The Raymond and
Beverly Sackler Faculty
of Exact Sciences
Tel Aviv University

On the Distribution of Symbols in Codewords of Algebraic-Geometric Codes

Tel-Aviv University
Raymond & Beverly Sackler Faculty of Exact Sciences

This work is submitted as part
of the requirements for the degree
“Master of Science”

School of Mathematical Sciences

By
Kedem Yakirevitch

Under the supervision of
Professor Amnon Ta Shma

The Raymond and
Beverly Sackler Faculty
of Exact Sciences
Tel Aviv University

On the Distribution of Symbols in Codewords of Algebraic-Geometric Codes

Tel-Aviv University
Raymond & Beverly Sackler Faculty of Exact Sciences

This work is submitted as part
of the requirements for the degree
“Master of Science”

School of Mathematical Sciences

By
Kedem Yakirevitch

Under the supervision of
Professor Amnon Ta Shma

Acknowledgements

I would like to thank my advisor, Professor Ta-Shma for his support, his continued passion for research, and great help in refining my understanding of the field.

I would also like to thank Professor Kopparty for many innovative ideas and fruitful discussions, as well as pointing us to very useful references.

Table of contents

Abstract

Algebraic Geometric Codes, or Goppa codes, denoted C(D,G), are error correcting codes that generalize the Reed-Solomon codes. They are linear codes over the field $\mathbb{F}_q$. A codeword is defined for every function in the Riemann-Roch space associated with the divisor G. given such f, the codeword includes the value of f at each of the points on the curve included in the divisor D.

Algebraic Geometric codes are an important construction in Theoretical Computer Science since they were an important step to our understanding of the trade-off between rate and distance of error correcting codes over fields of size at least 49.

This work deals with the problem of proving bounds on the distribution of the symbols of $\mathbb{F}_q$ that appear in a codeword by bounding the probability of events of the form ‘a random symbol from the word belongs to a specific subset of $\mathbb{F}_q$’. We choose the sets that define these events to have algebraic significance, thus enabling us to prove bounds via the counting of points on certain algebraic curves.

The need to count points on curves begs the use of powerful tools from Algebraic Geometry such as the Weil Bound. However, the curves that are relevant to the construction of Algebraic Geometric Codes typically have a large genus, which makes the classical results yield only trivial bounds.

In this work we use elementary tools to bound the number of codeword symbols that are ℓ-th powers in the multiplicative subgroup of $\mathbb{F}_q$. We generalize the Stepanov Method introduced in 1969. Adapting it to work over curves other than the projective line requires basic tools from the theory of function fields as well as carful description of the structure we require from the function fields we work with.

1 Introduction

This work deals with the problem of proving bounds on character sums over function fields. One typical example of such character sums is the following classic theorem:

Theorem 1.1. *(Weil) Let $f \in \mathbb{F}_q[x]$ be a non-square polynomial of degree d, and χ the quadratic residue character (i.e., $\chi(a)$ is 0 if $a = 0$, 1 if a is a square and -1 otherwise). Then*

$$|\sum_{a \in \mathbb{F}_q} \chi(f(a))| \leq O(d\sqrt{q}).$$

One way to prove Theorem 1.1 is the following. Our starting point is the Hasse-Weil bound:

Theorem 1.2. *(Hasse-Weil Bound [Sti09, Theorem 5.2.3]) The number N_1 of places of degree one on a curve over $\mathbb{F}_q$ with genus g is at most*

$$N_1 \leq q + 1 + 2g\sqrt{q}$$

Having the Hasse-Weil bound, we define the curve $\mathbb{F}_q(X, Z) \mod (Z^2 - f(X))$. Note that the number of rational points on the curve is about twice the number of points x such that $\chi(f(x)) = 1$. The genus of this curve is $O(d)$. It therefore follows that this number is at most $\frac{q}{2} + O(d\sqrt{q})$. Multiplying f by a non-square, gives a bound on the number of non-residues, and together we see that the number of residues and non-residues is almost balanced, and therefore their bias (which is captured by $|\sum \chi(f(x))|$) is bounded by $O(d\sqrt{q})$.

One can generalize the approach to low-genus general function fields (the above example was for the genus zero rational function field), but the approach fails when trying to work with high genus function fields.

In 1969 Stepanov [Ste69] published an elementary proof of a slightly weaker version of some specific cases of the Hasse-Weil bound, and this was later generalized by Bombieri [Bom06] to give:

Theorem 1.3. *(Stepanov-Bombieri version of the Hasse-Weil Bound (Taken from [Tao14])) The number N_1 of degree one places on a curve over $\mathbb{F}_q$ with genus g is at most*

$$N_1 \leq q + 1 + (2g + 1)\sqrt{q}$$

when q is a prime power square and $q \geq (g + 1)^4$.

In this work we use the Stepanov-Bombieri method directly, to prove a character sum bound over function fields of very high genus. Our results do no use the method as a black-box, as we have already mentioned that even the tight Hasse-Weil bound does not suffice. Instead, we show that for a certain (natural) class of function fields, the technique can be used to directly bound the character sum. In Section 4 we explain what function fields are captured, and the bound that we get. We demonstrate our result with an example:

Theorem 1.4. *Let C be the Hermitian curve $\mathbb{F}_q(x,y) \mod (y^p + y - x^{p+1})$ where $q = p^2$. Let $f(x,y)$ be a polynomial with odd valuation at P_∞ and total degree $d < \frac{p}{2}$. Let χ be the quadratic residue character. Then $|\sum_{x \in C} \chi(f(x))| \leq O(\sqrt{d}p^{2.5})$.*

Notice that the bias is $o(N_1)$ (when we think of p as going to infinity) proving that for any such f, the residues and non-residues are almost balanced.

Our techniques generalize to many other function fields, including, e.g., the Garcia-Stichtenoth curve $\mathrm{F}_q(x,y) \mod (y^p + y - \frac{x^p}{x^{p-1}+1})$, the Hermitian tower, the Garcia-Stichtenoth tower and more.

1.1 More about the technique

In the polynomial method, we want to bound the number of elements with some combinatorial property. We do that by presenting a (low-degree) polynomial Q such that all these elements can be derived from Q (e.g., they are roots of Q). For example, suppose we are given as input a set $\{(a_i, b_i) \in \mathbb{F}_q \times \mathbb{F}_q\}$ and we want to bound the number of degree d polynomials $p \in \mathbb{F}_q[X]$ such that $f(a_i) = b_i$ for at least A values i. The Guruswami-Sudan algorithm [GS98] does that by first finding a low-degree polynomial $Q \in \mathbb{F}_q[X,Y]$ such that Q vanishes with high multiplicity over all points (a_i, b_i) in the set, and then proves that every solution f gives a factor $y - f(x)$ of Q. The Guruswami-Sudan algorithm can explicitly finds these solutions.

The Stepanov method is similar, except that the polynomial Q has to vanish with high multiplicity over a variety, rather than just an arbitrary set. For example, this variety might be the set of (x,y) such that $y^2 = f(x)$. In the polynomial method, one usually has independent constraints per different points. However, it is usually cheaper to enforce that Q vanishes as a polynomial over the variety, and this is a key ingredient in Stepanov's method.

In this work we want to count the number of points $P \in C$, such that $f(P)$ is a non-zero square. As before, this corresponds (up to a factor of 2) to the number of points on the curve $F' = F(Z)$ where $Z^2 = F$. We want to use the Stepanov method to find a Q that vanishes with high multiplicity on the rational points of F'. This is fairly straight forward when F is the rational function field. However, when F is a large genus function field, things get complicated. To begin with, one needs to have derivatives in the function field, and the theory behind this is well studied and well understood. However, while derivatives in function fields share many properties with derivatives over the rational function field, many essential differences exist. For example, the degree of the derivative might be much larger than the degree of the original function. These differences are responsible for many of the complications that arise. To overcome these difficulties, we employ a general, powerful tool relating the pole divisor of the derivatives of $f \in F$ with the pole divisor of f. We prove:

Theorem 1.5. *Let F be a function field of genus g, and $x \in F$ a separating element of F. There exists $\omega \in F$ such that for every $f \in F$ with poles only at P_∞ and pole order at most A, the derivative of f with respect to x, denoted $D_x(f)$, satisfies:*

- *$\omega D_x(f)$ has poles only at P_∞*
- *The pole order of $\omega D_x(f)$ is at most $A + 3g - 2 + 2\deg(x)$*

We are unaware of previous results of this form, even though it may well be the case that such results exist unbeknownst to us.

Many problems are left open. For example, we suspect that the $3g$ term in Theorem 1.5 should really be $2g$. Also, we do not know what is the true error term in Theorem 1.4, for example, it might be that under natural conditions on f, the error is bounded by $O(d\sqrt{N_1})$. Even more crucial is to generalize the Hermitian curve bound to degrees d above p, or for general curves to work with functions coming from Riemann spaces above the genus. We remark that such improvements might have far reaching consequences to the construction of explicit Binary error correcting codes close to the Gilbert-Varshamov bound.

The thesis organized as follows: In Section 2 we give an informal introduction to algebraic function fields, trying to focus on derivatives and differentials, and we also decribe the notation used throughout the thesis. In Section 3 we state and prove a generalization of Theorem 1.5. Then, in Section 4 we state the problem, specify the properties required from the function field, and state the result we obtain. In Sections 5 and 6 we prove the result itself.

2 Introduction to function fields and derivatives

In this section we give some background on algebraic function fields and introduce the notations that will be used throughout the paper. Our goal is to give an intuitive explanation of the mathematical objects and ideas. For a complete formal treatment of the subject we refer the interested reader to [Sti09].

The *rational function field* $K(x)$ is the field extension of K with a transcendental element x. A *function field* F/K is a finite extension of the rational function field $K(x)$[1]. For example, the Hermitian function field is $F = F_q(x,y) \bmod \phi(x,y)$, where $q = p^2$, p is a prime power and $\phi(x,y) = \mathsf{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(y) - N_{\mathbb{F}_q/\mathbb{F}_p}(x) = y^p + y - x^{p+1}$.

A place of F/K is analogous to a "point" at which we can "compute" or "evaluate" the elements $f \in F$. Let us take the rational function field $K(x)$ as example. For every $\alpha \in K$ there is a place P_α corresponding to $x-\alpha$ and if f has no pole at α then $f(P_\alpha) \overset{\text{def}}{=} f \bmod (x-\alpha) = f(\alpha)$. Another place is P_∞, where $\frac{f}{g}$ has a pole at P_∞ if $\deg(f) > \deg(g)$ and if $\frac{f}{g}$ does not have a pole at P_∞, its value can be computed by dividing the leading coefficients of f and g. There are more places of the rational function field $K(x)$: every irreducible polynomial $h \in K[x]$ has a corresponding place P_h where $f(P_h) \overset{\text{def}}{=} f \bmod h$. For example, in the rational function field $\mathbb{R}(x)$, evaluating f at the place P_{x^2+1}, corresponds to taking $f(x) \bmod (x^2+1)$ and this can be interpreted as $f(i) \in \mathbb{C}$, where $\mathbb{C}$ is the complex field $\mathbb{R}[x] \bmod (x^2+1)$. We say a place P has *degree* r, if the evaluation of elements $f \in F$ at P returns an element in a degree-r field extension of K. For example, the degree of P_{x^2+1} as a place of $\mathbb{R}(x)$ is 2, because it returns values in $\mathbb{C}$. If F/K is a function field, we let $\mathbb{P}_F$ denote the set of all places of F.

[1] We will only be concerned with the case where K is a perfect field. We will always assume K is perfect without restating this assumption.

Formally, a place P of a function field is a maximal ideal I of a valuation ring R of F, where R contains all elements of F without a pole at the place, and the maximal ideal I of R contains all elements of F that vanish at the place. We can now define an "evaluation function" $\phi_P : R \to (R \bmod I)$, which is called the *residue class map* of P, defined by $\phi_P(f) = f(\text{mod } I)$. ϕ_P returns values in the *residue class field* R/I which is isomorphic to a finite extension of the base field K. The degree of this extension is called the *degree* of P and denoted $\deg(P)$. For convenience, we sometimes call the residue class map ϕ_P an *evaluation function*, or simply an evaluation, and use the notation $f|_P \overset{\text{def}}{=} \phi_P(f)$.

With this in mind, we can think of elements in F as functions from $\mathbb{P}_F$ to finite extensions of K (or ∞ if the function has a pole at the place). A function $f \in F$ is *defined* at P if it belongs to the valuation ring R and then $f|_P$ is an element in the residue class field. If f is not defined at P we let $f|_P = \infty$.

When the function field is defined as the extension $F = K(x, y)/\varphi(x, y)$ of $K(x)$, any point $(\alpha, \beta) \in K \times K$ on the curve (i.e., $\varphi(\alpha, \beta) = 0$) has an associated degree one place $P = P_{\alpha,\beta}$. One can see it is a degree one place by noticing that $\phi_P(x) = \alpha$ and $\phi_P(y) = \beta$ and therefore ϕ_P returns elements in K. Thus, we can associate points on the (algebraic) curve with degree one places of the function field.

Naturally, given $f \in F$ and $P \in \mathbb{P}_F$, we are interested in the number of zeroes or poles f has at P. Formally, for every place P there is a *valuation* function $v_P : F \to \mathbb{Z} \cup \{\infty\}$ that counts the number of zeroes of f at P, namely $v_P(f) = k > 0$ means f has exactly k zeroes at P, $v_P(f) = k < 0$ means f has exactly k poles at P and $v_P(f) = 0$ means f has neither a zero nor a pole at P, and therefore $f(P)$ is a non-zero element in some extension field (of degree $\deg(P)$) of K. Also $v_P(0) = \infty$ for all places P.

An important fact is that every $0 \neq f \in F$ has a finite number of zeroes and poles, and furthermore the number of zeroes f has is the same as the number of poles when counted appropriately. For example, a degree r polynomial $f \in K[x]$ can have at most r zeroes and has exactly r poles at P_∞. The fundamental theorem of Algebra tells us that f has exactly r zeroes over the algebraic closure of K, and, in fact, this is true for any field K, not necessarily algebraically closed, if we count zeroes appropriately, i.e., accounting for the degree of places and multiplicity of roots. We denote this number of zeroes (or poles) of f by $\deg(f)$. It turns out that $\deg(f) = [F : K(f)]$ (see, [Sti09, Thm 1.4.11]).

We mention a few properties of valuations. Let F/K be a function field and v a valuation of F/K. Then:

- $v(f)$ is finite for $f \neq 0$ and $v(0) = \infty$.
- There exists an element $f \in F$ with $v(f) = 1$.
- $v(c) = 0$ for every element $0 \neq c \in F$ that is algebraic over K (and, in particular, for every $0 \neq c \in K$).

In fact, the functions that do not have any zeroes at all are exactly the elements $c \in F$ that are algebraic over K. These are called the *constants* of F/K and they form a field, the *field of constants* of F/K. We will assume K is algebraically closed in F and so the only constant functions are the elements of K. Also,

- $v(fg) = v(f) + v(g)$ and $v(\frac{1}{f}) = -v(f)$,
- $v(f+g) \geq min\{v(f), v(g)\}$ and if $v(f) \neq v(g)$ then $v(f+g) = min\{v(f), v(g)\}$ (this property is called the strict triangle inequality). More generally,

Corollary 2.1. *Let F/K be a function field and v a valuation of F/K, and let $0 \neq f_i \in F$ for $0 \leq i \leq M$ be nonzero elements in F. Suppose $v(f_i) \neq v(f_j)$ whenever $i \neq j$, then $v(\sum_{i=0}^{M} f_i) = min_i\{v(f_i)\}$ and in particular $v(\sum_{i=0}^{M} f_i) \neq \infty$ and so $\sum_{i=0}^{M} f_i \neq 0$*

A *divisor* is a formal sum of a finite number of places with integer coefficients. The divisors of F/K, denoted $Div(F)$, form an abelian group. We say the degree of a divisor $D = \sum_P d_P P$ is $\deg(D) = \sum_P d_P \deg(P)$. Each non-zero function $f \in F$ has an associated divisor $(f) = \sum_P v_P(f)P$ because it has a finite number of zeroes and poles, and $\deg((f)) = 0$ since f has the same number of zeroes and poles. We denote by $(f)_0$ and $(f)_\infty$ the zero-divisor and pole-divisor of f respectively so that $(f) = (f)_0 - (f)_\infty$. A non-zero function f is defined by its divisor up to multiplication by a constant (an element of K) because if $(f) = (g)$ then $(f/g) = (f) - (g) = 0$ and therefore f/g is a constant.

The *Riemann-Roch space* of a divisor $D = \sum_P d_P P$, is defined as

$$\mathcal{L}(D) = \{f \in F \mid \forall P \in \mathbb{P}_F, \quad v_P(f) \geq -d_P\},$$

i.e., $\mathcal{L}(D)$ contains all the functions $f \in F$ that have at most d_P poles at P when $d_P > 0$, and at least $-d_P$ zeroes at P when $d_P \leq 0$. For example, in the rational function field $K(x)$, $\mathcal{L}(n \cdot P_\infty)$ contains only polynomials in x (because it does not allow poles outside P_∞) and among the polynomials in $K[x]$ it contains only polynomials of degree at most n (because it allows at most n poles at P_∞). As another example, $\mathcal{L}(n \cdot P_\infty - 1 \cdot P_0)$ contains the polynomials of degree at most n that vanish at the point $x = 0$.

We can think about divisors as putting constraints on functions. The degree of a divisor D is the difference between then number of poles it allows and the number of zeroes it forces. We would have liked to think of it as the number of degrees of freedom it allows. The actual number of degrees of freedom is the dimension of $\mathcal{L}(D)$, also called the dimension of D. Thus, a natural question is what is the relationship between $\deg(D)$ and $\dim(\mathcal{L}(D))$?

To begin with, if $\deg(D) < 0$, then $\dim(\mathcal{L}(D)) = 0$. In particular, if an element $f \in F$ has at most A poles and at least $A+1$ zeroes, then $f = 0 \in F$. A useful alternate phrasing of this is:

Claim 2.2. *If $f \in F$ is non-zero and has at most A poles, then it has at most A zeroes.*

Also, if $\deg(D) \geq 0$ we have $\dim(\mathcal{L}(D)) \leq \deg(D) + 1$.

The Riemann-Roch theorem states that for any function field F/K there is a fixed quantity, called the *genus* of F/K and denoted genus(F), which gives an upper bound on the number of "holes" we may have, i.e., for any divisor D, $\dim(\mathcal{L}(D)) \geq \deg(D)+1-g$. Furthermore, there is a special class of divisors, called *canonical divisors*, all of which have degree $2g-2$, such that:

Theorem 2.3. *(The Riemann Roch Theorem) [Sti09, Thm 1.5.15]. Let D be a divisor of a function field of genus g and let W be any canonical divisor, then*

$$\dim(\mathcal{L}(D)) = \deg(D) + 1 - g + \dim(\mathcal{L}(W - D))$$

In particular:

- if $\deg(D) \geq g$ we have $\dim(\mathcal{L}(D)) \geq \deg(D) + 1 - g > 0$,
- if $\deg(D) \geq 2g - 1$ we have $\dim(\mathcal{L}(D)) = \deg(D) + 1 - g$.

We will get back to canonical divisors in Section 2.2.

In the rational function field, the genus is zero, and therefore the dimension of $\mathcal{L}(D)$ is equal to $\deg(D)+1$ as long as $\deg(D)$ is non-negative. In the Hermitian function field, the genus is $g = \frac{p(p-1)}{2}$. For example, for the divisor $D = (p^2-p-1)\cdot P_\infty$ we have $\deg(D) = p^2-p-1 = 2g-1$ and

$$\mathcal{L}(D) = \mathsf{Span}\left\{x^i y^j \mid pi + (p+1)j < p(p-1)\right\}$$

with dimension $g = \frac{p(p-1)}{2}$, and we indeed see that $\dim(\mathcal{L}(D)) = \deg(D) - g + 1$. For an example where the difference between the degree and the dimension is not $g-1$ we can take $D = kP_\infty$ for $0 \leq k < p$, then $\deg(D) = k$ while $\mathcal{L}(D)$ contains only the constant functions and is spanned by 1, so $\dim(\mathcal{L}(D)) = 1$.

2.1 Hasse derivatives

In calculus and in polynomial rings over fields we have a notion of derivatives which is useful for studying the multiplicity of zeroes of polynomials. Similarly, in function fields we can derive with respect to any separating element of F/K[2]. We denote by $D_z : F \to F$ the derivative with respect to z. These derivatives are K-linear and adhere to most rules we know from calculus:

- $D_z(z) = 1$,
- $D_z(xy) = xD_z(y) + yD_z(x)$,
- $D_z(c) = 0 (\forall c \in K)$,
- $D_z(x^p) = 0$, where p is the characteristic of F,
- $D_z(x) = D_y(x)D_z(y)$ whenever $y \in F$ is also separating.

We denote $D_z^m = (D_z)^m$ the m-th *iterated derivative* with respect to z. Note that D_z in F is an extension of the formal derivative in $K[z]$ and $K(z)$.

In complex analysis, where $F = \mathbb{C}(Z)$, iterated derivatives have a close relationship with multiplicity of zeroes. Namely, f has a zero of multiplicity at least m at a point x_0 if and only if the first m derivatives $D_z^0(f) = f, D_z^1(f) = f'..., D_z^{m-1}(f)$ all vanish at that point. This behavior breaks down when the

[2] $z \in F$ is called *separating* if the extension $F/K(z)$ is separable. In a function field F/K with characteristic $p \neq 0$ the non-separating elements are exactly the constant functions and the elements z s.t. $z = y^p$ for some $y \in F$.

characteristic is $p > 0$. For example, suppose $F = F_p(Z)$ and $f \in F$ is some non-constant function and look at $g = f^p$. Clearly, g has a bounded number of zeroes. However, $D_z^1(g) = D_z^1(f^p) = 0$ and therefore the iterated derivatives $D_z^m(f^p)$ are all zero for all $m > 0$. Thus, the number of vanishing derivatives does not give accurate information about the multiplicity of zeroes of $g = f^p$.

One way to think of the derivatives of an element f in the complex rational function field $\mathbb{C}(Z)$ is using Taylor expansion, which tells us that if f is a rational function then $f(z+u) = \sum_{m=0}^{\infty} \frac{D_z^m(f)}{m!} u^m$. The Hasse derivative $H_z^m(f)$ of $f \in \mathbb{C}(Z)$ is defined to be the coefficient function of u^m in the Taylor expansion $f(z+u) = \sum_{m=0}^{\infty} \frac{D_z^m(f)}{m!} u^m$, i.e., $D_z^m(f) = m! \cdot H_z^m(f)$. This idea also extends to rational function fields over finite fields: For $f \in F_p(Z)$, $f(z+u) = \sum_{m=0}^{\infty} h_m(z) u^m$, and the Hasse derivative is defined to be $H_z^m(f) = h_m(z)$. It is immediate that with this definition of Hasse derivative, if the first m Hasse derivatives of f vanish at some point x_0, then f has a zero of multiplicity at least m at x_0.

Notice that for $m = 1$ the Hasse derivative $H_z^1(f)$ coincides with $D_z^1(f)$, and for larger m they differ by a constant multiplicative factor of $m!$. The main point is that in finite characteristic $H_z^m(f)$ might be non-zero even though $D_z^m(f) = 0$, simply because $m! = 0$. The (minor) price we pay for working with Hasse derivatives rather than iterated derivatives is that iterating Hasse derivatives does not give a Hasse derivative.

In fact, this idea also generalizes to any function field F/K. Let F/K be a function field and $z \in F$ separating[2]. The m-th Hasse derivative with respect to z, denoted by H_z^m, is defined on $K[z]$ by the K-linear extension of $H_z^m(z^n) \triangleq \binom{n}{m} z^{n-m}$ to all of $K[z]$. H_z^m can be uniquely extended to all of F/K so that they satisfy:

1. $H_z^0 = id_F$
2. H_z^m vanish on K for all $m > 0$
3. $H_z^m(fg) = \sum_{j=0}^{m} H_z^j(f) H_z^{m-j}(g)$ (Product Rule)
4. $H_z^m \circ H_z^n = \binom{m+n}{m} H_z^{m+n}$ (Composition Rule)

These uniquely determined extensions are called the *Hasse derivatives.* A consequence of these properties is that

Corollary 2.4. *Let F/K be a function field of characteristic p and let z be a separating element. Then:*

$$m!H_z^m = D_z^m$$

where D_z^m is the iterated derivative and H_z^m is the m-th Hasse derivative. In particular, when $p = 0$ or when $p > 0$ and $m < p$ we get that H_z^m and D_z^m differ by a non-zero constant, and so $H_z^m(f) = 0$ if and only if $D_z^m(f) = 0$.

The fact that Hasse derivatives capture multiplicity is given in the following claim, which is an immediate corollary of [Gol03, Corollary 2.5.14 (Taylor's Theorem)],

Claim 2.5. *Let P be a place in F/K and let t be a separating element with $v_P(t) = 1$. Let $f \in F$ and $M \in \mathbb{N} \setminus \{0\}$, then*

$$v_P(f) \geq M \Longleftrightarrow \forall m < M \quad (H_t^m(f))(P) = 0.$$

For example, take $f = x^4(x+1)^2 \in \mathbb{F}_2(x)$. It is a square and so its derivative is identically 0, but by expanding it with respect to x and again with respect to $x+1$ we have $f = 1 \cdot x^4 + 1 \cdot x^6$ and $f = 1 \cdot (x+1)^2 + 1 \cdot (x+1)^6$ and by the coefficients it is clear that f has a double zero at $x = 1$ but a quadruple zero at $x = 0$. Let us name the places at $x = 0$ and $x = 1$ as P_0, P_1. Indeed, we find out that $H_x^1(f) = H_{x+1}^1(f) = 0$ and $H_{x-1}^2(f) = H_x^2(f) = x^4$. Thus, f vanishes exactly twice at P_1 and at least thrice at P_0. Further computing H_x^3 and H_x^4 shows f has exactly four zeroes at P_0. The reader might have noticed our computations yielded $H_x^1(f) = H_{x+1}^1(f)$ and $H_x^2(f) = H_{x+1}^2(f)$. This is not a coincidence, but in fact a special case of a more general truth (see Corollary 2.7 below).

Claim 2.6 (Chain Rule for Rational Functions)**.** *(see [Jeo11, Chain rule II]) Let f, g be two rational functions over K and consider $f(z), g(f(z))$ as elements of the function field $K(z)/K$. Then:*

$$H_z^m(g(f(z))) = \sum_{k=1}^{m} H_{f(z)}^k(g(f(z))) \sum \binom{k}{i_1, i_2, ..., i_m} (H_z^1(f))^{i_1} ... (H_z^m(f))^{i_m}$$

where the inner sum goes over $i_1, ... i_m \in \mathbb{N}$ with $i_1 + ... + i_m = k$ and $i_1 + 2i_2 + ... + mi_m = m$, where $\binom{k}{i_1, i_2, ..., i_m} = \frac{k!}{i_1! i_2! ... i_m!}$ is the multinomial coefficient.

For an analogous claim in a general function field we refer the reader to [Tor00, equation 2.4]. From the above claim we get:

Corollary 2.7 (Simple change of variable)**.** *Let z be a separating element in F/K, let $f \in F$ and $\alpha \in K$, then for every $m > 0$*

$$H_z^m(f) = H_{z-\alpha}^m(f)$$

Proof. It suffices to prove $H_z^m(f) = H_{z-\alpha}^m(f)$ in $K(z)/K$, since the extension of $H_z^m(f)$ in $K(z)/K$ to F is unique, so if $H_z^m(f) = H_{z-\alpha}^m(f)$ holds in $K(z)/K$ it also holds in F. Now let f be a rational function in z, and define $g(z) = f(z+\alpha)$ and $h(z) = z - \alpha$. Now we apply claim 2.6 to $f(z) = g(h(z))$ to get:

$$\begin{aligned} H_z^m(f) &= H_z^m(g(h(z))) \\ &= \sum_{k=1}^{m} H_{z-\alpha}^k(f) \sum \binom{k}{i_1, i_2, ..., i_m} (H_z^1(h))^{i_1} ... (H_z^m(h))^{i_m} \end{aligned}$$

noting that $H_z^j(h) = 0$ for $j > 1$ and $H_z^1(h) = 1$ we get that the only surviving term is the one with $i_1 = k = m$ and $i_j = 0$ for $j > 1$, giving us:

$$H_z^m(f) = H_{z-\alpha}^m(f) \binom{m}{m, 0, ..., 0} (H_z^1(h))^m = H_{z-\alpha}^m(f)$$

□

In Appendix A.1 we describe the Riemann-Roch spaces and Hasse derivatives in the rational function field.

We have demonstrated a connection between vanishing of Hasse derivatives and multiplicity (Claim 2.5) and saw that derivatives do not change under translation by a constant (Corollary 2.7). We now give a definition that will serve us later:

Definition 2.8. *Let F be a function field with constant field K. Let S be a set of degree one places (also called* rational points*) of F/K. We say $z \in F$ is* derivative-useful *for S, or, in short, S-useful, if for every $P \in S$ there exists $\alpha \in K$ such that $v_P(z - \alpha) = 1$.*

Intuitively this means the function z takes a value (has no pole) at every place of S, and takes this value with multiplicity 1. It can be pictured as the graph of z passing through (P, α) but not being tangent to the constant function α there. We have:

Claim 2.9. *If z is S-useful and for all $0 \leq m < M$ the function $H_z^m(f)$ vanishes at all places in S, then f vanishes with multiplicity at least M at every place of S (i.e. $v_P(f) \geq M$ for every $P \in S$).*

Proof. Fix $P \in S$. As z is S-useful there exists some $\alpha \in K$ such that $v_P(z-\alpha) = 1$. By Corollary 2.7 we see that $\left(H_{z-\alpha}^m(f)\right)|_P = \left(H_z^m(f)\right)|_P = 0$ for all $0 \leq m < M$. Hence Claim 2.5 tells us $v_P(f) \geq M$ as desired. □

Remark 2.10. *The term "S-useful" is not standard and does not hold any deeper meaning then saying z "works" for every place of S in the sense discussed above.*

2.1.1 Hasse derivatives of p-th powers

When the characteristic is $p > 0$ we know that the *non-separating* elements are exactly the ones that are p-th powers, and that $D_z(f^p) = 0$ for all $f \in F$. The following lemma tells us how Hasse derivatives behave on p-th powers:

Claim 2.11. *[Tor00, Remark 2.4 and Remark 2.5], [Jeo11, Theorem 3.1] Let $z \in F/K$ be a separating element of a function field of characteristic $p > 0$. Let $q = p^k$ be a power of p and $f \in F$. then:*

1. $H_z^m(f^q) = (H_z^{m/q}(f))^q$ *if q divides m and* $H_z^m(f^q) = 0$ *otherwise.*
2. $H_z^m(f) = 0$ *for* $m = 1, ..., q-1$ *if and only if there exists some $g \in F$ such that $f = g^q$*
3. $H_z^1(f) = H_z^p(f) = H_z^{p^2}(f) = ... = H_z^{p^{k-1}}(f) = 0$ *if and only if there exists some $g \in F$ such that $f = g^q$*

The following corollary will be useful to us later on:

Corollary 2.12. *Let $z \in F/K$ be a separating element of a function field of characteristic $p > 0$. Let q be a power of p, $m < q$ and $f, g \in F$, then:*

$$H_z^m(fg^q) = H_z^m(f)g^q$$

Proof. Since $m < q$, all of the derivatives of g^q that will appear in the expansion of $H_z^m(fg^q)$ by means of the product rule are zero (from Claim 2.11) except for the term $H_z^m(f)g^q$. □

2.2 Differentials

In real and complex analysis we have the notion of differentials. Informally, dx measures the change in x. Then, $D_x^1(f) = \frac{df}{dx}$ is the change in f with respect to the change in x, i.e., $\lim_{\varepsilon \to 0} \frac{f(x)-f(x+\varepsilon)}{(x+\varepsilon)-x}$. While the notion of derivative (i.e., the change of f with respect to the change in x) is well defined, the notion of change in x alone is ill-defined, as we can change the scale of change, e.g., make it twice faster. Thus, our first goal is to chose a canonical change, and define the change according to it. Our presentation is informal and we refer the reader to [Sti09, Chapter 4] for a formal treatment of the subject.

Let F/K be a function field. We model a change function by a *derivation of* F, which is a K-linear map D from F to some F-module that upholds the product rule of derivatives, i.e. $D(fg) = fD(g) + gD(f)$. For example $H_z^1 : F \to F$ is a derivation for every separable $z \in F$. One can define the module of differentials of F, denoted Δ_F, such that all derivations of F factor through Δ_F via a canonical mapping $d : F \to \Delta_F$, i.e., if $\delta : F \to M$ is a derivation of F into some F-module M, then there exists a unique F-linear map $\mu : \Delta_F \to M$ such that $\delta = \mu \circ d$. It turns out that d is itself a derivation. For $x \in F$, $d(x)$ is called the differential associated with x and is denoted dx. The set Δ_F of differentials of F contains all elements udx where $u \in F$ and x is separating, where this set is taken modulo the equivalence relation $udx = vdy$ if and only if $\frac{u}{v} = D_x^1(y)$. With this we get a notion of division of differentials via $\frac{udy}{vdx} = \frac{u}{v} D_x^1(y)$.

Originally, we defined valuation of elements in F. We now extend the notion of valuation to differentials. If $P \in \mathbb{P}_F$ is a place of F and $udx \in \Delta_F$ a differential of F, we define $v_P(udx)$ as follows. We pick a local parameter t of P (i.e., $v_P(t) = 1$) and we find $b \in F$ such that $udx = bdt$. Then $v_P(udx) = v_P(b)$. One can show that this definition is independent of the specific choice of local parameter t. As differentials have valuations, differentials also have zeroes and poles, i.e., places where the valuation is strictly positive or strictly negative, and this can be encoded in a divisor, denoted (udx) and called the divisor associated with the differential udx. It turns out any differential $udx \in \Delta_F$ has only finitely many zeroes or poles and so the associated divisor is indeed well defined. A divisor which is associated to some differential in Δ_F is called a *canonical divisor*. All canonical divisors have degree $2g - 2$ and their Riemann-Roch space has dimension g where $g = genus(F)$.

The following claims will be useful:

Claim 2.13. *Let $u \in F$, $x, y \in F$ separating, then:*

- $(udx) = (u) + (dx)$
- $(D^1_x(y)) = (\frac{dy}{dx}) = (dy) - (dx)$

The first bullet is a restatement of [Sti09, Proposition 1.5.13] and the second one is an immediate consequence of the first bullet and the equality $1dy = D^1_x(y)dx$.

There is a close relationship between the zeroes and poles of f and the zeroes and poles of df. The following claim is stated in [Mas84, Chapter I (6)] for the case where K is algebraically closed, but by considering a constant-field extension of F one can verify it holds exactly as stated for any perfect base field K and even when P is not a place of degree one (which is not a consideration when K is algebraically closed)[3].

Claim 2.14. *Let $f \in F/K$, df its associated differential, then:*

- *For every place P, $v_P(df) \geq v_P(f) - 1$. In particular, If f has zeroes at P, df can lose at most one zero at P. Also, if df has a pole at P, df can have at most one more pole at P. Also,*
- *If $v_P(f) \geq 0$ then $v_P(df) \geq 0$, i.e., df can have poles only at places where f has poles.*

As an example, let us compute (dx) in $K(x)/K$. We first compute $v_{P_\infty}(dx)$. We take $t = \frac{1}{x}$ to be the local element at P_∞ (as $v_{P_\infty}(x^{-1}) = 1$). We have $1dx = -x^2dt$ (since $1dt = \frac{dt}{dx}dx = D^1_x(\frac{1}{x})dx = \frac{-1}{x^2}dx$) and so $v_{P_\infty}(dx) = v_{P_\infty}(-x^2) = -2$. The other places of $K(x)/K$ are all of the form P_h where h is an irreducible polynomial in $K[x]$. Then $1dx = \frac{1}{h'(x)}dh$, where h' is the formal derivative of h as a polynomial in x (because $h'(x)dx = \frac{dh}{dx}dx = 1dh$). Thus, $v_h(dx) = -v_h(h'(x)) = 0$. In total we get $(dx) = -2P_\infty$. Note that while x has a single pole at P_∞, its differential dx has two poles there, and while x vanishes at P_{x-0}, dx does not vanish there. We proved $-2P_\infty$ is a canonical divisor of $K(x)/K$. Its degree is indeed $-2 = 2\text{genus}(K(x)/K) - 2$. In fact, every other divisor of degree -2 is also canonical in $K(x)/K$, since if $\deg(D) = -2$ then $\deg(D - (dx)) = 0$ and there is a function f with $(f) = D - dx$ (using the Riemann-Roch theorem for the genus 0 rational function field), and then $(fdx) = (f) + (dx) = D$.

[3] For completeness we prove this in appendix B.

We mentioned before that $\deg(df) = 2g - 2$ for canonical divisors (df), and therefore when g is large (df) has many more zeroes than f. We also know that (df) has a zero wherever f has a zero of multiplicity at least 2. Finding the other zeroes of df is a bit more complicated. It turns out that:

Claim 2.15. *[Sti09, Sections 3.4 and 3.5] The zeroes of (df) are either:*

- *at places that are zeroes of f, or,*
- *at places of F/K that are ramified when F is viewed as an extension of $K(f)/K$ (we discuss ramification later on).*

As an example let us compute (dx) in the Hermitian function field $F = K(x, y)/ < y^5 + y - x^6 >$, where $K = \mathbb{F}_{25}$. We know that

- $\deg(dx) = 2\text{genus}(F) - 2 = 2\binom{5}{2} - 2 = 18$,
- dx may have poles only where x has, i.e., only at P_∞,
- By Claim 2.15 the zeroes of (dx) can only be at places that are zeroes of x, or places that are ramified in $F/K(x)$.

When we look at the zeroes of x we find $5 = [F : K(x)]$ places $P_{(0,\beta)}$ that correspond to the points $\{(0, \beta) \in K \times K \mid \beta^5 + \beta = 0\}$, all of which are degree one places. The element $t = x - \beta$ is a local parameter of $P_{(0,\beta)}$, and $dx = \frac{dx}{dt}dt = D_x^1(t)dt = dt$, so $v_P(dx) = v_P(1) = 0$, and therefore dx does not have zeroes at these five places. It follows that the only zeroes of dx can be at places that ramify in $F/K(x)$. There is only place of $F/\mathbb{F}_{25}$ that ramifies in $F/K(x)$ and it is the place P_∞. Therefore dx has 18 zeroes at P_∞ and $(dx) = 18P_\infty$. A similar computation can be used to compute (dy), however, it is easier to use $\frac{dy}{dx} = D_x^1(y) = D_x^1(y^5 + y) = D_x^1(x^6) = x^5$ and get

$$\begin{aligned}(dy) &= (\frac{dy}{dx}dx) = (x^5dx) = 5(x) + (dx) = 5(x)_0 - 5(x)_\infty + (dx) \\ &= 5(x)_0 - 25P_\infty + 18P_\infty = 5(x)_0 - 7P_\infty,\end{aligned}$$

and so dy has 7 poles at P_∞ and 5 zeroes at each of the five places where x has a zero. We can verify that indeed $\deg((dy)) = 25 - 7 = 18 = 2g - 2$.

2.3 Function field extensions

A function field F/K is a finite field extension of the rational function field $K(x)$. Any finite field extension F' of F is, by itself, a finite field extension of $K(x)$, and therefore F' is also a function field. Many AG code constructions work by taking a sequence of finite field extensions of $K(x)$, resulting in a *tower* of fields $F_0 = K(x) \subset F_1 \ldots \subset F_n = F$, where the properties of the function field F/K (such as the genus and the number of degree one places) are derived by analyzing each finite field extension on its own. In this section we consider such finite field extensions of F/K. Our presentation is again informal, and for a formal treatment of the subject we refer the reader to [Sti09, chapter 3].

A finite field extension F'/F of a function field F/K might change (and enlarge) the field of constants (the field of functions that do not have zeroes or poles). We focus on function field extensions where the constant field remains the same. I.e., we fix the base field K, while letting the genus and the number of rational points of F_n go to infinity. For error correcting code constructions this corresponds to a family of codes over a fixed alphabet and length going to infinity.

Formally, a place P in a function field is a maximal ideal I in a valuation ring R of F (where R contains all elements of F with a non-negative valuation at the place, and the maximal ideal I of R contains all elements of F with a positive valuation in the place). Now suppose F'/F is a function field extension. A place Q' of F' is a maximal ideal in a valuation ring R' of F'. Given Q' define $R = R' \cap F$ and $Q = Q' \cap F$. Then, it turns out that R is a valuation ring of F and Q is a maximal ideal of R. We say the place Q' of F' *lies over* the place Q of F, and we denote it by $Q'|Q$ (the same notation as "Q' divides Q"). Every place of F' is lying over a single place of F, and every place of F has at least one place of F' lying above it (alternatively - every place of F is *lying below* some place of F'). We refer to elements and places of F'/K' as "above" and those of F/K as "below".

Similarly, the residue class map (evaluation function) associated with Q' is an extension of the residue class map of Q. Here extension means an extension of a function defined on F to a function defined on all of F'. I.e., if we denote the residue class maps by $\phi_{Q'}$ and ϕ_Q respectively, then for every $f \in F$ it holds that $\phi_{Q'}(f) = f \bmod Q' = f \bmod Q = \phi_Q(f)$. Note that $f \bmod Q'$ is defined because $f \in F \subset F'$.

Example 2.16. *We give an example demonstrating some of the behaviors places of F' lying over places of F might have. For simplicity we state some facts without a justification, and only later (Example 2.20), after giving some more definitions and tools, we explain why the stated facts are true. We fix $K = \mathbb{F}_5$ and $F' = K(x,y)/(y^2 - (x^3 - x))$. F' is an elliptic curve, it can be attained by starting with $F = K(x)$ and extending it with y that satisfies $y^2 = x^3 - x = (x-1)x(x+1)$. Let us now discuss the behavior of some places of $F = K(x)$ as we extend them to F'.*

- *There is only one place of F' lying over P_∞ of $K(x)$. We denote this place by P'_∞. It holds that $v_{P'_\infty}(x) = -2 = 2v_{P_\infty}(x)$ while $v_{P'_\infty}(y) = -3$. These are the only poles of x and y.*

- *We next look for the two zeroes of x and the three zeroes of y. The place $P_0 = P_{x-0}$ in $K(x)$ also has just one place $P'_{(0,0)}$ above it, corresponding to the point $(x = 0, y = 0)$ on the curve. $v_{P'_{(0,0)}}(x) = 2 = 2v_{P_0}(x)$ while $v_{P'_{(0,0)}}(y) = 1$. The two other zeroes of y are at $(x = 1, y = 0)$ and $(x = -1, y = 0)$ each of them being a simple zero.*

- *We now look at the function $\frac{y}{x}$. We see that $v_{P'_\infty}(\frac{y}{x}) = -3-(-2) = -1$ and $v_{P'_{(0,0)}}(\frac{y}{x}) = 1 - 2 = -1$. Thus the function $\frac{y}{x}$ has a simple pole at both P'_∞ and $P'_{(0,0)}$. The zeroes of $\frac{y}{x}$ are at $(x = 1, y = 0)$ and $(x = -1, y = 0)$ each of them being a simple zero.*

- *The place $P_3 = P_{x-3}$ of $F = K(x)$ splits in two, i.e., it has two places lying over it, namely $(x = 3, y = 2)$ and $(x = 3, y = 3 = -2)$. $x - 3$ has a simple zero at each of these places.*

So far we only looked at places of degree one. We now give some examples of places of higher degree.

- *The place P_w of F/K, corresponding to the irreducible polynomial $w(x) = x^3 + x^2 - x + 1$ over $K(x)$, splits in two, giving two degree-3 places $P'_{w,1}$ and $P'_{w,2}$ of F'/K. The two corresponding places (i.e., the ideals over in the valuation rings contained in F' which are composed of all functions that vanish at those places) are $I'_{w,1} = \langle x^3+x^2-x+1, y-(2x^2-x-1)\rangle$ and $I'_{w,2} = \langle x^3 + x^2 - x + 1, y + (2x^2 - x - 1)\rangle$ respectively. In the constant field extension $\mathbb{F}_{125}/\mathbb{F}_5$, we get six degree one places that can be interpreted as points on the curve $\mathbb{F}_{125}(x,y)(\text{mod } y^2 - x^3 + x)$: For* *each of the three $\alpha \in \mathbb{F}_{125}$ such that $\alpha^3+\alpha^2-\alpha+1=0$ and each of the two $\beta \in \mathbb{F}_{125}$ such that $\beta^2=\alpha^3-\alpha$ we have a degree one place in $\mathbb{F}_{125}(x,y)(\mathrm{mod} y^2-x^3+x)$ corresponding to the point $(x=\alpha, y=\beta)$.*

- *The place P_z of F/K corresponding to $z=x^3+x^2-x+3 \in K(x)$ has a single place of F'/K above it. We denote that place by P'_z. It turns out that $v_{P_z}(z)=v_{P'_z}(z)=1$.*

  P'_z is also the only zero of z in F'. As $v_{P'_\infty}(z)=-6$, and the number of zeroes of z equals the number of poles,we conclude that that P'_z must be of degree 6. This happens because in $\mathbb{F}_{125}$ there is no β that solves $\beta^2=\alpha^3-\alpha$ for the α that solve $\alpha^3+\alpha^2-\alpha+3=0$, and to get a solution we need to go to $\mathbb{F}_{125^2}=\mathbb{F}_{5^6}$. The residue class map of $P_{x^3+x^2-x+3}$ returns elements in $\mathbb{F}_{125}$, while The residue class map of $P'_{x^3+x^2-x+3}$ returns elements in $\mathbb{F}_{5^6}$.

In the above example we saw a few different behaviors of places $P'|P$: some places P have a single place P' above them while others split into a few distinct places. The residue class field sometimes stays the same and sometimes extends to a larger field, and the multiplicity of zeroes of a function $f \in F$ when considered at a place P' of F' sometimes stays the same and sometimes gets larger by an integer multiple.

We start with the valuation function. If $Q'|Q$, then $v_{Q'}: F' \to Z \cup \{\infty\}$ and $v_Q: F \to Z \cup \{\infty\}$, and both functions are defined over F. It is a fact that there is a constant $e(P'|P)$, that depends only on P', such that $v_{Q'}(f)=e(Q'|Q)\cdot v_Q(f)$. More formally,

Lemma 2.17. *(Ramification) Let F'/K' be a finite field extension of F/K. Let $Q \in \mathbb{P}_F$ and $Q' \in \mathbb{P}_{F'}$ such that $Q'|Q$. There is a positive integer $e=e(Q'|Q)$ such that for all $f \in F \subset F'$, $v_{Q'}(f)=e\cdot v_Q(f)$. $e(Q'|Q)$ is called the* ramification index *(or* ramification *for short) of Q' over Q.*

In particular, $f \in F$ has a pole (correspondingly, a zero) at Q' when considered as a function in F'/K' if and only if f has a pole (correspondingly, a zero) at the place $Q=Q'\cap F$ of the function field F. If F'/F is finite then $e(Q|P)$ divides the degree of the extension. [4]

We next move to the residue class field:

[4] For those with background in algebraic number theory - this is very similar to ramification in number fields, where if B/A an extension of rings of integers of number fields, then a prime ideal $\mathfrak{p} \in \mathrm{Spec}(A)$ has a decomposition in $\mathrm{Spec}(B)$ as $\mathfrak{p}=\prod \mathfrak{q}_i^{e_i}$ and e_i is the ramification of $\mathfrak{q}_i$.

Definition 2.18. *Let F'/K' be a finite field extension of F/K. Let $Q \in \mathbb{P}_F$ and $Q' \in \mathbb{P}_{F'}$ such that $Q'|Q$. Let L_Q (respectively $L_{Q'}$) be the field extension of K which is the image of the class residue map of Q (respectively Q'). The quantity $f(Q'|Q) \triangleq [L_{Q'} : L_Q] > 0$ is called the* relative degree *of $Q'|Q$.*

As $\deg(Q) = [L_Q : K]$ and $\deg(Q') = [L'_Q : K']$ we see that $f(Q'|Q) = \frac{1}{[K':K]} \frac{\deg(Q')}{\deg(Q)}$, and, in particular, the degree of Q' is always larger than the degree of Q. Also, $f(Q'|Q)$ divides $[F' : F]$.

Finally, as we saw before, different places P of F/K may have a varying number of places of F'/K' above them. We say P *splits* if there are two or more places of F'/K' lying above it.

In our example of the elliptic curve we saw a few examples of ramification, relative degree, and splitting. We saw:

- Places with ramification 2, no splitting and relative degree one,
- Places that split in two, ramification index 1 and relative degree 1, and,
- A place with relative degree 2, no splitting and ramification index one.

All of the above adhere to the following fundamental rule:

Theorem 2.19. *(Fundamental Equality [Sti09, Theorem 3.1.11]) Let F'/K' be a finite extension of F/K and $\{Q_i\}_{i=1,\dots,r}$ be the places laying over $P \in \mathbb{P}_F$. Let $e_i = e(Q_i|P)$ and $f_i = f(Q_i|P)$. Then*

$$\sum_{i=1}^{r} e_i f_i = [F' : F]$$

If P has only a single place above it with ramification index equal to $[F' : F]$ and relative degree one, we say P is *totally ramified* in F'. If P has $[F' : F]$ distinct extensions in F' (each with ramification 1 and relative degree 1) we say P is *totally split*.

In general, if Q_1, Q_2 are two distinct places lying over P then $e(Q_1|P)$ and $e(Q_2|P)$ can be unrelated, and the same for $f(Q_1|P)$ and $f(Q_2|P)$. However, when F'/F is a Galois extension, the ramifications and the relative degrees of all places of F' lying over the same place of F are all the same, and in particular, if $Q_1, ...Q_r$ are all the places over P, the fundamental equality becomes $[F' : F] = efr$ where $e = e(Q_1|P)$ and $f = f(Q_1|P)$.

Example 2.20. *Let us return to example 2.16, where we considered F'/K where $K = \mathbb{F}_5$ and $F' = K(x,y)/(y^2-(x^3-x))$. We consider it as a degree-2 extension of $F = K(x)$, and note this is a Galois extension. Now we proceed to find the places of F' lying over a few places of $F = K(x)$.*

We know x has a single pole in $K(x)$, denote it P_∞. suppose P'_∞ is a place of F' above it. x must have a pole at P'_∞ and we get $2v_{P'_\infty}(y) = v_{P'_\infty}(y^2) = v_{P'_\infty}(x^3-x) = 3v_{P'_\infty}(x)$ (where the last equality is due to the strict triangle inequality and the fact that x has a pole at P'_∞). Thus, $2v_{P'_\infty}(y) = 3e(P'_\infty|P_\infty)v_{P_\infty}(x) = -3e(P'_\infty|P_\infty)$. By the fundamental equality in a Galois extension $e(P'_\infty|P_\infty)$ divides $[F' : F] = 2$, thus $e(P'_\infty|P_\infty)$ is either 1 or 2. As 2 divides $3e(P'_\infty|P_\infty)$ we have $e(P'_\infty|P_\infty) = 2$, and so P'_∞ is fully ramified, has degree one and is the only place lying over P_∞.

As $y^2 = x^3 - x$, if y has a pole at P, so does x. Thus, y has a pole only at P'_∞. As $2v_{P'_\infty}(y) = 3v_{P'_\infty}(x) = 6v_{P_\infty}(x) = -6$, we see that y has a pole of order 3 at P'_∞. The zeroes of y are at the places $P'_{(-1,0)}, P'_{(0,0)}, P'_{(1,0)}$ corresponding to the points $(x=-1, y=0), (x=0, y=0)$ and $(x=-1, y=0)$ on the curve. Since y has pole order 3 and all of these places are zeroes of y, these are all of the zeroes of y, the zeroes are simple zeroes and the places are degree one places.

The places $P'_{(-1,0)}, P'_{(0,0)}, P'_{(1,0)}$ totally ramify. We demonstrate this for $P'_{(0,0)}|P_0$. We have $2 = v_{0,0}(y^2) = v_{0,0}(x) + v_{0,0}(x^2-1) = v_{(0,0)}(x)$, since (x^2-1) does not vanish at $(0,0)$. Thus, $v_{0,0}(x) = 2 = 2 \cdot v_0(x)$ end $e(P'_{(0,0)}|P_0) = 2$.

2.4 Kummer extensions

An algebraic function field F'/K' is a *Kummer extension* of F/K if:

- K contains a primitive n-th root of unity,[5] and,
- $F' = F(Z) \mod (Z^n - u)$ where $u \in F$ and $u \neq w^d$ for all $w \in F$ and $d|n$ such that $d > 1$.

Kummer extensions are Galois. For example, the elliptic curve we discussed in Example 2.16 is a Kummer extension of the rational function field.

For $P \in \mathbb{P}_F$ we denote by $\mathcal{L}(P) \stackrel{\text{def}}{=} \cup_{m\in\mathbb{N}}\mathcal{L}(m \cdot P)$ the K-linear, infinite dimensional vector space of all function that have poles only at P. $\mathcal{L}(P)$ is the set of functions that are *regular* at P. The following claim follows

[5] When $K = \mathrm{F}_q$ this means $n|(q-1)$.

from [Sti09, Corollary 3.7.4 and Proposition 3.11.1] and the Hurwitz Genus Formula ([Sti09, Theorem 3.4.13]):

Claim 2.21. *Let P_∞ be a degree one place of a function field F/K of genus g, ℓ a prime number and $u \in \mathcal{L}(P_\infty)$ which is not an ℓ-th power in F. Denote $d = \deg(u) = -v_{P_\infty}(u)$ and assume d is co-prime to ℓ. Let $F' = F(Z)$ where $Z^\ell = u$ be the Kummer extension with respect to u. Then:*

- *F' is a degree ℓ extension of F*
- *P_∞ is totally ramified in F'.*[6] *Also K is the full constant field of F'.*
- *$Z \in \mathcal{L}(P'_\infty)$ and $\deg(Z) = d$*
- *$g' \overset{\text{def}}{=} \text{genus}(F')$ satisfies $\ell(g-1) \leq g'-1 \leq \ell(g-1)+d$*

From now on we assume that K is a finite field, $K = \mathbb{F}_q$ for some prime power q. Let ℓ be a prime number that divides $q-1$. Let P_∞ be a degree one place, and S a set of degree one places of F that does not contain P_∞. Let $u \in \mathcal{L}(P_\infty) \subset F$ such that u his not an ℓ-th power in F. We are interested in the number of $P \in S$ such that $u|_P \overset{\text{def}}{=} \phi_P(u) \in K$ is an ℓ-th power as an element of K (where ϕ_P is the evaluation function at P). [7] We claim that in this situation:

Claim 2.22. *Suppose $u|_P \neq 0$ for some degree one place $P \in S$. Then:*

- *If $u|_P$ is not an ℓ-th power in K, then there is a single place above P in F' and it is a place of degree ℓ (and ramification 1).*
- *If, however, $u|_P$ is a non-zero ℓ-th power in K, then the place P is totally split in F', i.e. there are ℓ distinct degree one places above P (that have all ramification 1).*

Proof. Let ϕ_P be the evaluation function corresponding to P. Since $P \in S$, u is regular and $P_\infty \notin S$ we know that u is defined at P, and therefore u is also defined at any place P' of F' which is above P. Since $u = Z^\ell$, their

[6] We remind the reader that this means that P'_∞ is the only place of F' above P_∞, has degree one and its ramification index over P_∞ is ℓ.

[7] Notice that $u|_P$ is defined because u does not have a pole at any $P \in S$, and $u|_P \in K$ because any $P \in S$ is degree one.

poles are in the same places, so Z must be defined at P'. $\phi_P(u) \in K$. We assume $\phi_P(u) \neq 0$.

Suppose $\phi_P(u)$ is not an ℓ-th power in $K^\times$. Let P' be some place of F' lying over P. We know $\phi_{P'}$ must be an extension of ϕ_P which is defined at Z, and so $\phi_P(u) = \phi_{P'}(u) = \phi_{P'}(Z^\ell) = \phi_{P'}(Z)^\ell$, meaning that $\phi_{P'}(Z)$ is an ℓ-th root of $\phi_P(u)$ which is not an ℓ-th power in K. This means that $\phi_{P'}(Z)$ is an element of an ℓ-th degree extension of K (since ℓ is prime), meaning P' is a place of degree at least ℓ. Since the the extension F'/F is of degree ℓ (claim 2.21), the fundemental equality tells us P' must be of degree exactly ℓ, be the only place above P, and have ramification 1.

Suppose $\phi_P(u)$ is an ℓ-th power in $K^\times$. We will define ℓ distinct evaluation functions that extend ϕ_P. The fact they are all distinct will mean they each correspond to a different place of F', giving ℓ distinct places of F' all lying over P, and by the fundamental equality we will get they are all of degree one and ramification one. Since $F' = F(Z)$, and Z is defined at all extensions of P, it is enough to define $\phi_{P'}$ on Z for it to be an extension of ϕ_P [8]. Since $\phi_P(u)$ is a non-zero ℓ-th power in $K^\times$, there are distinct $\alpha_1, ...\alpha_\ell$ with $\alpha_i^\ell = \phi_P(u) = \phi'_P(u)$, and setting $\phi'_P(Z) = \alpha_i$ will give an extension of ϕ_P. This is well defined since $\phi'_P(Z)^\ell = \phi'_P(u)$, meaning any two expressions over $F(Z)$ that differ by a multiple of $Z^\ell - u$ will give the same value under ϕ'_P. Since our ℓ choices of extension all differ in the value of Z it is clear these are ℓ distinct evaluations, and therefore they correspond to ℓ distinct plcaes. □

This behavior of splitting of places of S where u is a non-zero ℓ-th power leads us to the following useful claim:

Claim 2.23. *Let $F' = F(Z) \mod (Z^\ell - u)$ be a Kummer extension with ℓ prime and $u \in \mathcal{L}(P_\infty) \subset F$ such that u is not an ℓ'th power of an element in F. Further assume K is the full constant field of F'. Let S be a set of degree one places F/K and assume $P_\infty \notin S$. Suppose $S_\ell \subset S$ is such that $u|_P$ is a non-zero ℓ-th power for all $P \in S_\ell$, and let S'_ℓ be the set of all places of F' lying over S_ℓ.*

[8] Alternatively, one can pick a parametrization of F as a curve such that P is a rational point on the curve, and instead of finding ℓ extensions of the evaluation function, we will find ℓ rational points on the curve with an additional parameter Z and the additional equation $Z^\ell = u$, and finding ℓ points lying over the original point P proves the point fully splits.

Then: If $x \in F$ is S_ℓ-useful[9] *then x when considered as an element of F' is S'_ℓ-useful.*

Proof. Let $Q \in S'_\ell$ and denote $P \in S_\ell$ the place of F lying below Q. Since $u|_P$ is a non-zero ℓ-th power, P is totally split in F' (by claim 2.22). This means there are ℓ places lying over P (Q among them), each of them with relative degree one and ramification 1 over P. Since $x \in F$ is S-useful and $P \in S_\ell \subset S$ there exists an $\alpha \in K$ such that $v_P(X - \alpha) = 1$. Since Q is lying over P and has ramification 1 we get $v_Q(X - \alpha) = e(Q|P)v_P(X - \alpha) = 1 \cdot 1 = 1$. So for any $Q \in S'_\ell$ we found $\alpha \in K$ with $v_Q(X - \alpha) = 1$ which finishes the proof. $\square$

Definition 2.24. *The minimal degree of a non constant function in a function field is called the* gonality *of the function field.*

The following is an immediate consequence of [BATS09, Lemma 10] which is useful for us in Section 4.

Claim 2.25. *Let $F/\mathbb{F}_q$ be a function field over the finite field $\mathbb{F}_q$. Suppose the number of degree one places in F is equal to N. let $x \in F$ be a non constant function, then the degree of x (the number of poles/zeroes of x) is at least $\frac{N}{q+1}$. In other words: the* gonality *of F is at least $\frac{N}{q+1}$.*

Remark 2.26. *The functions in $\mathcal{L}(P)$ are often called* regular functions. *In this work we will always use this teminology with respect to places denoted by P_∞ or P'_∞.*

3 The derivative height bound

In the polynomial ring $K[X]$, the derivative of a non-constant polynomial is a polynomial of a strictly smaller degree, and the more times we derive the smaller the degree gets until we reach the zero polynomial. This gives the impression that derivatives are simpler, i.e. have less poles than the original function.

When transitioning to rational functions, this is no longer the case. For example, when m is smaller then the characteristic of K, $D_x^m(\frac{1}{x}) = \frac{c_m}{x^{m+1}}$ for

[9] In practice, our way of ensuring x is S_ℓ-useful will be to find an x which is useful for all of S.

some non-zero constants c_m. Now, the more we derive the more poles we get, and each derivation increases the pole order by one.

Another noteworthy example is the derivative of any quotient of polynomials $\frac{f(x)}{g(x)}$. We have:

$$\begin{aligned}
D_x^1(\frac{f}{g}) &= \frac{f'g - g'f}{g^2} \\
D_x^2(\frac{f}{g}) &= \frac{g^2f' - 2gf'g' - fgg'' + 2f(g')^2}{g^3} \\
D_x^3(\frac{f}{g}) &= \frac{f'''g^3 + 6gg'(f'g' + fg'') - g^2(3f''g' + 3f'g'' + fg''') - 6f(g')^3}{g^4}
\end{aligned}$$

At the m-th derivative we get some polynomial in the derivatives of f and g divided by g^{m+1}, meaning the poles at the zeroes of g increase many-fold as we derive. Thus, both in the case of $\frac{1}{x}$ and in the more general case of $\frac{f}{g}$, the poles "stay where they were", but the pole order increases. This gives us reason to hope that deriving a regular function will leave us with a regular function.

Now consider derivatives of the form $D_g^1(f)$ where $f, g \in K(x)/K$. Due to the chain rule

$$D_g^1(f) = \frac{df}{dg} = \frac{df}{dx}\frac{dx}{dg} = \frac{f'}{g'}$$

and we see that $D_g^1(f)$ may have poles also where g' has zeroes, and the more zeroes g has, the more new poles we introduce when deriving. Thus, it greatly matters with respect to which function g we choose to derive.

Next, we look beyond the genus zero rational function field. We take the Hermitian function field (see appendix A.2) as our working example. Let $F = \mathbb{F}_{p^2}(x, y) \mod y^p + y - x^{p+1}$. The elements x and y are regular, i.e., they only have poles at a single degree one place, which we denote P_∞. It holds that $v_{P_\infty}(x) = -p$ and $v_{P_\infty}(y) = -(p+1)$. Now,

$$x^p = D_x(x^{p+1}) = D_x(y^p + y) = D_x(y^p) + D_x(y) = D_x(y),$$

and so, $D_x(y) = x^p$ has p^2 poles at P_∞ while y has only $p + 1$ at P_∞, an increase of $p^2 - p - 1 = 2\text{genus}(F) - 1$.

Theorem 3.3 relates the divisor of a function and the divisor of its derivative. We focus on the case the derived function is supported on a single point.

We remind the reader that $H_x(f)$ is the Hasse derivative of f with respect to x. Also, $\deg(x) = [F : K(x)]$ is the total number of poles (or zeroes) of x in F. We also let $\mathrm{DegSupp}((x)_\infty)$ be the degree of the support of the pole divisor of x, i.e., the degree of the pole divisor of x when all positive coefficients are reduced to one. We prove:

Theorem 3.1. *Let F/K be a function field of genus g. Let $x \in F$ be a separating element of F/K and P_∞ a degree one place of F. Let*

$$\begin{aligned} G &= 3g - 2 + \deg(x) + \mathrm{DegSupp}((x)_\infty) \\ W &= G - \max\{v_\infty(dx), 0\} \\ D &= G \cdot P_\infty - (dx)_0, \\ \Delta &= G + \min\{v_\infty(dx), 0\}. \end{aligned}$$

Then there exists an element $0 \neq \omega = \omega(x, P_\infty) \in \mathcal{L}(D) \subseteq \mathcal{L}(WP_\infty)$ such that for every $f \in \mathcal{L}(AP_\infty)$ it holds that

$$\omega \cdot H_x(f) \in \mathcal{L}((A + \Delta + 1) \cdot P_\infty).$$

Proof. Let us denote $f' := H_x^1(f) = D_x^1(f)$. By Claim 2.13, $f' = \frac{df}{dx}$ and

$$(f') = (df) - (dx).$$

It follows that the poles of f' can come either:

- from poles of df, or,
- from zeroes of dx.

Since $f \in \mathcal{L}(AP_\infty)$, Claim 2.14 tells us all the poles of f and df are at P_∞. Claim 2.14 also tells us that $v_\infty(df) \geq v_\infty(f) - 1 \geq -(A+1)$, and so df has at most $A+1$ poles, all of which must be at P_∞. We wish to find $\omega \in F$ s.t. $\omega \cdot f' \in \mathcal{L}(P_\infty)$ so we need to choose ω that cancels the poles of f' at all places other than P_∞. These poles can arise only from zeroes of dx. More precisely, we are interested in the zeroes of dx *outside* P_∞. While we are interested in the zeroes of dx, we first consider the *poles* of dx. By Claim 2.14:

- The poles of dx are at the same places as the poles of x, i.e., $v_P(dx) < 0$ implies $v_P(x) < 0$, and,

- At any place P where dx and x have a pole, dx may have at most one more pole than x, i.e., $v_P(dx) \geq v_P(x) - 1$.

It therefore follows that $\deg((dx)_\infty) \leq \deg(x) + \mathrm{DegSupp}((x)_\infty)$. We now use the fact that (dx) is a canonical divisor, and therefore has degree $2g-2$ (see Section 2). Thus, the number of zeroes of dx is exactly $2g-2$ more than the number of poles of dx, and in total we get

$$\deg((dx)_0) \leq \deg(x) + \mathrm{DegSupp}((x)_\infty) + 2g - 2 = G - g.$$

Now, recall that $D = G \cdot P_\infty - (dx)_0$. Thus,

$$\deg(D) = G - \deg((dx)_0) \geq g.$$

By the Riemann-Roch Theorem (Theorem 2.3) there exists some $0 \neq \omega \in \mathcal{L}(D)$. Fix any such ω.

Claim 3.2. $\omega f' = \omega \cdot \frac{df}{dx} \in \mathcal{L}((A+1+\Delta)P_\infty)$.

Proof. For any $P \neq P_\infty$, $v_P(D) = -v_P((dx)_0)$. Hence,

$$\begin{aligned} v_P(\omega) &\geq -v_P(D) = v_P((dx)_0), \text{ and,} \\ v_P(\omega f') &= v_P(\omega) + v_P(df) - v_P(dx) \\ &\geq v_P(\omega) + v_P(df) - v_P((dx)_0) \geq v_P(df) \geq 0. \end{aligned}$$

Next we compute the pole order of wf' at P_∞. We have $w \in \mathcal{L}(D) \subseteq \mathcal{L}((G - \max\{v_\infty(dx), 0\})P_\infty)$. Thus,

$$\begin{aligned} -v_\infty(\omega f') &= v_\infty(dx) - v_\infty(\omega) - v_\infty(df) \\ &= v_\infty(dx) + G - \max\{v_\infty(dx), 0\} - v_\infty(df) \\ &\leq A + 1 + G + v_\infty(dx) - \max\{v_\infty(dx), 0\}, \end{aligned}$$

because $v_\infty(df) \geq v_\infty(f) - 1 \geq -A - 1 = -(A+1)$. However,

$$v_\infty(dx) - \max\{v_\infty(dx), 0\} = \min\{0, v_\infty(dx)\},$$

and the proof is complete. □

□

3.1 General derivation order

We now generalize Theorem 3.1 to any derivation order m. We remind the reader that $H_x^m(f)$ is the m-th Hasse derivative of f with respect to x.

Theorem 3.3. *Let F/K be a function field of genus g over a base field of characteristic p. Let $x \in F$ be a separating element of F/K and P_∞ a degree one place of F. Let G, W, D, Δ be as before. There exists an element $0 \neq \omega = w(x, P_\infty) \in \mathcal{L}(D) \subseteq \mathcal{L}(WP_\infty)$ such that for every positive integer $m < p$ (or any integer m, if $p = 0$)*

$$\forall f \in \mathcal{L}(A \cdot P_\infty), \quad \omega^{2m-1} \cdot H_x^m(f) \in \mathcal{L}(A_m \cdot P_\infty).$$

where $A_m = A - W + m \cdot (\Delta + W + 1)$.

Proof. We use the same w as before. We prove by induction. We already saw the $m = 1$ case. Assume for m and let us prove for $m+1$. The $m+1$-th Hasse derivative is the same as the $m+1$-th iterated derivative D_x^{m+1} up to multiplication by a non-zero scalar (see corollary 2.4 and using $m + 1 < p$ when the characteristics is finite). Now,

$$\begin{aligned} \omega^2 D_x(\omega^{2m-1} D_x^m f) &= \omega^2 \ [\ D_x(\omega^{2m-1}) D_x^m f + \omega^{2m-1} D_x(D_x^m f)\ ] \\ &= (2m-1) \cdot \omega D_x(\omega) \cdot \omega^{2m-1} D_x^m f + \omega^{2m+1} D_x^{m+1} f \end{aligned}$$

Thus,

$$\omega^{2m+1} D_x^{m+1} f = \omega^2 D_x(\omega^{2m-1} D_x^m f) - (2m-1) \cdot \omega D_x(\omega) \cdot \omega^{2m-1} D_x^m f.$$

By the induction hypothesis and the $m = 1$ case:

$$\begin{gathered} \omega^{2m-1} \cdot D_x^m f \in \mathcal{L}(A_m \cdot P_\infty), \\ \omega D_x(\omega^{2m-1} D_x^m f) \in \mathcal{L}((A_m + (\Delta + 1)) \cdot P_\infty). \end{gathered}$$

Also $\omega \in \mathcal{L}(WP_\infty)$. By the $m = 1$ case,

$$\omega \cdot D_x(\omega) \in \mathcal{L}((W + (\Delta + 1)) \cdot P_\infty)$$

The term $\omega^2 D_x(\omega^{2m-1} D_x^m f)$ is in $\mathcal{L}((A_m + W + \Delta + 1)P_\infty)$. The term $\omega D_x(\omega) \cdot \omega^{2m-1} D_x^m f$ is also in $\mathcal{L}((A_m + W + \Delta + 1)P_\infty)$. Altogether, $\omega^{2m+1} D_x^{m+1} f$ is in $\mathcal{L}(A_{m+1} P_\infty) = \mathcal{L}((A_m + W + \Delta + 1)P_\infty)$. □

Remark 3.4. *Note that if $D_x(\omega)$ is in $\mathcal{L}(P_\infty)$, we can multiply by a single ω per derivative, instead of multiplying by ω^2.*

Corollary 3.5. *Assume the above setting. Let $m > 0$ then $\omega \in \mathcal{L}((3g + 2\deg(x) - 1)P_\infty)$, and $A_m \leq A + (2m-1)(3g + 2\deg(x) - 1)$.*

3.2 Discussion

Example 3.6. *We saw that in the Hermitian function field $D_x(y) = x^p$. In fact, we saw in section 2.2, that in this case $(dx) = (2g-2)P_\infty$, i.e., it has no poles, and all its zeroes are at P_∞. Then, we can take $w = 1$. Furthermore, for every $f \in \mathcal{L}(AP_\infty)$, $-v_\infty(H_x(f)) = v_\infty(dx) - v_\infty(df) \leq 2g-2+A+1$. For a general m, $A_m \leq A + m(2g-1)$.*

Example 3.7. *Now consider the Hermitian function field when we derive by y. For example, $D_y(x) = \frac{1}{x^p}$. Things in this case are more complicated because we saw in section 2.2 that $(dy) = (p+2)P_\infty - p(x)_0$. Nevertheless, since all functions in $\mathcal{L}(P_\infty)$ are polynomials in x and y, we get that if we are deriving with respect to y we can choose w to be x^p to cancel out the $\frac{1}{x^p}$ which is the derivative of x with respect to y. With this choice of ω we again get that if $f \in \mathcal{L}(AP_\infty)$ then $\omega^m H^m(f) \in \mathcal{L}((A + m(2g-1))P_\infty)$.*

The bounds we obtained are worse. This is because:

- We paid an additive g to guarantee a certain Riemann-Roch space is not empty, by forcing the degree of its divisor to be at least g. While there are divisors of degree $g-1$ which have empty Riemann-Roch spaces, there are divisors of degree 0 which have non-empty Riemann-Roch spaces. It is conceivably possible that the $3g-1$ we have is not mandatory and can be replaced with $2g-1$ as we have in the Hermitian curve. Perhaps, using the Riemann-Roch theorem with canonical divisors would do the trick.

- Additionally, the $2m$ factor is a side effect of the inductive argument which requires us to apply the induction hypothesis twice - once for $H^{m-1}(f)$ and once for $H^1\omega$. If, however, $H^1\omega$ is regular, we can apply the induction hypothesis once and so ω^m would be sufficient. Alternatively, if the poles of $D^m(f)$ which exceed those of $D^{m-1}(f)$ behave like "dividing by a function again and again", similarly to what we saw with $D_x^m(\frac{f}{g})$ in $K(x)$ or to $D_y(f)$ for regular f in the Hermitian function field, we would again get that ω^m is sufficient.

- The requirement $m < p$ is also a side effect of the induction, but when looking at the p-th Hasse derivative of y^p we get from claim 2.11 $H_x^p(y^p) = H_x^1(y)^p = x^{p^2}$ which is of pole order $p^3 = p(p+1) + (2g-1)p$, an increase of exactly $2g-1$ times the order of the derivative.

To summarize this, an optimistic reading of the proof would lead us to believe that the following version of theorem 3.3 could hold:

Conjecture 3.8. *Let F/K be a function field of genus g. Let $x \in F$ be a separating element of F/k. Let P_∞ be a degree one place of F. There exists an element $0 \neq \omega = w(x, P_\infty) \in F$ such that for every $m \in \mathbb{N}$*

$$\forall f \in \mathcal{L}(P_\infty), \quad \omega^m \cdot H_x^m(f) \in \mathcal{L}(P_\infty).$$

Furthermore, $\omega \in \mathcal{L}((2g-1+\deg(x)+\mathrm{DegSupp}((x)_\infty)) \cdot P_\infty)$ and so if $f \in \mathcal{L}(A \cdot P_\infty)$ then $\omega^m \cdot H_x^m(f) \in \mathcal{L}(A_m \cdot P_\infty)$ for

$$A_m = A + m(2g - 1 + \deg(x) + \mathrm{DegSupp}((x)_\infty) + \min\{v_\infty(dx), 0\}).$$

4 The setting and our result

4.1 The function fields we work with

In the following we will work with:

- A function field F/F_q,
- A set S of degree one places,
- A degree one place we call P_∞, and,
- An element $X_0 \in \mathcal{L}(P_\infty)$ that is S-useful (see Definition 2.8). Note that this implies that $P_\infty \notin S$.

Here we state the assumptions we put on the function field F/F_q, S and X_0.

1. We assume $q = p^2$ and p is a prime number.[10]
2. We also want F to have many degree one places and a small genus. Let $\mathbb{P}_F^1$ denote the set of degree one places of F, and $N_1 = |\mathbb{P}_F^1|$. From the Drinfeld-Vladut Bound [Sti09, Theorem 7.1.3] we know that in any sequence of function fields over F_q, with N_1 going to infinity, the genus

[10] A large part of our work is applicable even when p is a prime power and not just prime, but the use of theorem 3.3 is pivotal, and at this point our proof only holds for $M < p$ where p is the characteristic of the field.

tends in the limit to at least $\frac{N_1}{p-1}$, and there are several constructions attaining this bound [Sti09, Section 7]. In particular we assume:

$$g_F \overset{\text{def}}{=} \text{genus}(F) \leq a \cdot \frac{N_1}{p}, \tag{1}$$

for some constant $a \geq \frac{p}{p-1} \geq 1$.

3. We would like $\deg(X_0)$ to be as small as possible. From the gonality lemma, Claim 2.25, we know that every element $f \in F$ with $\deg(f) > 0$ has $\deg(f) \geq \frac{N_1}{q+1}$. We assume

$$\deg(X_0) = b \cdot \frac{N_1}{q}, \tag{2}$$

for some constant b, and so $b \geq 1 - \frac{1}{q+1}$. We want b to be small.

We now see several examples to some of the function fields presented in Appendix A:

Example 4.1. *Let F/F_q be the Hermitian function field, with $N_1 = p^3 + 1$ and genus $\frac{p(p-1)}{2}$. Let $S = \mathbb{P}_F^1 \setminus P_\infty$, $|S| = p^3$. Let $X_0 = x$ and notice that indeed $X_0 = x$ is S-useful. We have* $\deg(X_0) = p$. *Thus,*

- $a = \frac{p \cdot g}{N_1} = \frac{p-1}{2}$, *and,*
- $b = \frac{q \cdot \deg(x)}{N_1} = 1 - \frac{1}{N_1}$.

Example 4.2. *Next, we look at the Hermitian tower function field of level e, F_e. When $2e < p$ we the genus of F_e is at most ep^e. Let S be all the degree one places other than P_∞, $|S| = p^{e+1}$. Let $X_0 = x_1$ and notice that indeed X_0 is S-useful. We have* $\deg(X_0) = p^{e-1}$. *Thus,*

- *We assume $2e < p$. Then, $a = \frac{p \cdot g}{N_1} = \frac{ep^{e+1}}{p^{e+1}} = e < \frac{p}{2}$, and,*
- $b = \frac{q \cdot \deg(x)}{N_1} = \frac{q \cdot p^{e-1}}{p^{e+1}} = 1$.

Example 4.3. *Our final example is the GS tower of level e. The genus of F_e is less then p^e. $X_0 = x_1$ is S-useful for a set of $p^e(p-1)$ degree one places (which are exactly the evaluation points in the GS error correcting code). We have* $\deg(X_0) = p^{e-1}$. *Thus,*

- $a = \frac{p \cdot g}{N_1} \leq \frac{p \cdot p^e}{p^e(p-1)} = \frac{p}{p-1}$, *and,*
- $b = \frac{q \cdot \deg(x)}{N_1} \leq \frac{q \cdot p^{e-1}}{p^e(p-1)} \leq \frac{p}{p-1}$.

4.2 The problem

We continue with the notation set before.

- Let ℓ be a prime number dividing $q-1$. Note that ℓ is different from the characteristic of F.
- $f \in \mathcal{L}(rN_1P_\infty)$, where r is a parameter, and,
- We assume $\deg(f) = -v_{P_\infty}(f)$ is coprime to ℓ. This assumption implies f is not an ℓ-th power in $\overline{\mathbb{F}_q}F$, where $\overline{\mathbb{F}_q}F$ is the constant field extension of F with the algebraic closure of $\mathbb{F}_q$.

Our goal is to estimate the number of places $P \in S$ such that $f|_P \in \mathbb{F}_q$ is an ℓ-th power. We define

$$F' = F(Z) \mod Z^\ell - f.$$

By Claim 2.21, F' is a Kummer extension of F and P_∞ is totally ramified in F'. Also $g' = \text{genus}(F')$ satisfies $\ell(g-1) \leq g'-1 \leq \ell(g-1) + \deg^F(f)$ Let P'_∞ denote the single place of F' above P_∞. As P'_∞ is totally ramified we have:

- $deg(P'_\infty) = 1$,
- $v_{P'_\infty}(X_0) = \ell \cdot v_{P_\infty}(X_0)$, and $v_{P'_\infty}(f) = \ell \cdot v_{P_\infty}(f)$,
- $\ell \cdot v_{P'_\infty}(Z) = v_{P'_\infty}(f) = \ell \cdot v_{P_\infty}(f)$ and so $v_{P'_\infty}(Z) = v_{P_\infty}(f) \leq rN_1$. In fact, $Z \in \mathcal{L}(rNP'_\infty)$.

Let $S_\ell \subseteq S$ be the set of all places $P \in S$ where $f|_P \in \mathbb{F}_q$ is a non-zero ℓ-th power. Let S'_ℓ be the places of F' that lie over S_ℓ. By Claim 2.22, S_ℓ totally split in F', and so

$$|S'_\ell| = \ell|S_\ell|.$$

In this terminology, our goal is to identify a large vector space of functions f, for which $|S_\ell|$, or equivalently, $|S'_\ell|$, is about right.

4.3 Our result

Our bound will be good for f such that $t = -v_{P'_\infty}(Z) = -v_{P_\infty}(f)$ is close to a multiple of $v_{P_\infty}(X_0)$ which is not a multiple of $\ell \cdot v_{P_\infty}(X_0)$.[11] Formally, write

$$-v_{P_\infty}(f) = -(\ell c_1 + d_1)v_{P_\infty}(X_0) + e_1 \tag{3}$$

where $c_1, d_1, e_1 \in \mathbb{Z}$, $0 < d_1 < \ell$ and $|e_1|$ minimal. We want $|e_1|$ to be small, and if $t = -v_{P_\infty}(f)$ is close to a multiple of $v_{P_\infty}(X_0)$ which is not a multiple of $\ell \cdot v_{P_\infty}(X_0)$, then $|e_1|$ is indeed small. If, however, t is close to a multiple of $\ell \cdot v_{P_\infty}(X_0)$, then, as we do not allow $d_1 = 0$, we must take $|e_1|$ to be fairly large (about $|v_{P_\infty}(X_0)|$).

Let A be some (large) positive integer.

In Section 5 we prove:

Theorem 4.4. *In the above notation, suppose $A < bN - (\ell-1)q|e_1|$ and let $\{a_i\}$ be any basis of $\mathcal{L}(AP'_\infty)$. Then $\{a_i X^{jq} Z^{kq} | j \in \mathbb{N}; 0 \le k < \ell\}$ are independent over $\mathbb{F}_q$.*

In Section 6 we prove:

Theorem 4.5. *In the above notation, assume further*

- $r < \frac{a}{p}$, *and,*
- $\frac{\ell^2}{\ell-1} < \frac{1}{9a+3b}(b - \frac{\ell q|e_1|+1}{N_1})\sqrt{\frac{rp^3}{a}}$.

Then:

$$|S_\ell| \le \frac{bN_1}{\ell}\left(1 + (\ell-1)\sqrt{\frac{rp}{a}} + \frac{\ell(9a+3b)\sqrt{a}(\frac{qr}{b} + \frac{\ell}{\ell-1})}{b\sqrt{rp^3} - \frac{\ell}{\ell-1}(9a+3b)\sqrt{a} - \frac{q\ell|e_1|+1}{N_1}}\right)$$

Note that if p is large and a and $|e_1|$ are small, then we can bound the second error term with:

$$\frac{\ell(9a+3b)\sqrt{a}(\frac{qr}{b} + \frac{\ell}{\ell-1})}{b\sqrt{rp^3} - \frac{\ell}{\ell-1}(9a+3b)\sqrt{a} - \frac{q\ell|e_1|+1}{N_1}} = O(\frac{\ell qr}{b\sqrt{rp^3}}) = O(\frac{\ell}{b} \cdot \sqrt{rp})$$

making it roughly equal to the first error term which is $(\ell-1)\sqrt{\frac{rp}{a}}$.

[11] Recall that $f, X_0 \in \mathcal{L}(P_\infty)$. If f is a polynomial in X_0, i.e., $f = P(X_0)$, then the requirement that $\deg(f)$ is not an ℓ-multiple of $\deg(X_0)$, implies that $\deg(P)$ is coprime to ℓ, and, in particular, f is not an ℓ'th power of a polynomial in X_0.

5 Independence - up-proof with valuations

Before we prove Theorem 4.4 we first focus on a special basis of a relevant Riemann-Roch space:

Let A be some (large) positive integer. Let $T \subseteq \mathbb{N}$ be the set of integers i such that there exists an element $b_i \in \mathcal{L}(P'_\infty)$ with $v_{P'_\infty}(b_i) = -i$.[12] The set $\{b_i\}_{i \in T, i \leq A}$ is a basis of $\mathcal{L}(A \cdot P'_\infty) \subset F'$.

Theorem 5.1. *In the above notation, suppose $A < bN - (\ell - 1)q|e_1|$. Let i, i', j, j', k, k' be non-negative integers, such that $i, i' \leq A$ and $k, k' < \ell$. Then two elements $b_i X^{jq} Z^{kq}$ and $b_{i'} X^{j'q} Z^{k'q}$ have the same P'_∞-valuation if and only if $(i, j, k) = (i', j', k')$.*

Proof. Let us compute $v_{P'_\infty}(b_i X_0^{jq} Z^{kq})$:

$$\begin{aligned} v_{P'_\infty}(b_i X_0^{jq} Z^{kq}) &= v_{P'_\infty}(b_i) + jq \cdot v_{P'_\infty}(X_0) + kq \cdot v_{P'_\infty}(Z) \\ &= -i + jq\ell \cdot v_{P_\infty}(X_0) + kq(\ell c_1 + d_1) \cdot v_{P_\infty}(X_0) - e_1 kq. \end{aligned}$$

Plugging in $v_{P_\infty}(X_0) = -b\frac{N_1}{q}$ we get:

$$\begin{aligned} v_{P'_\infty}(b_i X_0^{jq} Z^{kq}) &= -i - bN_1(\ell j + (\ell c_1 + d_1)k) - e_1 kq \\ &= -\ell b N_1 (j + kc_1 + k\frac{d_1}{\ell} + \frac{i + e_1 kq}{\ell b N_1}) \end{aligned}$$

and so if $v_{P'_\infty}(b_i X_0^{jq} Z^{kq}) = v_{P'_\infty}(b_{i'} X_0^{j'q} Z^{k'q})$ we get that:

$$j - j' + (k - k')(c_1 + \frac{d_1}{\ell}) = \frac{i' - i + (k' - k)qe_1}{\ell b N_1}$$

Which means $\frac{i' - i + (k' - k)qe_1}{\ell b N_1}$ must be an integer multiple of $\frac{1}{\ell}$. However, this quantity (in absolute value) is at most $\frac{A + (\ell - 1)q|e_1|}{\ell b N} < \frac{1}{\ell}$ by the assumption on A. And so we get that $\frac{i' - i + (k' - k)qe_1}{\ell b N} = 0$, giving us

$$j - j' + (k - k')(c_1 + \frac{d_1}{\ell}) = 0$$

Considering the fractional part of this equation and remembering $0 < d_1 < \ell$ gives $k = k'$, which in turn gives us $j = j'$ and $i = i'$, finishing the proof. □

[12] If $g' = \text{genus}(F') > 0$ then T is non-consecutive and contains up to g' gaps. However, it is a semi-group, and is called the Weierstrass semigroup of P'_∞.

Remark 5.2. *In the case where $v_{P_\infty}(f)$ is divisible by ℓ there are two cases to consider. If P_∞ does not split at all, and has a single extension in F' with full relative index, the proof can be modified to get a similar result to theorem 5.1, which is enough for us to continue the analysis as in the later sections of this work. If, however P_∞ has more than one place lying over it in F' the whole framework of our proof is no longer applicable. As the more general case is the one where P_∞ splits in F' we limit ourselves to the case where $v_{P_\infty}(f)$ is not divisible by ℓ for the sake of both simplicity and brevity.*

We are ready to prove Theorem 4.4:

Proof. (of Theorem 4.4) We first prove it for the basis $\{b_i\}_{i \in T, i \le A}$ from Theorem 5.1. Suppose $\sum c_{i,j,k} b_i X^{jq} Z^{kq} = 0$. As all the elements in the sum have distinct valuations at P'_∞, the valuation of the sum is the minimal valuation of $b_i X^{jq} Z^{kq}$ with a non-zero coefficient $c_{i,j,k}$. However, the valuation is $v(0) = \infty$. Hence all the coefficients $c_{i,j,k}$ are zero.

Now suppose $\sum_{j,k} g_{j,k} X_0^{jq} Z^{kq} = 0$ for $g_{j,k} \in \mathcal{L}(AP'_\infty)$. Write each $g_{j,k}$ as $\sum_i c_{i,j,k} b_i$. From the previous argument we see that all $c_{i,j,k}$ are zero, hence all $g_{j,k}$ are zero.

In particular let $\{a_i\}$ be an arbitrary basis of $\mathcal{L}(AP'_\infty)$. Let $g_{j,k} = \sum_i c_{i,j,k} a_i \in \mathcal{L}(AP'_\infty)$ to obtain $g_{j,k} = 0$ for all j, k. From the independence of a_i we conclude that all $c_{i,j,k}$ must be zero, finishing the proof. □

6 Bounding the bias - analysis of the up-proof

In this section we prove Theorem 4.5. We do this using a version of Stepanov method. We remind the reader that $S_\ell \subseteq S$ is the set of all places $P \in S$ where $f|_P \in \mathbb{F}_q$ is a non-zero ℓ-th power, and S'_ℓ is the set of places of F' that lie over S_ℓ. We also saw that by Claim 2.22, S_ℓ totally split in F', and so $|S'_\ell| = \ell |S_\ell|$.

Proof. Set an integer $M < p$ to be determined later. Our goal is to find $0 \ne R \in F'$ such that:

- $\deg(R)$ is not too large, and,
- for every $P' \in S'_\ell$, $v_{P'}(R) \ge M$.

It then follows from Claim 2.2 that $M \cdot |S'_\ell| \leq \deg(R)$ and therefore

$$|S_\ell| \leq \frac{\deg(R)}{\ell M}.$$

We search for R in the following vector space: Let $A < bN_1 - (\ell - 1)q|e_1|$ and B be parameters that will be chosen later. Let $\{a_i\}$ be a basis of $\mathcal{L}(AP'_\infty)$. Set

$$U = \{a_i X_0^{jq} Z^{kq} \mid j < b \text{ and } k < \ell\}$$

We search for R in the $\mathbb{F}_q$-linear span of U. By Theorem 4.4 the elements in U are independent and so the dimension of span(U) is the size of U. Hence,

$$\dim(\mathrm{span}(U)) \geq \ell \cdot B \cdot (A - g' + 1).$$

As $a_i \in \mathcal{L}(AP'_\infty)$, $X_0 \in \mathcal{L}(\ell b \frac{N}{q} P'_\infty)$, and $Z \in \mathcal{L}(rN_1 P'_\infty)$, we see that

$$\mathrm{span}(U) \subseteq \mathcal{L}((A + \ell(B-1)bN_1 + (\ell-1)qrN_1)P'_\infty). \tag{4}$$

In particular, if $R \in \mathrm{span}(U)$ then $\deg(R) \leq A + \ell(B-1)bN_1 + (\ell-1)qrN_1$.

Express $R = \sum c_{i,j,k} a_i X_0^{jq} Z^{kq}$. We want to find a set of linear constraints on $c_{i,j,k}$ that guarantees that $v_{P'}(R) \geq M$ for all $P' \in S'_\ell$. For that end, for $0 \leq m < M$ define:

$$g_m = \omega_m \cdot \sum c_{i,j,k} H^m_{X_0}(a_i) X_0^j Z^k,$$

where $\omega_0 = 1$ and $\omega_m = \omega^{2m-1}$ for $0 < m < M$, and ω is as in Theorem 3.3. We claim that it is enough to require the g_i are zero:

Lemma 6.1. *If $g_0 = g_1 = \ldots = g_{M-1} = 0$ as elements of F' then R vanishes M times on all of S'_ℓ.*

We give the proof in Section 6.1. Our next step is to show each requirement $g_i = 0$ imposes a bounded number of homogeneous linear constraints on the coefficients $c_{i,j,k}$. Specifically,

Lemma 6.2. *For every m,i, j, k, $\omega_m H^m_{X_0}(a_i) X_0^j Z^k \in \mathcal{L}(A_m P'_\infty)$ where $A_0 = A + (B-1)\ell b \frac{N_1}{q} + (\ell-1)rN_1$ and $A_m = A_0 + 3(2m-1)(\ell g + rN_1)$ for $m > 0$.*

We give the proof in Section 6.2.

Now choose a basis for $\mathcal{L}(A_m P'_\infty)$ and represent each $\omega_m H^m_{X_0}(a_i) X_0^j Z^k \in \mathcal{L}(A_m P'_\infty)$ as a vector of length $\dim(A_m P'_\infty)$. Then the constraint $g_m = 0$, where $g_m = \sum c_{i,j,k} \omega_m H^m_{X_0}(a_i) X_0^j Z^k$ and we keep $c_{i,j,k}$ as variables, gives $\dim(A_m P'_\infty) \leq A_m$ linear homogeneous equations in the variables $c_{i,j,k}$.

Altogether we get a system of $\sum_{m=0}^{M-1} A_m$ linear, homogeneous equations in $\ell \cdot B \cdot \dim(AP'_\infty)$ variables. Choosing parameters such that

$$\sum_{m=0}^{M-1} A_m \leq \ell \cdot B \cdot \dim(AP'_\infty),$$

guarantees a non-zero solution R, and then $|S_\ell| \leq \frac{\deg(R)}{\ell M}$.

What is left now is choosing parameters. There are several different parameters, and two conflicting error terms. In 6.3 we explain how to choose the parameters. Roughly speaking, M is chosen to be on the order of $\sqrt{rp^3}$ (assuming some other parameters, like a, b and ℓ are constant). In 6.3 we plug our choices for A, B and M and derive the declared bounds. □

6.1 The sufficiency of the conditions

Proof. (of Lemma 6.1) Fix $P' \in S'_\ell$ and $0 \leq m < M$. Assume $g_m = \omega_m \cdot \left(\sum c_{i,j,k} H^m_{X_0}(a_i) X_0^j Z^k\right)$ is zero as an element of F'. Notice that ω_m is either 1 or ω^{2m-1} where ω is not zero, and so ω_m is never the zero function, meaning it is invertible in F'. Therefore, $\sum c_{i,j,k} H^m_{X_0}(a_i) X_0^j Z^k$ is zero as an element of F'. In particular it is zero on P'.

Now,

$$\begin{aligned} H^m_{X_0}(R)|_{P'} &= H^m_{X_0}(\sum c_{i,j,k} a_i X_0^{jq} Z^{kq})|_{P'} \\ &= (\sum c_{i,j,k} H^m_{X_0}(a_i) X_0^{jq} Z^{kq})|_{P'}, \end{aligned}$$

using Corollary 2.12 and the $\mathbb{F}_q$-linearity of H^m. P' is a degree one place of F', and so $\varphi_{P'}(X_0) = X_0|_{P'}$ and $\varphi_{P'}(Z) = Z|_{P'}$ are both elements of $\mathbb{F}_q$ ($P' \neq P'_\infty$ so X_0 and Z are indeed defined at P'). Therefore

$$\begin{aligned} X_0^q|_{P'} &= \varphi_{P'}(X_0^q) = \varphi_{P'}(X_0)^q = \varphi_{P'}(X_0) = X_0|_{P'}, \\ Z^q|_{P'} &= \varphi_{P'}(Z^q) = \varphi_{P'}(Z)^q = \varphi_{P'}(Z) = Z|_{P'}, \end{aligned}$$

and $H^m_{X_0}(R)|_{P'} = \left(\sum c_{i,j,k} H^m_{X_0}(a_i) X_0^j Z^k\right)|_{P'} = 0$. We conclude that $H^m_{X_0}(R)$ vanishes on P'.

Now X_0 is S-useful, and therefore it is S_ℓ-useful. By Claim 2.23, X_0 is S'_ℓ-useful. As this is true for every $m < M$, Claim 2.9 implies that R vanishes M times on P', and the proof is complete. □

6.2 Describing the constraints

Proof. (of Lemma 6.2) $X_0^j Z^k$ and $\omega_m H^m_{X_0}(a_i)$ are regular at P'_∞. The degree of $X_0^j Z^k$ is at most $(B-1)\ell b\frac{N_1}{q} + (\ell-1)rN_1$. For $m = 0$, the degree of $\omega_m H^m_{X_0}(a_i) = a_i$ is at most A. For $m > 0$ we have $\omega_m H^m_{X_0}(a_i) = \omega^{2m-1} H^m_{X_0}(a_i)$, which by corollary 3.5 is a regular function with degree at most $A + (3g' - 1 + 2\deg(X_0))(2m-1)$, where $g' = \text{genus}(F') \le \ell g + rN_1$.

Altogether, $w_m H^m_{X_0}(a_i) X_0^j Z^k \in \mathcal{L}(A_m P'_\infty)$ for every i, j, k. □

6.3 Analysis of parameters and the bound on S_ℓ

In this part we will show some calculations that dictate the constraints on the parameters A, B and M. The number of constraints is at most

$$\sum_{m=0}^{M-1} A_m \le \sum_{m=0}^{M-1} (A_0 + (6g' + 4b\frac{N_1}{q})m) \;\le\; MA_0 + (6g' + 4b\frac{N_1}{q})\frac{M^2}{2}$$
$$\le MA + (3g' + 2b\frac{N_1}{q})M^2 + M((B-1)\ell b\frac{N_1}{q} + (\ell-1)rN_1).$$

Notice that the number of degrees of freedom is less than ℓBA while the number of constrains is more than MA. Therefore, in order for the number of degrees of freedom to exceed the number of constraints, we must have $M < \ell B$. We shall therefore write

$$\ell B = M + E.$$

We now compare the number of constraints with the number of degrees of freedom, demanding that the number of constraints be smaller:

$$(M+E)(A - g' + 1) > MA + (3g' + 2b\frac{N_1}{q})M^2 + M((B-1)\ell b\frac{N_1}{q} + (\ell-1)rN_1)$$
$$EA > \ell B(g' - 1) + (3g' + 2b\frac{N_1}{q})M^2 + M((B-1)\ell b\frac{N_1}{q} + (\ell-1)rN_1)$$

And so it is enough to ask:

$$\frac{E}{M} > g'(\frac{3M}{A} + \frac{\ell B}{MA}) + 2b\frac{MN_1}{qA} + (B-1)\ell b\frac{N_1}{qA} + (\ell-1)\frac{rN_1}{A} \tag{5}$$

With the above notation we restate the bound on $|S_\ell|$, using eq. (4) that states that $\deg(R) \leq A + \ell(B-1)bN_1 + (\ell-1)qrN_1$. We have

$$\begin{aligned} |S_\ell| \leq \frac{\deg(R)}{\ell M} &\leq \frac{A}{\ell M} + \frac{\ell(B-1)bN_1}{\ell M} + \frac{(\ell-1)qrN_1}{\ell M} \\ &< \frac{A}{\ell M} + \frac{(M+E)bN_1}{\ell M} + \frac{(\ell-1)qrN_1}{\ell M} \\ &< \frac{bN_1}{\ell}\left(1 + \frac{E}{M} + \frac{(\ell-1)qr}{bM} + \frac{A}{bN_1M}\right) \end{aligned}$$

and so

$$|S_\ell| < \frac{bN_1}{\ell}\left(1 + \frac{E+1}{M} + \frac{(\ell-1)qr}{bM}\right).$$

We note that since $\frac{E}{M} = \frac{B\ell - M}{M}$ is an error term, if it exceeds ℓ we get a trivial bound. So we assume $B \leq M$.

The probability a random number in F_q^x is a non-zero ℓ-th power is $\frac{1}{\ell}$. Thus, the term $\frac{N_1}{\ell}$ is about the expectation in a random process, assuming $S \subseteq \mathbb{P}^1_F \setminus P_\infty$ is a large faction of all degree one places. We have a multiplicative loss of b that we ignore. Other than that we have an error term $\mathbb{E}$ which is the sum of two error terms: $\mathbb{E} = \frac{E+1}{M} + \frac{(\ell-1)qr}{bM}$ and our bound on $|S_\ell|$ is minimal when the sum of these two error terms is minimal.

At first glance it would appear that the error shrinks as the value of M grows, leading us to taking a maximally large value of M. However further inspection reveals that $\frac{E}{M}$ actually increases as the value of M grows, leading to a tradeoff and an optimal choice for the value of M.

Let us break down the two error terms, starting with $\frac{E+1}{M}$. From Equation (5) we need to have:

$$\frac{E}{M} > g'(\frac{3M}{A} + \frac{\ell B}{MA}) + 2b\frac{MN_1}{qA} + (B-1)\ell b\frac{N_1}{qA} + (\ell-1)\frac{rN_1}{A}$$

Recalling our bounds on g' and g as noted in Section 4, namely $g' \leq \ell g + rN_1 \leq N(\frac{a\ell}{p} + r)$ we get that it is enough to have:

$$\frac{E}{M} \geq \frac{N_1}{A}\left((3M + \frac{\ell B}{M})(\frac{a\ell}{p} + r) + \frac{2bM + (B-1)\ell b}{q} + r(\ell - 1)\right)$$

We saw $B \leq M$. We will also assume $\ell \leq M$ and get it is enough to have:

$$\frac{E}{M} \geq \frac{MN_1\ell}{A}\left(\frac{4a}{p} + \frac{4r}{\ell} + \frac{3b}{q} + \frac{r(\ell-1)}{M\ell}\right) \tag{6}$$

From here it is rather easy to see that the error term $\frac{E}{M}$ grows as M grows.

The second error term is $\frac{(\ell-1)qr}{bM}$, which decays linearly in M. Since one error term grows with M and the other decays with M, the minimal error is at least half the error when the two terms are equal,[13] giving us a rough estimation for what the best value of M should be.

Equating the error terms we get:

$$\frac{(\ell-1)qr}{bM} \approx \frac{MN_1\ell}{A}(\frac{4a}{p} + \frac{4r}{\ell} + \frac{3b}{q} + \frac{r(\ell-1)}{M\ell})$$

Assuming $A = \Theta(bN_1)$, and that r is small (which turns out to be necessary) we get that the optimal choice of M is $M = \Theta\left(\sqrt{\frac{rp^3}{a}}\right)$

Putting aside the estimations above, we shall now give a choice for the parameters A, B, M and prove theorem 4.5

Proof of theorem 4.5. First we choose

$$\begin{aligned} A &= bN_1 - q\ell|e_1| - 1, \\ M &= \lfloor \frac{\ell-1}{\ell(9a+3b)} \frac{A}{N_1} \sqrt{\frac{rp^3}{a}} \rfloor, \\ B &= \lceil \frac{M}{\ell}(1 + \frac{MN_1\ell}{A}(\frac{4a}{p} + \frac{4r}{\ell} + \frac{3b}{q} + \frac{r(\ell-1)}{M\ell}))\rceil \end{aligned}$$

and denote $E = \ell B - M$.

We check that these choices satisfy our constraints. First,

[13] To see that assume the two term are equal when they have value a. Then the error that we get when they are equal is $2a$, and the minimal error is at least a.

- $A < bN_1 - q(\ell-1)|e_1|$, and,
- $M < p$ since $r < \frac{a}{p}$ and $A < N(9a+3b)$.

Also,

Claim 6.3. *$B \leq M$.*

Proof. It is enough to show that:

$$(1 + \frac{MN_1\ell}{A}(\frac{4a}{p} + \frac{4r}{\ell} + \frac{3b}{q} + \frac{r(\ell-1)}{M\ell})) \leq \ell.$$

Since $r < \frac{a}{p}$ it is enough to show that:

$$M \leq \frac{\ell-1}{\ell}\frac{A}{N_1}\frac{p}{9a+3b}$$

which holds because $r < \frac{a}{p}$. □

Also

Claim 6.4. *$\ell \leq M$.*

Proof. Since ℓ is an integer it is enough to show that $\ell < \frac{\ell-1}{\ell(9a+3b)}\frac{A}{N_1}\sqrt{\frac{rp^3}{a}}$, which holds because of our choice of A and the condition on ℓ in the statement of theorem 4.5. □

Also note that

$$E = \ell B - M \geq M\frac{MN_1\ell}{A}(\frac{4a}{p} + \frac{4r}{\ell} + \frac{3b}{q} + \frac{r(\ell-1)}{M\ell})$$

and therefore, due to Equation (6), if $B \leq M$ and $\ell \leq M$ then

$$\frac{E}{M} > g'(\frac{3M}{A} + \frac{\ell B}{MA}) + 2b\frac{MN_1}{qA} + (B-1)\ell b\frac{N_1}{qA} + (\ell-1)\frac{rN_1}{A}$$

as desired.

This concludes the check that our choices satisfy our constraints. We conclude that $|S_\ell| < \frac{bN_1}{\ell}\left(1 + \frac{E+1}{M} + \frac{(\ell-1)qr}{bM}\right)$. Substituting the values of M and E we get $|S_\ell| < \frac{bN_1}{\ell}\left(1 + \mathbb{E}\right)$ where

$$\begin{aligned}
\mathbb{E} &\leq \frac{E+1}{M} + \frac{(\ell-1)qr}{bM} \\
&\leq \frac{MN_1\ell}{A}\left(\frac{4a}{p} + \frac{4r}{\ell} + \frac{3b}{q} + \frac{r(\ell-1)}{M\ell}\right) + \frac{\ell}{M} + \frac{(\ell-1)qr}{bM} \\
&\leq \frac{\ell-1}{p}\sqrt{\frac{rp^3}{a}} + \frac{b\ell + (\ell-1)qr}{bM} \\
&\leq (\ell-1)\sqrt{\frac{rp}{a}} + \frac{\ell(9a+3b)\sqrt{a}\left(\frac{qr}{b} + \frac{\ell}{\ell-1}\right)}{b\sqrt{rp^3} - \frac{\ell}{\ell-1}(9a+3b)\sqrt{a} - \frac{q\ell|e_1|+1}{N}},
\end{aligned}$$

completing the proof. □

References

[BATS09] Avraham Ben-Aroya and Amnon Ta-Shma. Constructing small-bias sets from algebraic-geometric codes. In *Foundations of Computer Science, 2009. FOCS'09. 50th Annual IEEE Symposium on*, pages 191–197. IEEE, 2009.

[Bom06] Enrico Bombieri. Counting points on curves over finite fields: d'après sa stepanov. In *Séminaire Bourbaki vol. 1972/73 Exposés 418–435*, pages 234–241. Springer, 2006.

[BSC13] Ben Blum-Smith and Samuel Coskey. The fundamental theorem on symmetric polynomials: History's first whiff of galois theory. *The College Mathematics Journal*, 48, 01 2013.

[Gol03] David M. Goldschmidt. *Algebraic Functions and Projective Curves*, volume 215. Springer New York, NY, 2003.

[GS96] Arnaldo Garcia and Henning Stichtenoth. On the asymptotic behaviour of some towers of function fields over finite fields. *Journal of Number Theory*, 61(2):248–273, 1996.

[GS98] Venkatesan Guruswami and Madhu Sudan. Improved decoding of reed-solomon and algebraic-geometric codes. In *Proceedings 39th Annual Symposium on Foundations of Computer Science (Cat. No. 98CB36280)*, pages 28–37. IEEE, 1998.

[GX12] Venkatesan Guruswami and Chaoping Xing. Folded codes from function field towers and improved optimal rate list decoding. *CoRR*, abs/1204.4209, 2012.

[Jeo11] Sangtae Jeong. Calculus in positive characteristic p. *Journal of Number Theory*, 131(6):1089–1104, 2011.

[Mas84] R. C. Mason. *Diophantine Equations over Function Fields*. London Mathematical Society Lecture Note Series. Cambridge University Press, 1984.

[SAK$^+$01] K.W. Shum, I. Aleshnikov, P.V. Kumar, H. Stichtenoth, and V. Deolalikar. A low-complexity algorithm for the construction of algebraic-geometric codes better than the gilbert-varshamov bound. *IEEE Transactions on Information Theory*, 47(6):2225–2241, 2001.

[Sch06] Wolfgang M Schmidt. *Equations over finite fields: an elementary approach*, volume 536. Springer, 2006.

[Ste69] Sergei Aleksandrovich Stepanov. On the number of points of a hyperelliptic curve over a finite prime field. *Mathematics of the USSR-Izvestiya*, 3(5):1103, 1969.

[Sti09] Henning Stichtenoth. *Algebraic function fields and codes*, volume 254. Springer Science & Business Media, 2009.

[Tao14] Terry Tao. The bombieri-stepanov proof of the hasse-weil bound. `https://terrytao.wordpress.com/2014/05/02/the-bombieri-stepanov-proof-of-the-hasse-weil-bound/`, 2014.

[Tor00] Fernando Torres. The approach of stöhr-voloch to the hasse-weil bound with applications to optimal curves and plane arcs, 2000.

[Xin95] Chaoping Xing. On automorphism groups of the hermitian codes. *IEEE Transactions on Information Theory*, 41(6):1629–1635, 1995.

A Some examples of function fields

A.1 The rational function field

Let us consider $F = \mathbb{F}_5(x)$, the rational function field over the field with five elements. The elements of F are the rational functions in x. F/K has a degree one place P_∞ corresponding to a 'point at infinity'. A rational function vanishes at P_∞ if the denominator has a higher degree as a polynomial than the numerator. More generally the valuation corresponding to P_∞ is v_∞ defined by $v_\infty(\frac{f(x)}{g(x)}) = \deg(g) - \deg(f)$.

The evaluation function (also known as residue class map) associated with P_∞ is ϕ_∞, it is defined over all $\frac{f(x)}{g(x)}$ such that $n = \deg(g) \geq \deg(f)$ and if $g(x) = \sum_{i=0}^{n} g_i x^i$ and $f(x) = \sum_{i=0}^{n} f_i x^i$ then $\phi_\infty(\frac{f(x)}{g(x)}) = \frac{f_n}{g_n}$ (note that f_n might be zero but g_n is not zero). All other places of F are places associated with irreducible polynomials in $\mathbb{F}_5[x]$. Let $h(x) \in \mathbb{F}_5[x]$ be some irreducible polynomial, then it defines a place of degree $\deg(h)$ denoted P_h. The valuation v_h associated with it is $v_h(\frac{f(x)}{g(x)}) =$ "the number of times h divides f minus the number of times h divides g". the associated evaluation ϕ_h is defined on all $\frac{f(x)}{g(x)}$ where h divides g fewer times than h divides f. ϕ_h can be calculated in two equivalent ways either $\phi_h(\frac{f(x)}{g(x)}) = \frac{f(x)}{g(x)}(\text{mod} h)$ or $\phi_h(\frac{f(x)}{g(x)}) = \frac{f(\alpha)}{g(\alpha)}$ where $\alpha \in \mathbb{F}_{5^{\deg(h)}}$ is such that $h(\alpha) = 0$.

The divisor of a rational function $\frac{f(x)}{g(x)} = c * \prod a_i(x)^{e_i}$ where $c \in \mathbb{F}_5[x]$, a_i are distinct irreducible polynomials and $e_i \in \mathbb{Z}$ is $(\frac{f(x)}{g(x)}) = (\deg(g) - \deg(f))P_\infty + \sum e_i P_{a_i}$. Since the degree of a place P_h is exactly $\deg(h)$ it is clear that for every rational function this divisor is of degree 0, and that the divisor is trivial if and only if the function is a constant. In the other direction, if a divisor $KP_\infty + \sum e_i P_{a_i}$ is of degree zero then its Riemann-Roch space is exactly $c * \prod a_i(x)^{-e_i}$ (where $c \in \mathbb{F}_5$) which is 1 dimensional as a vector space over $\mathbb{F}_5$, just as the Riemann-Roch theorem (Theorem 2.3) predicts. In the more general case if $D = KP_\infty + \sum e_i P_{a_i}$ is some divisor of positive degree then

$$\mathcal{L}(D) = \mathsf{Span}\left\{x^j \prod a_i(x)^{-e_i} \mid 0 \leq j \leq \deg(D)\right\}$$

and this space is of dimension $\deg(D) + 1$.

The derivative with respect to x in F is exactly like the derivative of a rational function in analysis (we just need to remember our arithmetic operations all take place in the field $\mathbb{F}_5$). if we want to derive a function z with respect to y instead of x we can use the chain rule $D_y(z) = \frac{dz}{dy} = \frac{dz}{dx}\frac{dx}{dy} = D_x(z)\frac{1}{D_x(y)}$. For Hasse derivatives we can expand a rational function $\frac{f(x)}{g(x)}$ as a power series in x (or in $x - c$ for $c \in \mathbb{F}_5$ if we so desire) and then use

$$H_x^m(\sum_{n=n_0\in\mathbb{Z}}^{\infty} c_n x^n) = \sum_{n=n_0\in\mathbb{Z}}^{\infty} c_n \binom{n}{m} x^{n-m}$$

to compute the Hasse derivative of $\frac{f(x)}{g(x)}$. Note that the value at 0 of the m-th Hasse derivative is exactly the coefficient of x^m in the power series (so long as $\frac{f(x)}{g(x)}$ is defined at zero, meaning there are no terms of the form x^{-k} and so the Hasse derivative has a value at zero). We refer the reader to the end of section 2.2 for an example of a canonical divisor in $K(x)/K$.

A.2 The Hermitian function field

Let p be a prime power and denote $q = p^2$. The Hermitian function field is $F = \mathbb{F}_q(x, y)/\varphi(x, y)$ where $\varphi(x, y) = \mathsf{Tr}_{\mathbb{F}_p}^{\mathbb{F}_q}(y) - \mathsf{N}_{\mathbb{F}_p}^{\mathbb{F}_q}(x) = y^p + y - x^{p+1}$. The genus of F is $\frac{p(p-1)}{2}$. When viewed as an extension of $\mathbb{F}_q(x)$, the infinite place is fully ramified, and all other degree one places are fully split, giving a total of $p^3 + 1$ degree one places. The degree one places other then infinity (which is denoted P_∞) correspond to pairs $(\alpha, \beta) \in \mathbb{F}_q^2$ with $\mathsf{Tr}(\beta) = \mathsf{N}(\alpha)$ and denoted $P_{\alpha,\beta}$. The function x is "useful for the set of all degree one places except P_∞ while y is "useful" for all degree one places $P_{\alpha,\beta}$ with $\alpha \neq 0$ (this is a set of size $p^3 - p$).

x has p poles at P_∞ and p simple zeroes (at points $P_{0,\beta}$ with $\mathsf{Tr}(\beta) = 0$). y has $p+1$ poles at P_∞ and $p+1$ zeroes at $P_{0,0}$. x and y are both regular (poles only at P_∞). In fact, powers of x and y form a basis for the space of regular functions, namely - $\mathcal{L}(kP_\infty) = \mathsf{Span}\left\{x^i y^j \mid pi + (p+1)j \leq k\right\}$ and since $x^{p+1} \in \mathsf{Span}\{y, y^p\}$ it is enough to take $i \leq p$.

We refer the reader to the end of section 2.2 for an example of a canonical divisor in the Hermitian function field.

A.3 The Hermitian tower

A lot of what we bring here is presented in [GX12, Section 3.1]. The Hermitian tower is a generalization of the Hermitian function field. With the same definitions of $p, q, \mathbb{F}_q, \varphi$, the e-level Hermitian tower is $F_e = \mathbb{F}_q(x_1, ...x_e)$ where $\varphi(x_i, x_{i+1}) = 0$. F_1 is just a rational function field, while F_2 is the Hermitian function field. the point at infinity is fully ramified at each level of the tower, and so is fully ramified at F_e. Each of the other q degree one places of $F_1 = \mathbb{F}_q(x_1)$ is fully split at every level of the tower and so has p^{e-1} points lying over it in F_e. The degree one places of F_e except infinity correspond to tuples $(\alpha_1, \alpha_2, ...\alpha_e)$ with $\varphi(\alpha_i, \alpha_{i+1}) = 0$. So the e level tower has $1 + p^{e+1}$ places of degree one, roughly multiplying by a factor of p at every level of the tower.

The genus of F_e is $g_e = \frac{1}{2}(\sum_{i=1}^{e-1} p^e(1 + \frac{1}{p})^{i-1} - (p+1)^{e-1} + 1)$ and when $2e \leq p$ we get $g_e \leq ep^e$, so the genus also increases at every level by about a factor of p.

$x_i \in F_e$ are regular functions with pole order $-v_{P_\infty}(x_i) = p^{e-i}(p+1)^{i-1}$. The zeroes of x_i are at the places matching the tuples $(0, ..., 0, \alpha_{i+1}, ..., \alpha_e)$, these are p^{e-i} places, each of them with degree one and the valuation of x_i there is $(p+1)^{i-1}$. x_1 is "useful" for all the degree one places except infinity, and each other x_i is "useful" for the set of degree one places where α_{i-1} is non-zero.

The Riemann-Roch spaces of regular functions are spanned by monomials in x_i:

$$\mathcal{L}(kP_\infty) = \mathsf{Span}\left\{x_1^{j_1} \cdots x_e^{j_e} \mid \sum j_i p^{e-i}(p+1)^{i-1} \leq k\right\}$$

A.4 The GS tower

A lot of what we bring here is presented in [GS96, Section 3] and we invite the reader to read further in order to fully admire the intricacies of what happens in the GS tower.

For p a prime power and $q = p^2$ the e-level GS tower is defined as $F_e =$

$\mathbb{F}_q(x_1,...x_e)$ where $\psi(x_i,x_{i+1})=0$ for

$$\psi(x,y)=y^p+y-\frac{x^p}{x^{p-1}+1}=\mathsf{Tr}(y)-\frac{\mathsf{N}(x)}{\mathsf{Tr}(x)}$$

The genus of F_e is less than p^e. Each point P_α of $F_1=\mathbb{F}_q(x_1)$ for α with $\mathsf{Tr}(alpha)\neq 0$ splits completely in F_e. Giving a set is of size $p^e(p-1)$ of degree one places, and x_1 is "useful" for this set. P_∞ is totally ramified in F_e and all of the poles of x_1 are there. $x_1, x_2...x_e$ are all of degree p^{e-1} but only x_1 is regular, the rest have poles at certain degree one places that correspond to $(\alpha_1,..\alpha_e)$ where some of the α_i-s have trace 0 or even to places where some of the x_i have poles.

In [SAK$^+$01] an algorithmic process for finding a basis for the Riemann-Roch space $\mathcal{L}(kP_\infty)$ is specified.

B Miscellaneous proofs

Proof of claim 2.14. Let $f\in F/K$, $P\in\mathbb{P}_F$, $t\in F$ with $v_P(t)=1$. We are interested in $(df)^F$ the divisor of df over F. We move to $\bar{F}/\bar{K}=\bar{K}\cdot F/K=\bar{K}F/\bar{K}$ which is the constant field extension of F/K with all of $\bar{K}$, the algebraic closure of K. Let $\bar{P}\in\mathbb{P}_{\bar{F}}$ be a place lying over P. Since $\bar{K}$ is algebraically closed we know $\deg(\bar{P})=1$. From [Sti09, Theorem 3.6.3] we learn that $v_{\bar{P}}(t)=v_P(t)=1$ and we can write:

$$f=\sum_{n=n_0\in\mathbb{Z}}^{\infty}c_nt^n \quad (c_n\in\bar{k}, c_{n_0}\neq 0)$$
$$D_t^1(f)=\sum_{n=n_0\in\mathbb{Z}}^{\infty}n\cdot c_nt^{n-1} \quad (c_n\in\bar{k}, c_{n_0}\neq 0)$$

From the definition of valuation for differential we know that

$$v_{\bar{P}}(1df)=v_{\bar{P}}(D_t^1(f)dt)=v_{\bar{P}}(D_t^1(f))\geq n_0-1$$

From [Sti09, Theorem 3.6.3] we know that $v_{\bar{P}}(1df)=v_P(1df)$ and $v_P(f)=v_{\bar{P}}(f)$ and so we get $v_P(1df)\geq v_P(f)-1$. Furthermore, if f has no pole at P, then f has no pole at $\bar{P}$ and so $n_0\geq 0$ and so $D_t^1(f)$ has no pole at $\bar{P}$ and therefore at P, meaning $v_P(1df)\geq 0$. □

C Documentation of research exceeding the scope of the main work

Remark C.1. *Regarding the choice of X_0 - we could pick Y that is S-useful, and X_0 that is regular and defined at places of S without capturing them. In this case we would pay for Y in the application of the DHB. However, if Y is regular it doesn't incur an extra cost in DHB, so finding a small function that is regular and also S-useful is the best. If, however, we fail to find a small regular function that is S-useful we could find a small regular function, and find a small S-useful function separately.*

C.1 Nontrivial values of multiplicative character

In theorem 4.5 we bound the number of places of S where f is a nonzero ℓ-th power. This can be interpreted as the number of places $P \in S$ where f is non-zero and the character $\chi : \mathbb{F}_q^\times \to \mathbb{Z}/\ell\mathbb{Z}$ gives 0 when applied to $f|_P$. It is also interesting to bound the number of times $\chi(f|_P)$ is equal to any $0 < t < \ell$. to achieve this bound note that for $\gamma \in \mathbb{F}_q^\times$ applying theorem 4.5 to γf gives a bound on the number of places from S where $\chi(f|_P) = -\chi(\gamma)$. It is also interesting to get a lower bound on these quantities, rather than just an upper bound. In the book of Schmidt [Sch06] there might be some tricks as to how to do this better than the obvious way, considering N, N_0, N_1, N_2 as he defines them on page 16 an utilizes them on page 22 (and other places perhaps). Here we give the simplest way to get a lower bound. Since f is defined on all of S, then for every $P \in S$ either f vanishes at P or $\chi(f|_P)$ is some number between 0 and $\ell - 1$. From claim 2.2 we have an upper bound on the number of places where f vanishes - rN, and from theorem 4.5 we have an upper bound on the size of the preimage of each number $< \ell$ under χ. The sum of the sizes these $\ell + 1$ sets is precisely $|S|$ so combining all of the upper bounds with the sum gives us a lower bound, it has a larger error term (by a multiplicative factor of $(\ell - 1)$ and an additive factor of rN) but it is still a correct lower bound achieved without further research or additional techniques.

C.2 Down proof independence and analysis

The "up proof" is nice because it does not use a lot of information about the function field F. However, it has a big problem. Since we want to work in F' and want P'_∞ to be fully ramified we must limit ourselves to working with function $f \in F$ with pole order that is coprime to ℓ. For comparison see remark C.3.

another problem with the up proof is, that we pay the maximum possible payment for each derivative, namely $g' \approx \ell g + rN$ (this is due to theorem 3.3). Ideally we would like to get a more direct bound on the number of linear constraints each derivative incurs by way of using a specific set monomials, and keeping track of how each derivative looks - if we can show a derivative lives in some relatively small linear space we only need to pay its dimension, and perhaps that will be less than $O(m(\ell g + rN))$.

The "down proof" means picking R from a space U of monomials in F, and demanding it vanish at the places of S_ℓ which are places of F/K, without ever discussing $F' = F(Z)$. Our choice of U will be $\{a_i X_0^{jq} f^{k(q-1)/\ell}\}$ where $a_i \in \mathcal{L}^F(AP_\infty)$, $j < B$ and $k < \ell$.

We present a brief version of an analogue of theorem 4.4:

Theorem C.2. *Suppose $\ell A < bN - (\ell - 1)(|v_{P_\infty}(f)| + q|e_1|)$ and $\{a_i\}$ is some (any) basis for $\mathcal{L}(AP'_\infty)$. Suppose we have a vanishing combination*

$$0 = \sum c_{i,j,k} a_i X_0^{jq} f^{k(q-1)/\ell};\ j \in \mathbb{N},\ 0 \le k < \ell,\ c_{i,j,k} \in \mathbb{F}_q$$

then all $c_{i,j,k}$ are zero.

Proof. The crux of the proof is showing that elements of the form $b_i X_0^{jq} f^{k(q-1)/\ell}$ have distinct valuations when either i, j or k are different (here b_i is a basis for $\mathcal{L}(AP_\infty)$ where $v_{P_\infty}(b_i) = -i$). by computing and lugging in $v_{P_\infty}(X_0) = -b\frac{N}{q}$ we get:

$$\begin{aligned}
v_{P_\infty}(b_i X_0^{jq} f^{k(q-1)/\ell}) &= v_{P_\infty}(b_i) + jq v_{P_\infty}(X_0) + k\frac{(q-1)}{\ell} v_{P_\infty}(f) \\
&= -i - jbN + \frac{1}{\ell} kq((\ell c_1 + d_1)(-b\frac{N}{q}) + e_1) - \frac{k}{\ell} v_{P_\infty}(f) \\
&= -i - jbN - bNk(c_1 + \frac{d_1}{\ell}) + \frac{e_1 kq}{\ell} - \frac{k}{\ell} v_{P_\infty}(f) \\
&= -bN\left(j + kc_1 + \frac{kd_1}{\ell} + \frac{\ell i + k v_{P_\infty}(f) - kqe_1}{bN\ell}\right)
\end{aligned}$$

Which means that if $\ell A < bN - (\ell - 1)(|v_{P_\infty}(f)| + q|e_1|)$ the only way for two expressions of this form to be equal is to have $i = i', j = j', k = k'$. The rest of the proof is identical to theorem 4.4 □

Remark C.3 (An incredible remark!)**.** *This independence proof (theorem C.2) works even when the degree of f is a multiple of ℓ, but the main theorem of the bound on the size of S_ℓ does not hold for functions that are ℓ-th powers. We believe the explanation for that is that there cannot be ℓ-th powers with degree significantly below the genus without, in some sense being powers of X_0 or at least having pole order that is very close to that of some power of X_0^ℓ, meaning the error e_1 will have to be huge and A would have to be too small to give an effective bound on S_ℓ.*

As for achieving the bound on $|S_\ell$, we proceed with the polynomial method. However instead of using a polynomial from the span of $U = \{a_i X_0^{jq} f^{k(q-1)/\ell}\}$, we define $R = f^M Q$ where Q is from the span of Q. The motivation for doing this is that when we derive Q one of the terms looses the $f^{k(q-1)/\ell}$ part, as the derivative of $f^{k(q-1)/\ell}$ is $f^{-1+k(q-1)/\ell} H^1(f)$. We wish to keep the $f^{k(q-1)/\ell}$ since whenever $P \in S_\ell$ we have $f|_P^{k(q-1)/\ell} = f|_P(q-1)/\ell^k = 1^k = 1$ and so f vanishes from the equations. With the form $R = f^M Q$ we get (from the product rule) that

$$H^m(R) = f^{M-m} \sum c_{i,j,k} a_i X_0^{jq} f^{k(q-1)/\ell} \sum_{s<m} H^s a_i H^{m-s} f$$

and by considering $\omega^{2m-1} \sum_{s<m} H^s a_i H^{m-s} f$ and applying theorem 3.3 we get a bound for the number of linear constraints it would take to force R to vanish M times at S_ℓ.

Remark C.4. *Notice that since $R = f^M Q$ and Q is a regular function, R also vanishes M times wherever f vanishes. This slightly affects the calculation on the upper and lower bounds we get.*

We now present a short-form version of the calculation of the parameters of the down proof:

The degrees of freedom - at least $\ell B(A - g + 1)$

Constraints - since we have $H^s a_i H^{m-s} f$ we still need to use theorem 3.3, and so we pay for the genus, but only for the genus of F and not the larger genus of F' (since F' does not appear in this proof at all). The analogue we would get for lemma 6.2 would bound the degree of

$$\sum c_{i,j,k} X_0^j \omega^{2m-1} \sum_{s<m} H^s a_i H^{m-s} f$$

with

$$A_m = (B-1)b\frac{N}{q} + (2m-1)(3g-1) + A + rN$$

and summing over $m < M$ would give a total number of constraints of

$$MA + (M-1)^2(3g-1) + M((B-1)b\frac{N}{q} + rN)$$

Together these give (in a way analogue to section 6):

$$\frac{E}{M} > \frac{M}{A}(3g-1) + (B-1)b\frac{N}{qA} + \frac{rN}{A}$$

The degree of R is bounded by $MrN + A + BbN + (q-1)rN\frac{\ell-1}{\ell}$ and the bound we get on $|S_\ell|$ is $\frac{\deg(R)}{M}$ which assuming A is close enough to bN is bounded by:

$$|S_\ell| < \frac{bN}{\ell}\left(1 + 2(\frac{E}{M} + \frac{\ell r q}{bM})\right)$$

optimizing for smallest error terms gives a choice of $M \approx \sqrt{\ell r q}$ and error term $O(\sqrt{\ell r q})$.

Remark C.5. *It appears that the dependence in ℓ is different between the up proof and the down proof. This calls for a deeper dive into the exact choice of the parameters.*

Remark C.6. *Notice that while we did not to pay for rN in g' (through the application of theorem 3.3), we did need to pay for it in the degree of R, since we had to multiply Q by f^M to maintain the nice form for our equations (having f appear with power that is an integer multiple of $\frac{q-1}{\ell}$). It seems that we cannot dodge the combined payment of $O(g)$ and $O(rN)$, which leads us to try to look for methods that avoid these payments even if only for a special case of a specific curve. This leads us to appendix C.3*

C.3 Custom independence for Hermitian curve - proof without valuations

We would like to get results of the form of theorem 4.5 for functions that are not necessarily close to a multiple of the pole order of X_0, but rather any function f that is not an ℓ-th power in F or a constant field extension of F. The independence claim which is the basis for our use of the polynomial method is highly reliant upon these "modular" properties of the pole order of f because the argument hinges on corollary 2.1. Instead of that argument we would like to use a modified version of [Sch06, Chapter I, section 5]. This will be challenging because we are working over some function field F/K while Schmidt works over the rational function field $K(X)/K$. There are a few key properties of the rational function field that come in useful during the proof but are not trivial for us when trying to adapt the argument to a different setting:

1. The derivative of a polynomial is polynomial with fewer poles.
2. There is a single element X which is "useful" for all degree one places of $K(X)/K$ except one.
3. This X has small pole order and only a simple zero.

We will now explain how we prove an independence claim (more similar to that of the down proof than the up proof) for the Hermitian curve $F/\mathbb{F}_q$ for bounding the number of ℓ-th powers a function $f \in \mathcal{L}(rNP_\infty)$ takes at the non-infinite degree one places of the curve, under the assumption that $Z^\ell - f(X,Y)$ is absolutely irreducible mod $\varphi(X,Y)$, meaning it is irreducible in $\left(\overline{\mathbb{F}_p}(X,Y)/\varphi(X,Y)\right)[Z]$. If $\ell > 2$ we also need the assumption that f is not of the form $f = xh$ for h that is a regular function. This additional assumption may be removed with further research.

C.3.1 Monomial form

Following the idea of the down proof, we will work in F rather than F' and use powers of $f^{\frac{q-1}{\ell}}$. However, unlike the proofs above we will not take a whole basis for $\mathcal{L}(AP_\infty)$, but rather use a very particular linear space of regular functions which will enable us to have more information about the derivatives of $R = f^M Q$. We will select Q from the span of $U = \left\{x^{i_1} y^{i_2} y^{i_3 p} y^{i_4 q} f^{i_5 (q-1)/\ell} \mid i_1 + i_2 < A;\ i_3 < C;\ i_4 < D;\ i_5 < \ell\right\}$. We call these select function monomials, and the main goal of this section is to show a proof of their independence. If you want some intuition for the sizes, A, C should be thought of as $\frac{p}{10}$ and D should be though of like B from the up proof. Indeed if $A \approx p$ and $C \approx p - 1$ the $x^{i_1}y^{i_2}y^{i_3p}$ would be a basis for $\mathcal{L}NP_\infty$ much like $\{b_i | i < A\}$ were. It turns out that these "holes" won't harm the analysis too much, though a deep dive into the parameters is in order for further research. The form of the monomials we use has several beneficial properties when considered alongside the properties of the Hermitian function field:

1. The derivative with respect to x of regular functions is regular, and the derivative with respect to y of a regular function is $\frac{1}{x^p}$ times a regular function
2. Any regular function in F (and in particular $f, x^p H_y^1(f)$) has a representation as a polynomial in x and y
3. x is "useful" for all degree one places except P_∞. We will be deriving with respect to x. The derivative of x is 1 and the derivative of y is x^p.
4. Since this is the Hermitian curve and $x^{p+1} = y^p + y$.
5. y has a zero only at the point $P_{0,0}$ and that zero is with valuation $p+1$. x has a simple zero at $P_{0,0}$.

The algebraic relation between x and y is particularly useful since when we get an "unwanted" x^p from deriving a y, we can "steal" an existing x and write the derivative as a combination of other monomials, though we will perhaps need larger bounds on the degrees. This means it is more convenient to work with $i_1 \geq M$ so we always have an x to steal. The increase in the bounds after each consecutive derivation is that A needs to increase by one less than the total degree of f (viewed as a polynomial in x and y), and C needs to increase by one. By "accommodating" the additional terms that appear in the derivative into the $x^{i_1}y^{i_2}y^{i_3p}$-part of the monomials we manage to easily identify a linear space of functions to which the m-th derivative of R belongs, thus getting a clear bound on the number of linear constraints needed to make it vanish without applying theorem 3.3.

Remark C.7. *Since we avoid using theorem 3.3 the analogues for the various lemmas of section 6 stay correct even for values of M which are above* *the characteristic and even further. In particular this form of proof for the Hermitian curve the only result we demonstrate over $\mathbb{F}_q$ for $q = p^2$ where p is some prime power that is not itself prime. This is an important benefit which demands further research into more delicate choices of monomials / linear spaces.*

There is a small technical detail that is important to note when working with M larger than the characteristic - the Hasse derivative is no longer the iterated derivative up to a constant, so one should carefully analyze the form of the Hasse derivatives of R. In the case of the Hermitian curve it is possible to analyze the form of the hasse derivative of f^M times a monomial for specific choices of monomial families, though we warn this needs to be handled with care.

We shall prove the monomials of U are independent by way of the following theorem:

Theorem C.8. *Let f be a regular function in the Hermitian function field such that $Z^\ell - f$ is absolutely irreducible*[14]. *Assume $f|_{P_{0,0}} \neq 0$ (or, when viewing f as a polynomial in x and y and assume $f(0,0) \neq 0$). The monomials $x^{i_1} y^{i_2} y^{jp} f^{k(q-1)/\ell}$ are independent whenever $0 \leq k < \ell$ and $(p+1)A < \frac{q}{\ell} - \frac{(\ell-1)|v_{P_\infty}(f)|}{\ell}$. Note we did not restrict the value of j.*

Note the additional assumption that $f|_{P_{0,0}} \neq 0$. We partially address this assumption in appendix C.3.4

C.3.2 The special case $\ell = 2$

We begin by proving theorem C.8 for the case $\ell = 2$. the proof for this case is somewhat simpler and aids in understanding the proof of the general case.

Proof. Let

$$0 = \sum c_{i_1,i_2,j,k} x^{i_1} y^{i_2} y^{jp} f^{k(q-1)/2} \tag{7}$$

be a vanishing combination of the monomials. We may assume the minimal value of j is non negative since we can multiply the equation by $y^{p \cdot |j_{min}|}$ where j_{min} is the most negative value of j that appears. Now, we will prove

[14] In particular this means f is not an ℓ-th power over any constant field extension of $F/\mathbb{F}_q$.

all $c_{i_1,i_2,0,k}$ are zero, and then we can divide the equation by y^j and proceed by induction to prove all $c_{i_1,i_2,j,k}$ are zero.

Separating by the values of k, denoting $h_k(X,Y) = \sum c_{i_1,i_2,j,k} X^{i_1} Y^{i_2} Y^{jp}$ and rearranging eq. (7), and squaring, we get:

$$\begin{aligned} h_0(x,y) + h_1(x,y) f^{(q-1)/2} & \\ h_0^2(x,y) &= h_1^2(x,y) f^{q-1} \\ h_0^2(x,y) f &= h_1^2(x,y) f^q \end{aligned}$$

Recalling f must have a form as a polynomial in x and y (as all regular functions in the Hermitian curve have), we abuse the notation and write $f = f(x,y)$, and now:

$$h_0^2(x,y) f = h_1^2(x,y) f^q(x,y) = h_1^2(x,y) f(x^q, y^q) \tag{8}$$

since q is a power of the characteristic of F.

Denote as m_0 the maximal ideal associated with the place $P_{0,0}$. A function in F that is zero mod m_0^t has a zero of multiplicity at least t at $P_{0,0}$. Note that x^q and y^p are both in m_0^q

Denote $\overline{h}_k = \sum c_{i_1,i_2,0,k} x^{i_1} y^{i_2}$, note that $h_k \equiv \overline{h}_k(\text{ mod } m_0^q)$ and take eq. (8) mod m_0^q to get:

$$\begin{aligned} \overline{h}_0^2 f &\equiv \overline{h}_1^2 f|_{P_{0,0}} && (\text{mod} m_0^q) \\ \overline{h}_0^2 f - \overline{h}_1^2 f|_{P_{0,0}} &\equiv 0 && (\text{mod} m_0^q) \end{aligned}$$

consider the regular function $\overline{h}_0^2 f - \overline{h}_1^2 f|_{P_{0,0}}$, it has q zeroes but from the bound in A it has less then q poles, meaning (by claim 2.2) it is identically zero in F. From this we get:

$$f = f(0,0) \left(\frac{\overline{h}_1}{\overline{h}_0} \right)^2$$

giving us that f is a square over any extension of F where $f(0,0)$ has a square root. This would be a contradiction, meaning the division by $\overline{h}_0$ was not allowed, i.e. $\overline{h}_0$ is zero. Since $f|_{P_{0,0}} \neq 0$ we also get $\overline{h}_1$ is zero. $\overline{h}_0, \overline{h}_1$ are combinations of $x^{i_1} y^{i_2}$, which are independent since they have different valuations at P_∞, so we get that $c_{i_1,i_2,0,k} = 0$ for all i_1, i_2, k, which finishes the proof. □

C.3.3 The case of general ℓ

In order to prove the case $\ell > 2$ we will use the following property of symmetric polynomials:

Theorem C.9. *(see [Sch06] or [BSC13]) let $Q(X_1, ..., X_\ell)$ be a symmetric polynomial in ℓ variables over a field. it can be (uniquely) written as*
$Q(X_1, ..., X_\ell) = P(S_1(X_1, ..., X_\ell), ...S_r(X_1, ..., X_\ell)$
where P is a polynomial over the same field and $S_i(X_1, ..., X_\ell)$ is the i-th elementary symmetric polynomial (which up-to sign is the sum of all products of i distinct variables $X_{j_1} * ... * X_{j_i}$). The total degree of P is equal to the degree of Q in X_1 (or in any of the other variables due to symmetry).

We will now introduce some notation following [Sch06, Chapter I section 5].

Given $H_0, ...H_{\ell-1}$ in some field we define:

$$a(Z; H_0, ...H_{\ell-1}) = H_0 + H_1 Z + ... + H_{\ell-1} Z^{\ell-1}$$

Let $\zeta_1, ...\zeta_\ell$ be the distinct ℓ-th roots of unity in $\overline{\mathbb{F}_p}$, now define

$$b(Z; H_0, ...H_{\ell-1}) = \prod_{i=1}^{\ell} a(\zeta_i Z; H_0, ...H_{\ell-1})$$

b is symmetric in $\zeta_1 Z, ...\zeta_\ell Z$ and so from theorem C.9 we know it has a representation as a polynomial in the elementary symmetric polynomials on $\zeta_1 Z, ...\zeta_\ell Z$. However, the elemental symmetric polynomials on $\zeta_1 Z, ...\zeta_\ell Z$ are all identically equal to 0 except the last one which is (up-to sign) equal to Z^ℓ. so we get some c s.t.

$$c(Z^\ell; H_0, ...H_{\ell-1}) = b(Z; H_0, ...H_{\ell-1})$$

Finally we will consider the homogenization of c with respect to W, i.e.

$$d(U, V; H_0...H_{\ell-1}) = V^{\ell-1} c(U/V; H_0...H_{\ell-1})$$

Clearly d is a rational function, but closer inspection reveals it is in fact a polynomial. We now calculate the degrees of a, b, c, d:

Claim C.10. *with the above notations:*

1. *$a(Z; H_0, ...H_{\ell-1})$ has degree $\ell - 1$ in Z and total degree 1 in all the H_i.*
2. *$b(Z; H_0, ...H_{\ell-1})$ has degree $\ell(\ell-1)$ in Z and total degree ℓ each all the H_i.*
3. *$c(W; H_0...H_{\ell-1})$ has degree $\ell - 1$ in W and total degree ℓ in all the H_i.*
4. *$d(U, V; H_0...H_{\ell-1})$ has degree $\ell - 1$ in U and V, and total degree ℓ in all the H_i.*

Proof. The degrees of a are clear from its definition, and the rest are simple observations. □

We are now ready to prove theorem C.8 for the case of general ℓ:

Proof. (of theorem C.8) Let

$$0 = \sum c_{i_1,i_2,j,k} x^{i_1} y^{i_2} y^{jp} f^{k(q-1)/\ell} \tag{9}$$

be a vanishing combination of the monomials. Like the case $\ell = 2$ we may assume the minimal value of j is non negative and need only to prove all $c_{i_1,i_2,0,k}$ are zero.

Denote $g = f^{\frac{q-1}{\ell}}$, and $h_k(X, Y) = \sum c_{i_1,i_2,j,k} X^{i_1} Y^{i_2} Y^{jp}$, now we rewrite eq. (9) and get:

$$\begin{aligned} h_0(x, y) + h_1(x, y)g(x, y) + ... + h_{\ell-1}g(x, y)^{\ell-1} &= 0 \\ a(g; h_0, ..., h_{\ell-1}) &= 0 \end{aligned}$$

Now, recalling $\zeta_1 = 1$:

$$\begin{aligned} 0 &= \prod_{i=1}^{\ell} a(\zeta_i g; h_0, ...h_{\ell-1}) \\ &= b(g; h_0, ..., h_{\ell-1}) \\ &= c(g^\ell; h_0, ..., h_{\ell-1}) \\ &= c(f^q/f; h_0, ..., h_{\ell-1}) \\ &= d(f^q, f; h_0, ..., h_{\ell-1}) \end{aligned}$$

Denote $\overline{h}_k = \sum c_{i_1,i_2,0,k} x^{i_1} y^{i_2}$, note that $h_k \equiv \overline{h}_k (\mathrm{mod} m_0^q)$ and the pole orders of $\overline{h}_k$ are less than $\frac{q}{\ell} - \frac{(\ell-1)|v_\infty(f)|}{\ell}$. Also note that $f^q \equiv f|_{P_{0,0}} (\bmod m_0^q)$ and now we get mod m_0^q the equivalence:

$$d(f|_{P_{0,0}}, f; \overline{h}_0, ..., \overline{h}_{\ell-1}) \equiv 0 (\mathrm{mod} m_0^q)$$

Now since $f|_{P_{0,0}}$ is non-zero, and from bound on the degree of d in each variable attained in claim C.10, we get that the degree of $d(f|_{P_{0,0}}, f; \overline{h}_0, ..., \overline{h}_{\ell-1})$ is less then $(\ell-1)|v_{P_\infty(f)}| + \ell(\frac{q}{\ell} - \frac{(\ell-1)|v_\infty(f)|}{\ell}) = q$. So $d(f|_{P_{0,0}}, f; \overline{h}_0, ..., \overline{h}_{\ell-1})$ has more zeroes then poles and by claim 2.2 it is the zero function.

Let $\mathfrak{Y}$ be some ℓ-th root of $\frac{f}{f|_{P_{0,0}}}$ in the algebraic closure of $F = \mathbb{F}_q[x,y]/\varphi(x,y)$. Since $Z^\ell - f$ is absolutely irreducible $\mathfrak{Y}$ must be of degree exactly ℓ over F. now:

$$\begin{aligned} 0 &= d(f|_{P_{0,0}}, f; \overline{h}_0, ..., \overline{h}_{\ell-1}) \\ &= c(\frac{f|_{P_{0,0}}}{f}; \overline{h}_0, ..., \overline{h}_{\ell-1}) \\ &= c(\frac{1}{\mathfrak{Y}}^\ell; \overline{h}_0, ..., \overline{h}_{\ell-1}) \\ &= b(\frac{1}{\mathfrak{Y}}; \overline{h}_0, ..., \overline{h}_{\ell-1}) \\ &= \prod_{i=1}^{\ell} a(\frac{\zeta_i}{\mathfrak{Y}}; \overline{h}_0, ..., \overline{h}_{\ell-1}) \end{aligned}$$

So for some ζ_i it must hold that $a(\frac{\zeta_i}{\mathfrak{Y}}; \overline{h}_0, ..., \overline{h}_{\ell-1}) = 0$. However, $a(Z; H_0, ...H_{\ell-1})$ is of degree $\ell - 1$ in Z, so if $a(Z; \overline{h}_0, ..., \overline{h}_{\ell-1})$ is not the zero polynomial it would mean there is a polynomial in $\mathfrak{Y}$ of degree less than ℓ which vanishes, which is a contradiction to $\mathfrak{Y}$ being of degree ℓ over F. So $a(Z; \overline{h}_0, ..., \overline{h}_{\ell-1})$ is the zero polynomial, which by the structure of a means each $\overline{h}_k$ is the zero polynomial, which by corollary 2.1 means all $c_{i_1,i_2,0,k}$ are zero, finishing the proof. □

C.3.4 The case $f|_{P_{0,0}} = 0$

In the proof of theorem theorem C.8 we used both P_∞ and $P_{0,0}$ heavily. The use of P_∞ makes a lot of sense since this whole work deals with regular functions. The use of $P_{0,0}$ however seems less natural and should not be mandatory. Though it is very convenient to use $P_{0,0}$ during the proof, f could vanish there, which would invalidate our argument. Ideally we would like to use a change of variables - send x, y to $x-a, y-b$, get the monomial independence from the monomials after the shift and then proceed with the argument for bounding the size of S_ℓ. We must be mindful however, since not all changes of variables in x and y preserve equality in F, and therefore also do not preserve independence. The variable changes we are allowed to preform are those that are isomorphisms of the function field $F/\mathbb{F}_q$. In [Xin95], there is a description of these automorphisms. The only automorphisms that preserve our monomials (i.e., send a linear combination of monomials to another linear combination of monomials) are those of the form $x, y \to x, y+\beta$ where $Tr(\beta) = \beta^p + \beta = 0$. We now use these automorphisms to extend the function for which our argument works to those that are not divisible by x:

Claim C.11. *Suppose f is not of the form $f = xh$ where h is regular, then theorem C.8 holds for f even without the assumption that $f|_{P_{0,0}} \neq 0$.*

Proof. If f vanishes at $0, \beta$ for all β with $Tr(\beta) = 0$ then f vanishes at every place where x vanishes. Since all the zeroes of x are simple zeroes, this means that $\frac{f}{x}$ is regular, contradicting the assumption.

Let β be such that f does not vanish at $0, \beta$, and denote $g(x, y) = f(x, y+\beta)$. Let $\sum c_{i_1,i_2,j,k} x^{i_1} y^{i_2+jp} f^{k(q-1)/\ell}$ be a vanishing combination of $x^{i_1} y^{i_2} y^{jp} f^{k(q-1)/\ell}$. Since $x, y \to x, y+\beta$ is an isomorphism of F, we also know $\sum c_{i_1,i_2,j,k} x^{i_1} (y+\beta)^{i_2+jp} g^{k(q-1)/\ell}$ vanishes. Simplifying, we would get $\sum d_{i_1,i_2,j,k} x^{i_1} (y)^{i_2+jp} g^{k(q-1)/\ell}$ vanishes, where the values of $d_{i_1,i_2,j,k}$ can be computed by a linear transformation on the values of $c_{i_1,i_2,j,k}$ (the transformation is invertible since $c_{i_1,i_2,j,k}$ can be obtained from $d_{i_1,i_2,j,k}$ by applying the inverse automorphism $x, y \to x, y-\beta$ to the vanishing combination with the $d_{i_1,i_2,j,k}$). Since $g|_{P_{0,0}} = f|_{P_{0,\beta}} \neq 0$ and it is of the same pole order as f, the conditions of theorem C.8 hold for g, and there for all values of $d_{i_1,i_2,j,k}$ are zero, and therefore the values of $c_{i_1,i_2,j,k}$, which are a linear transformation on the values of $d_{i_1,i_2,j,k}$, are also all zero, proving the independence. □

It now remains to handle the case where $f = x^s g$ where $0 < s < \ell$ and g is regular and not divisible by x (if we wish, we may assume specifically that $g|_{P_{0,0}} \neq 0$). The case where $s < \ell$ is enough since dividing by x^ℓ does not change S_ℓ. There can be two strategies for handling the case where $f = x^s g$:

- adapt the proof of theorem C.8

- prove directly that S_ℓ is small since $f = x^s g$.

The latter option might be feasible since character sums on functions with good structure tend to be good (x^s is a function whose characters are very close to uniform, so it is reasonable to believe multiplying by it is good).

We give here an adaptation of the proof of theorem C.8 for the special case $\ell = 2$ and $f = xg$.

Proof. Continuing from eq. (8), and substituting $f = xg$ we get:

$$h_0^2(x,y)f = h_1^2(x,y)f^q(x,y) = h_1^2(x,y)x^q g(x^q, y^q)$$

Denote $\overline{h}_k = \sum c_{i_1,i_2,0,k} x^{i_1} y^{i_2}$ and take mod m_0^q to get

$$\overline{h}_0^2 f \equiv 0 \qquad\qquad (\mathrm{mod} m_0^q)$$

By by claim 2.2 $\overline{h}_0 = 0$ since it has q zeroes but fewer than q poles. Now taking mod m_0^{2q} instead we get that $x^q \overline{h}_1^2 g(0,0)$ has $2q$ zeroes at $P_{0,0}$. Since $g(0,0) \neq 0$ and x^q has exactly q zeroes at $P_{0,0}$, we get that $\overline{h}_1^2$ has q zeroes at $P_{0,0}$, but it does not have enough poles, so again by claim 2.2 we get it is also equal to zero, finishing the proof. □

The proof for the case where $\ell > 2$ has not been adapted, and this calls for further research.

תוכן עניינים

תקציר העבודה

קודים אלגבריים גיאומטריים, או Goppa Codes המסומנים C(D,G), הם קודים לתיקון שגיאות המכלילים את קודי Reed-Solomon. הקודים האלה הם קודים ליניאריים מעל השדה $\mathbb{F}_q$. מילת קוד מוגדרת עבור כל פונקציה במרחב ה Riemann-Roch שמתאים לדיוויזור G. בהינתן כזו f, מילת קוד כוללת, עבור כל נקודה על העקום שכלולה בדיוויזור D, את הערך של f בנקודה הזו.

קודים אלגבריים גיאומטריים הם בניה חשובה עבור התיאוריה של מדעי המחשב שכן הם היוו צעד משמעותי בהבנה של הקהילה המדעית לגבי שקלול התמורות (Trade-off) בין המרחק והממד של קודים לתיקון שגיאות מעל שדות החל מגודל 49.

עבודה זו עוסקת בבעיה של הוכחת חסמים על ההתפלגות של הסימבולים מתוך השדה $\mathbb{F}_q$ שמופיעים במילת קוד על ידי חסימה של ההסתברות של מאורעות ספציפיים מהסוג 'סימבול אקראי מהמילה שייך לתת קבוצה מסוימת של $\mathbb{F}_q$'. את תתי הקבוצות שמגדירות את המאורעות אנחנו בוחרים כך שתהיה להן משמעות אלגברית, ובכך נוכח להוכיח חסמים באמצעות ספירת נקודות על עקומים אלגבריים מסוימים.

בגלל הצורך בספירת נקודות על עקומים טבעי לנסות להשתמש בכלים חזקים מגיאומטריה אלגברית כמו חסם Weil, אך העקומים הרלוונטיים לקודים אלגבריים גיאומטריים הם בעלי גזע (genus) גדול, מה שגורם לחסמים הקלאסיים להיות לא אינפורמטיביים.

בעבודה זו אנחנו משתמשים בכלים אלמנטריים כדי לחסום את כמות הסימבולים במילת קוד יכולים להיות חזקה ℓ-ית בחבורה הכפלית של $\mathbb{F}_q$.

טכניקת ההוכחה מכלילה את השיטה של Stepanov שהוצגה ב-1969 לחסימת כמות הנקודות על עקום אלגברי בכלים אלמנטריים. ההכללה של הטכניקה לעקומים יותר כלליים מאשר הישר הפרויקטיבי דורשת כלים בסיסיים מהתורה של שדות פונקציות וכן ניסוח נכון של המבנה הנחוץ לנו בעקומים עליהם אנחנו עובדים.

הפקולטה למדעים
מדויקים ע"ש ריימונד
ובברלי סאקלר
אוניברסיטת תל אביב

אוניברסיטת תל-אביב
הפקולטה למדעים מדויקים
ע"ש ריימונד ובברלי סאקלר

על ההתפלגות של סימבולים במילות קוד של קודים אלגבריים-גיאומטריים

חיבור זה הוגש כחלק מהדרישות לקבלת התואר
"מוסמך אוניברסיטה" M.Sc. - באוניברסיטת תל-אביב

בית הספר למדעי המתמטיקה

על ידי
קדם יקירביץ

העבודה הוכנה בהדרכתו של
פרופסור אמנון תא שמע

הפקולטה למדעים
מדויקים ע"ש ריימונד
ובברלי סאקלר
אוניברסיטת תל אביב

אוניברסיטת תל-אביב
הפקולטה למדעים מדויקים
ע"ש ריימונד ובברלי סאקלר

על ההתפלגות של סימבולים במילות קוד של קודים אלגבריים-גיאומטריים

חיבור זה הוגש כחלק מהדרישות לקבלת התואר
"מוסמך אוניברסיטה" M.Sc. - באוניברסיטת תל-אביב

בית הספר למדעי המתמטיקה

על ידי
קדם יקירביץ

העבודה הוכנה בהדרכתו של
פרופסור אמנון תא שמע