mathbb{F}_p[x], \quad (3.4)$$

*and it holds that  $\text{coker}(\mathbf{M} - x\mathbf{I}, \zeta)_{p,\beta} \cong 0$  for every  $\beta \not\equiv x - a \pmod{p}$ .*

*Proof.* Note that a  $\mathbb{Z}[x]$ -module  $\mathcal{M}$  satisfies  $\mathcal{M}_p \cong \mathbb{Z}/p\mathbb{Z}$  as a group (resp.  $\mathcal{M}_p \cong 0$ ) if and only if  $\mathcal{M}_p \cong \mathbb{F}_p[x]/(x-a)\mathbb{F}_p[x]$  as a module for some  $a \in \mathbb{Z}$  (resp. if and only if it is the zero module). The result is hence immediate from (3.3) and Lemmas 2.3 and 3.1.  $\square$

To understand how often the determinant of the walk matrix is square-free, it now suffices to study the  $\mathbb{Z}[x]$ -module  $\text{coker}(\mathbf{M} - x\mathbf{I}, \zeta)$ . This is done in Section 4.3 for a model where  $\mathbf{M}$  and  $\zeta$  are both taken to have Haar random entries on the profinite completion of  $\mathbb{Z}[x]$ .

**3.2. Regarding the discriminant.** We next rephrase the condition from Theorem 1.6 based on the discriminant in terms of  $\text{coker}(\mathbf{M} - x\mathbf{I})$ . We start in Section 3.2.1 by rephrasing the event where  $p^2$  divides the discriminant in terms of the factorization of the polynomial. A rephrasing in terms of the cokernel is next given in Section 3.2.2.

**3.2.1. Preliminaries.** Consider the  $\mathbb{Z}$ -module of polynomials with degree strictly smaller than  $i \geq 1$ :

$$\mathcal{P}_i := \{f(x) \in \mathbb{Z}[x] : \deg(f) < i\}. \quad (3.5)$$

Given  $\phi, \psi \in \mathbb{Z}[x]$ , we define the *Sylvester map* to be the  $\mathbb{Z}$ -module morphism specified by

$$\mathcal{S}_{\phi,\psi} : \mathcal{P}_{\deg(\psi)} \oplus \mathcal{P}_{\deg(\phi)} \rightarrow \mathcal{P}_{\deg(\psi)+\deg(\phi)} : (f, g) \mapsto f\phi + g\psi. \quad (3.6)$$

If one uses the monomials  $1, x, x^2, \dots$  as a basis for  $\mathcal{P}_i$  then one can represent  $\mathcal{S}_{\phi,\psi}$  as a square matrix whose entries are the coefficients of  $\phi$  and  $\psi$  with shifts from one row to the next; see e.g., [55, §2.3]. The determinant in this basis is usually called the *resultant of  $\phi$  and  $\psi$* :

$$\text{Res}(\phi, \psi) := \det(\mathcal{S}_{\phi,\psi}). \quad (3.7)$$

A different choice of  $\mathbb{Z}$ -module basis for the domain and codomain can change the determinant, but only by a factor  $\pm 1$ . Ambiguity up to a unit will not matter for us, so we may simply refer to the determinant of the Sylvester map for a canonical perspective. The relevance for our purposes occurs when the second polynomial is the derivative of the first:

**Definition 3.3.** Consider a monic polynomial  $\phi \in \mathbb{Z}[x]$  with degree no less than one. Then, the resultant of  $\phi$  and its formal derivative  $\phi'$  is called its *discriminant* and is denoted  $\Delta_\phi := \text{Res}(\phi, \phi')$ .

It may be shown that Definition 3.3 is equivalent to the formula in terms of roots given in (1.4). We will not need that formula but refer the interested reader to [20, Chapter 12].

Definition 3.3 implies that the discriminant of an integer polynomial is divisible by  $p$  if and only if the Sylvester map of  $\phi$  and  $\phi'$  is singular over  $\mathbb{F}_p$ . In this context, note that if  $\mathbb{K}$  is a field, then Bézout's identity in principle ideal domain  $\mathbb{K}[x]$  states that for every  $\phi, \psi \in \mathbb{K}[x]$ ,

$$\{f(x)\phi(x) + g(x)\psi : f(x), g(x) \in \mathbb{K}[x]\} = \{h(x) \text{gcd}(\phi, \psi) : h(x) \in \mathbb{K}[x]\}. \quad (3.8)$$

In particular, the Sylvester map is nonsingular modulo  $p$  if and only if the polynomials  $\phi$  and  $\psi$  are coprime over  $\mathbb{F}_p$ . (We here use that a linear transformation is nonsingular if and only if it is surjective.) This yields the following classical Proposition 3.4. A polynomial  $\phi \in \mathbb{F}_p[x]$  is said to be *square-free* if there does not exist any irreducible  $\beta \in \mathbb{F}_p[x]$  with  $\deg(\beta) \geq 1$  and  $\beta^2 \mid \phi$ .

**Proposition 3.4.** *Consider some monic  $\phi \in \mathbb{Z}[x]$  with  $\deg(\phi) \geq 1$ . Then,  $p \nmid \Delta_\phi$  if and only if  $\phi \pmod{p}$  is square-free over  $\mathbb{F}_p$ .*

*Proof.* Let  $\phi \equiv \prod_i \beta_i(x)^{n_i} \pmod{p}$  be the factorization of  $\phi$  into powers of distinct irreducible monic polynomials  $\beta_i \in \mathbb{F}_p[x]$ . Then,  $\phi' = \sum_i n_i \beta_i(x)^{n_i-1} \beta_i'(x) \prod_{j \neq i} \beta_j(x)^{n_j}$  and we observe that  $\beta_i \mid \phi'$  if and only if  $n_i \geq 2$ . Thus,  $\text{gcd}(\phi, \phi') = 1$  if and only if  $\phi$  is not divisible by  $\beta^2$  for all irreducible  $\beta$ . In other words, the Sylvester map is nonsingular modulo  $p$  if and only if  $\phi$  is square-free.  $\square$

An integer  $d \in \mathbb{Z}$  is said to be *exactly divisible by  $p$* , denoted  $p \parallel d$ , if  $p \mid d$  but  $p^2 \nmid d$ . A proof of the following characterization of the event where the discriminant is exactly divisible by an odd prime can be found in work of Ash, Brackenhoff, and Zarrabi [2, Proposition 6.7]. One of the implications also appears in the proof of the sufficient condition Theorem 1.6 by Wang and Yu [55, Section 4] with a different argument that relies on a direct analysis of the Sylvester map.

**Proposition 3.5** ([2, 55]). *Consider an odd prime  $p$  and a monic polynomial  $\phi \in \mathbb{Z}[x]$  with  $\deg(\phi) \geq 1$ . Then, it holds that  $p \parallel \Delta_\phi$  if and only if there exists some  $a \in \mathbb{Z}$  and a square-free polynomial  $\xi \in \mathbb{F}_p[x]$  with  $\xi(a) \not\equiv 0 \pmod{p}$  such that  $\phi(x) \equiv (x-a)^2 \xi(x) \pmod{p}$  and  $p^2 \nmid \phi(a)$ .*

**Remark 3.6.** A priori, the event in Proposition 3.5 depends on  $a \pmod{p^2}$  but [2, Proposition 6.7] shows that it actually only depends on the reduction modulo  $p$ . That is, if  $\phi(x) \equiv (x-a)^2 \xi(x) \pmod{p}$  for square-free  $\xi$  with  $\xi(a) \not\equiv 0 \pmod{p}$  and  $p^2 \nmid \phi(a)$ , then  $p^2 \nmid \phi(b)$  for all  $b \equiv a \pmod{p}$ .

3.2.2. *Connection to the cokernel.* We next rephrase Propositions 3.4 and 3.5 in terms of  $\text{coker}(\mathbf{M} - x\mathbf{I})$  in Propositions 3.8 and 3.10, respectively. The proofs rely on the following Lemma 3.7.

The *length* of a module  $\mathcal{N}$  over a ring  $R$  is the maximal length of a chain of proper submodules:

$$\text{Length}_R(\mathcal{N}) := \sup\{L \geq 1 : \exists \mathcal{N}_0 \subsetneq \mathcal{N}_1 \subsetneq \dots \subsetneq \mathcal{N}_L \text{ with } \mathcal{N}_0 = 0 \text{ and } \mathcal{N}_L = \mathcal{N}\}. \quad (3.9)$$

**Lemma 3.7.** *Fix a monic polynomial  $\beta \in \mathbb{Z}[x]$  with  $\deg(\beta) \geq 1$  and irreducible reduction in  $\mathbb{F}_p$ . Then,*

$$\max\{k \geq 0 : \beta(x)^k \mid \varphi_{\mathbf{M}}(x) \pmod{p}\} = \text{Length}_{R_{p,\beta}/pR_{p,\beta}}\left(\text{coker}\left(\frac{(\mathbf{M} - x\mathbf{I})_{p,\beta}}{p \text{coker}(\mathbf{M} - x\mathbf{I})_{p,\beta}}\right)\right). \quad (3.10)$$

*Proof.* Consider the factorization  $\varphi_{\mathbf{M}}(x) \equiv \prod_i \beta_i^{k_i} \pmod{p}$  of the characteristic polynomial into powers of distinct irreducible monic polynomials  $\beta_i \in \mathbb{F}_p[x]$ . Then, the rational canonical form [14, §12.2] of  $\bar{\mathbf{M}} := \mathbf{M} \pmod{p}$  over  $\mathbb{F}_p$  yields nonnegative integers  $\lambda_{i,j} \geq 0$  with  $\sum_j \lambda_{i,j} = k_i$  and

$$\frac{\text{coker}(\mathbf{M} - x\mathbf{I})}{p \text{coker}(\mathbf{M} - x\mathbf{I})} \cong \text{coker}(\bar{\mathbf{M}} - x\mathbf{I}) \cong \prod_i \prod_j \frac{\mathbb{F}_p[x]}{\beta_i^{\lambda_{i,j}} \mathbb{F}_p[x]}. \quad (3.11)$$

It follows directly from the definition of  $R_{p,\beta}$  that  $(\mathbb{F}_p[x]/\beta^\lambda \mathbb{F}_p[x]) \otimes_{\mathbb{Z}[x]} R_{p,\beta} = \mathbb{F}_p[x]/\beta^\lambda \mathbb{F}_p[x]$ . Further,  $(\mathbb{F}_p[x]/\gamma^\lambda \mathbb{F}_p[x]) \otimes_{\mathbb{Z}[x]} R_{p,\beta} = 0$  for  $\gamma$  with coprime reduction to  $\beta$ . (The latter can be shown using that  $\beta^\lambda$  is then invertible in  $R_{p,\gamma}$ , or as a consequence of the previous sentence with  $\gamma = \beta$  and Lemma 2.3.) Hence, taking a tensor product with  $R_{p,\beta_i}$  in (3.11),

$$\frac{\text{coker}(\mathbf{M} - x\mathbf{I})_{p,\beta_i}}{p \text{coker}(\mathbf{M} - x\mathbf{I})_{p,\beta_i}} \cong \prod_j \frac{\mathbb{F}_p[x]}{\beta_i^{\lambda_{i,j}} \mathbb{F}_p[x]}. \quad (3.12)$$

Note that  $\text{Length}_R(\prod_j \mathcal{N}_j) = \sum_j \text{Length}_R(\mathcal{N}_j)$  for any finite product of  $R$ -modules. Further, the submodules of  $\mathcal{N} := \mathbb{F}_p[x]/\beta^\lambda \mathbb{F}_p[x]$  are  $\beta^j \mathcal{N}$  and consequently  $\text{Length}_{R_{p,\beta}/pR_{p,\beta}}(\mathcal{N}) = \lambda$ . Hence, using that  $\sum_j \lambda_{i,j} = k_i$  with  $k_i$  the power of  $\beta_i$  in the factorization of  $\varphi_{\mathbf{M}}$  yields (3.10).  $\square$

**Proposition 3.8.** *It holds that  $p \nmid \Delta_{\mathbf{M}}$  if and only if it holds for all monic  $\beta(x) \in \mathbb{Z}[x]$  with irreducible reduction in  $\mathbb{F}_p[x]$  that, as  $\mathbb{Z}[x]$ -modules,*

$$\frac{\text{coker}(\mathbf{M} - x\mathbf{I})_{p,\beta}}{p \text{coker}(\mathbf{M} - x\mathbf{I})_{p,\beta}} \cong 0 \quad \text{or} \quad \frac{\text{coker}(\mathbf{M} - x\mathbf{I})_{p,\beta}}{p \text{coker}(\mathbf{M} - x\mathbf{I})_{p,\beta}} \cong \frac{\mathbb{F}_p[x]}{\beta(x) \mathbb{F}_p[x]}. \quad (3.13)$$

*Proof.* Recall from Proposition 3.4 that  $p \nmid \Delta_{\mathbf{M}}$  if and only if  $\beta^2 \nmid \varphi_{\mathbf{M}} \pmod{p}$  for all irreducible  $\beta \in \mathbb{F}_p[x]$ . The result is hence immediate from Lemma 3.7. Indeed, recall that  $\text{coker}(\mathbf{M} - x\mathbf{I})_{p,\beta}/p \text{coker}(\mathbf{M} - x\mathbf{I})_{p,\beta}$  has the form (3.12) and note that the modules of length  $< 2$  are those in (3.13).  $\square$

**Lemma 3.9.** *It holds that  $p \parallel \det(\mathbf{M} - a\mathbf{I})$  for  $a \in \mathbb{Z}$  if and only if as  $\mathbb{Z}[x]$ -modules,*

$$\frac{\text{coker}(\mathbf{M} - x\mathbf{I})_{p,x-a}}{(x-a) \text{coker}(\mathbf{M} - x\mathbf{I})_{p,x-a}} \cong \frac{\mathbb{F}_p[x]}{(x-a) \mathbb{F}_p[x]} \quad (3.14)$$

*Proof.* It holds for any integer matrix  $\mathbf{N} \in \mathbb{Z}^{n \times n}$  that  $|\det(\mathbf{N})| = \# \text{coker}(\mathbf{N})$ . Indeed, this may be verified by considering the Smith normal form, similar to the proof of Lemma 3.1. Hence, it follows from Lemma 2.2 that  $p \parallel \det(\mathbf{N})$  if and only if  $\text{coker}(\mathbf{N})_p \cong \mathbb{F}_p$  as a group. It remains to show that  $\text{coker}(\mathbf{M} - a\mathbf{I})_p \cong \mathbb{F}_p$  as groups if and only if (3.14) holds.

Note that we have an isomorphism of groups  $\text{coker}(\mathbf{M} - a\mathbf{I}) \cong \text{coker}(\mathbf{M} - x\mathbf{I}) / (x - a) \text{coker}(\mathbf{M} - x\mathbf{I})$ . Hence, using the associativity of tensor products,

$$\text{coker}(\mathbf{M} - a\mathbf{I}) \otimes_{\mathbb{Z}} \mathbb{Z}_p \cong \text{coker}(\mathbf{M} - x\mathbf{I}) \otimes_{\mathbb{Z}[x]} \frac{\mathbb{Z}_p[x]}{(x - a)\mathbb{Z}_p[x]}. \quad (3.15)$$

It follows directly from the definition (2.7) that  $\mathbb{Z}_p[x]/(x - a)\mathbb{Z}_p[x]$  is a quotient of  $R_{p,x-a}$ . In particular,  $\mathbb{Z}_p[x]/(x - a)\mathbb{Z}_p[x] \cong R_{p,x-a} \otimes_{R_{p,x-a}} (\mathbb{Z}_p[x]/(x - a)\mathbb{Z}_p[x])$ . Hence, again using the associativity of tensor products and recalling the definition (2.9),

$$\text{coker}(\mathbf{M} - x\mathbf{I}) \otimes_{\mathbb{Z}[x]} \frac{\mathbb{Z}_p[x]}{(x - a)\mathbb{Z}_p[x]} \cong \text{coker}(\mathbf{M} - x\mathbf{I})_{p,x-a} \otimes_{R_{p,x-a}} \frac{\mathbb{Z}_p[x]}{(x - a)\mathbb{Z}_p[x]}. \quad (3.16)$$

Combining (3.15) and (3.16) with the definition (2.9), we have the following isomorphism of groups:

$$\text{coker}(\mathbf{M} - a\mathbf{I})_p \cong \frac{\text{coker}(\mathbf{M} - x\mathbf{I})_{p,x-a}}{(x - a) \text{coker}(\mathbf{M} - x\mathbf{I})_{p,x-a}}. \quad (3.17)$$

Note that the unique  $\mathbb{Z}[x]$ -module structure on the group  $\mathbb{F}_p$  such that  $x$  acts as multiplication by  $a$  is given by  $\mathbb{F}_p[x]/(x - a)\mathbb{F}_p[x]$ . It hence follows from (3.17) that  $\text{coker}(\mathbf{M} - a\mathbf{I})_p \cong \mathbb{F}_p$  as a group if and only if (3.14) occurs, concluding the proof.  $\square$

**Proposition 3.10.** *Consider an odd prime  $p$ . Then, it holds that  $p \parallel \Delta_{\mathbf{M}}$  if and only if there exists  $a \in \mathbb{Z}$  such that (3.13) is satisfied for every  $\beta \not\equiv x - a \pmod{p}$  and it holds that, as  $\mathbb{Z}[x]$ -modules,*

$$\frac{\text{coker}(\mathbf{M} - x\mathbf{I})_{p,x-a}}{p \text{coker}(\mathbf{M} - x\mathbf{I})_{p,x-a}} \cong \frac{\mathbb{F}_p[x]}{(x - a)^2 \mathbb{F}_p[x]} \quad \text{and} \quad \frac{\text{coker}(\mathbf{M} - x\mathbf{I})_{p,x-a}}{(x - a) \text{coker}(\mathbf{M} - x\mathbf{I})_{p,x-a}} \cong \frac{\mathbb{F}_p[x]}{(x - a)\mathbb{F}_p[x]}. \quad (3.18)$$

*Proof.* Recall that Proposition 3.5 states that  $p \parallel \Delta_{\mathbf{M}}$  if and only if there exists  $a \in \mathbb{Z}$  with  $p \parallel \varphi_{\mathbf{M}}(a)$  such that  $\varphi_{\mathbf{M}}(x) \equiv (x - a)^2 \xi(x) \pmod{p}$  for square-free  $\xi \in \mathbb{F}_p[x]$  with  $\xi(a) \not\equiv 0 \pmod{p}$ . Here, as in the proof of Proposition 3.8 we have that (3.13) holds if and only if  $\beta^2 \nmid \varphi_{\mathbf{M}} \pmod{p}$ . It hence remains to argue that (3.18) is equivalent to having  $p \parallel \varphi_{\mathbf{M}}(a)$  and  $\max\{k \geq 0 : (x - a)^k \mid \varphi_{\mathbf{M}} \pmod{p}\} = 2$ .

Lemma 3.7 yields that  $\max\{k \geq 0 : (x - a)^k \mid \varphi_{\mathbf{M}} \pmod{p}\} = 2$  if and only if

$$\frac{\text{coker}(\mathbf{M} - x\mathbf{I})_{p,x-a}}{p \text{coker}(\mathbf{M} - x\mathbf{I})_{p,x-a}} \cong \left( \frac{\mathbb{F}_p[x]}{(x - a)\mathbb{F}_p[x]} \right)^2 \quad \text{or} \quad \frac{\text{coker}(\mathbf{M} - x\mathbf{I})_{p,x-a}}{p \text{coker}(\mathbf{M} - x\mathbf{I})_{p,x-a}} \cong \frac{\mathbb{F}_p[x]}{(x - a)^2 \mathbb{F}_p[x]}. \quad (3.19)$$

Moreover, recall from Lemma 3.9 that  $p \parallel \varphi_{\mathbf{M}}(a)$  if and only if

$$\frac{\text{coker}(\mathbf{M} - x\mathbf{I})_{p,x-a}}{(x - a) \text{coker}(\mathbf{M} - x\mathbf{I})_{p,x-a}} \cong \frac{\mathbb{F}_p[x]}{(x - a)\mathbb{F}_p[x]}. \quad (3.20)$$

It hence remains to show that a  $R_{p,x-a}$ -module  $N$  cannot simultaneously satisfy  $N/pN \cong (\mathbb{F}[x]/(x - a)\mathbb{F}_p[x])^2$  and  $N/(x - a)N \cong \mathbb{F}_p[x]/(x - a)\mathbb{F}_p[x]$ . Indeed, if such a module were to exist, then taking additional quotients would yield that  $N/(pN + (x - a)N) \cong (\mathbb{F}[x]/(x - a)\mathbb{F}_p[x])^2$  and  $N/(x - a)N / (pN + (x - a)N) \cong \mathbb{F}_p[x]/(x - a)\mathbb{F}_p[x]$ , a contradiction. This concludes the proof.  $\square$

**Remark 3.11.** There are also different ways to relate the discriminant to cokernels:

- (1) It follows from (3.7) and Definition 3.3 that  $|\Delta_{\phi}| = \# \text{coker}(\mathcal{S}_{\phi, \phi'})$ .
- (2) It follows from (1.4) that  $\Delta_{\mathbf{M}} = \det(\varphi'_{\mathbf{M}}(\mathbf{M}))$  with  $\varphi'_{\mathbf{M}} \in \mathbb{Z}[x]$  the derivative of the characteristic polynomial. This implies that  $|\Delta_{\mathbf{M}}| = \# \text{coker}(\varphi'_{\mathbf{M}}(\mathbf{M}))$ .

It unclear whether these alternative perspectives are helpful in probabilistic study. For instance, while the law of  $\text{coker}(P(\mathbf{M}))$  with  $P \in \mathbb{Z}[x]$  deterministic has been studied in the previous works (recall Section 1.3), the polynomial  $\varphi'_{\mathbf{M}}$  has nontrivial dependence on  $\mathbf{M}$ . Propositions 3.8 and 3.10 have the advantage that they depend on  $\mathbf{M}$  in a linear way.

#### 4. MODULE STATISTICS FOR PROFINITE RANDOM MATRIX ENSEMBLES

We found in Section 3 that a unifying feature of the sufficient conditions in Theorems 1.3 and 1.6 is that they can both be rephrased in the  $\mathbb{Z}[x]$ -module structure of  $\text{coker}(\mathbf{M} - x\mathbf{I})$ . To understand the satisfaction frequency of the conditions, it hence remains to understand the distribution of the module when  $\mathbf{M}$  is a random matrix. We here do this for a matrix ensemble with entries Haar distributed on the profinite completion of  $\mathbb{Z}[x]$ . Our main results are Theorems 4.11 and 4.17.

**4.1. Model definition.** Throughout this section, we denote  $R := \mathbb{Z}[x]$ . Recall the definition of the profinite completion  $\widehat{R}$  and its Haar distribution from Section 2.

Denote  $\text{SymHaar}(\widehat{R}^{n \times n})$  for the probability distributions on symmetric random matrices  $\mathbf{M}$  with values in  $\widehat{R}^{n \times n}$  whose entries are Haar distributed and independent up to the symmetry constraint. That is,  $\mathbf{M} = \mathbf{M}^T$  and the upper-triangle satisfies

$$\mathbb{P}(\mathbf{M}_{i,j} \in \mathcal{E}_{i,j} : \forall i \leq j) = \prod_{i \leq j} \mathbb{P}(\text{Haar}(\widehat{R}) \in \mathcal{E}_{i,j}) \quad (4.1)$$

for all measurable subsets  $\mathcal{E}_{i,j} \subseteq \widehat{R}$ . We shall study the  $\widehat{R}$ -module  $\text{coker}(\mathbf{M} - x\mathbf{I})$  as a model for the modules appearing in Propositions 3.2, 3.8 and 3.10. Thus, instead of a matrix with entries from  $\mathbb{Z}$  or  $\{0, 1\}$  we now consider entries from profinite completion of  $\mathbb{Z}[x]$ . Most crucially, the model  $\mathbf{M}$  retains the symmetry constraint that is necessary for the sufficient conditions for spectral characterization of integer matrices in Theorems 1.3 and 1.6.

Given that the Haar measure is preserved by additive shifts, the matrix  $\mathbf{M} - x\mathbf{I}$  has exactly the same distribution as the original matrix  $\mathbf{M}$ . In particular, the cokernels have the same distributions:

$$\mathbb{P}(\text{coker}(\mathbf{M} - x\mathbf{I}) \in \cdot) = \mathbb{P}(\text{coker}(\mathbf{M}) \in \cdot) \quad \text{if } \mathbf{M} \sim \text{SymHaar}(\widehat{R}). \quad (4.2)$$

Recall from Section 2.2.1 that  $\widehat{R} \cong \prod_p \prod_{\beta(x)} R_{p,\beta}$ . Let  $\mathbf{M}_{p,\beta} \in R_{p,\beta}^{n \times n}$  be the matrices that are found by applying this isomorphism entry-wise to  $\mathbf{M}$ . Then, since the cokernel of a matrix over a product ring always decomposes as a product corresponding to the factors,

$$\text{coker}(\mathbf{M}) \cong \prod_p \prod_{\beta(x)} \text{coker}(\mathbf{M}_{p,\beta}) \quad \text{where } \mathbf{M}_{p,\beta} \sim \text{SymHaar}(R_{p,\beta}^{n \times n}), \quad (4.3)$$

where the isomorphism is as  $\widehat{R}$ -modules. It here holds that  $\text{coker}(\mathbf{M}_{p,\beta}) \cong \text{coker}(\mathbf{M}) \otimes_{\widehat{R}} R_{p,\beta}$  so that the pieces in the decomposition (4.3) are analogous to the pieces of  $\mathbb{Z}[x]$ -modules defined in (2.9), except that the tensor product is now over the profinite completion instead of over  $\mathbb{Z}[x]$ . Our goal is to determine the probability that the constraints in Propositions 3.2, 3.8 and 3.10 are satisfied when the modules  $\text{coker}(\cdot)_{p,\beta}$  are formally replaced by the corresponding pieces in (4.3).

**Remark 4.1.** Removing the symmetry constraint from the profinite Haar model can also be used to give an alternative justification for a conjecture in [46] concerning walk matrix statistics without symmetry constraint. That argument does not directly contribute to our main goal, as the symmetry constraint is essential for Theorems 4.11 and 4.17 to apply, except that the fact that one can recover previous conjectures may give some additional confidence in the modeling approach of the present paper. We give details on the alternative argument for [46, Conjecture 1.4] in Appendix B.

**Remark 4.2.** While the translational invariance of the Haar distribution in (4.2) also applies for any other symmetric shift, we expect that the specific occurrence of  $x\mathbf{I}$  in  $\text{coker}(\mathbf{M} - x\mathbf{I})$  will be important in universality principles that allow different laws for the entries of  $\mathbf{M}$ . For example, Kahn and Komlós [28, Theorem 1.3] show that the rank of a random matrix over a finite field is only universal if the entries are not in a proper affine subfield. The latter implies that  $\text{coker}(\mathbf{M} - x\mathbf{J}) \otimes_{\widehat{R}} \mathbb{F}_p[x] / \beta \mathbb{F}_p[x]$  with  $\mathbf{J}$  the all-ones matrix is *not* universal when  $\mathbf{M}$  has integer entries without symmetry constraint since  $\mathbf{M} - x\mathbf{J} \pmod{p, \beta}$  then has all entries in the same affine subfield  $\mathbb{F}_p + x$  of  $\mathbb{F}_p[x] / \beta \mathbb{F}_p[x]$ , which is proper when  $\deg(\beta) > 1$ . The presence of the identity in  $x\mathbf{I}$  is indeed used in previous arguments on universality of  $\mathbb{Z}[x]$ -modules for random matrices without symmetry constraints [10, 46].

**4.2. General reduction result.** Since the Haar measure on  $\widehat{R}$  induces independent elements on the different factors, the pieces in the decomposition (4.3) are independent. It hence suffices to study their distributions separately. The key fact for this purpose will be that  $R_{p,\beta}$  is a compact Noetherian local ring. We present our arguments in this general setting and return to  $R_{p,\beta}$  in Corollary 4.6.

All rings in the present paper are commutative and unital. Recall that a ring is *Noetherian* if all ideals are finitely generated. A *local ring* is a ring  $\mathcal{O}$  with a unique maximal ideal  $\mathfrak{m} \subsetneq \mathcal{O}$ . Krull's intersection theorem yields that  $\bigcap_{k>0} \mathfrak{m}^k = 0$  for any Noetherian local ring [3, Corollary 10.19], so we can define a metric on  $\mathcal{O}$  by  $d(x, y) := 2^{-v(x-y)}$  with  $v(r) := \sup\{k \geq 0 : r \in \mathfrak{m}^k\}$ . From here on, we fix a Noetherian local ring  $\mathcal{O}$ . We further assume that  $\mathcal{O}$  is compact as a metric space, which is equivalent to the residue field  $\mathcal{O}/\mathfrak{m}$  being finite.<sup>2</sup> In particular,  $(\mathcal{O}, +)$  is then a compact Hausdorff topological group and hence admits a unique Haar probability measure. Denote  $q := \#\mathcal{O}/\mathfrak{m}$ . We use  $\text{rank}_q(\cdot)$  to refer to the rank over  $\mathbb{F}_q \cong \mathcal{O}/\mathfrak{m}$  of the reduction modulo  $\mathfrak{m}$  of a matrix over  $\mathcal{O}$ .

Now consider a random matrix  $\mathbf{M} \sim \text{SymHaar}(\mathcal{O}^{n \times n})$ . Then, the reduction  $\mathbf{M} \bmod \mathfrak{m}$  is a uniform random symmetric matrix over  $\mathbb{F}_q$ . The number of symmetric matrices over a finite field with a given rank is classical, dating back to Carlitz [5] for odd  $q$ , and MacWilliams [33] for both odd and even  $q$ . It follows from their results (see e.g., [19, Eq.(20)]) that for any fixed integer  $k \geq 0$ ,

$$\lim_{n \rightarrow \infty} \mathbb{P}(\text{rank}_q(\mathbf{M}) = n - k) = \frac{\prod_{i \geq 0} (1 - q^{-2i-1})}{\prod_{i=1}^k (q^i - 1)}, \quad (4.4)$$

where the empty product yields unity if  $k = 0$ . The goal in the remainder of this section is to understand the distribution of the cokernel conditional on the rank. This is achieved in Proposition 4.5 which yields a reduction to matrices of bounded dimensionality and is the core mathematical ingredient for the subsequent computations. First, we consider preliminaries in Lemmas 4.3 and 4.4.

**Lemma 4.3.** *Consider a matrix  $\mathbf{M} \in \mathcal{O}^{n \times n}$  that is symmetric,  $\mathbf{M} = \mathbf{M}^\top$ . Then, for every  $k \leq n$ , it holds that  $\text{rank}_q(\mathbf{M}) = n - k$  if and only if there exists invertible  $\mathbf{G} \in \text{GL}_n(\mathcal{O})$  such that*

$$\mathbf{G}^\top \mathbf{M} \mathbf{G} = \begin{pmatrix} \mathbf{Q} & 0 \\ 0 & \mathbf{K} \end{pmatrix} \quad (4.5)$$

for some symmetric  $\mathbf{K} \in \mathfrak{m}^{k \times k}$  and invertible symmetric  $\mathbf{Q} \in \text{GL}_{n-k}(\mathcal{O})$ .

*Proof.* A square matrix over  $\mathcal{O}$  is invertible if and only if its reduction modulo  $\mathfrak{m}$  is so over  $\mathbb{F}_q \cong \mathcal{O}/\mathfrak{m}$ . (This follows from the adjoint formula for the inverse by using that the invertible elements of a local ring are those that are not in the maximal ideal to the determinant. Alternatively, one can use Nakayama's lemma.) That  $\text{rank}_q(\mathbf{M}) = n - k$  whenever (4.5) is satisfied is hence immediate by taking the reduction modulo  $\mathfrak{m}$  since  $\mathbf{G}$  and  $\mathbf{Q}$  then reduce to invertible matrices over  $\mathbb{F}_q$ .

Now suppose that  $\text{rank}_q(\mathbf{M}) = n - k$ . To start, we then claim that there then exist invertible matrices  $\mathbf{G}_0 \in \text{GL}_n(\mathbb{F}_q)$  and  $\mathbf{Q}_0 \in \text{GL}_{n-k}(\mathbb{F}_q)$  over  $\mathbb{F}_q$  with

$$\mathbf{G}_0^\top \mathbf{M} \mathbf{G}_0 \equiv \begin{pmatrix} \mathbf{Q}_0 & 0 \\ 0 & 0 \end{pmatrix} \pmod{\mathfrak{m}}. \quad (4.6)$$

Indeed, let  $e_1, \dots, e_n \in \mathbb{F}_q^n$  be the standard basis and note that the assumption on the rank of  $\mathbf{M}$  ensures that there exists some invertible  $\mathbf{G}_0 \in \text{GL}_n(\mathbb{F}_q)$  that maps the final  $k$  basis vectors into the kernel of  $\mathbf{M} \bmod \mathfrak{m}$ . That is, with  $\mathbf{M} \mathbf{G}_0 e_{n-i} = 0$  over  $\mathbb{F}_q$  for all  $i < k$ . Then also  $e_{n-i}^\top \mathbf{G}_0^\top \mathbf{M} = 0$  by taking the transpose. Thus, the final  $k$  rows and columns of  $\mathbf{G}_0^\top \mathbf{M} \mathbf{G}_0$  are zero, and the remaining  $(n - k) \times (n - k)$  block has to be invertible since  $\mathbf{M}_0$  has rank  $n - k$ .

Pick arbitrary lifts of  $\mathbf{G}_0$  and  $\mathbf{Q}_0$  to matrices over  $\mathcal{O}$ , subject to the constraint that  $\mathbf{Q}_0$  remains symmetric. Then, these lifts are invertible over  $\mathcal{O}$ . Moreover, (4.6) means that

$$\mathbf{G}_0^\top \mathbf{M} \mathbf{G}_0 = \begin{pmatrix} \mathbf{Q}_0 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} \mathbf{D}_{1,1} & \mathbf{D}_{1,2} \\ \mathbf{D}_{1,2}^\top & \mathbf{D}_{2,2} \end{pmatrix} \quad (4.7)$$

for certain matrices  $\mathbf{D}_{i,j}$  of appropriate dimension whose entries are in  $\mathfrak{m}$  and where the diagonal matrices are symmetric, i.e.,  $\mathbf{D}_{i,i} = \mathbf{D}_{i,i}^\top$ . Then, with  $\mathbf{I}$  the identity matrix and  $\mathbf{Q}_1 := \mathbf{Q}_0 + \mathbf{D}_{1,1}$ ,

$$\mathbf{G}_1^\top \mathbf{G}_0^\top \mathbf{M} \mathbf{G}_0 \mathbf{G}_1 = \begin{pmatrix} \mathbf{Q}_0 + \mathbf{D}_{1,1} & 0 \\ 0 & \mathbf{D}_{2,2} - \mathbf{D}_{1,2}^\top \mathbf{Q}_1^{-1} \mathbf{D}_{1,2} \end{pmatrix} \quad \text{with} \quad \mathbf{G}_1 := \mathbf{I} - \begin{pmatrix} 0 & \mathbf{Q}_1^{-1} \mathbf{D}_{1,2} \\ 0 & 0 \end{pmatrix}. \quad (4.8)$$

Let  $\mathbf{G} = \mathbf{G}_0 \mathbf{G}_1$  and  $\mathbf{Q} := \mathbf{Q}_1$ , and take  $\mathbf{K} = \mathbf{D}_{2,2} - \mathbf{D}_{1,2}^\top \mathbf{Q}_1^{-1} \mathbf{D}_{1,2}$  to conclude.  $\square$

<sup>2</sup>Indeed, note that  $\mathfrak{m}^j / \mathfrak{m}^{j+1}$  is a finite-dimensional vector space over  $\mathcal{O}/\mathfrak{m}$  by Noetherianity and hence  $\mathcal{O}/\mathfrak{m}^j$  is finite if and only if  $\mathcal{O}/\mathfrak{m}$  is so. That  $\mathcal{O}/\mathfrak{m}^j$  is finite for all  $j$  is equivalent to compactness of  $\mathcal{O}$ , as may be verified directly from the definition of the metric on the local ring.

Let it be understood that the *Haar measure on an ideal*  $\mathfrak{a} \subseteq \mathcal{O}$  refers to the the unique probability measure that is preserved by additive translation with elements from  $\mathfrak{a}$ . If  $a_1, \dots, a_r \in \mathfrak{a}$  are generators for the ideal, then this distribution corresponds to the law of  $a_1 H_1 + \dots + a_r H_r$  with  $H_i$  independent Haar( $\mathcal{O}$ )-distributed elements. Define a probability distribution  $\text{SymHaar}(\mathfrak{a}^{n \times n})$  on symmetric matrices exactly like in (4.1).

**Lemma 4.4** (Invariance property). *Suppose that  $\mathbf{M} \sim \text{SymHaar}(\mathfrak{a}^{n \times n})$  and consider some deterministic invertible matrix  $\mathbf{G} \in \text{GL}_n(\mathcal{O})$ . Then, the matrix  $\mathbf{G}^\top \mathbf{M} \mathbf{G}$  is again  $\text{SymHaar}(\mathfrak{a}^{n \times n})$ -distributed.*

*Proof.* Suppose that  $\mathbf{M} \sim \text{SymHaar}(\mathfrak{a}^{n \times n})$  and consider some arbitrary matrix  $\mathbf{S} \in \mathfrak{a}^{n \times n}$  that is symmetric  $\mathbf{S} = \mathbf{S}^\top$ . Then,  $\mathbf{G}^\top \mathbf{M} \mathbf{G} + \mathbf{S} = \mathbf{G}^\top (\mathbf{M} + \mathbf{S}') \mathbf{G}$  with  $\mathbf{S}' := (\mathbf{G}^\top)^{-1} \mathbf{S} \mathbf{G}^{-1}$ . Now, using that the Haar measure is preserved by additive translations on  $\mathbf{M} + \mathbf{S}'$  yields that  $\mathbf{G}^\top \mathbf{M} \mathbf{G} + \mathbf{S}$  has the same distribution as  $\mathbf{G}^\top \mathbf{M} \mathbf{G}$ . Thus, the law of  $\mathbf{G}^\top \mathbf{M} \mathbf{G}$  is also preserved by translation. Recall that invariance by translation characterizes the Haar measure to conclude.  $\square$

**Proposition 4.5.** *Suppose that  $\mathbf{M} \sim \text{SymHaar}(\mathcal{O}^{n \times n})$ . Fix some  $k \leq n$ . Then, we have an equality in distribution of random  $\mathcal{O}$ -modules:*

$$\mathbb{P}\left(\text{coker}(\mathbf{M}) \in * \mid \text{rank}_q(\mathbf{M}) = n - k\right) = \mathbb{P}\left(\text{coker}(\mathbf{K}) \in *\right), \quad (4.9)$$

where  $\mathbf{K} \sim \text{SymHaar}(\mathfrak{m}^{k \times k})$  is a symmetric  $k \times k$  matrix with entries Haar distributed on  $\mathfrak{m}$ .

*Proof.* Let  $\mathbf{M}$  be a  $\text{SymHaar}(\mathcal{O}^{n \times n})$  distributed matrix conditioned to have rank  $n - k$ . Then, Lemma 4.3 ensures there exist random invertible  $\mathbf{G} \in \text{GL}_n(\mathcal{O})$  and invertible symmetric  $\mathbf{Q} \in \text{GL}_{n-k}(\mathcal{O})$  as well as a random symmetric matrix  $\mathbf{K} \in \mathfrak{m}^{k \times k}$  such that  $\mathbf{G}^\top \mathbf{M} \mathbf{G} = \text{diag}(\mathbf{Q}, \mathbf{K})$ .

We claim that it can here be assumed without loss of generality that  $\mathbf{K} \sim \text{SymHaar}(\mathfrak{m}^{k \times k})$ . To see this, note that  $\mathbf{M}$  has the same distribution as  $\mathbf{M} + \Delta$  with  $\Delta \sim \text{SymHaar}(\mathfrak{m}^{n \times n})$  an independent random matrix. Lemma 4.4 further implies that  $\mathbf{D} := \mathbf{G}^\top \Delta \mathbf{G}$  is again  $\text{SymHaar}(\mathfrak{m}^{n \times n})$  distributed and independent from  $\mathbf{M}, \mathbf{K}, \mathbf{G}$  and  $\mathbf{Q}$ . The matrix  $\mathbf{G}^\top (\mathbf{M} + \Delta) \mathbf{G} = \mathbf{G}^\top \mathbf{M} \mathbf{G} + \mathbf{D}$  may not be in block diagonal form anymore, but off-diagonal blocks can be cleared exactly as in (4.7)–(4.8) in the proof of Lemma 4.3. That is, writing  $\mathbf{D}$  in block diagonal form as in (4.7), it holds with  $\mathbf{Q}_\Delta := \mathbf{Q} + \mathbf{D}_{1,1}$  that

$$\mathbf{G}_\Delta^\top \mathbf{G}^\top (\mathbf{M} + \Delta) \mathbf{G} \mathbf{G}_\Delta = \begin{pmatrix} \mathbf{Q}_\Delta & 0 \\ 0 & \mathbf{K} + \mathbf{D}_{2,2} - \mathbf{D}_{1,2}^\top \mathbf{Q}_\Delta^{-1} \mathbf{D}_{1,2} \end{pmatrix} \quad \text{with} \quad \mathbf{G}_\Delta := \mathbf{I} - \begin{pmatrix} 0 & \mathbf{Q}_\Delta^{-1} \mathbf{D}_{1,2} \\ 0 & 0 \end{pmatrix} \quad (4.10)$$

Here, note that  $\mathbf{D}_{2,2}$  is independent from  $\mathbf{D}_{1,2}^\top \mathbf{Q}_\Delta^{-1} \mathbf{D}_{1,2}$  and  $\mathbf{K}$  due to the independence of  $\mathbf{D}$  from  $\mathbf{Q}$  and  $\mathbf{K}$ , as well as the independence of the blocks in  $\mathbf{D}$  that follow from the matrix being  $\text{SymHaar}(\mathfrak{m}^{n \times n})$  distributed. Consequently, the translation invariance of  $\text{SymHaar}(\mathfrak{m}^{k \times k})$  applied to  $\mathbf{D}_{2,2}$  ensures that the lower-right block is again Haar distributed:

$$\mathbf{K} + \mathbf{D}_{2,2} - \mathbf{D}_{1,2}^\top \mathbf{Q}_\Delta^{-1} \mathbf{D}_{1,2} \sim \text{SymHaar}(\mathfrak{m}^{k \times k}). \quad (4.11)$$

Thus, we can indeed assume that  $\mathbf{G}^\top \mathbf{M} \mathbf{G} = \text{diag}(\mathbf{Q}, \mathbf{K})$  with  $\mathbf{K} \sim \text{SymHaar}(\mathfrak{m}^{k \times k})$ . (Indeed, replace  $\mathbf{M}$  by  $\mathbf{M} + \Delta$ , replace  $\mathbf{K}$  by  $\mathbf{K} + \mathbf{D}_{2,2} - \mathbf{D}_{1,2}^\top \mathbf{Q}_\Delta^{-1} \mathbf{D}_{1,2}$ , and replace  $\mathbf{G}$  and  $\mathbf{Q}$  by  $\mathbf{G} \mathbf{G}_\Delta$  and  $\mathbf{Q}_\Delta$ , respectively.)

It follows directly from the definition of the cokernel (2.1) that  $\text{coker}(\mathbf{U} \mathbf{M} \mathbf{V}) \cong \text{coker}(\mathbf{M})$  for every  $\mathbf{U}, \mathbf{V} \in \text{GL}_n(\mathcal{O})$ . Moreover, also directly from the definition, the cokernel of a block diagonal matrix is the direct sum of the cokernels of its diagonal blocks, and an invertible matrix always has trivial cokernel. Hence,

$$\text{coker}(\mathbf{M}) \cong \text{coker}(\mathbf{G}^\top \mathbf{M} \mathbf{G}) \cong \text{coker}(\mathbf{Q}) \oplus \text{coker}(\mathbf{K}) \cong \text{coker}(\mathbf{K}). \quad (4.12)$$

This concludes the proof.  $\square$

**Corollary 4.6.** *Suppose that  $\mathbf{M}_{p,\beta} \sim \text{SymHaar}(R_{p,\beta}^{n \times n})$ . Let it be understood that  $\text{rank}_q(\cdot)$  refers to the rank over  $\mathbb{F}_q \cong \mathbb{Z}[x]/(p\mathbb{Z}[x] + \beta(x)\mathbb{Z}[x])$ . Then, for every  $k \leq n$ , as random  $R_{p,\beta}$  modules,*

$$\mathbb{P}\left(\text{coker}(\mathbf{M}_{p,\beta}) \in * \mid \text{rank}_q(\mathbf{M}_{p,\beta}) = n - k\right) = \mathbb{P}\left(\text{coker}(\mathbf{K}) \in *\right), \quad (4.13)$$

where  $\mathbf{K}$  is a symmetric  $k \times k$  matrix with entries Haar distributed on  $pR_{p,\beta} + \beta(x)R_{p,\beta}$ . That is,

$$\mathbf{K} \sim p \text{SymHaar}(R_{p,\beta}^{k \times k}) + \beta(x) \text{SymHaar}(R_{p,\beta}^{k \times k}). \quad (4.14)$$

*Proof.* This is immediate from Proposition 4.5 since  $R_{p,\beta}$  is a compact Noetherian local ring with maximal ideal  $\widehat{\mathfrak{m}} = pR_{p,\beta} + \beta(x)R_{p,\beta}$ . Indeed, the  $\mathfrak{m}$ -adic completion of a ring at a maximal ideal  $\mathfrak{m}$  is always a local ring [3, Proposition 10.16], it is Noetherian when the original ring is so [3, Theorem 10.26], and it is compact if and only if the residue field modulo  $\mathfrak{m}$  is finite (recall footnote 2).  $\square$

**4.3. Conditions based on the walk matrix.** The following definition provides a profinite analogue for the rephrasing of the condition in Proposition 3.2:

**Definition 4.7.** Fix a prime  $p$ . Then, a  $\widehat{R}$ -module  $\mathcal{M}$  is said to satisfy *condition  $\mathcal{W}_p$*  if one of the following two events is satisfied:

- (W1) It holds that  $\mathcal{M} \otimes_{\widehat{R}} R_{p,\beta} \cong 0$  for every monic  $\beta(x) \in \mathbb{Z}[x]$  with irreducible reduction in  $\mathbb{F}_p[x]$ .
- (W2) Or, there exists  $a \in \mathbb{Z}$  such that  $\mathcal{M} \otimes_{\widehat{R}} R_{p,x-a} \cong \mathbb{F}_p[x]/(x-a)\mathbb{F}_p[x]$  and  $\mathcal{M} \otimes_{\widehat{R}} R_{p,\beta} \cong 0$  for every  $\beta \not\equiv x-a \pmod{p}$ .

To model Conjecture 1.4, we study the frequency of condition  $\mathcal{W}_p$  for the module  $\text{coker}(\mathbf{M} - x\mathbf{I}, \zeta)$  with  $\zeta \sim \text{Haar}(\widehat{R}^n)$  a random vector that is independent of the random matrix  $\mathbf{M}$ . Exactly as in (4.2)–(4.3), the random modules  $\text{coker}(\mathbf{M} - x\mathbf{I}, \zeta) \otimes_{\widehat{R}} R_{p,\beta}$  for varying  $(p, \beta)$  are independent with the same distribution as  $\text{coker}(\mathbf{M}_{p,\beta}, \zeta_{p,\beta})$  for  $\mathbf{M}_{p,\beta} \sim \text{SymHaar}(R_{p,\beta}^{n \times n})$  and  $\zeta_{p,\beta} \sim \text{Haar}(R_{p,\beta}^n)$ . It hence suffices to study the distribution of these pieces individually. Corollary 4.6 reduces the latter problem to a finite direct computation, whose details we next provide in Lemmas 4.8 and 4.9:

**Lemma 4.8.** *Let  $q := p^{\deg(\beta)}$ . Then, for every  $n \geq 1$ ,*

$$\left| \mathbb{P}(\text{coker}(\mathbf{M}_{p,\beta}, \zeta_{p,\beta}) \cong 0) - \left(1 - \frac{1}{q^2}\right) \prod_{i \geq 1} \left(1 - \frac{1}{q^{2i+1}}\right) \right| \leq \frac{6}{q^n}. \quad (4.15)$$

*Proof.* Nakayama's lemma [3, Proposition 2.6] applied over  $R_{p,\beta}$  yields that  $\text{coker}(\mathbf{M}_{p,\beta}, \zeta_{p,\beta}) \cong 0$  if and only if  $[\mathbf{M}_{p,\beta}, \zeta_{p,\beta}]$  has full rank over  $\mathbb{F}_q := \mathbb{F}_p[x]/\beta(x)\mathbb{F}_p[x]$ . The rank of that rectangular matrix is at most one higher than that of  $\mathbf{M}_{p,\beta}$ . Hence, by the law of total probability,

$$\begin{aligned} \mathbb{P}(\text{coker}(\mathbf{M}_{p,\beta}, \zeta_{p,\beta}) \cong 0) &= \mathbb{P}(\text{rank}_q(\mathbf{M}_{p,\beta}) = n) \\ &\quad + \mathbb{P}(\text{rank}_q(\mathbf{M}_{p,\beta}) = n-1) \mathbb{P}(\text{rank}_q(\mathbf{M}_{p,\beta}, \zeta_{p,\beta}) = n \mid \text{rank}_q(\mathbf{M}_{p,\beta}) = n-1). \end{aligned} \quad (4.16)$$

Fulman and Goldstein [19, Theorem 4.1] gave bounds on the total variation distance between the probability distribution of the rank of a uniform random symmetric  $n \times n$  matrix over  $\mathbb{F}_q$  and the limiting law (4.4). In particular, their bounds imply that for every  $k \leq n$ ,

$$\left| \mathbb{P}(\text{rank}_q(\mathbf{M}_{p,\beta}) = n-k) - \prod_{i=1}^k (q^i - 1)^{-1} \prod_{i \geq 0} (1 - q^{-2i-1}) \right| \leq 3/q^n. \quad (4.17)$$

Conditional on the event  $\text{rank}_q(\mathbf{M}_{p,\beta}) = n-1$  it occurs that  $\text{rank}_q(\mathbf{M}_{p,\beta}, \zeta_{p,\beta}) = n$  if and only if  $\zeta_{p,\beta}$  reduces to a nonzero element in the one-dimensional  $\mathbb{F}_q$  vector space  $\text{coker}(\mathbf{M}_{p,\beta}) \otimes_{R_{p,\beta}} \mathbb{F}_q$ . Thus, since  $\zeta_{p,\beta}$  yields a uniform random element of that one-dimensional vector space,

$$\mathbb{P}(\text{rank}_q(\mathbf{M}_{p,\beta}, \zeta_{p,\beta}) = n \mid \text{rank}_q(\mathbf{M}_{p,\beta}) = n-1) = 1 - 1/q. \quad (4.18)$$

Substitute (4.17) and (4.18) in (4.16) and simplify by using that  $1 + (q-1)^{-1}(1 - q^{-1}) = 1 + q^{-1}$  to find (4.15). Here, the product in (4.15) starts at  $i = 1$  because the factor with  $i = 0$  from (4.17) was rewritten using that  $(1 + q^{-1})(1 - q^{-1}) = 1 - q^{-2}$ .  $\square$

**Lemma 4.9.** *Let  $q := p^{\deg(\beta)}$ . Then, every  $n \geq 2$ ,*

$$\left| \mathbb{P}\left(\text{coker}(\mathbf{M}_{p,\beta}, \zeta_{p,\beta}) \cong \frac{\mathbb{F}_p[x]}{\beta(x)\mathbb{F}_p[x]}\right) - \frac{1}{q^2} \left(1 - \frac{1}{q^2}\right)^2 \prod_{i \geq 1} \left(1 - \frac{1}{q^{2i+1}}\right) \right| \leq \frac{6}{q^n}. \quad (4.19)$$

*Proof.* Denote  $\mathbb{F}_q := \mathbb{F}_p[x]/\beta(x)\mathbb{F}_p[x]$ . Note that  $\text{coker}(\mathbf{M}_{p,\beta}, \zeta_{p,\beta}) \cong \mathbb{F}_q$  as a  $R_{p,\beta}$ -module implies that  $\text{coker}(\mathbf{M}_{p,\beta}, \zeta_{p,\beta}) \otimes_{R_{p,\beta}} \mathbb{F}_q \cong \mathbb{F}_q$ , and hence necessitates that the matrix  $[\mathbf{M}_{p,\beta}, \zeta_{p,\beta}]$  reduces to a matrix with rank  $n-1$  over  $\mathbb{F}_q$ . Hence, by the law of total probability,

$$\begin{aligned} \mathbb{P}(\text{coker}(\mathbf{M}_{p,\beta}, \zeta_{p,\beta}) \cong \mathbb{F}_q) &= \mathbb{P}(\text{coker}(\mathbf{M}_{p,\beta}, \zeta_{p,\beta}) \cong \mathbb{F}_q \mid \text{rank}_q(\mathbf{M}_{p,\beta}) = n-1) \mathbb{P}(\text{rank}_q(\mathbf{M}_{p,\beta}) = n-1) \\ &\quad + \mathbb{P}(\text{coker}(\mathbf{M}_{p,\beta}, \zeta_{p,\beta}) \cong \mathbb{F}_q \mid \text{rank}_q(\mathbf{M}_{p,\beta}) = n-2) \mathbb{P}(\text{rank}_q(\mathbf{M}_{p,\beta}) = n-2). \end{aligned} \quad (4.20)$$

We start with the probability conditional on rank  $n-1$ . Then, Corollary 4.6 yields that  $\text{coker}(\mathbf{M}_{p,\beta})$  has the same distribution as  $\text{coker}(k_1)$  with  $k_1 \sim p \text{Haar}(R_{p,\beta}) + \beta(x) \text{Haar}(R_{p,\beta})$ . Consequently,  $\text{coker}(\mathbf{M}_{p,\beta}, \zeta_{p,\beta})$  then has the same distribution as  $\text{coker}(k_1, z)$  with  $z \sim \text{Haar}(R_{p,\beta})$ . If  $z$  has nonzero reduction in  $\mathbb{F}_q$  then  $\text{coker}(z) \cong 0$  and hence also  $\text{coker}(k_1, z) \cong 0$ . Hence, since  $z$  reduces to zero with probability  $1/q$ , it holds with  $k_1, k_2 \sim p \text{Haar}(R_{p,\beta}) + \beta(x) \text{Haar}(R_{p,\beta})$  independent that

$$\mathbb{P}(\text{coker}(\mathbf{M}_{p,\beta(x)}, \zeta_{p,\beta}) \cong \mathbb{F}_q \mid \text{rank}_q(\mathbf{M}_{p,\beta}) = n-1) = q^{-1} \mathbb{P}(\text{coker}(k_1, k_2) \cong \mathbb{F}_q). \quad (4.21)$$

Nakayama's lemma [3, Proposition 2.8] implies that two elements of  $\widehat{\mathbf{m}} = pR_{p,\beta} + \beta(x)R_{p,\beta}$  generate this ideal if and only if their reduction to  $\widehat{\mathbf{m}}/\widehat{\mathbf{m}}^2$  generate the latter as a vector space over  $\mathbb{F}_q$ . Here,  $\widehat{\mathbf{m}}/\widehat{\mathbf{m}}^2 \cong \mathbb{F}_q^2$  as a vector space since  $p$  and  $\beta(x)$  yield a basis. Consequently, using that  $R_{p,\beta}/\widehat{\mathbf{m}} \cong \mathbb{F}_q$  and that the probability that two random vectors generate  $\mathbb{F}_q^2$  is exactly  $(1-1/q^2)(1-1/q)$ ,

$$\mathbb{P}(\text{coker}(\mathbf{M}_{p,\beta(x)}, \zeta_{p,\beta}) \cong \mathbb{F}_q \mid \text{rank}_q(\mathbf{M}_{p,\beta}) = n-1) = q^{-1}(1-q^{-2})(1-q^{-1}). \quad (4.22)$$

The probability conditional on rank  $n-2$  proceeds with a similar strategy. On that event, Corollary 4.6 yields that  $\text{coker}(\mathbf{M}_{p,\beta})$  has the same distribution as  $\text{coker}(\mathbf{K})$  with  $\mathbf{K}$  a symmetric  $2 \times 2$  matrix with entries Haar distributed on  $pR_{p,\beta} + \beta(x)R_{p,\beta}$ . Then,  $\text{coker}(\mathbf{M}_{p,\beta}, \zeta_{p,\beta})$  has the same distribution as  $\text{coker}(\mathbf{K}, Z)$  with  $Z \sim \text{Haar}(R_{p,\beta}^2)$ . If  $Z$  reduces to zero in  $\mathbb{F}_q^2$ , then  $\text{coker}(\mathbf{K}, Z) \otimes_{R_{p,\beta}} \mathbb{F}_q$  is a 2-dimensional vector space so that  $\text{coker}(\mathbf{K}, Z)$  could not be isomorphic to  $\mathbb{F}_q$  as a  $R_{p,\beta}$ -module. Hence, since  $Z$  reduces to zero with probability  $1/q^2$ ,

$$\begin{aligned} \mathbb{P}(\text{coker}(\mathbf{M}_{p,\beta}, \zeta_{p,\beta}) \cong \mathbb{F}_q \mid \text{rank}_q(\mathbf{M}_{p,\beta}) = n-2) \\ = (1-q^{-2}) \mathbb{P}(\text{coker}(\mathbf{K}, Z) \cong \mathbb{F}_q \mid Z \not\equiv 0 \pmod{pR_{p,\beta} + \beta(x)R_{p,\beta}}). \end{aligned} \quad (4.23)$$

That  $Z$  has nonzero reduction is equivalent to the existence of a matrix  $\mathbf{G} \in \text{GL}_2(R_{p,\beta})$  such that  $\mathbf{G}Z = (1, 0)^\top$ . The matrix  $\mathbf{G}$  only depends on  $Z$ , so the invariance from Lemma 4.4 implies that  $\tilde{\mathbf{K}} = \mathbf{Q}\mathbf{K}\mathbf{Q}^\top$  has the same distribution as  $\mathbf{K}$ . Further,

$$\text{coker}(\mathbf{K}, Z) \cong \text{coker}(\mathbf{Q}\mathbf{K}\mathbf{Q}^\top, \mathbf{Q}Z) = \text{coker} \begin{pmatrix} \tilde{\mathbf{K}}_{1,1} & \tilde{\mathbf{K}}_{1,2} & 1 \\ \tilde{\mathbf{K}}_{1,2} & \tilde{\mathbf{K}}_{2,2} & 0 \end{pmatrix} \cong \text{coker}(\tilde{\mathbf{K}}_{1,2}, \tilde{\mathbf{K}}_{2,2}). \quad (4.24)$$

Note that  $\tilde{\mathbf{K}}_{1,2}, \tilde{\mathbf{K}}_{2,2} \sim p \text{Haar}(R_{p,\beta}) + \beta(x) \text{Haar}(R_{p,\beta})$ . Consequently, by the arguments in (4.21)–(4.22), it holds that  $\mathbb{P}(\text{coker}(\tilde{\mathbf{K}}_{1,2}, \tilde{\mathbf{K}}_{2,2}) \cong \mathbb{F}_q) = (1-1/q^2)(1-1/q)$ . Hence, using (4.23),

$$\mathbb{P}(\text{coker}(\mathbf{M}_{p,\beta}, \zeta_{p,\beta}) \cong \mathbb{F}_q \mid \text{rank}_q(\mathbf{M}_{p,\beta}) = n-2) = (1-q^{-2})^2(1-q^{-1}). \quad (4.25)$$

Substitution of (4.22) and (4.25) in (4.20) now yields that

$$\begin{aligned} \mathbb{P}(\text{coker}(\mathbf{M}_{p,\beta}, \zeta_{p,\beta}) \cong \mathbb{F}_q) = q^{-1}(1-q^{-2})(1-q^{-1}) \mathbb{P}(\text{rank}_q(\mathbf{M}_{p,\beta}) = n-1) \\ + (1-q^{-2})^2(1-q^{-1}) \mathbb{P}(\text{rank}_q(\mathbf{M}_{p,\beta}) = n-2). \end{aligned} \quad (4.26)$$

By [19, Theorem 4.1], we can replace  $\mathbb{P}(\text{rank}_q(\mathbf{M}_{p,\beta}) = n-k)$  by its limiting value up to an error  $\leq 3/q^n$ ; recall (4.17). The desired result (4.19) now follows after simplifying the prefactors, since

$$\frac{(1-q^{-2})(1-q^{-1})}{q(q-1)} + \frac{(1-q^{-2})^2(1-q^{-1})}{(q-1)(q^2-1)} = \frac{(1-q^{-2})^2}{q^2(1-q^{-1})}. \quad (4.27)$$

Here, the product in (4.19) starts at  $i=1$  because  $(1-q^{-1})^{-1}$  cancels the factor for  $i=0$  in (4.17).  $\square$

It now remains to combine Lemmas 4.8 and 4.9 which involves taking the product of the probabilities. To simplify the latter we will use the following Lemma 4.10:

**Lemma 4.10.** *Fix a prime  $p$ . Then, for every real  $s > 1$ ,*

$$\prod_{\beta(x)} \left(1 - \frac{1}{p^{\deg(\beta)s}}\right) = 1 - \frac{1}{p^{s-1}}. \quad (4.28)$$

Here, the product runs over all monic irreducible  $\beta(x) \in \mathbb{F}_p[x]$ .

*Proof.* This follows from the Euler product formula for the zeta function of the ring  $\mathbb{F}_p[x]$ . That is, by evaluating  $\sum_{\text{monic } f \in \mathbb{F}_p[x]} p^{-\deg(f)s}$  in two ways; see e.g., [42, Chapter 2, Equations (1)&(2)].  $\square$

Combining Lemmas 4.8 to 4.10 now yields our main result: the exact limiting probability that condition  $\mathcal{W}_p$  is satisfied in the profinite model; recall Definition 4.7. In particular, the following Theorem 4.11 justifies Conjecture 1.4.

**Theorem 4.11.** *Let  $\mathbf{M} \sim \text{SymHaar}(\widehat{R}^{n \times n})$  and  $\zeta \sim \text{Haar}(\widehat{R}^n)$ . Then, for every fixed prime  $p$ ,*

$$\lim_{n \rightarrow \infty} \mathbb{P}\left(\text{coker}(\mathbf{M} - x\mathbf{I}, \zeta) \text{ satisfies condition } \mathcal{W}_p\right) = \left(1 - \frac{1}{p^2} - \frac{1}{p^3} + \frac{1}{p^4}\right) \prod_{i=1}^{\infty} \left(1 - \frac{1}{p^{2i}}\right). \quad (4.29)$$

Moreover, for any set of primes  $\mathcal{P}$ ,

$$\lim_{n \rightarrow \infty} \mathbb{P}\left(\forall p \in \mathcal{P} : \text{coker}(\mathbf{M} - x\mathbf{I}, \zeta) \text{ satisfies } \mathcal{W}_p\right) = \prod_{p \in \mathcal{P}} \left(1 - \frac{1}{p^2} - \frac{1}{p^3} + \frac{1}{p^4}\right) \prod_{i=1}^{\infty} \left(1 - \frac{1}{p^{2i}}\right). \quad (4.30)$$

*Proof.* Consider the following abbreviations for any prime  $p$ , polynomial  $\beta(x)$ , and integer  $a \in \mathbb{Z}$ :

$$P_n(p, \beta) := \mathbb{P}\left(\text{coker}(\mathbf{M}_{p, \beta}, \zeta_{p, \beta}) \cong 0\right), \quad Q_n(p, a) := \mathbb{P}\left(\text{coker}(\mathbf{M}_{p, x-a}, \zeta_{p, x-a}) \cong \frac{\mathbb{F}_p[x]}{(x-a)\mathbb{F}_p[x]}\right).$$

Note that the two events (W1) and (W2) in Definition 4.7 are mutually exclusive. Moreover, the event (W2) can be further subdivided in  $p$  disjoint events corresponding to the options for  $a \bmod p$ . Hence, using the law of total probability as well as the independence and law of the pieces associated with varying  $\beta(x)$  that was remarked upon preceding Lemma 4.8,

$$\mathbb{P}\left(\text{coker}(\mathbf{M} - x\mathbf{I}, \zeta) \text{ satisfies condition } \mathcal{W}_p\right) = \prod_{\beta(x)} P_n(p, \beta) + \sum_{a=0}^{p-1} Q_n(p, a) \prod_{\beta(x) \neq x-a} P_n(p, \beta). \quad (4.31)$$

Further, again using the independence,

$$\mathbb{P}\left(\forall p \in \mathcal{P} : \text{coker}(\mathbf{M} - x\mathbf{I}, \zeta) \text{ satisfies } \mathcal{W}_p\right) = \prod_{p \in \mathcal{P}} \mathbb{P}\left(\text{coker}(\mathbf{M} - x\mathbf{I}, \zeta) \text{ satisfies } \mathcal{W}_p\right). \quad (4.32)$$

We start by formally computing the right-hand side of (4.31) for  $n = \infty$ . Lemmas 4.8 and 4.9 ensure that  $P_\infty(p, \beta) := \lim_{n \rightarrow \infty} P_n(p, \beta)$  and  $Q_\infty(p, a) := \lim_{n \rightarrow \infty} Q_n(p, \beta)$  exist. Substituting the values for  $P_\infty(p, \beta)$  from Lemma 4.8 and subsequently using Lemma 4.10 yields that

$$\prod_{\beta(x)} P_\infty(p, \beta) = \prod_{\beta(x)} \left( \left(1 - \frac{1}{p^{2 \deg(\beta)}}\right) \prod_{i \geq 1} \left(1 - \frac{1}{p^{(2i+1) \deg(\beta)}}\right) \right) = \left(1 - \frac{1}{p}\right) \prod_{i \geq 1} \left(1 - \frac{1}{p^{2i}}\right). \quad (4.33)$$

Comparing Lemmas 4.8 and 4.9 shows that  $Q_\infty(p, a) = p^{-2}(1 - p^{-2})P_\infty(p, x-a)$ . In particular,

$$\sum_{a=0}^{p-1} Q_\infty(p, a) \prod_{\beta(x) \neq x-a} P_\infty(p, \beta) = \frac{1}{p} \left(1 - \frac{1}{p^2}\right) \prod_{\beta(x)} P_\infty(p, \beta) \quad (4.34)$$

Consequently, using (4.33) and that  $(1 + p^{-1}(1 - p^{-2}))(1 - p^{-1}) = 1 - p^{-2} - p^{-3} + p^{-4}$ ,

$$\prod_{\beta(x)} P_\infty(p, \beta) + \sum_{a=0}^{p-1} Q_\infty(p, a) \prod_{\beta(x) \neq x-a} P_\infty(p, \beta) = \left(1 - \frac{1}{p^2} - \frac{1}{p^3} + \frac{1}{p^4}\right) \prod_{i=1}^{\infty} \left(1 - \frac{1}{p^{2i}}\right). \quad (4.35)$$

It remains to justify that the limit and product may be exchanged in (4.31) and (4.32). This follows from the error bounds in Lemmas 4.8 and 4.9 by a direct computation, whose details we next provide.

Define scalars  $\mathfrak{p}_n(p, \beta), \mathfrak{q}_n(p, a) \in \mathbb{R}$  by  $P_n(p, \beta) = (1 + \mathfrak{p}_n(p, \beta))P_\infty(p, \beta)$  and  $Q_n(p, a) = (1 + \mathfrak{q}_n(p, a))Q_\infty(p, a)$ . The explicit value for  $P_\infty(p, \beta)$  in Lemma 4.8 is an increasing function of  $p$  and the degree of  $\beta$ . In particular,  $P_\infty(p, \beta) \geq P_\infty(p, x) \geq P_\infty(2, x) \geq c_1$  for some absolute constant  $c_1 > 0$ . Hence, the error bounds from Lemma 4.8 imply that  $|\mathfrak{p}_n(p, \beta)| \leq c_2 p^{-n \deg(\beta)}$  with  $c_2 = 6/c_1$ . It similarly follows from Lemma 4.9 that there exists  $c_3 > 0$  with  $|\mathfrak{q}_n(p, a)| \leq c_3 p^{-(n-2)}$ . Let  $c_4 > 0$  be a sufficiently large constant so that  $c_2 p^{-n} \leq p^{-(n-c_4)}$  and  $c_3 p^{-(n-2)} \leq p^{-(n-c_4)}$ .

There are at most  $p^d$  monic irreducible polynomials  $\beta \in \mathbb{F}_p[x]$  with degree  $d$ . Hence, for  $n > c_4$ ,

$$\prod_{d \geq 1} (1 - p^{-d(n-c_4)})^{p^d} \leq \prod_{\beta} (1 + \mathfrak{p}_n(p, \beta)) \leq \prod_{d \geq 1} (1 + p^{-d(n-c_4)})^{p^d}, \quad (4.36)$$

$$\prod_{d \geq 1} (1 - p^{-d(n-c_4)})^{p^d} \leq (1 + \mathfrak{q}(p, a)) \prod_{\beta \neq x-a} (1 + \mathfrak{p}_n(p, \beta)) \leq \prod_{d \geq 1} (1 + p^{-d(n-c_4)})^{p^d}. \quad (4.37)$$

Using that  $1 + x \leq \exp(x)$  for  $x \geq 0$ , we have  $\prod_{d \geq 1} (1 + p^{-d(n-c_4)})^{p^d} \leq \exp(\sum_{d \geq 1} p^{-d(n-c_4-1)})$ . Summing the series and using a Taylor approximation, there hence exists  $c_5 > 0$  with  $\prod_{d \geq 1} (1 + p^{-d(n-c_4)})^{p^d} \leq 1 + c_5 p^{-(n-c_4-1)}$  for large  $n$ . For the lower bound, note that a Taylor approximation yields  $c_6 > 0$  with  $1/(1 - p^{-d(n-c_4)}) \leq 1 + c_6 p^{-d(n-c_4)}$ . Absorbing the constant in the exponent allows upper bounding  $1/\prod_d (1 - p^{-d(n-c_4)})^{p^d}$  as above, which yields a lower bound on  $\prod_d (1 - p^{-d(n-c_4)})^{p^d}$ . It follows in this fashion that there exists an absolute constant  $c_7 > 0$  such that for all large  $n$ ,

$$\prod_{d \geq 1} (1 + p^{-(n-c_4)})^{p^d} \leq 1 + p^{-(n-c_7)} \quad \text{and} \quad \prod_{d \geq 1} (1 - p^{-d(n-c_4)})^{p^d} \geq 1 - p^{-(n-c_7)}. \quad (4.38)$$

Recall that  $P_n(p, \beta) = (1 + \mathfrak{p}_n(p, \beta))P_\infty(p, \beta)$  and  $Q_n(p, a) = (1 + \mathfrak{q}_n(p, a))Q_\infty(p, a)$ . It consequently follows from (4.36)–(4.38) that for every set of primes  $\mathcal{P}$ ,

$$\prod_{p \in \mathcal{P}} \left(1 - \frac{1}{p^{n-c_7}}\right) \leq \prod_{p \in \mathcal{P}} \frac{P_n(p, \beta) + \sum_{a=0}^{p-1} Q_n(p, a) \prod_{\beta \neq x-a} P_n(p, \beta)}{P_\infty(p, \beta) + \sum_{a=0}^{p-1} Q_\infty(p, a) \prod_{\beta \neq x-a} P_\infty(p, \beta)} \leq \prod_{p \in \mathcal{P}} \left(1 + \frac{1}{p^{n-c_7}}\right). \quad (4.39)$$

Expanding the product in the lower bound (4.39) to all primes  $p$  yields  $1/\zeta(n-c_7)$  with  $\zeta$  the Riemann zeta function, while the upper bound yields  $\zeta(n-c_7)/\zeta(2(n-c_7))$ . Use that  $\zeta(x) \rightarrow 1$  as  $x \rightarrow +\infty$  to conclude from (4.35) that (4.30) holds true, and hence also (4.29) as the case  $\mathcal{P} = \{p\}$ .  $\square$

**4.4. Conditions based on the discriminant.** The following Definitions 4.12 and 4.13 give profinite analogues for the conditions in Propositions 3.8 and 3.10. Both definitions also allow  $p = 2$ .

**Definition 4.12.** Fix a prime  $p$ . Then, a  $\widehat{R}$ -module  $\mathcal{M}$  is said to satisfy *condition  $\mathcal{D}_p^1$*  if it holds for every monic  $\beta(x) \in \mathbb{Z}[x]$  with irreducible reduction in  $\mathbb{F}_p[x]$  that  $\widehat{\mathcal{M}}_{p,\beta} := \mathcal{M} \otimes_{\widehat{R}} R_{p,\beta}$  satisfies

$$\widehat{\mathcal{M}}_{p,\beta}/p\widehat{\mathcal{M}}_{p,\beta} \cong 0 \quad \text{or} \quad \widehat{\mathcal{M}}_{p,\beta}/p\widehat{\mathcal{M}}_{p,\beta} \cong \mathbb{F}_p[x]/\beta(x)\mathbb{F}_p[x]. \quad (4.40)$$

**Definition 4.13.** Fix a prime  $p$ . Then, a  $\widehat{R}$ -module  $\mathcal{M}$  is said to satisfy *condition  $\mathcal{D}_p^2$*  if there exists  $a \in \mathbb{Z}_p$  such that (4.40) holds for every  $\beta \neq x - a \pmod{p}$ , and

$$\widehat{\mathcal{M}}_{p,x-a}/p\widehat{\mathcal{M}}_{p,x-a} \cong \mathbb{F}_p[x]/(x-a)^2\mathbb{F}_p[x] \quad \text{and} \quad \widehat{\mathcal{M}}_{p,x-a}/(x-a)\widehat{\mathcal{M}}_{p,x-a} \cong \mathbb{F}_p[x]/(x-a)\mathbb{F}_p[x]. \quad (4.41)$$

The hat in the notation  $\widehat{\mathcal{M}}_{p,\beta}$  serves to emphasize that the tensor product is taken over the profinite completion  $\widehat{R}$ , not over  $R = \mathbb{Z}[x]$  itself as in (2.9). This serves to avoid ambiguity related to  $\widehat{R}$ -modules also being  $R$ -modules but will otherwise not be significant.

In view of Proposition 3.8, the discriminant being odd can be modeled by the event that  $\mathcal{D}_p^1$  is satisfied for  $p = 2$ . Further, considering Proposition 3.10, additionally imposing square-freeness can be modeled by  $\mathcal{D}_p^1$  or  $\mathcal{D}_p^2$  being satisfied for all odd primes  $p$ . Thus, we find a profinite model for the setting of Conjecture 1.7.

Recall from (4.2)–(4.3) that it holds for  $\mathbf{M} \sim \text{SymHaar}(\widehat{R}^{n \times n})$  that the random modules  $\text{coker}(\mathbf{M} - x\mathbf{I}) \otimes_{\widehat{R}} R_{p,\beta}$  for varying  $(p, \beta)$  are independent with the same distribution as  $\text{coker}(\mathbf{M}_{p,\beta})$  for  $\mathbf{M}_{p,\beta} \sim \text{SymHaar}(R_{p,\beta}^{n \times n})$ . It hence suffices to study these pieces separately, which Corollary 4.6 again reduces to a finite direct computation in Lemmas 4.14 to 4.16. We conclude in Theorem 4.17.

**Lemma 4.14.** *Let  $q = p^{\deg(\beta)}$ . Then, for every  $n \geq 1$ ,*

$$\left| \mathbb{P}\left(\frac{\text{coker}(\mathbf{M}_{p,\beta})}{p \text{coker}(\mathbf{M}_{p,\beta})} \cong 0\right) - \prod_{i \geq 0} \left(1 - \frac{1}{q^{2i+1}}\right) \right| \leq \frac{3}{q^n}. \quad (4.42)$$

*Proof.* Nakayama's lemma [3, Proposition 2.6] applied to the local ring  $R_{p,\beta}/pR_{p,\beta}$  yields that the quotient  $\text{coker}(\mathbf{M}_{p,\beta})/p \text{coker}(\mathbf{M}_{p,\beta})$  is trivial if and only if  $\mathbf{M}_{p,\beta}$  is full rank over the finite field  $\mathbb{F}_q := \mathbb{F}_p[x]/\beta(x)\mathbb{F}_p[x]$ . The result is hence immediate from [19, Theorem 4.1]; recall also (4.17).  $\square$

**Lemma 4.15.** *Let  $q = p^{\deg(\beta)}$ . Then, for every  $n \geq 1$ ,*

$$\left| \mathbb{P}\left(\frac{\text{coker}(\mathbf{M}_{p,\beta})}{p \text{coker}(\mathbf{M}_{p,\beta})} \cong \frac{\mathbb{F}_p[x]}{\beta(x)\mathbb{F}_p[x]}\right) - \frac{1}{q} \prod_{i \geq 0} \left(1 - \frac{1}{q^{2i+1}}\right) \right| \leq \frac{3}{q^n} \quad (4.43)$$

*Proof.* Denote  $\mathbb{F}_q \cong \mathbb{F}_p[x]/\beta(x)\mathbb{F}_p[x]$ . Note that  $\text{coker}(\mathbf{M}_{p,\beta})/p \text{coker}(\mathbf{M}_{p,\beta}) \cong \mathbb{F}_q$  implies that  $\text{coker}(\mathbf{M}_{p,\beta}) \otimes_{R_{p,\beta}} \mathbb{F}_q \cong \mathbb{F}_q$  which is only possible if  $\mathbf{M}_{p,\beta}$  has rank  $n-1$  over  $\mathbb{F}_q$ . Hence, by Corollary 4.6, it holds with  $k \sim \text{Haar}(pR_{p,\beta} + \beta(x)R_{p,\beta})$  that

$$\mathbb{P}(\text{coker}(\mathbf{M}_{p,\beta})/p \text{coker}(\mathbf{M}_{p,\beta}) \cong \mathbb{F}_q) = \mathbb{P}(\text{rank}_q(\mathbf{M}_{p,\beta}) = n-1) \mathbb{P}(\text{coker}(k)/p \text{coker}(k) \cong \mathbb{F}_q). \quad (4.44)$$

Decompose  $k = k_1p + k_2\beta(x)$  for  $k_1, k_2 \sim \text{Haar}(R_{p,\beta})$ . Then, it holds that  $\text{coker}(k)/p \text{coker}(k) \cong \mathbb{F}_q$  if and only if and only if  $k_2 \notin pR_{p,\beta} + \beta(x)R_{p,\beta}$ . Hence, (4.43) follows from (4.44) by using [19, Theorem 4.1] (recall (4.17)) to estimate the probability of rank  $n-1$  and using that  $k_2$  reduces to a nonzero element in  $\mathbb{F}_q$  with probability  $1 - 1/q$ . We here simplified using that  $(1 - 1/q)/(q - 1) = 1/q$ .  $\square$

**Lemma 4.16.** *Let  $q = p^{\deg(\beta)}$ . Then, for every  $n \geq 1$ ,*

$$\left| \mathbb{P}\left(\frac{\text{coker}(\mathbf{M}_{p,\beta})}{p \text{coker}(\mathbf{M}_{p,\beta})} \cong \frac{\mathbb{F}_p[x]}{\beta(x)^2\mathbb{F}_p[x]}, \frac{\text{coker}(\mathbf{M}_{p,\beta})}{\beta(x) \text{coker}(\mathbf{M}_{p,\beta})} \cong \frac{\mathbb{F}_p[x]}{\beta(x)\mathbb{F}_p[x]}\right) - \frac{1}{q^2} \left(1 - \frac{1}{q}\right) \prod_{i \geq 0} \left(1 - \frac{1}{q^{2i+1}}\right) \right| \leq \frac{3}{q^n}. \quad (4.45)$$

*Proof.* Denote  $\mathbb{F}_q := \mathbb{F}_p[x]/\beta(x)\mathbb{F}_p[x]$ . In particular, the event on the left-hand side of (4.45) implies that  $\text{coker}(\mathbf{M}_{p,\beta}) \otimes_{R_{p,\beta}} \mathbb{F}_q \cong \mathbb{F}_q$ , which necessitates that  $\text{rank}_q(\mathbf{M}_{p,\beta}) = n-1$ . Hence, by the law of total probability and Corollary 4.6, it holds with  $k \sim \text{Haar}(pR_{p,\beta} + \beta(x)R_{p,\beta})$  that

$$\begin{aligned} & \mathbb{P}\left(\frac{\text{coker}(\mathbf{M}_{p,\beta})}{p \text{coker}(\mathbf{M}_{p,\beta})} \cong \frac{\mathbb{F}_p[x]}{\beta(x)^2\mathbb{F}_p[x]}, \frac{\text{coker}(\mathbf{M}_{p,\beta})}{\beta(x) \text{coker}(\mathbf{M}_{p,\beta})} \cong \frac{\mathbb{F}_p[x]}{\beta(x)\mathbb{F}_p[x]}\right) \\ &= \mathbb{P}\left(\text{rank}_q(\mathbf{M}_{p,\beta}) = n-1\right) \mathbb{P}\left(\frac{\text{coker}(k)}{p \text{coker}(k)} \cong \frac{\mathbb{F}_p[x]}{\beta(x)^2\mathbb{F}_p[x]}, \frac{\text{coker}(k)}{\beta(x) \text{coker}(k)} \cong \frac{\mathbb{F}_p[x]}{\beta(x)\mathbb{F}_p[x]}\right). \end{aligned} \quad (4.46)$$

Decompose  $k = k_1p + k_2\beta(x)$  for  $k_1, k_2 \sim \text{Haar}(R_{p,\beta})$  independent. Then,  $\text{coker}(k)/p \text{coker}(k) \cong \mathbb{F}_p[x]/\beta(x)^2\mathbb{F}_p[x]$  if and only if  $k_2 \equiv c\beta(x) \pmod{pR_{p,\beta} + \beta^2R_{p,\beta}}$  for some  $c \in \mathbb{F}_q \setminus \{0\}$ . It follows from the explicit power series representation (2.8) that this occurs with probability  $q^{-1}(1 - q^{-1})$ , since we require that the first coefficient in  $k_2 = \sum_{i=0}^{\infty} c_i\beta^i$  vanishes modulo  $p$  while the second should not. It further holds that  $\text{coker}(k)/\beta(x) \text{coker}(k) \cong \mathbb{F}_p[x]/\beta(x)\mathbb{F}_p[x]$  if and only if  $k_1$  has nonzero reduction in  $\mathbb{F}_q$ , which occurs with probability  $1 - q^{-1}$ . Hence, by the independence of  $k_1$  and  $k_2$ ,

$$\mathbb{P}\left(\frac{\text{coker}(k)}{p \text{coker}(k)} \cong \frac{\mathbb{F}_p[x]}{\beta(x)^2\mathbb{F}_p[x]}, \frac{\text{coker}(k)}{\beta(x) \text{coker}(k)} \cong \frac{\mathbb{F}_p[x]}{\beta(x)\mathbb{F}_p[x]}\right) = \frac{1}{q} \left(1 - \frac{1}{q}\right)^2. \quad (4.47)$$

Using [19, Theorem 4.1] (recall (4.17)) to estimate the probability of rank  $n-1$  in (4.46) and simplifying using that  $q^{-1}(1 - q^{-1})^2/(q - 1) = q^{-2}(1 - q^{-1})$  now yields (4.45).  $\square$

Recall conditions  $\mathcal{D}_p^1$  and  $\mathcal{D}_p^2$  from Definitions 4.12 and 4.13. Combining Lemmas 4.14 to 4.16 yields our main result concerning the satisfaction frequency of these conditions in the profinite model. In particular, the following Theorem 4.17 justifies Conjecture 1.7:

**Theorem 4.17.** *Let  $\mathbf{M} \sim \text{SymHaar}(\widehat{R}^{n \times n})$ . Then, for every fixed prime  $p$ ,*

$$\lim_{n \rightarrow \infty} \mathbb{P}\left(\text{coker}(\mathbf{M} - x\mathbf{I}) \text{ satisfies condition } \mathcal{D}_p^1\right) = \left(1 - \frac{1}{p}\right) \prod_{i=1}^{\infty} \left(1 - \frac{1}{p^{2i}}\right), \quad (4.48)$$

$$\lim_{n \rightarrow \infty} \mathbb{P}\left(\text{coker}(\mathbf{M} - x\mathbf{I}) \text{ satisfies condition } \mathcal{D}_p^1 \text{ or } \mathcal{D}_p^2\right) = \left(1 - \frac{1}{p^2} \frac{3p-1}{p+1}\right) \prod_{i=1}^{\infty} \left(1 - \frac{1}{p^{2i}}\right). \quad (4.49)$$

Moreover, let  $\mathcal{D}^*$  denote the condition that  $\mathcal{D}_p^1$  or  $\mathcal{D}_p^2$  is satisfied for every odd prime  $p$ , and that  $\mathcal{D}_p^1$  is satisfied for  $p = 2$ . Then,

$$\lim_{n \rightarrow \infty} \mathbb{P}\left(\text{coker}(\mathbf{M} - x\mathbf{I}) \text{ satisfies condition } \mathcal{D}^*\right) = \frac{6}{7} \prod_{\text{primes } p} \left(1 - \frac{1}{p^2} \frac{3p-1}{p+1}\right) \prod_{i=1}^{\infty} \left(1 - \frac{1}{p^{2i}}\right). \quad (4.50)$$

*Proof.* That limits may be exchanged with infinite products here follows similarly to the proof of Theorem 4.11, so we omit these details for brevity. It then follows by substituting the limiting values of Lemmas 4.14 and 4.15 in Definition 4.12 using independence that

$$\lim_{n \rightarrow \infty} \mathbb{P} \left( \text{coker}(\mathbf{M} - x\mathbf{I}) \text{ satisfies condition } \mathcal{D}_p^1 \right) = \prod_{\beta(x)} \left( 1 + \frac{1}{p^{\deg(\beta)}} \right) \prod_{i=0}^{\infty} \left( 1 - \frac{1}{p^{(2i+1)\deg(\beta)}} \right). \quad (4.51)$$

Combining the first factor and the factor with  $i = 0$  in the second product using that  $(1 + p^{-\deg(\beta)})(1 - p^{-\deg(\beta)}) = 1 - p^{2\deg(\beta)}$  and subsequently using Lemma 4.10 now yields (4.42).

The event  $\mathcal{D}_p^2$  can be subdivided in  $p$  mutually exclusive events depending on  $a \bmod p$ . Hence, substituting the limiting values from Lemmas 4.14 to 4.16 in Definition 4.13,

$$\begin{aligned} & \lim_{n \rightarrow \infty} \mathbb{P} \left( \text{coker}(\mathbf{M} - x\mathbf{I}) \text{ satisfies condition } \mathcal{D}_p^2 \right) \quad (4.52) \\ &= \sum_{a=0}^{p-1} \left( \frac{1}{p^2} \left( 1 - \frac{1}{p} \right) \prod_{i=0}^{\infty} \left( 1 - \frac{1}{p^{2i+1}} \right) \right) \prod_{\beta \neq x-a} \left( 1 + \frac{1}{p^{\deg(\beta)}} \right) \prod_{i=0}^{\infty} \left( 1 - \frac{1}{p^{(2i+1)\deg(\beta)}} \right) \\ &= \frac{1}{p} \frac{1 - 1/p}{1 + 1/p} \prod_{\beta(x)} \left( 1 + \frac{1}{p^{\deg(\beta)}} \right) \prod_{i=0}^{\infty} \left( 1 - \frac{1}{p^{(2i+1)\deg(\beta)}} \right) \\ &= \frac{1}{p} \frac{1 - 1/p}{1 + 1/p} \lim_{n \rightarrow \infty} \mathbb{P} \left( \text{coker}(\mathbf{M} - x\mathbf{I}) \text{ satisfies condition } \mathcal{D}_p^1 \right). \end{aligned}$$

Here, the final equality used (4.51). Combine (4.48) and (4.52) using that  $\mathcal{D}_p^1$  and  $\mathcal{D}_p^2$  are mutually exclusive, and simplify using that  $(1 + p^{-1}(1 - p^{-1})/(1 + p^{-1})) \times (1 - p^{-1}) = 1 - p^{-2}(3p - 1)/(p + 1)$  to find (4.49).

Finally, (4.50) follows by taking the product of (4.49) over all odd primes  $p$ , and multiplying with the value of (4.48) at  $p = 2$ , using that  $1 - p^{-1} = (6/7)(1 - p^{-2}(3p - 1)/(p + 1))$  for  $p = 2$ .  $\square$

**Remark 4.18.** Note that while (4.49) is also valid for  $p = 2$ , the rephrasing of  $p \parallel \Delta_{\mathbf{M}}$  in Propositions 3.5 and 3.10 are only valid for odd primes. Indeed,  $2 \mid \Delta_{\phi}$  implies that  $2^2 \mid \Delta_{\phi}$  for any monic  $\phi \in \mathbb{Z}[x]$ ; see [2, Proposition 6.7]. This is why (1.6) in Conjecture 1.7 is specific to odd primes.

## 5. CONCLUSION

Prior to this work, the probabilistic understanding of spectral characterization conditions was mostly limited to numerical data, especially in the presence of a symmetry constraint. We here developed a theoretical framework that involves studying abstract-algebraic objects in analytically tractable profinite random matrix ensembles. In particular, this enabled the first specific conjectures on the satisfaction frequency of spectral characterization conditions. Further, the rigorous theory of the considered conditions is now reduced to specific but nontrivial technical challenges, such as universality results that would enable extension beyond analytically tractable ensembles.

The developed framework has potential for application to other sufficient conditions and settings. One question in this regard surrounds the exceptional phenomena surrounding the prime 2, such as the fact that different behavior for  $\det(\mathbf{W})$  and  $\Delta_{\mathbf{M}}$  then occurs for simple graphs, or if the random vector  $\zeta$  is replaced by the all-ones vector. Specifically, Tables 3 and 4 suggests that the prediction in (1.2) for the probability that  $p^2$  divides the determinant is universal in terms of the vector  $\zeta$ , *except* for the all-ones vector. For the latter, the empirical probabilities agree with those from Table 1 and Conjecture 1.4 for odd primes, but a slightly different empirical probability arises when  $p = 2$ .

In a future work, we intend to pursue extensions of the framework of the present paper to explain such exceptional phenomena. This will involve richer algebraic structures and different analytically tractable random matrix models.

**Acknowledgements.** Alexander Van Werde is funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany's Excellence Strategy EXC 2044/2 - 390685587, Mathematics Münster: Dynamics–Geometry–Structure.

**Code.** The code used to produce Tables 1 to 4 can be found at <https://github.com/Alexander-Van-Werde/SourceCode-On-the-satisfaction-frequency-of-spectral-characterization-conditions>

$p^2 \nmid \det(\mathbf{W})$	$n = 8$	$n = 10$	$n = 12$	$n = 15$	$n = 25$	$n = 50$	$n = 100$	Conjecture 1.4
$p = 2$	0.414	0.423	0.428	0.430	0.430	0.431	0.431	0.47336955677...
$p = 3$	0.556	0.653	0.712	0.748	0.758	0.758	0.757	0.75752129361...
$p = 5$	0.608	0.746	0.839	0.898	0.914	0.914	0.914	0.91393033780...
$p = 7$	0.622	0.771	0.872	0.939	0.957	0.957	0.957	0.95674525798...
$p = 11$	0.630	0.785	0.892	0.963	0.983	0.983	0.983	0.98279431682...

TABLE 3. Estimated probability that  $p^2 \nmid \det(\mathbf{W})$  when  $\mathbf{M}$  is the adjacency matrix of a random graph with loops, as in Conjecture 1.4, but  $\zeta = (1, \dots, 1)^\top$  deterministically. For  $p = 2$ , we observe a statistically significant discrepancy with the setting of Conjecture 1.4 and Table 1 where  $\zeta$  was random. These estimates used  $10^6$  samples.

$p^2 \nmid \det(\mathbf{W})$	$n = 8$	$n = 10$	$n = 12$	$n = 15$	$n = 25$	$n = 50$	$n = 100$	Conjecture 1.4
$p = 2$	0.440	0.459	0.468	0.472	0.473	0.474	0.473	0.47336955677...
$p = 3$	0.565	0.657	0.714	0.748	0.757	0.758	0.757	0.75752129361...
$p = 5$	0.618	0.657	0.840	0.898	0.913	0.914	0.914	0.91393033780...
$p = 7$	0.632	0.773	0.873	0.939	0.957	0.956	0.957	0.95674525798...
$p = 11$	0.641	0.788	0.893	0.963	0.983	0.983	0.983	0.98279431682...

TABLE 4. Estimated probability that  $p^2 \nmid \det(\mathbf{W})$  when  $\mathbf{M}$  is the adjacency matrix of a random graph with loops but  $\zeta = (1, 0, \dots, 0)^\top$  is the indicator vector of the first coordinate. The indicator vector was here arbitrarily chosen as a vector that has different structure from both the all-ones vector and a random vector, thus giving a natural test for what universality could be expected. We observe that the data matches Conjecture 1.4, also for  $p = 2$ . These estimates used  $10^6$  samples.

#### REFERENCES

- [1] G. Anderson, A. Guionnet, and O. Zeitouni. *An introduction to random matrices*. Cambridge university press, 2010. doi: 10.1017/CBO9780511801334.
- [2] A. Ash, J. Brakenhoff, and T. Zarrabi. Equality of polynomial and field discriminants. *Experimental Mathematics*, 2007. doi: 10.1080/10586458.2007.10129001.
- [3] M. Atiyah and I. Macdonald. *Introduction to commutative algebra*. Addison-Wesley Publishing Company, 1969. doi: 10.1201/9780429493638.
- [4] 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.
- [5] L. Carlitz. Representations by quadratic forms in a finite field. *Duke Mathematical Journal*, 1954. doi: 10.1215/S0012-7094-54-02114-6.
- [6] Y. Chao, W. Wang, and H. Zhang. A new criterion for oriented graphs to be determined by their generalized skew spectrum. *Linear Algebra and its Applications*, 2025. doi: 10.1016/j.laa.2025.04.026.
- [7] G. Cheong and Y. Huang. The cokernel of a polynomial push-forward of a random integral matrix with concentrated residue. *Mathematical Proceedings of the Cambridge Philosophical Society*, 2025. doi: 10.1017/S0305004125000064.
- [8] G. Cheong and N. Kaplan. Generalizations of results of Friedman and Washington on cokernels of random  $p$ -adic matrices. *Journal of Algebra*, 2022. doi: 10.1016/j.jalgebra.2022.03.035.
- [9] G. Cheong, Y. Liang, and M. Strand. Polynomial equations for matrices over integers modulo a prime power and the cokernel of a random matrix. *Linear Algebra and its Applications*, 2023. doi: 10.1016/j.laa.2023.07.031.
- [10] G. Cheong and M. Yu. The distribution of the cokernel of a polynomial evaluated at a random integral matrix. *arXiv preprint arXiv:2303.09125*, 2023. doi: 10.48550/arXiv.2303.09125.
- [11] J. Clancy, N. Kaplan, T. Leake, S. Payne, and M. Wood. On a Cohen–Lenstra heuristic for Jacobians of random graphs. *Journal of Algebraic Combinatorics*, 2015. doi: 10.1007/s10801-015-0598-x.

- [12] J. Clancy, T. Leake, and S. Payne. A note on Jacobians, Tutte polynomials, and two-variable zeta functions of graphs. *Experimental Mathematics*, 2015. doi: 10.1080/10586458.2014.917443.
- [13] L. Collatz and U. Sinogowitz. Spektren endlicher Grafen. In *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, 1957. doi: 10.1007/BF02941924.
- [14] D. Dummit and R. Foote. *Abstract Algebra*. John Wiley & Sons, third edition, 2004.
- [15] D. Eisenbud. *Commutative algebra: with a view toward algebraic geometry*. Springer Science & Business Media, 1995. doi: 10.1007/978-1-4612-5350-1.
- [16] L. Erdős, A. Knowles, H.-T. Yau, and J. Yin. Spectral statistics of Erdős–Rényi graphs I: Local semicircle law. *Annals of Probability*, 2013. doi: 10.1214/11-AOP734.
- [17] S. Evans. Elementary divisors and determinants of random matrices over a local field. *Stochastic Processes and their Applications*, 2002. doi: 10.1016/S0304-4149(02)00187-4.
- [18] A. Farrugia. The overgraphs of generalized cospectral controllable graphs. *The Electronic Journal of Combinatorics*, 2019. doi: 10.37236/7883.
- [19] J. Fulman and L. Goldstein. Stein’s method and the rank distribution of random matrices over finite fields. *Annals of Probability*, 2015. doi: 10.1214/13-AOP889.
- [20] I. Gelfand, M. Kapranov, and A. Zelevinsky. *Discriminants, Resultants, and Multidimensional Determinants*. Birkhäuser Boston, 1994. doi: 10.1007/978-0-8176-4771-1.
- [21] C. Godsil and B. McKay. Constructing cospectral graphs. *Aequationes Mathematicae*, 1982. doi: 10.1007/BF02189621.
- [22] F. Gouvêa. *p-adic numbers: an introduction*. Springer, 2020. doi: 10.1007/978-3-030-47295-5.
- [23] S. Guo and W. Wang. Primary decomposition theorem and generalized spectral characterization of graphs. *Advances in Applied Mathematics*, 2025. doi: 10.1016/j.aam.2025.102927.
- [24] W. Haemers and E. Spence. Enumeration of cospectral graphs. *European Journal of Combinatorics*, 2004. doi: 10.1016/S0195-6698(03)00100-8.
- [25] E. Hodges. The distribution of sandpile groups of random graphs with their pairings. *Transactions of the American Mathematical Society*, 2024. doi: 10.1090/tran/9244.
- [26] A. Jaikin-Zapirain. The finite and solvable genus of finitely generated free and surface groups. *Research in the Mathematical Sciences*, 2023. doi: 10.1007/s40687-023-00408-9.
- [27] 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.
- [28] J. Kahn and J. Komlós. Singularity probabilities for random matrices over finite fields. *Combinatorics, Probability and Computing*, 2001. doi: 10.1017/S096354830100462X.
- [29] S. Katok. *p-adic analysis compared with real*. American Mathematical Society, 2007.
- [30] I. Koval and M. Kwan. Exponentially many graphs are determined by their spectrum. *The Quarterly Journal of Mathematics*, 2024. doi: 10.1093/qmath/haae030.
- [31] J. Lee. Joint distribution of the cokernels of random  $p$ -adic matrices. *Forum Mathematicum*, 2023. doi: 10.1515/forum-2022-0209.
- [32] K. Luh and S. O’Rourke. Eigenvectors and controllability of non-hermitian random matrices and directed graphs. *Electronic Journal of Probability*, 2021. doi: 10.1214/21-EJP588.
- [33] J. MacWilliams. Orthogonal matrices over finite fields. *The American Mathematical Monthly*, 1969. doi: 10.2307/2317262.
- [34] S. Meehan and H. Nguyen. Eigenvectors of random matrices of symmetric entry distributions. *Proceedings of the American Mathematical Society*, 2019. doi: 10.1090/proc/14284.
- [35] H. Nguyen and M. Wood. Local and global universality of random matrix cokernels. *Mathematische Annalen*, 2025. doi: 10.1007/s00208-024-03050-0.
- [36] 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.
- [37] 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.
- [38] L. Qiu, W. Wang, and H. Zhang. Smith normal form and the generalized spectral characterization of graphs. *Discrete Mathematics*, 2023. doi: 10.1016/j.disc.2022.113177.
- [39] M. Reid. *Undergraduate commutative algebra*. Cambridge University Press, 1995. doi: 10.1017/CBO9781139172721.
- [40] L. Ribes. *Profinite graphs and groups*. Springer, 2017. doi: 10.1007/978-3-319-61199-0.

- [41] A. Robert. *A course in  $p$ -adic analysis*. Springer Science & Business Media, 2000. doi: 10.1007/978-1-4757-3254-2.
- [42] M. Rosen. *Number theory in function fields*. Springer Science & Business Media, 2013. doi: 10.1007/978-1-4757-6046-0.
- [43] J. Shen and R. Van Peski. Eigenvalues of  $p$ -adic random matrices. *arXiv preprint arXiv:2601.06283*, 2026. doi: 10.48550/arXiv.2601.06283.
- [44] 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.
- [45] A. Van Werde. In preparation.
- [46] A. Van Werde. Cokernel statistics for walk matrices of directed and weighted random graphs. *Combinatorics, Probability and Computing*, 2025. doi: 10.1017/S0963548324000312.
- [47] 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.
- [48] A. Van Werde. Exact cospectrality probabilities for uniform random matrices. *arXiv preprint arXiv:2602.00233*, 2026. doi: 10.48550/arXiv.2602.00233.
- [49] V. Vu. Combinatorial problems in random matrix theory. In *Proceedings of the International Congress of Mathematicians, Seoul 2014*, volume IV, pages 489–508, 2014. <https://www.mathunion.org/fileadmin/ICM/Proceedings/ICM2014.4/ICM2014.4.pdf>.
- [50] V. Vu. Recent progress in combinatorial random matrix theory. *Probability Surveys*, 2021. doi: 10.1214/20-PS346.
- [51] 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.
- [52] W. Wang and F. Liu. Generalized spectral characterizations of almost controllable graphs. *European Journal of Combinatorics*, 2021. doi: 10.1016/j.ejc.2021.103348.
- [53] W. Wang and W. Wang. Haemers’ conjecture: an algorithmic perspective. *Experimental Mathematics*, 2025. doi: 10.1080/10586458.2024.2337229.
- [54] 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.
- [55] 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.
- [56] W. Wang and F. Zhu. An improved condition for a graph to be determined by its generalized spectrum. *European Journal of Combinatorics*, 2023. doi: 10.1016/j.ejc.2022.103638.
- [57] G. Wilkes. *Profinite groups and residual finiteness*. EMS Press, 2024. doi: 10.4171/ETB/27.
- [58] M. Wood. The distribution of sandpile groups of random graphs. *Journal of the American Mathematical Society*, 2017. doi: 10.1090/jams/866.
- [59] M. Wood. Random integral matrices and the Cohen–Lenstra heuristics. *American Journal of Mathematics*, 2019. doi: 10.1353/ajm.2019.0008.
- [60] J. Yang and W. Wang. An improved condition for a family of trees being determined by their generalized spectrum. *Discrete Mathematics*, 2024. doi: 10.1016/j.disc.2024.113956.

APPENDIX A. PROOF OF LEMMA 2.3

*Proof.* By the Cayley–Hamilton theorem applied to the finitely generated  $\mathbb{Z}$ -module  $\mathcal{M}$ , there exists a non-constant monic polynomial  $Q \in \mathbb{Z}[x]$  with  $Q(x)\mathcal{M} = 0$  [3, Proposition 2.4]. Consider the factorization  $Q \equiv \prod_i \beta_i(x)^{e_i} \pmod{p}$  into powers of coprime irreducible monic polynomials  $\beta_i(x) \in \mathbb{F}_p[x]$ . Hensel’s lemma [22, Theorem 4.7.2] then yields monic polynomials  $Q_i \in \mathbb{Z}_p[x]$  with

$$Q(x) = \prod_i Q_i(x) \quad \text{and} \quad Q_i(x) \equiv \beta_i(x)^{e_i} \pmod{p}. \quad (\text{A.1})$$

The ideals  $Q_i\mathbb{Z}_p[x]$  and  $Q_j\mathbb{Z}_p[x]$  are coprime for  $i \neq j$ . Indeed,  $\mathbb{F}_p[x]/(\beta_i^{e_i}[x]\mathbb{F}_p[x] + \beta_j^{e_j}\mathbb{F}_p[x]) = 0$  by coprimality of the  $\beta_i$  and hence  $\mathbb{Z}_p[x]/(Q_i\mathbb{Z}_p[x] + Q_j\mathbb{Z}_p[x]) = 0$  by Nakayama’s lemma over  $\mathbb{Z}_p$  [3, Proposition 2.6]. Hence,  $\mathbb{Z}_p[x]/Q(x)\mathbb{Z}_p[x] \cong \bigoplus_i \mathbb{Z}_p[x]/Q_i(x)\mathbb{Z}_p[x]$  by the Chinese remainder theorem. Now, using that  $Q(x)\mathcal{M}_p = 0$  by the definition of  $Q$ ,

$$\mathcal{M}_p \cong \mathcal{M}_p \otimes_{\mathbb{Z}_p[x]} \frac{\mathbb{Z}_p[x]}{Q(x)\mathbb{Z}_p[x]} \cong \bigoplus_i \left( \mathcal{M}_p \otimes_{\mathbb{Z}_p[x]} \frac{\mathbb{Z}_p[x]}{Q_i(x)\mathbb{Z}_p[x]} \right). \quad (\text{A.2})$$

We claim that it now remains to prove that

$$(\mathbb{Z}_p[x]/Q_i(x)\mathbb{Z}_p[x]) \otimes_{\mathbb{Z}_p[x]} R_{p,\beta_j} = \begin{cases} \mathbb{Z}_p[x]/Q_i(x)\mathbb{Z}_p[x] & \text{if } i = j, \\ 0 & \text{else.} \end{cases} \quad (\text{A.3})$$

Indeed, using (A.3) and  $\mathcal{M}_{p,\beta} = \mathcal{M}_p \otimes_{\mathbb{Z}_p[x]} R_{p,\beta}$  with the associativity in the tensor product in (A.2) then yields  $\mathcal{M}_p \otimes_{\mathbb{Z}_p[x]} \mathbb{Z}_p[x]/Q_i\mathbb{Z}_p[x] \cong \mathcal{M}_{p,\beta}$ , so that Lemma 2.3 indeed follows.

We next prove (A.3). Recall the classical fact that  $I$ -adic completion of a finitely generated module over a Noetherian ring is equivalent to an extension of scalars [3, Proposition 10.13]. That is, if  $\hat{\mathcal{N}}_I$  is the  $I$ -adic completion of a finitely generated  $R$ -module  $\mathcal{N}$  for an ideal  $I \subseteq R$  of a Noetherian ring  $R$ , defined as the inverse limit of the system  $\{\mathcal{N}/I^n\mathcal{N} : n \geq 1\}$ , then  $\hat{\mathcal{N}}_I \cong \mathcal{N} \otimes_R \hat{R}_I$  with  $\hat{R}_I$  the  $I$ -adic completion of the ring. Denote  $\mathcal{Q}_i := \mathbb{Z}_p[x]/Q_i(x)\mathbb{Z}_p[x]$  and  $\mathfrak{m}_j = p\mathbb{Z}_p[x] + \beta_j(x)\mathbb{Z}_p[x]$ . Then,

$$\mathcal{Q}_i \otimes_{\mathbb{Z}_p[x]} R_{p,\beta_j} \cong \widehat{(\mathcal{Q}_i)_{\mathfrak{m}_j}} = \left\{ (q_n)_{n \geq 1} \in \prod_{n \geq 1} \frac{\mathcal{Q}_i}{\mathfrak{m}_j^n \mathcal{Q}_i} : \forall n, q_{n+1} \equiv q_n \pmod{\mathfrak{m}_j^n \mathcal{Q}_i} \right\}. \quad (\text{A.4})$$

Let us start with the case  $i \neq j$  in (A.3). The assumption that the  $\beta_i$  have coprime reductions in  $\mathbb{F}_p[x]$  implies that  $\beta_i^{e_i}\mathbb{F}_p[x] + \beta_j\mathbb{F}_p[x] = \mathbb{F}_p[x]$ . Thus, it follows from  $Q_i \equiv \beta_i^{e_i} \pmod{p}$  that  $\mathcal{Q}_i/\mathfrak{m}_j\mathcal{Q}_i \cong \mathbb{Z}_p[x]/(Q_i\mathbb{Z}_p[x] + p\mathbb{Z}_p[x] + \beta_j\mathbb{Z}_p[x]) \cong \mathbb{F}_p[x]/(\beta_i^{e_i}\mathbb{F}_p[x] + \beta_j\mathbb{F}_p[x]) \cong 0$ . This means that  $\mathfrak{m}_j\mathcal{Q}_i = \mathcal{Q}_i$  and hence  $\mathfrak{m}_j^n\mathcal{Q}_i = \mathcal{Q}_i$  for all  $n \geq 1$ . Hence,  $\mathcal{Q}_i \otimes_{\mathbb{Z}_p[x]} R_{p,\beta_j} \cong 0$  by (A.4), as desired.

Now assume that  $i = j$ . The assumption that  $Q_i \equiv \beta_i^{e_i} \pmod{p}$  then implies that  $\beta_i^{e_i}\mathcal{Q}_i \subseteq p\mathcal{Q}_i$ . It follows that  $(\mathfrak{m}_i)^{e_i}\mathcal{Q}_i \subseteq p\mathcal{Q}_i \subseteq \mathfrak{m}_i\mathcal{Q}_i$  and hence, for all  $n \geq 1$ ,

$$(\mathfrak{m}_i)^{ne_i}\mathcal{Q}_i \subseteq p^n\mathcal{Q}_i \subseteq \mathfrak{m}_i^n\mathcal{Q}_i. \quad (\text{A.5})$$

Inclusion of ideal filtrations implies isomorphism of the associated completions [15, Lemma 7.14]. Hence,  $\widehat{(\mathcal{Q}_i)_{\mathfrak{m}_i}} \cong \widehat{(\mathcal{Q}_i)_{p\mathbb{Z}_p[x]}}$ . Now, using that completion are the same thing as extensions of scalars [3, Proposition 10.13] (recall (A.4)) and using that  $\mathbb{Z}_p[x]$  is its own  $p$ -adic completion,

$$\mathcal{Q}_i \otimes_{\mathbb{Z}_p[x]} R_{p,\beta_i} \cong \widehat{(\mathcal{Q}_i)_{\mathfrak{m}_i}} \cong \widehat{(\mathcal{Q}_i)_{p\mathbb{Z}_p[x]}} \cong \mathcal{Q}_i \otimes_{\mathbb{Z}_p[x]} \mathbb{Z}_p[x] \cong \mathcal{Q}_i. \quad (\text{A.6})$$

This yields the case  $i = j$  in (A.3) and hence concludes the proof.  $\square$

APPENDIX B. RECOVERING CONJECTURES WITHOUT SYMMETRY CONSTRAINT

Recall we claimed in Remark 4.1 that one can also use the profinite Haar method to recover [46, Conjecture 1.4] concerning walk matrices in a setting without symmetry. The conjecture is there stated in a setting with sparse matrices and specifically with odd primes and the all-ones vector, but those complications should not affect the universality class in the setting without symmetries. (A universality statement to this effect is given in [46, Theorem 1.3].) Hence, the key content that we wish to give an alternative justification for is as follows:

**Conjecture B.1.** Let  $\mathbf{M}$  be uniformly distributed on  $\{0, 1\}^{n \times n}$  and consider an independent uniform random vector  $\zeta \in \{0, 1\}^{n \times n}$ . Then,  $\mathbf{W} = [\zeta, \mathbf{M}\zeta, \dots, \mathbf{M}^{n-1}\zeta]$  satisfies that for every prime  $p$ ,

$$\lim_{n \rightarrow \infty} \mathbb{P}\left(p^2 \nmid \det(\mathbf{W})\right) = \left(1 + \frac{1}{p}\right) \prod_{i=1}^{\infty} \left(1 - \frac{1}{p^i}\right) \quad (\text{B.1})$$

The difference with the setting of Conjecture 1.4 is that the symmetry constraint is now removed. This makes the sufficient condition Theorem 4.11 non-applicable, but the walk matrix itself is naturally still a well-defined object and the rephrasing in Proposition 3.2 is still applicable.

Similar to Sections 4.1 and 4.3, we model Conjecture B.1 by studying the satisfaction frequency of condition  $\mathcal{W}_p$  for  $\text{coker}(\mathbf{M} - x\mathbf{I}, \zeta)$  when  $\mathbf{M} \sim \text{Haar}(\widehat{R}^{n \times n})$  and  $\zeta \sim \text{Haar}(\widehat{R}^n)$ . By translation invariance and independence, this again reduces to the study of the pieces over the local ring  $R_{p,\beta}$ .

**B.1. Reduction result.** Let  $(\mathcal{O}, \mathfrak{m})$  be a compact Noetherian local ring and recall that  $\text{rank}_q(\cdot)$  refers to the rank of a matrix over  $\mathbb{F}_q \cong \mathcal{O}/\mathfrak{m}$ . It follows from [19, Theorem 1.1] that a uniform random rectangular matrix  $\mathbf{U} \in \mathbb{F}_q^{n \times (n+m)}$  with  $m \geq 0$  satisfies that for every  $k \leq n$ ,

$$\left| \mathbb{P}(\text{rank}_q(\mathbf{U}) = n - k) - \frac{1}{q^{k(m+k)}} \frac{\prod_{i=k+1}^{\infty} (1 - 1/q^i)}{\prod_{i=1}^{k+m} (1 - 1/q^i)} \right| \leq \frac{3}{q^n}. \quad (\text{B.2})$$

The cokernel conditional on the rank is described by the following variant on Proposition 4.5:

**Proposition B.2.** Suppose that  $\mathbf{M} \sim \text{Haar}(\mathcal{O}^{n \times n})$ . Fix some  $k \leq n$  and let  $\mathbf{K} \sim \text{Haar}(\mathfrak{m}^{k \times k})$ . Then, we have an equality in distribution of random  $\mathcal{O}$ -modules:

$$\mathbb{P}\left(\text{coker}(\mathbf{M}) \in * \mid \text{rank}_q(\mathbf{M}) = n - k\right) = \mathbb{P}\left(\text{coker}(\mathbf{K}) \in *\right). \quad (\text{B.3})$$

*Proof.* This follows analogously to Proposition 4.5. Indeed, similar to Lemma 4.4 the  $\text{Haar}(\mathfrak{a}^{n \times n})$  distribution for any ideal  $\mathfrak{a} \subseteq \mathcal{O}$  is invariant under the map  $\mathbf{M} \mapsto \mathbf{G}_1 \mathbf{M} \mathbf{G}_2$  for any fixed  $\mathbf{G}_1, \mathbf{G}_2 \in \text{GL}_n(\mathcal{O})$ . Further, similar to Lemma 4.3 a matrix  $\mathbf{M} \in \mathcal{O}^{n \times n}$  has rank  $n - k$  if and only if there exist invertible  $\mathbf{G}_1, \mathbf{G}_2 \in \text{GL}_n(\mathcal{O})$  with  $\mathbf{G}_1 \mathbf{M} \mathbf{G}_2 = \text{diag}(\mathbf{Q}, \mathbf{K})$  for some  $\mathbf{K} \in \mathfrak{m}^{k \times k}$  and invertible  $\mathbf{Q} \in \text{GL}_{n-k}(\mathcal{O})$ . Using the aforementioned invariance similarly to the arguments preceding (4.11) allows us to assume without loss of generality that  $\mathbf{K} \sim \text{Haar}(\mathfrak{m}^{k \times k})$ , which yields (B.3).  $\square$

**Corollary B.3.** Suppose that  $\mathbf{M}_{p,\beta} \sim \text{Haar}(R_{p,\beta}^{n \times n})$ . Let  $\text{rank}_q(\cdot)$  refer to the rank over  $\mathbb{F}_q \cong \mathbb{Z}[x]/(p\mathbb{Z}[x] + \beta(x)\mathbb{Z}[x])$ . Then, for every  $k \leq n$ , as random  $R_{p,\beta}$  modules,

$$\mathbb{P}\left(\text{coker}(\mathbf{M}_{p,\beta}) \in * \mid \text{rank}_q(\mathbf{M}_{p,\beta}) = n - k\right) = \mathbb{P}\left(\text{coker}(\mathbf{K}) \in *\right), \quad (\text{B.4})$$

where  $\mathbf{K}$  is a  $k \times k$  matrix with entries Haar distributed on  $pR_{p,\beta} + \beta(x)R_{p,\beta}$ . That is,

$$\mathbf{K} \sim p \text{Haar}(R_{p,\beta}^{k \times k}) + \beta(x) \text{Haar}(R_{p,\beta}^{k \times k}). \quad (\text{B.5})$$

*Proof.* This is immediate from Proposition B.2 with  $\mathcal{O} = R_{p,\beta}$ .  $\square$

**B.2. Satisfaction frequency of condition  $\mathcal{W}_p$ .** Let  $\mathbf{M}_{p,\beta} \sim \text{Haar}(R_{p,\beta}^{n \times n})$  and  $\zeta_{p,\beta} \sim \text{Haar}(R_{p,\beta}^n)$ . The following Lemmas B.4 and B.5 replace the role of Lemmas 4.8 and 4.9.

**Lemma B.4.** Let  $q := p^{\deg(\beta)}$ . Then, for every  $n \geq 1$ ,

$$\left| \mathbb{P}(\text{coker}(\mathbf{M}_{p,\beta}, \zeta_{p,\beta}) \cong 0) - \prod_{i=2}^{\infty} \left(1 - \frac{1}{q^i}\right) \right| \leq \frac{3}{q^n}. \quad (\text{B.6})$$

*Proof.* Let  $\mathbb{F}_q := \mathbb{F}_p[x]/\beta(x)\mathbb{F}_p[x]$ . Then,

$$\mathbb{P}(\text{coker}(\mathbf{M}_{p,\beta}, \zeta_{p,\beta}) \cong 0) = \mathbb{P}(\text{rank}_q(\mathbf{M}_{p,\beta}, \zeta_{p,\beta}) = n). \quad (\text{B.7})$$

Applying (B.2) with  $\mathbf{U} = [\mathbf{M}_{p,\beta}, \zeta_{p,\beta}] \bmod p, \beta$  by taking  $m = 1$  and  $k = 0$  yields (B.6).  $\square$

**Lemma B.5.** Let  $q := p^{\deg(\beta)}$ . Then, every  $n \geq 2$ ,

$$\left| \mathbb{P}\left(\text{coker}(\mathbf{M}_{p,\beta}, \zeta_{p,\beta}) \cong \frac{\mathbb{F}_p[x]}{\beta(x)\mathbb{F}_p[x]}\right) - \frac{1}{q^2} \prod_{i=2}^{\infty} \left(1 - \frac{1}{q^i}\right) \right| \leq \frac{6}{q^n}. \quad (\text{B.8})$$

*Proof.* Let  $\mathbb{F}_q := \mathbb{F}_p[x]/\beta(x)\mathbb{F}_p[x]$ . By the law of total probability,

$$\begin{aligned} \mathbb{P}(\text{coker}(\mathbf{M}_{p,\beta}, \zeta_{p,\beta}) \cong \mathbb{F}_q) & \tag{B.9} \\ &= \mathbb{P}(\text{coker}(\mathbf{M}_{p,\beta}, \zeta_{p,\beta}) \cong \mathbb{F}_q \mid \text{rank}_q(\mathbf{M}_{p,\beta}) = n-1) \mathbb{P}(\text{rank}_q(\mathbf{M}_{p,\beta}) = n-1) \\ & \quad + \mathbb{P}(\text{coker}(\mathbf{M}_{p,\beta}, \zeta_{p,\beta}) \cong \mathbb{F}_q \mid \text{rank}_q(\mathbf{M}_{p,\beta}) = n-2) \mathbb{P}(\text{rank}_q(\mathbf{M}_{p,\beta}) = n-2). \end{aligned}$$

The probability conditional on rank  $n-1$  can be estimated as in (4.21)–(4.22) by using Corollary B.3 instead of Corollary 4.6. The arguments are entirely unchanged because symmetry constraints had no effect in the one-dimensional computations involved. In particular, we again find that

$$\mathbb{P}(\text{coker}(\mathbf{M}_{p,\beta(x)}, \zeta_{p,\beta}) \cong \mathbb{F}_q \mid \text{rank}_q(\mathbf{M}_{p,\beta}) = n-1) = q^{-1}(1-q^{-2})(1-q^{-1}). \tag{B.10}$$

Conditional on rank  $n-2$ , Corollary B.3 yields that  $\text{coker}(\mathbf{M}_{p,\beta})$  then has the same distribution as  $\text{coker}(\mathbf{K})$  with  $\mathbf{K}$  a  $2 \times 2$  matrix with entries Haar distributed on  $pR_{p,\beta} + \beta(x)R_{p,\beta}$ . Then,  $\text{coker}(\mathbf{M}_{p,\beta}, \zeta_{p,\beta})$  has the same distribution as  $\text{coker}(\mathbf{K}, Z)$  with  $Z \sim \text{Haar}(R_{p,\beta}^2)$ . Here, using that  $Z$  reduces to zero in  $\mathbb{F}_q^2$  with probability  $1/q^2$  as in (4.23),

$$\begin{aligned} \mathbb{P}(\text{coker}(\mathbf{M}_{p,\beta}, \zeta_{p,\beta}) \cong \mathbb{F}_q \mid \text{rank}_q(\mathbf{M}_{p,\beta}) = n-2) & \tag{B.11} \\ &= (1-q^{-2}) \mathbb{P}(\text{coker}(\mathbf{K}, Z) \cong \mathbb{F}_q \mid Z \not\equiv 0 \pmod{pR_{p,\beta} + \beta(x)R_{p,\beta}}). \end{aligned}$$

That  $Z$  has nonzero reduction is equivalent to the existence of  $\mathbf{G} \in \text{GL}_2(R_{p,\beta})$  with  $\mathbf{G}Z = (1, 0)^\top$ . The invariance of Haar( $\mathfrak{m}_{p,\beta}^{2 \times 2}$ ) here implies that  $\tilde{\mathbf{K}} = \mathbf{Q}\mathbf{K}$  has the same distribution as  $\mathbf{K}$ . Further,

$$\text{coker}(\mathbf{K}, Z) \cong \text{coker}(\mathbf{Q}\mathbf{K}, \mathbf{Q}Z) = \text{coker} \begin{pmatrix} \tilde{\mathbf{K}}_{1,1} & \tilde{\mathbf{K}}_{1,2} & 1 \\ \tilde{\mathbf{K}}_{2,1} & \tilde{\mathbf{K}}_{2,2} & 0 \end{pmatrix} \cong \text{coker}(\tilde{\mathbf{K}}_{2,1}, \tilde{\mathbf{K}}_{2,2}). \tag{B.12}$$

From here on, the arguments are again identical to those for Lemma 4.9. We thus again find that

$$\begin{aligned} \mathbb{P}(\text{coker}(\mathbf{M}_{p,\beta}, \zeta_{p,\beta}) \cong \mathbb{F}_q) & \tag{B.13} \\ &= q^{-1}(1-q^{-2})(1-q^{-1}) \mathbb{P}(\text{rank}_q(\mathbf{M}_{p,\beta}) = n-1) \\ & \quad + (1-q^{-2})^2(1-q^{-1}) \mathbb{P}(\text{rank}_q(\mathbf{M}_{p,\beta}) = n-2). \end{aligned}$$

The result (B.8) now follows from (B.2) with  $m=0$  and  $k \in \{1, 2\}$  by simplifying prefactors, since

$$\frac{(1-1/q^2)(1-1/q) \prod_{i=2}^{\infty} (1-1/q^i)}{q} + \frac{(1-1/q)(1-1/q^2)^2 \prod_{i=3}^{\infty} (1-1/q^i)}{q^4} = \frac{1}{q^2} \prod_{i=2}^{\infty} \left(1 - \frac{1}{q^i}\right). \tag{B.14}$$

□

Recall Definition 4.7 concerning condition  $\mathcal{W}_p$ . Combining Lemmas B.4 and B.5 yields the satisfaction frequency of this condition in the absence of a symmetry constraint. In particular, this provides an alternative justification for Conjecture B.1.

**Theorem B.6.** *Let  $\mathbf{M} \sim \text{Haar}(\widehat{R}^{n \times n})$  and  $\zeta \sim \text{Haar}(\widehat{R}^n)$ . Then, for every fixed prime  $p$ ,*

$$\lim_{n \rightarrow \infty} \mathbb{P}(\text{coker}(\mathbf{M} - x\mathbf{I}, \zeta) \text{ satisfies condition } \mathcal{W}_p) = \left(1 + \frac{1}{p}\right) \prod_{i=1}^{\infty} \left(1 - \frac{1}{p^i}\right). \tag{B.15}$$

*Proof.* That limits may be exchanged with infinite products here follows similarly to the proof of Theorem 4.11, so we omit these details for brevity. Using the translation invariance of the Haar distribution, studying  $\text{coker}(\mathbf{M} - x\mathbf{I}, \zeta)$  may be reduced to modules of the form  $\text{coker}(\mathbf{M}_{p,\beta}, \zeta_{p,\beta})$ . Hence, using that (W1) and (W2) are mutually exclusive in Definition 4.7 and subdividing the case (W2) by the  $p$  possibilities for  $a$  and using independence, it follows from Lemmas B.4 and B.5 that

$$\begin{aligned} \lim_{n \rightarrow \infty} \mathbb{P}(\text{coker}(\mathbf{M} - x\mathbf{I}, \zeta) \text{ satisfies condition } \mathcal{W}_p) & \tag{B.16} \\ &= \prod_{\beta(x)} \prod_{i=2}^{\infty} \left(1 - \frac{1}{p^{i \deg(\beta)}}\right) + \sum_{a=0}^{p-1} \frac{1}{p^2} \prod_{\beta(x)} \prod_{i=2}^{\infty} \left(1 - \frac{1}{p^{i \deg(\beta)}}\right) = \left(1 + \frac{1}{p}\right) \prod_{\beta(x)} \prod_{i=2}^{\infty} \left(1 - \frac{1}{p^{i \deg(\beta)}}\right). \end{aligned}$$

Use Lemma 4.10 to conclude. □