Research Statement

Yifeng Huang

One of my long-term research focus is to explore the combinatorics arising from algebraic or geometric objects. A prototypical example is the number of $\mathbb{F}_q$ points of the projective space $\mathbb{P}^n$ as a function of $n$. Many of these objects studied are examples of moduli spaces, spaces that classify all structures of a certain kind that one can possibly attach to a given object. The configuration spaces of $n$ points and the Hilbert schemes of $n$ points are typical examples of such spaces. The geometry of moduli spaces has played a crucial role in understanding these classifications. An important way to detect the geometry is via concrete numerical invariants, including Betti numbers and point counting over finite fields, and numerous results in the past decades reveal that these quantities often fit together well combinatorially.

It frequently appears that a combinatorial phenomenon is shared by several seemingly unrelated instances of the problem above. I have been investigating specific problems motivated by such an analogy, and it has led me to discover surprising connections between different numerical invariants and different moduli spaces. These works are described in Section 1 and 2 below.

Apart from this long-term project, I have also worked on Diophantine theory in noncommutative setting and arithmetic dynamics (Section 3), as well as random matrices over the $p$-adic integers $\mathbb{Z}_p$ (Section 4).

1 Cohomology of configuration spaces [5, 15]

The configuration space of $n$ points on a topological space $X$ can be thought of as a space that classifies all $n$-element subsets of $X$. In specific, the (unordered) configuration space of $n$ points on $X$ is a space defined as:

$$\text{Conf}^n(X) := \{(x_1, \ldots, x_n) \in X^n : x_i \neq x_j \text{ for } i \neq j\},$$

where the symmetric group $S_n$ acts on $X^n$ by permuting coordinates.

The topology of configuration spaces has long been an active research area, and the study of its cohomology has been fruitful. In 1969, Arnol’d [1] found the Betti numbers of $\text{Conf}^n(X)$ for all $n$ if $X = \mathbb{R}^2$. More and more examples of $X$ have been studied ever since, and the answers are sensitive to the topology of $X$. However, the point-count story has a uniform answer: if $X$ is a quasi-projective variety over a finite field $\mathbb{F}_q$, then $\text{Conf}^n(X)$ is also defined as a quasiprojective variety, and [27] by Vakil and Wood shows that $\# \text{Conf}^n(X)(\mathbb{F}_q)$ can be computed from a rational generating function via a single formula that works for all quasiprojective $X$.

The nicest case in the story for Betti numbers of configuration spaces is the case $X = \mathbb{C} - \{P_1, \ldots, P_r\}$, where $r \geq 0$ and $P_1, \ldots, P_r$ are points. Here, the Betti numbers of $\text{Conf}^n(X)$ can be extracted from the “same” rational generating function that gives $\# \text{Conf}^n(X)(\mathbb{F}_q)$. It is natural to ask if a similar phenomenon can occur for another space $X$.

1.1 Punctured torus [5]

G. Cheong and I [5] recently found a rational generating function whose coefficients give the singular Betti numbers $h^i(\text{Conf}^n(X))$, where $X$ is a one-punctured elliptic curve over $\mathbb{C}$ (namely, an elliptic curve with one point removed).

**Theorem 1.1** (Cheong and H.). Keeping the notation above, we have

$$\sum_{n=0}^{\infty} \sum_{i=0}^{\infty} (-1)^i h^i(\text{Conf}^n(X)) u^{2n-i} t^n = \frac{(1 - ut)^2(1 - u^2t^2)}{(1 - u^2t)(1 - ut^2)^2},$$

where

$$w(i) := \begin{cases} 3i/2 & \text{if } i \text{ is even} \\ (3i - 1)/2 & \text{if } i \text{ is odd}. \end{cases}$$
The method we used in this result is to study the mixed Hodge structure (an enrichment of the cohomology group studied by Deligne [7]) of \( H^i(\text{Conf}^n(X); \mathbb{Q}) \) via explicit algebraic and combinatoric tools developed in [20], [26], etc. The mixed Hodge structure turns out to be an important reason, both conceptual and technical, behind the analogy between the Betti number story and the point-count story of configuration spaces. In the same paper, a generating function for the mixed Hodge numbers \( h^{p,q,i}(\text{Conf}^n(X)) \) (dimensions of certain vector spaces associated to the mixed Hodge structure of \( H^i(\text{Conf}^n(X); \mathbb{Q}) \)) is also obtained.

### 1.2 Punctured varieties [15]

I studied the relation between a smooth quasiprojective complex variety \( X \) and its one-puncture \( X - P \), namely, the variety \( X \) with a point \( P \) removed. There is a simple story that relate the point-counts of their configuration spaces, and in the case where \( X \) is a smooth nonprojective curve or more generally, a smooth punctured variety (a smooth projective variety with \( r \geq 1 \) points removed), there is a similar story ([22, Theorem 2] and [17, Theorem 1.5(4)], respectively) about the Betti numbers of their configuration spaces. This motivates the study of the relevant mixed Hodge numbers in an attempt to explain this analogy. For \( X \) in the cases above, I proved in [15] that the mixed Hodge numbers \( h^{p,q,i}(\text{Conf}^n(X - P)) \) can be computed from the mixed Hodge numbers of \( \text{Conf}^m(X) \) for \( 0 \leq m \leq n \), which simultaneously implies the aforementioned Betti number results and a consequence of the point counting story due to Vakil and Wood.

**Theorem 1.2** (H.). If \( X \) is a smooth punctured variety of complex dimension \( d \), and \( P \) is a point of \( X \), then we have an identity of mixed Hodge numbers

\[
h^{p,q,i}(\text{Conf}^n(X - P)) = \sum_{t=0}^{\infty} h^{p-dt,q-dt;-(2d-1)t}(\text{Conf}^{n-t}(X)).
\]

In the same paper, I also proved that the formula holds for several other classes of smooth nonprojective varieties. I conjecture that this formula holds for any smooth nonprojective quasiprojective variety. I used a spectral sequence [24] that generalizes the existing ones to higher dimensions, and I expect that deeper understanding of this spectral sequence will lead to more results towards this conjecture.

### 1.3 Applications

Combining the two results above, we obtain the mixed Hodge numbers of configuration spaces on multi-punctured elliptic curves.

I plan to develop more applications of these methods and results. For example, if \( X \) is a one-punctured smooth projective variety, I expect that the mixed Hodge structure of \( H^i(\text{Conf}^n(X); \mathbb{Q}) \) will be nicer to describe than in general. Combined with the results of [15] and their potential generalizations, it is then viable to study the mixed Hodge structure of \( \text{Conf}^n(X) \) for the multi-punctured case and even for more general examples of smooth nonprojective varieties.

### 2 Enumeration of commuting matrices satisfying polynomial equations [14]

Consider a finite collection of polynomials \( f_1, \ldots, f_r \in k[x_1, \ldots, x_m] \) over a finite field \( k = \mathbb{F}_q \). The variety of commuting \( n \times n \) matrices satisfying \( f_1, \ldots, f_r \) is a \( k \)-variety \( M_n \) given by

\[
M_n(k) := \{ \begin{pmatrix} A_1 & \cdots & A_m \end{pmatrix} \in (\text{Mat}_n(k))^m : A_iA_j = A_jA_i \text{ for all } 1 \leq i, j \leq m \text{ and } f_s(A) = 0 \text{ for all } 1 \leq s \leq r \}.
\]

The main goal is to study the cardinality of \( M_n(k) \) and several of its variants (for example, where some or all of \( A_i \) are required to be nilpotent or invertible). Apart from being a matrix enumeration problem, it appears in two other contexts as well.
First, a moduli problem. It turns out that the isomorphism class of the variety $M_n$ is determined by the affine variety

$$X := \{ \mathbf{x} \in \mathbb{A}^m : f_1(\mathbf{x}) = \cdots = f_r(\mathbf{x}) = 0 \},$$

so we may denote the variety $M_n$ by $M_n(X)$. More generally, it is possible to define $M_n(X)$ for any quasiprojective variety $X$. The variety $M_n(X)$ can almost be thought of as a moduli space of torsion coherent sheaves of length $n$ on $X$, where the length of a torsion coherent sheaf is the $k$-dimension of its global sections. Specifically, $\#M_n(X)(\mathbb{F}_q)/\# \text{GL}_n(\mathbb{F}_q)$ is the weighted number of isomorphism classes of torsion coherent sheaves of length $n$ on $X$, where each sheaf $M$ is counted with a weight $1/\text{Aut}(M)$. While such a classification is in general very hard, it is possible to study a quantitative aspect of it, encoded in a version of “zeta function” attached to $X$ defined as

$$\hat{Z}_X(t) := \sum_{n=0}^{\infty} \frac{\#(M_n(X))(\mathbb{F}_q)}{\# \text{GL}_n(\mathbb{F}_q)} t^n.$$ 

Second, a problem in commutative algebra. Consider a complete Noetherian local ring $A$ whose residue field is a finite field $\mathbb{F}_q$. The classification of finite-length modules over $A$ has been studied in several examples, including $A = \mathbb{F}_q[[x, y]]$ and $A = \mathbb{F}_q[[x, y]]/(xy)$, but is difficult in general. However, it is possible to understand the following enumeration problem in some cases where a classification is absent: given $n$, count the number of $A$-modules of length $n$, inversely weighted by the size of the automorphism group. (This being said, this problem is still interesting and nontrivial even if we know the classification.) In the case where $A = \mathcal{O}_{X, p}$, the completion of the stalk of a $\mathbb{F}_q$-variety $X$ over a closed point $p$, the count above is the weighted number of isomorphism classes of torsion coherent sheaves of length $n$ on $X$ that are supported at $p$. This is closely related to $M_n(X)(\mathbb{F}_q)$ via a formula similar to the Euler formula of the Hasse–Weil zeta function.

The formula for $\hat{Z}_X(t)$ is well-known if $X$ is a smooth curve over $\mathbb{F}_q$, and this formula was useful in the study of the distribution of abelian groups [6] and of matrices over finite fields [18, 25]. Cheong and I [2] also used it in the study of the distribution of a polynomial of a random matrix over a finite field; see Section 4. The formula for $\hat{Z}_X$ is also known if $X$ is a smooth surface over $\mathbb{F}_q$ (see [2], essentially a consequence of Feit and Fine [8]).

In all other cases, the property of $\hat{Z}$ (and thus the point count of $M_n(X)$) is wide open. On the other hand, the varieties $M_n(X)$ share many properties with the Hilbert schemes $\text{Hilb}^n(X)$ (a moduli space that classifies zero-dimensional subscheme of $X$ of length $n$), and the point-count formulae for $\text{Hilb}^n(X)$ have long been known in precisely these two cases: $X$ being a smooth curve or a smooth surface [5]. In 2014, Göttscbe and Shende [11] discovered a result for $\text{Hilb}^n(X)$ where $X$ is a smooth curve on a plane. It is then natural to wonder if anything can be said about $\hat{Z}_X(t)$ if $X$ is a singular curve.

I recently proved [14] the following theorem that locates all the poles of $\hat{Z}_X(t)$ if $X$ is a curve over $\mathbb{F}_q$ such that all singularities of $X_{\mathbb{F}_q}$ are nodes (i.e. singularities analytically isomorphic to $xy = 0$).

**Theorem 2.1 (H.).** Assume $X$ is a nodal curve over $\mathbb{F}_q$ and $\tilde{X}$ is its normalization (resolution of singularities). Then

$$H_X(t) := \frac{\hat{Z}_X(t)}{\hat{Z}_{\tilde{X}}(t)} = \sum_{n=0}^{\infty} \frac{\#(M_n(X))(\mathbb{F}_q)}{\# \text{GL}_n(\mathbb{F}_q)} t^n$$

is an explicit holomorphic function defined for all $t \in \mathbb{C}$.

Moreover, $H_X(t)$ exhibits some puzzling behaviors that are yet to be understood, especially the distribution of zeros that suggests an “almost” functional equation. The computation of $H_X(t)$ uses the theory of partitions and $q$-series.

I am also working on the case where $X$ has other types of singularities, and I conjecture that $H_X(t)$ is an entire function for any singular curve $X$ that is Gorenstein (a condition on the singularities). One reason to expect the conjecture to hold is Göttscbe–Shende’s [11, Proposition 15], an analogue of the theorem
above with \( \#M_n(X)(\mathbb{F}_q)/\# \text{GL}_n(\mathbb{F}_q) \) replaced by \( \text{Hilb}^n(X)(\mathbb{F}_q) \). However, we emphasize that none of the connections between the \( \text{Hilb}^n(X) \) and \( M_n(X) \) (e.g., the GIT quotient and the wall-crossing, see [12] and [21]) is known to have an application to the study of \( \hat{Z}_X(t) \), and Theorem 2.1 is the first evidence that a connection relevant to this problem might exist. A driving motivation to study generalizations of Theorem 2.1 is to understand this heuristics.

3 Unit equations on quaternions and other division algebras [16]

A unit equation is an equation of the form \( x_1 + \cdots + x_n = 1 \), where \( x_i \) ranges from some multiplicative group of “units”. The fundamental theorem in the study of unit equations is, if \( \Gamma_1, \ldots, \Gamma_n \) are finitely generated multiplicative subgroups of \( \mathbb{C}^\times \), then the unit equation \( x_1 + \cdots + x_n = 1 \) only has finitely many nondegenerate solutions with \( x_i \in \Gamma_i \), where a solution is nondegenerate if no subsum equals to 1. Moreover, there are effective bounds for the solutions. The finiteness theorem above has applications [13, 19] to the study of Diophantine equations (polynomial equations asking for integer solutions) and arithmetic dynamics (the behavior of iterations of algebra-geometric maps, such as polynomials and rational functions).

One way to apply the unit equations is to study the dynamics of a geometric object \( X \) by studying the set of endomorphisms of \( X \) using the unit equations whenever applicable. For example, Odesky [23, Theorem 1.2.3] shows that if \( f \) and \( g \) are non-injective regular self-maps on an elliptic curve \( E \) over \( \mathbb{C} \), then they must have a common iterate whenever there exist a forward orbit of \( f \) and a forward orbit of \( g \) that intersect at infinitely many points. The key is reducing the problem to a unit equation on the endomorphism algebra \( \text{End}(E) \), where the finiteness theorem applies. The same technique works if \( E \) is replaced by a high dimensional analogue, namely, an abelian variety \( A \), as long as a version of the finiteness theorem holds for unit equations on \( \text{End}(A) \), which may not be commutative. This motivates the study of unit equations on noncommutative algebras. Little has been known about unit equations in the noncommutative setting, where many important techniques (such as \( p \)-adic completion) do not exist.

I proved a finiteness result [16] for unit equations on the algebra \( \mathbb{H}_n \) of quaternions \( a + bi + cj + dk \) with \( a, b, c, d \) being real algebraic numbers. The norm of a quaternion \( a + bi + cj + dk \) is \( \sqrt{a^2 + b^2 + c^2 + d^2} \).

**Theorem 3.1 (H.).** Let \( \Gamma_1, \Gamma_2 \) be semigroups of \( \mathbb{H}_n^\times \) generated by finitely many elements of norms greater than 1, and fix \( a, a', b, b' \in \mathbb{H}_n^\times \). If \( \Gamma_1 \) is commutative, then the equation

\[
afa' + bgb' = 1
\]

has only finitely many solutions with \( f \in \Gamma_1 \) and \( g \in \Gamma_2 \).

This implies an analogue of Odesky’s orbit intersection result, where \( E \) is replaced by an elliptic curve in positive characteristic. I conjecture that the finiteness result holds for any finite dimensional division algebra over \( \mathbb{Q} \) and all choices of finitely generated semigroups. After the submission of [16], the referee has discovered some important cases where the conjecture holds [16] Propositions 1.5 and A.2], which implies an analogue of Odesky’s orbit intersection result for any simple abelian variety in any characteristic [16 Corollary 1.7].

4 Distribution of cokernels of polynomials of random matrices over \( \mathbb{Z}_p \)

[4]

For a prime \( p \), consider the ring \( \mathbb{Z}_p \) of \( p \)-adic integers and equip the additive group \( \text{Mat}_n(\mathbb{Z}_p) \) of \( n \) by \( n \) matrices with the Haar measure with total measure 1. Questions can be asked about how a certain quantity associated to a random matrix distributes. Friedman and Washington [9] proved the following formulas about the distribution of the cokernel: Let \( H \) be a finite abelian \( p \)-group, then
\[
\lim_{n \to \infty} \frac{\text{Prob}_{A \in \text{Mat}_n(\mathbb{Z}_p)}}{\text{Aut}(H)^{-1} \prod_{i=1}^{\infty} (1 - p^{-i})} = |H|^{-1} \prod_{i=1}^{\infty} (1 - p^{-i}),
\]

where \(1_n\) is the \(n \times n\) identity matrix and the probability measure on \(\text{GL}_n(\mathbb{Z}_p)\) is the restriction of the measure on \(\text{Mat}_n(\mathbb{Z}_p)\) but with the total measure normalized to 1.

The cokernels of both samples of matrices produce the same distribution (called the Cohen–Lenstra distribution), which is conjectured by Cohen and Lenstra [6] to be the distribution of the class group of a random imaginary quadratic number field when \(p\) is odd. These papers [6, 9] also discussed heuristic reasons why both sampling produce the Cohen–Lenstra distribution.

It turns out that the Cohen–Lenstra distribution appears in a wider context, where heuristic connections to number-theoretic problems are absent. My focus is to investigate the Cohen–Lenstra distribution arising in problems about cokernels of random matrices.

In [4], G. Cheong and I found a common generalization of (4.1) and (4.2).

Theorem 4.1 (Cheong and H.). Let \(P_1(t), \ldots, P_r(t) \in \mathbb{Z}[t]\) be monic polynomials whose reductions mod \(p\) are distinct irreducible polynomials in \(\mathbb{F}_p[t]\). Suppose \(\deg P_r(t) = 1\), then given a finite abelian \(p\)-group \(H\), we have

\[
\lim_{n \to \infty} \frac{\text{Prob}_{A \in \text{Mat}_n(\mathbb{Z}_p)}}{\text{Aut}(H)^{-1} \prod_{i=1}^{\infty} (1 - p^{-i})} = |H|^{-1} \prod_{i=1}^{\infty} (1 - p^{-i} \deg P_i)
\]

This formula specializes to (4.1) if we take \(r = 1\) and \(P_1(t) = t\), and it specializes to (4.2) if we take \(r = 2\), \(P_1(t) = t\) and \(P_2(t) = t - 1\). The proof of Theorem 4.1 relies on the study of another random matrix problem, namely, the distribution of the rational canonical form of a random matrix over a finite field \(\mathbb{F}_q\). This uses the cycle index, a combinatorial method used by Cheong and H. that can be interpreted as the “zeta function” \(\hat{Z}(X)\) defined in Section 2 for the affine line \(X = \mathbb{A}^1_{\mathbb{F}_q}\); see [4, §8.2] for an explanation. In fact, random matrix problems over a finite field also see the same Cohen–Lenstra distribution, actually in a greater generality than Theorem 4.1. For example, Fulman [10] showed that for any distinct monic irreducible polynomials \(P_1(t), \ldots, P_r(t) \in \mathbb{F}[t]\), the nilpotent parts of the rational canonical forms of \(P_1(A), \ldots, P_r(A)\) (where \(A\) is a random matrix in \(\text{GL}_n(\mathbb{F}_q)\)) distribute independently as \(n \to \infty\) and each follows a version of the Cohen–Lenstra distribution. Part of our motivation is to unify the Cohen–Lenstra distribution arising in the cokernels of random \(\mathbb{Z}_p\) matrices and the Cohen–Lenstra distribution arising in the rational canonical forms of random \(\mathbb{F}_q\) matrices. Motivated by the existing analogy between the two contexts, we conjectured the distribution of \(\text{coker} P_j(A)\) for \(A \in \text{Mat}_n(\mathbb{Z}_p)\) as \(n \to \infty\) in [4 Conjecture 2.3].

References


