Generating function from counting mutually annihilating matrices and alike

Yifeng Huang

University of Michigan

May 12, 2021

Main problems

Problem 1

Let $f_1, \ldots, f_r \in \mathbb{F}_q[t_1, \ldots, t_m]$ be polynomials in m variables over the finite field $\mathbb{F}_q$. Given n, how many m-tuples $A = (A_1, \ldots, A_m)$ of mutually commuting $n \times n$ matrices satisfy $f_1(A) = \cdots = f_r(A) = 0$? How does the number grow with n?

Problem 1'

What if we impose additional conditions to some or all of the matrices, such as nilpotency, invertibility, or a factorization statistics of the characteristic polynomial?

Fact: we know a lot, not only special cases, but families of examples.

Examples of Problem 1

1. One variable, no polynomial condition. Then we are just counting $n \times n$ matrices. There are q^{n^2} of them.
2. Two variables, no polynomial condition. Then we are counting pairs of commuting matrices. We have (Feit–Fine '60)

$$\sum_{n=0}^{\infty} \frac{|\{A, B \in \mathrm{Mat}_n(\mathbb{F}_q) : AB = BA\}|}{|\mathrm{GL}_n(\mathbb{F}_q)|} x^n = \prod_{i \geq 1, j \geq 0} (1 - q^{1-j} x^i)^{-1}$$

3. One variable, one polynomial f. Then the number of $n \times n$ matrices A satisfying $f(A) = 0$ is of the order $O(q^{(1-\frac{1}{\deg f})n^2})$. (Stong '88)

Examples of Problem 1'

1. The number of $n \times n$ nilpotent matrices is q^{n^2-n}. (Fine–Herstein '58)
2. The number of pairs of commuting nilpotent matrices is given by (Fulman–Guralnick '18)

$$\sum_{n=0}^{\infty} \frac{|\{A, B \in \mathrm{Nilp}_n(\mathbb{F}_q) : AB = BA\}|}{|\mathrm{GL}_n(\mathbb{F}_q)|} x^n = \prod_{i \geq 1, j \geq 2} (1 - q^{1-j} x^i)^{-1}$$

3. Fix an irreducible polynomial $P(t) \in \mathbb{F}_q[t]$ of degree d. Then the number of $dn \times dn$ matrices whose characteristic polynomial is a power of $P(t)$ is

$$\frac{q^{d(n^2-n)}}{|\mathrm{GL}_n(\mathbb{F}_{q^d})|} |\mathrm{GL}_n(\mathbb{F}_q)|,$$

using the cycle index method of Kung and Stong.

Questions to answer

At this point, there are several natural questions to ask

1. What are known so far?
2. Is there any pattern?
3. What open cases seem interesting?

We will discuss them in the talk.

A generating function

The pattern is best understood using the following generating function. Let's introduce the notation.

Given polynomials $f_1, \dots, f_r$ over $\mathbb{F}_q$ in m variables. Consider the ring $R = \mathbb{F}_q[t_1, \dots, t_m]/(f_1, \dots, f_r)$. Denote

$$\widehat{Z}_R(x) := \sum_{n=0}^{\infty} \frac{|\{(A_1, \dots, A_m) : A_i \in \mathrm{Mat}_n(\mathbb{F}_q), [A_i, A_j] = 0, f_s(\mathbf{A}) = 0\}|}{|\mathrm{GL}_n(\mathbb{F}_q)|} x^n$$

(This notation implicit assumes that $\widehat{Z}_R(x)$ depends only on the ring R, not on the full data $f_1, \dots, f_r$. We will explain why this is true.)
Note that the numerator in the coefficient is the answer to Problem 1.

The ring R should be viewed geometrically

We will consider the affine variety $X = \operatorname{Spec} R$, namely, the variety cut out by the equations. We can talk about its dimension, smoothness and singularities.

Topologically, they can be visualized by pretending the polynomials were over $\mathbb{C}$, and thinking of X as

$$\{(t_1, \ldots, t_m) \in \mathbb{C}^m : f_1(\mathbf{t}) = \cdots = f_r(\mathbf{t}) = 0\}$$

The dimension of X is its complex dimension. The smoothness and singularities can be visualized likewise, barring some bad cases in low characteristics.
We denote $\widehat{Z}_X(x) := \widehat{Z}_R(x)$.

Problem 1 in $\widehat{Z}$ notation: Examples

We restate some aforementioned examples in terms of this notation.

1. One variable, no polynomial. The ring is $R = \mathbb{F}_q[t]$, and the variety is a line $X = \mathbb{A}^1$. We have

$$\widehat{Z}_R(x) = \sum_{n=0}^{\infty} \frac{|\mathrm{Mat}_n(\mathbb{F}_q)|}{|\mathrm{GL}_n(\mathbb{F}_q)|} x^n = \prod_{i=0}^{\infty} \frac{1}{1 - q^{-i}x}.$$

2. Two variables, no polynomial. The ring is $R = \mathbb{F}_q[u, v]$, and the variety is a plane $X = \mathbb{A}^2$. The result counting pairs of commuting matrices read

$$\widehat{Z}_R(x) = \sum_{n=0}^{\infty} \frac{|\{A, B \in \mathrm{Mat}_n(\mathbb{F}_q) : AB = BA\}|}{|\mathrm{GL}_n(\mathbb{F}_q)|} x^n = \prod_{\substack{i \geq 1 \\ j \geq 0}} \frac{1}{1 - q^{1-j} x^i}$$

Known cases of Problem 1

It turns out that the knowledge about a line and a plane generalizes to all smooth curves and smooth surfaces.

Proposition

For any variety X over $\mathbb{F}_q$, let $Z_X(x)$ be its Hasse–Weil zeta function. We have $Z_{\mathbb{A}^n}(x) = \dfrac{1}{1 - q^n x}$ for example. Then

1. If X is a smooth curve, then

$$\widehat{Z}_X(x) = \prod_{i=1}^{\infty} Z_X(q^{-i}x);$$

2. If X is a smooth surface, then

$$\widehat{Z}_X(x) = \prod_{i,j \geq 1} Z_X(q^{-j}x^i).$$

A new case for Problem 1

Our main result deals with the singular curve $\{uv = 0\}$.

Theorem 1 (H., 2021+)

$$\widehat{Z}_{\mathbb{F}_q[u,v]/(uv)}(x) = \sum_{n=0}^{\infty} \frac{|\{A, B \in \mathrm{Mat}_n(\mathbb{F}_q) : AB = BA = 0\}|}{|\mathrm{GL}_n(\mathbb{F}_q)|} x^n$$
$$= \big((1-x)(1-q^{-1}x)(1-q^{-2}x)\dots\big)^{-2} H_q(x),$$

where $H_q(x)$ is the entire function

$$H_q(x) = \sum_{k=0}^{\infty} \frac{q^{-k^2} x^{2k}}{(1-q^{-1})\dots(1-q^{-k})} (1-q^{-k-1}x)(1-q^{-k-2}x)\dots$$

In particular, $\widehat{Z}_{\mathbb{F}_q[u,v]/(uv)}(x)$ has a meromorphic continuation to all of $\mathbb{C}$.

Artinian modules: Towards Problem 1'

We answer Problem 1' as far as we know, using a related generating function, but about weighted counting of Artinian modules.

Let R be a finitely generated $\mathbb{F}_q$-algebra and P be a maximal ideal. An Artinian module over the local ring R_P is an R_P module that is a finite-dimensional vector space over $\mathbb{F}_q$. (For example, $R/P \oplus R/P^3$, but not R_P itself; also note that there are Artinian modules not of a similar form if R is not Dedekind.)

An Artinian module over R is an R module that is a finite-dimensional vector space over $\mathbb{F}_q$. It can always be uniquely written as $\oplus_P M_P$ where P ranges over a finite collection of maximal ideals of R, and M_P is an Artinian R_P module.

Module counting generating function

Let S be R or R_P above. (Namely, let S be a finitely generated $\mathbb{F}_q$-algebra or its localization at a maximal ideal.) Define

$$\widehat{Z}_S(x) := \sum_M \frac{1}{|\mathrm{Aut}\, M|} x^{\dim_{\mathbb{F}_q} M}$$

where M ranges over all Artinian modules of S.

If $S = R = \mathbb{F}_q[t_1, \ldots, t_m]/(f_1, \ldots, f_r)$, then this definition of $\widehat{Z}_R(x)$ agrees with the previous one using matrix counting.

Sketch of proof: to give an R-module structure to ${\mathbb{F}_q}^n$, we specify how $t_1, \ldots, t_m$ act as matrices $A_1, \ldots, A_m$. They must commute and satisfy the polynomials. The ambiguity comes from simultaneous conjugation by $\mathrm{GL}_n(\mathbb{F}_q)$, and the proof is finished by the orbit-stabilizer theorem.

Problem 1' in $\widehat{Z}$ notation: Examples

1. Let $R = \mathbb{F}_q[t], P = (t), S = R_P$. Then

$$\widehat{Z}_S(x) = \sum_{n=0}^{\infty} \frac{|\mathrm{Nilp}_n(\mathbb{F}_q)|}{|\mathrm{GL}_n(\mathbb{F}_q)|} x^n$$

   because an Artinian R-module is also an R_P module if and only if t acts nilpotently.

2. Let $R = \mathbb{F}_q[t], P = (P(t))$ where $P(t)$ is an irreducible polynomial. Then

$$\widehat{Z}_{R_P}(x) = \sum_{n=0}^{\infty} \frac{|\{A \in \mathrm{Mat}_n(\mathbb{F}_q) : \mathrm{charpoly}(A) \text{ is a power of } P(t)\}|}{|\mathrm{GL}_n(\mathbb{F}_q)|} x^n$$

Known cases of Problem 1'

If an instance of Problem 1' can be converted to a question of $\widehat{Z}_{R_P}(x)$, then here is what we know:

1. $\widehat{Z}_{R_P}(x) = \widehat{Z}_{\widehat{R_P}}(x)$, because Artinian R_P-modules and Artinian $\widehat{R_P}$-modules are the same thing;
2. $\widehat{Z}_{\mathbb{F}_q[[t]]}(x) = \prod_{i=1}^{\infty} \dfrac{1}{1-q^{-i}x}$; (Fine–Herstein '58)
3. $\widehat{Z}_{\mathbb{F}_q[[u,v]]}(x) = \prod_{i,j\geq 1} \dfrac{1}{1-q^{-j}x^i}$. (Fulman–Guralnick '18)

This solves the case where R_P is the local ring of a smooth closed point on a curve or a surface, because the completion of R_P will be of the form $\mathbb{F}_{q^d}[[t]]$ or $\mathbb{F}_{q^d}[[u,v]]$ by Cohen's structure theorem.

A new case for Problem 1'

Theorem 1' (H., 2021+)

$$\widehat{Z}_{\mathbb{F}_q[[u,v]]/(uv)}(x) = \sum_{n=0}^{\infty} \frac{|\{A, B \in \mathrm{Nilp}_n(\mathbb{F}_q) : AB = BA = 0\}|}{|\mathrm{GL}_n(\mathbb{F}_q)|} x^n$$
$$= \left((1 - q^{-1}x)(1 - q^{-2}x)\dots\right)^{-2} H_q(x),$$

where $H_q(x)$ is the entire function

$$H_q(x) = \sum_{k=0}^{\infty} \frac{q^{-k^2} x^{2k}}{(1 - q^{-1}) \dots (1 - q^{-k})} (1 - q^{-k-1}x)(1 - q^{-k-2}x) \dots$$

We remark that Laubenbacher–Sturmfels '95 has classified Artinian $k[u, v]/(uv)$ modules for a field k.

Idea of proof of Theorem 1

$$\sum_{n=0}^{\infty} \frac{|\{A, B \in \mathrm{Mat}_n(\mathbb{F}_q) : AB = BA = 0\}|}{|\mathrm{GL}_n(\mathbb{F}_q)|} x^n$$
$$= \big((1-x)(1-q^{-1}x)(1-q^{-2}x)\dots\big)^{-2} H_q(x)$$

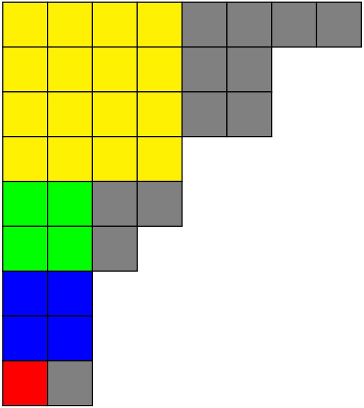
- Count such pairs of matrices by fixing the rank of A first. The number of B that mutually annihilate A only depends on $\operatorname{rk} A$.
- The LHS will be an infinite sum (denoting $t = q^{-1}$)

$$\sum_{n} \sum_{\ell(\lambda) \le n} t^{|\lambda| - \sigma_1(\lambda)^2} x^n$$

where λ ranges over all partitions, $|\lambda|$ is the size, $\ell(\lambda)$ is the length, and $\sigma_1(\lambda)$ is the sidelength of (the first) Durfee square (the largest square that fits inside the Young diagram of λ).

Durfee squares

This is what Durfee squares look like:



In this example, $\sigma_1(\lambda) = 4$, $\sigma_2(\lambda) = 2$, etc.

Idea of proof of Theorem 1

$$\sum_{n=0}^{\infty} \frac{|\{A, B \in \mathrm{Mat}_n(\mathbb{F}_q) : AB = BA = 0\}|}{|\mathrm{GL}_n(\mathbb{F}_q)|} x^n$$
$$= \left((1-x)(1-q^{-1}x)(1-q^{-2}x)\dots\right)^{-2} H_q(x)$$

- Rewrite the sum by fixing $\sigma_1(\lambda)$, $\sigma_2(\lambda)$ first. Here, $\sigma_2(\lambda)$ (called the second Durfee square) is the largest square that fits below the first Durfee square.
- This turns out to give the factorization. The form of $H_q(x)$ is

$$\sum_{n=0}^{\infty} t^{n^2} x^n \cdot (\text{bounded}),$$

giving the convergence for all x.

Proof of Theorem 1'

$$\widehat{Z}_{\mathbb{F}_q[[u,v]]/(uv)}(x) = \sum_{n=0}^{\infty} \frac{|\{A, B \in \mathrm{Nilp}_n(\mathbb{F}_q) : AB = BA = 0\}|}{|\mathrm{GL}_n(\mathbb{F}_q)|} x^n$$

$$= \left((1 - q^{-1}x)(1 - q^{-2}x)\dots\right)^{-2} H_q(x),$$

1. It turns out that a proof with direct counting works, but is much harder than the case of Theorem 1.
2. Theorem 1' is about a weighted count of Artinian modules over $\mathbb{F}_q[[u,v]]/(uv)$. It seems impossible to use the Laubenbacher–Sturmfels classification because of the complexity, and we need to consider the automorphism group, too.
3. The simplest proof known to me is to apply Theorem 1, thanks to the nice behaviors of the $\widehat{Z}$ generating functions.

Euler product

We have

$$\widehat{Z}_R(x) = \prod_P \widehat{Z}_{R_P}(x),$$

where P ranges over all maximal ideals of R. This is because an Artinian R-module is uniquely decomposable into Artinian R_P-modules, and different P's don't interact when taking automorphism groups.

Now apply this to both $X = \operatorname{Spec} \mathbb{F}_q[u,v]/(uv)$ and X minus the origin (which is just two copies of $\mathbb{A}^1$ minus the origin), we get

$$\widehat{Z}_{\mathbb{F}_q[[u,v]]/(uv)}(x) = \widehat{Z}_{\mathbb{F}_q[u,v]/(uv)}(x)/\widehat{Z}_{\mathbb{A}^1-0}(x)^2$$

This allows the computation of Theorem 1' from the right-hand side (which is known due to Theorem 1).

Open question

The main result has an equivalent restatement

$$\frac{\widehat{Z}_{\{uv=0\}}(x)}{\widehat{Z}_{(\text{two lines})}(x)} = H_q(x) \text{ is an entire function.}$$

Notice that resolving the singular point of $\{uv = 0\}$ results in two lines.

Conjecture (H.)

Let X be any curve over $\mathbb{F}_q$ with only planar singularities, and assume $\widetilde{X}$ is a resolution of singularity of X. Then $\dfrac{\widehat{Z}_X(x)}{\widehat{Z}_{\widetilde{X}}(x)}$ is entire in x.

We remark that the question only depends on the type of the singularity.
The main result implies the conjecture holds for nodes.
In particular, the conjecture predicts an asymptotics about $|\{AB = BA, B^2 = A^3\}|$:

$$\widehat{Z}_{\{v^2=u^3\}} = \big((1-x)(1-q^{-1}x)(1-q^{-2}x)\dots\big)^{-1} \cdot (\text{entire})$$

Final remarks

- The coefficient of $\widehat{Z}_X(x)$ is actually the point-count of the stack of finite-length coherent sheaves over X.
- I don't know a geometric proof of the main result.
- The form of $H_q(x)$ is too complicated so that it is not likely to be a consequence of general arguments in algebraic geometry.
- (Very recent observation) The case where X is 0-dim (not necessarily reduced) is surprisingly interesting. The $\widehat{Z}_X(x)$ seems to be entire and related to "partial theta functions". Entireness is known for $X = \operatorname{Spec} \mathbb{F}_q[t]/f(t)$ (using the asymptotic given by Stong '88) but there could be other examples like $\{AB = BA, A^2 = B^3 = 0\}$.

Thank you!