Problems for Arizona Winter School 2014: Distribution of discriminants of polynomials over finite fields

Jordan S. Ellenberg

1 Feb 2014

In the lectures, we discuss the relationship between questions about probability distributions arising from variation of arithmetic objects – the family of questions sometimes called "arithmetic statistics" – and questions about cohomology of moduli spaces. I have in mind several such questions that I think the problem group can productively consider.

Fix a finite field $\mathbb{F}_q$. If f is a monic squarefree polynomial of degree n, then the discriminant $\Delta(f)$ is an element of $\mathbb{F}_q^*$. Thus, taking f to be a *random* polynomial (chosen uniformly from monic squarefrees), the values of $\Delta(f)$ give a probability distribution on $\mathbb{F}_q^*$. We know (and I will probably discuss in the talk) that the probability that $\Delta(f) = 0$ is exactly $1/q$ for all $n > 1$. What's more, when q is odd and $n > 1$, the probability that $\Delta(f)$ is a nonzero quadratic residue is exactly the same as the probability that $\Delta(f)$ is a nonzero quadratic non-residue. These facts might naturally lead you to wonder whether the distribution of $\Delta(f)$ is in fact *uniform* on $\mathbb{F}_q$.

This is not true in general. For instance, you can look at the discriminants of degree-9 monic polynomials over $\mathbb{F}_7$. Using Sage, I computed 70,000 randomly chosen such polynomials (this is really fast) and found that their discriminants were distributed as follows:

0	9926
1	9531
2	11256
3	10391
4	9545
5	8922
6	10429

which is very far from anything likely to be obtained by sampling from a uniform distribution. But note that the number of 0s is almost exactly 10000, and the number of quadratic residues is almost exactly 30000, just as one might expect.

The distribution of discriminants is related to the cohomology of braid groups with non-constant coefficients of a certain kind. For instance, we can ask about the distribution of $\Delta(f)$ in $\mathbb{F}_q^*/(\mathbb{F}_q^*)^6$ for various q and n, as f ranges over monic squarefree polynomials in $\mathbb{F}_q[x]$ of degree n; denote this distribution P_6. On the other hand, the Artin braid group has a

1-dimensional representation V_6 in which each standard generator is mapped to a primitive 6th root of unity. The deviation of P_6 from uniformity is governed by the cohomology of the Artin braid group with coefficients in V_6, along the lines of the problems described in the lectures. (If you're reading this beforep the lectures, you can also look at the arXiv preprint "Representation stability in cohomology and asymptotics for families of varieties over finite fields," by Tom Church, Benson Farb, and me, to see many examples of this kind worked out in detail.)

For instance: to ask

> For how many monic squarefree polynomials of degree n is $\mathcal{D}(f)$ a 6th power?

is precisely to count $\mathbb{F}_q$-rational points on a certain 6-fold cover of configuration space, which is controlled by the cohomology of this space via the Lefschetz trace formula; and this cohomology can in turn be described in terms of the cohomology of the braid group with coefficients V_6. Of course, for $q = 7$ it is also the same question as

> How many monic squarefree polynomials of degree n have $\mathcal{D}(f) = 1$?

Of course, one can define P_m and V_m for any positive integer m along the same lines.

In fact, a great deal is known about the cohomology of the braid group with coefficients of this kind. For instance, see the 1999 paper "Arithmetic Properties of the Cohomology of Braid Groups," by De Concini, Procesi, Salvetti, which computes the rational cohomology of the braid group with coefficients in any V_m.

Problem:

- Using the results of DeConcini-Procesi-Salvetti, give upper bounds on the deviation of P_6 from the uniform distribution; in particular, prove that the distribution of P_6 (or more generally P_m) approaches the uniform distribution as $n \to \infty$ with q fixed, and give bounds for the speed of convergence.
- What can we say in general about the number of monic squarefrees over $\mathbb{F}_q$ of degree n whose discriminant is 1? As n varies with q fixed, how much does this vary from the expected answer q^{n-1}? How quickly does the distribution of discriminants approach uniformity as n grows?
- If you can prove that the etale cohomology groups corresponding to those appearing in DC-P-S are all of Tate type (which is what I'd expect) you can get more refined formulas; for instance, there should be a formula for the number of monic squarefree polynomials of degree n whose discriminant is a 6th power which looks something like $(1/6)q^n + cq^{n'} + o(q^{n'})$ where n' is on order $2n/3$. Can you guess or even prove such a formula?

This already might be enough for the week, but if people want to go further, here is another question along the same lines, suggested by Kent Morrison, which I've thought less about but which I'll bet is interesting:

- What if we play this whole game with resultants of pairs of polynomials in place of discriminants of a single polynomial? For instance, is it the case that the resultant of two random coprime polynomials is a quadratic residue exactly half the time? If there's a deviation from uniformity here, can we describe the geometry that governs it?

Recommended reading

The mostly expository paper "Representation stability in cohomology and asymptotics for families of varieties over finite fields," by me, Tom Church, and Benson Farb gives an introduction to the relationship between cohomology of moduli spaces and counting problems over finite fields, especially regarding random squarefree polynomials. For basics on the braid group from a topologist's perspective, I recommend Farb and Margalit's book "A primer on mapping class groups" – braid groups are treated in section 9 (this doesn't require you read the first 8 chapters, but they are certainly good reading...) Kent Morrison's paper "Random polynomials over finite fields" covers some of the basic questions about random polynomials from a combinatorial point of view.