THE LEFSCHETZ FIXED POINT THEOREM AND SOLUTIONS TO POLYNOMIALS OVER FINITE FIELDS

ANG LI

Contents

1. Introduction

Suppose we have an equation with integer coefficients, e.g. $y^2 = x^3 + x$ and we want to understand its solutions over a finite field. If we consider the solutions over $\mathbb{C}$, the set of solutions is a complex manifold and can be studied using the powerful tools of complex analysis and algebraic topology. However, since the set of solutions over a finite field is also finite, and any obvious topology makes the set into a finite discrete set, there is little hope of using topological tools over the finite field. The goal of this paper is to demonstrate the idea that counting points provides a good replacement for algebraic topology over finite fields by analyzing some examples. We begin by counting points in some specific examples of algebraic varieties, which are sets that can be locally described as the zero set of some polynomial.

Example 1.1. (The Projective Space) $\mathbb{P}^n(\mathbb{F}_q)$ can be viewed as the collection of distinct lines in the vector space $\mathbb{F}_q^{n+1}$. Thus the cardinality of $\mathbb{P}^n(\mathbb{F}_q)$ can be calculated by counting number of distinct lines and we have

$$|\mathbb{P}^n(\mathbb{F}_q)| = \sum_{i=0}^{n} q^i. \tag{1.2}$$

Observe that the number of points in projective space over $\mathbb{F}_q$ is a polynomial in q and the coefficient of $q^{k/2}$ is the k-th Betti number of $\mathbb{P}^n(\mathbb{C})$. We will compute these Betti numbers in Example 2.19.

Example 1.3. (Grassmannians) $Gr(n,k)(\mathbb{F}_q)$ is the collection of distinct k-dimensional subspaces in the vector space $\mathbb{F}_q^n$. And the number of distinct k-dimensional subspaces is

$$|Gr(n,k)(\mathbb{F}_q)| = \frac{(q^n-1)(q^n-q)...(q^n-q^{k-1})}{(q^k-1)(q^k-q)...(q^k-q^{k-1})}. \tag{1.4}$$

Similar to projective plane, the number of points on Grassmannian over $\mathbb{F}_q$ is also a polynomial in q. For example, if we look at $Gr(4,2)(\mathbb{F}_q)$, the cardinality is $1+q+2q^2+q^3+q^4$ by above computation and we also have the coefficient of $q^{k/2}$ is the Betti number of $Gr(4,2)(\mathbb{C})$. We will compute the Betti numbers in Example 2.24.

Example 1.5. We use an open-source mathematical software called Sage to count the number of solutions of $y^2 = x^3 + x$ in finite fields $\mathbb{F}_q$ for small prime powers and we also count the point at infinity as one solution:

q	Number of solutions
5	$4 = 5 + 2 \cdot (-0.447) \cdot 5^{1/2} + 1$
5^2	$32 = 5^2 + 2 \cdot (0.6) \cdot (5^2)^{1/2} + 1$
5^3	$148 = 5^3 + 2 \cdot (0.98) \cdot (5^3)^{1/2} + 1$
7	$8 = 7 + 2 \cdot (0) \cdot 7^{1/2} + 1$
7^2	$64 = 7^2 + 2 \cdot (1) \cdot (7^2)^{1/2} + 1$
7^3	$344 = 7^3 + 2 \cdot (0) \cdot (7^3)^{1/2} + 1$
11	$12 = 11 + 2 \cdot (0) \cdot 11^{1/2} + 1$
11^2	$144 = 11^2 + 2 \cdot (1) \cdot (11^2)^{1/2} + 1$
11^3	$1332 = 11^3 + 2 \cdot (0) \cdot (11^3)^{1/2} + 1$
13	$20 = 13 + 2 \cdot (0.832) \cdot 13^{1/2} + 1$
13^2	$160 = 13^2 + 2 \cdot (-0.385) \cdot (13^2)^{1/2} + 1$

Notice that the number of solutions in the finite field $\mathbb{F}_q$ is in the form

$$q + 2 \cdot d(q) \cdot q^{1/2} + 1, \tag{1.6}$$

where $d(q)$ is a constant depending on q with absolute value less than 1. This connection is interesting because the number of solutions on the finite field $\mathbb{F}_q$ look almost like a polynomial function of q and the coefficient of $q^{k/2}$ is the k-th Betti number of $\mathbb{C}/\Lambda$. We will explain the computation of these Betti numbers in Example 2.26.

This connection between coefficients and Betti numbers is not a coincidence and in order to understand this connection, first we need to re-interpret the number of points on a variety as the number of fixed points of an algebraic map. Let X be the solutions of the equation in $\overline{\mathbb{F}_q}$. Then any solution in $\mathbb{F}_q$ is just a fixed point under the Frobenius map

$$\text{Frob} : X \to X, \tag{1.7}$$

raising each coordinate of a point x in the projective space to the q-th power.

So the number of solutions is the number of fixed points of the Frobenius map. A lift of the Frobenius map over $\mathbb{C}$ is a polynomial with coefficients that make sense in both $\overline{\mathbb{F}}_q$ and $\mathbb{C}$ and defines the Frobenius map over $\overline{\mathbb{F}}_q$. If we can lift the Frobenius map to field of characteristic 0 without changing the number of fixed points, we can apply the following Lefschetz fixed point theorem to study the number of fixed points of the lift on a smooth manifold.

Theorem 1.8. *(The Lefschetz fixed point theorem) Let X be a closed smooth manifold and let $f : X \to X$ be a smooth map with all fixed points nondegenerate. Then*

$$L(f) = \sum_i (-1)^i Tr(f_* : H_i(X;\mathbb{Q}) \to H_i(X;\mathbb{Q})), \tag{1.9}$$

where $L(f)$ is the Lefschetz number which counts the number of fixed points with some signed multiplicity. Using the Lefschetz theorem, we can calculate the number of fixed points of the Frobenius map by calculating traces of the induced homomorphisms on homology groups and the number of fixed points is then just the number of points on the variety. We give more details in section 4.

To prove the Lefschetz fixed point theorem, we will use that the number of fixed points of a map is the number of points in the intersection of the graph with the diagonal, and thus we will need to develop intersection theory on manifolds. We will also need Kunneth formula and Poincaré duality to express the intersection using homology. We will start with background knowledge on intersection theory and algebraic topology in section 2. Then we will prove the Lefschetz fixed point theorem in section 3 and look at counting fixed points of the Frobenius map in section 4.

2. Background on manifolds and algebraic topology

We begin with some background knowledge on intersection theory and algebraic topology; see [1, 3] for intersection theory and [2] for algebraic topology.

The following will be assumed in this section: X, Y and Z are boundaryless manifolds, X is compact, Z is a closed submanifold of Y and X and Z have complementary dimensions, i.e. $\dim X + \dim Z = \dim Y$.

Definition 2.1. Suppose $f : X \to Y$ is transverse to Z. Given any point such that $f(x) = z \in Z$, we have

$$df_x T_x(X) \oplus T_z(Z) = T_z(Y). \tag{2.2}$$

Further $f^{-1}(Z)$ is a finite number of points, each with orientation number 1 or -1 by the preimage orientation, which is 1 if the orientation on $df_x T_x(X) \oplus T_z(Z)$ is the same as the prescribed orientation on $T_z(Y)$, and -1 otherwise. Define the *intersection number* $I(f, Z)$ to be the sum over all fixed points of these orientation numbers.

Proposition 2.3. *If $X = \partial W$ and $f : X \to Y$ extends to W, then $I(f, Z) = 0$.*

Proof. Suppose f extends to F, which we may assume to be transverse to Z by the Extension Theorem [1, p. 72]. Then $f^{-1}(Z) = \partial F^{-1}(Z)$. Since $F^{-1}(Z)$ is an one-manifold with boundary, $I(f, Z) = 0$. □

Proposition 2.4. *Homotopic maps always have the same intersection number.*

Then we can define the intersection number for any function.

Definition 2.5. Given any $g : X \to Y$, pick f such that f is homotopic to g and f is transverse to Z. Define the intersection number $I(g, Z) = I(f, Z)$.

By the previous proposition, the intersection number is well defined.

Definition 2.6. When Y is connected and X has the same dimension as Y, we define the degree of an arbitrary smooth map $f : X \to Y$ to be the intersection number $I(f, \{y\})$.

Proposition 2.7. *Suppose that $f : X \to Y$ is a smooth map of compact oriented manifolds having the same dimension and that $X = \partial W$. If f can be extended to all of W, then $deg(f) = 0$.*

Proposition 2.8. *Let W be a smooth compact region in $\mathbb{C}$ whose boundary contains no zeros of the polynomial p. Then the total number of zeros of p inside W counting multiplicities is the degree of the map $p/|p| : \partial W \to S^1$.*

Proposition 2.9. *$f \pitchfork g$ if and only if $f \times g \pitchfork \Delta$, and then*

$$I(f, g) = (-1)^{dimZ} I(f \times g, \Delta). \tag{2.10}$$

Definition 2.11. For arbitrary maps $f : X \to Y$, $g : Z \to Y$, we define $I(f, g) = (-1)^{dimZ} I(f \times g, \Delta)$.

Proposition 2.12. *If f_0 and g_0 are respectively homotopic to f_1 and g_1, then $I(f_0, g_0) = I(f_1, g_1)$.*

Proposition 2.13. $I(f, g) = (-1)^{(dimX)(dimZ)} I(g, f)$.

Let X be a closed oriented smooth manifold of dimension n. Let A and B be closed oriented smooth submanifolds of X of dimensions $n-i$ and $n-j$ respectively which intersect transversally. Then $A \cap B$ is a submanifold of dimension $n-(i+j)$. When $i + j = n$, $A \cap B$ is a finite set of points.

By Poincaré duality, there is a isomorphism $D : H^i(M, \mathbb{Z}) \to H_{n-i}(M)$ such that $D(\alpha) = [M] \frown \alpha$, where $\frown$ is the cap product. Let $[A], [B], [A \cap B]$ be images of the fundamental classes of $A, B, A \cap B$ under the inclusion map into X. Then we have $[A] \in H_{n-i}(X)$, $[B] \in H_{n-j}(X)$ and $[A \cap B] \in H_{n-(i+j)}(X)$. We denote their Poincaré duals by $[A]^*$, $[B]^*$ and $[A \cap B]^*$. Cup product is Poincaré dual to intersection [3, p. 2]:

Theorem 2.14. $[A]^* \smile [B]^* = [A \cap B]^*$.

We can use Poincaré duality to define a intersection pairing for homology groups.

Definition 2.15. Given X a closed oriented manifold of dimension n, we define the *intersection pairing*

$$\cdot : H_{n-i}(X) \otimes H^{n-j}(X) \to H^{n-i-j}(X) \tag{2.16}$$

by first applying Poincaré duality, taking the cup product and then applying Poincaré duality again:

$$\alpha \cdot \beta = [X] \frown (\alpha^* \smile \beta^*). \tag{2.17}$$

By Theorem 2.14, we have

$$[A] \cdot [B] = [A \cap B]. \tag{2.18}$$

When A and B have complementary dimensions and X is connected, we have $[A] \cdot [B] \in H_0(X) = \mathbb{Z}$ is the signed number of intersection points.

Now we calculate the cohomology groups of the complex points of the algebraic varieties from earlier examples: the projective plane, more general Grassmannians

and solutions of the equation $y^2 = x^3 + x$. These computations will confirm the connection between the coefficient of $q^{k/2}$ in the cardinality of solutions in $\overline{\mathbb{F}_q}$ and the k-th Betti number. We first calculate the cohomology groups for the complex projective plane by cell decomposition.

Example 2.19. (The Complex Projective Plane) $\mathbb{CP}^n$ has the cell decomposition

$$\mathbb{CP}^n = [1 : x_1 : .. : x_n] \sqcup [0 : x_1 : ... : x_n] = [1 : x_1 : ... : x_n] \sqcup \mathbb{CP}^{n-1}, \tag{2.20}$$

where $[1 : x_1 : ... : x_n]$ is isomorphic to the $\mathbb{C}^n$. Inductively, we have

$$\mathbb{CP}^n = \mathbb{C}^n \sqcup \mathbb{C}^{n-1} \sqcup ... \sqcup \mathbb{C} \sqcup [0 : ... : 0 : 1]. \tag{2.21}$$

Since $\mathbb{C}$ is a dimension 2 manifold, $\mathbb{CP}^n$ has no odd dimensional cells. Thus, $H_i(\mathbb{CP}^n, \mathbb{Z}) = 0$ for i odd and $H_i(\mathbb{CP}^n, \mathbb{Z}) = \mathbb{Z}$ for $0 \leq i \leq 2n$ even. Using the universal coefficients theorem for cohomology, the same is true for cohomology groups.

Besides, $H^*(\mathbb{CP}^n, \mathbb{Z}) = \oplus_{i=0}^{2n} H^i(\mathbb{CP}^n, \mathbb{Z})$ has a graded ring structure under the cup product. Notice that an element of degree $2k$ is a the fundamental class of $\mathbb{CP}^k$ inside $\mathbb{CP}^n$ and by (2.18) we know that

$$[\mathbb{CP}^{n-1}] \cdot [\mathbb{CP}^k] = [\mathbb{CP}^{n-1} \cap \mathbb{CP}^k] = [\mathbb{CP}^{k-1}]. \tag{2.22}$$

Thus if we let T be an element of order 2, we know that H^* has the following graded ring structure:

$$H^*(\mathbb{CP}^n, \mathbb{Z}) = \mathbb{Z}[T]/(T^{n+1}). \tag{2.23}$$

Similarly, we can calculate the cohomology groups of a Grassmannian by a Schubert cell decomposition, see [5].

Example 2.24. (Grassmannian) Let $Gr(n, k)$ denote the Grassmannian that parametrizes k-dimensional linear subspaces of n-dimensional vector space $\mathbb{C}^n$. Fix the flag to be the standard flag of $\mathbb{C}^n$. Then $Gr(n, k)$ has a decomposition as the disjoint union of Schubert cells:

$$Gr(n, k) = \sqcup_{\mathbf{j} \in [n]} \mathcal{C}_{\mathbf{j}}, \tag{2.25}$$

where for each index $\mathbf{j} = \{j_1, ..., j_k\}$, the Schubert cell $\mathcal{C}_{\mathbf{j}}$ has a unique representation as a $k \times n$ matrix in row echelon form, where (l, j_l) position contains 1 and zeros above, below and to the right in l-th row [5, p. 2]. Note that the Schubert cell $\mathcal{C}_{\mathbf{j}}$ has dimension $\sum_l (j_l - l)$. To calculate the cohomology of $Gr(n, k)$, we quote the following proposition from Hatcher [2].

Proposition 2.26. *The cells $\mathcal{C}_j$ are the cells of a CW structure on $Gr(n, k)$.*

Furthermore, the cell $\mathcal{C}_{\mathbf{j}} \cong \mathbb{C}^a$, where $a = \sum j_l - l$. Hence, $Gr(n, k)$ has just even dimensional cells.

We can calculate the cohomology groups for some specific n and k. For instance, when $n = 4$ and $k = 2$, the Grassmannian $Gr(4, 2)$ can be decomposed to 6 Schubert cells with $\mathbf{j} = \{1, 2\}, \{1, 3\}, \{1, 4\}, \{2, 3\}, \{2, 4\}, \{3, 4\}$. With respect to the standard flag, they are parametrized as follows:

$$\mathcal{C}_{\{1,2\}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}; \mathcal{C}_{\{1,3\}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & * & 1 & 0 \end{pmatrix}; \mathcal{C}_{\{1,4\}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & * & * & 1 \end{pmatrix}; \tag{2.27}$$

$$\mathcal{C}_{\{2,3\}} = \begin{pmatrix} * & 1 & 0 & 0 \\ * & 0 & 1 & 0 \end{pmatrix}; \mathcal{C}_{\{2,4\}} = \begin{pmatrix} * & 1 & 0 & 0 \\ * & 0 & * & 4 \end{pmatrix}; \mathcal{C}_{\{3,4\}} = \begin{pmatrix} * & * & 1 & 0 \\ * & * & 0 & 1 \end{pmatrix}. \tag{2.28}$$

Thus cells of $Gr(4,2)$ have dimension $0,2,4,4,6,8$. Thus we have $H_i(Gr(4,2)) = \mathbb{Z}$ for $i = 0,2,6,8$ and $H_i(Gr(4,2)) = \mathbb{Z}^2$ for $i = 4$. By the universal coefficient theorem, the cohomology groups are the same.

The cohomology groups of the elliptic curve $y^2 = x^3 + x$ in $\mathbb{C}$ can be calculated using some facts from complex analysis.

Example 2.29. Let $E(\mathbb{C})$ denote the elliptic curve $y^2 = x^3 + x$ for $x, y \in \mathbb{C}$. By the theory of elliptic curves from complex analysis, we know $E(\mathbb{C})$ and $\mathbb{C}/\Lambda$ have natural structures as complex analytic manifolds and they are biholomorphic, where Λ is the lattice generated by 1 and i [7].

The quotient $\mathbb{C}/\Lambda$ can be identified as the torus $S^1 \times S^1$, with homology groups $H_0(S^1 \times S^1; \mathbb{Z}) = H_2(S^1 \times S^1; \mathbb{Z}) = \mathbb{Z}$ and $H_1(S^1 \times S^1; \mathbb{Z}) = \mathbb{Z}^2$. Using the universal coefficients theorem for cohomology, we know that the associated Betti numbers are $1, 2, 1, 0, ...$ for $E(\mathbb{C})$. Recalling the cardinality of solutions in $\overline{\mathbb{F}_q}$ from the introduction, we have the coefficient of $q^{k/2}$ is the corresponding k-th Betti number of $E(\mathbb{C})$. This is not merely a coincidence and we will give more detailed explanations in section 4.

3. The Lefschetz fixed point theorem

We now use intersection theory to prove the Lefschetz fixed point theorem.We first define the global Lefschetz number and introduce some properties of the Lefschetz number.

Definition 3.1. Define the *diagonal* to be

$$\Delta = \{(x,x) | x \in X\} \subset X \times X. \tag{3.2}$$

Also define the *graph* of f to be

$$\Gamma(f) = \{(x, f(x)) | x \in X\} \subset X \times X. \tag{3.3}$$

Definition 3.4. The global Lefschetz number of f is the intersection number $I(\Delta, \Gamma(f))$, denoted $L(f)$.

We have the following theorem directly from the definition of Lefschetz number [1, p. 119-120].

Theorem 3.5. *Let $f : X \to X$ be a smooth map on a compact orientable manifold. If $L(f) \neq 0$, then f has a fixed point.*

Proposition 3.6. *$L(f)$ is a homotopy invariant.*

Then we can prove the Lefschetz fixed point theorem stated in section 1:

Theorem. *(The Lefschetz fixed point theorem) Let X be a closed smooth manifold and let $f : X \to X$ be a smooth map with all fixed points nondegenerate. Then*

$$L(f) = \sum_i (-1)^i Tr(f_* : H_i(X; \mathbb{Q}) \to H_i(X; \mathbb{Q})). \tag{3.7}$$

It follows from the universal coefficient theorem that the above traces are integers. Since p is a fixed point is equivalent to $p \in \Delta \cap \Gamma(f)$, to prove the Lefschetz theorem, we will look at $\Delta \cap \Gamma(f) \subset X \times X$. We also have

Lemma 3.8. *f has nondegenerate fixed points if and only if $\Gamma(f)$ and Δ intersect transversally in $X \times X$* [3, p. 5].

It follows that if f has only nondegerate fixed points, we have

$$L(f) = [\Gamma(f) \cap \Delta] = [\Gamma(f)] \cdot [\Delta]. \tag{3.9}$$

To prove the Lefschetz theorem, we just need to compute the intersection number $[\Gamma(f)] \cdot [\Delta]$.

Recall that for any topological spaces X and Y there is a homology cross product

$$\times : H_i(X) \otimes H_j(Y) \to H_{i+j}(X \times Y). \tag{3.10}$$

If X and Y are smooth manifolds and A and B are closed oriented submanifolds of X and Y, then we have

$$[A] \times [B] = [A \times B]. \tag{3.11}$$

Let $n = dim(X)$. For $\alpha \in H_*(X)$ of pure degree, we denote the degree by $|\alpha|$. We have the following lemmas [3, p. 6]:

Lemma 3.12. *Let $\alpha, \beta, \gamma, \delta \in H^*(X)$ with $|\alpha| + |\beta| = |\gamma| + |\delta| = n$. Then*

$$(\alpha \times \beta) \cdot (\gamma \times \delta) = (-1)^{|\beta|}(\alpha \cdot \gamma)(\beta \cdot \delta), \tag{3.13}$$

if $|\beta| = |\gamma|$; and 0 otherwise.

Lemma 3.14. *If $\alpha, \beta \in H^*(X)$ with $|\alpha| + |\beta| = n$, then*

$$[\Gamma(f)] \cdot (\alpha \times \beta) = (-1)^{|\alpha|} f_* \alpha \cdot \beta. \tag{3.15}$$

Note that if $\alpha, \beta, \gamma, \delta$ can be represented by submanifolds, the above lemmas can be proved by Theorem 1.1. In general, these two lemmas follow from the basic properties of cup products and we skip the computation here.

Let $\{e_k\}$ be a basis for the vector space $H^*(X; \mathbb{Q})$ and let $\{e'_k\}$ be the dual basis of $H^*(X; \mathbb{Q})$, with respect to the intersection pairing $\cdot$, i.e., $e_i \cdot e'_j = \delta_{i,j}$. This dual basis exists and is unique since the intersection pairing is a perfect pairing.

By the Kunneth theorem $H^*(X \times X; \mathbb{Q}) = H^*(X; \mathbb{Q}) \otimes H^*(X; \mathbb{Q})$, with the isomorphism given by homology cross product. Then $\{e_i \times e'_j\}$ is a basis for $H^*(X \times X; \mathbb{Q})$. Then we can write $[\Delta]$ in terms of these basis elements:

Lemma 3.16. $[\Delta] = \sum_k e_k \times e'_k$.

Proof. Since $\{e'_i \times e_j\}$ is also a basis, it is sufficient to check that both sides have the same intersection pairing with $e'_i \times e_j$ for any $|e'_i| + |e_j| = n$.

$$(\sum_k e_k \times e'_k) \cdot (e'_i \times e_j) = \sum_{k:|e'_k|=|e'_i|} (-1)^{|e'_i|}(e_k \cdot e'_i)(e'_k \cdot e_j) \tag{3.17}$$

$$= (-1)^{|e'_i|} e'_i \cdot e_j \tag{3.18}$$

$$= [\Delta] \cdot (e'_i \times e_j). \tag{3.19}$$

Then we have $[\Delta] = \sum_k e_k \times e'_k$ as desired. □

With this equality, we can prove the Lefschetz fixed point theorem.

Proof. By the previous lemmas, we have

$$[\Gamma(f)] \cdot [\Delta] = [\Gamma(f)] \cdot \sum_k e_k \times e'_k \tag{3.20}$$

$$= \sum_k (-1)^{|e_k|} f_* e_k \cdot e'_k \tag{3.21}$$

$$= \sum_i (-1)^i Tr(f_* : H_i(X) \to H_i(X)). \tag{3.22}$$

□

Then we use three examples to illustrate how to use Theorem 3.7 [1]. We start with the well-known Brouwer fixed point theorem.

Theorem 3.23. *(Brouwer Fixed Point Theorem) Any smooth map $f : D^n \to D^n$ has a fixed point.*

Proof. To prove the Brouwer fixed point theorem from the Lefschetz fixed point theorem, simply notice that $H_0(D^n)$ is the only non-trivial homology group of D^n and since D^n is connected, $L(f) = 1$ for any $f : D^n \to D^n$ smooth. $L(f) \neq 0$ implies that f has a fixed point. □

We denote the Euler characteristic of a manifold X by $\chi(X)$, which is defined by

$$\chi(X) = \sum_i (-1)^i \dim(H_i(X)). \tag{3.24}$$

We can also use Lefschetz fixed point theorem to calculate the Euler characteristic of a manifold simply by looking at the number of fixed points of a map homotopic to the identity map.

Example 3.25. The Euler characteristic of S^2 is 2.

Proof. Just look at the map $f(x) = \pi(x + (0, 0, -1/2))$, where π is the projection from $\mathbb{R}^3$ to S^2 defined by

$$\pi(x) = x/\|x\|. \tag{3.26}$$

The map f is homotopic to the identity map by the homotopy $F : S^2 \times I \to S^2$ defined by

$$F(x, t) = \pi(x + (0, 0, -t/2)). \tag{3.27}$$

The map f has two fixed points, $(0, 0, 1)$ and $(0, 0, -1)$, which both have positive orientation number. So the we have

$$L(f) = 2, \tag{3.28}$$

which implies $\chi(X) = 2$. □

Another similar example is the calculation of the Euler characteristic of a compact connected Lie group.

Example 3.29. The Euler characteristic of a compact connected Lie group is zero.

Proof. Let the compact connected Lie group be G and let $g \in G$ such that $g \neq 1$. Define $f : G \to G$ by $f(x) = g \cdot x$. This smooth map is homotopic to id_G since the Lie group G is a connected manifold but has no fixed point. Then we know

$$\chi(G) = L(f) = 0. \tag{3.30}$$

□

4. Fixed points of Frobenius and counting points

Suppose we want to count the number of solutions of $y^2 = x^3 + x$ for $x, y \in \mathbb{F}_q$. The problem with a finite field is that the set of solutions is finite and thus does not have an obvious geometric structure to which we can apply topological tools. For this particular reason, we will first count the number of solutions in the infinite algebraic closure $\overline{\mathbb{F}_q}$ and decide which solutions lie in $\mathbb{F}_q$. We will use Lefschetz fixed point theorem to count the number of solutions and since we need a compact manifold to apply Lefschetz fixed point theorem, we assume that there is a point at infinity and our varieties are compact.

Recall that we understand the set of solutions of $y^2 = x^3 + x$ in $\mathbb{C}$ in Example 2.29. A good analogue of solving the equation in $\mathbb{C}$ is to solve the equation in the algebraic closure $\overline{\mathbb{F}_q} = \cup_n \mathbb{F}_{q^n}$. Let X be the set of solutions (x, y) of $y^2 = x^3 + x$ for $x, y \in \overline{\mathbb{F}_q}$. Given any $(x, y) \in X$,we have $(x^q, y^q) \in X$ since

$$(y^q)^2 = (x^3 + x)^q = (x^q)^3 + x^q, \tag{4.1}$$

which follows from the binomial theorem and the fact that $q = 0$ in $\mathbb{F}_q$.

Besides, given (x, y) such that $(x^q, y^q) = (x, y)$, we have

$$x^{q-1} = y^{q-1} = 1, \tag{4.2}$$

which means $(x, y) \in \mathbb{F}_q \times \mathbb{F}_q$. Hence the condition $(x, y) \in \mathbb{F}_q \times \mathbb{F}_q$ is equivalent to $(x^q, y^q) = (x, y)$. Let

$$\text{Frob} : X \to X \tag{4.3}$$

be the map sending (x, y) to (x^q, y^q). Then the number of solutions for $x, y \in \mathbb{F}_q$ is just the number of fixed points of Frob.

Suppose that we have some homology theory $'H_i'$ in this geometry X and we have the Lefschetz fixed point theorem with respect to this homology theory. Suppose f is any map defined by a polynomial which makes sense in both $\mathbb{C}$ and $\overline{\mathbb{F}}_q$. We know that

$$L(f) = \sum_i (-1)^i Tr(f_* :' H_i'(X) \to' H_i'(X)). \tag{4.4}$$

If we further assume that Betti numbers as well as traces of f_* are the same over $\mathbb{F}_q$ and $\mathbb{C}$ for any general map f that can be described by polynomials with integer coefficients, then sometimes we can compute number solutions using complex geometry. For example we can look at the Frobenius map on the projective plane:

Example 4.5. For a prime power q, the Frobenius map on the complex projective space $\mathbb{F}^q$ is defined by

$$\text{Frob}([x_0 : ... : x_n]) = [x_0^q : ... : x_n^q], \tag{4.6}$$

and the same polynomials define a map from $\mathbb{CP}^n$ to $\mathbb{CP}^n$. Then we can compute the number of fixed point directly. Give $[x_0 : ... : x_n]$ a fixed point, we have

$$(x_0, ..., x_n) = c \cdot (x_0^q, ...x_n^q). \tag{4.7}$$

There are q choices for x_i, any $q-1$-th root of unity and 0 but the x_i cannot all be 0. Further, each $[x_0 : ... : x_n]$ is counted $q-1$ times. Thus there are $\frac{q^n-1}{q-1} = \sum_{i=0}^{n-1} q^i$ fixed points. On the other hand, any nontrivial cohomology group of $\mathbb{CP}^n$ has even dimension and the trace is q^{k-1} on the cohomology group $H^{2k}(\mathbb{CP}^n)$. By the Lefschetz fixed point theorem, there are $1 + q + ... + q^{n-1}$ fixed points, which is consistent with our direct computation. As observed in Example 1.1, this is also the cardinality of $\mathbb{P}^n(\mathbb{F}_q)$.

Remark 4.8. A similar computation can be carried out for the Grassmannians and the number of fixed points is $1 + q + 2q^2 + q^3 + q^4$ for $Gr(4, 2)(\mathbb{C})$, which is the cardinality of $Gr(4, 2)(\mathbb{F}_q)$ as observed in Example 1.3.

However, this simple computation for the projective space does not work for the solutions of $y^2 = x^3 + x$ since given a solution $(x, y) \in \mathbb{C} \times \mathbb{C}$, the image (x^q, y^q) is not guaranteed to be another solution. It is not hopeless to lift the Frobenius map in another way because we can write the Frobenius map in $\mathbb{F}_q$ as $(x, y) \to (x + q \cdot f_1(x, y), y + q \cdot f_2(x, y))$ for any polynomials f_1 and f_2 and it is possible that some f_1, f_2 still makes sense in $\mathbb{C}$. But it might be difficult to find f_1 and f_2 explicitly. So instead we use the non-trivial theory of elliptic curves to show that a lifting exists in some special cases.

Recall from Example 2.29 that the set of solutions over $\mathbb{C}$ is isomorphic to $\mathbb{C}/\Lambda$, where Λ is the lattice $\langle 1, i\rangle$ in the complex plane. We know that multiplication by any $c \in \Lambda$ gives an endomorphism $f : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda$ and the following proposition shows that in fact any holomophic map is of this form.

Proposition 4.9. *Any holomorphic map $f : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda$ such that $f(0) = 0$ is given by multiplication by some $c \in \Lambda$, and thus the set of endomorphisms of $\mathbb{C}/\Lambda$ is $\mathbb{Z}[i]$.*

Proposition 4.10. *Holomorphic maps from $E(\mathbb{C})$ to $E(\mathbb{C})$ are all algebraic maps. i.e. $c \in \mathbb{Z}[i]$ gives a map from $E(\mathbb{C})$ to $E(\mathbb{C})$, which sends (x, y) to $(f(x, y), g(x, y))$ with $f, g \in \mathbb{Z}[i, 1/2][x, y]$.*

We also need the following proposition to lift the Frobenius map to $\mathbb{C}$.

Proposition 4.11. *If q is a prime power and $q \equiv 1$ mod 4, there exists $c \in \mathbb{Z}[i]$ such that $\|c\|^2 = q$ and multiplication by c is an endomorphism which lifts the Frobenius map.*

The first proposition can be proved using properties of a holomorphic function, basic complex analysis and algebraic topology but the other two propositions are non-trivial consequences of the algebraic theory of elliptic curves. The complete proofs of these propositions are beyond the scope of this paper, but cf. [4].

With these propositions, we can lift the Frobenius map to $\mathbb{C}$ and calculate the Lefschetz number. Let multiplication by $c \in \mathbb{Z}[i]$ denote the lifting of Frobenius map, call it F. We first look at the degree of this map.

The degree of the map $F : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda$ is the number of preimages of a class

$[z] \in \mathbb{C}/\Lambda$. We calculate the number of preimages of 0. Let z be a preimage of 0, we have:

$$c \cdot (z) = 0 + \lambda, \tag{4.12}$$

where $\lambda \in \Lambda$. Let $c = a + bi$, where $a, b \in \mathbb{Z}$. With $\lambda \in \Lambda$, we know that the number of preimages is just the number of lattice points in the square with vertices $(0,0), (a,b), (b,-a)$ and $(a-b, a+b)$, which is $a^2 + b^2 = \|c\|^2$. Thus $\|c\|^2 = q$ because by assumption the degree of F is q. Hence

$$Tr(F_* : H_2(E(\mathbb{C})) \to H_2(E(\mathbb{C}))) = q. \tag{4.13}$$

Then we look at trace of F_* on $H_1(E(\mathbb{C}))$. In this case, F_* is the linear operator represented by the matrix $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ where a is the real part of c and b is the imaginary part. Then the trace of F_* is simply $2a$. Further, we know that

$$2a \leq 2\|c\| = 2\sqrt{q}. \tag{4.14}$$

Since we assume that the Betti numbers as well as the traces of f_* are the same over $\mathbb{F}_q$ and $\mathbb{C}$, the Lefschetz number of the Frobenius map in $\overline{\mathbb{F}_q}$ equals the Lefschetz number of the lifting F in $\mathbb{C}$. Then we have

$$L(\text{Frob}) = L(F) = \sum_i (-1)^i Tr(F_* : H_i(E(\mathbb{C}))) = q - 2d\sqrt{q} + 1, \tag{4.15}$$

where $|d| = |a/\sqrt{q}| \leq 1$. And thus the number of solutions of the equation in $\mathbb{F}_q$ is just the number of fixed points of the Frobenius map, which is $q - 2d\sqrt{q} + 1$.

Remark 4.16. The Lefschetz fixed point theorem gives us the value of Lefschetz number, i.e. the signed sum of number of fixed point, which is not necessarily equal to the actual number of fixed points. However, in the complex case, we always have distinguished orientations so intersections are always positive. Since we are working by analogy with the complex case, the Lefschetz number is exactly the actual number of fixed points.

This result is consistent of our computation earlier in Example 1.5 since the coefficient of $q^{1/2}$ has absolute value less than or equal to 2. By using the Lefschetz fixed point theorem as well as other tools in complex analysis and algebraic topology, we have partially explained why the number of points in $\mathbb{F}_q$ on this curve looks almost like a polynomial function in q and why the coefficient of $(q^{1/2})^k$ is the k-th Betti number.

Acknowledgments. It is a pleasure to thank my mentor, Sean Howe, for picking this interesting topic and giving helpful advice.

References

[1] Victor Guillemin and Allan Pollack. Differential Topology. American Mathematical Society. 2010.
[2] Allen Hatcher. Algebraic Topology. http://www.math.cornell.edu/ hatcher/AT/AT.pdf.
[3] Michael Hutchings. Cup product and intersections. http://math.berkeley.edu/ hutching/teach/215b-2011/cup.pdf.
[4] Silverman, Joseph H. The Arithmetic of Elliptic Curves. Second Edition. Graduate Texts in Mathematics, 106. Springer, Dordrecht, 2009.
[5] Veerle Ledoux and Simon J.A. Malham. Introductory Schubert Calculus http://www.macs.hw.ac.uk/ simonm/schubertcalculusreview.pdf

[6] Elias M. Stein and Rami Shakarchi. Complex Analysis. Princeton University Press. 2005.
[7] Andrew Sutherland. Elliptic Curves Lecture Notes. http://ocw.mit.edu/courses/mathematics/18-783-elliptic-curves-spring-2013/lecture-notes/MIT18_783S13_lec17.pdf.