The Weil Conjectures II

and why you should care...

1 Introduction

We start by introducing two questions about which you may care, even if you are not directly interested in the Weil Conjectures because you think you do not care about results over finite fields:

- Let $f(x) \in \mathbb{Z}[x]$ be such that for all natural numbers n, the value $f(n)$ is a square number. Is the polynomial $f(x)$ itself a square?

- Consider the set of isomorphism classes $[X]$ of projective varieties X defined over $\mathbb{C}$ (and ignore that this may be set-theoretically dodgy). Take the abelian group freely generated by these classes and factor out by the relations

  $$[X - Y] = [X] - [Y]$$

  for closed immersions $Y \hookrightarrow X$. This is the so-called Grothendieck group of varieties $K_0(\mathrm{Var}/\mathbb{C})$. In it, we have equalities like:

  $$\mathbb{P}^2 = \mathbb{A}^2 + \mathbb{A}^1 + \mathbb{A}^0$$

  Addition is realised by disjoint unions

  $$[X] + [Y] = [X \sqcup Y]$$

  One can also equip K_0 with a ring structure by setting

  $$[X][Y] = [X \times Y]$$

  and arrive at the Grothendieck ring of varieties. Does $[X] = [Y]$ in K_0 imply $\dim X = \dim Y$? Does it even imply that X and Y have the same number of maximal-dimensional irreducible components?

Exercise: Compute the Grothendieck group of nicely compactifiable differentiable manifolds (i.e. submanifolds of compact differentiable manifolds with compact differentiable complement). Hint: Euler characteristic with compact support, the answer is $\mathbb{Z}$. For uniqueness, write the real line as union of a point and two copies of itself. Then triangularise manifolds (e.g. using Morse theory.) For additivity, use an appropiate long exact sequence.

The result motivates why we may think of the Grothendieck group in the algebraic setting as the attempt to construct a universal Euler characteristic. It also remarkably shows that if the claim about dimensions in the Grothendieck ring of varieties is true, it cannot be solved by purely topological arguments.

Both questions provide examples[1] of situations that can be analysed with finite field methods and then transferred, as we will see later. In the next section, we first describe how results for finite fields can be transferred in elementary cases where the Weil Conjectures are not needed.

2 Transfer

A famous transfer result is[2]:

Theorem 1 (Ax-Grothendieck). *Let $P = (P_1, \ldots, P_n) : \mathbb{C}^n \to \mathbb{C}^n$ be a polynomial map. If P is injective, then it is also surjective.*

The situation is very easy to analyse for finite fields. Then it just reduces to the set-theoretic statement that injective self-maps are surjective. The result then also holds for the direct limit (union) of all finite fields of given characteristic p, i.e. the algebraic closure $\overline{\mathbb{F}_p}$. In case you are confused later on: This limit procedure breaks for the converse direction as the restriction of a surjective polynomial map $\overline{\mathbb{F}_p}^n \to \overline{\mathbb{F}_p}^n$ to $\mathbb{F}_{p^m}^n \to \mathbb{F}_{p^m}^n$ is not necessarily surjective.

Having established the result for finite fields and their algebraic closures, there are two ways to transfer this result to prove Ax-Grothendieck:

2.1 Mathematical Logic approach: Compactness Theorem and The Lefschetz Principle

The Lefschetz Principle for first-order logic states:

Theorem 2. *Let ϕ be a first-order sentence in the language $0, 1, +, -, \cdot$. Then the following are equivalent:*

(i). ϕ is true for some algebraically closed field of characteristic 0.

(ii). ϕ is true for all algebraically closed fields of characteristic 0.

(iii). ϕ is true for algebraically closed fields of arbitrarily large characteristic p.

(iv). ϕ is true for algebraically closed fields of sufficiently large characteristic p (greater than some P depending on ϕ).

First-order means that ϕ is assembled from the above language symbols, as well as logical operators and quantifiers over elements from the field (not relations – that would be second-order). Then the Lefschetz principle is a combination of

[1] For more examples, read Serre's educational paper *How to use finite fields for problems concerning infinite fields* at `http://arxiv.org/abs/0903.0517`

[2] A. Borel also gives a topological proof.

- the compactness theorem: If every finite subset of sentences has a model structure that satisfies it, then the set itself has a model structure that satisfies it. This is a corollary of Gödel's completeness theorem which characterises implications syntactically, so if you can derive a contradiction from a sentence set, then you can already derive it from a finite subset.
- the completeness of the theories of algebraically closed fields: Any first-order sentence either holds in all algebraically closed fields of a fixed characteristic or in none. This can be checked with the so-called Łoś-Vaught test (which in the end also boils down to a corollary of the compactness theorem).

Now for Ax-Grothendieck, apply the Lefschetz theorem for each (multi-)degree of P.

2.2 Commutative Algebra approach: Spreading out and Grothendieck transfer

We use the Hilbert Nullstellensatz: Injectivity can be expressed by saying that there exists polynomial map $(f_1, \dots, f_n) : \mathbb{C}^n \times \mathbb{C}^n \to \mathbb{C}^n$ and a natural exponent r such that

$$(P_i(x) - P_i(y))f_i(x, y) = (x - y)^r$$

Lack of surjectivity is given by the existence of $g : \mathbb{C}^n \to \mathbb{C}^n$ and a point x_0 such that (using the scalar product)

$$(P(x) - x_0)g(x) = 1$$

Now take the collection C of all coefficients in P, the witnesses f and g and x_0. They generate a ring $\mathbb{Z}[C]$ finitely presented over $\mathbb{Z}$. This passage is known as *spreading out*.

Exercise Complete the proof by factoring modulo a maximal ideal. [The lecture notes were much sketchier here, so I have already given enough hints.]

At the end of this section, let's have another exercise for transfer:

Exercise Let G be a finitely presented group. Define its profinite completion $\hat{G}$ as the inverse limit over all finite quotients. Then in the following, the first statement implies the second:

(i). $\hat{G}$ is trivial, i.e. G has no non-trivial, finite quotients.

(ii). The representation category of G is trivial, i.e. every finite dimensional complex representation is trivial.

Hint: Note that any action of G on a finite vector space factors through $\hat{G}$. Then apply spreading out using the finite presentation of G.

Grothendieck's motivation for considering this problem was to understand the relation between the étale and the de Rham fundamental group, the former being the profinite completion and the latter the algebraic envelope[3] of the topological fundamental group. Of course, he proved this in much greater generality[4].

[3] mumble mumble... Tannakian

[4] http://www.ams.org/mathscinet-getitem?mr=262386

3 Counting Points

3.1 Grothendieck group

A useful way to study the Grothendieck ring of varieties is via its realisation maps into a group A, also known as *motivic measures* or *additive invariants*. These are maps from isomorphism classes of varieties that behave additive under disjoint unions, i.e. descend to $K_0 \to A$. One such measure is counting points:

$$\# : K_0(\mathrm{Var}/\mathbb{F}_q) \to \mathbb{Z}, [X] \to \#X(\mathbb{F}_{q^m})$$

For example:

$$\# \mathbb{A}^n(\mathbb{F}_q) = q^m$$

$$\# \mathbb{A}^n(\mathbb{F}_{q^m}) = q^{mn}$$

$$\# \mathbb{P}^n(\mathbb{F}_{q^m}) = \frac{q^{(n+1)m}}{q^m - 1} = 1 + q^m + \cdots + q^{mn}$$

$$\# \operatorname{Spec} \mathbb{F}_{q^m}(\mathbb{F}_{q^r}) = \operatorname{Hom}(\operatorname{Spec} \mathbb{F}_{q^r}, \operatorname{Spec} \mathbb{F}_{q^m}) = \operatorname{Hom}(\mathbb{F}_{q^m}, \mathbb{F}_{q^r}) = \begin{cases} m & m|r \\ 0 & \text{else} \end{cases}$$

From the Weil Conjectures, it will follow that if a projective variety X of dimension n is the union of N smooth, geometrically irreducible (i.e. after base change to an algebraic closure) components of maximal dimension, then

$$\#X(\mathbb{F}_{q^m}) = Nq^{mn} + \text{smaller terms}$$

Exercise Complete this argument to show the claim about K_0.

3.2 Square polynomials

We can also tackle the first problem now and prove that $f(x)$ assuming square values for all integers is itself the square of a polynomial in $\mathbb{C}[x]$ (although showing $\mathbb{Z}[x]$ is also possible). For this, observe that $f(x)$ is a square if and only if the hyperelliptic curve C given by

$$y^2 = f(x)$$

has two irreducible components. This however can be established over finite fields and then be transferred. Reducing the curve C modulo q (not a power of 2), the number of $\mathbb{F}_{q^m}$-rational points is governed by $2 \cdot q^m$: For each $x \in \mathbb{F}_{q^m}$ (except for the roots of f whose number is bounded by $\deg f$), we get two solutions for y.

Alternatively (or equivalently), one can use the Weil estimate for smooth, projective, geom. irreducible curves of genus g:

$$|X(\mathbb{F}_q) - (q+1)| \leq 2g\sqrt{q}$$

Exercise Formulate and prove the most general version of this type of claim you can imagine. Possible answer: Let $f(\underline{x})$ be a multivariate polynomial that assumes perfect power values at all integral points (possibly with different exponents). Then f is a perfect power. . .

4 Zeta functions

Let X be a smooth, projective variety over $\mathbb{F}_q$. We can try to combine all counting measures into one generating function. More precisely, we define an Euler product

$$Z_X(t) = \prod_{x \in |X|} (1 - t^{\deg(x)})^{-1}$$

where $|X|$ is the set of closed points in X and $\deg(x) = [k(x) : \mathbb{F}_q]$ is the degree of the residue field $k(x)$ at x. This converges because there are only finitely many points with a given degree.

Compare this to the Riemann zeta function:

$$\zeta_{\mathbb{Z}}(s) = \prod_p (1 - p^{-s})^{-1} = \prod_{x \in |\operatorname{Spec} \mathbb{Z}|} (1 - \#k(x)^{-s})^{-1}$$

or more generally the zeta function of a scheme X of finite type over the integers or a finite field:

$$\zeta_X = \prod_{x \in |X|} (1 - \#k(x)^{-s})^{-1}$$

(This also specialises to the Dedekind zeta function of a number field.)

Then $Z_X(q^{-s}) = \zeta_X(s)$. So in the case of a finite ground field, we got around the nasty exponent because unlike over $\mathbb{Z}$ we have a uniform base q.

Exercise

$$Z_X(t) = \exp\left(\sum_{m=1}^{\infty} \frac{\#X(\mathbb{F}_{q^m})}{m} t^m\right)$$

Hint: Use the identity $\log(1/(1-s)) = \sum_{m \geq 1} \frac{t^m}{m}$.

Also, note that the logarithmic derivative of $Z_X(t)$ is in fact the generating function for $\#X(\mathbb{F}_{q^m})$.

Exercise Let's compute $Z_{\mathbb{P}^1}(t)$ with the Euler product:

$$\begin{aligned} Z_{\mathbb{P}^1}(t) = Z_\infty(t) Z_{\mathbb{A}^1}(t) &= \frac{1}{1-t} \prod_{0 \neq f \text{ irred. monic}} \frac{1}{1 - t^{\deg(f)}} \\ &= \frac{1}{1-t} \sum_{0 \neq f \text{ monic}} t^{\deg(f)} = \frac{1}{1-t} \sum_{n=0}^{\infty} q^n t^n = \frac{1}{(1-t)(1-qt)} \end{aligned}$$

Further examples The zeta functions of elliptic curves can be computed via the action of Frobenius on the Tate module. (This is very enlightening and foreshadows the use of l-adic cohomology in the general case: The Tate module is nothing else but H^1.)

Weil himself was able to prove the conjectures for curves and abelian varieties (Knowing the l-adic cohomology, it is not surprising that these cases were easier: The cohomology of abelian varieties are the exterior powers of its Tate module and for curves, we have the Jacobian.)[5]

5 The Weil Conjectures

We can finally state the conjectures for the zeta function $Z_X(t)$ formulated by André Weil in 1949 and proven completely by Deligne in 1974. Let $\dim X = n$.

Rationality $Z_X(t)$ is a rational function with integer coefficients of the form

$$\frac{P_1(t)P_3(t)\dots P_{2n-1}(t)}{P_0(t)P_2(t)\dots P_{2n}(t)}$$

with all the P_i being polynomials and $P_0(t) = 1 - t$, $P_{2n}(t) = 1 - q^n t$.

Functional equation

$$Z_X(1/(q^n t)) = \pm q^{nE/2} t^E Z(t)$$

with E is the self-intersection number of the diagonal of $X \times X$.

Betti numbers Setting $B_i := \deg P_i(t)$ the i-th Betti number yields $E = \sum(-1)^i B_i$. If X is the reduction of a variety Y over a number ring R modulo a prime ideal, then $B_i = h^i((Y \times_R \mathbb{C})_h, \mathbb{Z})$ where $_h$ is the associated analytic space.

Riemann hypothesis $P_i(t)$ is a (unique) polynomial with integer coefficients looking like $\prod(1 - \alpha_{ij})$ where a_{ij} are algebraic integers satisfying $|a_{ij}| = q^{i/2}$ for any embedding $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$. (Then the zeros of $\zeta_X(s)$ satisfy the usual Riemann hypothesis.)

Caveats

- The rationality does not imply that the P_i have integer coefficients, only that after reducing, the whole fraction has integer coefficients.

[5] For abelian varieties, see Mumford's book or Milne's notes *Abelian varieties*, which also contains a proof for curves using the Jacobian. For an intersection-theoretic proof of WC for curves, see last year's notes or Stichtenoth's *Algebraic Function Fields and Codes* for a very elementary (but not enlightening) proof due to Stepanov-Bombieri. The case that convinced Weil to publish his conjectures was the one of certain hypersurfaces that he tackled with character theory and can be found in Ireland-Rosen's *Classical Introduction to Modern Number Theory.* I also enjoyed reading the Secret Blogging Seminar posts (`https://sbseminar.wordpress.com/2010/06/10/motive-ating-the-weil-conjecture-proof`) with some remarks on Grothendieck's Standard Conjectures.

- In the setting of X having a model over a number ring like $\mathbb{Z}$, we do not require this model to be smooth. In fact, Fontaine showed that the only smooth projective curve over $\operatorname{Spec}\mathbb{Z}$ is $\mathbb{P}^1$. Relating the B_i to the topological Betti numbers exhibits E as the topological Euler characteristic.
- Algebraic numbers α for which all embeddings have the same absolute value $|q|^{i/2}$ are quite special. They are called *q-Weil numbers of weight i.*

Example In our computed example of $\mathbb{P}^1$, the Betti numbers are $1, 0, 1$ which coincides with the degrees of $1-t, 1, 1-qt$.

5.1 Estimates

Knowing the zeta function (and its logarithm), we can recover a formula for the point counts:

$$\#X(\mathbb{F}_{q^m}) = \sum_{i=0}^{2n}(-1)^i\sum_{j=1}^{B_i}\alpha_{ij}^m = 1+q^{mn}+\sum_{i=1}^{2n-1}(-1)^i\sum_{j=1}^{B_i}\alpha_{ij}^m = 1+q^{mn}+O(q^{m(n-1/2)})$$

In the case of a smooth projective curve of genus g, we find:

$$|\#X(\mathbb{F}_q)-(q+1)| \leq 2g\sqrt{q}$$

which is a direct generalisation of the Hasse-Weil for elliptic curves.

5.2 Personal side remark

Kapranov defines a *motivic zeta function* as

$$Z'_X(t) = \sum_{m\geq 0}[X^{(n)}]t^m$$

where $X^{(n)}$ is the n-th symmetric power of X. In the topological setting, by a theorem of Macdonald (with an easy one-line-proof):

$$Z'_X(t) = 1/(1-t)^{\chi(X)}$$

On the other hand, in the algebraic setting after applying the counting measure, we recover the local zeta function appearing in the Weil conjectures. (How does one prove this?) So in two rather different situations, we have arrived at a rational function!

Where does this phenomenon come from? Is Kapranov's zeta function always rational? The answer to the second question is *No*, Larsen-Lunts gave a counter-example over $\mathbb{C}$ with a specially constructed motivic measure. This measure vanishes on $[\mathbb{A}^1]$, in consequence rationality is still an open question if we localise by $[\mathbb{A}^1]$.[6]

[6] I found these things in notes by Vakil (`http://swc.math.arizona.edu/aws/2015/2015VakilNotes.pdf`) which contain more intriguing facts and questions about the Grothendieck ring of varieties.

Weil cohomology theories

The way to prove the Weil conjectures is to give them a cohomological interpretation. Much of the algebraic geometry initiated Grothendieck was devoted to finding the right cohomology theory, from which the conjectures could be deduced. This so-called *Weil cohomology theory* should be modelled after singular cohomology for smooth, projective complex varieties.

Let k be any field and K a field of characteristic 0. We have the following wish list:

- A Weil cohomology theory over k with coefficients in K should be a contravariant functor

$$\begin{array}{rcl} \{\text{smooth, projective varieties}/k\} & \to & \{\text{graded } K\text{-algebras}\} \\ X & \mapsto & H^*(X,K) = \bigoplus H^i(X,K) \end{array}$$

  where the graded components are finite dimensional K-vector spaces and zero outside $0 \leq i \leq 2\dim X$.

- Poincaré duality: Multiplication induces perfect pairings:

$$H^i(X,K) \times H^{2d-i}(X,K) \to H^{2d}(X,K) \cong K$$

- Künneth formula:

$$H^*(X \times Y, K) = H^*(X,K) \otimes H^*(Y,K)$$

- Cycle map: There exists a $(cl) : Z^i(X) \to H^{2i}(X,K)$ for where Z_i denotes the group of algebraic cycles of codimension i.

- Lefschetz trace formula: For any endomorphism $f : X \to X$ over $k = \overline{k}$ with graph Γ_f, we can compute the number of fixed-points:

$$(\Gamma_f \cdot \Delta_X) = \sum_{i=0}^{2d} (-1)^i \operatorname{Trace}(f^* | H^i(X,K))$$

- Hard Lefschetz Theorem: If $H \subset X$ is a hyperplane section, then multiplication by $\mathrm{cl}(H)^i$ induces an isomorphism $H^i(X,K) \to H^{2d-i}(X,K)$.

- Comparison theorem: For $X/\mathbb{C}$ and $K \subset \mathbb{C}$, $H^*(X,K) \otimes_K \mathbb{C} \cong H^*_{\text{sing}}(X,\mathbb{C})$.

There are different known Weil cohomology theories apart from the traditional singular and de Rham, which do not work over finite fields. These are l-adic cohomology building upon étale cohomology with $K = \mathbb{Q}_l$ ($l \neq \mathrm{char} k$ prime) and crystalline cohomology with $K = W(k)$ (the Witt vectors of k). Rigid cohomology is a p-adic cohomology theory that extends crystalline cohomology.

The Lefschetz formula allows us to count points cohomologically, using the fact that the fixed-points under the Frobenius map F (raising coordinates to the q-th power) are the $\mathbb{F}_q$-points of X:

$$\#X(\mathbb{F}_{q^m}) = (\Gamma_{F^m} \cdot \Delta_X) = \sum_{i=0}^{2d} (-1)^i \operatorname{Trace}((f^m)^* | H^i(X, K))$$

Using the lemma that

$$-\log(\operatorname{charpoly}(\phi)) = \sum_{m \geq 1} \operatorname{Trace}(\phi^m) \frac{t^m}{m}$$

for general vector space endomorphisms ϕ, we can deduce the required rationality with

$$P_i = \operatorname{charpoly}(F | H^i(X, K))$$

(Integrality follows once we see that Z_X is a power series with coefficients in $\mathbb{Z}$ and by the above a rational function in K.)

The functional equation can be derived from Poincaré duality while the Riemann hypothesis is a deeper fact and amounts to the fact of proving that the eigenvalues of the Frobenius map acting on cohomology are Weil numbers.[7]

[7] For a reference, try Deligne's original Weil papers or Freitag-Kiehl's book/Milne's notes on Étale Cohomology.