Random Variety in Projective Spaces: Polynomial Count in $\mathbb{P}^1(\mathbb{F}_q)$ and Newton Diagram in $\mathbb{P}^2(\mathbb{F}_q)$

Kevin Choi

Summer 2016

Abstract

In $\mathbb{P}^1(\mathbb{F}_q)$, we answer the question: given a random homogeneous polynomial $F(x,y)$ in $\mathbb{F}_q[x,y]$ of degree d, what is the probability that it has k distinct points in $\mathbb{P}^1(\mathbb{F}_q)$? We do so by counting the exact number of polynomials in each case. In $\mathbb{P}^2(\mathbb{F}_q)$, we switch gears to the concept of Newton polytope and Newton polygon, through which we discuss two things. One, absolute irreducibility of a polynomial via indecomposability of its Newton polytope. Two, an easy way to compute the Milnor number μ, the branching number r, the delta-invariant δ, and the (geometric) genus g via Newton polygon, and an easier way to compute the genus g via Newton polytope. These numbers matter in the context of algebraic geometric coding theory, e.g. Goppa code.

1 Introduction

How many distinct points are on $x^2y - 3xy^2 + 2y^3 = (x-y)(x-2y)y$ in $\mathbb{P}^1(\mathbb{F}_5)$? There are three: $[1:1]$, $[2:1]$, and $[1:0]$. As this example illustrates, counting points on a polynomial in $\mathbb{P}^1(\mathbb{F}_q)$ is fairly simple, because a point $[\alpha:\beta]$ corresponds to a linear factor of $F(x,y)$ such that

$$F(x,y) = (\beta_1 x - \alpha_1 y)...(\beta_k x - \alpha_k y) \cdot f(x,y) \tag{1}$$

will have $k \leq q+1 = \#\mathbb{P}^1(\mathbb{F}_q)$ distinct points, assuming $[\alpha_i : \beta_i], [\alpha_j : \beta_j]$ distinct. Hence, this is the form we start with, as every degree d polynomial having k points can be reduced to this form. Then the number of such (not necessarily monic) polynomials, denoted by $N(d,k,q)$, can be obtained via combinatorics of the linear factors and $f(x,y)$.

Since we know that the total number of degree d polynomials is $q^{\binom{d+1}{1}} - 1 = q^{d+1} - 1$, we can then divide $N(d,k,q)$ by $q^{d+1}-1$ to obtain the desired probability of a degree d polynomial having k points in $\mathbb{P}^1(\mathbb{F}_q)$. Also, what happens to the probability if we fix d and take $q \to \infty$? How about for some fixed q and $d \to \infty$? What is the expected value of k, i.e. the number of points on a random polynomial? We'll see that Euler's constant e pops up in one of the results. This concludes the first part of the paper.

In the second part, we tinker with the notion of Newton polytope and Newton polygon, a distinction of which should be made clear soon. With regards to Newton polytope, we start out by looking at the following theorem, known as the Bertini irreducibility theorem over finite fields.

Theorem 1.1 ([7]) *Let $I_n(d)$ denote the number of monic, degree d, irreducible polynomials in $\mathbb{P}^n(\mathbb{F}_q)$ with $n > 1$ and let $N_n(d)$ denote the total number of monic, degree d polynomials. Then*

$$\lim_{d\to\infty} I_n(d)/N_n(d) = 1$$

In this paper, a combinatorial analogy has been made in $\mathbb{P}^2$ to see if a randomly chosen Newton polytope corresponds to an absolutely irreducible polynomial. Then we look at both Newton polygon and polytope to easily compute the following numbers: the Milnor number μ, the branching number r, the delta-invariant δ, and the (geometric) genus g.

Definition The following terms are preliminaries to the second part of the paper.

- Given $f(x, y) = \sum a_{ij}x^iy^j$, plot the points (i, j) on the x-y plane and look at the resulting convex hull, called the *Newton polytope* of f, denoted by P_f. Note that coefficients of f do not matter at all.

- The region bounded by the lower convex hull of P_f and the x-y coordinate axes is called the *Newton polygon* of f, denoted by N_f. Note that we focus on f that is irreducible, i.e. the lower convex hull of P_f always intersects the axes.

- f is called *absolutely irreducible* if it is irreducible in the algebraic closure of the ground field, i.e. it is geometrically irreducible.

- Suppose $F(x, y, z) = z^d f(x/z, y/z)$ in $\mathbb{P}^2$ is irreducible with a singular point at $P = [0 : 0 : 1]$, i.e. $F(0, 0, 1) = \frac{\partial F}{\partial x}(0, 0, 1) = \frac{\partial F}{\partial y}(0, 0, 1) = \frac{\partial F}{\partial z}(0, 0, 1) = 0$. Since $z \neq 1$ around that point, it makes sense to look at $f(x, y)$ in the affine space. This condition might be implicit in the paper. Then the *Milnor number* is defined by

$$\mu(f) = dim\ \overline{\mathbb{F}}[[x, y]]/J_f$$

where J_f denotes the Jacobian ideal $< \frac{\partial f}{\partial x}, \frac{\partial f}{\partial y} >$ and $\overline{\mathbb{F}}[[x, y]]$ denotes the ring of formal power series with the field being the algebraic closure of $\mathbb{F}$.

- The *branching number* $r(f)$ at a singular point P on f is the number of points that P splits into in the nonsingular model of the curve, i.e. resolution of the curve, which can be obtained by a finite sequence of maps called blow ups that can desingularize the singularity. That is, there exists a map $C' \longrightarrow C$ where C is a given singular curve and C' is a smooth curve that is birationally equivalent to C. Hence, $r(f)$ is the number of points in C' that map to P in C.

- The *delta-invariant* is defined by

$$\delta(f) = dim\ \overline{\mathcal{O}}_P/\mathcal{O}_P$$

where $\mathcal{O}_P$ is the local ring at P, i.e. the set of rational functions on f that are defined at P, and $\overline{\mathcal{O}}_P$ is the integral closure of $\mathcal{O}_P$.

Remark

- The traditional notion of Newton polygon involves the lower convex hull of the points based on the coefficients of $f(x) = \sum a_ix^i$ such that each point (i, j) corresponds to $(i, ord(a_i))$. Taking the order function to be $ord(a) = v_p(a)$, one can even generalize Eisenstein's criterion [1]. Here, note that we take a slightly different notion of Newton polygon.

- In the above definitions of $\mu(f)$, $r(f)$, and $\delta(f)$, we assume that f has a singularity at the origin, i.e. the three numbers are local at the origin. Since this is the case, the three numbers can also be notated as μ_P, r_P, and δ_P, respectively.
- The Milnor formula, which describes the relationship between the three numbers, is given by
$$2\delta(f) = \mu(f) + r(f) - 1$$
Note that on a smooth point $P \in C$, $\mu_P = \delta_P = 0$ while $r_P = 1$. Also, these three numbers are invariant under local change of variables.
- There is also a type of genus called the arithmetic genus. It agrees with the geometric genus if the given degree d curve C is smooth, in which case $g = \binom{d-1}{2}$. Given singular points on C, however, the geometric genus is given by
$$g = \binom{d-1}{2} - \delta = \binom{d-1}{2} - \sum_{P \in C} \delta_P$$
while the arithmetic genus stays as $\binom{d-1}{2}$. Then from the resolution map $C' \longrightarrow C$, it can be interpreted that the geometric genus is in fact the genus of the nonsingular model C' of C, as the geometric genus is a birational invariant. We focus on the geometric genus in this paper.

Then we show that the easy method to compute these numbers involves counting the number of integral lattice points on N_f and P_f in some manner. With this, we look at various examples of singularity. Eventually, we conclude with the method's application to algebraic geometric coding theory, e.g. Goppa code.

2 Counting polynomials with k points in $\mathbb{P}^1(\mathbb{F}_q)$

Recall a concept called multichoose. Whereas $\binom{n}{k}$ is the number of ways to choose k elements out of n elements, multiplicity plays a role in multichoose, denoted $\left(\!\binom{n}{k}\!\right)$. Sometimes called the "stars and bars" problem, it gives the number of nonnegative integer solutions to the Diophantine equation:
$$x_1 + x_2 + ... + x_n = k$$
Then from the idea of stars and bars:
$$\left(\!\binom{n}{k}\!\right) = \binom{n+k-1}{k}$$

Proposition 2.1 *Given $N(d, 0, q)$ = number of degree d, not necessarily monic, polynomials that have 0 point in $\mathbb{P}^1(\mathbb{F}_q)$, we have*
$$N(d,0,q) = \begin{cases} (q-1)\sum_{i=0}^{d}(-1)^i\binom{q}{i}q^{d-i} & \text{if } d \le q \\ q^{d-q} \cdot N(q,0,q) & \text{if } d > q \end{cases}$$

Proof Recall a theorem from the concept of generating functions, where letting

- $P_n :=$ number of monic polynomials of degree n with no rational zeros

- $Q_n :=$ number of monic irreducible polynomials of degree n

the following holds true:

- $F(x) := \sum_{n=0}^{\infty} P_n x^n = \prod_{m=2}^{\infty}(1-x^m)^{-Q_m}$
- $G(x) := \sum_{n=0}^{\infty} q^n x^n = \prod_{m=1}^{\infty}(1-x^m)^{-Q_m}$

$$\begin{aligned}\therefore F(x) &= (1-x)^q G(x)\\ &= \left(1 - qx + \binom{q}{2}x^2 - \binom{q}{3}x^3 + ... + (-1)^q x^q\right)\left(1 + qx + q^2x^2 + q^3x^3 + ...\right)\end{aligned}$$

With this identity, we compare coefficients to compute P_n. ■

Theorem 2.2 *For $k \geq 1$, we have*

$$N(d,k,q) = \binom{q+1}{k}\sum_{i=k}^{d}\binom{i-1}{k-1}N(d-i,0,q)$$

Proof For some fixed k, recall the form at (1) where $F(x,y) \in \mathbb{F}_q[x,y]$ is of degree d and has k distinct points. Then the idea is quite straightforward. In order for $F(x,y)$ to have degree d, note that $f(x,y)$ must have degree $d-k$. Also, since we want exactly k roots, $f(x,y)$ should not contain points other than $[\alpha_1 : \beta_1], ..., [\alpha_k : \beta_k]$. On the flip side, it may contain $[\alpha_1 : \beta_1]$,..., or $[\alpha_k : \beta_k]$ since multiplicity of those roots does not affect the fact that $F(x,y)$ has k distinct points.

So the following are the only possible options for $f(x,y)$ when factored:

- (no linear factor) $\cdot$ (degree $d-k$ polynomial with no zero)
- (1 linear factor) $\cdot$ (degree $d-k-1$ polynomial with no zero)
- ...
- ($d-k$ linear factors) $\cdot$ (degree 0 polynomial with no zero)

Note that if $f(x,y)$ contains n linear factors, those factors need not be distinct. This is where the concept of multichoose is relevant. In other words:

$$f(x,y) = (i \text{ linear factors}) \cdot (\text{degree } d-k-i \text{ polynomial with no zero})$$

$$\implies \left(\!\!\binom{k}{i}\!\!\right) \cdot N(d-k-i,0,q) \text{ possible options}$$

Thus, the number of possible $f(x,y)$'s is given by

$$\sum_{i=0}^{d-k}\left(\!\!\binom{k}{i}\!\!\right)N(d-k-i,0,q) = \sum_{i=k}^{d}\binom{i-1}{k-1}N(d-i,0,q)$$

via re-indexing and the identity $\left(\!\binom{n}{m}\!\right) = \binom{n+m-1}{m}$. Then we need to multiply this sum by $\binom{q+1}{k}$ since we choose k distinct points on $F(x,y)$ in the first place. ■

Example

- $N(2,1,2) = 3$, and the 3 corresponding degree 2 polynomials in $\mathbb{F}_2[x,y]$ having 1 root are: $x^2, y^2, x^2 + y^2$
- $N(2,2,2) = 3$, and the corresponding polynomials are: $x^2 + xy, xy + y^2, xy$
- $N(0,0,q) = q - 1$
- $N(1,0,q) = 0$

Corollary 2.3 *Now, fix d and take $q \to \infty$. Then we have*

$$P(\textit{polynomial of deg } d \textit{ has } k \textit{ points in } \mathbb{P}^1(\mathbb{F}_q)) = \frac{1}{k!}\sum_{i=0}^{d-k}\frac{(-1)^i}{i!}$$

Proof Recall from Proposition 2.1 that $N(d,0,q)$, for large q, is given by

$$N(d,0,q) = (q-1)\sum_{i=0}^{d}(-1)^i\binom{q}{i}q^{d-i}$$

In other words, $N(d,0,q) = (\sum_{i=0}^{d}\frac{(-1)^i}{i!})q^{d+1} + o(q^{d+1})$ where $o()$ is the little-o notation. From Theorem 2.2, this implies that for general k, $N(d,k,q) = (\frac{\sum_{i=0}^{d-k}\frac{(-1)^i}{i!}}{k!})q^{d+1} + o(q^{d+1})$ so that

$$\frac{N(d,k,q)}{(\text{total number of polynomials})} = \frac{N(d,k,q)}{q^{d+1}-1} \to \frac{1}{k!}\sum_{i=0}^{d-k}\frac{(-1)^i}{i!}$$

as $q \to \infty$ ■

Remark Then taking $d \to \infty$, we have

$$P(\text{polynomial has } k \text{ points in } \mathbb{P}^1(\mathbb{F}_q)) = \frac{1}{e \cdot k!}$$

where e is Euler's constant, i.e. the base of the natural logarithm.

Corollary 2.4 *The expected value of the number of points a random polynomial of fixed degree d has in $\mathbb{P}^1(\mathbb{F}_q)$ for q big enough is given by*

$$E[\textit{number of points}] = 1$$

Proof Recall the concept of derangement, which is a permutation of elements such that no element appears in its original position in the set. Then one can define subfactorial, denoted $!n$, which gives the number of derangements given n elements. It satisfies the identity:

$$!n = n!\sum_{i=0}^{n}\frac{(-1)^i}{i!}$$

Given this, what is the probability of a permutation fixing k points? First, choose k points that would be fixed, i.e. $\binom{n}{k}$. Then the rest of the points should not be fixed by the permutation, which gives $!(n-k)$ possible number of permutations. So the desired probability is given by

$$P(\text{permutation fixes } k \text{ points}) = \binom{n}{k}\frac{!(n-k)}{n!} = \frac{!(n-k)}{k!(n-k)!}$$

Then note that the expected value of the number of fixed elements given a random permutation is in fact 1, because one can consider $X = X_1 + ... + X_n$ where

$$X_i = \begin{cases} 1 & \text{if permutation fixes i} \\ 0 & \text{otherwise} \end{cases}$$

such that $E[X] = \sum_{i=1}^n E[X_i] = \sum_{i=1}^n \frac{1}{n} = 1$. Combining this fact with the above probability, we have

$$E[\text{fixed points}] = \sum_{k=0}^{n} k \cdot \frac{!(n-k)}{k!(n-k)!} = 1$$

Going back to our problem, we use the identity to obtain

$$E[\text{number of points}] = \sum_{k=0}^{d} k \cdot \frac{1}{k!}\sum_{i=0}^{d-k}\frac{(-1)^i}{i!} = \sum_{k=0}^{d} k \cdot \frac{!(d-k)}{k!(d-k)!} = 1$$

■

So far, it's been fixing d and taking $q \to \infty$. What if we fix q and take $d \to \infty$? In this case, the proved formula in Theorem 2.2 for $k \geq 1$

$$N(d,k,q) = \binom{q+1}{k}\sum_{i=k}^{d}\binom{i-1}{k-1}N(d-i,0,q)$$

poses a problem, because the summation becomes infinite while the summand does not have a nice closed form. So we need a new approach.

Theorem 2.5 *Again, let $N(d,k,q)$ be the number of degree d polynomials, not necessarily monic, with k points in $\mathbb{P}^1(\mathbb{F}_q)$. Then assuming $d \geq q+1$, we have*

$$N(d,k,q) = \begin{cases} q^{d-q} \cdot (q-1)^{q+1-k} \cdot \binom{q+1}{k} & \textit{if } k \leq q \\ q^{d-q} - 1 & \textit{if } k = q+1 \end{cases}$$

Proof As for the first formula, note that the factor $(q-1)$ is merely a scalar factor, so it suffices to consider monic polynomials only. This means the coefficient on the highest degree of x in the coordinate system of $[x:y]$ is 1, e.g. $x^3y + 2x^2y^2$ and y are monic whereas $2y$ is not.

Then we choose k roots out of $q+1$ elements, i.e. $\binom{q+1}{k}$.

Then recall the form at (1) where in this case we want $f(x,y)$ to be monic of degree $d-k$. Like before, note that we want exactly k roots, i.e. $f(x,y) \in \mathbb{F}_q[x,y]$ such that the remaining points in $\mathbb{P}^1(\mathbb{F}_q)$, say $\gamma_1, ..., \gamma_s$, where $s = q+1-k$ are not on $f(x,y)$. With these restrictions, we compute the number of possible $f(x,y)$'s. The total number of monic, homogeneous, and degree $m = d - k$ polynomials is given by

$$\frac{q^{m+1}-1}{q-1} = q^m + q^{m-1} + ... + q + 1$$

From this, we need to subtract the number of polynomials that vanish on any of γ_1,...,γ_s.

Here, the idea is to apply the inclusion-exclusion principle. Say among the $q^m + q^{m-1} + ... + q + 1$ polynomials, we subtract those that vanish on γ_i, i.e. the number of polynomials of the form $\gamma_i(x,y)g(x,y)$ where $\gamma_i(x,y)$ represents the monic linear factor that vanishes on γ_i and $g(x,y)$ represents whichever monic, homogeneous polynomial of degree $m-1$. Since there are $\frac{q^m-1}{q-1}$ options for $g(x,y)$, there are $\frac{q^m-1}{q-1}$ options for $\gamma_i(x,y)g(x,y)$. Doing this for $i = 1, ..., s$ and subtracting the resulting sum from the total above, we get

$$\frac{q^{m+1}-1}{q-1} - \binom{s}{1}\frac{q^m-1}{q-1}$$

or equivalently

$$(q^m + q^{m-1} + ... + q + 1) - \binom{s}{1}(q^{m-1} + q^{m-2} + ... + q + 1)$$

However, note that we have subtracted those that vanish on any two of γ_1,...,γ_s twice, e.g. we have subtracted both $\gamma_1(x,y)g_1(x,y)$ and $\gamma_2(x,y)g_2(x,y)$ while $g_1(x,y)$ and $g_2(x,y)$ may vanish on γ_2 and γ_1, respectively. So we need to add the number of polynomials of the form $\gamma_i(x,y)\gamma_j(x,y)h(x,y)$, where $i \neq j$ and $h(x,y)$ represents whichever monic, homogeneous polynomial of degree $m-2$. There are $\binom{s}{2}$ ways to choose $\gamma_i(x,y)$ and $\gamma_j(x,y)$ while $\frac{q^{m-1}-1}{q-1}$ options for $h(x,y)$. Consequently, now we have

$$(q^m + q^{m-1} + ... + q + 1) - \binom{s}{1}(q^{m-1} + q^{m-2} + ... + q + 1) + \binom{s}{2}(q^{m-2} + q^{m-3} + ... + q + 1)$$

Continuing this idea of inclusion and exclusion, we ultimately have

$$\begin{aligned}
\text{number of possible } f(x,y)\text{'s} &= q^m + \left(\sum_{j=0}^{1}(-1)^j\binom{s}{j}\right)q^{m-1} + ... + \left(\sum_{j=0}^{s}(-1)^j\binom{s}{j}\right)q^{m-s} \\
&\quad + \left(\sum_{j=0}^{s}(-1)^j\binom{s}{j}\right)q^{m-s-1} + ... + \left(\sum_{j=0}^{s}(-1)^j\binom{s}{j}\right) \\
&= \sum_{i=0}^{s-1}(-1)^i\binom{s-1}{i}q^{m-i} \\
&= \sum_{i=0}^{q-k}(-1)^i\binom{q-k}{i}q^{d-k-i} \\
&= q^{d-k}\sum_{i=0}^{q-k}(-1)^i\binom{q-k}{i}(q^{-1})^i \\
&= q^{d-k}(1-q^{-1})^{q-k} \\
&= q^{d-q}(q-1)^{q-k}
\end{aligned}$$

where the following facts are used:

- $\sum_{j=0}^{i}(-1)^j\binom{s}{j} = (-1)^i\binom{s-1}{i}$ for $i \le s-1$
- $\sum_{j=0}^{s}(-1)^j\binom{s}{j} = 0$
- $s = q+1-k$ and $m = d-k$ from their definition
- $\sum_{i=0}^{n}(-1)^i\binom{n}{i}x^i = (1-x)^n$ from Taylor expansion

This proves the first formula of the theorem in the case $k \le q$. For $k = q+1$, the inclusion-exclusion principle is unnecessary since $f(x,y)$ can include or exclude any of the $q+1$ roots. In fact, $f(x,y)$ can be any monic, homogeneous polynomial of degree $d-k = d-q-1$. This yields $\frac{q^{d-q}-1}{q-1}$ possible polynomials. Multiplying this by the scalar factor $(q-1)$ then proves the formula. ■

Corollary 2.6 *Fixing q and taking $d \to \infty$, we have*

$$P(\textit{polynomial has } k \textit{ points in } \mathbb{P}^1(\mathbb{F}_q)) = \frac{(q-1)^{q+1-k}}{q^{q+1}}\binom{q+1}{k}$$

Proof

$$\lim_{d\to\infty}\frac{N(d,k,q)}{q^{d+1}-1} = \frac{(q-1)^{q+1-k}}{q^{q+1}}\binom{q+1}{k}$$

■

Corollary 2.7

- *The expected value of the number of points on a random polynomial of degree d big enough is given by*

$$E[\textit{number of points}] = \sum_{k=0}^{q+1} k\cdot\frac{(q-1)^{q+1-k}}{q^{q+1}}\binom{q+1}{k} = 1+\frac{1}{q}$$

- $$Var(X) = E[X^2]-E[X]^2 = 1-\frac{1}{q^2}$$

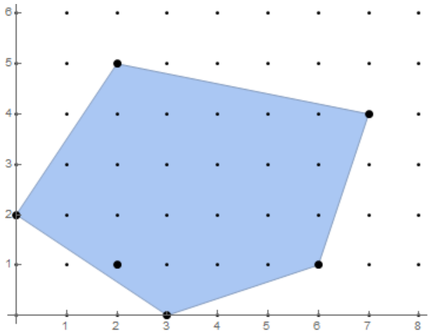
Remark Now taking $q \to \infty$ in the probability in Corollary 2.6, we have

$$P(\text{polynomial has } k \text{ points in } \mathbb{P}^1(\mathbb{F}_q)) = \frac{1}{e\cdot k!}$$

which matches up with the aforementioned case when we let $q \to \infty$ then $d \to \infty$.

3 Newton polytope and absolute irreducibility

Example We look at a solid example to solidify our notion of Newton polytope. The Newton polytope of $f(x,y) = x^3+2x^2y+3x^2y^5+4x^7y^4+5x^6y+6y^2$ is given by



Recall that the Minkowski sum of two sets is defined by $A + B = \{a + b \mid a \in A, b \in B\}$. Then the relationship between absolute irreducibility and a Newton polytope P_f of $f(x, y) = \sum a_{ij} x^i y^j$ essentially relies on the following proposition.

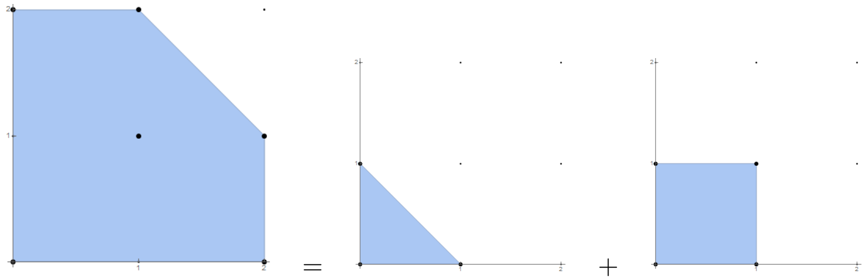
Proposition 3.1 ([1]) *Let $f(x, y) = g(x, y)h(x, y)$ where neither of g or h is trivial. Then*

$$P_f = P_g + P_h$$

In this case, we call P_f decomposable*.*

Taking the contrapositive, we see that whenever P_f is *indecomposable*, f is absolutely irreducible regardless of its coefficients. For some interesting criteria (involving cones and subsets of a cone) to check whether a given Newton polytope is indecomposable, see [1].

Example Consider $f(x, y) = 1 + x^2 + xy + x^2y + y^2 + xy^2$. This is irreducible over $\mathbb{Q}$ but factors into $f = (1 + x + y)(1 + x + y + xy)$ over $\mathbb{F}_2$. The decomposition of P_f is given by



By the nature of Minkowski sum, $P_f = P_g + P_h$ implies that ∂P_g and ∂P_h (denoting the boundaries of P_g and P_h, respectively) are shifted to form ∂P_f. Thus, a brute force algorithm can be implemented by computing all possibilities of the sum based on ∂P_f. Here, a computer program using Mathematica has been used to check whether or not a randomly chosen Newton polytope corresponds to an absolutely irreducible polynomial. The algorithm can be found in [2, Algorithm 15].

Since the focus is on $\mathbb{P}^2(\mathbb{F}_q)$, a set of points were randomly chosen in the triangular region bounded by $(0, 0)$, $(d, 0)$, and $(0, d)$ where d is the degree of the polynomial. The region had to be triangular, because we want the homogenization of $f(x, y)$ with respect to z to be a degree d polynomial. Each point was chosen with probability $\frac{q-1}{q}$, representing uniform distribution of choosing $F(x, y, z) \in \mathbb{F}_q[x, y, z]$. The data are given by

(d,q)	2	3	5	101
2	5933/4067	3805/6195	1753/8247	5/9995
3	3722/6278	1508/8492	363/9637	0/10000
4	1959/8041	498/9502	73/9927	0/10000
5	1043/8957	163/9837	11/9989	0/10000
6	570/9430	50/9950	0/100	0/100

Here, each entry means $\#_{indecomposable}/\#_{decomposable}$. In other words, both in the case of fixing d then $q \to \infty$ and the case of fixing q then $d \to \infty$, the data show less and less indecomposable randomly chosen polytopes. Hence, it can be gleaned that the Bertini irreducibility theorem for finite fields does not seem to be true in this particular setting. It makes sense, as the condition that a Newton polytope is indecomposable is in fact a stronger one. Indecomposability implies not just absolute irreducibility over one fixed ground field (in this case $\mathbb{F}_q$ for some fixed q), but that over any ground field.

On a side note, we provide the growth of the ratio irreducible-to-total as d grows, building off of [7].

Lemma 3.2 ([11]) *Let $\hat{I}_n(d)$ denote the number of monic, degree d, irreducible polynomials with $n > 1$ variables in the affine space over $\mathbb{F}_q$ and let $\hat{N}_n(d)$ denote the total number of monic, degree d polynomials with n variables. Then as d grows:*

$$1 - \frac{\hat{I}_n(d)}{\hat{N}_n(d)} \sim \frac{q^{n+1}-q}{q-1} \cdot \frac{1}{q^{\binom{n+d-1}{n-1}}}$$

Proposition 3.3

$$\hat{N}_n(d) = \frac{1}{q-1}(q^{\binom{n+d-1}{n-1}} - 1)q^{\binom{n+d-1}{n}}$$

Proof In the affine space, a polynomial of degree d need not consist of degree d monomials only, e.g. $x^3 + x + 2$ has degree 3, whereas we need at least one monomial of degree d. So there are $\frac{q^{\binom{n+d-1}{n-1}}-1}{q-1}$ homogeneous polynomials of degree d whereas $q^{\binom{n+d-1}{n}}$ polynomials, not necessarily homogeneous, of degree less than d. ■

Lemma 3.4

$$(q-1)\hat{I}_n(d) = q^{\binom{n+d}{n}} - \left(\frac{q^{n+1}-1}{q-1}\right) q^{\binom{n+d-1}{n}} + o(q^{\binom{n+d-1}{n}})$$

Proof From Lemma 3.2:

$$1 - \frac{\hat{I}_n(d)}{\hat{N}_n(d)} = \frac{q^{n+1}-q}{q-1} \cdot \frac{1}{q^{\binom{n+d-1}{n-1}}} + o(\frac{1}{q^{\binom{n+d-1}{n-1}}})$$

Now, using the formula above for $\hat{N}_n(d)$, we rearrange. ■

Theorem 3.5 *Let $I_n(d)$ denote the number of monic, degree d, irreducible polynomials in $\mathbb{P}^n(\mathbb{F}_q)$ with $n > 1$ and let $N_n(d)$ denote the total number of monic, degree d polynomials. Then as d grows:*

$$\frac{I_n(d)}{N_n(d)} \sim \frac{q^{\binom{n+d}{n}} - \left(\frac{q^{n+1}-q}{q-1}\right) q^{\binom{n+d-1}{n}}}{q^{\binom{n+d}{n}} - 1}$$

Proof Note that

$$\frac{I_n(d)}{N_n(d)} = \frac{\sum_{i=0}^{d} \hat{I}_n(i)}{\sum_{j=0}^{d} \hat{N}_n(j)} = \frac{(q-1)\sum_{i=0}^{d} \hat{I}_n(i)}{(q-1)\sum_{j=0}^{d} \hat{N}_n(j)} = \frac{(q-1)\sum_{i=0}^{d} \hat{I}_n(i)}{q^{\binom{n+d}{n}} - 1}$$

Then proceed with Lemma 3.4. ■

4 Newton polygon concerning singularity

Now, we turn to the Milnor number $\mu(f)$, the branching number $r(f)$, and the delta-invariant $\delta(f)$, given that $C = F(x,y,z)$ has a singular point at $[0:0:1]$ while $f(x,y) = F(x,y,1)$ has a singularity at the origin. The main takeaway from the definitions from the beginning of this paper is that these numbers are not easy to compute. In order to understand an easy way to compute these, we look closely at the Newton polygon of f, i.e. N_f.

Definition

- Let $\hat{N}_f \in \partial N_f$ be the upper boundary of N_f.
- $\mu(N_f) := 1 - V_1 + 2V_2$ where V_k is the k-dimensional volume of N_f's intersection with k-dimensional coordinate axes. In this case, V_1 is the length of the x-y axes that intersect with N_f and V_2 is the area of N_f. Note that $\mu(N_f)$ is sometimes called the *Newton number* of f.
- $r(N_f) := \#\{\textit{lattice points on } \hat{N}_f\} - 1$
- $\delta(N_f) := \#\{\textit{lattice points on } N_f \textit{ but not on axes}\}$
- Given an edge $\gamma \in \hat{N}_f$, f_γ is the part of f, i.e. the set of monomials $\sum c_{ij}x^i y^j$ whose points (i,j) lie on γ.
- Call f *degenerate* if there exists an edge $\gamma \in \hat{N}_f$ such that f_γ has a singular point in $(k^*)^2$ where k is an algebraically closed field. Otherwise, f is called *nondegenerate*.

Proposition 4.1 (Quasi-Milnor Formula)

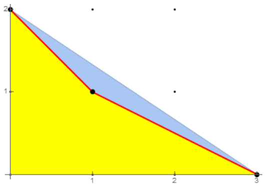
$$2\delta(N_f) = \mu(N_f) + r(N_f) - 1$$

Proof Recall Pick's theorem:

$$A = i + \frac{b}{2} - 1$$

where A is the area of the polygon on the lattice plane, i is the number of interior lattice points, and b is the number of lattice points on the polygon's boundary. Since this is the case, we rearrange the equation in terms of $\delta(N_f)$, $\mu(N_f)$, and $r(N_f)$. ■

Example Consider the polynomial $f(x,y) = x^3 + xy + y^2$.



P_f: blue, N_f: yellow, $\hat{N}_f$: red

- $\mu(N_f) = 1 - V_1 + 2V_2 = 1$
- $r(N_f) = 3 - 1 = 2$
- $\delta(N_f) = 1$

Lemma 4.2

$$r(f) = \#\{distinct\ irreducible\ factors\ of\ f \in \overline{\mathbb{F}}[[x,y]]\}$$

where r is the branching number of f and $\overline{\mathbb{F}}[[x,y]]$ is the ring of formal power series

This lemma itself does not prove the upcoming theorem, but at least provides insight into how the method of Newton polygon is related to the number of points that the singular point P splits into in the resolution of the singular curve.

Theorem 4.3 ([3], [4])

$$\mu(N_f) \leq \mu(f)$$
$$r(f) \leq r(N_f)$$

where equality holds if f is nondegenerate. It turns out that any generic curve is nondegenerate, i.e. equality holds for any generic curve.

Corollary 4.4 *If f is nondegenerate, then*

$$\delta(N_f) = \delta(f)$$

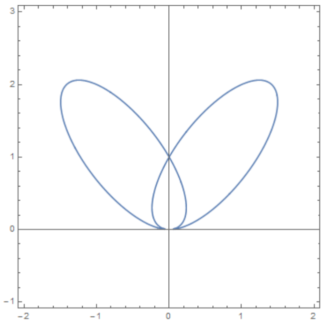
Proof If f is nondegenerate, then $\mu(N_f) = \mu(f)$ and $r(N_f) = r(f)$. The result follows from Proposition 4.1. ■

The point here is that the numbers $\mu(N_f)$, $r(N_f)$, and $\delta(N_f)$ only depend on the polygonal geometry of N_f while counting the number of points on N_f is not an expensive operation at all. As a result, we can now easily compute the Milnor number, the branching number, and the delta-invariant, as long as f is nondegenerate. The following proposition provides a quick check on whether or not f is degenerate or nondegenerate.

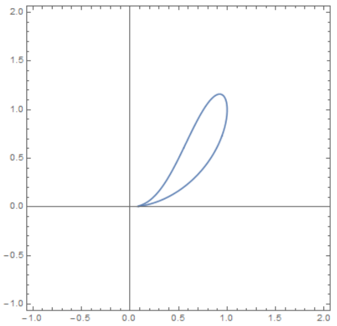
Proposition 4.5 ([5])

- *If f_γ has 2 terms only, then f is nondegenerate on γ.*
- *f_γ is degenerate iff f_γ has a multiple factor that is not a monomial.*

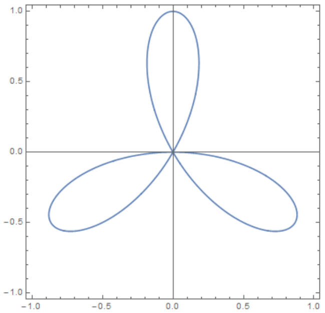
Example

- Nodal elliptic curve ($y^2 = x^3 + x^2$): $(\mu(N_f), r(N_f), \delta(N_f)) = (1, 2, 1)$
- Cuspidal elliptic curve ($y^2 = x^3$): $(\mu(N_f), r(N_f), \delta(N_f)) = (2, 1, 1)$
- 

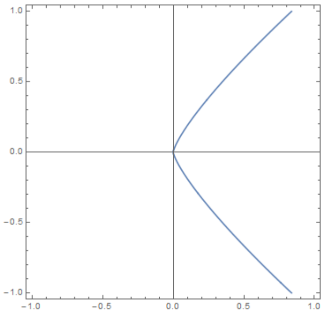
$2x^4 - 3x^2y + y^2 - 2y^3 + y^4 = 0$
$(\mu, r, \delta) = (3, 2, 2)$
Tacnode



$x^4 + x^2y^2 - 2x^2y - xy^2 + y^2 = 0$
$(\mu, r, \delta) = (4, 1, 2)$
Ramphoid cusp

- 

$(x^2+y^2)^2+3x^2y-y^3=0$
$(\mu, r, \delta)=(4,3,3)$
Rose with 3 petals



$y^6-x^3y^2-x^5=0$
$(\mu, r, \delta)=(18,3,10)$

Remark The case of ramphoid cusp above is where f is actually degenerate. Because f is degenerate, we see that a straightforward calculation yields $(\mu(N_f), r(N_f), \delta(N_f))=(3,2,2)$ which is reflective of Theorem 4.3. Then we make a change of variables that induces an automorphism of the ring $k[[x,y]]$. In this case, let $y \mapsto y+x^2$, i.e. let $h(x,y)=f(x,y+x^2)$ so that $(\mu(N_h), r(N_h), \delta(N_h))=(\mu, r, \delta)=(4,1,2)$.

5 Newton polytope, genus, and Goppa code

Once again, we look at the Newton polytope of f, i.e. P_f.

Theorem 5.1 ([9]) *Let $g(P_f)$ denote the number of interior lattice points in P_f, i.e. those inside the boundary but not on the boundary of P_f. Then*

$$g \leq g(P_f)$$

where g is the genus of the curve $C = F(x,y,z) = z^d f(x/z, y/z)$. Equality holds if f is nondegenerate while singular points of $F(x,y,z)$ are among $[1:0:0]$, $[0:1:0]$, and $[0:0:1]$. Here, nondegenerate means with respect to ∂P_f rather than with respect to $\hat{N_f}$ as in Theorem 4.3.

Example Consider $F(x,y,z)=x^5+x^3z^2+y^2z^3$, which has singular points at $P=[0:0:1]$ and $Q=[0:1:0]$.

1. Let $f(x,y)=F(x,y,1)$. Then $(\mu(N_f), r(N_f), \delta(N_f))=(2,1,1)$ while $g(P_f)=1$.
2. Let $g(x,z)=F(x,1,z)$. Then $(\mu(N_g), r(N_g), \delta(N_g))=(8,1,4)$ while $g(P_g)=1$.

Note that the geometric genus $g=\binom{d-1}{2}-\delta=6-(1+4)=1$. This example is included to show that μ_P, r_P, and δ_P are local whereas the genus g is global, in the projective sense.

So why do these numbers matter? In algebraic geometric coding theory, curves (and points in $\mathbb{P}^2(\mathbb{F}_q)$ that are on each curve) are used to generate $[n,k,d]$ error-correcting codes, otherwise known as Goppa codes. The construction of a Goppa code can be found at [8] and [10], or online.

The ratio k/n is called the transmission rate whereas the ratio d/n is called the relative distance. The interpretation is: the higher the ratio k/n, the more transmission of information that can take place whereas the higher the ratio d/n, the more errors the code can correct. In essence, the point is that we want to maximize $k/n+d/n$. Via Riemann-Roch, it can then be shown that as long as $deg(D) > 2g-2$ (where D is a chosen divisor to generate a Goppa code):

- $n \leq \#C(\mathbb{F}_q)$
- $k = deg(D) + 1 - g$
- $d \geq n - deg(D)$

where $\#C(\mathbb{F}_q)$ is the number of points on curve C. Hence, we obtain an inequality given by

$$k/n + d/n \geq 1 + 1/n - g/n$$

Since we want to maximize the left-hand side, we then want to minimize the ratio g/n, or similarly $g/\#C(\mathbb{F}_q)$.

An important remark here is that the Riemann-Roch formula involves the arithmetic genus rather than the geometric genus. Not only that, it mostly concerns curves that are smooth, although extra effort can be made to make sense of the formula with singular curves. Because this is the case, it may seem odd to consider singular curves and their corresponding geometric genus in the context of Goppa code. However, the crux is that if the curve is singular, we consider the nonsingular model of the curve. In other words, given a resolution map $C' \longrightarrow C$, we consider the arithmetic genus of C' (which is the geometric genus of C) and $\#C'(\mathbb{F}_q)$ rather than $\#C(\mathbb{F}_q)$ (which is where the branching number r is relevant). It is currently an open problem today to minimize the ratio $g/\#C(\mathbb{F}_q)$ for some given genus.

References

[1] S. Gao. *Absolute irreducibility of polynomials via Newton polytopes*, J. Algebra (2001), **501-520**, Volume 237.

[2] S. Gao and A.G.B. Lauder. *Decomposition of polytopes and polynomials*, Discrete and Computational Geometry (2001), **89-104**, Volume: 26.

[3] A.G. Kouchnirenko. *Polyedres de Newton et nombres de Milnor*, Inventiones Mathematicae (1976), **1-31**, Volume: 32.

[4] A. Ploski. *Milnor number of a plane curve and Newton polygons*, Univ. Iagel. Acta Math. (1999), **75-80**, Volume: 37.

[5] S. Brzostowski. *Degenerate singularities and their Milnor numbers*, Universitatis Iagellonicae Acta Mathematica (2015), **37-44**, Volume: 49.

[6] G. Hache and D. Le Brigand. *Effective construction of algebraic geometry codes*, IEEE Transactions on Information Theory (1995), **1615-1628**, Volume: 41.6.

[7] F. Charles and B. Poonen. *Bertini irreducibility theorems over finite fields*, Journal of the American Mathematical Society (2016), **81-94**, Volume: 29.1.

[8] J. Justesen, et al. *Construction and decoding of a class of algebraic geometry codes*, IEEE Transactions on Information Theory (1989), **811-821**, Volume: 35.4.

[9] P. Beelen and R. Pellikaan. *The Newton polygon of plane curves with many rational points*, Designs, Codes and Cryptography (2000), **41-67**, Volume: 21.1.

[10] Z.J. Dai. *Algebraic geometric coding theory*, Diss. School of Mathematics and Statistics, University of Sydney, Australia (2006), Volume: 26.

[11] A. Bodin. *Number of irreducible polynomials in several variables over finite fields*, The American Mathematical Monthly (2008), **653-660**, Volume: 115.7.