A theoretic background on Pollard's Rho algorithm

Iterations of quadratic and cubic polynomials over finite fields

An Honours thesis presented to Utrecht University
in fulfillment of the requirement for the degree of
Bachelor in Computer Science, Mathematics and Physics.

By:
Ludo Pulles

Supervised by:
dr. Damaris Schindler

Utrecht University

December 5, 2018

Acknowledgement

I would like to thank Damaris Schindler for the encouraging conversations we had during my thesis. I would like to thank my parents for their support and I would like to thank my friends for their interest in my thesis. Finally, I would like to thank Roger Heath-Brown for the nice response to some questions I had on his paper.

Contents

1 Introduction

In mathematics, the prime numbers are well known and studied numbers. Not only do primes have interesting properties, they have some important applications as well, for example in cryptography. It is known for a long time that every natural number can be expressed uniquely as a product of prime numbers up to reshuffling. However, really finding this unique representation appears to be a rather computationally difficult problem. Over the years, a lot of different methods and approaches try to tackle this problem. However, no really fast algorithm – that is, the required time is polynomial in $\log n$ – has been found.

One such algorithm for factorization is Pollard's "Rho algorithm" and in this thesis we will focus on this algorithm. In section 2 we will introduce this algorithm. We will first explain why the difficulty of prime factorization algorithms are important to cryptology in section 2.1, after which the algorithm is discussed. In section 2.4, we will explain why one can expect that the Rho algorithm runs in $\mathcal{O}(\sqrt[4]{N})$ time which is found experimentally.

We will discuss the results for the cycle length of quadratic polynomials in section 4. First, we calculate the cycle lengths for $f(X) = X^2$ and $f(X) = X^2 - 2$.

Next in section 4.3, we will prove, as is done in [OS10], the following theorem:

Theorem 1.1 ([OS10, Theorem 1])**.** *Let q be odd and $f(X) = aX^2 + bX + c \in \mathbb{F}_q[X]$ be any stable (as defined in 4.1) quadratic polynomial. Then,*

$$\mu + \lambda = \mathcal{O}(q^{3/4}), \tag{1}$$

where μ is the initial cycle length and λ the cycle length – as defined in 2.3 – of the orbit starting at $-\dfrac{b}{2a}$.

Then in section 5, we will discuss the result of Heath-Brown on general quadratic polynomials:

Theorem 1.2 ([Hea17, Theorem 1])**.** *Let $\mathbb{F}_q$ be a finite field of characteristic $p \neq 2$, and let $f(X) = aX^2 + c \in \mathbb{F}_q[X]$ with $a \neq 0$. Suppose that $f^i(0) \neq f^j(0)$ for $0 \leq i < j \leq r$. Then,*

$$\#f^r(\mathbb{F}_q) = \mu_r q + \mathcal{O}(2^{4^r}\sqrt{q}), \tag{2}$$

uniformly in a and c, where the constant μ_r is defined recursively by taking $\mu_0 = 1$ and

$$\mu_{r+1} = \mu_r - \frac{1}{2}\mu_r^2. \tag{3}$$

Moreover we have $\mu_r \sim 2/r$ as $r \to \infty$.

This result can be generalized to all quadratic polynomials of the form $f(X) = aX^2 + bX + c$ using lemma 3.2 which is proven in section 3.

In section 6.1, we will find polynomials of degree $d = 2, 3, \ldots$ which are permutations. Then, in section 6.2 we will look at the number of roots of unity of degree d in $\mathbb{F}_p$ and we show that this is equal to $\gcd(d, p-1)$. Using this

result, we work out the heuristic that we expect for any degree d polynomial, that $\#f^n(\mathbb{F}_p) \approx \kappa_n p$, where $\kappa_0 = 1$ and for $n > 0$,

$$\kappa_n = \frac{1 - (1 - \kappa_{n-1})^r}{r}, \tag{4}$$

where $r = \gcd(d, p-1)$. We will find the asymptotic behaviour of this recurrence of κ_n first for $r = 3$ in section 6.3.1 and after that we will show that in section 6.3.2 that for any $r \geq 2$,

$$\kappa_n \sim \frac{2}{n(r-1)}, \quad (\text{as } n \to \infty). \tag{5}$$

Now using this heuristic, we have found some expectation of what the image size of cubic polynomials will be. We will prove in section 7 and 8 a generalization of the work by [Hea17] to cubic polynomials:

Theorem 1.3. *Let $\mathbb{F}_q$ be a finite field of 1) order q a perfect square and $\mathrm{char}(\mathbb{F}_q) \neq 3$ or 2) characteristic $p \equiv 1 \mod 6$. And let $f(X) = aX^3 + c \in \mathbb{F}_q[X]$ with $a \neq 0$ be a cubic polynomial. Suppose that for all $0 \leq i < j < r$,*

$$f^i(0) \neq f^j(0). \tag{6}$$

Then,

$$\#f^r(\mathbb{F}_q) = \mu_r q + \mathcal{O}(3^{4^r}\sqrt{q}), \tag{7}$$

uniformly in c, where the series $(\mu_r)_{r\in\mathbb{N}}$ is given by $\mu_0 = 1$ and

$$\mu_{r+1} = \frac{1 - (1 - \mu_r)^3}{3}, \quad (\textit{for all } r \in \mathbb{N}). \tag{8}$$

Moreover we have $\mu_r \sim 1/r$ as $r \to \infty$.

We show that $p \equiv 1 \mod 6$ implies that $\mathbb{F}_{p^k}$ contains a cube root of unity in section 7.4. We will show that a finite field of order $q = t^2$ has a cube root of unity as well for fields of characteristic $p \neq 3$, in section 7.4. Note that when $\mathrm{char}(\mathbb{F}_q) = 3$, we have that $X^3 - 1 = (X-1)^3$ thus the cube root of unity is inseparable. Table 1 contains an overview of all finite fields, which have a cubic root, or which have cubic polynomials that are permutations.

The image size for finite fields of characteristic 3 is found in section 7.2.

A corollary of theorem 1.3 will be 8.18, which we will prove at the end.

Throughout the proofs of theorem 1.2 and 1.3, we might use some terminology from algebraic geometry. If the reader is not acquainted, appendix B can be used a reference for this.

1.1 Primality tests

In contrary to prime factorization, numerous efficient algorithms for determining whether a number is prime or composite have been developed.

For example, a probabilistic algorithm by Rabin determines if a number n is prime with a probability of $(1/2)^{2k}$ that n is composite but the primality test says it is prime, where k is the number of times the test is run (every run is different since a number in the test is randomly chosen). If n is prime, the primality test always gives the right result. The running time of this primality test is $k(2\log_2 n + l \cdot \log_2 n)$, where $l \in \mathbb{N}$ is chosen such that $n - 1 = 2^l m$ and m is odd. This primality test is really easy to implement [Rab80].

Miller showed in [Mil76] a deterministic variant of this primality test under the assumption of the General Riemann Hypothesis (GRH) of quadratic Dirichlet characters. Then, this primality test has a running time of at most $\mathcal{O}(\log^4 n)$. It is based on the following theorem:

Theorem 1.4 ([Sch08, Theorem. 1.1])**.** *(GRH) Let n be an odd positive integer. Let $n - 1 = 2^k m$ for some exponent $k \geq 1$ and some odd integer m. If for all $1 \leq x \leq 2\log^2 n$ one has*

$$x^m \equiv 1 \mod n, \quad \textit{or} \quad x^{2^i m} \equiv -1 \mod n \quad (\textit{for some } 0 \leq i < k), \tag{9}$$

then n is a prime number.

In 2004, Agrawal, Kayal and Saxena presented an unconditional deterministic primality test with a running time of $\mathcal{O}(\log^{7.5} n)$ times some $\log\log n$ factor [AKS04]. Lenstra and Pomerance modified this algorithm around the same time, to obtain an algorithm with a running time of $\mathcal{O}(\log^6 n)$ times the same factor [LJP02]. For more information about primality tests, one could take a look at [Pom10].

We may conclude now that, while factorizing N, we can assume that this number will be composite. Since, if we have some N, we first check if it is a prime. If it is a prime, we do not have to use the factorization algorithm anymore.

1.2 Checking for squares, cubes or higher powers

Let $N > 1$ be some number. Then, one can determine efficiently if we can write $N = n^k$ for some $k = 2, 3, \ldots$. We will explain why.

Note for $k > \log_2 N$ that we have

$$2^k > 2^{\log_2 N} = N. \tag{10}$$

Then, since $N > 1$, this would give that all $n > 1$ have $n^k \geq 2^k > N$ and thus we cannot write $N = n^k$ whenever $k > \log_2 N$.

Now fix some value for $k \in \{\, 2, 3, \ldots, \lfloor \log_2 N \rfloor \,\}$. We want to determine if there exists a value $n \in \mathbb{N}$ such that $n^k = N$ and, if it exists, we want to know this value. To solve this problem, we may find the largest value m such that $m^k \leq N$ instead. Now if we have $m^k = N$, then we know $n = m$. Else, we see that $m^k \neq N$ and since m was maximal, for all $M > m$, $M^k > N$ so no n exists.

To find this value m, we observe that $1^k \leq N$ satisfies this but might not be the largest, and $N^k \geq N^2 > N$ does not satisfy this. Furthermore, we observe

that for all $m_1 \leq m_2$ we have

$$m_2^k \leq N \implies m_1^k \leq N. \tag{11}$$

Thus, let us set the variable $l = 1$ and $r = N$. Our invariant is that $l \leq m < r$ which will hold after the iterations which we will explain now.

We iterate repeatedly the following steps until $l + 1 = r$: Let $M = \lfloor (l+r)/2 \rfloor$. If $M^k \leq N$ by maximality of m, we know that $M < m$ so we could set $l = M$ without violating the invariant. In the other case $M^k > N$ and we could set $r = M$ without violating the invariant either. In both cases, we see that the invariant still holds, but $|r - l|$ decreases by a factor of two since M is in the middle of l and r. Thus, we do at most $\log_2 N$ iterations in this loop for a value of k after which $l + 1 = r$. And now we conclude that $m = l$.

Thus, we conclude that we can check now if $N = n^k$ for some $k \geq 2$ by only performing at most $(\log_2 N)^2$ evaluations of M^k for some number M containing $\log_2 N$ bits, up to a power of $k \leq \log_2 N$.

If we want to raise a number u to a k^{th} power, then write this k as $k = 2l + 1$ or $k = 2l$ depending on its parity. In both cases, we first calculate recursively u^l, after which we multiply u^l with itself. Now if $k = 2l + 1$, then we multiply this with u to obtain u^{2l+1}. And thus, we see that we need to perform at most $2 \log_2 k$ multiplications to calculate u^k. As shown by [SS71], one can multiply B-bit numbers in $\mathcal{O}(B \log B \log \log B)$ time.

Using these two observations, we see that the running time of this method to determine if $N = n^k$ is at most:

$$(\log_2 N)^2 \cdot (2 \log_2 \log_2 N) \cdot \mathcal{O}(\log N \log \log N \log \log \log N) \leq \mathcal{O}(\log^4 N). \tag{12}$$

This is in fact faster than the primality checks covered in section 1.1. Thus, when we talk about Pollard's Rho algorithm, we may safely assume that the number N that we want to factorize, is 1) not a prime number and 2) is not a power of another number. By combining 1) and 2) we may conclude that there are at least two distinct prime factors $p \neq q$ which divide N whenever we apply the Rho algorithm.

1.3 Notational conventions

Throughout this article, we will use the following notation:

1. $\#S$ will denote the size of set S.
2. $\mathbb{N} = \{ 0, 1, 2, \dots \}$ and $\mathbb{N}_{>0} = \{ 1, 2, \dots \}$.
3. For any proposition P depending on variable(s) x,

$$[P(x)] = \begin{cases} 1, & \text{if } P(x) \text{ holds} \\ 0 & \text{otherwise.} \end{cases} \tag{13}$$

4. The identity function is denoted by $\mathrm{id}\colon x \mapsto x$.

5. For any function f, $f^0 = \mathrm{id}$ and for $n \in \mathbb{N}_{>0}$, the n^{th} iterate of f is

$$f^n = \underbrace{f \circ f \circ \ldots \circ f}_{n \text{ times}}. \tag{14}$$

6. We denote a finite field of order q as $\mathbb{F}_q$. It can be shown that $q = p^k$ where p is some prime number. The characteristic of a finite field $\mathbb{F}_{p^k}$ is $\mathrm{char}(\mathbb{F}_{p^k}) = p$.

2 Pollard's "Rho algorithm"

The Rho algorithm is an algorithm which finds a non-trivial divisor d of a composite number N. A non-trivial divisor of N is a number d, such that $d \mid N$ and $1 < d < N$. It was discussed for the first time by John Pollard in [Pol75] in 1975.

First we will explain some application of factorization algorithms to show the importance of the subject. After that we will explain how the algorithm works. Next, we will cover some special cases of polynomial functions for the algorithm. Finally, we will prove some lemma useful for limiting the number of polynomials that need to be analyzed to say something about all polynomials.

2.1 RSA: an application for factorization

These factorization algorithms are useful in cryptography where encryption methods like RSA use prime numbers in their protocol.

RSA is a public-key cryptographic system. This means that someone, say Alice, can read messages from other people securely by using RSA. For setting up RSA, Alice needs two - preferably large - distinct prime numbers $p, q \in \mathbb{N}$. After this, Alice should find two numbers $d, e \in \mathbb{Z}/\phi(n)\mathbb{Z}$ such that

$$d \cdot e \equiv 1 \mod \phi(n) \tag{15}$$

where $n = pq$ and ϕ is Euler's totient function[1]. Now (e, n) is made public and people can encode their messages with

$$E(m) = m^e \mod n \tag{16}$$

and send the ciphertext $E(m)$ to Alice, after which she can decrypt the ciphertext c by

$$D(c) = c^d \mod n \tag{17}$$

since as we will show $D(E(m)) \equiv m^{ed} \equiv m \mod n$. However, if an eavesdropper determines the factorization of n into p and q, he can compute $d \equiv e^{-1} \mod \phi(n)$ using the *Extended Euclidean algorithm*[2] and this allows the eavesdropper to decrypt as well, thus breaking the encryption [RSA78].

[1] Note that $\phi(pq) = \phi(p)\phi(q) = (p-1)(q-1)$.

[2] Knuth covers and analyses this algorithm in detail in Chapter 4.5.2 of [Knu81]

The running time of the Rho algorithm is therefore important, because this indicates the safety of certain sizes of prime numbers. If the algorithm has an extremely low upper bound on its running time, large numbers should be chosen. Therefore we want a sharp asymptotic upper bound on the running time of this algorithm.

We will conclude this section by proving that the decryption function D restores the original message.

Proposition 2.1. [*RSA78, Section VI*] *Let p, q be two distinct prime numbers and n, d, e, D, E as defined above. Then,*

$$D \circ E = \mathrm{id} = E \circ D. \tag{18}$$

Proof. Let $m \in \mathbb{Z}/n\mathbb{Z}$. Note that

$$D(E(m)) = (m^e)^d = m^{e \cdot d} = m^{d \cdot e} = (m^d)^e = E(D(m)). \tag{19}$$

The lemma is therefore proven if $m^{d \cdot e} \equiv m \mod n$.

Remember that Euler's theorem states that for $a, n \in \mathbb{N}$ such that $\gcd(a, n) = 1$, $a^{\phi}(n) \equiv 1 \mod n$.

Assume $m \not\equiv 0 \mod p$. Now $\gcd(m, p) = 1$ so $m^{p-1} \equiv 1 \mod p$. Since $d \cdot e \equiv 1 \mod \phi(n)$, there exists some $k \in \mathbb{Z}$ such that $d \cdot e = k \cdot \phi(n) + 1 = k(q-1)(p-1) + 1$. Thus,

$$m^{de} \equiv (m^{p-1})^{k(q-1)} \cdot m \equiv 1^{k(q-1)} \cdot m \equiv m \mod p. \tag{20}$$

If instead, $m \equiv 0 \mod p$, we have as well that

$$m^{de} \equiv 0 \equiv m \mod p. \tag{21}$$

Therefore, this equation holds for all $m \in \mathbb{Z}/n\mathbb{Z}$.

Similarly, for q we find the expression:

$$m^{de} \equiv m \mod q. \tag{22}$$

Now, by the Chinese Remainder Theorem, it follows that $m^{de} \equiv 1 \mod n$. □

2.2 Procedure

The Rho algorithm requires a composite number N and will produce a non-trivial divisor d of N. It has two parameters on which the running-time is dependent:

1. a start value $x_0 \in \mathbb{Z}/N\mathbb{Z}$,
2. a polynomial $f(X) \in \mathbb{Z}/N\mathbb{Z}[X]$.

Given this polynomial f and start value x_0, we let for all $i \in \mathbb{N}$

$$x_i = f^i(x_0) \mod N. \tag{23}$$

Note that there exists some prime number p such that $p \mid N$ since N is composite. Let us take a look at the directed graph which is induced by the map f.

Definition 2.2. Suppose k is some field, and $f(X) \in k[X]$. Then the graph of f is

$$\Gamma_f = (k, A_f)\,. \tag{24}$$

Here the set of vertices is k and the graph has directed edges, which we call 'arcs', mapping x to its image of f:

$$A_f = \{\, (x, f(x)) \mid x \in k \,\}\,. \tag{25}$$

It is clear that for any finite field k, the graph will contain cycles since the map

$$\begin{aligned} I\colon \quad & \mathbb{N} \to k, \\ & n \mapsto f^n(x) \end{aligned}$$

cannot be injective.

When we apply this fact on the field $\mod p$, we see that there exist indices $i, j \in \mathbb{Z}_{\geq 0}$ such that $x_i \equiv x_j \mod p$. Suppose now that for one of those possible i, j,

$$x_i \not\equiv x_j \mod N \tag{26}$$

holds. Then we have $p \mid (x_i - x_j)$. Now define $d := \gcd(x_i - x_j, N)$. Observe that $d > 1$ since $p \mid (x_i - x_j)$ and $p \mid N$ making p a common divisor so $d \geq p > 1$. Furthermore, $d < N$ since $d = N$ would imply that $N \mid (x_i - x_j)$ which is not the case. We can conclude that d is a non-trivial divisor of N.

In short, if one finds indices i, j such that $i \neq j$ and

$$1 < \gcd(x_i - x_j, N) < N, \tag{27}$$

then a non-trivial divisor is found. Finding these indices which are congruent modulo p is similar to the "Cycle detection problem".

2.3 Cycle detection

Finding a cycle can be done faster than doing it the naive way.

Naively, one would first find all the values up to some index M. And after that, one could check for all $i, j \in \{\, 0, \ldots, M \,\}$ whether $\gcd(x_i - x_j, N) > 1$. However this requires $\mathcal{O}\left(M^2\right)$ comparisons, which is far from optimal.

The Rho algorithm employs a method mentioned by Knuth in Chapter 3.1, Exercise 6 [Knu81]. Note that

$$\gcd(x_i - x_j, N) > 1 \iff \exists p \mid N \colon p \,\text{prime} \wedge x_i \equiv x_j \mod p. \tag{28}$$

Definition 2.3. Let p be a prime number. Suppose for some $\mu \in \mathbb{N}, \lambda \in \mathbb{N}_{>0}$ the values

$$x_0, x_1, \ldots, x_\mu, \ldots, x_{\mu+\lambda-1} \tag{29}$$

are distinct modulo p and $x_n \equiv x_{n+\lambda} \mod p$ for all $n \geq \mu$. Then we say, we have a cycle with an initial segment of length μ and a cycle length λ. Moreover, $x_0, x_1, \ldots, x_{\mu-1}$ is the pre-cyclic path. A cycle with an empty pre-cyclic "tail" ($\mu = 0$) is called a "pure cycle".

The name of the "Rho algorithm" comes from the visualization of the cycle. By repeatedly using $x_n \equiv x_{n+\lambda} \mod p$, we see for $n \geq \mu$ that

$$x_n \equiv x_{n+q\lambda} \mod p \quad \forall q \in \mathbb{N}. \tag{30}$$

There exists a unique index $\mu \leq i < \mu + \lambda$ such that $\lambda \mid i$. Thus we see that

$$x_{2i} \equiv x_{i+\frac{i}{\lambda}\lambda} \equiv x_i \mod p \tag{31}$$

and we can conclude that $p \mid (x_i - x_{2i})$. It can be shown that $i = \mu$ if $\lambda \mid \mu$ and else $i = \mu + \lambda - (\mu \mod \lambda) < \mu + \lambda$.

We conclude that for some N, it is enough to calculate $\gcd(x_i - x_{2i}, N)$ and check if this gives a non-trivial divisor. In the unfortunate case of $N \mid (x_i - x_{2i})$, no non-trivial divisor is obtained.

The rho algorithm has a low running time, if for some composite number N, a prime factor p exists with a small cycle (equivalently, with a small $\mu + \lambda$) for the given polynomial f. Therefore, we are interested in some analysis in the distribution of cycles over all the possible polynomials f.

2.4 A heuristic average case

We can analyze Pollard's Rho algorithm by using simple heuristics. If we assume that, for some prime number p, $f(X)$ is a uniformly distributed random mapping from $\mathbb{F}_p$ to itself, it follows from an exercise of [Knu81, p. 8] that, using the same μ and λ as in section 2.3, $\mu + \lambda$ is on average roughly:

$$\sqrt{\frac{\pi p}{8}} - \frac{1}{3} \leq 0.6267\sqrt{p}. \tag{32}$$

Since we can find a congruence modulo p in at most $\mu + \lambda$ iterations, we need on average around $\mathcal{O}(\sqrt{p})$ multiplication and gcd operations before finding a non-trivial divisor of N if $p \mid N$.

Now if p is the smallest prime dividing N, then $p^2 \leq N$.

Proof. If $p \mid N$ is the smallest prime and $p^2 > N$, then we would have $\frac{N}{p} < p$. However, $\frac{N}{p}$ could be a prime number and else it would have a smaller prime factor $r < \frac{N}{p} \leq p$. We find contradictory to our assumptions that p is not the smallest prime dividing N. Thus we conclude, $p^2 \leq N$. □

Thus, the average running time of the Pollard's Rho algorithm would be around $\mathcal{O}(N^{1/4})$ if we assume that the function f used by the algorithm is randomly chosen. As put by [Bac91],

> However, very little is known in a rigorous sense about why it works. Experience and probabilistic intuition indicate that it will remove a prime factor p from n after about $\sqrt{p}$ steps; [...] However, this running time bound has never been proved.

3 Isomorphism between conjugated polynomials

Pollard's algorithm requires some polynomial $f \in \mathbb{F}_q[X]$ and an analysis for general polynomials f is much harder than polynomials of the form

$$f(X) = X^d + c. \tag{33}$$

The latter are much easier to factorize into irreducible components than the former and thus analysis on this class of polynomials might be easier to do.

However, since a result which depends on this simple factorization would only apply to the polynomials inside that class, We will prove a lemma which provides some way to extend this result to polynomials outside that class. But first, we define when polynomials have a similar structure.

Definition 3.1. Let $f, g \in \mathbb{F}_q[X]$ be two functions. We say f and g are conjugated, iff there exists some $h \in \mathbb{F}_q$ such that

1. h is bijective,
2. $g = h^{-1} \circ f \circ h$.

In particular we say 'f is conjugated with g by h'.

From this, it naturally follows that conjugation is an equivalence relation on $\mathbb{F}_q[X]$:

1. Reflexivity: $f = \mathrm{id}^{-1} \circ f \circ \mathrm{id}$,
2. Symmetry: if f is conjugated with g by h then g is conjugated with f by h^{-1},
3. Transitivity: if 1) f_1 is conjugated with f_2 by h_1 and 2) f_2 is conjugated with f_3 by h_2, then f_1 is conjugated with f_2 by $h_1 \circ h_2$.

Lemma 3.2. *Let $f \in \mathbb{F}_q[X]$ be conjugated with $g \in \mathbb{F}_q[X]$ by h. Then for all $r \in \mathbb{N}$,*

1. *f^r is conjugated with g^r by h,*
2. *h is a bijective function from $g^r(\mathbb{F}_q)$ to $f^r(\mathbb{F}_q)$,*
3. *h is a graph isomorphism between Γ_g and Γ_f,*

where Γ_f is defined in 2.2.

Proof. We will prove the first statement by induction. The base case $r = 0$ follows quite easily:

$$g^0 = \mathrm{id} = h^{-1} \circ \mathrm{id} \circ h = h^{-1} \circ f^0 \circ h. \tag{34}$$

Now suppose f^k is conjugated with g^k by h for some $k \in \mathbb{N}$. We see that:

$$g^{k+1} = g \circ g^k = (h^{-1} \circ f \circ h) \circ (h^{-1} \circ f^k \circ h) = h^{-1} \circ f^{k+1} \circ h. \tag{35}$$

This finishes the induction argument.

To prove the second statement, suppose $x \in g^r(\mathbb{F}_q)$. Since $h \circ g^r = f^r \circ h$, then,

$$h(x) \in (h \circ g^r)(\mathbb{F}_q) = (f^r \circ h)(\mathbb{F}_q) = f^r(h(\mathbb{F}_q)). \tag{36}$$

Since h is a bijection, it is also a surjection so $h(\mathbb{F}_q) = \mathbb{F}_q$ which implies that $h(x) \in f^r(\mathbb{F}_q)$. Thus, $h(g^r(\mathbb{F}_q)) \subseteq f^r(\mathbb{F}_q)$. For the other inclusion, the argument is similar except that we have swapped the roles of f and g, and we have replaced h by h^{-1}.

To prove the third statement, we first notice that the vertices of the graph Γ_g is permuted by h to obtain the vertices of Γ_f. Suppose there is an arc $(x, g(x)) \in A_g$. Since $(h(x), f(h(x))) \in A_f$ we see that $(h(x), h(g(x))) \in A_f$ because $h \circ g = f \circ h$. Suppose there is an arc $(y, f(y)) \in A_f$. Since $(h^{-1}(y), g(h^{-1}(y))) \in A_f$ we see that $(h^{-1}(y), h^{-1}(f(y))) \in A_f$ because $h^{-1} \circ f = g \circ h^{-1}$. This shows that h is an edge-preserving bijection and therefore gives a graph isomorphism between Γ_g and Γ_f. □

Now let us take a look at simple affine transformations.

Corollary 3.3. *The function $S_b \colon \mathbb{F}_q \to \mathbb{F}_q, X \mapsto bX$ is bijective for all $0 \neq b \in \mathbb{F}_q$. Suppose $f(X) = \sum_{i=0}^{n} a_i X^i$ with $a_n \neq 0$. Then, f^r is conjugated with g^r by S_b, where*

$$g(X) = b^{-1} \sum_{i=0}^{n} a_i \, (bX)^i = \sum_{i=0}^{n} a_i b^{i-1} X^i. \tag{37}$$

In particular, if for such a f there exists some non-zero $z \in \mathbb{F}_q$ such that $z^{n-1} = a_n$ then we find that g has leading coefficient

$$a_n \, (1/z)^{n-1} = z^{n-1} z^{1-n} = 1 \tag{38}$$

when applying the transformation $S_{1/z}$ as defined in the corollary from above. Thus Γ_f is isomorphic with a monic polynomial.

When we look at quadratic polynomials, we see that every $x \in \mathbb{F}_q$ has a first root (namely x) thus for every quadratic polynomial f, Γ_f is isomorphic to some graph of a monic quadratic polynomial.

Let us look at a finite field $\mathbb{F}_q$ having $\mathrm{char}(\mathbb{F}_q) \neq 3$ and a cubic polynomial

$$f(X) = a_3 X^3 + a_2 X^2 + a_1 X + a_0, \quad a_0, a_1, a_2, a_3 \in \mathbb{F}_q \tag{39}$$

where $a_3 \neq 0$. If a_3 is a quadratic residue, Γ_f is isomorphic to a monic cubic polynomial by the argument from above. Else, suppose r is some non-quadratic residue as well. From elementary number theory we know that $a_3 r$ is a quadratic residue, thus there exists some $s \in \mathbb{F}_q$ such that $s^2 = a_3 r$. Define $t = r/s$. By using f and S_t in the lemma from above, we find that g has leading coefficient:

$$a_3 t^2 = a_3 \left(\frac{r}{s}\right)^2 = \frac{a_3 r^2}{a_3 r} = r. \tag{40}$$

Thus for every finite field $\mathbb{F}_q$ having some non-quadratic residue r, we find that every cubic polynomial having a non-quadratic residue as leading coefficient has a graph isomorphic to a cubic polynomial with leading coefficient r.

Corollary 3.4. *The function $T_c \colon \mathbb{F}_q \to \mathbb{F}_q, X \mapsto X + c$ is bijective for all $c \in \mathbb{F}_q$. Suppose $f(X) = \sum_{i=0}^{n} a_i X^i$ with $a_n \neq 0$. Then, f^r is conjugated with g^r by T_c, where*

$$g(X) = \left[\sum_{i=0}^{n} a_i (X + c)^i\right] - c = -c + \sum_{j=0}^{n} \left[\sum_{i=j}^{n} a_i \binom{i}{j} c^{i-j}\right] X^j. \tag{41}$$

In particular, the coefficient in front of X^{n-1} in $g(X)$ is equal to:

$$a_{n-1} + cn \cdot a_n. \tag{42}$$

Assuming $a_n \not\equiv 0$ and $\mathrm{char}(\mathbb{F}_q) \nmid n$, we see that T_s gives a bijection between $f^r(\mathbb{F}_q)$ and $g^r(\mathbb{F}_q)$, where

$$s = -\frac{a_{n-1}}{n a_n} \tag{43}$$

and g is a polynomial where the coefficient in front of X^{n-1} is equal to zero.

To be specific, for $n = 2$ we see that every monic quadratic polynomial of the form $f(X) = X^2 + aX + b$, has an image bijective to the image of $g(X)$ where $g(X) = X^2 + \left(b + \frac{a(2-a)}{4}\right)$ if $\mathbb{F}_q$ has odd characteristic.

Therefore, we only have to look at polynomials of the form $f(X) = X^2 + c$ to say something about the distribution of cycle lengths for all quadratic polynomials.

4 Quadratic polynomials

In this section we will investigate the cycle length for quadratic polynomials

$$f(X) = X^2 + c \tag{44}$$

in a finite field $\mathbb{F}_q$. In fact, this will establish results for all quadratic polynomials by the bijections found in section 3.

First we will examine the special cases where $f(X) = X^2$ and $f(X) = X^2 - 2$. Next, the article of [OS10] will be discussed which has an upper bound on the

cycle length which is polynomially smaller than $\mathcal{O}(q)$. After that, we will show the result from [Hea17] on all quadratic polynomials of the form $f(X) = X^2 + c$. We will provide an intuitive view on how the image size of f^n will decrease with more iterations of f.

4.1 Cycle lengths for $f(X) = X^2$

In this section, we will investigate how the function $f(X) = X^2$ will behave for the Rho algorithm.

First, we see that $f^n(X) = X^{2^n}$. It can be shown that when

1. $q = 2r + 1$,
2. q, r are odd primes,
3. 2 is a primitive root modulo r

then $m \in \mathbb{F}_q$ is part of a pure cycle of length $r - 1 = \frac{q-3}{2}$ whenever m has order r modulo q as is shown by [Hea17, p. 2].

4.2 Behaviour for $f(X) = X^2 - 2$

Now let us analyze $f(X) = X^2 - 2$. This case was mentioned by [Hea17, p. 2] to be interesting since it does not match the implications of theorem 1.2. Let $h : \mathbb{F}_q \setminus \{0\} \to \mathbb{F}_q, a \mapsto a + a^{-1}$. One can show that

$$\#h(\mathbb{F}_q \setminus \{0\}) = \frac{q+1}{2}. \tag{45}$$

Setting $m = a + a^{-1}$, we find that

$$(2a - m)^2 = m^2 - 4. \tag{46}$$

Thus, when $m^2 - 4$ is not a quadratic residue, $h^{-1}(m) = \varnothing$; when $m = \pm 2$, $a = \frac{m}{2} = \pm 1$; otherwise $m^2 - 4$ is a non-zero quadratic residue and $\#h^{-1}(m) = 2$. Let us denote the number of values for m that fall in the last category by N. We see that

$$q - 1 = \#h^{-1}(\mathbb{F}_q) = 2 + 2N. \tag{47}$$

Thus, $N = \frac{q-3}{2}$ and we find that $\#h(\mathbb{F}_q) = \frac{q-3}{2} + 2 = \frac{q+1}{2}$

These values of $h(\mathbb{F}_q)$ obey the relation

$$\begin{aligned} f(a + a^{-1}) &= (a^2) + (a^2)^{-1} \\ f^r(a + a^{-1}) &= (a^{2^r}) + (a^{2^r})^{-1}. \end{aligned} \tag{48}$$

When the first two conditions from above hold, the order of a in $\mathbb{F}_q$ is an element of $\{ 1, 2, r, 2r \}$. In the first case, $a = 1$ and $f^r(2) = 2$ for all $r \geq 0$ so 1 is a fixed point. In the second case $a = -1$ and $f(-2) = 2$, so -1 ends in a fixed point after one step.

Suppose a has order $2r$, then a^2 has order r. If for some $i < j$, $f^i(a + a^{-1}) = f^j(a + a^{-1})$, we have $a^{2^i} = a^{\pm 2^j}$ since $\#h^{-1}(a + a^{-1}) \leq 2$. Thus $2^i \equiv \pm 2^j \mod 2r$. Since $j > 0$, the right hand side is even, thus 2^i must be even so $i > 0$. Therefore, the pre-cyclic tail is non-empty and we could look at $f(a + a^{-1}) = a^2 + (a^2)^{-1}$ instead. Since a^2 has order r, we will examine this in the case below.

Therefore the case of a having order r remains. Let l be the length of the pure cycle[3]. Similarly, we have

$$2^l \equiv \pm 1 \mod r. \tag{49}$$

Therefore,

$$l = \begin{cases} \frac{1}{2}\mathrm{ord}_r(2), & 2 \mid \mathrm{ord}_r(2) \\ \mathrm{ord}_r(2), & \text{otherwise} \end{cases} \tag{50}$$

Now, if 2 is a primitive root modulo r, $\mathrm{ord}_r(2) = r - 1$ is even, so $l = \frac{r-1}{2} = \frac{q-3}{4}$. Although it is not known if there are infinite pairs of (q, r) satisfying these conditions, it is conjectured to be so. Note that the number of a having order r or $2r$ is $q - 3$. If the conjecture is true, $f(X) = X^2 - 2$ has, except a finite number of exceptions, a cycle length of $l \sim q/4$ as $q \to \infty$.

We will now show that the assumptions of 1.2 do not hold and the conclusion of this does not hold either. If the result of theorem 1.2 were to be true, then taking $r = 9$ yields, for some appropriate constant C,

$$\#f^9(\mathbb{F}_q) \leq \frac{2}{9}q + C2^{4^8}\sqrt{q} \ll q/4 - 10 \tag{51}$$

as q becomes large. On the other hand, since the cycle has a length of approximately $q/4$,

$$f^9(0), f^{10}(0), \ldots, f^{\lfloor q/4 \rfloor}(0) \tag{52}$$

have to be distinct. And now we have a contradiction, because (52) implies that $f^9(\mathbb{F}_q)$ contains at least $\lfloor q/4 \rfloor - 8$ different values. Now we conclude that the theorem cannot be true for $f(X) = X^2 - 2$. However, since the assumption does not hold, the theorem is still valid. The assumption does not hold since it can be seen that $f(2) = 2$ and thus

$$f^2(0) = f^3(0) = \cdots = f^n(0) = 2, \quad \text{for any } n \geq 2. \tag{53}$$

4.3 Critical orbit length

In this section, we will prove theorem 1.1. This theorem says something about stable polynomials, which we will define below. We will find a property about stable polynomials such that we can use Weil's bound on character sums which makes use of this property to give a bound on the cycle length.

Now we will define what we mean with stable polynomials:

[3] this is a pure cycle because it resembles the case of $f(X) = X^2$

Definition 4.1 ([JB12, Def. 2.1])**.** Let K be a field, $f(X) \in K[X]$. $f(X)$ is stable iff $f^n(X)$ is irreducible over K for all $n \in \mathbb{N}_{>0}$.

In the case of a quadratic polynomial $f(X) = aX^2 + bX + c$, we define:

Definition 4.2 ([JB12, p. 1851],[Jon07, p. 1109])**.** For K a field, $f(X) \in K[X]$ quadratic. $\gamma = -\frac{b}{2a}$ is the 'unique critical point' of f. The critical orbit is:

$$\mathrm{Orb}(f) = \{\, f^n(\gamma) \mid n \in \mathbb{N}_{\geq 2} \,\}, \tag{54}$$

and the adjusted forward orbit is:

$$\overline{\mathrm{Orb}(f)} = \{\, -f(\gamma) \,\} \cup \mathrm{Orb}(f). \tag{55}$$

We motivate the use of these two definitions, by the following property of the adjusted forward orbit generated by a stable polynomial:

Proposition 4.3 (adopted from [JB12, Prop 2.3])**.** *Let K have characteristic not equal to two. A quadratic polynomial $f \in K[x]$ is stable if $a\overline{\mathrm{Orb}(f)}$ contains no squares. In the case where K is a finite field, f is stable if and only if $a\overline{\mathrm{Orb}(f)}$ contains no squares.*

We note that we have modified the proposition in comparison to [JB12] since for $f(X) = 2X^2 + 2 \in \mathbb{F}_3[X]$, $f^2(X)$ is irreducible but $f^2(\gamma) = 1$ is a square. However, the result of [JB12] is still valid if one requires a to be a square. If a, to the contrary, is not a square, then it should state: $\overline{\mathrm{Orb}(f)}$ contains only squares.

The proposition can be proven with the use of Capelli's lemma:

Lemma 4.4 (Capelli's lemma)**.** *Let K be a field, $f(X), g(X) \in K[X]$, and let $\beta \in \overline{K}$ be any root of $g(X)$. Then $g(f(X))$ is irreducible over K if and only if both g is irreducible over K and $f(X) - \beta$ is irreducible over $K(\beta)$.*

The proof for this lemma can be found in [Tsc50, pp. 288-290]. Now we will prove the proposition:

Proof of proposition 4.3. We will use Capelli's lemma for f^{n-1} and f.

We prove the proposition by contrapositive. Let $f(X) = aX^2+bX+c \in K[X]$ be a quadratic polynomial. Suppose f is not stable. Then, let $n \in \mathbb{N}$ be the smallest such that $f^n(X) = f^{n-1}(f(X))$ is reducible. By Capelli's lemma, either $n = 1$ or both $n > 1$ and (since f^{n-1} must be irreducible) $f(X) - \beta$ is reducible in $K(\beta)$.

Case 1) $n = 1$.

If $f(X)$ is reducible in K, there exists a $r \in K$ such that $f(r) = 0$, since we have found a linear factor of $f(X)$. Then, we have

$$-af(\gamma) = \frac{1}{4}\left(b^2 - 4ac\right) = \left(\frac{2ax+b}{2}\right)^2 \tag{56}$$

which is a square so $a\overline{\mathrm{Orb}}(f)$ contains a square.

Case 2) $n > 1$ **and** $f(X) - \beta$ **is reducible in** $K(\beta)$.
Similarly, we now see that there exists a root $r \in K(\beta)$ such that $f(r) = 0$ so

$$b^2 - 4ac + 4a\beta = (2ar + b)^2 \tag{57}$$

is a square in $K(\beta)$. It is seen by induction that the leading coefficient of $f^{n-1}(X)$ is a^{d-1} with $d = \deg(f^{n-1}) = 2^{n-1}$ the degree of $f^{n-1}(X)$. Since β was a root of $f^{n-1}(X)$ which was irreducible, its minimal polynomial is the monic polynomial

$$g(X) = a^{1-d} f^{n-1}(X). \tag{58}$$

In the algebraic closure of K we have:

$$g(X) = \prod_{i=1}^{d} (X - \zeta_i), \quad \text{(for some } \zeta_1, \ldots, \zeta_d \in \overline{K}). \tag{59}$$

Let us look at the norm map which uses $g(X)$:

$$\begin{aligned} N_{K(\beta)/K} \colon K(\beta) &\to K \\ h(\beta) &\mapsto \prod_{i=1}^{d} h(\zeta_i). \end{aligned}$$

Note that this map is well-defined since the image is the same for any permutation of roots so it is inside K. From the definition we see that $N(x) = x^d$ and $N(x - \beta) = g(x)$ for all $x \in K$, thus we have:

$$\begin{aligned} N_{K(\beta)/K}\left(b^2 - 4ac + 4a\beta\right) &= \prod_{i=1}^{d} \left[b^2 - 4ac + 4a\zeta_i\right] \\ &= (-4a)^d \prod_{i=1}^{d} \left[c - \frac{b^2}{4a} - \zeta_i\right] \\ &= (-4a)^d g\left(c - \frac{b^2}{4a}\right) \\ &= (-4a)^d a^{1-d} f^n(\gamma) = a(-4)^d f^n(\gamma). \end{aligned} \tag{60}$$

It can be proven that N is a multiplicative homomorphism ($N(xy) = N(x)N(y)$). Therefore, a square $s = x^2$ in $K(\beta)$ gets mapped to $N(s) = N(x)^2$ a square in K. Using $n > 1$, d is even, so we see that $af^n(\gamma)$ is a square in K so $a\overline{\mathrm{Orb}}$ contains a square.

K **is a finite field**
What remains to be proven is that if K is finite, f is not stable if $a\overline{\mathrm{Orb}(f)}$ contains squares. In the case of $n = 1$, if $-af(\gamma)$ is a square, $f(X)$ has a solution and is thus reducible.

Suppose for some $n > 1$, for all $m < n$ that $f^m(X)$ is irreducible and $af^n(\gamma)$ is a square. Since in a finite field K, $N_{K(\beta)/K}$ maps only squares to squares, we see that $b^4 - 4ac + 4a\beta$ is a square from the above. Thus, $f(X) - \beta \in K(\beta)[X]$ has a root so it is reducible. By Capelli's lemma, now f^n is reducible. □

Now we are able to prove theorem 1.1.

Proof of theorem 1.1. Suppose q is an odd prime power, and $f(X) = aX^2 + bX + c \in \mathbb{F}_q[X]$ $(a \neq 0)$ is a stable quadratic polynomial. By proposition 4.3, we see that $a\overline{\mathrm{Orb}(f)}$ contains no squares. Let us denote the quadratic character of $\mathbb{F}_q$ by $\chi(x)$, which maps squares to 1, non-squares to -1 and $\chi(0) = 0$. Thus, for all $n \geq 2$ we have

$$\chi(af^n(\gamma)) = -1. \tag{61}$$

Let us denote the pre-cyclic path and cycle with $x_0, x_1, \ldots, x_\mu, \ldots, x_{\mu+\lambda-1}$ where all values are distinct and $x_i = f^i(\gamma)$. Fix some integer parameter $K \geq 1$. Define

$$\mathcal{T}(K) = \{\, x \in \mathbb{F}_q \mid \forall 1 \leq k \leq K : \chi(af^k(x)) = -1 \,\}. \tag{62}$$

We see for all $2 \leq n < \mu + \lambda$ that $x_n \in \mathcal{T}(K)$. Since these values are distinct, $\mu + \lambda - 2 \leq \#\mathcal{T}(K)$.

It is clear that:

$$\left[\forall 1 \leq k \leq K : \chi(af^k(x)) = -1\right] = \frac{1}{2^K} \prod_{k=1}^{K} (1 - \chi(af^k(x))). \tag{63}$$

Since, if $x \in \mathcal{T}(K)$, then $1 - \chi(af^k(x)) = 2$. If $x \notin \mathcal{T}(K)$, then there exists some $1 \leq k \leq K$ such that $\chi(af^k(x)) \neq -1$. Then, $\chi(af^k(x)) = 1$ since the irreducibility of $f^k(X)$ in $\mathbb{F}_q$ implies that $af^k(x) \neq 0$. And then, the product evaluates to zero.

Therefore,

$$\#\mathcal{T}(K) = \frac{1}{2^K} \sum_{x \in \mathbb{F}_q} \prod_{k=1}^{K} \left[1 - \chi(af^k(x))\right]. \tag{64}$$

Now we can write out the parenthesis to obtain 2^K terms. But after using multiplicity of χ, we find

$$\#\mathcal{T}(K) = \frac{1}{2^K} \sum_{S \subseteq \{\, 1, \ldots, K \,\}} \sum_{x \in \mathbb{F}_q} (-\chi(a))^{\#S} \chi\left(\prod_{k \in S} f^k(x)\right). \tag{65}$$

For the empty set, we get a term of q. For the other terms, we use Weil's bound for character sums (see [Sch06]) to estimate that:

$$\left| \sum_{x \in \mathbb{F}_q} \chi(f(x)) \right| \leq \deg(f)\sqrt{q} \tag{66}$$

for any multiplicative character χ of order m such that f is a polynomial which is not a m^{th} power of a polynomial.

In this case, χ has order 2 and clearly any product of $f^k(x)$ cannot be a square since every $f^k(X)$ are irreducible. Furthermore, for some $S \subseteq \{1, \ldots, K\}$ we see that:

$$\deg\left(\prod_{k\in S} f^k(x)\right) = \sum_{k\in S} 2^k \leq \sum_{k=1}^{K} 2^k \leq 2\cdot 2^K. \tag{67}$$

And by using this in the Weil bound, we see:

$$\left|\sum_{x\in\mathbb{F}_q} (-\chi(a))^{\#S}\chi\left(\prod_{k\in S} f^k(x)\right)\right| \leq \left|\sum_{x\in\mathbb{F}_q} \chi\left(\prod_{k\in S} f^k(x)\right)\right| \leq 2\cdot 2^K\sqrt{q}. \tag{68}$$

Thus, we find:

$$\left|\#\mathcal{T}(K) - \frac{q}{2^K}\right| \leq 2\cdot 2^K\sqrt{q}. \tag{69}$$

Now by setting $K \in \mathbb{N}$ to a value satisfying

$$2^K \leq q^{1/4} < 2\cdot 2^K \tag{70}$$

we see that:

$$\#\mathcal{T}(K) \leq \frac{q}{2^K} + 2\cdot q^{3/4} < 4\cdot q^{3/4}. \tag{71}$$

Thus, $\mu + \lambda = \mathcal{O}(q^{3/4})$. This finishes the proof of theorem 1.1. □

5 The image size of iterations of quadratic polynomial

In this section, we will investigate the proof of theorem 1.2 as given by [Hea17]. This proof will be crucial to understand before we can generalize this result to cubic polynomials as we do in section 7. Before we look at the proof, we will explain why one can expect the recurrence relation for μ_r.

First, it might be nice to look at the following example of the theorem, which is very simple to check.

Example 5.1. Consider theorem 1.2 for $r = 1$ and suppose that f is a quadratic polynomial of the form $f(X) = X^2 + c$. We can calculate $\#f(\mathbb{F}_q)$ explicitly. There are $\frac{q-1}{2}$ quadratic residues in $\mathbb{F}_q$. We see that:

$$f(\mathbb{F}_q) = \{\, y \mid \exists x \in \mathbb{F}_q \colon y - c = x^2 \,\}. \tag{72}$$

Therefore $\#f(\mathbb{F}_q) = 1 + \frac{q-1}{2} = \frac{q+1}{2}$.

5.1 Heuristic argument

A heuristic argument for this theorem can be done by using some probability theory. For $r = 0$, we obviously have the statement, because $f^0(x) = x$. This means $\#f^0(\mathbb{F}_q) = q$.

Suppose we have proven for some $s \in \mathbb{N}$ that $\#f^s(\mathbb{F}_q) \sim \mu_s q$. In order words, for some (uniformly) randomly chosen element $x \in \mathbb{F}_q$ there is a probability of μ_s that $\exists y \in \mathbb{F}_q$: $f^s(y) = x$.

Observe that $x \in f^{s+1}(\mathbb{F}_q)$ if and only if there is a $y \in f^s(\mathbb{F}_q)$ for which $f(y) = x$. The probability that some random element from $\mathbb{F}_q$ is in $f^s(\mathbb{F}_q)$ is by induction approximately μ_s. Suppose we take a random element $x \in \mathbb{F}_q$. The probability that this element is in $f^{s+1}(\mathbb{F}_q)$, is the probability that it is an element of $f(\mathbb{F}_q)$ multiplied with probability that one of the preimage elements is an element of $f^s(\mathbb{F}_q)$.

The probability that an element is in the image of f, is equal to the ratio of numbers that can be expressed as squares. From number theory, we know that $\mathbb{F}_q$ contains $(q-1)/2$ quadratic residues. This follows from the fact that the multiplicative group of $\mathbb{F}_q$ is cyclic if q is a prime power, i.e. there is an element ξ with order $q-1$ and this generates all the quadratic residues:

$$\xi^0, \xi^2, \xi^4, \ldots, \xi^{q-3}. \tag{73}$$

And every quadratic residue has precisely two roots, namely: ξ^m and $\xi^{m+\frac{q-1}{2}}$ are the roots of ξ^{2m}.

However, we have to count 0 as a square too so there are $(q+1)/2$ squares out of q elements. This gives a probability of $\frac{1}{2}(1+1/q) \sim \frac{1}{2}$.

For the second probability, we need to use that every quadratic residue, has two solutions. Suppose f is of the simple form $f(X) = aX^2 + b$. Then, $f(X) = f(-X)$ so if there exists a solution x for $y = f(x)$, then $f(-x) = y$ as well. These solutions are the same if $x = -x \Leftrightarrow x = 0$ (note $q \neq 2$). So except for the case of $x = 0$, we have exactly two solutions. Suppose we have any quadratic polynomial, $f(X) = aX^2 + bX + c$. We can rewrite this as $f(X) = a\left(X + \frac{b}{2a}\right)^2 + c - \frac{b^2}{4a}$. Because $\mathbb{F}_q$ is a field with characteristic $p \neq 2$, 2 has an inverse so the equation $f(X) = y$ has two solutions because $f(X) = g(X + \frac{b}{2a})$ where g is a quadratic polynomial of the simple form from above, if $y \neq c - \frac{b^2}{4a}$. Now we can calculate this probability, by using the inclusion-exclusion principle. Suppose we have some $x \in f^{s+1}(\mathbb{F}_q)$ having two solutions y for $f(y) = x$. The probability that one of those solutions y is in $f^s(\mathbb{F}_q)$ is equal to $2\mu_s - \mu_s^2$.

So, the probability that a randomly chosen $x \in \mathbb{F}_q$ is in $f^{s+1}(\mathbb{F}_q)$, is approximately:

$$q\,\frac{1}{2} \cdot (2\mu_s - \mu_s^2) = \left(\mu_s - \frac{1}{2}\mu_s^2\right) q = \mu_{s+1} q. \tag{74}$$

However, this argument uses that there is a 'probability' distributed in a uniform way. This cannot be proven in an easy way. That is why the article uses a different way to prove the result.

5.2 Expressing the image size in terms of the k^{th} moments

In the next sections we will prove theorem 1.2.

First we define the following:

Definition 5.2. The k^{th} moment, $N(r;k)$, is defined as:

$$N(r;k) = \sum_{m \in \mathbb{F}_q} \rho_r(m)^k \quad (r = 0, 1, \dots, k = 1, 2, \dots) \tag{75}$$

where

$$\rho_r(m) = \#\{\, x \in \mathbb{F}_q \mid f^r(x) = m \,\}. \tag{76}$$

We can find an expression for $\#f^r(\mathbb{F}_q)$ in terms of the k^{th} moments. First, observe that

$$\begin{aligned} \#f^r(\mathbb{F}_q) &= q - \#\{\, m \in \mathbb{F}_q \mid \forall x \in \mathbb{F}_q : f^r(x) \neq m \,\} \\ &= q - \#\{\, m \in \mathbb{F}_q \mid \rho_r(m) = 0 \,\}. \end{aligned} \tag{77}$$

We let $D = D(r) = \deg(f^r)$ be the degree of f^r. Currently, f is quadratic so $D = 2^r$. For a cubic polynomial f, we have instead $D = 3^r$. Since f^r has at most D solutions in $\mathbb{F}_q$ we have the bound $0 \leq \rho_r(m) \leq D$.

We will define coefficients $C_{r,k}$ as the coefficients of the polynomial[4]

$$G_r(T) := \frac{1}{D!} \prod_{j=1}^{D} (j - T) = \sum_{k=0}^{D} C_{r,k} T^k. \tag{78}$$

Because of the bounds on $\rho_r(m)$ we see that

$$G_r(\rho_r(m)) = [\rho_r(m) = 0] \tag{79}$$

since $G_r(0) = D!/D! = 1$, and for $1 \leq i \leq D$, $G_r(i) = 0$.

Using this, we then have

$$\#f^r(\mathbb{F}_q) = q - \sum_{m \in \mathbb{F}_q} [\rho_r(m) = 0] = q - \sum_{m \in \mathbb{F}_q} \sum_{k=0}^{D} C_{r,k} \rho_r(m)^k \tag{80}$$

$$= q - \sum_{k=0}^{D} C_{r,k} N(r;k). \tag{81}$$

As done in the article, an estimate on $N(r;k)$ is obtained to yield an estimate for $\#f^r(\mathbb{F}_q)$.

5.3 Coefficients

Even though the article does not go into detail about $C_{r,k}$, these numbers are well known in fact. We can express $C_{r,k}$ in the signed Stirling numbers of the

[4]Note that [Hea17, p. 20] defines $G_r(T)$ as well but this is slightly different up to absolute value over $C_{r,k}$

first kind, $s(n,k)$. These numbers $s(n,k)$ are defined as the coefficients of the polynomial

$$\prod_{i=0}^{n-1}(x-i) = \sum_{k=0}^{n} s(n,k)\, x^k. \tag{82}$$

Furthermore, the unsigned Stirling numbers of the first kind are $\left[{n \atop k}\right]$, where these are the coefficients of the polynomial

$$\prod_{i=0}^{n-1}(x+i) = \sum_{k=0}^{n} \left[{n \atop k}\right] x^k. \tag{83}$$

The relation between the two, can be found filling in $-x$ into one of the two, by which we find that

$$s(n,k) = (-1)^{n-k}\left[{n \atop k}\right]. \tag{84}$$

Now we see that

$$\prod_{j=1}^{D}(j-T) = (-1)^D T^{-1} \prod_{j=0}^{D}(T-j) = (-1)^D \sum_{k=0}^{D+1} s(D+1,k)\, T^{k-1}. \tag{85}$$

Since $s(n,0) = 0$, we can substitute k by $k+1$ to obtain:

$$G_r(T) = \frac{(-1)^D}{D!} \sum_{k=0}^{D} s(D+1,k+1)\, T^k. \tag{86}$$

Thus,

$$C_{r,k} = \frac{(-1)^D}{D!} s(D+1,k+1). \tag{87}$$

By taking absolute values, we see that

$$\sum_{k=0}^{D} |C_{r,k}|\, T^k = \frac{1}{D!} \sum_{k=0}^{D} \left[{D+1 \atop k+1}\right] T^k = \frac{1}{D!}(T+1)(T+2)\ldots(T+D). \tag{88}$$

Assume now that $3 \le D \le T$. Then we find the estimate

$$\sum_{k=0}^{D} |C_{r,k}|\, T^k \le \frac{(T+1)(T+D)}{D} \prod_{i=2}^{D-1} \frac{T+i}{i}. \tag{89}$$

Each numerator in the product is smaller than $T+D \le 2T$. Also the first term is smaller than

$$\frac{T^2+(D+1)T+1}{D} \le \frac{1}{3}(T^2+4T+1) \le \frac{T^2}{3} + \frac{4T^2}{9} + \frac{T^2}{27} \le \frac{22}{27}T^2 < T^2. \tag{90}$$

We can use this to find

$$\sum_{k=0}^{D} |C_{r,k}|\, T^k \le T^2 \prod_{i=2}^{D-1} \frac{2T}{i} < T^D. \tag{91}$$

We will use this estimate at the end of this proof.

5.4 Number of solutions

The quantity $N(r;k)$ is equal to the number of solutions of

$$f^r(x_1) = f^r(x_2) = \cdots = f^r(x_k). \tag{92}$$

And these equations define an (algebraic) curve over $\mathbb{F}_q$, an object which is studied in algebraic geometry. A curve is a set of points which are the zeros of $k-1$ polynomials.

For estimating the number of solutions, Heath-Brown used the Hasse-Weil bound[5] which gives an estimate for the number of solutions for an absolutely irreducible curve. An irreducible curve, is a curve which cannot be written as the intersection of two non-empty curves, or equivalently in the case of 1 polynomial f, that f is irreducible (since in particular $\mathbb{F}_q$ is a domain). A curve C over K is absolutely irreducible if and only if C is irreducible over $\overline{K}$, the algebraic closure of K.

However to use the Hasse-Weil bound from section B.3, equation (92) must be an absolutely irreducible curve or else it must be split into absolutely irreducible curves.

If the polynomials defining this curve are not irreducible, the curve is not irreducible as well. And this exactly the case for quadratic polynomials of the form $f(X) = X^2 + c$ where we have

$$\begin{aligned} f^r(X) - f^r(Y) &= \left(f^{r-1}(X)\right)^2 + c - \left[\left(f^{r-1}(Y)^2\right) + c\right] \\ &= \left(f^{r-1}(X) - f^{r-1}(Y)\right)\left(f^{r-1}(X) + f^{r-1}(Y)\right). \end{aligned} \tag{93}$$

Heath-Brown finds by induction that

$$f^r(X) - f^r(Y) = (X-Y)\prod_{j=0}^{r-1}\left(f^j(X) + f^j(Y)\right). \tag{94}$$

Since $X - Y = 0$ is of degree 1 it is obvious that this curve is absolutely irreducible. For the remaining $f^j(X) + f^j(Y) = 0$, it remains to be seen. However, Heath-Brown proves that $f^j(X) + f^j(Y)$ is irreducible over $\overline{\mathbb{F}_q}$ when the assumptions of theorem 1 hold. Thus, for the case of $k = 2$, we find that $f^r(X) = f^r(Y)$ has $r+1$ irreducible factors.

For the general case of $k \geq 1$, Heath-Brown builds – for some solution $x_1, \ldots, x_k$ of (92) – a complete graph G[6], with vertices $V = \{1, 2, \ldots, k\}$ and defines the weight $d = d(i,j)$ for $i, j \in V$ as the smallest value for which $\phi(x_i, x_j; d) = 0$ holds, where

$$\phi(X, Y; d) = \begin{cases} X - Y, & d = -1 \\ f^d(X) + f^d(Y), & d \geq 0 \end{cases} \tag{95}$$

[5] For more information about this hypothesis, we refer to [Sch06] or B.3

[6] A graph G is complete iff for all vertices $i, j \in V$ there is an edge $(i,j) \in E$ between them.

And the corresponding homogeneous equations are:

$$\Phi(X,Y,Z;d) = \begin{cases} X-Y, & d=-1 \\ Z^{2^d}\phi(X/Z,Y/Z;d), & d\geq 0 \end{cases} \tag{96}$$

By only limiting d to be the smallest value, it is shown that all graphs built from solutions have a rather simple structure in terms of the edges of graph. Heath-Brown arrives at lemma 6 to show that the curve $\mathcal{C}$ given by

$$\mathcal{C}\colon\ \Phi(X_i,X_{i+1},X_0;d_i)=0, \quad (1\leq i<k) \tag{97}$$

is absolutely irreducible with degree at most $2^{(k-1)(r-1)}$.

However, when we look at all solutions, each of them is part of a graph and thus of a curve $\mathcal{C}$ but the number of curves can be rather large.

5.5 Using the Hasse-Weil bound to bound the number of solutions

In this section we will use (427) to get a bound on the number of solutions of the curves $\mathcal{C}$ we have encountered. In this bound, the genus is used. We will not tell what this is, but we will use a bound on the genus.

The Castelnuovo genus bound [Cas89] states for a curve $\mathcal{C}$ with degree D in $\mathbb{P}^k$ $(k\geq 2)$ that

$$g \leq (k-1)\frac{m(m-1)}{2} + m\epsilon \tag{98}$$

where

$$D-1 = m(k-1)+\epsilon, \quad 0\leq\epsilon<k-1. \tag{99}$$

It is obvious that $m = \left\lfloor \frac{D-1}{k-1} \right\rfloor \leq D-1$, by which we find

$$\begin{aligned} g &\leq \frac{m}{2}\left[m(k-1)-(k-1)+2\epsilon\right] \\ &= \frac{m}{2}\left[(D-1)-(k-1-\epsilon)\right] \\ &\leq \frac{m}{2}\left[D-2\right] \\ &\leq \frac{(D-1)(D-2)}{2}. \end{aligned} \tag{100}$$

By plugging (100) into (427) and using $D\leq 2^{rk}$, we find that:

$$|\#\mathcal{C}(\mathbb{F}_q)-(q+1)| \leq 4^{kr}\sqrt{q}. \tag{101}$$

Now observe that

$$N(r;k) = \#\left[\bigcup_{\mathcal{C}}\mathcal{C}\right](\mathbb{F}_q). \tag{102}$$

and by the inclusion-exclusion principle we can estimate this by

$$\sum_{\mathcal{C}} \#\mathcal{C}(\mathbb{F}_q) - \frac{1}{2} \sum_{\mathcal{C}_1 \neq \mathcal{C}_2} \#(\mathcal{C}_1 \cap C_2)(\mathbb{F}_q) \leq N(r;k) \leq \sum_{\mathcal{C}} \#\mathcal{C}(\mathbb{F}_q). \tag{103}$$

Bézout's theorem (see [Har77, I, Theorem 7.7]) states that $\#(\mathcal{C}_1 \cap \mathcal{C}_2)(\mathbb{F}_q) \leq \deg(C_1)\deg(C_2)$, thus in our case, $\#(\mathcal{C}_1 \cap \mathcal{C}_2)(\mathbb{F}_q) \leq 4^{kr}$.

Let $\mathcal{N}(r;k)$ be the number of curves $\mathcal{C}$. Then we find

$$\left| N(r;k) - \sum_{\mathcal{C}} \#\mathcal{C}(\mathbb{F}_q) \right| \leq \frac{1}{2}\mathcal{N}(r;k)^2 4^{kr}. \tag{104}$$

By using the triangle inequality on (101) and (104), we find that:

$$|N(r;k) - \mathcal{N}(r;k)(q+1)| \leq 4^{kr}\mathcal{N}(r;k)\left[\frac{1}{2}\mathcal{N}(r;k) + \sqrt{q}\right]. \tag{105}$$

5.6 Estimate on the number of curves

By having an upper bound on $\mathcal{N}(r;k)$ expressed in r and k makes this expression easier to analyze. We use the result of Heath-Brown for this to find a better upper bound on $\mathcal{N}(r;k)$ than the 'crude bound' Heath-Brown proposed in equation (11) of [Hea17].

Heath-Brown uses arguments from the graph representation of the curve that

$$\mathcal{N}(r;k) = \frac{1}{2}\sum_{a=0}^{k} \binom{k}{a} \mathcal{N}(r-1;a)\,\mathcal{N}(r-1;k-a), \quad (r,k \geq 1) \tag{106}$$

and $\mathcal{N}(r;0) = 1$ for $r \geq 0$. Heath-Brown finds an absolutely convergent power-series

$$E(X;r) := \sum_{k=0}^{\infty} \frac{\mathcal{N}(r;k)}{k!} X^k \tag{107}$$

for $|X| < (r+1)^{-1}$ which satisfies the recurrence

$$E(X;r) = \frac{1 + E(X;r-1)^2}{2}. \tag{108}$$

Since $\mathcal{N}(0;k) = 1$ for all $k \geq 0$ we find $E(X;0) = \exp(X)$ and by induction, there exist non-negative **rational** coefficients $\nu(r;m)$ summing to 1 such that:

$$E(X;r) = \sum_{m=0}^{2^r} \nu(r;m) e^{mX}. \tag{109}$$

Using the power series for the exponential function and using absolute convergence, we rearrange the terms such that:

$$E(X;r) = \sum_{k=0}^{\infty} \left(\sum_{m=0}^{2^r} \nu(r;m) m^k \right) \frac{X^k}{k!} \tag{110}$$

yielding

$$\mathcal{N}(r;k) = \sum_{m=0}^{2^r} \nu(r;m)\, m^k. \tag{111}$$

Therefore we find as an estimate for $\mathcal{N}(r;k)$:

$$\mathcal{N}(r;k) \leq 2^{rk} \sum_{m=0}^{2^r} \nu(r;m) = 2^{rk}. \tag{112}$$

By plugging this into equation (105) we obtain

$$|N(r;k) - \mathcal{N}(r;k)(q+1)| \leq 8^{kr} \left[2^{kr-1} + \sqrt{q}\right]. \tag{113}$$

Since both $2^{kr-1} > 1$ and $\sqrt{q} > 1$, $2^{kr-1} + \sqrt{q} \leq 2^{kr}\sqrt{q}$, finding:

$$|N(r;k) - \mathcal{N}(r;k)(q+1)| \leq 16^{kr}\sqrt{q}. \tag{114}$$

We notice that by writing out the first functions $E(X;r)$ that this estimate of $\mathcal{N}(r;k)$ might be improved since the distribution of 1 over $\nu(r;m)$ is mainly found in small values of m:

1. $E(X;0) = \exp(X)$
2. $2\,E(X;1) = 1 + \exp(2X)$
3. $8\,E(X;2) = 5 + 2\exp(2X) + \exp(4X)$
4. $128\,E(X;3) = 89 + 20\exp(2X) + 14\exp(4X) + 4\exp(6X) + \exp(8X)$
5. ...

5.7 Estimate on $G_r(T)$

The recurrence relation in (108) implies for $\nu(r;0)$ that

$$\nu(r;0) = \frac{1 + \nu(r-1;0)^2}{2}. \tag{115}$$

Now we define $\mu_r = 1 - \nu(r;0)$. We see that $\nu(0;0) = 0 = 1 - \mu_0$ and $1 - \nu(r;0) = \mu_r$ satisfies the recurrence relation from theorem 1:

$$\begin{aligned}
\mu_r &= 1 - \nu(r;0) \\
&= \frac{1 - \nu(r-1;0)^2}{2} \\
&= (1 - \nu(r-1;0)) - \frac{(1 - \nu(r-1;0))^2}{2} \\
&= \mu_{r-1} - \frac{\mu_{r-1}^2}{2}.
\end{aligned}$$

Bringing it all together, we find that:

$$\#f^r(\mathbb{F}_{\text{ıı}}) - \mu_r q = (1-\mu_r)q - \sum_{k=0}^{D} C_{r,k} N(r;k). \tag{116}$$

By using equation (111) and (79), we find that

$$\sum_{k=0}^{2^r} C_{r,k} \mathcal{N}(r;k) = \sum_{m=0}^{2^r} \nu(r;m)\, G_r(m) = \nu(r;0). \tag{117}$$

We can use this and the rough estimate of (114) in (116) to find with the triangle inequality that

$$\begin{aligned} |\#f^r(\mathbb{F}_q) - \mu_r q| &= \left| \left(\sum_{k=0}^{2^r} C_{r,k} N(r;k) \right) - \nu(r;0)\, q \right| \\ &\leq \sqrt{q} \sum_{k=0}^{2^r} |C_{r,k}|\, 16^{kr} + \left| (q+1)\nu(r;0) - \nu(r;0)\, q \right| \\ &\leq 1 + \sqrt{q} \sum_{k=0}^{2^r} |C_{r,k}|\, (16^r)^k. \end{aligned} \tag{118}$$

Since $3 \leq 2^r \leq 16^r$, we may now use (91) to find that

$$|\#f^r(\mathbb{F}_q) - \mu_r q| \leq 2^{4r2^r} \sqrt{q}. \tag{119}$$

For all $r \geq 4$, $4r \leq 2^r$ so

$$|\#f^r(\mathbb{F}_q) - \mu_r q| \leq \sqrt{q}\, 2^{4^r}. \tag{120}$$

This proves theorem 1. □

6 Higher degree polynomials

In this section we will analyze polynomials $f(X)$ with degree $n \geq 3$.

6.1 Polynomial permutations

We will show that for any $d \geq 3$, we can find a polynomial function of degree d such that this function is bijective for some prime number p, or alternatively it permutes all the elements of $\mathbb{F}_p$.

Suppose p is a prime number, and $d \in \mathbb{N}$ such that $\gcd(d, p-1) = 1$. Then, there exist $u, v \in \mathbb{Z}$ such that

$$ud + v(p-1) = 1 \tag{121}$$

which is called Bézout's identity.

We construct the function

$$f(X) = X^d + c \tag{122}$$

which is bijective since the inverse function is:

$$f^{-1}(Y) = (Y - c)^u. \tag{123}$$

It can be checked by noticing that for $0 \neq x \in \mathbb{F}_p$:

$$\begin{aligned} f^{-1}(f(x)) &= x^{ud} \\ &= x^{1-v(p-1)} \\ &= x\left(x^{p-1}\right)^{-v} \\ &= x. \end{aligned} \tag{124}$$

Here we have used Fermat's theorem stating $x^{p-1} \equiv 1 \mod p$ whenever $x \not\equiv 0$. Furthermore, for $x = 0$

$$f^{-1}(f(0)) = f^{-1}(c) = 0. \tag{125}$$

Thus we see that f^r is a bijection for any $r \in \mathbb{N}$ as well. This means that we have found a set of functions of degree d that will not have an image that decreases by the number of iterations. Therefore, we will not expect to find a similar statement as theorem 1.2 over every polynomial of degree d. Rather we will have to restrict ourselves to some class of polynomials not containing permutations.

Note that for the quadratic polynomials ($d = 2$), the assumption never holds for $p \geq 3$ since we have $\gcd(2, p-1) = 2$. Furthermore, for a finite field with characteristic $p \neq 2$ and $f(X) = aX^2 + bX + c$, we see that for any $X \in \mathbb{F}_q$,

$$f(X) = f\left(-X - \frac{b}{a}\right). \tag{126}$$

Thus, by choosing $X \neq -\frac{b}{2a}$, this shows that f is not injective.

6.2 Polynomials of the form $f(X) = X^d + c$

Assume that $p \in \mathbb{N}$ is a prime number and $d \in \mathbb{N}$.

We will first prove the following lemma to find an expression for the image size of the function $f(X) = X^d + c$.

Lemma 6.1. *Let p be a prime, $d \in \mathbb{N}$ and $x \in \mathbb{F}_p^\times$. Then there exist $\gcd(d, p-1)$ different residue classes in $\mathbb{F}_p$ such that $x^d \equiv 1$.*

Proof. Let us denote $r := \gcd(d, p-1)$. Now, we know there will exist $u, v \in \mathbb{Z}$ such that

$$ud + v(p-1) = r. \tag{127}$$

Let $x \in \mathbb{F}_p$ be a residue class such that $x^d \equiv 1$. Furthermore, as shown before, $\mathbb{F}_p^\times$ is a cyclic group, so let ξ be a generator of this group. There exists some $0 \leq k < p-1$ such that $\xi^k \equiv x$. Thus,

$$\xi^{kd} \equiv 1 \equiv \xi^0. \tag{128}$$

Since ξ has order $p-1$, we have $kd \equiv 0 \mod (p-1)$. Thus, there exists some $t \in \mathbb{Z}$ such that $kd = t(p-1)$. Combining this with (127), we find:

$$\begin{cases} ukd = k\left(r - v(p-1)\right) = kr - kv(p-1) \\ ukd = ut(p-1) \end{cases} \tag{129}$$

Now this gives:

$$k = (kv + ut)\,\frac{p-1}{r}. \tag{130}$$

Since $r \mid (p-1)$ we see that $\frac{p-1}{r}$ is a natural number and divides k. Since $0 \leq k < p-1$ we see that there are at most r options for k.

Furthermore, for every option $k = i\frac{p-1}{r}$ where $0 \leq i < r$, we see because $\frac{d}{r} \in \mathbb{N}$ that

$$\xi^{kd} \equiv \left(\xi^{p-1}\right)^{i\frac{d}{r}} \equiv 1. \tag{131}$$

Thus the elements satisfying $x^d \equiv 1$ are:

$$\xi^0,\, \xi^{(p-1)/r},\, \ldots,\, \xi^{(r-1)(p-1)/r}. \tag{132}$$

□

Now, let $f(X) = X^d + c$, $r = \gcd(d, p-1)$ and suppose that $f(x) \equiv f(y) \mod p$ for some $x, y \in \mathbb{F}_p$ both non-zero. Then we have $x^d \equiv y^d$, thus

$$\left(\frac{x}{y}\right)^d \equiv 1. \tag{133}$$

By the lemma from above, we see that based on the value of x, we could have r different values for y. Furthermore, $f(x) \not\equiv c \equiv f(0)$ for all $x \in \mathbb{F}_p$ non-zero. Therefore, $\#f^{-1}(c) = 1$ and $\#f^{-1}(x)$ is either r or 0. Since

$$\sum_{x \in \mathbb{F}_p} \#f^{-1}(x) = \#\mathbb{F}_p = p \tag{134}$$

we see for $r > 1$ that for $\frac{p-1}{r}$ values of x, $\#f^{-1}(x) = r$ holds.

6.3 Generalized heuristic argument

Let us now generalize the heuristic argument of section 5.1 to a recurrence relation for the polynomial $f(X) = X^d + c$. Suppose $r = \gcd(d, p-1) > 1$.

Now we will assume that function f behaves like a random map, in the following way: Let $n \in \mathbb{N}$ and $x \in \mathbb{F}_p$. Then the probability to find x in the image of f^n is equal to:

$$\mathbb{P}(x \in f^n(\mathbb{F}_p)) = \frac{\#f^n(\mathbb{F}_p)}{p} \leq 1. \tag{135}$$

We will find a recurrence relation for $(\kappa_n)_{n\in\mathbb{N}}$ such that

$$\#f^n(\mathbb{F}_p) \approx \kappa_n p \tag{136}$$

by induction on n. If $n = 0$, $\#f^n(\mathbb{F}_p) = p$ so we find

$$\kappa_0 = 1. \tag{137}$$

Now let $n \geq 0$ and suppose that $\#f^n(\mathbb{F}_p) = \kappa_n p$. The probability that $c \in f^{n+1}$ is equal to

$$\frac{\#f^n(\mathbb{F}_p)}{p} = \kappa_n. \tag{138}$$

Since only 0 has c as its image. Let $x \in \mathbb{F}_p$ such that $x \not\equiv c$. The preimage has size either 0 or r. As shown above, $\frac{p-1}{r}$ of the elements is part of the latter. Thus the probability that $x \in f(\mathbb{F}_p)$ is equal to $\frac{1}{r}$. Else $x \notin f^{n+1}(\mathbb{F}_p)$, so assume that x is in the image of f. Now we know there must exist some $y \in \mathbb{F}_p$ such that $f(y) = x$. Since there are r possible values for y, call these values $y_1, \ldots, y_r$. Observe that

$$\mathbb{P}(x \in f^{n+1}(\mathbb{F}_p)) = \mathbb{P}(y_1 \in f^n(\mathbb{F}_p) \vee \ldots \vee y_r \in f^n(\mathbb{F}_p)). \tag{139}$$

Therefore we find

$$1 - \mathbb{P}(x \in f^{n+1}(\mathbb{F}_p)) = \mathbb{P}(y_1 \notin f^n(\mathbb{F}_p) \wedge \ldots \wedge y_r \notin f^n(\mathbb{F}_p)). \tag{140}$$

Now since we assume that the probabilities are uniformly random, the probability of y_1 being in the image of f^n is the same as for any y_i, so

$$1 - \mathbb{P}(x \in f^{n+1}(\mathbb{F}_p)) = \mathbb{P}(y_1 \notin f^n(\mathbb{F}_p))^r = (1 - \kappa_n)^r. \tag{141}$$

We can conclude that inductively,

$$\#f^{n+1}(\mathbb{F}_p) = \kappa_n + \frac{p-1}{r}\left(1 - (1 - \kappa_n)^r\right). \tag{142}$$

Since p will be large in general, and $\kappa_n \leq 1$ we can approximate this as:

$$\#f^{n+1}(\mathbb{F}_p) \approx \frac{p}{r}\left(1 - (1 - \kappa_n)^r\right). \tag{143}$$

Thus, we define

$$\kappa_{n+1} := \frac{1 - (1 - \kappa_n)^r}{r} \tag{144}$$

for $n \in \mathbb{N}$ and $\kappa_0 = 1$. We see that the heuristic gives

$$\#f^n(\mathbb{F}_p) \approx \kappa_n p, \quad \text{(for all } n \in \mathbb{N}). \tag{145}$$

Note that $\kappa_1 = 1/r$.

In the remaining of this section, we will prove the following proposition:

Proposition 6.2. *Let $r \geq 2$, $\kappa_0 = 1$ and κ_n defined by (144). Then, for all $n \geq 1$,*

$$n + 1 < \tau_n < n + 4 + \ln(n), \tag{146}$$

where we let

$$\tau_n = \frac{2}{\kappa_n(r-1)}. \tag{147}$$

An immediate result of this, with use of the squeeze theorem, is

Corollary 6.3. *Let $r \geq 2$. The asymptotic behaviour of τ_n and κ_n as $n \to \infty$ is*

$$\lim_{n\to\infty} \frac{\tau_n}{n} = 1. \tag{148}$$

and

$$\kappa_n \sim \frac{2}{n(r-1)}, \quad \text{as } n \to \infty. \tag{149}$$

However, let us first take a step back. We want to point out that [Hea17] covers $r = 2$, since the quadratic case was analyzed. Thus in that case $r = d = 2$ for odd primes so our κ_n is equal to the μ_n from [Hea17, Th. 1]. Here it is shown that indeed $\mu_n \sim 2/n$, confirming the proposition for $r = 2$. In fact, it was shown that for $r = 2$:

$$n + 2 \leq \tau_n \leq n + 3 + \ln(n). \tag{150}$$

In section 6.3.1, the case of $r = 3$ will be covered and a sharper bound than the proposition is achieved. Furthermore, in section 6.3.2 we will prove the proposition in general. At this point, we want to mention that our conjecture follows from the proof of [Juu17, Prop. 3.5] where b_n is used for our τ_n and d is used in place of of our r.

6.3.1 Heuristic for $r = 3$

Now let us analyze the case of $r = 3$. We see that:

$$\kappa_{n+1} = \frac{1 - (1 - 3\kappa_n + 3\kappa_n^2 - \kappa_n^3)}{3} = \kappa_n - \kappa_n^2 + \frac{1}{3}\kappa_n^3. \tag{151}$$

Furthermore, we have $\tau_n = 1/\kappa_n$. With this definition, the recurrence relation for $n \in \mathbb{N}$ is

$$\tau_{n+1} = \frac{\tau_n^3}{\frac{1}{3} - \tau_n + \tau_n^2}. \tag{152}$$

Lemma 6.4. *Let τ_n be defined as above. Then $\tau_n \geq n + 2$ for all $n \in \mathbb{N}_{>0}$.*

Proof. We proceed by induction on n.

For $n = 1$ we see $\tau_1 = \frac{1}{\kappa_1} = 3 \geq 1 + 2$.

Now suppose for some $n \in \mathbb{N}_{>0}$ we have $\tau_n \geq n + 2$. Then by extracting a term of τ_n from the recurrence relation, we see that:

$$\tau_{n+1} = \tau_n + \frac{\tau_n^2 - \frac{1}{3}}{\frac{1}{3} - \tau_n + \tau_n^2} = \tau_n + 1 + \frac{\tau_n - \frac{2}{3}}{\frac{1}{3} - \tau_n + \tau_n^2}. \tag{153}$$

Since $\tau_n^2 - \tau_n + \frac{1}{3} = \tau_n(\tau_n - 1) + \frac{1}{3} \geq \frac{1}{3}$ for $\tau_n \geq 1$, we see that the denominator is strictly positive. The numerator is clearly positive for $\tau_n \geq 1$. Thus, we can estimate that

$$\tau_{n+1} \geq \tau_n + 1 \geq (n+2) + 1 = n + 3. \tag{154}$$

□

Now we have a lower bound for τ_n, we will try to find an upper bound.

Lemma 6.5. *For $n \in \mathbb{N}_{>0}$,*

$$\tau_n \leq n + 1 + \sum_{j=1}^{n} \frac{1}{j}. \tag{155}$$

Proof. We proceed again by induction.

For $n = 1$ we see that

$$\tau_1 = 3 \leq 1 + 1 + \frac{1}{1}. \tag{156}$$

Suppose the equation holds for some $n \geq 1$. Again we have the identity:

$$\tau_{n+1} = \tau_n + 1 + \frac{\tau_n - \frac{2}{3}}{\frac{1}{3} - \tau_n + \tau_n^2}. \tag{157}$$

Because $\tau_n - \frac{2}{3} \leq \tau_n$ and $\frac{1}{3} - \tau_n + \tau_n^2 \geq \tau_n(\tau_n - 1)$, we get the estimation:

$$\tau_{n+1} \leq \tau_n + 1 + \frac{\tau_n}{\tau_n(\tau_n - 1)} = \tau_n + 1 + \frac{1}{\tau_n - 1} \leq \tau_n + 1 + \frac{1}{n+1}. \tag{158}$$

Thus, by substituting the induction hypothesis

$$\tau_{n+1} \leq n + 2 + \left(\sum_{j=1}^{n} \frac{1}{j} \right) + \frac{1}{n+1} = n + 2 + \sum_{j=1}^{n+1} \frac{1}{j}. \tag{159}$$

□

Now we can estimate this summation by estimating the area under the curve $1/x$ for $n \geq 1$:

$$\sum_{j=1}^{n} \frac{1}{j} \leq 1 + \int_{1}^{n} \frac{\mathrm{d}\, x}{x} = 1 + \ln n. \tag{160}$$

Thus, we get combined with the result of lemma (6.4):

$$n + 2 \leq \tau_n \leq n + 2 + \ln n. \tag{161}$$

Observe that this implies the result of proposition 6.2 for $r = 3$.

6.3.2 Heuristic for general $r > 1$

Let us try to generalize the ideas used to prove the bounds for $r = 3$ to any $r > 1$. In the general case, we have by combining (144) and (147) for $n \in \mathbb{N}$:

$$\tau_{n+1} = \frac{2r}{r-1}\left[1 - \left(1 - \frac{2}{\tau_n(r-1)}\right)^r\right]^{-1} = \frac{2r}{r-1} \cdot \frac{\tau_n^r}{\tau_n^r - \left(\tau_n - \frac{2}{r-1}\right)^r} \tag{162}$$

and $\tau_0 = \frac{2}{r-1}$.

By using τ_0 we can rewrite the recurrence to:

$$\tau_{n+1} = \frac{\tau_0 \tau_n^r r}{\tau_n^r - (\tau_n - \tau_0)^r}. \tag{163}$$

In analogy to [Juu17, Prop. 3.5], we will prove proposition 6.2 now.

Proof. Observe that (163) gives $\tau_1 = \tau_0 r = \frac{2r}{r-1}$. Since $r \geq 2$,

$$\tau_1 = \frac{2r}{r-1} > \frac{2r-2}{r-1} = 2 \tag{164}$$

and

$$\tau_1 = \frac{2r}{r-1} \leq \frac{2r + 2(r-2)}{r-1} = \frac{4(r-1)}{r-1} = 4. \tag{165}$$

In short, $2 < \tau_1 \leq 4$. Also,

$$1 + 1 < \tau_1 \leq 4 < 4 + 1 + \ln(1) \tag{166}$$

so the case for $n = 1$ is proven.

Now we will prove the result for $n > 1$. But in order to do this, we will estimate the recurrent relation first. For this, we will need that $\tau_n \geq \tau_0 r$, and later on we will show that this condition is true for $n \geq 1$. First, notice that

$$\tau_{n+1} = \tau_n + 1 + \frac{\tau_0 \tau_n^r r - (\tau_n + 1)\left(\tau_n^r - (\tau_n - \tau_0)^r\right)}{\tau_n^r - (\tau_n - \tau_0)^r}. \tag{167}$$

For the sake of brevity, let us call the numerator of the last term N and the denominator D.

We can expand D with the binomium of Newton and since the 0^{th} term cancels with τ_n^r we get:

$$D := \tau_n^r - (\tau_n - \tau_0)^r = \sum_{j=1}^{r} \binom{r}{j} (-1)^{j-1} \tau_n^{r-j} \tau_0^j. \tag{168}$$

By denoting the j^{th} term of this sum as a_j, we will see that $(a_j)_{j \in \mathbb{N}_{>0}}$ (and $a_j = 0$ for $j > r$) is a decreasing alternating sequence as defined in appendix A [7]. It is

[7] Note that we use the extended definition, with starting index $N = 1$.

obvious that for $k \in \mathbb{N}$, we have $a_{2k+1} \geq 0$ and $a_{2k} \leq 0$. And it can be seen for $0 < j < r$ that

$$-\frac{a_{j+1}}{a_j} = \frac{\binom{r}{j+1}\tau_0}{\binom{r}{j}\tau_n} = \frac{(r-j)\tau_0}{(j+1)\tau_n} \leq \frac{\tau_0 r}{\tau_n} \tag{169}$$

and this ratio is smaller than 1 if $\tau_n \geq \tau_0 r$. From this, we see that for all $k \in \mathbb{N}$, we have

$$-a_{2k+2} \leq a_{2k+1} \leq -a_{2k}. \tag{170}$$

Now we can use the result of lemma A.1, giving us:

$$D \geq a_1 + a_2 = r\tau_n^{r-1}\tau_0 - \frac{r(r-1)}{2}\tau_n^{r-2}\tau_0^2 = \tau_0\tau_n^{r-2}r\left(\tau_n - 1\right). \tag{171}$$

Now, we will prove that N is positive. For this, we will write down the polynomial in τ_n by using the binomium again:

$$\begin{aligned} N &= \tau_0\tau_n^r r - (\tau_n+1)\sum_{j=1}^{r}\binom{r}{j}(-1)^{j-1}\tau_n^{r-j}\tau_0^j \\ &= \tau_0\tau_n^r r - \left[\sum_{j=1}^{r}\binom{r}{j}(-1)^{j-1}\tau_n^{r-j+1}\tau_0^j\right] - \left[\sum_{j=1}^{r}\binom{r}{j}(-1)^{j-1}\tau_n^{r-j}\tau_0^j\right]. \end{aligned} \tag{172}$$

Since the term with $j = 1$ of the first summation cancels with the term $\tau_0\tau_n^r r$, we get

$$\begin{aligned} N &= \sum_{j=2}^{r}\binom{r}{j}(-1)^j\tau_n^{r-j+1}\tau_0^j + \sum_{j=1}^{r}\binom{r}{j}(-1)^j\tau_n^{r-j}\tau_0^j \\ &= \sum_{j=1}^{r-1}\binom{r}{j+1}(-1)^{j+1}\tau_n^{r-j}\tau_0^{j+1} + \sum_{j=1}^{r}\binom{r}{j}(-1)^j\tau_n^{r-j}\tau_0^j \\ &= (-1)^r\tau_0^r + \sum_{j=1}^{r-1}\left[\binom{r}{j} - \tau_0\binom{r}{j+1}\right](-1)^j\tau_n^{r-j}\tau_0^j. \end{aligned} \tag{173}$$

Now, we use for $1 \leq j < r$ that

$$\begin{aligned} \binom{r}{j} - \tau_0\binom{r}{j+1} &= \frac{r!}{j!\,(r-j)!} - \frac{2}{r-1}\frac{r!}{(j+1)!\,(r-j-1)!} \\ &= \frac{r!}{j!\,(r-j)!}\left[1 - \frac{2(r-j)}{(r-1)(j+1)}\right] \\ &= \frac{(r+1)!}{(j+1)!\,(r-j)!}\left[\frac{j+1}{r+1} - \frac{2(r-j)}{r^2-1}\right]. \end{aligned} \tag{174}$$

This term in square brackets is equal to:

$$\frac{(j+1)(r-1) - 2r + 2j}{r^2-1} = \frac{(j-1)(r+1)}{r^2-1} = \frac{j-1}{r-1} \tag{175}$$

so we have

$$N = \sum_{j=2}^{r} \binom{r+1}{j+1} \frac{j-1}{r-1} (-1)^j \tau_n^{r-j} \tau_0^j \tag{176}$$

since we have $\binom{r+1}{r+1}\frac{r-1}{r-1}(-1)^r\tau_n^{r-r}\tau_0^r = (-1)^r\tau_0^r$, and the term with $j = 1$ is zero.

Now, by denoting the j^{th} term with $b_j, (j \geq 2)$, we see that b_j is a decreasing alternating sequence with start index 2. Showing the alternation is trivial, and the ratio for $2 \leq j < r$ can be estimated as:

$$-\frac{b_{j+1}}{b_j} = \frac{\binom{r+1}{j+2} j\tau_0}{\binom{r+1}{j+1}(j-1)\tau_n} = \frac{(r-j)j\tau_0}{(j+2)(j-1)\tau_n}. \tag{177}$$

By noticing that $(j+2)(j-1) = j^2 + j - 2 \geq 3j - 2 \geq 2j$ we see that

$$-\frac{b_{j+1}}{b_j} \leq \frac{\tau_0 r}{\tau_n} \tag{178}$$

which again is smaller than one if $\tau_n \geq \tau_0 r$. Under this condition, we can estimate N by:

$$0 \leq b_2 + b_3 \leq N \leq b_2 = \binom{r+1}{3} \frac{1}{r-1} \tau_n^{r-2} \tau_0^2 = \tau_0^2 \tau_n^{r-2} \frac{r(r+1)}{6}. \tag{179}$$

Therefore, by combining this result with (171), we have

$$0 \leq \frac{N}{D} \leq \frac{\tau_0(r+1)}{6(\tau_n - 1)}. \tag{180}$$

Since $r \geq 2$, we see that $r + 1 \leq (r-3) + 2r = 3(r-1) = 6/\tau_0$. By plugging this into the equation, we find

$$0 \leq \frac{N}{D} \leq \frac{1}{\tau_n - 1} \tag{181}$$

where the upper bound has an equality for $r = 2$.

We will show by induction that for all $n \in \mathbb{N}_{>0}$:

$$n + 1 < \tau_n, \quad \tau_n \geq \tau_0 r. \tag{182}$$

For $n = 1$, we see that $2 < \tau_1 = \frac{2r}{r-1}$ and $\tau_1 = \tau_0 r$. Now, if for some $n \geq 1$, (182) is satisfied, then we satisfy the condition for (171) and (179), so we can use (181) to find that:

$$\tau_n + 1 \leq \tau_{n+1} \leq \tau_n + 1 + \frac{1}{\tau_n - 1}. \tag{183}$$

Thus, $\tau_{n+1} \geq \tau_n + 1 > (n+1) + 1$ and $\tau_{n+1} \geq \tau_n \geq \tau_0 r$. This concludes the induction.

Now, for $n \geq 1$, we see that:

$$\tau_{n+1} \leq \tau_n + 1 + \frac{1}{\tau_n - 1} < \tau_n + 1 + \frac{1}{n}. \tag{184}$$

By repeated use of this, we find for $n \geq 2$:

$$\begin{aligned}\tau_n &< \tau_{n-1} + 1 + \frac{1}{n-1} \\ &< \tau_{n-2} + 2 + \frac{1}{n-1} + \frac{1}{n-2} \\ &< \cdots \\ &< \tau_1 + (n-1) + \sum_{j=1}^{n-1} \frac{1}{j}.\end{aligned} \tag{185}$$

Now by using (160), this holds:

$$\tau_n < \tau_1 + (n-1) + 1 + \ln(n-1) < 4 + n + \ln(n). \tag{186}$$

□

7 Cubic polynomials

In section 5, theorem 1.2 was proven which was about quadratic polynomials of the form $f(X) = aX^2 + c$. In this section, we will generalize the argument of this theorem, to prove a similar result – theorem 1.3 – for cubic polynomials $f(X) = aX^3 + c$.

We want to point out to the reader that this theorem is in accordance with the heuristic developed in section 6.3 and equation (145) in particular, is expected to be the main term of the size of $f^r(\mathbb{F}_q)$. We also want to mention the work performed by Jamie Juul. Our result matches her result as done in [Juu17, Example 4.4].

We will prove theorem 1.3 in the rest of the section. However, first some different cases will be looked at. For proving the theorem, we will be using the Hasse-Weil bound again, so we need to split $f^n(X) - f^n(Y)$ up into absolutely irreducible parts as done in section 7.3. After this we will try to find structure in the system of equations $f^n(x_1) = \cdots = f^n(x_k)$ to estimate $N(r; k)$. The case for $k = 2$ is done separately in section 7.5 to show what is going on more explicitly.

7.1 Different cases

In the quadratic case, theorem 1.2 was only applicable on fields with odd characteristic. Similarly, for cubic polynomials we thus want to divide the finite fields by their characteristic modulo 3.

The characteristic p of a finite field of order p^k is always prime, and we can divide the prime numbers into three classes:

1. $p = 3$,
2. $p \equiv 1 \mod 3$,
3. $p \equiv 2 \mod 3$.

The first case is trivial and is not interesting. Since we are concerned about the running time of the Rho algorithm, this is irrelevant to us, because we can simply check if $3 \mid N$ when we want to factorize N. However, this case appears to be simple and we will analyze this in section 7.2. We will also look at some fields with even characteristic, in section 7.4.3.

In the last case, we use the result of section 6.1 where we now have $d = 3$ and $p-1 \equiv 1 \mod 3$. Thus we see that polynomials of the form $f(X) = (X+a)^3+b$ are permutations having $\#f^r(\mathbb{F}_p) = p$.

In the rest of this section, let us look at prime numbers $p \equiv 1 \mod 3$. Remember that $\mathbb{F}_p^\times$ is a multiplicative cyclic group thus is generated by some element $\xi \in \mathbb{F}_{p^\times}$ with order $p-1$. Observe that $p-1 = 3 \cdot l$ for some $l \in \mathbb{N}$. Thus, $\xi^3, \xi^6, \ldots, \xi^{3l-3}$ are all cubic residues and they have 3 roots each. There is only one number left which is 0. Therefore, $\frac{1}{3}$ of $\mathbb{F}_p^\times$ are cubic residues, and $\frac{2}{3}$ are cubic nonresidues.

We conclude that for cubic polynomials of the form $f(X) = (X+a)^3 + b$, $\#f(\mathbb{F}_p) = 1 + \frac{p-1}{3} = \frac{p+2}{3}$.

We note that theorem only says something about $p \equiv 1 \mod 6$. Since p is a prime number, either $p = 2$, $p = 3$, $p \equiv 1 \mod 6$ or else $p \equiv 5 \mod 6$. As discussed above, when $p \equiv 5 \mod 6$, or $p = 2$ we see that $\mathbb{F}_p$ is a bijection. Let us first discuss the case where $p = 3$.

7.2 Finite fields of order $q = 3^k$

Let us consider in this section, finite fields of order $q = 3^k$ with characteristic 3 where $k \in \mathbb{N}_{>0}$. We consider the iterates of $f(X) = aX^3 + c$ with $a \neq 0$.

Since we have characteristic 3, the following holds in $\mathbb{F}_q$:

$$(X+Y)^3 = X^3 + Y^3. \tag{187}$$

In particular we see,

$$\begin{aligned} f^r(X) - f^r(Y) &= a\left(f^{r-1}(X)\right)^3 - a\left(f^{r-1}(Y)\right)^3 \\ &= a\left(f^{r-1}(X)\right)^3 + a\left(-f^{r-1}(Y)\right)^3 \\ &= a\left(f^{r-1}(X) - f^{r-1}(Y)\right)^3. \end{aligned} \tag{188}$$

Now, by induction we will show that $f^r(X) - f^r(Y) = a^{u_r}(X-Y)^{v_r}$ for some recurrent series $(u_r)_{r\in\mathbb{N}}, (v_r)_{r\in\mathbb{N}}$. For the base case, it is easy to see that $u_0 = 0$ and $v_0 = 1$ since $f^0(X) - f^0(Y) = a^0(X-Y)^1$. Using equation (188), we see that we have the recurrence

$$\begin{cases} u_{r+1} &= 3u_r + 1, \\ v_{r+1} &= 3v_r. \end{cases} \tag{189}$$

This is easy to solve:

$$\begin{cases} u_r &= \frac{1}{2}(3^r - 1), \\ v_r &= 3^r. \end{cases} \tag{190}$$

Thus, we conclude that

$$f^r(X) = f^r(Y) = a^{\frac{1}{2}(3^r-1)}(X-Y)^{3^r}. \tag{191}$$

In addition, if $f^r(X) - f^r(Y) = 0$, then by this equation we find that $X = Y$.

We now have found enough information about the k^{th} moments, $N(r;k)$. This allows us to estimate $\#f^r(\mathbb{F}_q)$. Recall, that $N(r;k)$ was equal to the number of solution for

$$f^r(x_1) = f^r(x_2) = \cdots = f^r(x_k). \tag{192}$$

Using equation (191), we thus see that $x_1 = x_2 = \cdots = x_k$. Since $x_i \in \mathbb{F}_q$ we have q options which are all valid. Thus, $N(r;k) = q$.

For the cubic case, we will define $G_r(T)$ similarly to the case of quadratic polynomials, as done in equation (78). We let,

$$G_r(T) = \frac{1}{3^r!}\prod_{j=1}^{3^r}(j-T) = \sum_{k=0}^{3^r} C_{r,k}T^k, \tag{193}$$

where $C_{r,k}$ are coefficients chosen to satisfy this equation. Now we can derive a similar equation as (81) for the cubic case:

$$\#f^r(\mathbb{F}_q) = q - \sum_{k=0}^{3^r} C_{r,k}N(r;k) \tag{194}$$

where we have used that the degree of f^r is 3^r.

We now conclude that

$$\#f^r(\mathbb{F}_q) = q - q\sum_{k=0}^{3^r} C_{r,k} = q - qG_r(1) = q. \tag{195}$$

Thus, we have found that the function $f(X) = aX^3 + c$ is a bijection and therefore all of its iterates as well.

We want to remark that this result is obvious for $q = 3$, since all $x \in \mathbb{F}_3$ satisfy $x^3 - x = 0$ so $ax^3 + c = ax + c$ for all $x \in \mathbb{F}_3$. The polynomial $f(X) = aX + c$ defines a simple affine transformation which is clearly bijective (for $a \neq 0$).

We have covered the case of characteristic three now completely. Thus, for the rest of the section, we will assume

$$\text{char}(\mathbb{F}_q) \neq 3. \tag{196}$$

7.3 Absolute irreducibility of $f^n(X) - f^n(Y)$

For proving a similar result as in theorem 1.2 for cubic polynomials, we might want to investigate $N(r,k)$ in the cubic case to estimate $\#f^r(\mathbb{F}_q)$.

Let us take a look at the polynomial $f(X) = aX^3 + c$ with $a, c \in \mathbb{F}_q$ and $a \neq 0$. We make the same definition for $N(r;k)$ as in the quadratic case:

$$N(r;k) = \sum_{m\in\mathbb{F}_q} \left(\#\{\, x \in \mathbb{F}_q \mid f^r(x) = m \,\}\right)^k. \tag{197}$$

We can see that $N(r;k)$ is equal to the number of solutions over $\mathbb{F}_q$ satisfying:

$$f^r(x_1) = f^r(x_2) = \cdots = f^r(x_k). \tag{198}$$

Thus, we are interested in the number of solutions for the equation $f^r(x) - f^r(y) = 0$. We can use the Hasse-Weil bound only on absolutely irreducible curves, and the curve defined by this equation is far from that. We will show for finite fields containing an element ω such that $\omega^3 = 1$ but $\omega \neq 1$, factorizes $f^r(x) - f^r(y) = 0$ into absolutely irreducible polynomials in $\mathbb{F}_q(\omega)[X]$.

Thus, let us take a look at the cubic polynomial $f(X) = aX^3 + c$ where $a \neq 0$ and $a, c \in \mathbb{F}_q$. Let us define ω as a root of the equation $X^2 + X + 1$. We see that in $\mathbb{F}_5$, we have $X^2 + X + 1 \neq 0$ for all $X \in \mathbb{F}_5$. Thus, $\mathbb{F}_5 \subset \mathbb{F}_5(\omega)$. On the other hand, in $\mathbb{F}_7$ we have $X^2 + X + 1 = X^2 + 8X + 15 = (X + 5)(X + 3)$. In this case, $\omega \in \mathbb{F}_7 = \mathbb{F}_7(\omega)$ and ω can be either 2 or 4.

However in general, in $\mathbb{F}_q$, we cannot have $X^2 + X + 1 = (X - r)^2 = 0$ for some $r \in \mathbb{F}_q$. Since, by expanding parentheses, this would imply:

$$-2r = 1 \text{ and } r^2 = 1 \tag{199}$$

and therefore,

$$1 = (-2r)^2 = 4r^2 = 4. \tag{200}$$

However, this contradicts the assumption $\mathrm{char}(\mathbb{F}_q) \neq 3$. Therefore, $X^2 + X + 1$ is separable in $\mathbb{F}_q$.

Now we will use the properties of ω to factorize $f^r(X) - f^r(Y)$. Since ω is a root of $1 + X + X^2 = 0$, we see that

$$\begin{aligned}(X - Y)(X - \omega Y)(X - \omega^2 Y) &= X^3 - X^2Y(1 + \omega + \omega^2) + XY^2(1 + \omega + \omega^2) - Y^3 \\ &= X^3 - Y^3.\end{aligned} \tag{201}$$

Thus, it can be seen for $r > 0$ that:

$$\begin{aligned}f^r(X) - f^r(Y) &= a\left(f^{r-1}(X)\right)^3 - a\left(f^{r-1}(Y)\right)^3 \\ &= a(f^{r-1}(X) - f^{r-1}(Y)) \cdot (f^{r-1}(X) - \omega f^{r-1}(Y)) \\ &\quad \cdot (f^{r-1}(X) - \omega^2 f^{r-1}(Y)) \\ &= \cdots \\ &= a^r(X - Y) \prod_{m=0}^{r-1} (f^m(X) - \omega f^m(Y)) \left(f^m(X) - \omega^2 f^m(Y)\right) \\ &= (-a\omega)^r(X - Y) \prod_{m=0}^{r-1} (f^m(X) - \omega f^m(Y)) (f^m(Y) - \omega f^m(X)).\end{aligned} \tag{202}$$

Note this this last line actually holds for $r = 0$ as well, where $f^0(X) - f^0(Y) = X - Y$. Since then we have an empty product:

$$\prod_{m=0}^{-1} (\dots) = 1. \tag{203}$$

At this point, we have found that $f^r(X) - f^r(Y)$ factors into $2r+1$ polynomials in the algebraic closure $\overline{\mathbb{F}_q}[X,Y]$ (since in any case, $\omega \in \overline{\mathbb{F}_q}$). We do not know however, if these are absolutely irreducible. Although it is obvious that for $m = 0$ we have two absolutely irreducible polynomials since these have degree 1, it is not clear in general. We will prove, after making some definitions, in lemma 7.3 that in fact these factors are absolutely irreducible as well.

Definition 7.1. Let $f(X) = aX^3 + c$ be a cubic polynomial in $\mathbb{F}_q$ with $a \neq 0$. Then the corresponding form is given for $m \in \mathbb{N}$ by

$$F^m(X,Z) = Z^{3^m} f^m(X/Z). \tag{204}$$

Furthermore, we let

$$\phi(X,Y;-1) = X - Y, \tag{205}$$

and for $0 \leq d < r$ we let

$$\phi(X,Y;d) = f^d(X) - \omega f^d(Y). \tag{206}$$

Now the corresponding form is given for -1 as

$$\Phi(X,Y,Z;-1) = X - Y, \tag{207}$$

and for $0 \leq d < r$ as

$$\Phi(X,Y,Z;d) = Z^{3^d} \phi(X/Z, Y/Z; d). \tag{208}$$

It is obvious that F^m is a form (or equivalently, homogeneous polynomial), since $F^m(\lambda U, \lambda W) = \lambda^{3^m} F^m(U,W)$. Furthermore, we see that Φ is a form as well since $\phi(X,Y;d)$ has degree 3^d.

With this rewriting, we can simplify equation (202) to

$$f^r(X) - f^r(Y) = (-a\omega)^r (X - Y) \prod_{m=0}^{r-1} \phi(X,Y;d)\phi(Y,X;d), \quad (r \geq 0). \tag{209}$$

This allows us to state this as the following claim:

Claim 7.2. *$f^r(x) = f^r(y)$ for some $x, y \in \mathbb{F}_q$, if and only if $x = y$ or there is some $0 \leq m < r$ such that:*

$$\phi(x,y;m) = 0, \text{ or } \phi(y,x;m) = 0. \tag{210}$$

Now with all the useful definitions in 7.1, we can state the following lemma:

Lemma 7.3. *Let $\mathbb{F}_q$ be a finite field with an element $\omega \in \mathbb{F}_q$ satisfying $\omega^2 + \omega + 1 = 0$. Suppose*

$$f^i(0) = f^j(0) \implies i = j, \quad \text{for all } 0 \leq i, j \leq r. \tag{211}$$

Then for all $0 \leq m < r$, $\phi(X,Y;m)$ is absolutely irreducible in $\mathbb{F}_q[X,Y]$, where $\phi(X,Y;m)$ is defined in (206).

Proof. We will first find a criterion when a polynomial is absolutely irreducible.

As stated in [Har77, I, Exercise 3.7 a)], the intersection of two projective curves in $\mathbb{P}^2$ is non-empty. This provides us with a criterion.

Suppose (in general) that $\Phi(U,V,W)$ is some form which factors in the algebraic completion as

$$\Phi(U,V,W) = \Phi_1(U,V,W) \cdot \Phi_2(U,V,W), \tag{212}$$

then by the above, there exists some $(u,v,w) \in \overline{\mathbb{F}_q}^3$ such that $\Phi_1(u,v,w) = \Phi_2(u,v,w) = 0$ and $(u,v,w) \neq (0,0,0)$. Note that we can define derivatives on polynomial as well even though we are working in a finite field, since we can apply the chain rule and such in this simply on the polynomial ring. Now in particular, at this point, $\Phi(u,v,w) = 0$ and the product rule provides that

$$\nabla\Phi(u,v,w) = \nabla\Phi_1(u,v,w) \cdot \Phi_2(u,v,w) + \Phi_1(u,v,w) \cdot \nabla\Phi_2(u,v,w) = \vec{0}. \tag{213}$$

Now we take the contraposition of this and we conclude that Φ is absolutely irreducible if for all $\vec{0} \neq (u,v,w) \in \overline{\mathbb{F}_q}$, $\Phi(u,v,w) \neq 0$ or $\nabla\Phi(u,v,w) \neq \vec{0}$.

What we want to show is that for $0 \leq m < r$, $\phi(X,Y;m)$ is absolutely irreducible. It can be easily seen that this equivalent to showing that $\Phi(X,Y,Z;m)$, as defined in (208), is absolutely irreducible. Now combining the two observations, we see that we need to prove that $\nabla\Phi(u,v,w) \neq \vec{0}$ whenever $\Phi(u,v,w) = 0$ for some $\vec{0} \neq (u,v,w) \in \overline{\mathbb{F}_q}^3$.

By using (208), we see immediately that

$$\nabla\Phi(U,V,W;m) = \begin{pmatrix} W^{3^m-1}(f^m)'(U/W) \\ -\omega W^{3^m-1}(f^m)'(V/W) \\ \frac{\partial}{\partial W}\Phi(U,V,W;m) \end{pmatrix}. \tag{214}$$

Since $f(X) = aX^3 + c$, we use the chain rule to obtain

$$(f^m)'(x) = \frac{\mathrm{d}f(x)}{\mathrm{d}x} \cdot (f^{m-1})'(x) = 3a\left[f^{m-1}(x)\right]^2 \cdot (f^{m-1})'(x). \tag{215}$$

By a simple induction with $(f^0)'(x) = 1$ as a base case, it can be shown that

$$(f^m)'(x) = (3a)^m \prod_{l=0}^{m-1} \left(f^l(x)\right)^2. \tag{216}$$

We use this for the U-component of (214) to find

$$W^{3^m-1}(f^m)'(U/W) = W^{3^m-1}(3a)^m \prod_{l=0}^{m-1} \left(W^{-3^l}F^l(U/W)\right)^2. \tag{217}$$

However, this power of W is in fact equal to

$$3^m - 1 - 2\sum_{l=0}^{m-1} 3^l = 3^m - 1 - 2\frac{3^m-1}{3-1} = 0. \tag{218}$$

Thus, the U-component and V-component of (214) are given by:

$$W^{3^m-1}(f^m)'(U/W) = (3a)^m \prod_{l=0}^{m-1} \Big(F^l(U,W) \Big)^2. \tag{219}$$

and

$$\omega W^{3^m-1}(f^m)'(V/W) = \omega(3a)^m \prod_{l=0}^{m-1} \Big(F^l(V,W) \Big)^2. \tag{220}$$

What we wanted to show was that $\nabla\Phi(U,V,W;m) \neq \vec{0}$ and we will continue the proof by proving this by contradiction.

Suppose now that

$$\Phi(u,v,w;m) = 0 \quad \text{ and } \nabla\Phi(u,v,w;m) = \vec{0} \tag{221}$$

for some $\vec{0} \neq (u,v,w) \in \overline{\mathbb{F}_q}^3$. Then, using (219) and (220), we know there must exist $0 \leq s,t < m$ such that

$$F^s(u,w) = 0 \qquad \text{and} \qquad F^t(v,w) = 0. \tag{222}$$

We can see for $m > 0$ that:

$$\begin{aligned} F^m(u,w) &= w^{3^m} f^m(u/w) \\ &= w^{3^m} \Big(a f^{m-1}(u/w)^3 + c \Big) \\ &= a \Big(w^{3^{m-1}} F^{m-1}(u,w) \Big)^3 + c w^{3^m} \\ &= a \left(F^{m-1}(u,w) \right)^3 + c w^{3^m}. \end{aligned} \tag{223}$$

For $m = 0$ we find similarly,

$$F^0(u,w) = w^{3^0} f^0(u/w) = w \cdot (u/w) = u. \tag{224}$$

Note that we have used relation (204) since we cannot see F^m as an m^{th} iterate of F because then it would not be homogeneous anymore. Now by a simple induction on (223), we derive for $0 \leq m < r$, that

$$F^m(u,0) = a^{\frac{1}{2}(3^m-1)} u^{3^m}. \tag{225}$$

Here, we have used that the power of a satisfies the same recurrence as u_r from (189) and the power of u that of v_r.

Thus, if $w = 0$, (222) implies that $u^{3^s} = v^{3^t} = 0$ and then we see that $u = v = w = 0$ is the zero-solution. However, we assumed that this was not the zero-solution. Thus, we must have $w \neq 0$ for a vanishing solution $\nabla\Phi(u,v,w) = \vec{0}$.

Now since $w \neq 0$, equation (222) implies that

$$f^s(u/w) = f^t(v/w) = 0. \tag{226}$$

Recall that we assumed that $\Phi(u, v, w; m) = 0$ as well. Since $w \neq 0$, this yields

$$f^m(u/w) - \omega f^m(v/w) = 0. \tag{227}$$

Now observe that

$$f^m(u/w) = f^{m-s}(f^s(u/w)) = f^{m-s}(0), \tag{228}$$

$$f^m(v/w) = f^{m-t}(f^s(v/w)) = f^{m-t}(0). \tag{229}$$

Thus we can rewrite equation (227) now as

$$f^{m-s}(0) - \omega f^{m-t}(0) = 0. \tag{230}$$

If $s = t$, we see that $0 < m - s \leq m$ and $f^{m-s}(0) = 0 = f^0(0)$ which contradicts our assumption of (211). Thus, we conclude that $s \neq t$. Notice that now

$$\begin{aligned} f^{m-s+1}(0) &= f(f^{m-s}(0)) \\ &= f(\omega f^{m-t}(0)) \\ &= a(\omega f^{m-t}(0))^3 + c \\ &= a\omega^3 f^{m-t}(0)^3 + c \\ &= f^{m-t+1}(0), \end{aligned} \tag{231}$$

where we have used (230) and $\omega^3 = 1$.

We observe that $m - s + 1 \neq m - t + 1$ and

$$1 < m - s + 1, m - t + 1 \leq m + 1 \leq r. \tag{232}$$

Thus (231) contradicts the assumptions in (211).

Therefore, we see that the assumption of (221) led in all cases to a contradiction, and thus, this statement cannot be true. Therefore, we see that $\Phi(U, V, W; m)$ must be absolutely irreducible. And likewise, $\phi(U, V; m)$ is absolutely irreducible. □

In particular, we see that this lemma implies that the factorization as done in (209) factorizes into $2r + 1$ absolutely irreducible polynomials which is a quite strong statement.

7.4 Existence of a root of $X^2 + X + 1 = 0$ in $\mathbb{F}_q$

We are still interested in knowing when $\omega \in \mathbb{F}_q$ and when it is not. This is important because we want to know if $\mathbb{F}_q(\omega) = \mathbb{F}_q$, else it is a finite extension. Observe that $\omega^2 + \omega + 1 = 0$ has as a solution:

$$\omega = \frac{-1 \pm \sqrt{1^2 - 4 \cdot 1 \cdot 1}}{2} = \frac{1 \pm \sqrt{-3}}{2}, \tag{233}$$

when $\mathbb{F}_q$ is of odd characteristic (because only then 2 has an inverse). So we see that $\omega \in \mathbb{F}_q$ iff -3 is a square in $\mathbb{F}_q$.

7.4.1 Finite fields of order $q = p$

For finite fields of order p where p is a prime number, we can use the quadratic reciprocity theorem, to find out if -3 is a square or not. Assume that $p \neq 2$ since we had to take the inverse of 2 in equation (233) to find ω. Also assume that $p \neq 3$ since this case was solved in section 7.2. Then, the quadratic reciprocity theorem states for p, q odd prime numbers:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}. \tag{234}$$

Here $\left(\frac{p}{q}\right)$ is the Legendre symbol:

$$\left(\frac{p}{q}\right) = \begin{cases} 0, & q \mid p, \\ 1, & p \text{ is a quadratic residue modulo } q, \\ -1, & p \text{ is a quadratic non-residue modulo } q. \end{cases} \tag{235}$$

Thus in our case,

$$\left(\frac{p}{3}\right)\left(\frac{3}{p}\right) = (-1)^{(p-1)/2}. \tag{236}$$

Since $3 \nmid p$, we have:

$$\left(\frac{-3}{p}\right) = (-1)^{(p-1)/2}\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right). \tag{237}$$

We see that modulo 3, only 1 is a quadratic residue, so

$$\left(\frac{-3}{p}\right) = \begin{cases} 0, & p = 3, \\ 1, & p \equiv 1 \mod 3, \\ -1, & p \equiv 2 \mod 3. \end{cases} \tag{238}$$

We can now conclude that $\omega \in \mathbb{F}_p$ if and only if:

$$p \equiv 1 \mod 6. \tag{239}$$

Due to Dirichlet's theorem on arithmetic progressions, we know that this holds for infinitely primes and moreover, 'half' of the primes are of this form.

In the other case, $p \equiv 5 \mod 6$ and as we have shown before, the two options for ω are different since $X^2 + X + 1$ is separable.

Note that if -3 is a square in $\mathbb{F}_p$ for some prime number p, then it is a square as well in $\mathbb{F}_{p^k}$ since this is a field extension. Thus, we conclude that $\omega \in \mathbb{F}_q$ if $\text{char}(\mathbb{F}_q) \equiv 1 \mod 6$.

7.4.2 Field extensions of $\mathbb{F}_q$

We can establish a stronger result for finite fields of order q^2 and show that we can always embed a finite field $\mathbb{F}_q$ into the extension $\mathbb{F}_{q^2}$ such that ω exists inside the latter.

Lemma 7.4. *Let $\mathbb{F}_q$ be a finite field of order $q = p^k$ where p is some prime. Then $\mathbb{F}_{q^2}$ contains an element $\omega \in \mathbb{F}_{q^2}$ such that*

$$\omega^2 + \omega + 1 = 0. \tag{240}$$

Proof. Let us look at $\mathbb{F}_q$ first. Either there exists some $\omega \in \mathbb{F}_q$ satisfying (240) or not.

In the former case, we are done because of the inclusion $\omega \in \mathbb{F}_q \subset \mathbb{F}_{q^2}$.

In the latter, we deduce the following: Let $f(X) = X^2 + X + 1 \in \mathbb{F}_q[X]$ be a quadratic polynomial. If $f(X)$ was reducible in $\mathbb{F}_q[X]$, it would have a root $\omega \in \mathbb{F}_q$ which we assumed was not the case. Thus $f(X)$ is irreducible and $f(X)$ is a minimal polynomial. Now, let ω be some root of $f(X)$, then $\mathbb{F}_q(\omega)$ is a field extension of degree 2 so $\#\mathbb{F}_q(f) = q^2$. Furthermore it is clear that $\omega \in \mathbb{F}_q(\omega)$. As is shown in the course on "Rings and Galois theory" [Beu17, Thm. 10.1.2], there exists only one finite field of order q^2, $\mathbb{F}_{q^2}$, up to isomorphisms. Thus, $\mathbb{F}(\omega)$ is isomorphic to $\mathbb{F}_{q^2}$ and therefore ω corresponds to some $\omega' \in \mathbb{F}_{q^2}$ satisfying (240). □

Since there is a natural injection from the solutions in $\mathbb{F}_q$ to $\mathbb{F}_{q^2}$, namely the identity map on $\mathbb{F}_{q^2}$ restricted to the domain $\mathbb{F}_q$, we can estimate that the number of solutions for (198) in $\mathbb{F}_q$ is at most the number of solutions for (198) in $\mathbb{F}_{q^2}$. Suppose $N_q(r;k)$ is the number of solutions for (198) over the finite field $\mathbb{F}_q$. Then, the above statement translates to:

$$N_q(r;k) \leq N_{q^2}(r;k). \tag{241}$$

We want to point out that the number of solutions of $N_q(r;k)$ can be refined from the solutions in $\mathbb{F}_{q^2}$ by using Galois theory. We know that solutions, which are not fixed by all $\mathbb{F}_q$-automorphism, cannot be in $N_q(r;k)$ since these automorphisms fix by definition all $x \in \mathbb{F}_q$. Since we only use the estimation from q^2 when $\omega \notin \mathbb{F}_q$, we can assume that $\mathbb{F}_{q^2}/\mathbb{F}_q$ is a Galois extension since its two roots must be distinct as shown in the beginning of section 7.3. This extension is of degree 2 and thus the Galois group is $G = \{ e, \tau \}$ and we see that this τ maps its root as:

$$\tau(\omega) = -(\omega + 1). \tag{242}$$

This argument might be useful for good estimates in fields not containing ω but in the rest we will focus on fields containing ω.

7.4.3 Finite fields of order $q = 2^k$

Let us now look at fields with characteristic 2, and of order 2^k, with $k > 0$. We consider the iterates of $f(X) = aX^3 + c$ with $a \neq 0$.

When k is even, we see that $\mathbb{F}_q$ contains a subfield isomorphic to $\mathbb{F}_{\sqrt{q}}$ which has $\sqrt{q} = p^{k/2}$ elements. In this case, by lemma 7.4, we see that $\omega \in \mathbb{F}_q$. Therefore, 7.3 applies as well. So even though $p \not\equiv 1 \mod 6$, theorem 1.3 still applies.

Table 1: Table for every finite field $\mathbb{F}_{p^{2l+r}}$ with $r = 0, 1$.

	$k = 1$	$k = 2l$	$k = 2l + 1$
$p = 2$	permutation	$\omega \in \mathbb{F}_{2^k}$	-
$p = 3$	permutation	permutation	permutation
$p \equiv 1 \mod 6$	$\omega \in \mathbb{F}_p$	$\omega \in \mathbb{F}_{p^k}$	$\omega \in \mathbb{F}_{p^k}$
$p \equiv 5 \mod 6$	permutation	$\omega \in \mathbb{F}_{p^k}$	-

Now we will look at the case of $\mathbb{F}_2$. We see that there are only two functions of the form $f(X) = aX^3 + c$:

$$f(X) = X^3, \quad \text{and} \quad g(X) = X^3 + 1. \tag{243}$$

In the first case, $f = \mathrm{id}$ and the other case gives:

$$g(0) = 1, g(1) = 0. \tag{244}$$

This is thus a permutation. So we see that $\#f^n(\mathbb{F}_2) = \#g^n(\mathbb{F}_2) = 2$.

Let us move to the next field that was not covered yet: $q = 2^3$. We see that $\mathbb{F}_8 = \mathbb{F}_2[X]/(X^3 + X^2 + 1)$ since this polynomial does not have any linear factors. If R is one root of $X^3 + X^2 + 1$, then the other ones are given by R^2 and $R^2 + R + 1$. Now consider the polynomial $f(X) = X^2 + 1$. Then, one can see that

$$\begin{aligned} f(0) &= 1, & f(1) &= 0, \\ f(R) &= R^2, & f(R+1) &= R + 1 \\ f(R^2) &= R^2 + R + 1, & f(R^2 + 1) &= R^2 + 1, \\ f(R^2 + R) &= R^2 + R, & f(R^2 + R + 1) &= R. \end{aligned}$$

Thus, this is a permutation. We believe that it is not unlikely that there are more fields of order 2^{2l+1} such that there is a polynomial $f(X) = aX^3 + c$ which is a permutation.

We now provide a summary in table 1 of all different finite fields, if all functions $f(X) = aX^3 + c$ with $a \neq 0$ are permutations, or if they contain a third root of unity ω satisfying $\omega^2 + \omega + 1 = 0$ or if we do not know what happens (denoted with '-'). We believe that the fields containing a '-', might have functions $f(X) = aX^3 + c$ which are permutations.

7.5 A second moment estimate for $\omega \in \mathbb{F}_q$

In this section and the next ones, we will estimate the number of solutions for (198) over $\mathbb{F}_q$. For this we assume the following:

$$q = p^k, \text{ with } p \neq 3 \qquad \exists \omega \in \mathbb{F}_q : \omega^2 + \omega + 1 = 0. \tag{245}$$

In this section, we will estimate $N(r; 2)$, which is the number of solutions to $f^r(X) = f^r(Y)$ in $\mathbb{F}_q$. We will first find an upper bound, and after that a lower bound.

7.5.1 An upper bound

We can estimate $N(r;2)$ now with use of the inclusion-exclusion principle on claim 7.2:

$$N(r;2) \leq q + \sum_{m=0}^{r-1} \left[\#\mathcal{C}_{m,1}(\mathbb{F}_q) + \#\mathcal{C}_{m,2}(\mathbb{F}_q) \right]. \tag{246}$$

Here,

$$\mathcal{C}_{m,1} = \{ (x,y) \in \mathbb{F}_q^2 \mid \phi(x,y;m) = 0 \},$$
$$\mathcal{C}_{m,2} = \{ (x,y) \in \mathbb{F}_q^2 \mid \phi(y,x;m) = 0 \},$$

where ϕ is defined in (206).

which can be turned into projective curves in $\mathbb{P}^2$. Note that these curves are under the assumptions of lemma 7.3, the lemma implies that these curves are absolutely irreducible.

Let $D = 3^m$ and N_r the number of projective points on one of the curves. Then, the Hasse-Weil bound tells us that:

$$|N_r - (q+1)| \leq (D-1)(D-2)\sqrt{q}. \tag{247}$$

There are also points at infinity. These have $W = 0$ after homogenization. Thus, the number of points at infinity for $\mathcal{C}_{m,1}$ is the number of solutions for:

$$U^{3^m} - \omega V^{3^m} = 0. \tag{248}$$

which is at most 3^m. One might think that it is at most $q3^m$, but we can do better than this bound, since we must remember that we are working in the projective plane. Here solutions $(U,V,0), (U',V',0)$ are choices for the same point in $\mathbb{P}^2$ if for some λ, $U = \lambda U'$ and $V = \lambda V'$ (see definition B.6 for the terminology). Since we assumed $W = 0$, we see that all points in $\mathbb{P}^2$ with $W = 0$, is the point $[1:0:0]$ and the set

$$\{ [u:1:0] \mid u \in \mathbb{F}_q \}. \tag{249}$$

The point $[1:0:0]$ is clearly not a solution of (248). And then for the other points in the set, (248) becomes $U^{3^m} = \omega$ which is clearly bounded by 3^m solutions.

Similarly, $\mathcal{C}_{m,2}$ has at most 3^m points at infinitely. Thus, we see that:

$$|\#\mathcal{C}_{m,i}(\mathbb{F}_q) - q| \leq D^2\sqrt{q}, \quad \text{for } i = 1,2. \tag{250}$$

From (246) we see that:

$$\left| \sum_{m=0}^{r-1} [\#\mathcal{C}_{m,1}(\mathbb{F}_q) + \#\mathcal{C}_{m,2}(\mathbb{F}_q)] - 2rq \right| \leq 2rD^2\sqrt{q}. \tag{251}$$

In particular,

$$N(r;2) \leq (2r+1)q + 2r3^{2r}\sqrt{q}. \tag{252}$$

7.5.2 A lower bound

Now let $\Delta = \{ (x, y) \in \mathbb{F}_q^2 \mid x = y \}$.

By the inclusion-exclusion principle:

$$N(r;2) \geq q + \sum_{m=0}^{r-1} \left[\#\mathcal{C}_{m,1}(\mathbb{F}_q) + \#\mathcal{C}_{m,2}(\mathbb{F}_q) \right] - \sum_{0 \leq m < r} A_m - \frac{1}{2} \sum_{0 \leq m,l < r} \sum_{i,j=1,2} B_{ml,ij}. \tag{253}$$

Here,

$$A_m = \#\left(\mathcal{C}_{m,1} \cap \Delta\right)(\mathbb{F}_q) + \#\left(\mathcal{C}_{m,2} \cap \Delta\right)(\mathbb{F}_q). \tag{254}$$

and for $m \neq l$ or $i \neq j$:

$$B_{ml,ij} = \#\left(\mathcal{C}_{m,i} \cap \mathcal{C}_{l,j}\right)(\mathbb{F}_q) \tag{255}$$

while $B_{mm,ii} = 0$.

Estimating A_m is rather simple. When $x = y$, we are interested in the number of solutions for

$$(1 - \omega^i) f^m(x) = 0, \quad (i = 1, 2). \tag{256}$$

which is bounded by $\deg(f^m) = 3^m$. Thus, $A_m \leq 2 \cdot 3^m$. Therefore, we see that:

$$\sum_{m=0}^{r-1} A_m \leq 2 \sum_{m=0}^{r-1} 3^m = 3^r - 1 < 3^r. \tag{257}$$

Estimating $B_{ml,ij}$ takes more effort. Our first case is $m = l, i \neq j$. We see that $B_{mm,ij}$ is the number of solutions for:

$$f^m(x) - \omega f^m(y) = f^m(x) - \omega^2 f^m(y) = 0. \tag{258}$$

This implies $(\omega - \omega^2) f^m(y) = (2\omega + 1) f^m(y) = 0$. Suppose $2\omega + 1 = 0$. Then,

$$0 = 4(\omega^2 + \omega + 1) = 4\omega^2 + 4\omega + 1 + 3 = (2\omega + 1)^2 + 3 = 3. \tag{259}$$

However, $\mathrm{char}(\mathbb{F}_q) \neq 3$, so we have a contradiction. Therefore, $2\omega + 1 \neq 0$. Thus, this means $f^m(y) = 0$, which in its turn implies that $f^m(x) = 0$ as well. Therefore, we have found that:

$$B_{mm,ij} = \#\left\{ x \in \mathbb{F}_q \mid f^m(x) = 0 \right\}^2 \leq 3^{2m}. \tag{260}$$

We observe that

$$\sum_{m=0}^{r-1} B_{mm,12} \leq \sum_{m=0}^{r-1} 9^m = \frac{9^r - 1}{8} \leq 3^{2r}/8. \tag{261}$$

Now let us take a look at $B_{ml,ij}$ where $m < l$. Then $B_{ml,ij}$ is equal to the number of solutions of:

$$f^m(x) - \omega^i f^m(y) = 0 \tag{262}$$

$$f^l(x) - \omega^j f^l(y) = 0. \tag{263}$$

Now we will use that:

$$f(\omega^k x) = \omega^{3k} x^3 + c = x^3 + c = f(x) \tag{264}$$

since ω is a cube root of unity. Thus we see that:

$$f^l(x) = f^{l-m}(f^m(x)) = f^{l-m}(\omega^i f^m(y)) = f^{l-m}(f^m(y)) = f^l(y). \tag{265}$$

Since $\omega, \omega^2 \neq 1$ we see that (263) now gives

$$f^l(x) = f^l(y) = 0. \tag{266}$$

We now know that $f^l(x)$ has at most 3^l choices for x and for every x, y must satisfy (262), thus there remain only 3^m choices after x is fixed. This gives an estimation that:

$$B_{ml,ij} \leq 3^{m+l}. \tag{267}$$

This yields:

$$\sum_{i,j=1,2} B_{ml,ij} \leq 4 \cdot 3^{m+l}, \quad \text{for } m < l. \tag{268}$$

Finally we can sum over all contributions to see that:

$$\begin{aligned}
\frac{1}{2} \sum_{0 \leq m,l<r} \sum_{i,j=1,2} B_{ml,ij} &= \sum_{m=0}^{r-1} B_{mm,12} + \sum_{0 \leq m<l<r} \sum_{i,j=1,2} B_{ml,ij} \\
&\leq 3^{2r}/8 + 4 \sum_{l=0}^{r-1} \sum_{m=0}^{l-1} 3^{m+l} \\
&= 3^{2r}/8 + 2 \sum_{l=0}^{r-1} 3^l (3^l - 1) \\
&\leq 3^{2r}/8 + 2 \sum_{l=0}^{r-1} 9^l \\
&\leq 3^{2r}/8 + 3^{2r}/4 \\
&= \frac{3}{8} 3^{2r}.
\end{aligned} \tag{269}$$

Combining this with (257), (253) becomes:

$$N(r;2) \geq q + \sum_{m=0}^{r-1} \left[\#\mathcal{C}_{m,1}(\mathbb{F}_q) + \#\mathcal{C}_{m,2}(\mathbb{F}_q) \right] - 3^{2r}. \tag{270}$$

This error bound is significantly smaller than found for the estimation of the curve sizes as in (251). Therefore we can estimate:

$$N(r;2) \geq (2r+1)q - 3^{2r}(1 + 2r\sqrt{q}). \tag{271}$$

Finally, we can finish our estimate of $N(r;2)$ by combining this equation with (252). We conclude that under the assumption of lemma 7.3,

$$\left| N(r;2) - (2r+1)q \right| \leq 3r 3^{2r} \sqrt{q} \leq 3^{3r} \sqrt{q}. \tag{272}$$

8 Higher moment estimates for cubic polynomials

Now we have done a second moment estimate of $N(r;2)$, we want to generalize this to higher moments $k > 2$. As [Hea17] used graphs to characterize every curve of which the algebraic set $f^r(x_1) = f^r(x_2) = \cdots = f^r(x_k)$ is the union. We will first investigate how the graphs will look like in the case of cubic polynomials. When we know how the graph looks like, we will know how the curve looks like and out of which polynomials this set can be generated. Furthermore, we show that the curve is nonsingular. As a consequence, we may use the Hasse-Weil bound on the curve to find a bound on the number of solutions on one curve. After that, in section 8.3.1, we will dive into some combinatorics finding a recurrent relation for the number of graphs (or equivalently the number of ideals) as function of k. With this, we will be able to find an expression of the image size of the n^{th} iterate of $f(X) = aX^3 + c$.

8.1 Graph representation

Suppose we have some solution $x_1, \ldots, x_k$ of (198). Then we can construct a directed graph $G = (V, A)$ with vertices $V = \{\, 1, 2, \ldots, k \,\}$, arcs (directed edges) A and a weight function

$$d\colon A \to \{\, -1, 0, \ldots, r-1 \,\} \tag{273}$$

following this procedure:

1. If $x_i = x_j$, both $(i,j) \in A$ and $(j,i) \in A$ and $d(i,j) = d(j,i) = -1$.
2. If $x_i \neq x_j$, then let $0 \leq m$ be the smallest value such that one of these two holds:

$$\phi(x_i, x_j; m) = 0 \qquad\qquad \phi(x_j, x_i; m) = 0, \tag{274}$$

   where $\phi(X, Y; m)$ was defined in (206). Then we let $(i,j) \in A$ having weight $d(i,j) = m$ in the first case; and $(j,i) \in A$ with weight $d(j,i) = m$ in the second case.

Proposition 8.1. *Suppose we have constructed a directed graph $G = (V, A)$ from a solution $x_1, \ldots, x_k$. Then for $x_i \neq x_j$, we have either $(i,j) \notin A$ or $(j,i) \notin A$.*

Proof. Let us assume that $\phi(x_i, x_j; m) = \phi(x_j, x_i; m) = 0$ for some $m \geq 0$. We will try to deduce a contradiction.

By combining the two equations defined in (206), we see that

$$f^m(x_i) = \omega f^m(x_j), \quad f^m(x_j) = \omega f^m(x_i), \tag{275}$$

thus, $(1 - \omega^2) f^m(x_i) = 0$ as well as $(1 - \omega^2) f^m(x_j) = 0$. Since $\operatorname{char}(\mathbb{F}_q) \neq 3$ – recall (245) – we have $1 - \omega^2 \neq 0$, thus $f^m(x_i) = f^m(x_j) = 0$. This, in turn, implies that

$$f^m(x_i) - f^m(x_j) = 0, \tag{276}$$

so this can be factorized in the same manner as (209). We assumed that $x_i \neq x_j$ so $\phi(x_i, x_j; l) = 0$ or $\phi(x_j, x_i; l) = 0$ for some $0 \leq l < m$. However this contradicts the choice that m was minimal. Furthermore, note that, when $m = 0$, we see that (276) implies $x_i = x_j$ which contradicts the assumption that $x_i \neq x_j$. □

Now we see that for any solution $\vec{x}$, there is only one graph that can be built from $\vec{x}$ since every arc is taken to be -1 undirected, or minimal with only one direction. This relation between solutions $\vec{x}$ and graphs G is thus a function.

Definition 8.2. Let γ be the function mapping solutions $\vec{x}$ of (198) to the graph $\gamma(\vec{x})$ following the procedure from above.

Notation

Let us introduce the following notation for directed graphs $G = (V, A)$ with a weight function d and some $\{ v_1, v_2, \dots v_n \} \subseteq V$:

$$v_1 \to v_2 \to \dots \to v_n \Leftrightarrow (v_1, v_2), \dots, (v_{n-1}, v_n) \in A. \tag{277}$$

And moreover, $v_1 \xrightarrow{d_1} v_2 \xrightarrow{d_2} \dots \xrightarrow{d_{n-1}} v_n$ whenever for all $1 \leq i < n$:

$$(v_i, v_{i+1}) \in A \text{ and } d(v_i, v_{i+1}) = d_i. \tag{278}$$

Whenever the used graph is not clear from the context, we will denote an arc u, v with weight d in G' as:

$$u \xrightarrow[G']{d} v \tag{279}$$

or replace G' by A' if its vertices are clear from the context but the arcs not.

The graphs generated by the cubic polynomials seem to be rather different than those generated by the quadratic polynomials. We have seen that the factorization of $f^r(X) - f^r(Y) = 0$ contains a term $\phi(x_i, x_j; m)\phi(x_j, x_i; m)$, and since these two are not symmetric in x_i, x_j, these two options are different which was not the case for quadratic polynomials.

These options demand us to change the undirected graphs of [Hea17, Def. 1] to graphs that will be directed graphs. Therefore, we have found that the following definition will suit us in the rest of this proof:

Definition 8.3. A "(D,k)-graph" is a weighted graph $G = (V, A)$ on k vertices ($k = \#V$), for which any arc $(i, j) \in A$ has integral weight in the range $[-1, D]$. We say we have a "strict (D, k)-graph, if there exist $v, w \in V$ such that

$$v \xrightarrow{D} w. \tag{280}$$

If for all $v, w \in V$, we have $v \to w$ or $w \to v$, then we say that the graph is a "complete (D, k)-graph".

Furthermore, we want to step away from the algebraic properties of the solutions, to look at a purely graph-theoretic description of the constructed graph. For this, we will need enough properties from the solutions which we can apply on the graph. We have come up with the following definition to obtain this goal:

Definition 8.4. Let $G = (V, A)$ be a **complete** (D, k)-graph. Then G is said to be a proper (D, k)-graph whenever for all distinct $u, v, w \in V$:

(i) If $v \to w \to v$, then $v \xrightarrow{-1} w \xrightarrow{-1} v$.

(ii) If $v \xrightarrow{-1} w$, then $w \xrightarrow{-1} v$.

(iii) If $u \xrightarrow{m} v \xrightarrow{m} w$ for some $-1 \leq m \leq k$, then $w \xrightarrow{m} u$.

(iv) If 1) $u \xrightarrow{m} v$ or $v \xrightarrow{m} u$ and 2) $m < m'$, then

$$u \xrightarrow{m'} w \implies v \xrightarrow{m'} w \tag{281}$$

and

$$w \xrightarrow{m'} u \implies w \xrightarrow{m'} v. \tag{282}$$

From this definition, we can make two assertions:

Proposition 8.5. *Let G be a proper (D, k)-graph. If u, v, w are distinct vertices such that*

$$u \xrightarrow{m} v \xrightarrow{m'} w \text{ and } u \xrightarrow{m} w \tag{283}$$

then

$$m = m = -1 \text{ or } m' < m. \tag{284}$$

Proposition 8.6. *Let G be a proper (D, k)-graph. If u, v, w are distinct vertices such that*

$$u \xrightarrow{m'} v \xrightarrow{m} w \text{ and } u \xrightarrow{m} w \tag{285}$$

then

$$m = m = -1 \text{ or } m' < m. \tag{286}$$

Proof of Prop 8.5. We prove by contradiction so assume, 1) $m \neq -1$ or $m' \neq -1$ and 2) $m' \geq m$.

Suppose $m = m'$. Then, by property (iii), we see that $w \xrightarrow{m} u \xrightarrow{m} w$. Now by property (i), we obtain that $m = m' = -1$ which contradicts our assumption. We conclude that $m < m'$.

Now we make use of property (iv) on v, u and w to obtain that $u \xrightarrow{m'} w$. But since $u \xrightarrow{m} w$ and only one weight is assigned, we have found our contradiction. Thus, 1) or 2) must be true. □

Proof of Prop 8.6. We prove by contradiction so assume, 1) $m \neq -1$ or $m' \neq -1$ and 2) $m' \geq m$.

Suppose $m = m'$. Again using properties (iii) and (i), we obtain that $m = m' = -1$ which contradicts our assumption. We conclude that $m < m'$.

Now property (iv) applied on v, w and u implies that: $u \xrightarrow{m'} w$. But since $u \xrightarrow{m} w$ and only one weight is assigned, we have found our contradiction. Thus, 1) or 2) must be true. □

This definition becomes clear because we have the following lemma:

Lemma 8.7. *Let $\vec{x}$ be a solution to (198). Then $\gamma(\vec{x})$ is a proper, complete $(r-1, k)$-graph.*

Proof. It is clear from the construction of $\gamma(\vec{x})$ from $\vec{x}$ that $\gamma(\vec{x})$ is a complete $(r-1, k)$-graph. We will prove the conditions of definition 8.4:

(i) This follows directly from proposition 8.1: if $i \to j \to i$ then $x_i = x_j$ so

$$i \xrightarrow{-1} j \xrightarrow{-1} i. \tag{287}$$

(ii) If $v \xrightarrow{-1} w$, then $x_v = x_w$ so $x_w = x_v$ thus $w \xrightarrow{-1} v$.

(iii) If $m = -1$, then $x_u = x_v = x_w$ so $w \xrightarrow{-1} u$. Else, let us assume $m \geq 0$ and

$$f^m(x_u) - \omega f^m(x_v) = 0, \qquad f^m(x_v) - \omega f^m(x_w) = 0. \tag{288}$$

Then,

$$\omega f^m(x_u) = \omega^2 f^m(x_v) = \omega^3 f^m(x_w) = f^m(x_w) \tag{289}$$

so $f^m(x_w) - \omega f^m(x_u) = 0$ and $w \xrightarrow{m} u$.

(iv) Suppose 1) $u \xrightarrow{m} v$ or $v \xrightarrow{m} u$ and 2) $m < m'$, then

$$x_u = x_v \text{ or } f^m(x_u) - \omega f^m(x_v) = 0 \text{ or } f^m(x_v) - \omega f^m(x_u) = 0 \tag{290}$$

so claim 7.2 implies that

$$f^{m'}(x_u) = f^{m'}(x_v). \tag{291}$$

We prove the first implication by assuming now that $u \xrightarrow{m'} w$, so

$$f^{m'}(x_u) - \omega f^{m'}(x_w) = 0. \tag{292}$$

Using (291), we get

$$f^{m'}(x_v) - \omega f^{m'}(x_w) = 0. \tag{293}$$

Now we show that m' is minimal for $v \to w$. Suppose to the contrary that $v \xrightarrow{m''} w$ or $w \xrightarrow{m''} v$ for some $m'' < m'$. Then, by using claim 7.2 we have

$f^{m'}(x_v) = f^{m'}(x_w)$. Since $\omega \neq 1$ and (293), $f^{m'}(x_w) = 0$, thus from (292) $f^{m'}(x_u) = 0$. Now, we have found that $f^{m'}(x_u) - f^{m'}(x_w) = 0$ and by applying claim 7.2, we conclude that m' is not minimal for $u \to w$. We have a contradiction, so m' must be minimal: $v \xrightarrow{m'} w$.

Now, for the second implication, suppose $w \xrightarrow{m'} u$. Using (291), we have

$$f^{m'}(x_w) - \omega f^{m'}(x_u) = f^{m'}(x_w) - \omega f^{m'}(x_v) = 0. \tag{294}$$

If m' were not minimal for $w \xrightarrow{m'} v$, then we see that:

$$f^{m'}(x_w) = f^{m'}(x_u) = 0 \tag{295}$$

contradicting that m' was minimal for $w \to u$ similarly because $\omega \neq 1$. Thus, we see by the same argumentation, m' must be minimal so $w \xrightarrow{m'} v$.

□

In analogy to [Hea17, Lemma 3], we have the following theorem on the constructed graph:

Lemma 8.8. *For any proper strict (D, k)-graph $G = (V, \mathcal{A})$, with $D \geq 0$, we have a unique partition $V = A \cup B \cup C$ (with at most one set empty) such that for all $a \in A, b \in B, c \in C$, we have:*

$$a \xrightarrow{D} b \xrightarrow{D} c. \tag{296}$$

In addition, the induced subgraphs A, B and C are proper $(D-1, k')$-graphs ($k' = \#A, \#B$ resp. $\#C$).

Proof. First of all, note that a subgraph of a proper (D, k)-graph is a proper (D, k')-graph.

Uniqueness: We will first prove uniqueness (up to shuffling of A, B and C). Suppose A, B, C and A', B', C' are two valid partitions. Since G is strict, there exist $a \in A$ and $b \in B$ (shuffle A, B, C if one of them is empty). Now shuffle A', B', C' such that $a \in A'$.

If $a' \in A$, then, by completeness, $a \to a'$ or $a' \to a$ with weight $d < D$. If $a' \notin A'$ would hold, then $a \xrightarrow{D} a'$ or $a' \xrightarrow{D} a$. However, by (i) of definition 8.4 we get a contradiction. Thus, $a' \in A'$ and in particular $A \subseteq A'$. The converse goes similarly and we see that $A = A'$.

We now see that $b \notin A' = A$. Shuffle B', C' such that $b \in B'$. By the same argumentation as above, we see that $B = B'$. Since C and C' are $V \setminus (A \cup B)$, $C = C'$. Thus we conclude, A, B, C and A', B', C' are the same and the partition must be unique.

Existence: First, we note that G is strict, so let $a, b \in V$ be distinct such that $a \xrightarrow{D} b$. Now let A be the set of a and all $v \in V$ such that for some $m < D$:

$$a \xrightarrow{m} v \text{ or } v \xrightarrow{m} a. \tag{297}$$

In addition, let B be the set of b and all $v \in V$ such that for some $m < D$:

$$b \xrightarrow{m} v \text{ or } v \xrightarrow{m} b. \tag{298}$$

Observe that A and B cannot contain arcs $i \xrightarrow{D} j$, since this implies that as well for some $m < D$, $j \xrightarrow{m} i$ and then $D = -1$. Therefore, A and B are both proper $(D-1, k)$-graphs.

Now let $C = V \setminus (A \cup B)$. Now what remains to prove is that this partition satisfies the properties.

Look at (iv) of definition 8.4.

Let $a' \in A$, so either $a \xrightarrow{m} a'$ or $a' \xrightarrow{m} a$. In both cases, we see from property (iv) that $a \xrightarrow{D} b$ implies $a' \xrightarrow{D} b$ as well. Since $D \geq 0$, we cannot have that $b \to a'$ by property (i). Thus $a' \notin B$. Therefore, A and B are disjoint. Furthermore, let $b' \in B$ as well. We know that $a' \xrightarrow{D} b$ and by application of (iv) on b and b' we find as well that:

$$a' \xrightarrow{D} b'. \tag{299}$$

First of all, we see that $C \cap A = \emptyset$ and $C \cap B = \emptyset$ since C was the complement of the union of these. Thus, A, B and C form a partition of V.

Furthermore, let $c \in C$. By definition of A and B, we must have: 1) $a \xrightarrow{D} c$ or $c \xrightarrow{D} a$ and 2) $b \xrightarrow{D} c$ or $c \xrightarrow{D} b$. However, $a \xrightarrow{D} c \xrightarrow{D} b$ implies with property (iii) that $b \xrightarrow{D} a \xrightarrow{D} b$, so $D = -1$ by (i) which is contradictory. The options $a \xrightarrow{D} c$, $b \xrightarrow{D} c$, and $c \xrightarrow{D} a$, $c \xrightarrow{D} b$ contradict with proposition 8.5, respectively 8.6. We have eliminated 3 out of 4 options. Thus there remains only one:

$$b \xrightarrow{D} c \xrightarrow{D} a. \tag{300}$$

We remain to show that in fact for all $a' \in A, b' \in B$:

$$b' \xrightarrow{D} c \xrightarrow{D} a'. \tag{301}$$

However, this follows easily by applying property (iv) on (b, b', c), respectively (a, a', c). Note that c was chosen arbitrarily, thus we have proven for all $a' \in A$, $b' \in B$, $c' \in C$ that (296) holds.

The only thing left to prove is that C is a proper $(D-1, \#C)$-graph. Suppose $c, c' \in C$ and $c \xrightarrow{D} c'$. Then by applying proposition 8.5 on $a \xrightarrow{D} c \xrightarrow{D} c'$ and $a \xrightarrow{D} c'$, we see that we have $m = m'$, so $D = -1$ which is a contradiction. Thus we conclude that $c \xrightarrow{D} c'$ cannot hold. □

We still have a graph with at least $\frac{k(k-1)}{2}$ arcs, however, most of them are implied from the definitions of a (D, k)-graph. This motivates us to define when a (D, k)-graph comes from a smaller graph. We note that this definition is rather different than [Hea17, Definition 3] since the graphs are now directed and the definition of a proper graph is different.

Definition 8.9. Let $G = (V, A)$ be a complete (D, k)-graph, and suppose $G_0 = (V, A_0)$ is a subgraph of G with $A_0 \subseteq A$. We then say that G_0 "generates" G if there is some $n \in \mathbb{N}$ such that

$$A_0 \subset A_1 \subset \ldots \subset A_{n-1} \subset A_n = A \tag{302}$$

and in every step exactly one arc is added to A_{i+1} is added following one of these procedures:

(1) if $w \xrightarrow[A_i]{-1} u$, we can add $u \xrightarrow[A_{i+1}]{-1} w$.

(2) if $u \xrightarrow[A_i]{m} v \xrightarrow[A_i]{m} w$ for some $-1 \leq m < k$, we can add $w \xrightarrow[A_i]{m} u$.

(3) if for some $m < m'$, we have $u \xrightarrow[A_i]{m} v$ or $v \xrightarrow[A_i]{m} u$:

a) we can add $u \xrightarrow[A_{i+1}]{m'} w$ if $v \xrightarrow[A_i]{m'} w$.

or b) else if $w \xrightarrow[A_i]{m'} u$, we can add $w \xrightarrow[A_{i+1}]{m'} v$.

8.2 Ideals of solutions

We will define an ideal belonging to any (D, k)-graph:

Definition 8.10. Let G be a (D, k)-graph. Then, we define the ideal of G as

$$\mathcal{I}(G) = \left(\{ \phi(x_i, x_j; d) \mid i \xrightarrow{d} j \} \right) \subseteq \mathbb{F}_q[x_1, \ldots, x_k], \tag{303}$$

the ideal generated by all $\phi(x_i, x_j; d)$ where $\phi(X, Y; d)$ is defined in (206).

The motivation of definition 8.9 is now that we can remove arcs from a (D, k)-graph G, whereas $\mathcal{I}(G)$ is invariant under this removal of arcs, which we will state as a claim:

Claim 8.11. *Suppose G_0 generates a (D, k)-graph G. Then, $\mathcal{I}(G_0) = \mathcal{I}(G)$.*

Proof. First of all, note that any subgraph of a (D, k)-graph G is a (D, k)-graph as well, thus $\mathcal{I}(G)$ is defined by definition 8.10.

Let $G_0 \subseteq G_1 \subseteq \ldots \subseteq G_n = G$ be the chain of graphs. Since $A_i \subseteq A_{i+1}$, we see that

$$\mathcal{I}(G_0) \subseteq \mathcal{I}(G_1) \subseteq \ldots \subseteq \mathcal{I}(G). \tag{304}$$

Suppose now $0 \leq i < n$. In order to prove the statement, observe that we have to prove that $\phi(X_i, X_j; d) \in \mathcal{I}(G_i)$ when we added $i \xrightarrow{d} j$ to G_{i+1} since then it follows that $\mathcal{I}(G_{i+1}) = \mathcal{I}(G_i)$.

First, if we use rule (1) in A_i, then $w \xrightarrow[A_i]{-1} u$ so

$$X_w - X_u = \phi(X_w, X_u; -1) \in \mathcal{I}(G_i). \tag{305}$$

Now using (I3) we see that

$$\phi(X_u, X_w; -1) = X_u - X_w = (-1)(X_w - X_u) \in \mathcal{I}(G_i). \tag{306}$$

Next, consider rule (2). If $m = -1$, then by (I2) and $u \xrightarrow{-1} v \xrightarrow{-1} w$ we get

$$X_u - X_w = (X_u - X_v) + (X_v - X_w) \in \mathcal{I}(G_i) \tag{307}$$

since both terms were in $\mathcal{I}(G_i)$. Else $m \geq 0$ and

$$f^m(X_u) - \omega f^m(X_v),\ f^m(X_v) - \omega f^m(X_w) \in \mathcal{I}(G_i). \tag{308}$$

Now we see that

$$f^m(X_w) - \omega f^m(X_u) = -\omega^2 \phi(X_v, X_w; m) - \omega\phi(X_u, X_v; m) \in \mathcal{I}(G_i). \tag{309}$$

Lastly, consider rule (3). We now have $u \xrightarrow{m} v$ or $v \xrightarrow{m} u$. In both cases, when $m' > m$ we see using claim 7.2 that

$$f^{m'}(X_u) - f^{m'}(X_v) \in \mathcal{I}(G_i). \tag{310}$$

So if we use rule (3a), then $\phi(X_v, X_w; m') \in \mathcal{I}(G_i)$ and

$$\phi(X_u, X_w; m') = \phi(X_v, X_w; m') + (f^{m'}(X_u) - f^{m'}(X_v)) \in \mathcal{I}(G_i). \tag{311}$$

In the case of rule (3b), then $\phi(X_w, X_u, m') \in \mathcal{I}(G_i)$ and thus

$$\phi(X_w, X_v; m') = \phi(X_w, X_u; m') + (f^{m'}(X_u) - f^{m'}(X_v)) \in \mathcal{I}(G_i). \tag{312}$$

We now apply induction to find that

$$\mathcal{I}(G_0) = \mathcal{I}(G_1) = \cdots = \mathcal{I}(G). \tag{313}$$

□

We extend the chain definition for the directed graphs:

Definition 8.12. A (D, k)-graph $G = (V, A)$ is said to be a "chain" if there is a permutation $\sigma \in S_k$ such that this are the only arcs in G:

$$\sigma(1) \to \sigma(2) \to \ldots \to \sigma(k-1) \to \sigma(k) \tag{314}$$

and, for any $1 \leq s < t < k$, the maximum of

$$d(\sigma(s), \sigma(s+1)), d(\sigma(s+1), \sigma(s+2)), \ldots, d(\sigma(t), \sigma(t+1)) \tag{315}$$

is either -1 or attained at at most 2 points.

We have to make the chain definition larger than [Hea17, Def. 4], because we will glue three partitions and thus we have two arcs with weight D.

Lemma 8.13. *For every proper (D,k)-graph G, there is a chain (D,k)-graph G_0 which generates G.*

Proof. We prove this by induction on D.

Suppose $D=-1$. Since G is proper, it is complete as well, thus combining this with property (ii), for all $v,w\in V$,

$$v \xrightarrow{-1} w. \tag{316}$$

Thus, G is generated by the arcs $i \xrightarrow{-1} (i+1)$ where $1\leq i<k$ since repeated use of (1) and (2) give all arcs.

Now assume that $D\geq 0$ and the result is proven for all proper (d,k)-graphs ($-1\leq d<D$). If G is not a strict (D,k)-graph, it is a strict (d,k)-graph for some $d<D$ thus the result is implied by the induction hypothesis.

Thus assume that G is a strict proper (D,k)-graph. Now we can use lemma 8.8. Denote the partition by $V=A\cup B\cup C$ and the subgraphs by G_A,G_B,G_C. By the induction hypothesis, these are generated by the chains G_1,G_2,G_3 respectively and there exist permutations σ,τ,υ such that the arcs of G_1,G_2,G_3 are exactly:

$$\begin{aligned}\sigma(1)\to\ldots\to\sigma(\#A),\\ \tau(1)\to\ldots\to\tau(\#B),\\ \upsilon(1)\to\ldots\to\upsilon(\#C).\end{aligned}$$

Now by lemma 8.8, we have

$$\sigma(\#A)\xrightarrow[G]{D}\tau(1)\ \text{ and if } C\neq\emptyset\text{: }\tau(\#B)\xrightarrow[G]{D}\upsilon(1). \tag{317}$$

Using this fact, we can construct G_0 as the graph with the arcs:

$$\sigma(1)\to\ldots\to\sigma(\#A)\xrightarrow{D}\tau(1)\to\ldots\to\tau(\#B)\xrightarrow{D}\upsilon(1)\to\ldots\to\upsilon(\#C) \tag{318}$$

which we will prove is a chain and generates G. We only need to show that the maximum of a subarray is -1 or attained at two points. Denote the permutation $\sigma(1),\ldots,\tau(\#C)$ by $i_1,\ldots,i_k$.

Let $1<s<t<k$. Suppose the maximum of $d(i_l,i_{l+1})$ with $s\leq i\leq t$ is equal to D. Since the only arcs with weight D are in (317) and not in one G_1,G_2,G_3 (by lemma 8.8) we conclude that this maximum is in at most 2 points. Else the maximum is smaller than D and is thus obtained in a subset of the arcs of G_1,G_2 or G_3. By induction this satisfies the chain condition.

We will show that G_0 generates G. First, note that G_1,G_2 and G_3 generate G_A,G_B respectively G_C. Thus, we know already that G_0 generates the arcs $\mathcal{A}^*$ containing the arcs of G_A,G_B,G_C and the arcs of (317). Suppose $i\to j$ is in $G\setminus\mathcal{A}^*$. Then, we know that i and j must belong to different partitions. Note that from 8.8 the only ordered possibilities are $(A,B),(B,C)$ or (C,A) since any other would imply an arc of weight -1 between partitions due to property (i) (and for (A,C) we need property (iii)).

Let us take $i \in A$, $j \in B$ such that $i \to j$ is an arc of G but not of $\mathcal{A}^*$. By lemma 8.8 this arc has weight D. Furthermore, $\mathcal{A}^*$ contains the arc between i and $\sigma(\#A)$ and between j and $\tau(1)$ of weight $< D$ and $\sigma(\#A) \xrightarrow{D} \tau(1)$. By applying rule (3a) on $i, \sigma(\#A), \tau(1)$, we see that $\mathcal{A}^*$ can be extended by the arc

$$i \xrightarrow{D} \tau(1). \tag{319}$$

Now by applying rule (3b) on $\tau(1), j, i$ we see that we can extend by one more arc:

$$i \xrightarrow{D} j. \tag{320}$$

When we do this for all $i \in A, j \in B$, in the end G_0 generates all the arcs going from A to B.

Analogously, one can do this for all arcs from B to C but now with $\tau(\#B) \to \upsilon(1)$. At this point arcs from C to A follows rather straight-forward: if $i \in C$, $j \in A$ but $i \to j \notin \mathcal{A}^*$, pick some $b \in B \neq \emptyset$. This one satisfies

$$j \xrightarrow[\mathcal{A}^*]{D} b \xrightarrow[\mathcal{A}^*]{D} i, \tag{321}$$

thus by using rule (2), we can extend $\mathcal{A}^*$ by $i \xrightarrow{D} j$. Thus $\mathcal{A}^*$ can be extended to contain all arcs of G and G_0 generates G. □

8.3 Curves of solutions

Let us define the solutions for a graph G by $V(\mathcal{I}(G))$ (see B for the definition of V). In particular it is easy to see that $\gamma^{-1}(G) \subseteq V(\mathcal{I}(G))$: Suppose for some solution $\vec{x} \in \mathbb{F}_q^n$, that $\gamma(\vec{x}) = G$. Then clearly $\phi(x_i, x_j; d_{ij}) = 0$ for all arcs $i \xrightarrow{d_{ij}} j$ in G by construction of G. Therefore, $\vec{x} \in V(\mathcal{I}(G))$.

It is clear from the definition that $V(\mathcal{I}(G))$ is an algebraic set and we will focus on this in this subsection. However, since the Hasse-Weil bound applies on projective varieties, we will have to find the equivalent homogeneous algebraic set. Furthermore we will need to analyze what this algebraic set looks like.

First, we will need to show that all possible curves $\mathcal{C}$ are projective varieties.

Lemma 8.14. *Suppose the conditions of lemma 7.3 holds. Every proper (D, k)-graph G corresponds to a projective variety $\mathcal{C}$ given by*

$$\mathcal{C}\colon \Phi(X_i, X_{i+1}, X_0; d_i) = 0 \quad (1 \leq i < k) \tag{322}$$

where $\Phi(X, Y, Z; d)$ is defined in (208). Moreover, if $1 \leq i < j < k$ then the maximum of $x_i, \ldots, x_j$ is -1 or occurs at at most two points.

Proof. Using lemma 8.13 in combination with claim 8.11, we see that $\mathcal{I}(G)$ is generated by

$$\phi(X_i, X_{i+1}; d_i) \quad (\text{for } 1 \leq i < k), \tag{323}$$

and the homogeneous ideal $\mathcal{I}(G)^*$ is generated by

$$\Phi(X_i, X_{i+1}, X_0; d_i) \quad (\text{for } 1 \leq i < k). \tag{324}$$

Now we let the curve $\mathcal{C}$ be the algebraic set of this ideal:

$$\mathcal{C} = V(\mathcal{I}(G)^*) = \bigcap_{1 \leq i < k} V\Big(\Phi(X_i, X_{i+1}; d_i)\Big) \tag{325}$$

where we have used the equation (416) of the zero locus, $V(S)$.

Now using the result of 7.3, we see that $\phi(X_i, X_{i+1})$ is irreducible in $\mathbb{F}_q$. Since $\mathbb{F}_q$ is a field and thus a unique factorization domain, [Beu17, Thm. 5.1.3] yields that

$$(\phi(X_i, X_{i+1}; d_i)) \tag{326}$$

is a prime ideal. Ultimately, by using B.10 and B.11 we conclude that

$$V(\Phi(X_i, X_{i+1}, X_0; d_i)) \tag{327}$$

is a projective variety.

In particular, we are done if $k = 2$.

However if $k > 2$, we see that $\mathcal{C}$ is a finite intersection of projective varieties. As shown in [Har77, I, Ex. 2.16], an intersection of varieties is not necessarily a variety. But in this case, the irreducibility follows from the absolute irreducibility from the next lemma below. □

We furthermore extend [Hea17, Lemma 6] to cubic polynomials.

Lemma 8.15. *Under assumption of lemma 7.3, the chain system $\mathcal{C}$ from (322) is a nonsingular complete intersection. Hence $\mathcal{C}$ is an absolutely irreducible curve over $\mathbb{F}_q$, with degree at most $3^{(k-1)(d-1)}$.*

Proof. What we will need to show is that $\mathcal{C}$ is nonsingular.

By definition, this is equivalent to showing that for all points $(x_0, x_1, \ldots, x_n) \in \mathcal{C}$ and all coefficients $c_i \in k$ such that

$$\sum_{i=1}^{k-1} c_i \nabla \Phi(x_i, x_{i+1}, x_0; d_i) = \vec{0} \tag{328}$$

implies that all $c_i = 0$ (proving linear independence of the vectors $\Phi(x_i, x_{i+1}, x_0; d_i)$ for every point in $\mathcal{C}$).

We will prove this by contradiction. Thus, assume not all c_i are zero and let c_s be the first non-zero and c_t the last non-zero coefficient. Then we have $0 < s \leq t < k$ and

$$\sum_{i=s}^{t} c_i \nabla \Phi(x_i, x_{i+1}, x_0; d_i) = \vec{0}. \tag{329}$$

This is a system of equations, and in particular for the s^{th} component we see that this simplifies to

$$c_s \frac{\partial}{\partial x_s} \Phi(x_s, x_{s+1}, x_0; d_s) = 0 \tag{330}$$

and likewise for c_{t+1}:

$$c_t \frac{\partial}{\partial x_{t+1}} \Phi(x_t, x_{t+1}, x_0; d_t) = 0. \tag{331}$$

Since $(\partial/\partial x)\Phi(x, y, z; d) = 1$ for $d = -1, 0$ we see that $d_s \geq 1$. Similarly it can be seen that $d_t \geq 1$ as well. Therefore, we can use the earlier result of equations (219) and (220) which is in this case

$$\frac{\partial}{\partial x_s} \Phi(x_s, x_{s+1}, x_0; d_s) = (3a)^{d_s} \prod_{l=0}^{d_s - 1} \left[F^l(x_s, x_0)\right]^2 = 0, \tag{332}$$

and

$$\frac{\partial}{\partial x_{t+1}} \Phi(x_t, x_{t+1}, x_0; d_t) = \omega(3a)^{d_t} \prod_{l=0}^{d_t - 1} \left[F^l(x_{t+1}, x_0)\right]^2 = 0, \tag{333}$$

where $F(U, W)$ was defined in (204).

This shows the existence of indices $0 \leq i < d_s$ and $0 \leq j < d_t$ such that

$$F^i(x_s, x_0) = F^j(x_{t+1}, x_0) = 0. \tag{334}$$

Now we can determine for which points this could be possible.

Suppose that $x_0 = 0$. Combining this with (225), yields

$$x_s = 0, \quad \text{and } x_{t+1} = 0. \tag{335}$$

However, then we also see that for all $l \geq s$, if $x_l = 0$ then $\Phi(x_l, x_{l+1}, x_0; d_l) = 0$ implies that $x_{l+1} = 0$. Now using induction, we simply see that for all $l \geq s$, $x_l = 0$. Likewise, if for some $l < t$, $x_{l+1} = 0$ then, $\Phi(x_l, x_{l+1}, x_0; d_l) = 0$ implies that $x_l = 0$ as well. Thus, we have for all $l \leq t$ that $x_l = 0$ and so

$$(x_0, x_1, \ldots, x_k) = (0, 0, \ldots, 0) \notin \mathbb{P}^k, \tag{336}$$

which is in contradiction with $(x_0, \ldots, x_k)$ being a point on the curve.

Thus, we can assume that (334) is not attained in a point at infinity, but rather in the affine space. In particular our point $(x_0, \ldots, x_k)$ is now equivalent to

$$(1, x_1/x_0, x_2/x_0, \ldots x_k/x_0), \tag{337}$$

and without loss of generality we let $x_0 = 1$. Now we see that (334) yields that

$$f^i(x_s) = f^j(x_{t+1}) = 0. \tag{338}$$

Since $d_s, d_t \geq 1$, the maximum D of

$$d_s, d_{s+1}, \ldots, d_{t-1}, d_t \tag{339}$$

is attained in at most 2 points. Let these point(s) be $d_u = d_v = D$ with $u \leq v$.

Now for all $l \neq u, v$ we have $d_l < D$ and thus $\phi(x_l, x_{l+1}, d_u) = 0$ implies

$$f^D(x_l) = f^D(x_{l+1}). \tag{340}$$

Now by induction we see

$$\begin{aligned} f^D(x_s) = f^D(x_{s+1}) = \cdots = f^D(x_u), & \\ f^D(x_{u+1}) = f^D(x_{u+2}) = \cdots = f^D(x_v) & \qquad (\text{if } u < v), \\ f^D(x_{v+1}) = f^D(x_{v+2}) = \cdots = f^D(x_{t+1}). & \end{aligned}$$

On the other hand, at the maximum,

$$f^D(x_u) = \omega f^D(x_{u+1}), \quad \text{and} \quad f^D(x_v) = f^D(x_{v+1}). \tag{341}$$

Combining these two we see if $u = v$ that $f^D(x_s) = \omega f^D(x_{t+1})$ and else $f^D(x_s) = \omega^2 f^D(x_t)$.

In this, we now use (338) to see that

$$f^{D-i}(0) = f^D(x_s) = \omega^E f^D(x_{t+1}) = \omega^E f^{D-j}(0) \quad (\text{where } E = 1, 2). \tag{342}$$

If $i = j$ then this would produce – since $1 \neq \omega, \omega^2$ – that $f^{D-i}(0) = f^0(0)$ which violates the assumptions of lemma 7.3. Thus let us assume without loss of generality that $0 \leq i < j < D$. Now after one iteration of (342) we obtain

$$f^{D+1-i}(0) = f^{D+1-j}(0), \tag{343}$$

and since $D + 1 - j < D + 1 - i \leq D + 1 \leq r$ we have found a contradiction again. Thus in either case we contradict the assumption of lemma 7.3.

We conclude that $\mathcal{C}$ is a nonsingular curve. And this immediately implies that is a complete intersection as well by [BH14, lemma 3.2].

The degree of the curve and absolute irreducibility follow from [BH14, Lemma 3.2]. Note that $\omega^3 = 1$ so the forms defining $\mathcal{C}$ are integral. The lemma provides us that

$$\deg(\mathcal{C}) = \deg(\Phi(X_1, X_2, X_0; d_1)) \cdot \ldots \cdot \deg(\Phi(X_{k-1}, X_k, X_0; d_{k-1})). \tag{344}$$

We see that $\deg(\Phi(X, Y, Z; -1)) = 1$ and $\deg(\Phi(X, Y, Z; d)) = 3^d$ for $0 \leq d < r$. Thus, ignoring the fact that the maximum is in at most two points, we see that:

$$\deg(\mathcal{C}) \leq (3^{r-1})^{k-1} \leq 3^{rk}. \tag{345}$$

□

Now in contrast to (101), we have

$$|\#\mathcal{C}(\mathbb{F}_q) - (q+1)| \leq 3^{2rk}\sqrt{q}. \tag{346}$$

8.3.1 Counting curves

We can count the number of curves by counting the number of graphs since there is a bijection between them. It should be clear that a function $\mathfrak{C}$ from proper $(r-1,k)$-graphs to the curves that are used, is surjective tautologically.

Proposition 8.16. $\mathfrak{C}$ *is injective.*

Proof. Suppose we have two proper $(r-1,k)$-graphs $G_1 \neq G_2$ for which $\mathcal{C} = \mathfrak{C}(G_1) = \mathfrak{C}(G_2)$. Since G_1 and G_2 are different, then there are indices i, j such that the arc(s) between i and j is (are) different with weight d_1 and d_2 respectively. We distinguish two cases: $d_1, d_2 \neq -1$ and $\min(d_1, d_2) = -1$.

First, suppose $\min(d_1, d_2) = -1$. We cannot have both $d_1 = d_2 = -1$ since this would give the same arcs. Without loss of generality we can assume that $-1 = d_1 < d_2$ and $i \xrightarrow[G_2]{d_2} j$. Now, for all points in $\mathcal{C}$ we have $X_i = X_j$ and $f^{d_2}(X_i) = \omega f^{d_2}(X_j)$. Since $1 \neq \omega$, we see that $f^{d_2}(X_i) = 0$. This yields for all $1 \leq h \leq k$:

$$f^r(X_h) = f^r(X_i) = f^{r-d_2}(f^{d_2}(X_i)) = f^{r-d_2}(0). \tag{347}$$

Now, if $r_1, \ldots, r_M$ are all the distinct roots of these equation, then

$$\mathcal{C} \subseteq \{\, r_1, \ldots, r_M \,\}^k. \tag{348}$$

Thus, $\mathcal{C}$ would not be curve (dimension 1), but a variety consisting of points (dimension 0). Therefore we get a contradiction.

Consider the second case: $d_1, d_2 \geq 0$. When $d_1 = d_2$ we would have

$$i \xrightarrow[G_1]{d_1} j \text{ and } j \xrightarrow[G_2]{d_1} i. \tag{349}$$

Thus, $f^{d_1}(X_i) = \omega f^{d_1}(X_j)$ and $f^{d_1}(X_j) = \omega f^{d_1}(X_i)$ for all points on the curve $\mathcal{C}$. Using $\omega^2 \neq 1$ we obtain

$$f^{d_1}(X_i) = f^{d_1}(X_j) = 0 \tag{350}$$

and by the same reasoning we get the same contradiction. In the last case, assume without loss of generality that $d_1 > d_2$. Then, we have

$$f^{d_1}(X_i) = \omega f^{d_1}(X_j) \text{ and } f^{d_1}(X_j) = f^{d_1}(X_i). \tag{351}$$

Again $f^{d_1}(X_i) = f^{d_1}(X_j) = 0$ and we see that every case gives a contradiction.

We conclude that $\mathfrak{C}(G_1) \neq \mathfrak{C}(G_2)$. □

As in the quadratic case, we let $\mathcal{N}(r;k)$ be the number of curves $\mathcal{C}$. By proposition 8.16, this boils down to counting the number of proper $(r-1,k)$-graphs.

Lemma 8.8 is useful for counting the proper strict $(r-1,k)$-graphs. We see that the number of proper strict $(r-1,k)$-graphs is

$$\mathcal{N}(r;k) - \mathcal{N}(r-1;k). \tag{352}$$

Furthermore, we have for each a proper strict $(r-1,k)$-graph, a unique partition A, B, C (up to reordering), where each A, B, C are proper $(r-2,k')$-graphs. Using this information we can count the number of proper strict $(r-1,k)$-graphs. However, we need to pay attention that we do not count certain configurations more than once, since a cyclic permutation of (A, B, C) gives another proper strict $(r-1,k)$-graph. Thus let us assume A is of size a, B of size b and C of size c, and we sort them in ascending order:

$$a \leq b \leq c. \tag{353}$$

Now we only have two interchangeable sets if equality occurs.

In lemma 8.8, the partition could have at most one empty partition. Thus, let us consider the case that $A = \emptyset$. Now $B, C \neq \emptyset$. The lemma says that there are arcs from B to C or the other way. Thus, we decide that the arcs go from B to C. This decision implies that no graphs are counted twice since the direction of the arcs matters. Therefore, $A = \emptyset$ contributes

$$R_0 = \sum_{a=1}^{k-1} \binom{k}{a} \mathcal{N}(r-1;a)\,\mathcal{N}(r-1;k-a), \quad (\text{if } r \geq 1, k \geq 2) \tag{354}$$

to $\mathcal{N}(r;k)$. Interestingly, this is twice the formula for the quadratic case of [Hea17, p. 18], the direction of arcs matter in our case.

Let us consider the case that $A \neq \emptyset$. If $a < b < c$, we have two possible 3-cycles: arcs from A to B via C back to A, or $A \to C \to B \to A$. Thus, this contributes:

$$R_1 = \sum_{\substack{0<a<b<c<k \\ a+b+c=k}} \frac{2k!}{a!\,b!\,c!}\,\mathcal{N}(r-1;a)\,\mathcal{N}(r-1;b)\,\mathcal{N}(r-1;c) \tag{355}$$

The next case is that $a < b = c$. Now we observe that counting the subsets of $A \to B \to C \to A$ is sufficient. The reason for this is that we do not distinguish between B and C because they are of the same size. This contribution is thus half of (355):

$$R_2 = \sum_{\substack{0<a<b \\ a+2b=k}} \frac{k!}{a!\,b!^2}\,\mathcal{N}(r-1;a)\,\mathcal{N}(r-1;b)^2 \tag{356}$$

In the case of $a = b < c$, we see that the coefficient in front of (355) is the same as the last case,

$$R_3 = \sum_{\substack{0<a<c \\ 2a+c=k}} \frac{k!}{a!^2\,c!}\,\mathcal{N}(r-1;a)^2\,\mathcal{N}(r-1;c) \tag{357}$$

The last case and trickiest is when $a = b = c$ which is only possible if k is a multiple of 3. We now observe that all the sets are of same size. Since we consider direction but not a cyclic permutation, the contribution is

$$R_4 = \frac{[3 \mid k]\,k!}{3(k/3)!^3}\,\mathcal{N}(r-1;k)^3. \tag{358}$$

Bringing it all together, we obtain the formula:

$$\mathcal{N}(r;k) - \mathcal{N}(r-1;k) = R_0 + R_1 + R_2 + R_3 + R_4 \tag{359}$$

Since graphs with one vertex have no arcs, $\mathcal{N}(r;1) = 1$ follows naturally. The equation above satisfies this as well since the right-hand side only contains empty sums, thus we can relax the condition in (354) to $k \geq 1$.

We see that R_3 resembles R_2 since R_3 sums over $0 < b < a$ in fact and therefore

$$R_2 + R_3 = \sum_{\substack{0<i,j<k \\ i\neq j, i+2j=k}} \frac{k!}{i!\, j!^2} \mathcal{N}(r-1;i)\, \mathcal{N}(r-1;j)^2. \tag{360}$$

We can replace this by a sum over three indices which sum up to k such that exactly two indices are equal:

$$R_2 + R_3 = \frac{1}{3} \sum_{\substack{0<i_1,i_2,i_3<k \\ \#\{\, i_1,i_2,i_3 \,\}=2, \\ i_1+i_2+i_3=k}} \frac{k!}{i_1!\, i_2!\, i_3!} \mathcal{N}(r-1;i_1)\, \mathcal{N}(r-1;i_2)\, \mathcal{N}(r-1;i_3). \tag{361}$$

When we want to modify R_1 to sum over all distinct i_1, i_2, i_3, this is six times the summing of R_1 since for any term in R_1, we sum over permutations of i_1, i_2, i_3 in the distinct value summation. Thus, when we replace the sum by distinct indices, we have to divide the expression by 6 to account for this:

$$R_1 = \frac{1}{3} \sum_{\substack{0<i_1,i_2,i_3<k \\ \#\{\, i_1,i_2,i_3 \,\}=3, \\ i_1+i_2+i_3=k}} \frac{k!}{i_1!\, i_2!\, i_3!} \mathcal{N}(r-1;i_1)\, \mathcal{N}(r-1;i_2)\, \mathcal{N}(r-1;i_3). \tag{362}$$

Now we see that R_4 can be written similarly for an index-set with size 1. Thus I hope it is clear that we have reduced (359) to

$$\mathcal{N}(r;k) - \mathcal{N}(r;k-1) = R_0 + \frac{1}{3} \sum_{\substack{0<i_1,i_2,i_3<k, \\ i_1+i_2+i_3=k}} \frac{k!}{i_1!\, i_2!\, i_3!} \prod_{l=1}^{3} \mathcal{N}(r-1;i_l) \tag{363}$$

Now we will look at R_0. This case is equal to summing over a, b, c where $c = 0$ and $0 < a, b < k$ such that $a + b + c = k$. We see that $3R_0$ is equal to summing over a, b, c such that exactly one of them is zero and all are less than k. Thus, we could relax the lower-bound of (363) to $0 \leq i_l$ and absorb the term of R_0 inside this. Furthermore, if we extend the upper-bound of this sum to $\leq k$ (for $k > 0$), then the other two indices must be equal to zero. Thus we will define $\mathcal{N}(r;0) = 1$ so the function is defined here. three indices could be equal to k so this adds the term

$$3\frac{1}{3}\frac{k!}{k!\, 0!\, 0!} \mathcal{N}(r-1;k)\, \mathcal{N}(r-1;0)\, \mathcal{N}(r-1;0) = \mathcal{N}(r-1;k). \tag{364}$$

This term was in the left-hand side of (363), so we conclude that

$$\mathcal{N}(r;k) = \frac{1}{3} \sum_{\substack{0 \le i_1, i_2, i_3 \le k, \\ i_1+i_2+i_3=k}} \frac{k!}{i_1!\, i_2!\, i_3!} \prod_{l=1}^{3} \mathcal{N}(r-1; i_l), \quad (r, k \ge 1). \tag{365}$$

Furthermore, when $r = 0$ we see that a graph consists only of arcs with weight -1 and since the graph is proper, it is complete and thus there is only one such graph. This yields $\mathcal{N}(0;k) = 1$ for $k \ge 0$.

For some fixed $r \ge 1$ the exponential generating function is given by:

$$E(X;r) = \sum_{k=0}^{\infty} \frac{\mathcal{N}(r;k)}{k!} X^k. \tag{366}$$

Claim 8.17. *$E(X;r)$ converges absolutely for small enough X.*

Proof. We will show that this converges absolutely for small enough X by a crude bound on $\mathcal{N}(r;k)$. For this we use claim 8.14, to see that there are $k!$ relabelings possible for the curves of $\mathcal{N}(r;k)$. Moreover, each $d_i, 1 \le i < k$ is in the range $[-1, r)$. Thus we obtain the crude bound

$$\mathcal{N}(r;k) \le k!\,(r+1)^{k-1} \le k!\,(r+1)^k. \tag{367}$$

Now every coefficient of $E(X;r)$ is dominated by $(r+1)^k$ for positive $X > 0$. The series

$$\sum_{k \in \mathbb{N}} (r+1)^k X^k \tag{368}$$

converges absolutely when

$$\lim_{k \to \infty} \left| \frac{(r+1)^{k+1} X^{k+1}}{(r+1)^k X^k} \right| = (r+1)\,|X| < 1 \tag{369}$$

by the ratio test for series. Thus, if $0 < X < (r+1)^{-1}$, $E(X;r)$ converges absolutely. □

Now for $r > 0$ we see that, after finding the suitable constant term $2/3$,

$$\begin{aligned} E(X;r) &= 1 + \sum_{k=1}^{\infty} \frac{\mathcal{N}(r;k)}{k!} X^k \\ &= \frac{2}{3} + \frac{1}{3} \sum_{i_1=0}^{\infty} \sum_{i_2=0}^{\infty} \sum_{i_3=0}^{\infty} \prod_{l=1}^{3} \frac{\mathcal{N}(r-1; i_l)}{i_l!} X^{i_l} \\ &= \frac{2 + E(X;r-1)^3}{3} \end{aligned} \tag{370}$$

since we use the recurrence (365) for $k \ge 1$.

In particular, for $r = 0$ we see that $E(X; r)$ simplifies to

$$E(X; 0) = \exp(X). \tag{371}$$

Using (370) we claim that by induction, coefficients $\nu(r; m)$ $(0 \leq m \leq 3^r)$ summing up to 1 can be found such that

$$E(X; r) = \sum_{m=0}^{3^r} \nu(r; m) e^{mX}. \tag{372}$$

Absolute convergence of $E(X; r)$ allows us to rearrange terms and we find

$$E(X; r) = \sum_{k=0}^{\infty} \left(\sum_{m=0}^{3^r} \nu(r; m) m^k \right) \frac{X^k}{k!}. \tag{373}$$

Combining this with (366) yields

$$\mathcal{N}(r; k) = \sum_{m=0}^{3^r} \nu(r; m) m^k \leq 3^{rk}. \tag{374}$$

The recurrence of (370) gives in combination with (372) in particular for $\nu(r; 0)$:

$$\nu(r; 0) = \frac{2 + \nu(r-1; 0)^3}{3}. \tag{375}$$

Up to now, we have found all the required results to finish the estimation on $N(r; k)$. We can use similar steps as the ones used in section 5, but now the degree of all curves $\mathcal{C}$ is at most 3^{rk}.

One sees that $N(r; k) = \sum_{m \in \mathbb{F}_q} \#\{ x \in \mathbb{F}_q \mid f^r(x) = m \}^k$ corresponds to the number of solutions to

$$f^r(x_1) = f^r(x_2) = \cdots = f^r(x_k), \tag{376}$$

where all $x_i \in \mathbb{F}_q$. It is generally known that the canonical mapping

$$\begin{aligned} \phi_0 \colon \quad & \mathbb{A}^k \to \mathbb{P}^k \\ & (x_1, \ldots, x_k) \mapsto [1 : x_1 : x_2 : \cdots : x_k] \end{aligned}$$

is injective. Thus, we let $N_p(r; k)$ be the number of points $[x_0 : x_1 : \cdots : x_k] \in \mathbb{P}^k$ that satisfy

$$F^r(x_1, x_0) = F^r(x_2, x_0) = \cdots = F^r(x_k, x_0). \tag{377}$$

Now we see that $N(r; k)$ and $N_p(r; k)$ differ by only the points 'at infinity', that is, the number of points $p \in \mathbb{P}^k$ with $x_0 = 0$ satisfying (377). We now determine the number of points 'at infinity'. For this, we use equation (225) to see that these points $[0 : x_1 : x_2 : \cdots : x_k]$ must satisfy:

$$a^{(3^m-1)/2} x_1^{3^m} = a^{(3^m-1)/2} x_2^{3^m} = \cdots = a^{(3^m-1)/2} x_k^{3^m}. \tag{378}$$

And since $a \neq 0$ we see that $x_1 = x_2 = \cdots = x_k$ is the only solution. This corresponds to exactly one point in $\mathbb{P}^k$:

$$[0 : 1 : 1 : \cdots : 1]. \tag{379}$$

Thus, we know that

$$N(r;k) = N_p(r;k) - 1. \tag{380}$$

Furthermore, when we take the union over all curves that are allowed in lemma 8.14 we see

$$N_p = \#\left(\bigcup_{\mathcal{C}} \mathcal{C}\right)(\mathbb{F}_q). \tag{381}$$

In this case, we will use the inclusion-exclusion principle, in which we can bound the intersection of two curves by Bézout's theorem:

$$\#(\mathcal{C}_1 \cap \mathcal{C}_2)(\mathbb{F}_q) \leq \deg(\mathcal{C}_1) \cdot \deg(\mathcal{C}_2) \leq 3^{2rk}. \tag{382}$$

Similar to (104), we thus find that

$$\left| N(r;k) - \sum_{\mathcal{C}} \#\mathcal{C}(\mathbb{F}_q) \right| \leq 1 + \frac{1}{2}\mathcal{N}(r;k)^2 3^{2rk}. \tag{383}$$

We now use the Hasse-Weil bound and Castelnuovo's genus bound, to arrive at

$$|\#\mathcal{C}(\mathbb{F}_q) - (q+1)| \leq 3^{2rk}\sqrt{q}. \tag{384}$$

Note that we may use the Hasse-Weil bound because of lemma 8.15.

We now use the triangle inequality repeatedly on all the terms occurring in (383) and use the bound of (384). This yields

$$\begin{aligned} |N(r;k) - \mathcal{N}(r;k)(q+1)| &\leq 1 + \mathcal{N}(r;k)3^{2rk}\left(\frac{1}{2}\mathcal{N}(r;k) + \sqrt{q}\right) \\ &\leq 3^{4rk}\sqrt{q}, \end{aligned} \tag{385}$$

where we have used the bound (374) on $\mathcal{N}(r;k)$ in the last step. We see that the main term for (194) is

$$(q+1)\sum_{k=0}^{3^r} C_{r,k}\,\mathcal{N}(r;k) = (q+1)\sum_{m=0}^{3^r} \nu(r;m)\sum_{k=0}^{3^r} C_{r,k}m^k. \tag{386}$$

Again since $G_r(T) = [T = 0]$, as defined by (193), this simplifies to

$$(q+1)\nu(r;0). \tag{387}$$

So let $\mu_r = 1 - \nu(r;0)$. $\nu(0;0) = 0$ as can be seen from (371) and the recurrence for μ_r is

$$\mu_r = 1 - \frac{2 + \nu(r-1;0)^3}{3} = \frac{1 - (1-\mu_{r-1})^3}{3}. \tag{388}$$

The asymptotic behaviour of μ_r simply follows by corollary 6.3: $\mu_r \sim 1/r$.

Now using (194),

$$\#f^r(\mathbb{F}_q) - \mu_r q = q(1-\mu_r) - \sum_{k=0}^{3^r} C_{r,k} N(r;k). \tag{389}$$

By using the estimate of $N(r;k)$ from (385) results in

$$|\#f^r(\mathbb{F}_q) - \mu_r q| \leq \nu(r;0) + \sqrt{q} \sum_{k=0}^{3^r} |C_{r,k}| \left(3^{4r}\right)^k. \tag{390}$$

Recall, that we may use (91) again, since $3 \leq 3^r \leq 3^{4r}$. Now we see that

$$|\#f^r(\mathbb{F}_q) - \mu_r q| \leq 3^{4r3^r}\sqrt{q}. \tag{391}$$

Calculation shows for $r \geq 15$ that $4r \leq (4/3)^r$ so

$$|\#f^r(\mathbb{F}_q) - \mu_r q| \leq 3^{4^r}\sqrt{q}. \tag{392}$$

Thus we have proven theorem 1.3. □

Corollary 8.18. *Let $\mathbb{F}_q$ be some finite field of characteristic $p \equiv 1 \mod 6$ and let $f(X) = aX^3 + c$ with $a \neq 0$. Then $f^i(0) = f^j(0)$ for some i, j with*

$$i < j \ll \frac{q}{\log\log q} \tag{393}$$

Proof. Let $r = \lfloor \log_4(\log_3 q) \rfloor - 1$. Then either $f^i(0) = f^j(0)$ for some $i, j < r$ or not. In the first case we are done. In the second case, the assumptions of lemma 6.2 are satisfied. Thus, we may use (392) assuming that q is rather large ($r \geq 15$). We see that

$$|\#f^r(\mathbb{F}_q) - q/r| \leq 3^{\log_3 q/4}\sqrt{q} = q^{3/4} \tag{394}$$

Since q/r grows much faster than $q^{3/4}$, $\#f^r(\mathbb{F}_q) \leq Cq/r$ for some appropriate constant C and large enough q. Now let $k = \lceil Cq/r \rceil$. Then the values of $f^r(0), f^{r+1}(0), \ldots, f^{r+k}(0), f^{r+k}(0)$ are all elements of $f^r(\mathbb{F}_q)$. Because this are $k+1$ numbers, at least one value should occur twice by the pigeonhole principle. Thus there must exist $i < j \leq r + k$ for which the result follows. □

Appendices

A Decreasing alternating sequences

We define a sequence $(a_n)_{n\in\mathbb{N}}$ to be decreasing and alternating if and only if:

$$0 \leq \ldots \leq -a_{2k+1} \leq a_{2k} \leq -a_{2k-1} \leq \ldots \leq -a_3 \leq a_2 \leq -a_1 \leq a_0. \tag{395}$$

In this section we will prove the following useful lemma:

Lemma A.1. *Let $(a_n)_{n\in\mathbb{N}}$ be a decreasing alternating sequence and let*

$$s_n = \sum_{m=0}^{n} a_m, \quad \textit{for all } n \in \mathbb{N}. \tag{396}$$

Then for any $n \in \mathbb{N}$,

$$a_0 + a_1 = s_1 \leq s_n \leq s_0 = a_0. \tag{397}$$

Proof. We will prove this lemma by induction on n with base cases for $n = 0$ and $n = 1$ and the inductive step that the statements holds for $2k + 2$ and $2k + 3$ whenever it holds for $2k$ and $2k + 1$.

For the base case $n = 0, 1$ we use the fact that $a_1 \leq 0$ (since $0 \leq -a_1$) to see that

$$s_1 = a_0 + a_1 \leq a_0 = s_0 \tag{398}$$

so in particular, $s_1 \leq s_i \leq s_0$ for $i = 0, 1$.

Suppose for some $k \in \mathbb{N}$ that $s_1 \leq s_{2k+i} \leq s_0$ for $i = 0, 1$. Note that the base case $k = 0$ already satisfies this. Since $a_{2k+2} \leq -a_{2k+1}$ we have $a_{2k+1}+a_{2k+2} \leq 0$, thus

$$s_{2k+2} = s_{2k} + (a_{2k+1} + a_{2k+2}) \leq s_{2k} \leq s_0. \tag{399}$$

Furthermore, we have $a_{2k+3} \leq 0$, so

$$s_{2k+3} = s_{2k+2} + a_{2k+3} \leq s_{2k+2} \leq s_0. \tag{400}$$

On the other hand, $a_{2k+2} \geq 0$ so

$$s_{2k+2} = s_{2k+1} + a_{2k+2} \geq s_{2k+1} \geq s_1. \tag{401}$$

Lastly, we have $-a_{2k+3} \leq a_{2k+2}$ so $a_{2k+2} + a_{2k+3} \geq 0$. This yields:

$$s_{2k+3} = s_{2k+1} + a_{2k+2} + a_{2k+3} \geq s_{2k+1} \geq s_1. \tag{402}$$

Now we can conclude that from the induction hypothesis that

$$s_1 \leq s_{2(k+1)+i} \leq s_0 \tag{403}$$

where $i = 0$ or $i = 1$.

Now by the principle of induction we achieve the conclusion of the lemma. □

In some cases, we have constructed a sequence not starting from zero, but some $N \in \mathbb{N}_{>0}$. In this case, a sequence $(a_n)_{n\in\{\,N,N+1,\dots\,\}}$ is a decreasing alternating sequence if and only if:

$$0 \leq \ldots \leq -a_{N+2k+1} \leq a_{N+2k} \leq -a_{N+2k-1} \leq \ldots \leq -a_{N+1} \leq a_N \tag{404}$$

or equivalently iff $(b_n)_{n\in\mathbb{N}}$ with $b_n = a_{n+N}$ is a decreasing alternating sequence.

Now for any $M \geq N$, we have

$$a_N + a_{N+1} \leq \sum_{i=N}^{M} a_i \leq a_N \tag{405}$$

by applying b_n on the lemma from above.

B Algebraic geometry

The field of algebraic geometry contains tools to look at solutions of a set of polynomials in certain fields, which can be either $\mathbb{C}$ or $\mathbb{F}_q$.

First, we recall the definition of an ideal from [Beu17, Def. 2.1.5], which we will use in this section extensively:

Definition B.1. Let R be a ring. A subset $I \subset R$ is an ideal whenever it satisfies the properties:

(I1) $0 \in I$,

(I2) $a - b \in I$ for all $a, b \in I$,

(I3) for all $r \in R$, and $a \in I$ we have $ra \in I$.

Furthermore, the ideal generated by $a_1, \ldots, a_n$ is denoted by:

$$(a_1, \ldots, a_n) := \{\, r_1 a_1 + \cdots + r_n a_n \mid r_i \in R \,\}. \tag{406}$$

Now we will now introduce some concepts from algebraic geometry, taken from [Gat14, Ch. 1].

Definition B.2 ([Gat14, Def. 1.2 a)])**.** Let k be a field and

$$\mathbb{A}^n = \{\, (c_1, c_2, \ldots, c_n) \mid c_i \in k \text{ for } i = 1, \ldots, n \,\} \tag{407}$$

be the affine n-space over k.

Note that $\mathbb{A}^n$ is just k^n as a set. It is customary to use two different notations here since k is also a k-vector space and a ring. We will usually use the notation $\mathbb{A}^n$ if we want to ignore these additional structures:

for example, addition and scalar multiplication are defined on k^n, but not on $\mathbb{A}^n$. The affine space $\mathbb{A}^n$ will be the ambient space for our zero loci of polynomials below.

Definition B.3 ([Gat14, Def. 1.2 c)], [Ful08, Sect. 1.2]). For a subset $S \subset k[X_1, \ldots, X_n]$ of polynomials, we call

$$V(S) := \{\, x \in \mathbb{A}^n \mid f(x) = 0 \text{ for all } f \in S \,\} \tag{408}$$

the (affine) zero locus of S.

Suppose $X \subseteq \mathbb{A}^n$. If there is some zero locus S such that $X = V(S)$, then X is an 'algebraic set'. As a convention, we will use 'algebraic set' throughout this thesis. Note that some, like [Gat14], refer to this as an 'affine variety' but we will use this for the things described in definition B.8.

One can see that for an algebraic set X, there will be many sets S of polynomials having $X = V(S)$.

In particular, suppose $f \in S$ and $h(x) \in k[X_1, \ldots, X_n]$. Then, $h(x)f(x)$ has at least all zeros of $f(x)$ and thus we have

$$V(S \cup \{\, hf \,\}) = V(S). \tag{409}$$

Furthermore, for $f, g \in S$, if $f(X) = g(X) = 0$ then$f(X) + g(X) = 0$ as well, and now

$$V(S \cup \{\, f + g \,\}) = V(S). \tag{410}$$

We conclude that in fact

$$V(S) = V((S)) \tag{411}$$

where (S) is the ideal generated by S.

Definition B.4 ([Gat14, Def. 1.10]). Let $X \subset \mathbb{A}^n$. Then,

$$I(X) := \{\, f \in k[X_1, \ldots, X_n] \mid f(X) = 0 \text{ for all } x \in X \,\} \tag{412}$$

is the ideal of X.

B.1 Projective space

In algebraic geometry, projective space is studied as well. First, recall the definition of projective space:

Definition B.5. Let k be a field. The projective n-space over k, written $\mathbb{P}^n(k)$ or simply $\mathbb{P}^n$, is the set of all equivalence classes of the equivalence relation $\sim$ on $\mathbb{A}^{n+1} \setminus \{\, \vec{0} \,\}$ with

$$\vec{x} \sim \vec{y} \Leftrightarrow x = \lambda y \text{ for some } \lambda \in k. \tag{413}$$

Definition B.6. We denote the equivalence class of $\sim$, represented by some $(x_1, x_2, \ldots, x_{n+1})$, by

$$[x_1 : x_2 : \cdots : x_{n+1}] \in \mathbb{P}^n, \tag{414}$$

which we call points in $\mathbb{P}^n$. We say $(x_1, x_2, \ldots, x_{n+1})$ is a choice for the point $[x_1 : x_2 : \cdots : x_{n+1}]$.

Definition B.7 ([Ful08, p. 45])**.** Let k be a field.

For a function $f \in k[X_1, \ldots, X_{n+1}]$ and a point $p \in \mathbb{P}^n$, p is a zero of f if

$$f(x_1, \ldots, x_{n+1}) = 0 \tag{415}$$

for every choice of homogeneous coordinates $(x_1, \ldots, x_{n+1})$ of p.

A set $X \subseteq \mathbb{P}^n$ is a projective algebraic set, if there exists some set $S \subseteq k[X_1, \ldots, X_{n+1}]$ such that $X = V(S)$, where

$$V(S) = \{\, p \in \mathbb{P}^n \mid p \text{ zero of } f \text{ for all } f \in S \,\} \tag{416}$$

is the (projective) zero locus of S.

Definition B.8 (p. 45, [Ful08])**.** A *non-empty* affine (projective) algebraic set $V \subseteq \mathbb{P}^n$ is irreducible if it is not the union of two smaller affine (projective) algebraic sets. An irreducible affine (projective) algebraic set in $\mathbb{A}^n$ ($\mathbb{P}^n$) is called a affine (projective) variety.

Similar to (411), when I is the ideal generated by S, we see that $V(I) = V(S)$.

When f is a form, we have $f(\lambda\vec{x}) = \lambda^{\deg(f)} f(\vec{x})$ for all $\lambda \in k$. Now suppose for some point $p \in \mathbb{P}^n$ and some choice $(x_1, \ldots x_{n+1})$ of p satisfying $f(x_1, \ldots, x_{n+1}) = 0$, then for all choices $\vec{x}' \sim \vec{x}$ of p, $f(x') = 0$ as well.

There is a really strong connection between affine and projective varieties. We can go from affine space to projective space by the following homogenization:

Definition B.9. If $F(X_1, \ldots, X_n) \in \mathbb{A}^n$ has degree d, then

$$F^*(X_1, \ldots, X_{n+1}) = X_{n+1}^d F\left(\frac{X_1}{X_{n+1}}, \ldots, \frac{X_n}{X_{n+1}}\right). \tag{417}$$

Moreover, $I^* = \{\, F^* \mid F \in I \,\}$ is the homogeneous ideal of I.

That this definition is in fact 'right', is shown as well by this proposition:

Proposition B.10 (Prop. 4.3 (3), [Ful08])**.** *If V is irreducible in $\mathbb{A}^n$, then V^* is irreducible in $\mathbb{P}^n$.*

Furthermore, there is a connection between ideals and algebraic sets:

Corollary B.11 ([Ful08, Corollary 1.7.2])**.** *If $I \subset k[X_1, \ldots X_n]$ is a prime ideal, then $V(I)$ is an irreducible (affine) algebraic set.*

B.2 Dimensions

We can see varieties as spaces with dimensions as well, even though they are over a finite field. However this definition is based on a topological property for which we will first need to find a topology on algebraic sets. To begin, we observe that zero-loci satisfy:

Proposition B.12 ([Har77, I, Prop. 1.1])**.** *The union of two algebraic sets is an algebraic set.*

The intersection of any family of algebraic sets is an algebraic set.

The empty set and the whole space are algebraic sets.

Now remembering the axioms of a topological space, the complement of algebraic sets satisfy this and allows us to define a topology on the collection of algebraic sets:

Definition B.13 ([Har77, I, p. 2])**.** We define the Zariski topology on $\mathbb{A}^n$ by taking the open subsets to be the complements of the algebraic sets. This is a topology, because according to the proposition, the intersection of two open sets is open, and the union of any family of open sets is open. Furthermore, the empty set and the whole space are both open.

Definition B.14 ([Har77, I, p. 5])**.** If X is a topological space, we define the dimension of X (denoted $\dim X$) to be the supremum of all integers n such that there exists a chain

$$Z_0 \subset Z_1 \subset \ldots \subset Z_n \tag{418}$$

of distinct irreducible closed subsets of X.

We define the dimension of an algebraic set to be its dimension as a topological space.

Note that this is based on the fact that any subset of a topological space gives to the restricted topological space. As an example to make this definition clear:

Example B.15 ([Har77, I, 1.6.1])**.** The dimension of $\mathbb{A}^1$ is 1. Indeed, the only irreducible closed subsets of $\mathbb{A}^1$ are the whole space [that is, $\mathbb{A}^1$] and single points.

Furthermore, we speak of a 'curve' when an algebraic set has a dimension of one.

We would like to give the following example as well:

Example B.16. $\mathcal{C}$: $X - Y = 0$ over $\mathbb{A}^2$ is a curve.

We will show that $\dim(\mathcal{C}) = 1$. First, observe that there exists a chain of length $n = 1$:

$$\{\,(0,0)\,\} = Z(X,Y) \subset Z(X-Y) = \mathcal{C}. \tag{419}$$

Thus, $\dim(\mathcal{C}) \geq 1$.

Now suppose there exists a chain $Z_0 \subset Z_1 \subset Z_2 \subseteq \mathcal{C}$. Then by the reverse-inclusion relation of [Gat14, Lemma 1.12] we see that

$$I(Z_0) \supsetneq I(Z_1) \supsetneq I(Z_2) \supseteq (X - Y) \tag{420}$$

Furthermore, every $I(Z_i)$, $(0 \leq i \leq 2)$ must be a prime ideal ([Har77, I, Cor. 1.4])*.*. Now since $I(Z_1) \supsetneq (X - Y)$, there must be some polynomial

$F \in I(Z_1)$ such that $F \in k[Y]$. For suppose some $F \in I(Z_1)$ then we can write this as

$$F(X,Y) = X^m R_m(Y) + X^{m-1} R_{m+1}(Y) + \cdots + R_0(Y). \tag{421}$$

Now if there exists an F with a given $m \geq 1$, then

$$G(X,Y) = F(X,Y) + (Y - X)X^{m-1} R_m(Y) \tag{422}$$

is a polynomial with highest power of X at most $m-1$. Thus by induction we can find eventually a polynomial $H(X,Y) \in k[Y] \cap I(Z_1)$.

Now we know that $H(Y) \notin k$ because this implies $I(Z_1) = k[X,Y]$ contradicting the chain property (420). Thus $H(Y)$ is an irreducible polynomial in $k[Y]$ since $I(Z_1)$ is a prime ideal in $k[X,Y]$ and thus in $k[X][Y]$ as well.

But now, $I(Z_0) \supsetneq I(Z_1)$ and thus there is a different $J(Y) \in I(Z_0) \setminus I(Z_1)$. And by the euclidean method, there exist $Q(Y) \in k[Y], R(Y) \neq 0$ such that $H(Y) = Q(Y)J(Y) + R(Y)$. However, if for some $y \in k$, $J(y) = 0$, then, $H(y) = R(y) \neq 0$ since $R(y)$ was irreducible. We conclude that $Z_0 = \emptyset$ which contradicts that this chain could exist.

Therefore, $\dim(\mathcal{C}) = 1$.

Definition B.17 ([Har77, I, Ex. 2.17])**.** Let Y be an algebraic set of dimension r in $\mathbb{P}^n$. We say Y is a 'complete intersection' if $I(Y)$ can be generated by $n - r$ elements.

In [BH14, lemma 3.2] the notion of nonsingularity is used to show that a projective algebraic set $\mathcal{C}$ is a complete intersection. Nonsingularity is the following:

Definition B.18 ([Har77, I, p. 32])**.** Let $Y \subset \mathbb{A}^n$ be an affine algebraic set of dimension r, and let $f_1, \ldots f_r \in k[X_1, \ldots, X_n]$ be a set of generators for $I(Y)$. Y is 'nonsingular at a point $P \in Y$', if the rank of the matrix

$$\|(\partial f_i / \partial x_j)(P)\| \tag{423}$$

is $n - r$.

Y is nonsingular if it is nonsingular at every point.

B.3 Hasse-Weil bound

In this section, let us consider a non-singular n-dimensional projective irreducible curve $\mathcal{C}$ over $\mathbb{F}_q$ of genus g. The genus g is some invariant of a curve which tells much about the type of curve, but we will not go into detail on what this is.

In algebraic geometry, the Weil conjectures are statements concerning the generating function on $\#\mathcal{C}(\mathbb{F}_{q^r})$, the number of solutions on the curve $\mathcal{C}$ in a finite field extension $\mathbb{F}_{q^r}$ of $\mathbb{F}_q$. In particular, according to [Bom74],

$$\#\mathcal{C}(\mathbb{F}_{q^r}) = q^r - \sum_{i=1}^{2g} \omega_i^r + 1 \tag{424}$$

where ω_i are algebraic integers, not depending on r.

Now Weil's conjectures consist of multiple statements, one of them being that

$$|\omega| = \sqrt{q}. \tag{425}$$

This was proposed André Weil in [Wei49], and is called Weil's Riemann hypothesis. This statement appeared to be the hardest of the Weil conjectures but was later proven by Deligne in [Del74].

Using equations (424) and (425), we can derive the following bound on the number of points in $\mathcal{C}$:

$$|\#\mathcal{C}(\mathbb{F}_{q^r}) - (q^r + 1)| \leq \left| \sum_{i=1}^{2g} \omega^r \right| \leq 2g\sqrt{q^r}, \tag{426}$$

which is know as the Hasse-Weil bound. Now by simply taking $r = 1$, we get

$$|\#\mathcal{C}(\mathbb{F}_q) - (q + 1)| \leq 2g\sqrt{q}. \tag{427}$$

References

[AKS04] Manindra Agrawal, Neeraj Kayal, and Nitin Saxena. Primes is in p. *Annals of mathematics*, pages 781–793, 2004.

[Bac91] Eric Bach. Toward a theory of pollard's rho method. *Information and Computation*, 90(2):139–155, 1991.

[Beu17] Frits Beukers. Rings and galois theory (lecture notes), 2017.

[BH14] T. D. Browning and D. R. Heath-Brown. Forms in many variables and differing degrees. *ArXiv e-prints*, March 2014.

[Bom74] Enrico Bombieri. Counting points on curves over finite fields. In *Séminaire Bourbaki vol. 1972/73 Exposés 418–435*, pages 234–241, Berlin, Heidelberg, 1974. Springer Berlin Heidelberg.

[Cas89] G. Castelnuovo. Ricerche di geometria sulle curve algebriche. *Atti Reale Accademia delle Scienze di Torino*, pages 346–373, 1889.

[Del74] Pierre Deligne. La conjecture de weil. i. *Publications Mathématiques de l'Institut des Hautes Études Scientifiques*, 43(1):273–307, 1974.

[Ful08] William Fulton. *Algebraic curves, An Introduction to Algebraic Geometry*. Addison-Wesley, January 2008.

[Gat14] Andreas Gathmann. Algebraic geometry, class notes, 2014.

[Har77] Robin Hartshorne. *Algebraic geometry*. Springer, 1977.

[Hea17] D. R. Heath-Brown. Iteration of Quadratic Polynomials Over Finite Fields. *ArXiv e-prints*, January 2017.

[JB12] Rafe Jones and Nigel Boston. Settled polynomials over finite fields. *Proceedings of the American Mathematical Society*, 140(6):1849–1863, 2012.

[Jon07] Rafe Jones. Iterated galois towers, their associated martingales, and the p-adic mandelbrot set. *Compositio Mathematica*, 143(5):1108–1126, 2007.

[Juu17] Jamie Juul. The image size of iterated rational maps over finite fields. *ArXiv e-prints*, June 2017.

[Knu81] Donald E Knuth. *The Art of Computer Programming; Volume 2: Seminumeral Algorithms*. Addison-Wesley, 1981.

[LJP02] Hendrik W Lenstra Jr and Carl Pomerance. Primality testing with gaussian periods. In *FSTTCS*, page 1, 2002.

[Mil76] Gary L. Miller. Riemann's hypothesis and tests for primality. *Journal of Computer and System Sciences*, 13(3):300 – 317, 1976.

[OS10] Alina Ostafe and Igor Shparlinski. On the length of critical orbits of stable quadratic polynomials. *Proceedings of the American Mathematical Society*, 138(8):2653–2656, 2010.

[Pol75] John M Pollard. A monte carlo method for factorization. *BIT Numerical Mathematics*, 15(3):331–334, 1975.

[Pom10] Carl Pomerance. Primality testing: variations on a theme of lucas. *Congr. Numer*, 201:301–312, 2010.

[Rab80] Michael O Rabin. Probabilistic algorithm for testing primality. *Journal of Number Theory*, 12(1):128 – 138, 1980.

[RSA78] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM*, 21(2):120–126, February 1978.

[Sch06] Wolfgang M Schmidt. *Equations over finite fields: an elementary approach*, volume 536. Springer, 2006.

[Sch08] R. Schoof. Four primality testing algorithms. *ArXiv e-prints*, January 2008.

[SS71] A. Schönhage and V. Strassen. Schnelle multiplikation großer zahlen. *Computing*, 7(3):281–292, Sep 1971.

[Tsc50] N. G. Tschebotarev. *Grundzüge der Galois' schen Theorie* (*translated from Russian by H. Schwerdtfeger*). Noordhoff, 1950.

[Wei49] André Weil. Numbers of solutions of equations in finite fields. *Bulletin of the American Mathematical Society*, 55(5):497–508, 1949.