An Application of the Weil Conjectures to PAC and Large Fields

Erick Knight
Shotaro Makisumi

January 10, 2011

Abstract

This expository paper gives an elementary proof, using the Weil Conjectures for curves, that an infinite algebraic extension of a finite field is PAC and large.

1 Introduction

The aim of this expository paper is to provide an elementary proof that an infinite algebraic extension of a finite field is PAC and large. PAC fields and large fields are two classes of fields appearing in field arithmetic, both defined through the properties of rational points of varieties defined over them. Roughly, the proof reduces these fields to the case of smooth projective curves and applies the Weil Conjectures for curves, where an elementary proof is known.

The paper is organized as follows. Section 2 discusses the Weil Conjectures; Section 2.1 states the conjectures, first in the general case then specializing to curves, and Section 2.2 provides an elementary proof of the Riemann Hypothesis for curves, due to E. Bombieri [3]. Section 3 discusses PAC and large fields, and provides a reduction of their definition to smooth projective curves, following an argument by J. Kollár [1]. Finally, Section 4 uses these results to prove that an infinite algebraic extension of a finite field is PAC and large.

2 The Weil Conjectures

2.1 Introduction to the Weil Conjectures

Let V be a variety over k, a finite field of characteristic p and order q. A natural question concerns the number of points on V. More specifically, letting $k_n = \mathbb{F}_{q^n}$ (so $k = k_1$), one is interested in the number of k_n-rational points on V. It is natural to keep track of this information through a generating function, $\sum_{m=1}^{\infty} N_m X^m$, where $N_m = \#V(k_n)$. Since this sum turns out to be not so well-behaved, one instead considers the following:

Definition 1. *The* zeta function *of V/k is*

$$Z(V,T) = \exp\left(\sum_{m=1}^{\infty} \frac{N_m}{m} T^m \right).$$

Let V be a n-dimensional geometrically irreducible non-singular projective variety over $k = k_1$. Under this assumption, Weil made three conjectures about this zeta function.

Conjecture 1 (The Weil conjectures in full generality)**.**

Rationality: *$Z(V,T)$ is a rational function in T. More precisely, one can write*

$$Z(V,T) = \frac{P_1(T)P_3(T)\cdots P_{2n-1}(T)}{P_0(T)P_2(T)\cdots P_{2n}(T)},$$

where for each i, $P_i(T) \in \mathbb{Z}[T]$ and factors as $(1 - a_{i,1}T)(1 - a_{i,2}T)\cdots(1 - a_{i,j_i}T)$.

Functional Equation:

$$Z(V,T) = \pm q^{-nE/2} T^{-E} Z(V, 1/q^n T),$$

where E is the Euler characteristic of V.

Riemann Hypothesis: *For all i and j, $|a_{i,j}| = q^{\frac{i}{2}}$.*

If $\dim(V) = 1$, i.e. V is a smooth projective curve, then the conjectures are more explicit. Let g be the genus of V. Then, the Weil conjectures state:

Conjecture 2 (The Weil conjectures for curves)**.**

Rationality:

$$Z(V,T) = \frac{f_{2g}(T)}{(1-T)(1-qT)},$$

where f_{2g} is a degree-$2g$ polynomial in $\mathbb{Z}[x]$.

Functional Equation: *One can write*

$$f_{2g}(T) = (1 - \alpha_1 T)(1 - \alpha_2 T)\cdots(1 - \alpha_{2g} T),$$

where the α_is are algebraic integers, and $\alpha_i \alpha_{i+g} = q$ for $i = 1, \ldots, g$.

Riemann Hypothesis: *Moreover, $|\alpha_i| = \sqrt{q}$.*

To see why the third conjecture is called the Riemann hypothesis, let $\zeta(V,s) = Z(V, q^{-s})$. Then all the zeroes of ζ occur when $\mathrm{Re}(s) = \frac{1}{2}$. Moreover, the rationality implies that there are poles precisely at 0 and 1, and the functional equation relates the values of $\zeta(V,s)$ to those of $\zeta(V, 1-s)$ in the case of curves. This is analogous to the case for number fields, where there is a pole at 1 and the zeroes are conjectured to lie on the line $\mathrm{Re}(s) = \frac{1}{2}$.

These conjectures can be restated in terms of N_m. Assuming the conjectures and notation above, one can compute that $N_m = q^m - \sum_{i=1}^{2g} \alpha_i^m + 1$. This formulation is in fact equivalent to the original one, so that the Weil conjectures for curves may be written as follows.

Conjecture 3 (Weil conjectures for curves, enumerative version)**.**

Rationality: *There are* $2g$ *algebraic integers, denoted* α_i*, such that* $N_m = q^m - \sum_{i=1}^{2g} \alpha_i^m + 1$.

Functional Equation: $\alpha_i \alpha_{i+g} = q$ *for* $i = 1, \ldots, 2g$.

Riemann Hypothesis: $|\alpha_i| = \sqrt{q}$*, or equivalently* $\alpha_i = \overline{\alpha_{i+g}}$ *for* $i = 1, \ldots, g$.

While the rationality and the functional equation have straightforward proofs involving the Riemann-Roch theorem, the Riemann Hypothesis is a much deeper result. Assuming the first two parts, the following statements are equivalent:

(1) $|\alpha_i| = \sqrt{q}$ for all $i = 1, \ldots, 2g$.

(2) $|N_m - (q^m + 1)| \leq 2g\sqrt{q^m}$ for all $m \geq 1$.

(3) $N_m = q^m + O(\sqrt{q^m})$ for all $m \geq 1$.

Indeed, it is easy to show that (1) $\Rightarrow$ (2) $\Rightarrow$ (3) $\Rightarrow$ (1). The first two implications are trivial. If $|a_i| \neq \sqrt{q}$ for some a_i, we may assume by the functional equation that $|a_i| > \sqrt{q}$. Then a_i^m eventually dominates the growth of the error term for N_m, so $|N_m - q^m|$ grows faster than $\sqrt{q^m}$.

Finally, we would be remiss to not point out why one would expect the Weil conjectures to be true. Consider a hyperelliptic curve $y^2 = f_{2g+1}(x)$, where f_{2g+1} is a degree-$(2g+1)$ polynomial in x with no repeated roots. To count the number of points in k_m, let χ_2 by the character of order 2 of $k_m^\times$, with the convention that $\chi_2(0) = 0$. Then it is easy to see that the number of solutions to $y^2 = c$ is $1 + \chi_2(c)$, so the number of points on the curve is $\sum_{x \in k_m} (1 + \chi_2(f_{2g+1}(x))) + 1$, where the 1 outside the sum accounts for the point at infinity. This becomes $q^m + \sum_{x \in k_m} \chi_2(f_{2g+1}(x)) + 1$. Naively, one expects that, as m gets large, the values of $\chi_2(f_{2g+1}(x))$ are essentially random, so that the expected value for the error from $q^m + 1$ is $O(\sqrt{q^m})$. Although far from a proof, this suggests why such a theorem is possible.

2.2 An Elementary Proof of the Riemann Hypothesis for Curves

The proof of the Riemann Hypothesis in the general case uses cohomological techniques, which are beyond the scope of this paper. Instead, this section gives an elementary proof for the case of curves, due to E. Bombieri [3].

As is standard, view C as a curve over $\overline{k}$ and defined over k, equipped with a Frobeneous map φ, which is an algebraic bijection (but not an automorphism!) from C to C that is totally ramified everywhere. Then $C(k_m)$ are the fixed points of φ^m, so that one counts the fixed points of powers of φ rather than solutions to polynomial equations.

The proof will proceed in two steps: we first show an upper bound, then use this to show the lower bound. Additionally, it suffices to argue for only the even extensions of $\mathbb{F}_p$, as one only needs that $N_m = q^m + O(\sqrt{q^m})$ for a sequence of m that tends to infinity, and not all m.

Theorem 1 (The upper bound)**.** *Let $C/\overline{k}$ be a projective nonsingular irreducible curve of genus g, defined over a finite field k. If $[k : \mathbb{F}_p]$ is even and $q > (g+1)^4$, then one has that the number of k-rational points, which are the fixed points of the Frobeneous map φ, is less than $q+(2g+1)\sqrt{q}+1$.*

Proof. Assume that φ has at least one fixed point x_0 (otherwise the theorem is trivial). Let N_1 denote the number of k-rational points. By Riemann-Roch, one has that $m + 1 - g \leq \ell(m(x_0)) \leq m + 1$, with equality on the left when $m > 2g - 2$.

If $f \in L(D)$, then $f \circ \varphi \in L(q\varphi(D))$ (if $D = m(x_0)$, since $\varphi(x_0) = x_0$, one has that $f \circ \varphi \in L(qD)$); the image of such functions in $L(q\varphi(D))$ will be denoted $L(D)\circ\varphi$. Every element of the form $f\circ\varphi$ is a q^{th} power (as $(f\circ\varphi) = q\varphi((f))$). The image of the map from $L(D_1)\otimes_{\overline{k}}L(D_2) \to L(D_1+D_2)$ sending $f_1 \otimes f_2$ to f_1f_2 will be denoted $L(D_1)L(D_2)$. Also, the image of the inclusion from $L(D) \hookrightarrow L(p^cD)$ sending f to f^{p^c} will be denoted $L(D)^{(p^c)}$.

Lemma 2. *If $ap^c < q$, the natural map $L(a(x_0))^{(p^c)} \otimes_{\overline{k}} (L(m(x_0)) \circ \varphi) \to L(a(x_0))^{(p^c)}(L(m(x_0)) \circ \varphi)$ is an isomorphism.*

Proof. The map is by definition surjective, so it suffices to prove injectivity. Let $r = \ell(m(x_0))$. Since $\ell((m_0 + 1)(x_0)) \leq \ell(m_0(x_0)) + 1$ for any m_0, there is a basis $s_1, s_2, \ldots, s_r$ of $L(m(x_0))$ such that $\text{ord}_{x_0}(s_i) < \text{ord}_{x_0}(s_{i+1})$. Given r elements $g_i \in L(a(x_0))$ with $\sum_{i=1}^{r} g_i^{p^c}(s_i \circ \varphi) = 0$, it suffices to show that $g_i = 0$ for all i.

Assume otherwise, and let g_{i_0} be the non-zero g_i with the smallest index. Then, letting $g = -g_{i_0}^{p^c}(s_{i_0} \circ \varphi) = \sum_{i=i_0+1}^{r} g_i^{p^c}(s_i \circ \varphi)$, one can compute the order of g at x_0 in two ways and derive a contradiction.

To be precise, we have

$$\begin{aligned}
\text{ord}_{x_0}(g) &= \text{ord}_{x_0}\left(\sum_{i=i_0+1}^{r} g_i^{p^c}(s_i \circ \varphi)\right) \\
&\geq \min_{i>i_0}\left(\text{ord}_{x_0}(g_i^{p^c}(s_i \circ \varphi))\right) \\
&= \min_{i>i_0}\left(p^c \cdot \text{ord}_{x_0}(g_i) + q \cdot \text{ord}_{x_0}(s_i)\right) \\
&\geq -ap^c + q \cdot \text{ord}_{x_0}(s_{i_0+1}),
\end{aligned}$$

where the last inequality follows since $\mathrm{ord}_{x_0}(f) \geq -a$ for all $f \in L(a(x_0))$, and $\mathrm{ord}_{x_0}(s_i) < \mathrm{ord}_{x_0}(s_{i+1})$. On the other hand, $\mathrm{ord}_{x_0}(g) = p^c \cdot \mathrm{ord}_{x_0}(g_{i_0}) + q \cdot \mathrm{ord}_{x_0}(s_{i_0})$, so

$$p^c \cdot \mathrm{ord}_{x_0}(g_{i_0}) \geq -ap^c + q(\mathrm{ord}_{x_0}(s_{i_0+1}) - \mathrm{ord}_{x_0}(s_{i_0})) \geq -ap^c + q > 0.$$

But then g_{i_0} is regular (it has no pole outside of x_0 and is visibly regular there) and has a zero on a projective irreducible curve, so $g_{i_0} = 0$, a contradiction. Thus, the map is injective, and the lemma is proven. $\square$

Equating the dimensions of the two sides, we obtain

Corollary 3. *If $ap^c < q$, $\dim\left(L(a(x_0))^{p^c}(L(m(x_0)) \circ \varphi)\right) = \ell(a(x_0))\ell(m(x_0))$.*

Now, if $ap^c < q$, the composition

$$\delta : L(a(x_0))^{(p^c)}(L(m(x_0) \circ \varphi)) \to L(a(x_0))^{(p^c)} \otimes_{\overline{k}} (L(m(x_0)) \circ \varphi) \to L(a(x_0))^{(p^c)} \otimes_{\overline{k}} L(m(x_0))$$
$$\to L(a(x_0))^{(p^c)} L(m(x_0)) \to L((ap^c + m)(x_0))$$

is well-defined (the first arrow is the inverse of the isomorphism in the lemma, the second is an isomorphism, and the last two are the natural map and the inclusion defined above). If in addition we have that $a, m \geq g$, then by the corollary and Riemann-Roch,

$$\begin{aligned}\dim(\ker(\delta)) &\geq \ell(a(x_0))\ell(m(x_0)) - \ell((ap^c + m)(x_0)) \\ &\geq (a + 1 - g)(m + 1 - g) - (ap^c + m + 1 - g).\end{aligned}$$

If $q = p^\alpha$, choose $c = \frac{\alpha}{2}$ (since $\alpha = [k : \mathbb{F}_p]$ is even), $m = p^c + 2g$, and $a = \lfloor \frac{gp^c}{g+1} \rfloor + g + 1 = p^c - \lceil \frac{p^c}{g+1} \rceil + g + 1$. Since $p^{2c} = q > (g+1)^4$ by assumption, we have $a < p^c$ and so $ap^c < q$. Clearly $a, m \geq g$, so the above inequality applies, and we obtain $\dim(\ker(\delta)) > 0$. Thus there exists some non-zero $f \in \ker(\delta)$. For all x fixed by φ, except x_0 where f is not defined, one has $f(x) = (\delta(f))(x) = 0$. There are by definition $N_1 - 1$ such x, and moreover f is a p^c-th power, so f has at least $p^c(N_1 - 1)$ zeroes. But f only has a pole at x_0, of order at most $ap^c + mq$, so $N_1 \leq a + \frac{mq}{p^c} + 1$. Hence

$$N_1 < \sqrt{q} + \frac{(\sqrt{q} + 2g)q}{\sqrt{q}} + 1 = q + (2g+1)\sqrt{q} + 1,$$

which is what we wanted. $\square$

Theorem 4 (The complete Riemann Hypothesis for curves)**.** *With the assumptions and notations as above, one has that $N_1 = q + O(\sqrt{q})$.*

Proof. There is a separable map $C \to \mathbb{P}^1$ corresponding to a separable extension $\overline{k}(C)/\overline{k}(t)$. Let C' denote the curve corresponding to the normal closure of $\overline{k}(C)/\overline{k}(t)$. Let $G = \mathrm{Gal}(\overline{k}(C')/\overline{k}(t))$ and $H = \mathrm{Gal}(\overline{k}(C')/\overline{k}(C))$, so $H \subset G$. Then G acts via algebraic maps on C'; we may assume that the elements of G are defined over k (if not, make a finite base change, and we are fine for the same reason that we may assume that $[k : \mathbb{F}_p]$ is even). Recall that, in the general Galois covering scenario $X \to Y$ where X and Y are curves, one has that, for all points y lying over an unramified point of the cover, $\varphi(y) = g(y)$ for some g in the Galois group (the Frobeneous substitution at y).

Coming back to our case, let $\nu(C', g)$ be the number of points in C' with Frobeneous substitution g. One can argue as before, replacing $\delta : L(a(x_0))^{(p^c)}(L(m(x_0)) \circ \varphi) \to L(a(x_0))^{(p^c)}L(m(x_0))$ with

$$\delta_g : L(a(x_0))^{(p^c)}(L(m(x_0)) \circ \varphi) \to L(a(x_0))^{(p^c)}(L(m(x_0)) \circ g),$$

to get $\nu(C', g) \leq q + (2g'+1)\sqrt{q}$, where g' is the genus of C'. Meanwhile, we have that $\sum_{g \in G} \nu(C', g) = |G|(q+1) + O(1)$, as the left-hand side counts $|G|$ times the number of points in $\mathbb{P}^1$ unramified in the cover. Thus $\nu(C', g) = q + O(\sqrt{q})$. However, we also have that $\sum_{g \in H} \nu(C', g) = |H|N_1 + O(1)$, so $N_1 = q + O(\sqrt{q})$. □

It should perhaps be noted that the above proof of the lower bound lacks entirely of geometric content, shifting instead the bulk of the argument to an elementay fact in algebraic number theory.

3 PAC Fields and Large Fields

In this section, we look at two important classes of fields appearing in field arithmetic.

Definition 2. *A field k is called* PAC (pseudo-algebraically closed) *if every (non-empty) geometrically irreducible variety over k has a k-rational point.*

Example 1. *1. Algebraically closed fields are PAC.*

2. $\mathbb{R}$ is not PAC. The projective plane curve $(x^2 + y^2 + z^2 = 0) \in \mathbb{P}^2$ is geometrically irreducible and has no $\mathbb{R}$-point.

3. Finite fields are not PAC. For example, for $k = \mathbb{F}_q$ of characteristic $p > 3$, the projective plane curve $(x^q + y^q + z^q = 0) \in \mathbb{P}^2$ is geometrically irreducible and has no k-rational point. One can explicitly write down such a projective plane curve for the remaining cases as well; see [2], Section 11.2.

In examples 2 and 3, we were able to show that the fields were not PAC using not general varieties as in the definition of PAC, but projective plane curves. In fact, J. Kollár showed that this is the case for all non-PAC fields [1]. Since example 3 shows the case k finite, Kollár's proof starts with a geometrically irreducible variety X defined over an infinite field k with no k-rational point, and successively transforms X to obtain the desired plane curve. We shall only need the first step in his proof, the reduction to smooth projective curves, reproduced below. Note in particular that smoothness allows us to apply the Weil conjectures.

Theorem 5. *If k is not PAC, then there exists a (non-empty) geometrically irreducible smooth projective curve over k with no k-rational point.*

Proof. Let X be a geometrically irreducible variety defined over an infinite field k such that X has no k-rational point. Since birational transformations preserve geometric irreducibility, by intersecting with an affine chart if necessary, we may assume that X is affine. Successively intersect X with hyperplanes defined over k to obtain a curve B/k with no k-rational point. By Bertini's theorem, B is geometrically irreducible for general hyperplanes defined over $\overline{k}$. Since k is infinite, there exists a hyperplane defined over k such that this holds.

Let $\overline{B}$ be the projective closure of B. The finite set $\overline{B} \setminus B$ may contain k-rational points, but $\overline{B} \times \overline{B}$ contains at most finitely many k-rational points, so again intersecting with hyperplane defined over k and avoiding these points (which we can since k is infinite), we obtain a geometrically irreducible projective curve C_1/k with no k-rational point. Finally, normalize C_1 to obtain a smooth projective curve C/k with no k-rational point. □

The following class of fields, originally introduced in Galois theory, now appear in field arithmetic because of their nice embedding properties.

Definition 3. *A field k is called* large *(or* ample*) if every (non-empty) geometrically irreducible variety over k with a k-rational point has infinitely many k-rational points.*

Again, this definition may be reduced to smooth projective curves by essentially the same argument as for PAC fields. More precisely, we have

Theorem 6. *If k is not large, then there exists a (non-empty) geometrically irreducible smooth projective curve over k with at least one but only finitely many k-rational points.*

Proof. Finite fields are not large. Let X be a geometrically irreducible variety defined over an infinite field k such that X has at least one but only finitely many k-rational points. We may assume as before that X is affine. Fix a k-rational point p in X, and successively intersect X with hyperplanes defined over k and passing through p to obtain a curve B/k with finitely many k-rational points. Since k is infinite, again by Bertini's theorem, we may choose this hyperplane so that B is geometrically irreducible. Taking the projective closure $\overline{B}$ adds at most finitely many k-rational points. Now $\overline{B}$ has only finite many singular points. Normalize to obtain a smooth projective curve C/k. The preimage of any singular point is a closed subset of C, so this only adds finitely many k-rational points. □

As a consequence, the following is often taken in the literature as the definition of large fields.

Definition 4. *A field k is called* large *(or* ample*) if every (non-empty) geometrically irreducible smooth curve over k with a k-rational point has infinitely many k-rational points.*

It can be shown that every PAC field k is large, so that a non-empty geometrically irreducible variety over k in fact has infinitely many k-rational points. In particular, it is enough to prove just the first part of Theorem 7 below. However, we prove large directly since the argument is the same as that for PAC.

4 Putting Everything Together

We can now state and prove the claim mentioned in the introduction.

Theorem 7. *An infinite algebraic extension of a finite field is PAC and large.*

Proof. Let k be an infinite algebraic extension of $\mathbb{F}_p$. Let C be a smooth projective plane curve over k. To show that k is PAC, by Theorem 5, it suffices to show that C has a k-rational point. Since C is defined by finitely many polynomial equations with coefficients in k, it is in fact defined over $\mathbb{F}_{p^n} \subset k$ for all large enough n. Let g be the genus of C, and take n so large that $\sqrt{p^n} > 2g$. Then C has at least as many k-rational points as it has $\mathbb{F}_{p^n}$-rational points, of which there are, by Theorem 4 (Riemann Hypothesis), more than $(p^n + 1) - 2g\sqrt{p^n} \geq 1$.

For large, we use Theorem 6 and again apply the Riemann Hypothesis, noting that the bound above tends to infinity as $n \to \infty$. □

References

[1] J. Kollár, *Algebraic varieties over PAC fields*, Israel Journal of Math. **161** (2007), no. 1, 89–101.

[2] M. D. Fried and M. Jarden, *Field Arithmetic*, 2nd ed., Ergebnisse der Mathematik (3) **11**, Springer, Heidelberg, 2005.

[3] E. Bombieri, *Counting points on curves over finite fields d'après S. A. Stepanov*, Séminaire Bourbaki, vol. 1972/73 exposés 418-435, Lecture Notes in Mathematics, 1974, Volume 383/1974, 234–241.