Order Number 9207110

The Brill-Noether theorem with applications to A. G. Goppa codes and exponential sums

Polemis, Despina, Ph.D.

City University of New York, 1991

U·M·I
300 N. Zeeb Rd.
Ann Arbor, MI 48106

THE BRILL-NOETHER THEOREM WITH APPLICATIONS TO A.G. GOPPA CODES AND EXPONENTIAL SUMS

By
DESPINA POLEMIS

A DISSERTATION SUBMITTED TO THE GRADUATE FACULTY IN MATHEMATICS IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF DOCTOR OF PHILOSOPHY, THE CITY UNIVERSITY OF NEW YORK.

1991

This manuscript has been read and accepted for the Graduate Faculty in Mathematics in satisfaction of the dissertation requirement for the degree of Doctor of Philosophy.

September 20, 1991
Date

Carlos J. Moreno
Chair of Examining Committee

Sept. 27, 1991
Date

R Sabbele (for M. Markowitz)
Executive Officer

Supervisory Committee

The City of University of New York

Abstract

The Brill-Noether Theorem with Applications to A. G. Goppa Codes and Exponential Sums

by

Despina Polemis

Adviser: Professor Carlos J. Moreno

Throughout this dissertation we are primarily concerned with various algebraic and geometric properties of curves in relation to coding theory and the theory of exponential sums.

The curves of our interest are defined over finite fields which leads us to reconsider well known theorems as for instance the *Brill-Noether* theorem.

The problem of *resolution of singularities* lead us to investigate the selected methods available in order to desingularize a plane singular curve defined over a finite field. We present algorithmic models which describe these methods and we estimate their time complexities. We prove the relations among the exponential sums built from singular curves and the ones built from their equivalents.

The classical concepts of *adjoint divisors, adjoint curves* and their relation to the Brill-Noether theorem are reconsidered from a constructive point of view in which the field of constants is a finite field. We also compute the *discriminant divisor* utilizing a geometric and an algebraic method.

The problem of effectively calculating with the Riemann-Roch theorem is also considered in this thesis. We present two algorithmic constructions which estimate a basis for the vector space $\mathcal{L}(G)$. The first construction is the *algorithm EVG* based on the Cremona transformations and the second is the *algorithm MBR* based on the normalization process. We estimate the time complexity of both algorithms. They both serve as basic tools for the construction of algebraic geometric Goppa codes evolved by singular curves.

We give a new bound on the *minimum distance* of the dual of a Goppa binary subfield subcode generated from a singular curve. We obtain the new bound using exponential sum techniques.

Contents

Chapter 1

Introduction

1.1 Historical Perspective and New Results

Algebraic curves appear in many areas of mathematics and most notably in coding theory and in the theory of exponential sums. Throughout this thesis, various algebraic and geometric properties of curves defined over finite fields are considered in relation to coding theory.

A point on an algebraic curve is called *simple* if the multiplicity of the curve at this point is one, otherwise the point is *singular*. If the tangents of the curve at this point are distinct, then it is an *ordinary singular* point, otherwise it is a *nonordinary singular* point. A plane curve with all its points simple is called smooth, otherwise the curve is singular. The classical problem of *resolution of singularities* states that for every algebraic variety X over an algebraically closed field there exists a proper map $\pi : Y \longrightarrow X$ with Y nonsingular such that π is an isomorphism over some dense subset U of X. During the last century Kronecker, Max Noether, [53], [54], Bertini, [8], and others proved the resolution theorem for algebraic curves defined over the complex numbers using a succession of *Cremona transformations*, i.e., composition of projective and quadratic transformations. In [9], [10] Bliss presents a detailed development of this method . In 1936, Walker [70] solved the problem when X is a surface defined over complex numbers . In the 1940's, Zariski [73] solved the resolution problem for surfaces with π obtained by applying successive *blowing ups*, i.e., the *normalization* (σ-process). Abhyankar [3], [4] proved the resolution theorem for curves and surfaces over fields of non-zerocharacteristic using the normalization process as well. Recently Ford and Zassenhaus [20] introduced the *integral basis algorithm* which provides yet another way to desingularize a plane curve; this method was based on the relation of the nonsingular model of a curve with the integral closure of its coordinate ring. Trager [62] also discussed this method in his MIT thesis. Bronstein, Hassner, Vasquez and Williamson [15] used the integral basis algorithm to create a package in Scratchpad, a symbolic computer language developed at the IBM Research Mathematics Department [15]. Vasquez [68] has discussed the integral basis algorithm emphasizing the difficulties that arise over finite fields.

In this thesis we study on the resolution problem for plane algebraic curves over finite fields. We will describe three methods to desingularize a plane singular curve defined over a finite field. At first, we shall present the method based on successive blowing-ups (normalization process). Next, we will use on the method of Cremona transformations and finally we will consider the method based on the integral basis algorithm . We emphasize the constructive aspects of the three methods by presenting algorithmic models.

Concerning the *adjoint divisor* to a projective smooth curve, several definitions can be found in the classical as well as the recent literature. Brill and Noether define the adjoint divisor as a sum of points with pre assigned multiplicity, $r_i - 1$, where r_i is the multiplicity of the curve at those points. This classical definition appears in Fulton [21]. A geometric definition is presented by Gorenstein [27], and it describes the adjoint divisor in terms of the first kind differentials. It also appears in Kodaira [40], Samuel [56] and Arbarello [6]. Abhyankar [2], Samuel [56] and Serre [59] present an algebraic definition for the adjoint divisor which is motivated by the theory of the conductor ideal. Keller [37] assigns a certain positive integer α to each point in the adjoint divisor . This last definition is used by Le Brigand and Risler [14] in their recent work in coding theory. Our contribution in this thesis is to reconsider these definitions when the field of constants is finite and investigate the relations among them.

In [2] one of Abhyankar's aphorisms, states the following: "The discriminant locus (totality of roots) of a polynomial is the sum of the branch locus and the projection of the singular locus". The polynomial under consideration is an affine representation of a plane smooth curve defined over an algebraically closed field. During the course of our research we interpret the aphorism as a statement on the points which appear in the divisor described by the discriminant of the polynomial. In our case the polynomial is an affine representation of a plane, singular, absolutely irreducible curve. Unlike Abhyankar, we assume that the plane curve is defined over a finite field. We approach the computation of the *discriminant divisor* algebraically and a geometrically.

Brill and Noether in their theorem [14], [55], [13] construct a basis for the linear subspace $\mathcal{L}(G)$ in terms of certain homogeneous rational functions in the plane $\mathbf{P}^2(\mathbf{k})$. The field $\mathbf{k}$ can be any algebraically closed field of characteristic zero. In this thesis we reconsider the *Brill-Noether theorem* when the field of constants is a finite field and we introduce two algorithmic constructions which find a basis for the finite dimensional vector space $\mathcal{L}(G)$.

The theory of *algebraic geometric codes* relates the algebraic geometry of curves to coding theory. During the early 1980's, the Soviet mathematician Goppa [23], [22],[24],[25], [26] made the important discovery that curves with large number of rational points could be used to generate codes with good parameters. In his work, Goppa used the Brill-Noether theorem . Although he had all the ideas for constructing codes from algebraic curves, he did not consider the case where the curves are singular with nonordinary singularities. Goppa [26] presented an algorithm in order

to construct an a.g. Goppa code from singular curves having only ordinary singularities. These ideas were used by Tsfasman, Vladut and Zink [63] whose work won a scientific prize in 1984. Throughout their paper they construct algebraic geometric Goppa codes by means of *modular curves* and obtained an improvement to the Varshamov-Gilbert bound. Similar results were obtained independently by Ihara [33]. Manin and Vladut also [69] developed an algorithm which constructs a linear code using a family of Drinfeld modular curves. Le Brigand and Risler [43] approached the construction of a.g. Goppa codes constructively. Our objective in this thesis is to apply the algorithmic approaches of the Brill-Noether theorem to construct a.g. Goppa codes. The problem of effectively calculating with the Riemann- Roch theorem is also considered in this thesis.

The theory of *exponential sums* is another area of mathematics where curves have played an important role. Bombieri [11][th.5] presented a theorem which gave an estimate for an exponential sum built with rational functions on a nonsingular curve. C. Moreno and O. Moreno [49] have applied Bombieri's estimate to the rational functions of a nonsingular curve defined over the finite field $\mathbf{F}_{2^m}$ and they have obtained an improved Carlitz-Uchiyama bound. Bombieri [11][th.6] gave a similar estimate for an exponential sum built from rational functions on a singular curve.

In this thesis we obtain general formulas which compare exponential sums built from singular algebraic plane curves with their birational equivalent curves, where the singularities have been resolved using the normalization process and the Cremona transformations. The improvement on different bounds of the exponential sums plays a very important role on the theory of binary codes. In a series of papers by C. Moreno and O. Moreno [46], [51], [50], exponential sum techniques have been used to estimate the parameters of classical binary Goppa codes. In this thesis we also prove a new result on the *minimum distance of the dual of a Goppa binary subfield subcode* constructed from a singular curve over a finite field using exponential sum techniques.

1.2 Questions of Complexity

In this thesis, algorithmic emphasis is given to many abstract procedures. It is therefore natural to be concerned about the *computational complexity* of these algorithms. Some standard reference for analysis of algorithms are Knuth [38], Aho - Hopcroft-Ullman (AHU)[5] and Winograd [71].

In order to analyze the performance of an algorithm, some model of a computer is necessary, (AHU) [5] and Schonhage [57]. Some of the more conventional *computational models* are the following: The *Turing machine*, introduced by Alan Turing in 1937, provides intuitively appealing measures for the quantitative analysis of algorithms. These are machines with bounded memory. The *Random Access Machines* (RAM) are used for higher flexibility, in which a variety of instruction sets can be used. There are two types of RAM machines. The first is the RAM (*unit cost*) machine in which each RAM instruction requires one unit of time and each register requires one unit of space. The second type is the RAM (*logarithmic cost*) machine

in which the limited size of a real memory word is taken into account. The *straight-line program* is a simpler machine based on the RAM (unit-cost) which ignores some RAM instructions. The *bitwise computation* machine is a simplification of the RAM (logarithmic cost). The *Boolean circuits* are computation models for parallel computations. *Nonscalar complexity* an abstract model where refers only to multiplications and divisions are counted.

The other important notion for the analysis of an algorithm besides the computational model is the *measure of computation.* The two important computational measures are the time and space measure, cf Aho - Hopcroft- Ullman[5] and Cull [17]. The *time complexity* is the number of operations needed to run an algorithm in one of the computational models. It is expressed as a function of the size of the problem. The *space complexity* is the number of bits which the algorithm uses in order to store and manipulate data. Let n be a measure of the size of the problem. Consider two algorithms with running times $f(n)$ and $g(n)$. Their running times are of the *same order* if for some N there exist two positive constants c_1 and c_2 such that $c_1|g(n)| \leq |f(n)| \leq c_2|g(n)|$ for all $n \geq N$. We symbolize this relation by $f(n) = O(g(n))$ read "$f(n)$ is of order $g(n)$". We consider two algorithms to have the same time complexity if their running time is of the same order. We do not distinguish between algorithms whose running times are of the same order.

To discuss time and space complexity in the RAM models, the following conditions are selected concerning the encoding of input and output data, cf [57], Kannan [34] and Koblitz [39]. We assume that the integers are represented in standard binary form. The *size* of an integer N is $1 + [\log N]$ where the 1 stands for the sign of the integer. The [] is the greatest integer function. The elements in the finite field $\mathbf{F}$ are given as residues mod p. A rational number is represented by a pair of integers, i.e., the integer which appears in the numerator and the one in the denominator of the rational number.

We can only *compare* algorithms if we use the same computational model and the same complexity measure.

Knuth [38] uses the Turing machine to estimate the time complexity of certain algorithms. Abhyankar [1] utilizes the RAM (unit cost) model with basic arithmetic operations being of unit time cost and he computes the time complexity. Manin and Vladut [69] estimate the time and space complexity adopting the RAM (logarithmic cost) computational model [1]. In their estimates, they use the logarithmic function $l(p) = \log_2 p + 1$ where p is the characteristic of the field of constants. Borodin and Munro [12] use the straight-line program model of computation and they measure the time complexity by the number of arithmetical operations required. Winograd [71], [7] and Chudnovsky [16] measure the time complexity using nonscalar complexity. Bounds on time complexity, which are specified up to a polynomial, are independent of the selection of a computational model since all computational models are equivalent in the sense of polynomial time complexity, cf Grigor'ev [28] and Teitelbaum [61].

In our work we select the bitwise computation machine as computational model.

[1] They call it LRAM

Time complexity is thought of as the upper bound for the number of bit operations needed to perform an arithmetic task. The shift operations, memory access, etc. have not been considered in this thesis. We do not use procedures with the best bounds, but procedures with simple structure. We consider only procedures with polynomial time complexity.

We describe our algorithmic procedures explicitly according to the following scheme: We name the algorithm, we present the input data , the output data, and the method of operation. We describe the method of operation which we follow in the algorithm or we refer the reader to an already known procedure. We continue with estimating the time complexity of the algorithms. Finally, we compare the algorithms which describe the same construction.

The time complexity of some basic operations in the finite field $\mathbf{F}_q$ with $q = p^b$ elements where p is a prime number follow:

1. *Multiplication of two polynomials* in $\mathbf{F}_q[x]$ of degrees n and m where $n > m$ can be done using nm multiplications of elements in $\mathbf{F}_q$. Each multiplication requires $O(\log^3 q)$ time, cf Koblitz [39]. We also need some additions which require less time. Therefore the multiplication of polynomials requires $O(nm\log^3 q)$ time.

2. *Division of two polynomials* in $\mathbf{F}_q[x]$ of degrees n and m where $n > m$ requires $O(n^2)$ multiplications in $\mathbf{F}_q$ (of integers modulo p). Each such multiplication takes $O(\log^3 q)$ bit operations. Therefore the overall time needed to divide two polynomials is $O(n^2\log^3 q)$.

3. *Evaluation of a polynomial* $f(x)$ with coefficients in $\mathbf{F}_q$ at an element a in the finite field can be done by finding the remainder of $f(x) \bmod x - a$. If the degree of $f(x)$ is n then the evaluation requires $O(n^2\log^3 q)$ time.

4. *Evaluation of a polynomial at all the elements in* $\mathbf{F}_q$. We perform q evaluations. Each evaluation uses $O(n^2\log^3 q)$ time. Therefore the total time is $O(qn^2\log^3 q)$.

5. The calculation of the *Resultant* of two polynomials requires the same number of operations (Aho - Hopcroft - Ullman [5]) as the following : The *Determinant* of an $n \times n$ matrix; the *Solution of Simultaneous* linear equations $A\mathbf{x} = \mathbf{b}$ where A is an $n \times n$ matrix, $\mathbf{x}$ is the row vector of the n unknowns and $\mathbf{b}$ is the column vector of the n constants; the *matrix multiplication* of $n \times n$ matrices.

   Multiplication of matrices requires $O(n^3)$ multiplications of elements in $\mathbf{F}_q$ and some additions. Each multiplication of two elements in the finite field $\mathbf{F}_q$ requires $O(\log^3 q)$ bit operation (Koblitz [39]). Therefore the matrix multiplication can be done in $O(n^3\log^3 q)$.

We do not claim that the bounds which appear in this thesis are sharp. The primary significance of the results is the conclusion that the time complexity of the various algorithmic constructions can by measured by local data, (i.e., the degree of the curve, the characteristic of the finite field) and that the time complexity is polynomial.

Another important concept in the analysis of algorithms is their space complexity. In our future work we will consider this important problem.

1.3 The Scope of the thesis

Throughout this thesis the curves are absolutely irreducible and are defined over a finite field $\mathrm{k} = \mathbf{F}_q$ where $q = p^b$ and p is a prime number.

In the second chapter we present an algorithmic construction (algorithm SM) which computes the rational singularities of an absolutely irreducible singular plane curve and their multiplicities. The time complexity of the algorithm is proven to be polynomial in the degree of the curve (lemma 2.1). We also focus on selected methods available for dealing with singularities of algebraic curves over finite fields.

We consider the following three methods in order to desingularize a curve: The method based on the successive blowing-ups (normalization process), the one based on the Cremona transformations and the method which utilizes the integral basis algorithm. The algorithmic aspect of the above methods is discussed through the algorithms: BU (blowing-up), NOR (Normalization) , CT (Cremona Transformation), RC (Resolution through Cremona transformations), IBA (Integral Basis Algorithm) and NSM (Nonsingular Model). The time complexity of the algorithms is discussed in various lemmas (2.2, 2.3, 2.4, 2.5).

We also present examples which are meant to clarify the three mentioned methods: the normalization process (ex. 2.3 , 2.4), the Cremona transformations (ex. 2.5 , 2.6), the integral basis algorithm (ex. 2.7, 2.8).

In the third chapter, the classical concepts of adjoint divisors, adjoint curves and their relation to the Brill-Noether theorem are reconsidered when the field of constants is finite.

We define the adjoint divisor algebraically (def 3.2), geometrically (def. 3.3), computationally (def. 3.4) and classically (in the sense of Brill- Nother) (def. 3.5). In examples 3.1, 3.2 and 3.3 we find the adjoint divisors of singular curves using the previous definitions. We prove the equivalence of the first three definitions and show that the fourth is a special case of the third (th.3.1).

We prove that there are three equivalent conditions for a curve to be the adjoint curve (th. 3.2). The discriminant divisor for a polynomial of two variables is also computed in this chapter (th. 3.3, 3.4).

The topics discussed in the fourth chapter are: a proof of the Brill-Noether theorem when the field of constants is a finite field , the algorithmic approach to the Brill-Noether theorem and its application to the theory of algebraic geometric Goppa codes.

The Brill-Noether theorem implies an algorithmic development which constructs a basis for the vector space $\mathcal{L}(G)$ first realized by Goppa. We introduce the algorithm EVG which is an extended version of the one described by Goppa. The time complexity of the algorithm EVG is proven to be polynomial in the degree of the curve (lemma 4.2). We also develop the algorithm MBR which simultaneously serves as a

modification to the one described by Le Brigand and Risler. The time complexity of the algorithm MBR is computed in lemma 4.1. The direct application of the above algorithms is in the theory of algebraic geometric Goppa codes.

The last chapter of this thesis is dedicated to the theory of exponential sums and its interrelation with the theory of algebraic curves and coding theory.

We prove the relations among the exponential sums built by singular curves and the ones built by their desingularizations. We attain the results by reducing the singularities of the curves using the blowing-up method and the Cremona transformations (pr. 5.1–5.6). Various examples which appear in this chapter are meant to clarify the results (ex. 5.1-5.7).

We end this chapter by deriving a new bound on the minimum distance of the dual of a Goppa binary subfield subcode built from a singular curve (th.5.2). Our new bound depends on the adjoint divisor of the curve (th. 5.1) and its advantage is that we have various ways of computing the adjoint divisor.

The following is a list of the most important examples in this thesis:

Chapter2
normalization process: ex. 2.3, 2.4
Cremona transformations: ex. 2.5, 2.6
Integral basis algorithm: ex 2.7, 2.8

Chapter3
Adjoint Divisors: ex. 3.1 (Le Brigand-Risler [43]), ex. 3.2, ex. 3.3
Discriminant Divisors: ex. 3.6–3.8 (geometric approach), ex. 3.9–3.11 (algebraic approach)

Chapter4
Construction of A.G. Goppa Codes: ex. 4.1 (algorithm MBR), ex. 4.2 (algorithm EVG)

Chapter5
Exponential Sums and Mathematica: ex. 5.1–5.7
Minimum Distance of the Dual: ex. 5.8

1.4 Acknowledgements

I am grateful to my advisor, Professor Carlos Moreno, for advising me in the study of algebraic Goppa codes and exponential sums; for his many helpful suggestions to improve the readability of this thesis and most of all for his patience, tolerance and kindness.

I would like to thank Professor Al Vasquez for introducing me me into the study of algebraic geometry and for discussing many of the results in this thesis with me.

I would also like to thank Professor Lewittes and Professor Oscar Moreno for their educational discussions with me .

The economical and emotional support of my family through the years of my academic career is greatly appreciated.

But most of all I thank God for being besides me and helping me fulfill my dream.

Chapter 2

Resolution of Singularities

The purpose of this chapter is: to analyze the three best known methods for reducing the singularities of plane algebraic curves defined over a finite field, to produce algorithmic models and to give estimates for their time complexity.

The contents of the chapter are as follows: In the preliminary section 2.1 we provide an algorithm for finding the rational singularities of a plane projective curve and show that its time complexity is polynomial in both the degree of the curve and the cardinality of the finite field.

In section 2.2, following Shafarevich's treatment in [60], we describe algorithms for the blowing-up process and the normalization process and give estimates for their time complexity.

In section 2.3 we give algorithms for reducing and resolving the singularities of a plane projective curve by a combination of quadratic and projective transformations. The time complexity of these algorithms are also estimated under the assumption that the singularities of the curve are all rational.

The last section investigates the resolution of the singularities of a curve using the integral basis algorithm . We show that the time complexity of the algorithm is polynomial in the degree of the curve. We next present a construction which finds an affine non-singular model of a plane curve over the points away from the points at infinity.

2.1 Rational Singularities

Let $F(X, Y, Z)$ be a homogeneous form of degree d describing a plane projective curve C. We say that the point $P = (a, b, 1) \in C$ is a *singularity* if the Taylor expansion of the dehomogenized polynomial $f(x, y) = F(x, y, 1)$ about the point $(x, y) = (a, b)$ has the form

$$f_m(\xi, \eta) + ... + f_d(\xi, \eta)$$

where $\xi = x - a$, $\eta = y - b$ and the $f_i(\xi, \eta)$ are homogeneous forms of degree i and the lowest $m \geq 2$.

The smallest degree m of an f_i appearing above is called the *multiplicity* of the singularity P. If P is a singularity and we have a factorization

$$f_m(x,y) = \prod_{i=1}^{m} (\alpha_i x + \beta_i y)^{r_i}$$

we call P an *ordinary* singularity if all the r_i are equal to 1. Otherwise the singularity is called *nonordinary.*

A singularity $P = (a,b,c) \in C$, say with $c \neq 0$, is called *rational* over the field k, if $\frac{a}{c}, \frac{b}{c} \in k$.

Basic Rationality Assumption. All the singularities and the infinitely near points are rational.

The following algorithm computes the rational singularities of an irreducible plane projective curve with their multiplicities and their types, i.e., ordinary vs. nonordinary. Let F_q be the finite field of $q = p^b$ elements.

Algorithm SM * Singularities, Multiplicities *
Input: An irreducible plane projective curve $C : F(X,Y,Z) = 0$, defined by the homogeneous form $F \in F_q[X,Y,Z]$ of degree n.
Output: The rational singularities of C together with their multiplicities .
Method:

Step 1: Find the representation of the plane curve C in an affine neighborhood, i.e., dehomogenize the form $F(X,Y,Z)$ with respect to one coordinate:

$$F(X/X, Y/X, Z/X) = F_*(1,y,z)$$

The dehomogenized form $F_*(1,y,z)$ is equivalent to an affine polynomial $f(y,z)$.

Step 2: Find the partial derivatives of the polynomial $f(y,z)$ with respect to the local affine coordinates y and z i.e., $\partial f/\partial y$ and $\partial f/\partial z$.

Step 3: Find the distinct rational *singularities* of the curve C by solving the system of equations $f(y,z) = \partial f/\partial y = \partial f/\partial z = 0$.

Step 4: If a singular point P is at the origin then go to the fifth step otherwise translate the singular point P to the origin by applying an affine linear transformation. We again denote by $f(y,z)$ the resulting polynomial.

Step 5: Rewrite the polynomial $f(y,z)$ as follows:

$$f(y,z) = f_m(y,z) + f_{m+1}(y,z) + \ldots + f_n(y,z)$$

where f_i are forms of degree i and m is the multiplicity of the singularity. The factorization of $f_m(x,y)$ over F_q into irreducible factors will yield the type of singularities.

Step 6: Repeat steps four and five for all the singular points of the curve C lying in the present affine neighborhood.

Step 7: Repeat steps one through six for the dehomogenization of the homogeneous form $F(X,Y,Z)$ with respect to Y and Z.

Lemma 2.1 *Let $C : F(X,Y,Z) = 0$ be an irreducible plane projective curve defined by a form $F \in F_q(X,Y,Z)$ of degree n. The time complexity of the algorithm SM is polynomial in the degree n.*

Proof. The proof of the lemma is straight forward. The following argument actually yields an effective estimate.
(The elements of the finite field are polynomials with coefficients in $\mathbf{F}_p$ regarded modulo a primitive polynomial of degree b. The multiplication of an integer times a polynomial takes $O(b)$ multiplications of integers modulo p that requires $O(\log^2 p)$ bit operations, Koblitz [39].)
Let $C(i)$ denote the time complexity of the i-th step.

For the first step we have $C(1) = O(n)$ since dehomogenizing the homogeneous form $F(X,Y,Z)$ with respect to one homogeneous coordinate is equivalent to setting that coordinate equal to 1, a total of at most n substitutions are required.

In step 2 we calculate the partial derivatives of $f(y,z)$ with respect to y and z. Since $f(y,z)$ considered as a polynomial in y has at most $O(n)$ terms, then this operation involves at most $O(n)$ multiplications of integers (i.e., the exponents of y) times polynomials in z of degree at most $O(n)$ (i.e., the coefficients) hence the total number of multilications is $O(n^2)$. Each multiplication of an integer by a field element requires $O(b\log^2 p)$ operations. Hence the time complexity of $C(2)$ is $O(n^2 b\log^2 p)$ which can be replaced by $O(n^2\log^2 q)$.

For the third step we need to find the simultaneous solutions of the system $f(y,z) = 0$, $f_y(y,z) = 0$, $f_z(y,z) = 0$. Here we use an idea of Abhyankar ([1], pg. 276) where this problem can be obtained by finding those roots of $\mathrm{Res}_y(f_y, f_z) = 0$ and $\mathrm{Res}_z(f_y, f_z) = 0$ which are also the roots of $f(y,z) = 0$. To carry out this step we proceed as follows: we pick an element $a \in F_q$ and evaluate each polynomial entry in both matrices $\mathrm{Res}_y(f_y, f_z)$ and $\mathrm{Res}_z(f_y, f_z)$; since the evaluation of a polynomial of degree $\leq n$ at a requires $O(n^4\log^3 q)$ operations and the evaluation of the determinant of a matrix of size $O(n)$ with entries in F_q requires $O(n^3\log^3 q)$ operations, we conclude that the total number of operations required to find whether $z = a$ is a zero of $\mathrm{Res}_y(f_y, f_z) = 0$ is $O(n^4\log^3 q)$. Repeating this for each $a \in F_q$ gives that the time complexity of finding the zeros of $\mathrm{Res}_y(f_y, f_z)$ is $O(qn^4\log^3 q)$. We get a similar estimate for $\mathrm{Res}_z(f_y, f_z)$. We observe that the total number of points (a,b) with $\mathrm{Res}_y(f_y, f_z)(a) = 0$ and $\mathrm{Res}_z(f_y, f_z)(b) = 0$ is at most $O(q^2)$. Determining whether (a,b) is a zero of $f(x,y) = 0$ requires $O(n^3\log^3 q)$ operations. Hence the time complexity of $C(3)$ is $O(qn^4\log^3 q) + O(q^2 n^3\log^3 q) = O(q^2 n^4\log^3 q)$.

For the fourth step, we apply the affine transformation $y \longmapsto y+a$ and $z \longmapsto z+b$. This requires the evaluation of $f(y+a, z+b)$ as a polynomial in y and z. Therefore to

obtain an estimate for the complexity of this step we need to estimate the complexity of computing the representation:

$$(y+a)^i(z+b)^j = \sum_{k,l} y^k z^l P_{kl}(a,b)$$

where $i+j$ are $\leq n$. Since the complexity of multiplying two polynomials in $F_q[T]$ of degree N and M is $O(NM\log^3 q)$ we conclude that the complexity of obtaining the expansions $(y+a)^i$ and $(z+b)^j$ is at most $O(n^2\log^3 q)$. Hence the complexity of calculating $a_{ij}(y+a)^i(z+b)^j$ is again $O(n^2\log^3 q)$. Since $f(y,z)$ itself has $O(n^2)$ terms, the total complexity of step 4 is $C(4) = O(n^4\log^3 q)$. This clearly contains an estimate for step 5.

Step 6 requires that step 4 and 5 be repeated as many times as the number of rational singular points of C, i.e, $O(q^2)$. Hence the complexity of step 6 is $C(6) = O(q^2n^4\log^3 q)$.

Step 7 requires a repetion of Step1-6 for the other two dehomogenizations. Finally we estimate that the complexity of algorithm SM is at worst

$$O(q^2n^4\log^3 q)$$

□

Example 2.1 Consider the curve $C : Y^2X^3 + Y^2XZ^2 + Y^2Z^3 + YXZ^3 + YZ^4 + X^2Z^3 + XZ^4 = 0$ defined over the finite field $\mathbf{k} = \mathbf{F}_2$.

Step 1: The affine representation of the curve C in the affine neighborhood U_1 with local coordinates $s = Y/X$ and $t = Z/X$ is the intersection $U_1 \cap C$ represented by the polynomial $f(s,t) = s^2 + s^2t^2 + s^2t^3 + st^3 + st^4 + t^3 + t^4$.

Step 2: The partial derivatives of the polynomial f are $\partial f/\partial s = t^3 + t^4$ and $\partial f/\partial t = s^2t^2 + st^2 + t^2$.

Step 3: Solve the system of the three equations: $f(s,t) = \partial f/\partial s = \partial f/\partial t = 0$. The solution is the point $Q = (0,0)$.

Step 4: The multiplicity of C at Q is $m_Q(C) = 2$. The lower degree form in $f(s,t)$ is the $f_2(s,t) = s^2$. Thus there two non distinct tangents of C at Q given by $s = 0$ which implies that Q is a non-ordinary double point.

Step 5: We repeat the above steps for the other two affine pieces. The representation of the curve C at the affine neighborhood, U_2 with local coordinates $x = X/Y$ and $z = Z/Y$ is the intersection, $U_2 \cap C$ with affine equation, $f(x,z) = x^3 + xz^2 + z^3 + x^3z + xz^3 + z^4 + z^3x^2 + xz^4 = 0$. The partial derivatives are $\partial f/\partial x = x^2 + z^2 + x^2z + z^3 + z^4$ and $\partial f/\partial z = z^2 + x^3 + xz^2 + z^2x^2$. The solution of the above system is the point $P = (0,0)$ with multiplicity $m_P(C) = 3$. There are

three non distinct tangents of C at P given by the equation $x^3 + xz^2 + z^3 = 0$ we conclude that P is a non-ordinary point.

The representation of C in the last affine piece U_3 with local coordinates $y = Y/Z$ and $x = X/Z$ is given by

$$U_3 \cap C: f(x,y) = y^2x^3 + y^2x + y^2 + yx^3 + yx + y + x^2 + x = 0$$

and is non-singular.

Example 2.2 Consider the curve $C : Y^2X + X^2Y + Z^2X = 0$ defined over the finite field $\mathbf{k} = \mathbf{F}_{2^4}$.

The point $P = [0,1,1]$ is a singular point. The affine representation of C around the point P is given by the polynomial equation $f(x,y) = xy^2 + x^2y + x = 0$.

We have to transform P to the origin: Consider the affine transformation $T(x, y'+1)$: $\mathbf{A}^2(\mathbf{k}) \longrightarrow \mathbf{A}^2(\mathbf{k})$ where $\mathbf{P}^T = (0,0)$. The transformed polynomial is $f^T = f(x,y') = x^2 + xy'^2 + x^2y'$ and the multiplicity of the curve C at the point P is $m_P(C) = m_{P^T}(C^T) = 2$. There are two non distinct tangents of C at P given by the equation $x = 0$. Therefore P is a non-ordinary point.

2.2 Normalization Process

For further reading on the blowing-up process we suggest Shafarevich [60], Walker [70], Mumford [52] and Abhyankar [3] [4].

Consider the projective plane $\mathbf{P}^2(\mathbf{k})$. Let the curve C be an absolutely irreducible, projective plane curve over the finite field $\mathbf{k}$.

Definition 2.1 *The* blowing-up *of a point P_1 in $\mathbf{P}^2(\mathbf{k})$ is a birational morphism $\pi_1 : S_1 \longrightarrow \mathbf{P}^2$ where,*

i. S_1 is a projective smooth surface.

ii. $\pi_1^*(\mathbf{P}^2 - P_1) \simeq S_1 - E_1$.

iii. $\pi_1^{-1}(P_1) = E_1 \simeq \mathbf{P}^1(T_1)$.

T_1 is the locus of points on lines touching plane at the point P_1 i.e., the tangent space of $\mathbf{P}^2$ at P_1. The morphism π_1^* is the inverse of the morphism π_1 which is defined everywhere except at the point P_1. The projective line E_1 is the image of the point P_1 under the morphism π_1^*.

The blowing-up of the point P_1 in $\mathbf{P}^2$ induces the blowing-up of the point P_1 in the curve C in the following manner:

$$\begin{array}{ccccc} & & C_1 & \hookrightarrow & S_1 \supset E_1 \\ & & \tilde{\pi}_1 \downarrow & & \downarrow \pi_1 \\ P_1 & \in & C & \hookrightarrow & \mathbf{P}^2 \end{array}$$

The curve C_1 is the curve in the blown up surface S_1 lying above the curve C. The points in the intersection of the exceptional line E_1 and the curve C_1 are the *infinitely near points.* The blowing-up of a point is a *local process* (Shafarevich [60], pg. 123).

We will now make a small step toward approaching the blowing up process from the point of view of computational complexity. We will walk through the process a step at a time describing it algorithmically, considering the Basic Rationality assumption.

Algorithm BU * Blowing-Up Process *
Input: An irreducible plane projective curve $C : F(X,Y,Z) = 0$ defined by the homogeneous form $F \in F_q[X,Y,Z]$ of degree n, the rational singularities P_i of multiplicity r_i. The affine representation of C_1 around each P_i.
Output: Affine representations of the blown up curve C_2.
Method:

Step 1: Apply the affine quadratic transformation $Q_1(u,us)$ or $Q_2(vt,v)$ to $f(x,y)$ which is the affine representation of C_1 around P_1.

Step 2: Let us assume that we apply the affine quadratic transformation, Q_1 in the previous step. The quadratic transformation Q_1 transforms the curve C_1 into the curve $C_2 : f_2(u,s) = 0$ where $f(u,us) = u^{r_1}(f_2(u,s))$.

Step 3: The exceptional line $E_1 : u = 0$ intersects the curve C_2 in the infinitely near points, i.e., the points lying above the point P_1.

Step 4: Find the multiplicities of the infinitely near points.

Step 5: Repeat the steps one to four for the rest of the singular points of C.

Lemma 2.2 *The algorithm BU terminates and its time complexity is polynomial in the degree of the curve.*

Proof. The proof of the lemma is straight forward. The following argument actually yields an effective estimate considering the Rationality assumption.
Let $C(i)$ denote the time complexity of the i-th step.

The complexity of the first step $C(1)$ is contributed from the application of the quadratic transformation. Each quadratic transformation requires $O(n^2)$ time (Abhyankar ([1], pg. 277). This clearly contains an estimate for step 2.

In the third step we need to find the rational points of the polynomial $f_2(0,s) = 0$, i.e, we need to evaluate $f_2(0,s)$ at the q elements of the finite field. This requires $O(qn^2\log^3 q)$ time which becomes the estimate of the third step, $C(3)$.

In the fourth step we would have to transform the infinitely near points in the origin. That requires the application of affine transformations on every such infinitely near point, this time estimate is $O(n^4\log^3 q)$ (we refer the reader to the estimate of step 4 of algorithm SM). The number of the infinitely near points is at worst the same as the multiplicity r_1 of C at P_1 . Thus $C(4) = O(r_1 n^4 \log^3 q)$.

The process is repeated for all the singular points of the curve which are at most $O(q^2)$. Thus the algorithm BU needs at most

$$O(q^2 r n^4 \log^3 q)$$

bit operations where r is the maximum multiplicity of the curve at any of the singular points (the multiplicity of the worst singularity).
□

Note that the local blowing-up process reduces the multiplicities of the singular points. We resolve the singularities of the curve by using the *normalization* process which follows, Hartshorne [30].

The process of resolving the singularities of a singular curve via successive blowing-ups of the curve around each singular point, is called *normalization* (σ-) process. The *Brill Noether tower* describes the different morphisms involved in the normalization process. The following diagram is the Brill-Noether tower and clarifies the notation that we use in order to attain the non-singular model of the curve $\tilde{C}$.

$$\begin{array}{lcll}
\tilde{C} = & C_N & \hookrightarrow & S_N \quad = \tilde{S} \\
& {\scriptstyle \tilde{\pi}_N}\downarrow & & \downarrow{\scriptstyle \pi_N} \\
& \vdots & & \vdots \\
& \downarrow & & \downarrow \\
& C_i & \hookrightarrow & S_i \\
& {\scriptstyle \tilde{\pi}_i}\downarrow & & \downarrow{\scriptstyle \pi_i} \\
& \vdots & & \vdots \\
P_2 \in & C_1 & \hookrightarrow & S_1 \quad \supset E_1 \\
& {\scriptstyle \tilde{\pi}_1}\downarrow & & \downarrow{\scriptstyle \pi_1} \\
P_1 \in & C_0 & \hookrightarrow & S_0 = \mathbf{P}^2
\end{array}$$

Let $m_{P_i}(C_{i-1}) = r_i$ be the multiplicities of the successive curves C_{i-1} at the points P_i. The birational morphism $\pi = \pi_N \circ \cdots \circ \pi_1 : \tilde{S} \longrightarrow S_0$ maps the normalized surface $\tilde{S}$ to the original surface S_0. The birational morphism $\tilde{\pi} = \tilde{\pi}_N \circ \cdots \circ \tilde{\pi}_1 : \tilde{C} \longrightarrow C_0$ maps the normalized curve $\tilde{C}$ to the original curve C_0. The birational morphism π_i' maps the normalized surface $\tilde{S}$ to the surface S_i, i.e., $\pi_i' : \tilde{S} \longrightarrow S_i$. The strict transform of the exceptional divisor of the i-th blowing is $E_i' = \pi_i^*(E_i)$ which is a subset of the surface $\tilde{S}$. The birational morphism $\tilde{\pi}_i$ maps the normalized curve $\tilde{C}$ to the curve C_i. $\tilde{\pi}_i : \tilde{C} \longrightarrow C_i$. The intersection $E_i \cap C_i$ of the exceptional divisors E_i and the curves C_i yields the *infinitely near points* P_{i+1}.

The following is an algorithmic construction of the normalization process. The algorithm NOR resolves the rational singularities of the curve C applying the algorithm BU a finite number of times. It constructs the *singularity trees* of the singular points (Abhyankar [1], [3]; Manin, Vladut [69]).

Algorithm NOR : * Normalization process *
Input: An irreducible plane projective curve $C : F(X,Y,Z) = 0$, defined by the homogeneous form $F \in F_q[X,Y,Z]$ of degree n, where $q = p^b$. The singular points of the curve C and their multiplicities.
Output: Singularity trees of all the rational singular points of the curve C.
Method:

Step 1: Blow-up one of the singular points of the curve, for example the point P_1 of multiplicity r_1. The first blowing-up yields the infinitely near points P_{1i}.

Step 2: If C_1 is a smooth curve in the surface S_1 i.e., if all the points P_{1i} are simple then $C_1 = \tilde{C}$ is the normalized curve (*non-singular model*) of the curve C. If not, then blow up the curve C_1 around those infinitely near points P_{1i} that are singular.

Step 3: Repeat the second step until all the points lying above the singular point P_1 are simple (nonsingular). The collection of all the infinitely near points above P_1 which occurs after all blowing ups form the *singularity tree.* The point P_1 is the *root* of the tree and the infinitely near points are the *nodes.* We keep a count at each node equal the multiplicity of the transformed curve at the point.

Step 4: Construct the singularity trees of all the singular points of the curve C.

Lemma 2.3 *The time complexity of the algorithm NOR is polynomial in the degree of the curve.*

Proof. The proof of the lemma is straight forward. The following argument actually yields an effective estimate under the rationality assumption.
We need to apply at worst $O(n^2)$ many blowing ups (Abhyankar [1]) to each rational singularity in order to resolve it.
The degree of the original curve C will grow at worst $O(n^2)$ (Abhyankar [1]). Therefore the overall time bound for the construction of the singularity trees is $O(n^8q^2r\log^3 q)$ where r is the multiplicity of the curve C at its worst singularity. Therefore the time complexity of the algorithm NOR is

$$O(n^8q^2r\log^3 q)$$

□

In the next two examples we apply the algorithm NOR. The diagrams which accompany the examples are the singularity trees and they illustrate the calculations.

Example 2.3 Consider the plane curve $C : F = Y^5Z^4 - X^9 - XZ^8$ over the finite field $\mathbf{k} = \mathbf{F}_8$.

Step 1: We have to find the singularities of the curve C and their multiplicities.

Consider the set $U_1 = \{ [X,Y,Z] \in \mathbf{P}^2 : \ X \neq 0 \} \cong \{ (y,z) \in \mathbf{A}^2(\mathbf{k}) \}$ with local coordinates $y = Y/X$ and $z = Z/X$. The affine representation of the

curve at the neighborhood U_1 is the polynomial, $f(y,z) = y^5z^4 - 1 - z^8$. The partial derivatives with respect to the local coordinates are $\partial f/\partial y = y^4z^4$ and $\partial f/\partial z = 0$. Set the above three equations, described by the polynomial f and its derivatives, equal to zero and solve the system with respect to the local coordinates y and z. The solution is the singular point $P_1' = (0,1)$. We transform the singular point P_1' to the origin $(0,0)$ by applying the affine linear transformation $T(y,z'+1)$: $\mathbf{A}^2(\mathbf{k}) \longrightarrow \mathbf{A}^2(\mathbf{k})$. The local equation of the transformed curve C^T is denoted by the polynomial $f(y,z') = y^5(z')^4 + y^5 - (z')^8$. Thus, the multiplicity $m_{P_1'}(C) = m_{P_1'^T}(C^T) = 5$. We recall the transformed point $P_1'^T$ by P_1 with local coordinates y and z'. The tangent of the curve C at the point P_1 have the local equation $y = 0$. The multiplicity of the tangent is 5. Thus the point $P_1 = [0,0,1]$ is a *non-ordinary point,* of multiplicity $m_{P_1}(C) = 5$.

Consider the affine set $U_2 \cong (u,v) \in \mathbf{A}^2(\mathbf{k})$ with local coordinates $u = X/Y$ and $v = Z/Y$. The affine representation of the curve at the neighborhood U_2 is the polynomial $f(u,v) = v^4 - u^9 - uv^8 = 0$. The partial derivatives with respect to the local coordinates are $\partial f/\partial u = (u+v)^8$ and $\partial f/\partial v = 0$. The solution of the above three equations is the singular point $P_2 = (0,0)$ with multiplicity $m_{P_2}(C) = 4$. The four non-distinct tangents of the curve C at the point P_2 are given locally by the equation $v = 0$.

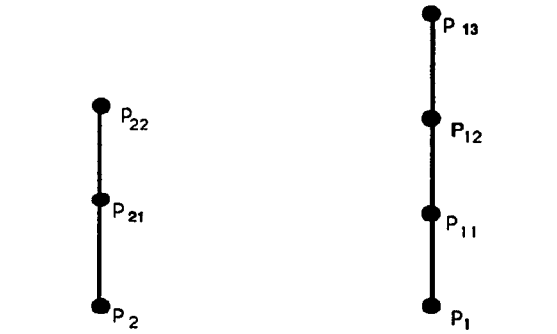
Consider the affine set $U_3 \cong \{(s,t) \in \mathbf{A}^2(\mathbf{k})\}$ with local coordinates $s = X/Z$ and $t = Y/Z$. The only point which remains to be checked is the point $P_3 = [0,0,1]$. The local equation of the curve C at the neighborhood U_3 is $f(s,t) = t^5 - s^9 - s = 0$. The evaluation of the polynomial $f(s,t)$ at the point P_3 is zero. The partial derivative $\partial f/\partial s = s + 1$ and $\partial f/\partial s(P_3) = 1$. Therefore the point P_3 is a non-singular point.

Step 2: In this step we have to resolve the singularities P_2 and P_1 of the curve C. Therefore we have to construct two singularity trees. The first tree has root the point P_2 and the root of the second tree is the point P_1.

Blow-up 1: of the point P_2. The point $P_2 \in U_2$ is of multiplicity $m_{P_2}(C) = 4$ with local coordinates u and v. The blown up set is $\pi_1^*(U_2) = \{((u,v),(\tilde{u},\tilde{v})) : u\tilde{v} - \tilde{u}v = 0\}$. Its subset is the affine set V_1 of points of the form, $(u, u\tilde{v})$. The local representation of the blown up curve is the polynomial equation $f_1(u,u\tilde{v}) = u^4(\tilde{v}^4 - u^5 - u^5\tilde{v}^8) = 0$. The equation of the local exceptional line E_1 in the affine neighborhood V_1 is given by the polynomial equation $u = 0$. The affine equation of the new curve C_1 is $f_2(u,\tilde{v}) = \tilde{v}^4 - u^5 - u^5\tilde{v}^8 = 0$. The point, lying above P_2 is the point P_{21} with multiplicity $m_{P_{21}}(C_1) = 4$. The point P_{21} is the node after the first blowing-up.

Blow-up 2: of the point $P_{21} \in V_1$ with local coordinates the functions u and $\tilde{v}$.

The blown up set is $\pi_2^*(V_1)$ whose subset is the affine set W_1 of points of the form $(u, \hat{v}u)$. The local representation of the blown up curve is the polynomial equation, $f_2(u, \hat{v}u) = u^4(\hat{v}^4 - u - u^9\hat{v}^8) = 0$. The equation of the local exceptional line E_2 is $u = 0$. The affine equation of the new curve C_2 is $\hat{v}^4 - u - u^9\hat{v}^8 = 0$. The point, lying above P_{21} is the point P_{22} of multiplicity $m_{P_{22}}(C_2) = 1$. The point P_{22} is the second node in the singularity tree. The representation of the exceptional line E_1 to the blown up surface $\pi_2^*(S_1)$ is the line E_1' with local equation $u' = 0$.



Blow-up i: of the point P_1: The point $P_1 \in U_1$ is the root of the second singularity tree and is of multiplicity $m_{P_1}(C) = 5$ with local coordinates y and z'. The blown up set is $\pi_1^*(U_1)$ whose subset is the affine set V_1 of points of the form, $(z'\tilde{y}, z')$. The equation of the local exceptional line E_1 is $z' = 0$. The affine equation of the new curve C_1 is $\tilde{y}^5 z'^4 + \tilde{y}^5 - z'^3 = 0$. The point, lying above P_1 is the point $P_{11} = (0,0)$ with multiplicity $m_{P_{11}}(C_1) = 3$. The point P_{11} is the node above the root in the singularity tree.

Blow-up ii: of the point $P_{11} \in V_1$ whose local coordinates are the functions $\tilde{y}$ and z'. The blown up set is $\pi_2^*(V_1)$ whose subset is the set W_1 with points of the form $(\tilde{y}, \tilde{y}\tilde{z})$. The equation of the local exceptional line E_2 is $\tilde{y} = 0$. The affine equation of the new curve C_2 is $\tilde{z}^3 + \tilde{y}^2 + \tilde{y}^6\tilde{z}^4 = 0$. The node lying above P_{11} is the point P_{12} with multiplicity $m_{P_{12}}(C_2) = 2$. The representation of the exceptional line E_1 to the blown up surface $\pi_2^*(S_1)$ is the line E_1' with local equation $z' = 0$.

Blow-up iii: of the point $P_{12} \in W_1$ with local coordinates $\tilde{y}$ and $\tilde{z}$.
The blown up set is $\pi_3^*(W_1)$ whose subset is the affine set W_2 with points of the form $(\tilde{z}\hat{y}, \tilde{z})$. The equation of the local exceptional line E_3 is $\hat{y} = 0$. The affine equation of the new curve C_3 is $\hat{y}^2 + \tilde{z}^8\hat{y}^6 + \tilde{z} = 0$. The node lying above the point P_{12} is the point P_{13} with multiplicity $m_{P_{13}}(C_3) = 1$. The representation of the exceptional line E_2 to the blown up surface $\pi_3^*(S_2)$ is the line E_2' with local equation $\hat{y} = 0$. The representation of the exceptional line, E_1 to the blown up surface $\pi_3^*(S_2)$ is the line, E_1'' with local equation $z' = 0$.

The next example is an exercise discussed by Vasquez (March, 1989).

Example 2.4 This is a special case of the curve which appears in Manin and Vladut's paper ([69], pg. 2627).

Consider the curve C defined over the finite field $\mathbf{k} = \mathbf{F}_q$ with $q = 2$ elements. The affine equation of the curve C is $F(x,y) = \sum_{k=0}^{3} \phi_k(x,y)$ where $\phi_k(x,y)$ are forms of degree, k. The forms of degree zero and $k+1$ are $\phi_0(x,y) = 1$ and $\phi_{k+1}(x,y) = x\phi_k^{q^2}(x,y) + y\phi_k^q(x,y)$ respectively. From the above general formulas we conclude that the forms of degree two and three are ,

$$\begin{aligned} \phi_2(x,y) &= x^5 + xy^4 + yx^2 + y^3 \\ \phi_3(x,y) &= x^{21} + x^5y^{16} + y^4x^9 + xy^{12} + yx^{10} + \\ &\quad x^2y^9 + y^3x^4 + y^7. \end{aligned}$$

Therefore the affine equation $F(x,y)$ of the curve becomes

$$\begin{aligned} F(x,y) &= x^{21} + x^5y^{16} + y^4x^9 + xy^{12} + yx^{10} \\ &\quad + x^2y^9 + y^3x^4 + y^7 + x + y + 1 \end{aligned}$$

The homogenization of the affine polynomial $F(x,y)$ is

$$\begin{aligned} F[X,Y,Z] = X^{21} + 5Y^{16} + Y^4X^9Z^8 + XY^{12}Z^8 + YX^{10}Z^{10} + \\ + X^2Y^9Z^{10} + Y^3X^4Z^{14} + Y^7Z^{14} + XZ^{20} + YZ^{20} + Z^{21} \end{aligned}$$

which is a homogeneous form of degree 21. The curve C has two non-ordinary singular points $P_2 = [1,1,0]$ of $m_{P_2}(C) = 16$ and $P_1 = [0,1,0]$ of $m_{P_1}(C) = 5$. We will first resolve the singularity of the point P_2:
The point $P_2 \in U_1$ has local coordinates the functions y and z. We transform the point P_2 to $P_2' = (0,0)$ with coordinates $y' = y - 1$ and z.
The local representation of the curve in the affine neighborhood U_1 is $C \cap U_1 = F(y',z) = z^{21} + y'^{16} + z^8y'^{12} + z^8y'^8 + z^{20}y' + z^{10}y'^9 + z^{10}y'^8 + z^{14}y'^7 + z^{14}y'^6 + z^{14}y'^5 + z^{14}y'^4$.

We will construct two singularity trees, the first has P_2 as its root where the second has the root P_1.

Blow-up 1: around the point P_2:

The equation of the local exceptional line E_1 is $z = 0$. The affine equation of the new curve C_1 is $f_1(y_1,z) = y_1^{16} + y_1^8 + z^5 + \cdots = 0$. Thus the points lying above the point $P_2 = (0,0)$ i.e., the nodes after the first blowing up are the points $P_{21} = (1,0)$ with local coordinates y_1 and z of multiplicity $m_{P_{21}}(f_1(y_1,z)) = 5$ and the point P_{22} of multiplicity $m_{P_{22}}(f_1(y_1,z)) = m_{(0,0)}(f_1(y_1',z)) = 5$.

Blow-up 2: around the point P_{22}:

The equation of the local exceptional line E_2 the affine equation of the new curve C_2 and the infinitely near points are described . The equation of the local exceptional line E_2 is $y_1' = 0$. The affine equation of the new curve C_2 is $f_2(y_1',\tilde{z}) = \tilde{z}^5 + y_1'^3 + \cdots = 0$. Thus the node lying above P_{22} is the point $P_{221} = (0,0)$ of multiplicity $m_{P_{221}}(C_2) = 3$.

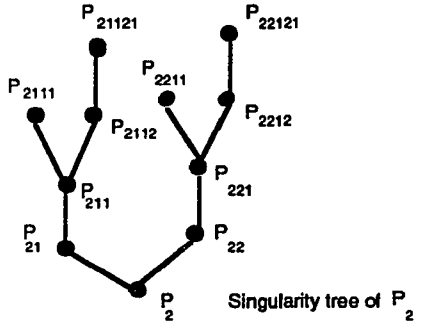
Blow-up 3: around the point P_{221}.
Preceding as above we have the nodes, P_{2211} of multiplicity $m_{P_{2211}}(C_3) = 1$ and the point P_{2212} where $m_{P_{2212}}(C_3) = 2$ lying above the blown up point P_{221}.

Blow-up 1: around the point P_{2212}:
The point, lying above P_{2212} is the point P_{22121} of multiplicity $m_{P_{22121}}(C_4) = 1$.

Blow-up 2: around the point P_{21} with local coordinates, y_1 and z and multiplicity $m_{P_{21}}(C_1) = 5$. The equation of the local exceptional line E_2 is $y_1 = 0$. The affine equation of the new curve C_2 is $f_2(y_1, z_1) = z_1^5 + y_1^3 + y_1^{11} + \cdots + z_1^2 y$. Thus the node lying above P_{21} is the point P_{211} with local coordinates y_1 and z_1 and multiplicity, $m_{P_{211}} = 3$.

Blow-up 3: around the point P_{211}. The equation of the local exceptional line E_3 is $z_1 = 0$. The affine equation of the new curve C_3 is $f_3(y_2, z_1) = y_2^3 + y_2 + z_1^2 + \cdots = 0$. The nodes lying above P_{211} are the points P_{2111} with local coordinates, y_2 and z_1 of multiplicity $m_{P_{2111}}(C_3) = 1$ and the point P_{2112} with local coordinates, $y_2 + 1 = y'$ and z_1 of multiplicity $m_{P_{2112}}(C_3) = 2$.

Blow-up 4: around the point P_{2112}. The equation of the local exceptional line E_4 is $y' = 0$. The affine equation of the new curve C_4 is $f_4(y', z_2) = y' + 1 + z_2^2 + \cdots = 0$. Thus the node lying above P_{2112} is the point P_{21121} with local coordinates y' and $z_2 + 1 = z'$ and multiplicity, $m_{P_{21121}}(C_4) = 1$.



Now we have to resolve the second singular point P_1 of C which is the root of the second singularity tree.

Blow-up i: of the point P_1 with local coordinates, x and z of multiplicity $m_{P_1}(C) = 5$. The equation of the local exceptional line E_1 is $z = 0$. The affine equation of the new curve C_1 is $f_1(x_1, z) = x_1^5 + x_1^{21} z^{16} + x_1^9 z^{12} + x_1 z^4 + \cdots$. The first node lying over P_1 is the point P_{11} with local coordinates, x_1 and z of multiplicity $m_{P_{11}}(C) = 5$.

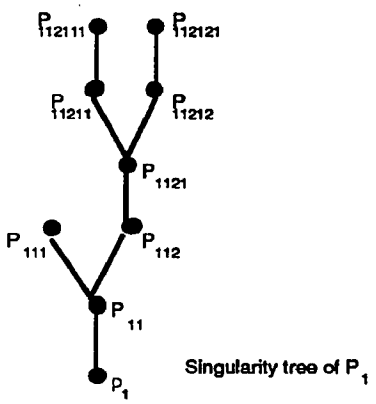
Blow-up ii: of the point P_{11}. The equation of the local exceptional line E_2 is $z = 0$. The affine equation of the new curve C_2 is $f_2(x_2, z) = z^5(x_2^5 + x_2 + z^4 + \cdots) = 0$. The nodes lying above P_{11} are P_{111} with local coordinates, x_2 and z of multiplicity $m_{P_{111}}(C_2) = 1$ and the point P_{112} with local coordinates, $x_2 + 1 = x'$ and z and multiplicity $m_{P_{112}}(C_2) = 4$.

Blow-up iii: of the point P_{112}. The equation of the local exceptional line E_2 is $z = 0$. The affine equation of the new curve C_3 is $f_3(x_3, z) = x_3^4 + z^2x_3^2 + \cdots = 0$. The node that is lying above P_{112} is P_{1121} with local coordinates x_3 and z of multiplicity $m_{P_{1121}}(C_3) = 4$.

Blow-up iv: of the point P_{1121}. The equation of the local exceptional line E_4 is $z = 0$. The affine equation of the new curve C_4 is $f_4(x_4, z) = x_4 + x_4^2 + \cdots = 0$. The nodes lying over the blown up point, P_{1121} are the points P_{11211} with local coordinates, x_4 and z of multiplicity $m_{P_{11211}}(C_4) = 2$ and the point P_{11212} with local coordinates, $x_4 + 1 = x'$ and z of multiplicity $m_{P_{11212}}(C_4) = 2$.

Blow-up v: of the point P_{11212}. The equation of the local exceptional line E_5 is $z = 0$. The affine equation of the new curve C_5 is $f_5(x_1', z) = x_1'^2 + z + z^2 + zx_1' + \cdots = 0$. The node lying above P_{11212} is the point P_{112121} with local coordinates x_1' and z of multiplicity, $m_{P_{112121}}(C_5) = 1$.

Blow-up vi: of the point P_{11211}. The equation of the local exceptional line E_5 is $z = 0$. The affine equation of the new curve C_5 is $f_5(x_5, z) = x_5^2 + 1 + z^2 + z + \cdots = 0$. The point, above P_{11211} is the point P_{112111} with local coordinates $x_5 + 1 = x''$ and z and multiplicity, $m_{P_{112111}}(C_5) = 1$.



Remarks. Notice that after the first blown up of the curve around its singular point, we do not attain a plane curve but a curve in the product space, $\mathbf{P^2} \times \mathbf{P^1}$. As the blowing-up process continues, the curve becomes a higher dimensional projective curve whose affine piece is represented by a polynomial equation. We can use the Veronese mapping (Mumford, [52]; Shafarevich [60]) to end up in some projective plane P^N.

2.3 Cremona transformations

In this section we will see how we can reduce singularities using birational or as it is called Cremona transformations. In this treatment we follow the suggestions of Fulton [21] and Goppa [26] concerning the proper treatment of terrible points (Moreno [45], pg. 237).

Remark. We might have to extend the field of constants in some cases as for instance, when the points are not rational (we do not consider such points in this section) and the tangents at the points are not rational; when the curve does not intersect the exceptional lines in distinct rational points. We might also have to extend the field of constants in order to eliminate a terrible point (Moreno [45], pg. 237).

We next describe an algorithmic construction which finds a birational equivalent curve having only ordinary singularities.

Algorithm CT: * Cremona Transformations *
Input: A plane curve $C : F = 0$ of degree n defined over the finite field, $\mathbf{k} = \mathbf{F}_{p^b}$. The singular points Q_i of the curve and their multiplicities.
Output: A curve C' birationally equivalent to the curve, C having only ordinary singular points.
Method:

Step 1: Eliminate the terrible points of the original curve C (Moreno [45], pg. 273).

Step 2: Choose a projective transformation $T: \mathbf{P}^2(\mathbf{k}) \longrightarrow \mathbf{P}^2(\mathbf{k})$ which transforms the singular points Q_i to the fundamental points P_i, $i = 1, 2, 3$ of multiplicities r_i and the transformed curve C^T to a curve in excellent position (Fulton, pg. 175).

Step 3: Evaluate the form $F^{T \circ Q}$ which yields the application of the composition of a projective and a quadratic transformation on the curve C.

Step 4: Factor the transformed form $F^{T \circ Q}$ as $X^{r_1} Y^{r_2} Z^{r_3}(F_1)$.

Step 5: The new curve C_1 is given by the form F_1. Find the singularities of the curve C_1 and their multiplicities.

Step 6: Repeat the steps one to five to the new curve C_1.

Step 7: Repeat the steps one to six until you get a curve C' having at worst ordinary singularities.

Remark. Step 1 is also dealt by Goppa ([26], pg.102).

Lemma 2.4 *The algorithm CT terminates and its time complexity is polynomial in the degree of the curve.*

Proof. The proof of the lemma is straight forward. The following argument actually yields an effective estimate considering the Rationality assumption.
The first step requires the elimination of a terrible point obtained by the application of a projective transformation (Moreno, [45], pg. 237). The Cremona transformation is the composition of a projective and a quadratic transformation . The application of the projective transformation requires most time. Therefore let us estimate the time comlexity required by the application of a projective transformation.
The computation of the transformed homogeneous form F^T requires the evaluation

$$F(a_1X + b_1Y + c_1Z, a_2X + b_2Y + c_2Z, a_3X + b_3Y + c_3Z)$$

as a homogeneous form in X, Y, Z.

For multiplying two homogeneous forms of degrees l and t we proceed as follows: Each homogeneous form of degree l (resp. t) contains $l(l+3)/2+1 = O(l^2)$ (resp. $O(t^2)$) terms (Fulton [21], pg.109). Each term of the $O(l^2)$ terms is multiplied by each of the $O(t^2)$ terms of the other homogeneous form. Each such multiplication is equivalent in multipling two elements in F_q which takes $O(\log^3 q)$ time. Thus the multiplication of two homogeneous forms of degrees l and t requires $O(l^2t^2\log^3 q)$ operations.

The complexity of computing each $(a_1X+b_1Y+c_1Z)^i$ requires at most $O(n^4\log^3 q)$ bit operations. This contains an estimate for the calculation of F^T which is of the form: $\alpha_{ij}(a_1X+b_1Y+c_1Z)^i(a_2X+b_2Y+c_2Z)^j(a_3X+b_3Y+c_3Z)^k$.
Since $F[X,Y,Z]$ it self has $O(n^2)$ terms then the total complexity of performing a quadratic transformation is $O(n^6\log^3 q)$.

Throughout the algorithm CT we need to apply $N+g^*(C)$ Cremona transformations (Fulton [21], pg.178) where N is the number of nonordinary singularities which is at most $O(q^2)$ and $g^*(C)$ is the virtual genus (Fulton [21], pg.176) of the curve which is at most $O(n^2)$.

We conclude that the time complexity of the algorithm CT is $O((n^2+q^2)n^6\log^3 q)$ which can be replaced by

$$O(q^2n^8\log^3 q)$$

□

Example 2.5 Consider the curve defined by the quartic, $F = Y^2Z^2+X^2Z^2+X^2Y^2 = 0$ over the finite field $\mathbf{k} = \mathbf{F}_3$.

The points $P_1 = [1,0,0]$, $P_2 = [0,1,0]$ and $P_3 = [0,0,1]$ are non-ordinary double points, i.e $m_{P_i} = 2$ The characteristic of the field $\mathbf{k}$ does not divide the difference degF $- m_{P_i}(C) = 4-2 = 2$. Thus the points P_i are not terrible points on the curve (Moreno [45], pg. 237). The quadratic transformation Q transforms the original curve to the curve with equation,

$$F^Q = X^2Z^2X^2Y^2 + Y^2Z^2X^2Y^2 + Y^2Z^2X^2Z^2 = 0$$

The transformed curve can be factored as $F^Q = (X^2Y^2Z^2)(X^2+Y^2+Z^2) = 0$ Thus, the homogeneous form $F_1 = X^2+Y^2+Z^2$ is the equation of the new curve C_1 which is a non-singular quadric.

The following algorithm finds the local representations of the nonsingular model of the curve C. It resolves the singularities in the following manner. It first finds a birational equivalent curve, C' to the original curve C having only ordinary singularities. Then it uses the algorithm BU in order to blow-up the curve C' around every ordinary singular point. Thus the local non-singular model, $\tilde{C}$ of the curve C' around each ordinary singularity is constructed through the composition of the Cremona transformations and the birational morphism $\pi: \tilde{C} \longrightarrow C'$ i.e.,

$$\tilde{C} \xrightarrow{\pi} C' \xrightarrow{T \circ Q} C$$

The composition of the projective and the quadratic transformation $T \circ Q$ is the *Cremona transformation.*

The fact that C' will be at worst a curve with only ordinary singularities is obtained from Noether's theorem (Noether [53], Fulton [21], pg.177; Bliss [9]).

Theorem 2.1 (Noether's theorem) *Every irreducible algebraic plane curve can be transformed into another with only ordinary singular points by the compositions of projective and quadratic transformations.*

The following algorithm illustrates the resolution of the rational singularities of the original curve by the successive applications of Cremona transformations and the birational morphism π.

Algorithm RC: * Resolution of singularities through Cremona transformations *

Input: A plane curve C defined over the finite field $\mathbf{k} = \mathbf{F}_q$ with $q = p^b$ elements. The singular points of the curve C and their multiplicities.
Output: A local representation of the non-singular model of the curve C' birational equivalent to the curve C around its ordinary singular points.
Method:

Step 1: Find a birational equivalent curve C' having only ordinary singularities applying the algorithm CT on the original curve C.

Step 2: Apply the (local) blowing-up process once, to each ordinary singular point, of the curve C' (algorithm BU).

Lemma 2.5 *The algorithm RC terminates and its time complexity is polynomial in the degree of the curve.*

Proof.
The proof of the lemma is straight forward. The following argument actually yields an effective estimate considering the Rationality assumption.
Applying the algorithm CT requires $O(n^8q^2\log^3 q)$ time which is the estimate of the first step of the algorithm. The curve C' which we obtain after $O(n^2 + q^2)$ steps is of degree $O(n^3 + nq^2)$, considering the grow of the degree of the curve after each Cremona transformation (Moreno [45], pg. 233).

We need to blow up the curve C' around each of the $O(q^2)$ ordinary singularities applying the algorithm BU whose time bound is $O(q^2rn^4\log^3 q)$ where r is the multiplicity of the curve C' at each worst singularity. Thus the overall time bound is $O(q^2r(n^3 + nq^2)^4\log^3 q)$ which can be replaced by $O(q^{10}rn^{12}\log^3 q)$. Thus $C(2) = O(q^{12}rn^{12}\log^3 q)$. Hence the time complexity of the algorithm RC is

$$O(q^{12}rn^{12}\log^3 q)$$

□

Example 2.6 (Klein Quartic) Consider the curve C defined by the homogeneous equation $F = XZ^3 + Y^3Z + XY^3 = 0$ over the finite field $\mathrm{k} = \mathbf{F}_4 = \{0, 1, \alpha, \beta\}$.

The curve C has a non-ordinary singular point $Q_1 = [1,0,0]$ of multiplicity $m_{Q_1}(C) = 3$. The three non distinct tangents of C at Q_1 are given by the local equation $z^3+y^3 = 0$ where the local affine parameters are $z = Z/X$ and $y = Y/X$. The other two fundamental points, $Q_2 = [0,1,0]$ and $Q_3 = [0,0,1]$ are non-singular.

The application of the quadratic transformation Q yields the transformed curve, described by the form, $F^Q = F(YZ, XZ, XY)$. The factorization of

$$F^Q = YX^3Z[Y^3 + XZ^2 + Z^3]$$

yields the birational equivalent curve C_1 with equation $F_1 = Y^3 + XZ^2 + Z^3 = 0$. The degree of the new form F_1 equals 3 , i.e., $2\mathrm{deg}F - m_{Q_1}(C) - m_{Q_2}(C) - m_{Q_3}(C)$ as is claimed (Fulton [21], pg.173). The multiplicity of Q_1 on the new curve C_1 is $m_{Q_1}(C_1) = \mathrm{deg}F - m_{Q_2}(C) - m_{Q_3}(C)$ and equals 2 as it was claimed.

We can check that $Q_1 = [1,0,0]$ is a non-ordinary point since there are two non distinct tangents of C_1 at Q_1 given by the polynomial equation $z = 0$. Since the characteristic of the finite field k which is 2 does not divide the difference, $\mathrm{deg}F_1 - m_{Q_1}(C_1) = 3 - 2$ (Moreno [45] pg. 237), we conclude that the point Q_1 is not a terrible point, on C_1.

Since C_1 has a non-ordinary point Q_1 then we have to apply again a composition of a projective and quadratic transformation (Cremona) centered at Q_1. The intersection divisors attained from intersecting the lines $X = 0$, $Y + \beta Z = 0$ and $Y + \alpha Z = 0$ by the curve C_1 with the homogeneous equation $F_1 = 0$ are as follows

$$\begin{aligned} X \quad &\bullet \quad F_1 = [0,1,1] + [0,\alpha,\beta] + [0,\beta,\alpha] \\ (Y+\beta Z) \quad &\bullet \quad F_1 = [0,\beta,1] + 2[1,0,0] \\ (Y+\alpha Z) \quad &\bullet \quad F_1 = [0,\alpha,1] + 2[1,0,0] \end{aligned}$$

Thus the needed projective transformation is :

$$T(X, Y+\beta Z, Y+\alpha Z) : \mathbf{P}^2(\mathbf{k}) \longrightarrow \mathbf{P}^2(\mathbf{k})$$

We apply the quadratic transformation to the transformed curve $F_1^T = Z^2Y + ZY^2 + XY^2 + \beta XZ^2$ to attain, $F_1^{T\circ Q} = X^2YZ(YX + XZ + Z^2 + \beta Y^2)$. The degree of C_2 described by the form $F_2 = YX + XZ + Z^2 + \beta Y^2$ is $\mathrm{deg}F_2 = 2\mathrm{deg}F_1 - m_{Q_1}(F_1) - m_{Q_2}(F_1) - m_{Q_3}(F_1) = 6 - 2 - 1 - 1 = 2$ where the projective transformation T transforms the points, $T(0,\alpha,1) = [0,1,0] = Q_2$ and $T(0,\beta,1) = [0,0,1] = Q_3$. We can check that the new curve C_2 is a non-singular curve.

Remark. Note that the curve $C : Y^2Z^3 + YZ^4 + X^5 = 0$ of degree 5 over the finite field $\mathbf{k} = \mathbf{F}_{16}$ is a singular curve where the point $P = [0,1,0]$ is nonordinary singular point of multiplicity $m_P(C) = 3$. The point P is a terrible point (since $2/(5\text{-}3)$). We need to extend the field of constants in order to eliminate the terrible point P since there is not such a projective transformation T (in the present field) which makes C^T to be in *excellent position* (for definition of excellent position see Fulton [21], pg. 175).

2.4 Integral Basis Algorithm

Another way to resolve the singularities of a singular plane curve is based on the integral basis algorithm. The algorithm has been initiated by Ford and Zassenhaus [20]. It also appears on Trager's thesis [62]. Ford and Zassenhaus were interested in the case of algebraic number fields but their algorithm also applied to function fields of one variable.

M. Hassner [15] and the research group from IBM applied the above results to create a program in Scratchpad, a symbolic computer language under development at the IBM Research Mathematics Department.

Vasquez [68] discussed the theoretical basis of the algorithms which Hassner presented, and clarified the basic concepts and definitions.

Our main contribution in this section is to modify the integral basis algorithm to the case where the function field of one variable is the function field of a curve. The curve is defined over a finite field. Our algorithmic construction IBA is based on Vasquez [15], [68]. It finds an integral basis of the integral closure of the coordinate ring of a plane curve. We show that the time complexity of the algorithm is polynomial in the degree of the curve. An example which illustrates the integral basis algorithm is presented (ex. 2.7). We next give the non-singular model construction NSM . This method finds the non-singular model of a plane curve lying over the points away from the point at infinity. Example 2.8 shows how we apply this technique; it also computes the infinitely near points.

2.4.1 Algorithm IBA

For the concepts which appear in this section, we refer the reader to Macdonald [44] , Van der Waerden [19] and Vasquez [68].

Definition 2.2 *Let m be an ideal of the ring R then the* radical *of the ideal m is the ideal*

$$\mathrm{rad}(m) = \{u \in R: \quad u^s \in m \text{ for } s \in Z\}$$

Definition 2.3 *The* idealizer *or the* conductor *of the ideal m is the set*

$$\mathrm{Id}(m) = \{u \in QF(R): \quad um \subset m\}$$

and is the largest ring of R in which m is still an ideal.

Notation. By A we denote the coordinate ring of the affine line.

In this section we will describe the integral basis algorithm IBA. This algorithmic construction estimates a basis of the integral closure of the coordinate ring of the curve. The integral basis algorithm states as follows:

Algorithm IBA *Integral Basis Algorithm*
Input: An irreducible plane projective curve $C : F(X, Y, Z) = 0$, defined by the homogeneous form $F \in F_q[X, Y, Z]$. The affine representation of the curve C around

its singular point P of multiplicity r is the polynomial $f(x,y)$ of degree n. The affine coordinate ring of C is $R_0 = \mathbf{k}[x,y]/(f)$. The prime factor p which appears in the discriminant of the polynomial f and has the point P as its root.
Output: An integral basis of the integral closure $\overline{R}_0$ of the coordinate ring R_0 of the curve C in its quotient field of the curve.

Step 1: Pick the trivial basis $\{1, y, ..., y^{n-1}\}$ of the coordinate ring R_0 considered as a free $A = \mathbf{k}[x]$-module.

Step 2: Find a basis for $\mathrm{rad}(pR_0)$.

We find a basis for $\mathrm{rad}(pR_0)$ considered as a free A-module by finding the basis of the inverse image of the set of all nilpotents of the quotient ring R_0/pR_0 under the homomorphism ϕ considered as a free A/pA-module.

Step 3: Find a basis of $R_1 = \mathrm{Id}(\mathrm{rad}(pR_0))$.

We set conditions on when an element b in the quotient field $QF(R_0)$ belongs in R_1.

Step 4: Calculate the dimension $\dim_{\mathbf{k}} R_1/R_0$.
If the dimension $\dim_{\mathbf{k}} R_1/R_0 = \dim_{\mathbf{k}} \overline{R}_0/R_0$, then the integral basis of $\overline{R}_0$ is the one found in step 3. Otherwise set $R_0 = R_1$ and go back to step 2.

Step 5: Repeat the process until you find a ring R_i such that $\dim_{\mathbf{k}} R_i/R_0 = \dim_{\mathbf{k}} \overline{R}_0/R_0$.

Lemma 2.6 *The integral basis algorithm terminates and its time complexity is polynomial in the degree of the curve.*

Proof.
In the second step of the algorithm we need to find the nilpotent elements of the quotient ring R_0/pR_0 and we proceed as follows:
In order to find the nilpotent elements of the ring $\phi^{-1}(\mathcal{A}_{pR_i})$ we proceed as follows: Let $\{u_i\}_{i=1}^n$ be a basis for the quotient ring R_i/pR_i as A/pA module. Let the cardinality[1] of the ring A/pA be denoted by q. We need to find the elements $(a_1, \cdots, a_n)$ in $(A/pA)^n$ such that the sum $a_1u_1 + \cdots + a_nu_n$ is a nilpotent element , i.e., $(a_1u_1 + \cdots + a_nu_n)^{q^d} = 0$ for an integer d such that $n \leq q^d$, i.e., we have to solve the equation $\sum_{i=1}^n a_i u_i^{q^d} = 0$ $(*)$. Thus we have to compute the elements $u_i^{q^d}$ such that $u_i^{q^d} = \sum c_{ij}u_j$ for some $c_{ij} \in A/pA$. Then equation $(*)$ becomes: $\sum_{i=1}^n a_i(\sum_j c_{ij}u_j) = 0$, i.e., $\sum_i c_{ij}a_i = 0, \forall j$. Thus using linear algebra we need to find a basis for the set of solutions imposed by the system of equations $\sum_i c_{ij}a_i = 0$.

The time complexity of the above system of equations is $O(n^3 \log^3 q)$ which becomes the time complexity of this step.

In the third step, where we need to find a basis for the idealizer of R_1 we proceed as follows: We first multiply both sides of the equation $b = \sum_{i=0}^{n-1} a_i y_i$ by x and y^i,

[1]The cardinality of A/pA is the same as the cardinality of the finite field, $\mathbf{k}$

$i = 1, ..., n-1$ (i.e., we obtain n equations). Each multiplication requires $O(n)$ time and we have n multiplications. Hence, $O(n^2)$ bit operations take place.
We now rewrite y^m as $\sum_{i=0}^{n-1} l_i(x)y_i$ where $l_i(x) \in \mathbf{k}[x]$ for each $m > n$. We achieve this by solving the equation $f(x,y) = 0$ with respect to y^n and then by multypling successively the resulting equation by y. There are $m-n$ many multiplications to be made. Thus the computation of y^m requires $O(n^2)$ bit operations.
Next, we make the substitution $y^m \longmapsto \sum_{i=0}^{n-1} l_i(x)y_i$ in the n equations (for each $m > n$) . Each substitution requires $n-1$ multiplications where each multiplication needs $O(n^3\log^3 q)$ time. There are $O(n^2)$ such substitutions to be made.
Hence the total complexity of this operation is $O(n^4\log^3 q)$.
Thus the total time complexity of the third step is $O(n^4\log^3 q)$.
We have to repeat the steps of the algorithm $\dim_{\mathbf{k}} \overline{R}_0/R_0 = r(r-1)/2$ number of times.
Thus the number of bit operations required by the integral basis algorithm is

$$O(r^2n^4\log^3 q)$$

□

In the following example we will apply the integral basis algorithm IBA in order to find a basis for the integral closure of the coordinate ring of the given curve C.

Example 2.7 Consider the curve $C : F = X^2Z^2 + XYZ^2 + Y^4 = 0$ defined over the finite field $\mathbf{k} = \mathbf{F}_2$.

The curve C has an ordinary point $P = [0,0,1]$ with multiplicity $r = 2$. The representation of the curve C around the point P is given by the polynomial equation $f(x,y) = x^2 + xy + y^4 = 0$. The local coordinates in this affine neighborhood are $x = X/Z$ and $y = Y/Z$.
The discriminant of the polynomial f is x^4 and the prime factor which appears in the discriminant is $p = x$. The affine coordinate of the curve is $R_0 = \mathbf{k}[x,y]/(x^2+xy+y^4)$.

Step 1: Let $R_0 = \mathbf{k}[x,y]/(f)$ be the affine coordinate ring of the curve C which is a free A-module with basis $\{1, y, y^2, y^3\}$.

Step 2: We want to find a basis of the radical ideal, $\mathrm{rad}(xR_0)$, as free A-module. This is equivalent to find the nilpotents in $R_0/(xR_0)$. From the equation $f = 0$ we conclude that the coordinate y can be written as $y^4 = x(x+y)$ which implies that the image of y^4 in $R_0/(xR_0)$ is zero, i.e., $\overline{y}^4 = 0$. Thus $\{\overline{y}, \overline{y}^2, \overline{y}^3\}$ are the nilpotent elements of R_0/xR_0 which implies that $\{x, y, y^2, y^3\}$ is the basis of $\mathrm{rad}(xR_0)$.

Step 3: Find a basis for the idealizer $R_1 = \mathrm{Id}(\mathrm{rad}(xR_0))$.

The ring $R_1 = \mathrm{Id}(\mathrm{rad}(xR_0))$ is the set, $\{b \in QF(R_0)\colon b\,\mathrm{rad}(xR_0) \subset \mathrm{rad}(xR_0)\}$. The ideal $\mathrm{rad}(xR_0)$ is generated by the elements $\{x, y_i\}$ where $i = 1,2,3$ i.e., $R_1 = \{b \in QF(R_0)\colon bx \in \mathrm{rad}(xR_0),\ by^i \in \mathrm{rad}(xR_0)\}$. Let b be an element of

the quotient field $QF(R_0)$. Then the element b can be written as the linear combination $b = a_0 + a_1y + a_2y^2 + a_3y^3$ where $a_i \in QF(A)$. The condition: $bx \in \text{rad}(xR_0)$ translates as $bx = a_0x + a_1xy + a_2xy^2 + a_3xy^3$ i.e., $a_0x \in A$, $a_1x \in A$, $a_2x \in A$ and $a_3x \in A$.

The condition $by^i \in \text{rad}(xR_0)$ translates as:

$by = a_3x^2 + (a_0 + a_3x)y + a_1y^2 + a_2y^3$ i.e., $a_3x^2 \in A$, $a_3x + a_0 \in A$, $a_1 \in A$ and $a_2 \in A$.

Similarly, $by^2 = a_2x^2 + (a_2x + a_3x^2)y + (a_0 + a_3x)y^2 + a_1y^3$i.e., $a_2x^2 \in A$, $a_2x + a_3x^2 \in A$, $a_0 + a_3x \in A$ and $a_1 \in A$.

Finally, $by^3 = a_1x^2+(a_1x+a_2x^2)y+(a_2x+a_3x^2)y^2+(a_0+a_3x)y^3$ i.e., $a_1x^2 \in A$, $a_1x + a_2x^2 \in A$, $a_2x + a_3x^2 \in A$ and $a_0 + a_3x \in A$.
Therefore the conditions for the element $b \in QF(R_0)$ to belong in R_1 are:

$$a_0 \in A,\ a_1 \in A,\ a_2 \in A,\ a_3x \in A$$

Thus the ring R_1 is a free A-module with basis, $\{1, y, y^2, y^3/x\}$.

Step 4: The ring R_1/R_0 is isomorphic to the direct sum, $A/A \oplus A/A \oplus A/A \oplus A/xA$ (Vasquez [68], pg.18) which implies that the dimension of the ring R_1/R_0 over $\mathbf{k}$ is one. Note that the dimension, $\dim_{\mathbf{k}} R_1/R_0$ is the same as the integer induced by $r(r-1)/2$ which is the dimension of the ring $\overline{R}_0/R_0$. Therefore, the ring R_1 is the integral closure $\overline{R}_0$. Thus the integral basis of the integral closure $\overline{R}_0$ is the set of functions $\{1, y, y^2, y^3/x\}$.

2.4.2 Nonsingular Model Construction

The underlining theme of this section is the connection of the desingularization process and the integral basis algorithm. We show that the calculation of the integral closure of the affine coordinate ring of a plane curve amounts to find the affine nonsingular model of the curve. The main theorem in this section is theorem 2.1 (see also Vasquez [68], pg.10) which implies the algorithmic construction NSM . The construction NSM computes an affine nonsingular model of a plane curve lying over the points away from the points at infinity.

Let the rational functions $\{u_0 = x, u_1, \cdots, u_n\}$ form a basis for the integral closure $\overline{R}_0$ of the affine coordinate ring of the curve C as an A-module. Recall that A is the coordinate ring of the affine line, $\mathbf{k}[x]$. Take all possible products of the elements in the base, i.e., $u_iu_j = \sum_{\alpha=0}^{n} a_{ij}^{\alpha}(x)u_\alpha$ where $a_{ij}^{\alpha} \in A$. Introduce new variables, $\{Y_0 = x, Y_1, \cdots, Y_n\}$ and form the functions $f_{ij}(Y_0 = x, Y_1, \cdots Y_n) = Y_iY_j - \sum_{\alpha=0}^{n} a_{ij}^{\alpha}(x)Y_\alpha$ in $\mathbf{k}[x, Y_1, \cdots, Y_n]$ where $i \geq 1$ and $j \leq n$. The variety V defined as $V = \{a \in \overline{k}^{n+1}:\ f_{ij}(a) = 0\, \forall i, j\}$ is a nonsingular affine curve. The ideal $I(V)$ of the variety V is the set, $I(V) = \{g \in \mathbf{k}[x, Y_1, \cdots, Y_n]:\ g(a) = 0\, \forall a \in V\} = (f_{ij})$. The affine

coordinate ring $\mathrm{k}[V]$ of the variety V is $\mathrm{k}[V] = \mathrm{k}[Y_0 = x, Y_1, \cdots, Y_n]/I(V)$. With the above notation we can have the following theorem:

Theorem 2.2 *Let y_i be the image of Y_i under the canonical map $\pi : \mathrm{k}[x, Y_1, \cdots, Y_n] \longrightarrow \mathrm{k}[x, Y_1, \cdots, Y_n]/I(V)$. We then have that the map $\tilde{\phi}$: $\mathrm{k}[V] = \mathrm{k}[x, Y_1, \cdots, Y_n]/I(V) \longrightarrow \overline{R_0}$ defined as $x \longmapsto x$ and $y_i \longmapsto u_i$ is a* k*-isomorphism of rings.*

proof
Consider the diagram,

$$\begin{array}{ccc} \mathrm{k}[x, Y_1, \cdots, Y_n] & \overset{\phi}{\hookrightarrow} & \overline{R_0} = \overline{\mathrm{k}[C]} \\ \pi \downarrow & & \\ \mathrm{k}[V] = \mathrm{k}[x, Y_1, \cdots, Y_n]/I(V) & & \end{array}$$

The map ϕ: $\mathrm{k}[x, Y_1, \cdots, Y_n] \longrightarrow \overline{R_0}$ defined as $\phi(g(x, Y_1, \cdots, Y_n)) = g(x, u_1, \cdots, u_n)$ is an epimorphism. If we show that the ideal $I(V)$ is the kernel of ϕ then by applying the first isomorphism theorem (Hungerford [32], pg.172) we will conclude that ϕ induces the ring isomorphism $\tilde{\phi}$. The kernel of the map, ϕ is the set

$$\mathrm{Ker}\phi = \{q \in \mathrm{k}[x, Y_1, \cdots, Y_n]: \quad q(x, u_1, \cdots, u_n) = 0\}$$

We first show that $I(V) = (f_{ij})$ is a subset of $\mathrm{Ker}\phi$.

Suppose the function g belongs in the ideal $I(V) = (f_{ij})$ then the function g is the sum $g = \sum a_i f_{ij}(x, Y_1, \cdots, Y_n)$. It implies that the image of g under ϕ is zero, i.e., $\phi(g) = \sum a_i f_{ij}(x, u_1, \cdots, u_n) = 0$. Thus, the function g belongs in the kernel $\mathrm{Ker}(\phi)$. It remains to show that $\mathrm{Ker}\phi$ is a subset of $I(V)$.

Let q be an element in the kernel of the map ϕ, i.e., $\phi(q) = q(x, u_1, \cdots, u_n) = 0$. Suppose $q \notin I(V) = (f_{ij})$ then $q \neq \sum_i a_i f_{ij}(x, Y_1, \cdots, Y_n)$. Define the nonzero functions m_{ij} as the difference $m_{ij} = q - \sum a_i f_{ij}(x, Y_1, \cdots, Y_n)$. The image of the functions m_{ij} under the map ϕ is $\phi(m_{ij}) = \phi(q) - \sum a_i \phi(f_{ij}(x, Y_1, \cdots, Y_n))$. In particular $\phi(m_{ij}) = \phi(q) - \sum a_i f_{ij}(x, u_1, \cdots, u_n)$. The last equation shows that $\phi(q) = \phi(m_{ij}) + \sum a_i f_{ij}(x, u_1, \cdots, u_n)$ which implies that $\phi(q) \neq 0$. Thus we are led to a contradiction since q belongs in the kernel of ϕ.
□

Remark . Another proof can be seen in Vasquez ([68], pg.10).

Corollary 2.2.1 *The variety V is that part of the nonsingular model $\tilde{C}$ of the curve C which lies over the points away from the points at infinity. The birational morphism $\pi: V \longrightarrow C$ corresponds to the* k*-isomorphism of the coordinate rings, i.e., $\mathrm{k}[C] \longrightarrow \mathrm{k}[V]$. The coordinate ring of the variety V is isomorphic to the integral closure of the coordinate ring of the curve C i.e., $\mathrm{k}[V] \cong \overline{\mathrm{k}[C]}$.*

Based on theorem 2.1 we present a construction which computes a nonsingular model of the curve lying over the points away from the points at infinity.

Algorithm NSM *Nonsingular Model Construction*
Input: The integral basis $\{u_0, u_1, ..., u_n\}$ of $\overline{R}_0$.
Output: The non-singular part of the curve C lying over the points away from the points at infinity.

Step 1: Introduce new variables $\{Y_i\}_{i=0}^n$ which correspond to the elements in the basis, i.e., Y_i corresponds to u_i.

Step 2: Consider the polynomial ring $\mathbf{k}[Y_0, ..., Y_n]/I$ where I is the ideal generated by the polynomials $f_{ij}(Y_0, ..., Y_n)$ in the ring of polynomials $\mathbf{k}[Y_0, ..., Y_n]$. Compute the polynomials f_{ij} of the form $f_{ij} = Y_iY_j - \sum a_{ij}^{\alpha}(x)Y_{\alpha}$.

Step 3: The variety $V = \{a \in \overline{\mathbf{k}}^{n+1} : f_{ij}(a) = 0 \forall i, j\} \subset \mathbf{k}^{n+1}$ is the affine nonsingular model of C defined over the points away from the points at infinity. The coordinate ring of V is $\mathbf{k}[V] = \mathbf{k}[Y_0, ..., Y_n]/(f_{ij})$.

Lemma 2.7 *The algorithm NSM terminates and its time complexity is polynomial in the degree of the curve.*

Proof.
For constructing each polynomial f_{ij} we need to replace y^m by $\sum_{i=0}^{n-1} l_i(x)y_i$ for each $m > n$. That takes $O(n^2)$ time (see proof of lemma 2.6). There are at most $O(n)$ such computations to be made.

We also need to perform a division which requires at most $O(n^2 \log^3 q)$ bit operations.

There are at most $(n-1)n/2 = O(n^2)$ polynomials f_{ij}. Thus the total time complexity of the algorithm NSM is

$$O(n^4 \log^3 q)$$

□

Example 2.8 We use the curve C described in example 2.5 and we construct the affine nonsingular model of C.

From example 2.5 we concluded that the basis of the integral closure $\overline{R}_0$ is the set of functions $\{1, y, y^2, y^3/x\}$. We find the points lying above the singular point P of the curve.

Step i: Represent the curve lying over the points away from the points at infinity, i.e., the affine nonsingular model of the curve C.

Introduce new variables $\{Y_i\}$ from $i = 0, ..., 3$ which correspond to the elements in the basis of the integral closure $\overline{R}_0$.

Step ii: Define polynomials $f_{ij} \in \mathbf{k}[x, Y_1, Y_2, Y_3]$ of the form $f_{ij} = Y_iY_j - \sum_{\alpha=0}^{3} a_{ij}^{\alpha}(x)Y_\alpha$. Consider the correspondence of the variables $\{Y_i\}_{i=0}^{3}$ with the elements in the integral basis and the original affine equation of the curve $f = x^2 + xy + y^4$ to find the polynomials f_{ij}.

$$\begin{aligned}
Y_1^2 = y^2 = Y_2 &\longleftrightarrow f_{11} = Y_1^2 - Y_2 \\
Y_1Y_2 = y^3 = xY_3 &\longleftrightarrow f_{12} = Y_1Y_2 - xY_3 \\
Y_1Y_3 = y^4/x = x + Y_1 &\longleftrightarrow f_{13} = Y_1Y_3 - (x + Y_1) \\
Y_2^2 = y^4 = x^2 + xY_1 &\longleftrightarrow f_{22} = Y_2^2 - x^2 - xY_1 \\
Y_2Y_3 = y^5/x = Y_1^2 + xY_1 &\longleftrightarrow f_{23} = Y_2Y_3 - Y_2 - xY_1 \\
Y_3^2 = y^6/x^2 = Y_2 + Y_3 &\longleftrightarrow f_{33} = Y_3^2 - Y_2 - Y_3
\end{aligned}$$

Step iii: Thus the non-singular model $\tilde{C}$ of the curve C lying over the singular point P is $\tilde{C} = \{a \in \overline{k}^4 \colon f_{ij}(a) = 0\}$. The coordinate ring of the affine nonsingular model $\tilde{C}$ of the curve is $\mathbf{k}(\tilde{C}) = \mathbf{k}[x, Y_1, Y_2, Y_3]/(f_{ij})$.

Step iv: Find the points lying above the singular point P where $x = 0$ i.e., infinitely near points.

We need to find the points which belong in the set

$$\pi^{-1}(P) = \{(0, Y_1, Y_2, Y_3) \colon f_{ij}(0, Y_1, Y_2, Y_3) = 0\}$$

The system of equations $f_{ij}(0, Y_1, Y_2, Y_3) = 0$ gives the solutions $P_1 = (0, 0, 0, 0)$ and $P_2 = (0, 0, 0, 1)$. The points P_1 and P_2 are the points lying above the singular point P. We can check that the curve $\tilde{C}$ is nonsingular around the points P_1 and P_2 by calculating the rank of the matrices $(\partial f_{ij}/\partial Y_i(P_1))_{0 \le i \le 3}$ and $(\partial f_{ij}/\partial Y_i(P_2))_{0 \le i \le 3}$. In both cases the rank of the matrices equals the number of variables (which is 4) minus the dimension of the curve (which is 1), i.e., in both cases the rank is 2.

Remark. The nonsingular model construction NSM is a local procedure. In particular, we resolve the singularities of the curve one at a time and we do not have to worry about field extensions.

The nonsingular model $\tilde{C}$ of the curve C is an affine model above the particular singularity which we examined. In order to resolve all the singularities of the curve C we have to apply the integral basis algorithm and then the nonsingular model construction for the $O(q^2)$ singular points of the curve. If we follow our complexity estimates the total resolution of the singular curve C will take the time to compute the integral basis algorithm plus the time taken to compute the nonsingular model construction. Thus the overall time bound to resolve the singularities of the curve via the integral basis algorithm is

$$O(n^6q^2r^2n^6\log^3 q))$$

where r is the multiplicity of the curve C at each worst singularity.

Chapter 3

Theory of Adjoints

The topics discussed in this chapter are related to the problem of effectively calculating with the Riemann-Roch theorem. Particularly the classical concepts of adjoint divisors, adjoint curves are reconsidered from a constructive point of view in which the field of constants is a finite field.

In the first section of the chapter we consider four different definitions of the adjoint divisor. Even though these definitions are quite classical, our main concern is to rework the definitions over a finite field of constants. The first definition (def. 3.2) is motivated by the theory of the conductor ideal. The discussion is based on Serre [58], [59], Abhyankar [2] and Samuel [56]. The second definition (def. 3.3) is of geometric nature and describes the adjoint divisor in terms of differentials of the first kind. It first appeared in Gorenstein [27] and it was discussed by Kodaira [40]; further information can be found in Samuel [56] and Arbarello [6]. The third definition (def. 3.4) is based on the normalization process and appears to be more computational; it was first presented by Keller [37] and is also used by Le Brigand and Risler [43]. The last definition considered (def. 3.5) is due to Noether and applies to curves defined over an algebraically closed field with only ordinary singularities. It also appears in Fulton [21] for the case where the field of constants is algebraically closed (of characteristic zero).

Our contribution in the first section is algorithm AD and theorem 3.1 which establishes the equivalence of the definitions of the adjoint divisors.

The definition of the adjoint curve is given in the second section whose main objective is to show the equivalence of three conditions for a curve to be an adjoint curve (th. 3.2).

The next section deals with the calculation of the discriminant divisor for a polynomial in two variables, which represents an affine neighborhood of a singular projective curve. Theorems 3.3 and 3.4 are the important theorems which provide two formulas for the computation of the discriminant divisor.

3.1 Four equivalent definitions of the adjoint divisor

In this section we state four definitions for the adjoint divisor which appear in the literature.
Notation: Let A be a subring of a field K. We denote by $\overline{A}$ the integral closure of A inside K. The local ring of a curve C at the point P is indicated by $\mathcal{O}_P(C)$.

Definition 3.1 *Let $f(x,y) = 0$ be the local equation of the curve C around its singular point P. The (local)* conductor *of $\overline{\mathcal{O}_P(C)}$ in $\mathcal{O}_P(C)$ is the ideal :*

$$Con(\overline{\mathcal{O}_P(C)}, \mathcal{O}_P(C)) = \left\{c \in \overline{\mathcal{O}_P(C)} : ac \in \mathcal{O}_P(C) \quad \forall a \in \overline{\mathcal{O}_P(C)}\right\}$$

Let us simplify the notation by denoting the (local) conductor $Con(\overline{\mathcal{O}_P(C)}, \mathcal{O}_P(C))$ by $\mathcal{C}$.
Facts.

i. The conductor $\mathcal{C}$ is an ideal of both $\overline{\mathcal{O}_P(C)}$ and $\mathcal{O}_P(C)$.

ii. The conductor as an ideal of $\overline{\mathcal{O}_P(C)}$ will follow the above properties, i.e., the conductor will be generated by a rational function g i.e., $\mathcal{C} = (g)$ where $g = \prod_{i=1}^{N} t_i^{\alpha_i}$ and the integers $\alpha_i = \min\{\text{ord}_{Q_i}(j) : j \in \mathcal{C}\}$.

iii. There are two methods of measuring how singular C is at P (Abhyankar [2]). The first, is the $\mathcal{O}_P(C)$-*length* of $\mathcal{O}_P(C)/\mathcal{C}$ which is the largest length p of sequences of $\mathcal{O}_P(C)$ modules, where $\mathcal{C} = I_0 \subset \cdots \subset I_p = \mathcal{O}_P(C)$. This number is denoted by $\delta(P)$ and is actually the dimension $dim_{\mathbf{k}}\mathcal{O}_P(C)/\mathcal{C} = dim_{\mathbf{k}}\overline{\mathcal{O}_P(C)}/\mathcal{O}_P(C)$. The second method, is the $\mathcal{O}_P(C)$-length of $\overline{\mathcal{O}_P(C)}/\mathcal{C}$. This number is denoted by $\delta^*(P)$ and is the dimension $dim_{\mathbf{k}}\overline{\mathcal{O}_P(C)}/\mathcal{C}$.

iv. Since the inclusions $\overline{\mathcal{O}_P(C)} \supset \mathcal{O}_P(C) \supset \mathcal{C}$ hold, we can conclude the *Dedekind's conductor theorem* which states the relation between the numbers $\delta^*(P)$ and $\delta(P)$ i.e., $\delta^*(P) = 2\delta(P)$ (Gorenstein [27]).

v. The genus of the curve is given by Plucker's formula [27], i.e., $g(C) = 1/2(d-1)(d-2) - \sum \delta(P)$ where d is the degree of the curve C and the sum is taken over all the singular points of the curve.

The conductor $\mathcal{C}$ determines a divisor associated with the rational function g called *adjoint divisor.* The above construction leads to the first definition of the adjoint divisor of the curve C at the point P. For the notation invlolved, we also refer the reader to section 2.2.

Definition 3.2 *The adjoint divisor $\mathcal{E}_P$ of the curve C at the point P is the sum $\sum_{i=1}^{n} \alpha_i Q_i$, where the integers $\alpha_i = min\{\text{ord}_{Q_i} j,\ j \in \mathcal{C}\}$. The points $\{Q_i\}_{i=1}^{n}$ are of degree d_i and belong in the set $\tilde{\pi}^{-1}(P)$. The adjoint divisor $\mathcal{E}$ of the curve C is the sum $\sum \mathcal{E}_P$ where the sum is taken over all the singular points of C.*

Note that $\mathcal{E}_P$ and $\mathcal{E}$ are divisors in the set of divisors of the normalization of C. The degree of $\mathcal{E}_P$ is the sum $\sum_{i=1}^{n} d_i\alpha_i$. If the degree d_i is one for all the points Q_i then the degree of $\mathcal{E}_P$ is $\delta^*(P) = \delta(P)/2$.

The second definition has been implied by Gorenstein ([27], pg.434) and has been stated explicitly by Arbarello ([6], appendix A) for the algebraically closed field case. Kodaira [40] and Samuel [56] share the same description. We reconsider the definition when the field of constants is a finite field.

Definition 3.3 *The adjoint divisor Δ_P is the sum $\sum -\mathrm{ord}_Q\omega\, Q$ where the sum is taken over all the points $Q \in \tilde{\pi}^{-1}(P)$ of degree $d(Q)$ and the first kind differential ω is defined as $\omega = \tilde{\pi}^*(dx/\partial f/\partial y) \in \Omega(\tilde{C})$. The adjoint divisor of the curve C is $\Delta = \sum \Delta_P$ where the sum is taken over all the singular points of the curve C.*

The third description of the adjoint divisor is given in terms of the Brill- Noether tower described in section 2.2 of this thesis. Let us recall some notation from section 2.2 : The number of points needed to be blown up in order to construct the Brill-Noether tower is denoted by N . The intersection divisor $\pi_i'^*(E_i) \bullet \tilde{C}$ is attained by intersecting the normalized curve $\tilde{C}$ with $\pi_i'^*(E_i)$, which is the image of the exceptional line E_i of the i-th blowing in the normalized surface .

Definition 3.4 *The adjoint divisor at the point P is defined by $\tilde{\Delta}_P = \sum_{i=1}^{N}(r_i - 1)\pi_i'^*(E_i) \bullet \tilde{C}$. The integers r_i indicate the multiplicities $m_{P_i}(C_{i-1})$ of the successive curves C_{i-1} at the points P_i which are the points lying above the point P. The adjoint divisor of C is $\tilde{\Delta} = \sum \Delta_P$ where the sum is taken over all the singular points of the curve C.*

From the definition of the intersection divisor we conclude that if we calculate the order $\mathrm{ord}_{Q_j}\pi_i'^*(E_i)$ we can find the adjoint divisor using the fourth definition.
We proceed with an algorithmic construction which estimates the integer $\mathrm{ord}_{Q_j}\pi_i'^*(E_i)$.

Algorithm AD * Adjoint Divisor *
Input: A curve C of degree n defined over the finite field $\mathbf{k} = \mathbf{F}_q$ where $q = p^b$. The rational singular points of the curve, the singularity trees, the exceptional lines after each blowing up, the images of the exceptional lines $\pi_i'^*(E_i)$ in the normalized curve .
Output: The order $\mathrm{ord}_{Q_j}\pi_i'^*(E_i)$ of the images of the exceptional lines from the i-th blowing at the points Q_j in the normalized surface.
Method:

Step 1: Let P be one of the singular points of the curve and P_i be its infinitely near points. Let $f(x,y) = 0$ be the local equation of the nonsingular model of the curve. Calculate the orders $ord_{Q_j}\pi_i'^*(E_i)$.

i Find the partial derivatives of the polynomial $f(x,y)$ with respect to both local coordinates x and y. Let P_k be one of the points in the normalized curve lying above the point P where $x(P_k) = y(P_k) = 0$. Since P_k is a

simple point we conclude that one of the partial derivatives evaluated at P_k is non zero, e.g. $\partial f/\partial x(P_k) \neq 0$. Thus y is the local uniformizing parameter around P_k. This implies that the order of y at P_k is one, i.e., $\text{ord}_{P_k} y = 1$.

ii Expand the polynomial $f(x, y)$ with respect to the local coordinate x. The first non zero coefficient is the order of the function x i.e., $\text{ord}_{P_k} x$. Since $\pi_i'^*(E_i)$ is a function with respect to x and y we can calculate its order, $\text{ord}_{P_k} \pi_i'^*(E_i)$.

Step 2: Repeat the first step for every singular point of the curve.

Lemma 3.1 *The time complexity of the algorithm AD is polynomial in the degree of the curve.*

Proof. The proof of the lemma is straight forward. The following argument actually yields an effective estimate considering the Rationality assumption.
Let $C(i)$ denote the time complexity of the i-th step.

The time to compute each partial derivative of $f(x, y)$ requires $O(n^2 \log^2 q)$ bit operations. (same as step 2 in lemma 2.1). Each evaluation of the partial derivatives at the $O(q^2)$ infinitely near points requires $O(n^3 \log^3 q)$ operations. Hence the time complexity of step 1i is $C(1_i) = O(q^2 n^3 \log^3 q)$. The power series expansion of the polynomial $f(x, y)$ with respect to x requires $O(n^4 b^2(\log p + 1))$ bit operations (Manin, Vladut [69]) which can be replaced by $O(n^4 \log^2 q)$. Thus $C(1_{ii}) = O(n^4 \log^2 q)$. Therefore the total time complexity of the first step is $C(1) = O(q^2 n^4 \log^3 q)$.

We repeat the first step for the $O(q^2)$ singular points of C thus the time complexity of the algorithm AD is

$$O(q^4 n^4 \log^3 q)$$

□

The last definition appears in Fulton [21] and applies to curves defined over *algebraically closed fields* (of characteristic zero) having only ordinary singularities.

Definition 3.5 *The adjoint divisor at the ordinary singular point P of multiplicity r is*

$$E'_P = \sum_{i=1}^{r} (r-1) Q_i$$

where $\pi^{-1}(P) = \{Q_i\}_{i=1}^{r}$.

Remark. If the curve is defined over a finite field and has only an ordinary (rational) singular point of multiplicity r then the adjoint divisor at the point P is $E'_P = \sum (r-1) Q_i$ where the sum is taken over the points $Q_i \in \pi^{-1}(P)$ of degree $d(Q_i)$. Note that in this case, the cardinality of the set $\pi^{-1}(P)$ is less or equal to r.

The main goal of the next theorem is to show that the above definitions are equivalent to each other. We refer the reader to section 2.2 for the notation involved in the proof of the next theorem.

Theorem 3.1 *Let C be a curve defined over the finite field* k *with the local affine equation $f(x,y) = 0$ around its singular point P. The adjoint divisor of the curve at the point P and the adjoint divisor of the curve C are given by the following four equivalent definitions:*

1. *The adjoint divisor at the point P is $\mathcal{E}_P = \sum \alpha_i Q_i$ where $\alpha_i = \min\{\mathrm{ord}_{Q_i} j : j \in C\}$ and the sum is taken over all the points $Q_i \in \pi^{-1}(P)$ of degree $d(Q_i)$. The adjoint divisor of the curve is $\mathcal{E} = \sum \mathcal{E}_P$ where the sum is taken over all the singular points of the curve.*
2. *The adjoint divisor at the point P is $\Delta_P = \sum -\mathrm{ord}_{Q_i}\omega\, Q_i$ where $\omega = \frac{dx}{\frac{\partial f}{\partial y}} \in \Omega(C)$. The adjoint divisor of the curve is $\Delta = \sum \Delta_P$ where the sum is taken over all the singular points of C.*
3. *The adjoint divisor at the point P is $\tilde{\Delta}_P = \sum (r_i - 1)\pi_i'^{*}(E_i) \bullet \tilde{C}$ where $i = 1, ..., N$ and the integers r_i are the multiplicities of the successive curves C_{i-1} at the points Q_i. The adjoint divisor of the curve is $\tilde{\Delta} = \sum \tilde{\Delta}_P$.*
4. *If C is a curve defined over an algebraically closed field with only ordinary multiple points then the adjoint divisor at the ordinary multiple point P of multiplicity r is $E'_P = \sum_{i=1}^{r}(r-1)Q_i$. The adjoint divisor of the curve is $E' = \sum E'_P$.*

Proof.
We first show that the second definition is equivalent to the third.

Let N indicate the number of points blown up in order to form the Brill-Noether tower. We will show that $\Delta_P = \tilde{\Delta}_P$ using induction on N.

- Let $N = 0$ i.e., the curve is nonsingular then the adjoint divisor at the point P is zero, i.e., $\Delta_P = \tilde{\Delta}_P = 0$.
- Assume that $\Delta_P(C_1) = \tilde{\Delta}_P(C_1)$ for $N - 1$.
- We need to show that $\Delta_P(C_0) = \tilde{\Delta}_P(C_0)$ is true.

From definition, $\tilde{\Delta}_P(C_0) = \sum_{i=1}^{N}(r_i - 1)\tilde{E}_i$ where $\tilde{E}_i$ is the intersection divisor $\pi_i'^{*}(E_i) \bullet \tilde{C}$. The adjoint divisor can be rewritten as the sum $(r_1 - 1)\tilde{E}_1 + \sum_{i=2}^{N}(r_i - 1)\tilde{E}_i$. But $\sum_{i=2}^{N}(r_i - 1)\tilde{E}_i = \tilde{\Delta}_P(C_1)$ therefore the $\tilde{\Delta}_P(C_0) - \tilde{\Delta}_P(C_1) = (r_1 - 1)\tilde{E}_1$.

It is enough to show that $\Delta_P(C_0) - \Delta_P(C_1) = (r_1 - 1)\tilde{E}_1$. Consider the birational morphism $\tilde{\pi} = \tilde{\pi}_N \circ \cdots \circ \tilde{\pi}_1 : \tilde{C}_N \longrightarrow C_0$ from the normalized curve to the original curve.

The $\tilde{\pi}$ induces the morphism $\tilde{\pi}'_1$ from the normalized curve to the curve C_1. The curve C_1 is attained after the first blow up of the original curve, i.e., from the morphism $\tilde{\pi}'_1 = \tilde{\pi}_N \circ \cdots \circ \tilde{\pi}_2$: $\tilde{C}_N \longrightarrow C_1$. Note that $\tilde{\pi}^{-1}(P) = \tilde{\pi}_1'^{-1}(\{Q_i\})$ where $\{Q_i\} = \tilde{\pi}_1^{-1}(P)$. Suppose $Q \in \{Q_i\}$. Since $\tilde{\pi}_1(Q) = P$ we can conclude that if the affine local coordinates of P are the functions x and y then the local coordinates of Q are x and $z - z(Q) = z - z(a)$ where $z = y/x$. If $f(x,y) = 0$ is the local equation of the curve

C at the singular point P then $g(x, z-a) = 0$ is the local equation of the curve lying above the original curve C_1 at Q.
The polynomial g is attained as follows: The composition $f \circ \tilde{\pi}_1$ yields the polynomial $f(x, xz)$ which can be factored as $x^{r_1}(f(1,z) + xf(1,z) + \cdots + x^m f(1,z))$. Let $g = (1,z) + xf(1,z) + \cdots + x^m f(1,z)$ thus $f(x, xz) = x^{r_1} g$. The partial derivative $\partial f(x,z)/\partial z = x^{r_1}\partial g/\partial z$. We rewrite $\partial f/\partial z$ as the product $\frac{\partial f}{\partial y}\frac{\partial y}{\partial z}$. Since $\partial y/\partial z = x$ we conclude that $\partial f/\partial y = x^{r_1-1}\partial g/\partial z$.

Therefore we establish the differential $\omega_0 = \frac{dx}{\frac{\partial f}{\partial y}} = 1/x^{r_1-1}\frac{dx}{\frac{\partial g}{\partial z}}$ i.e., $\omega_0 = 1/x^{r_1-1}\omega_1$, i.e., $(\omega_0) = -(r_1)(x) + (\omega_1)$. Consequently the difference $(\omega_0) - (\omega_1) = -(r_1 - 1)(x)$ from where we can conclude the relation on the orders of the differentials at the points, i.e., $\mathrm{ord}_{Q_i}\omega_0 - \mathrm{ord}_{Q_i}\omega_1 = -(r_1 - 1)\mathrm{ord}_{Q_i}x$.

The adjoint divisors at the point P evaluated at Q_i satisfy the equation $\Delta_P(C_0)\mid_{Q_i} - \Delta_P(C_1)\mid_{Q_i} = -\mathrm{ord}_{Q_i}\omega_0 + \mathrm{ord}_{Q_i}\omega_1$. The last sum equals $(r_1 - 1)\mathrm{ord}_{Q_i}x$.
The same holds for every point, Q_i therefore we proved the desired equation, i.e., $\Delta_P(C_0) - \Delta_P(C_1) = (r_1 - 1)\tilde{E}_1$. The equivalence of Δ and Δ' is obvious.

(Another way to prove the above equation is by using the definitions of the maps involved in constructing the Brill-Noether tower (sec 2.2).
The difference $\Delta_P(C_0) - \Delta_P(C_1)$ equals

$$\sum -\mathrm{ord}_{Q_i}\tilde{\pi}^*(dx/\partial f/\partial y)Q_i - \sum -\mathrm{ord}_{Q_i}\tilde{\pi}_1'^*(dx/\partial g/\partial z)Q_i)$$

where the sums are taken over all the points $Q_i \in \tilde{C}$; thus $\Delta_P(C_0) - \Delta_P(C_1)$ is

$$\sum [-\mathrm{ord}_{Q_i}\tilde{\pi}^*(dx/\partial f/\partial y) + \mathrm{ord}_{Q_i}\tilde{\pi}_1^*(dx/\partial g/\partial z)]\, Q_i$$

The map $\tilde{\pi}^* = \tilde{\pi}_1'^* \circ \tilde{\pi}_1$ hence $\Delta_P(C_0) - \Delta_P(C_1)$ equals $\sum[-\mathrm{ord}_{Q_i}(\tilde{\pi}_1'^* \circ \tilde{\pi}_1^*)(dx) + \mathrm{ord}_{Q_i}(\tilde{\pi}_1'^* \circ \tilde{\pi}_1^*)(\partial f/\partial y) + \mathrm{ord}_{Q_i}\tilde{\pi}_1'^*(dx) - \mathrm{ord}_{Q_i}\tilde{\pi}_1^*(\partial g/\partial z)]Q_i$ which is $\sum(r_1 - 1)\mathrm{ord}_{Q_i}\tilde{\pi}_1'^*(x)Q_i$.

Therefore $\Delta_P(C_0) - \Delta_P(C_1) = (r_1 - 1)\tilde{\pi}_1'^*(E_1) \bullet \tilde{C}$.

Now we will show that the first definition is equivalent to the second.

Let $\mathcal{C}$ be the divisor identified by the conductor $\mathcal{C}on(\overline{R}, R)$. The different $\mathcal{D}_{L/K}$ is another divisor in the normalization of the curve denoted by $\mathcal{D}$. The order of $\mathcal{C}$ at Q_i satisfies the equation $-\mathrm{ord}_{Q_i}\mathcal{C} = -[-\mathrm{ord}_{Q_i}\mathcal{D} + \mathrm{ord}_{Q_i}\mathcal{C} + \mathrm{ord}_{Q_i}\mathcal{D}]$. Recall Hecke's identity ([31], pg. 145) $(\partial f/\partial x) = \mathcal{C}\mathcal{D}$ which implies that $-\mathrm{ord}_{Q_i}\mathcal{C} = -[-\mathrm{ord}_{Q_i}(dx) + \mathrm{ord}_{Q_i}(\mathcal{C}\mathcal{D})$. Thus, $-\mathrm{ord}_{Q_i}\mathcal{C} = \mathrm{ord}_{Q_i}\frac{dx}{\frac{\partial f}{\partial y}}$ which yields the order of the differential $\mathrm{ord}_{Q_i}\omega$ where $\omega = \frac{dx}{\frac{\partial f}{\partial y}}$; thus $-\mathrm{ord}_{Q_i}\mathcal{C} = \mathrm{ord}_{Q_i}\omega$. From definition $\mathrm{ord}_{Q_i}\mathcal{C} = \alpha_i$ therefore $\mathrm{ord}_{Q_i}\omega = \alpha_i$. We conclude that the adjoint divisors $\mathcal{E}$ and Δ are equivalent. Consequenly, $\Delta_P = \mathcal{E}_P$.

It remains to show that the third definition is equivalent to the fourth. The third definition states that $\Delta_P = \sum(r_i - 1)\pi_i'^*(E_i) \bullet \tilde{C}$. Let us find the nonsingular model of

the curve C around its ordinary singular point P of multiplicity r. We only need one blowing up since P is an ordinary multiple point. Thus the adjoint divisor becomes $\sum(r-1)\text{ord}_{Q_i}(E_1)Q_i$ where the sum is taken over all the points $Q_i \in \pi^*(P)$ of degree $d(Q_i)$. Since the field of constants is algebraically closed, all the points of the $\tilde{C}$ are of degree one, i.e., $d(Q_i) = 1$ and the cardinality of the set $\pi^*(P)$ is exactly r and $\text{ord}_{Q_i}(E_1) = 1$ (Fulton [21], pg. 165). Therefore the adjoint divisor at P becomes $\sum_{i=1}^{r}(r-1)Q_i$.
□

In the following examples we calculate the adjoint divisor of the given curves using the previous definitions.

Example 3.1 Consider the plane curve C described by the homogeneous equation $F = Y^2Z^3 + YZ^4 + X^5 = 0$ over the finite field $\mathbf{k} = \mathbf{F}_{2^4}$.

The point, $P_1 = [0,1,0]$ is a non-ordinary singular point of multiplicity $m_{P_1}(C) = 3$. The local coordinates of the point P_1 in some affine neighborhood of the plane are given by the functions s and t. The local equation of the curve is $t^3 + t^4 + s^5 = 0$. The tangent of C at P_1 is given by the equation $t = 0$.
We first have to resolve the singularity.

1st blowing up of the point P_1.
The birational curve C_1 which lies above the original curve C is described by the local equation $t'^3 + st'^4 + s^2 = 0$. The exceptional line E_1 has local equation $s = 0$. The point lying over P_1 is $P_2 = (0,0)$ of multiplicity $m_{P_2}(C_1) = 2 = r_2$. If we consider the curve as a divisor then $\tilde{\pi}_1(C) = C_1 + 3E_1$.

2nd blowing up of the point P_2.
The birational curve C_2 which lies above C_1 is described by the local equation $(s')^2 + t' + (t')^3s' = 0$. The exceptional line is $E_2 : t' = 0$. The point lying over P_2 is $P_3 = (0,0)$ of multiplicity $m_{P_3}(C_2) = 1 = r_3$. If we consider the curve as a divisor then $\tilde{\pi}_2(C_1) = C_2 + 2E_2$.

Note that the curve C_2 is the local non-singular model $\tilde{C}$ of C. We will now calculate the adjoint divisor utilizing definitions 3.3 and 3.5.

Using **def. 3.3** we can calculate the adjoint divisor of C as follows. The differential $\omega = \pi^*(dt/\partial f/\partial s)$ which can be rewritten as $d(\pi^*t)/\pi^*(\partial f/\partial s)$. Finally if we consider the successive affine quadratic transformations during the blowing up process we attain that $\omega = ds'/s'^4t'^2$, thus $\text{ord}_{P_3}\omega = \text{ord}_{P_3}(ds') - \text{ord}_{P_3}(t')^2 = -8$. The adjoint divisor at the point P_1 is $\Delta_{P_1} = -\text{ord}_{P_3}\omega P_3 = 8P_3$. Since the point P_1 is the only singular point of the curve we conclude that $\Delta = \Delta_{P_1}$.

Using **def. 3.4** we have that the adjoint divisor at the point P_1 is the sum $\tilde{\Delta}_{P_1} = \sum_{i=1}^{2}(r_i - 1)\tilde{E}_i$ i.e., $\tilde{\Delta}_{P_1} = 2\tilde{E}_1 + \tilde{E}_2$. By definition $\tilde{E}_1 = \pi_1'^*(E_1) \bullet \tilde{C}$ and $\tilde{E}_2 = E_2' \bullet \tilde{C}$ but $\pi_1'^*(E_1) \bullet \tilde{C} = E_1' \bullet \tilde{C} + E_2' \bullet \tilde{C}$ therefore $\tilde{\Delta}_{P_1} = 2(E_1' \bullet \tilde{C}) + E_2' \bullet \tilde{C}$.

Let us now estimate the intersection divisor $E_2' \bullet \tilde{C}$. The local equation of $\tilde{C}$ is given by $(s')^2 + t' + (t')^3s' = 0$. The partial derivative $\partial f/\partial t$ evaluated at the point P_3 is not zero. Therefore we conclude that the local uniformizing parameter around P_3 is the function s' and consequently $\text{ord}_{P_3}s' = 1$. The local equation of the

curve C yields that the coordinate t' can be rewritten as $t' = (t')^3 s' + (s')^2$. The last equation implies that the order, $\mathrm{ord}_{P_3} t' = \mathrm{ord}_{P_3}[(t')^3 s' + (s')^2]$. Since $t'(P_3) = 0$ we conclude that the function t' belongs in the local ring of the curve C_2 at the point P_3. Thus the order $\mathrm{ord}_{P_3} t' \geq 0$ actually $\mathrm{ord}_{P_3} t' > 0$ since t' is not a constant. Therefore $\mathrm{ord}_{P_3} t'^3 s' \geq 3 + 1 = 4$ and $\mathrm{ord}_{P_3} t' = \mathrm{ord}_{P_3}[s'^2] = 2$. Thus the intersection divisor $E_2' \bullet \tilde{C} = \sum I(P_i(E_2' \cap \tilde{C})P_i$ where the sum is taken over all the points P_i in the intersection $E_2' \cap \tilde{C}$ becomes $E_2' \bullet \tilde{C} = \mathrm{ord}_{P_3} t' P_3 = 2P_3$. The intersection divisor $E_1' \bullet \tilde{C} = \mathrm{ord}_{P_3} s' P_3 = 1P_3$. The representation of the exceptional line E_1 in the normalized surface S_2 is given by the local equation $s' = 0$. Thus we conclude that the adjoint divisor of the curve at the point P_1 is $\tilde{\Delta}_{P_1} = 2E_1' \bullet \tilde{C} + 3E_2' \bullet \tilde{C} = 2(1P_3) + 3(2P_3) = 8P_3$. Since P_1 is the only singular point we conclude that $\tilde{\Delta} = \tilde{\Delta}_{P_1} = 8P_3$.

Therefore we conclude that the adjoint divisor of the curve is $8P_3$ and we note the error which appears in Le Brigand and Risler's paper [43] where this example was originally discussed.

Example 3.2 We consider example 2.3 where C is a plane curve described by the homogeneous form $F = Y^5 Z^4 - X^9 - XZ^8$ over the finite field $\mathbf{k} = \mathbf{F}_8$.

The points $P_1 = [0, 0, 1]$ of multiplicity $m_{P_1}(C) = 5$ and $P_2 = [0, 1, 0]$ with multiplicity $m_{P_2}(C) = 4$ are non-ordinary singular points.

Consulting the notation and the normalization process described in the second chapter we find the adjoint divisor $\tilde{\Delta}$ of the curve using the **def. 3.4** .

The adjoint divisor of C at the singular point P_1 is $\tilde{\Delta}_{P_1} = \sum_{i=1}^{3}(r_i - 1)\tilde{E}_i$. Recall that $\tilde{E}_i = \pi_1'^*(E_i) \bullet \tilde{C}$ where $\pi_1'^*(E_1) = E_1'' + E_2' + 2E_3'$, $\pi_2'^*(E_2) = E_2' + E_3$ and $\pi_3'^*(E_3) = E_3'$. Therefore the adjoint divisor is $\tilde{\Delta} = 4E_1'' \bullet \tilde{C} + 6E_2' \bullet \tilde{C} + 11E_3' \bullet \tilde{C}$.

The intersection divisor $E_1'' \bullet \tilde{C} = \sum \mathrm{ord}_{P_i} 0$ where the sum is taken over the points P_i in the intersection $E_1'' \cap \tilde{C} = \emptyset$, therefore $E_1'' \bullet \tilde{C} = 0$.

The intersection divisor $E_2' \bullet \tilde{C} = \sum \mathrm{ord}_{P_i} y_1 P_i$ where the sum is taken over the points, P_i in the intersection $E_1' \cap \tilde{C} = P_{13}$. Therefore the intersection divisor is $E_2' \bullet \tilde{C} = \mathrm{ord}_{P_{13}} y_1 P_{13} = 1P_{13}$.

Finally the intersection divisor $E_3' \bullet \tilde{C} = \sum \mathrm{ord}_{P_i} z_1 P_i$ where the sum is taken over the points $P_i \in E \cap \tilde{C} = P_{13}$. Therefore the intersection divisor $E_3' \bullet \tilde{C} = \mathrm{ord}_{P_{13}} z_1 P_{13} = 2P_{13}$.

Thus the adjoint divisor at the point P_1 is $\tilde{\Delta}_{P_1} = 28P_{13}$. Similarly $\tilde{\Delta}_{P_2} = \sum_{i=1}^{2}(r_i - 1)\tilde{E}_i$. Note that $\tilde{E}_i = \pi_1'^*(E_i) \bullet \tilde{C}$ where $\pi_1'^*(E_1) = E_1' + E_2' = \pi_2'^*(E_2) = E_2'$. Therefore the adjoint divisor at the singular point P_2 can be written as: $\tilde{\Delta}_{P_2} = 3E_1' \bullet \tilde{C} + 6E_2' \bullet \tilde{C}$.

The intersection divisor $E_1' \bullet \tilde{C} = \sum \mathrm{ord}_{P_i} u' P_i$ where the sum is taken over the points P_i in the intersection $E_1' \cap \tilde{C}$ which is empty.

The last intersection divisor is $E_2' \bullet \tilde{C} = \mathrm{ord}_{P_4} u P_4 = 4P_4$. Hence the adjoint divisor at the point P_2 is $\tilde{\Delta}_{P_2} = 24P_4$. Since $\tilde{\Delta} = \tilde{\Delta}_{P_1} + \tilde{\Delta}_{P_2}$ we conclude that the adjoint divisor of the curve is $\tilde{\Delta} = 28P_{13} + 24P_4$.

Another way to calculate the adjoint divisor of the curve is by using the **def. 3.3.** Recall that the affine equation of the curve around the singular point, P_1 is described by the polynomial $f(y,z') = y^5(z')^4 + y^5 - (z')^8$. The differential $\omega = \phi^*(dz'/\partial f/\partial y)$ is the quotient $\phi^*(dz')/\phi^*(y^4z^4 + y^4)$. Considering the successive affine quadratic transformations during the normalization process we can rewrite the last quotient as $dy_1/z_1^{18}y_1^{12} + z_1^{10}y_1^8$.

Thus the order of the differential ω at the point P_{13} is $\mathrm{ord}_{P_{13}}\omega = -\min(\mathrm{ord}_{P_{13}}z_1^{18}y_1^{12}, \mathrm{ord}_{P_{13}}z_1^{10}y_1^8) = 28$.

Therefore the adjoint divisor at the point P_{13} is $\Delta_{P_1} = 28P_{13}$. Recall that the affine equation of the curve around the singular point P_2 is described by the polynomial $f(u,v) = v^4 - u^9 - uv^8$. The differential $\omega = d\phi^*(v)/\phi^*(u^8 + v^8)$ i.e., $\omega = d(u^2v')/dv'/u^6(1 + u^8v'^8)$. So we conclude that $\mathrm{ord}_{P_4}\omega = \mathrm{ord}_{P_4}dv' - \mathrm{ord}_{P_4}u^6(1 + u^8v'^8) = -24$. The adjoint divisor of the curve C at the singular point P_2 is $\Delta_{P_2} = 24P_4$. The adjoint divisor of C is $\Delta = 28P_{13} + 24P_4$.

The next example illustrates how we can find the adjoint divisor of a singular curve whose singularities have been resolved using the integral basis algorithm described in this thesis (sec. 2.4).

Example 3.3 Recall examples 2.7 and 2.8 which appear in the second chapter of this thesis. The curve C is given by the homogeneous equation $X^2Z^2 + XYZ^2 + Y^4 = 0$ over the finite field $\mathbf{k} = \mathbf{F}_2$.

The curve C has on ordinary double point $P = [0,0,1]$.

The affine coordinate ring of the curve C is $R_0 = \mathbf{k}[x,y]/(f)$ where $f = x^2 + xy + y^4$ is the affine representation of C around its singular point P. It is a free $\mathbf{k}[x]$-module with basis $\{1, y, y^2, y^3\}$.

The integral closure of R_0 in the field of rational functions $\mathbf{k}(x,y)$ is a free $\mathbf{k}[x]$-module with basis $\{1, y, y^2, y^3/x\}$.

The nonsingular model of the curve C is the variety $\{a \in \overline{\mathbf{k}}^4 \colon f_{ij}(a) = 0\}$ where the polynomials f_{ij} are defined as follows,

$$\begin{aligned} f_{11} &= Y_1^2 - Y_2 \\ f_{12} &= Y_1Y_2 - xY_3 \\ f_{13} &= Y_1Y_3 - (x + Y_1) \\ f_{22} &= Y_2^2 - x^2 - xY_1 \\ f_{23} &= Y_2Y_3 - Y_2 - xY_1 \\ f_{33} &= Y_3^2 - Y^2 - Y_3 \end{aligned}$$

The points lying above P are $P_1 = (0,0,0,0)$ and $P_2 = (0,0,0,1)$ and they are simple points.

We calculate the matrix $(\partial f_{ij}/\partial Y_i)$ where the index $0 \leq i \leq 3$. We evaluate the matrix at the points P_1 and P_2. We note that $\partial f_{ij}/\partial Y_1(P_1) = 0$ from where we conclude that the local uniformizing parameter around P_1 is Y_1. Therefore the order of Y_1 at the point P_1 is $\text{ord}_{P_1} Y_1 = 1$. Similarly, since the partial derivative $\partial f_{ij}/\partial Y_1(P_2) = 0$ we conclude that the local uniformizing parameter around P_2 is Y_1 and therefore $\text{ord}_{P_2} Y_1 = 1$.

In order to find the orders of the functions x, Y_2 and Y_3 at the points P_1 and P_2 we will proceed as follows:
First, we express the functions x, Y_2 and Y_3 in terms of the local uniformizing parameter Y_1. Indeed $Y_2 = Y_1^2$, $Y_3 = Y_3^2 - Y_2$ and $x = Y_1Y_3 - Y_1$. Next we estimate the orders of the functions x, Y_2 and Y_3. From the previous equations we see that $\text{ord}_{P_1} Y_2 = 2$, $\text{ord}_{P_2} Y_2 = 2$, $\text{ord}_{P_1} Y_3 = 2$ and $\text{ord}_{P_2} Y_3 = 2$. Also the function x can be rewritten as $x = Y_1Y_3^2 - Y_1Y_2 - Y_1 = -Y_1 +$ terms of order ≥ 3. Therefore, $\text{ord}_{P_1} x = 1$ and $\text{ord}_{P_2} x = 1$.

Using definition 3.3 we calculate the adjoint divisor Δ of the curve C . Consider the differential $\omega = \pi^*(\frac{dx}{df/dy}) = dx/x$. Thus the order of the differential at the point P_1 is $\text{ord}_{P_1}\omega$ i.e., is the difference $\text{ord}_{P_1} dx - \text{ord}_{P_1} x = 0 - 1 = -1$. The order of the differential at the point P_2 is $\text{ord}_{P_2}\omega = \text{ord}_{P_2} dx - \text{ord}_{P_2} x = 0 - 1 = -1$. Therefore the adjoint divisor of C is $\Delta = \sum_{P_i \in \pi^{-1}(P)} -\text{ord}_{P_i}\omega P_i = P_1 + P_2$.

3.2 Adjoint Curve

After we discussed the adjoint divisor of a curve we can define the *adjoint curve.* For further reference on this topic we suggest Gorenstein [27] for the nonalgebraically closed field case, Hartshorne [30] and Fulton [21] for the algebraically closed field case. We use the notation of the second chapter of this thesis.

We start with an absolutely irreducible, singular, plane curve C defined over a finite field $\mathbf{k}$.

Definition 3.6 *Let C' be a plane projective curve which does not have C as a component. If the divisor cut by C' is greater or equal to the adjoint divisor of C then C' is called an adjoint curve of C.*

Remark. In the following an adjoint curve of C will be denoted by C_a.

There are three equivalent conditions for the curve C_a to be an adjoint curve of C. They are described in the next theorem. The first condition is motivated by Fulton [21]; the next, appears in Le Brigand [43]; the last condition is motivated by Abhyankar [2].

Theorem 3.2 *Let C_a be a curve not containing C as a component we then have that C_a is an adjoint curve of C if any of the following conditions hold:*

1. *The curve C has an ordinary singular point P of multiplicity r and $m_P(C_a) \geq (r-1)\text{ord}_{P_i} x$ where $x = 0$ is the local equation of the exceptional line E and $P_i \in \pi^*(P)$.*

2. *The curve C_a goes through every infinitely near point P_i with multiplicity $m_{P_i}(C_a) \geq m_{P_i}(C) - 1$, $1 \leq i \leq N$ where N is the number of points needed to be blown up in order to attain the Brill-Noether tower.*

3. *The curve C_a goes through every singular point P_i of C with multiplicity $m_{P_i}(C) \geq \alpha_{P_i}$ where $\alpha_{P_i} = sup_{1 \geq i \geq N} 1/n_i \sum_{j=1}^{i} m_{ji}(r_j - 1)$. The image of the exceptional lines in the normalized surface is $\pi_i'^{*}(E_i) = (m_{i1}E_1' + \cdots + m_{iN}E_N')$.*

4. *The rational function $g(x,y)$ which is the affine equation of C around a point P belongs in the conductor $\mathcal{C}$.*

Proof.
We start with the proof of the first statement of the theorem. The next two claims are needed for the proof.

Claim 3.1 *Suppose P is an ordinary multiple point of multiplicity r. The image of the point P under the morphism π is $\pi^{-1}(P) = \{P_i\}_{i=1}^{s}$, $s \leq r$ where P_i are the points lying above P. Let C_a be a plane curve with image g in the coordinate ring of the curve C then* $\mathrm{ord}_{P_i}^{\tilde{C}}(g) \geq m_P(C_a)$.

Proof. The intersection multiplicity $I(P, C \cap C_a) = \sum \mathrm{ord}_{P_i} g$ where the sum is taken over all the points P_i of degree $d(P_i)$ which belongs in the set $\pi^{-1}(P)$. Since P is an ordinary multiple point, the cardinality of the set $\{P_i\colon \pi(P_i) = P\}$ is at most r. Then the intersection multiplicity $I(P, C \cap C_a) \leq r\,\mathrm{ord}_{P_i} g$; on the other hand $I(P, C \cap C_a) \geq r m_P(C_a)$. Equality holds if the curves C_a and C have distinct tangents at P (Fulton [21]). Therefore the desired inequality $\mathrm{ord}_{P_i}^{\tilde{C}}(g) \geq m_P(C_a)$ becomes obvious. □

Claim 3.2 *With notation as above , we have that $m_P(C_a) \geq s$ if and only if* $\mathrm{ord}_{P_i} g \geq s$ *where s is some integer .*

The proof of the claim becomes obvious since it is an exact application of claim 3.1.

We now go back to the proof of the first statement of theorem 3.2 . The curve C_a : $g = 0$ is an adjoint of C implies that the divisor associated by C_a is greater or equal to the adjoint divisor $\sum(r_i - 1)\tilde{E}_i$ where the sum is taken over all the points $P_i \in \tilde{C}$ of degree $d(P_i)$. Let us assume that the curve C has only one ordinary multiple point of multiplicity r. The adjoint divisor of C is actually the sum $\sum(r-1)\mathrm{ord}_{P_i} x P_i$ where the sum is taken over the points $P_i \in \tilde{C}$ and $x = 0$ is the local equation of the exceptional line E_1 and the divisor associated by C_a is the sum $\sum \mathrm{ord}_{P_i} g\, P_i$. Let us recall that C_a is an adjoint curve, therefore we have the inequality $\mathrm{ord}_{P_i} g \geq (r-1)\mathrm{ord}_{P_i} x$ since the product $(r-1)\mathrm{ord}_{P_i} x = s$ thus the inequality becomes $\mathrm{ord}_{P_i} g \geq s$. From claim 3.2 we conclude that $m_P(C_a) \geq s$ i.e., $m_P(C_a) \geq (r-1)\mathrm{ord}_{P_i} x$. Note that if the field of constants was algebraically closed then $m_P(C_a) \geq (r-1)$ (Fulton [21], pg. 190). □

We continue with the second statement of theorem 3.1 . The proof of the second statement becomes apparent if we recall theorem 3.2.

The third statement of theorem 3.2 is proved by Le Brigand [43].

We finish up the proof of theorem 3.2 by proving the last statement. Let $g = 0$ be an affine equation of the plane curve C_a around the point P of the curve C. The curve C_a is an adjoint curve of C if and only if the divisor (g) associated with the function g is greater or equal to the adjoint divisor. Using definition 3.2, the adjoint divisor is the divisor described by the conductor $\mathcal{C}$ of the curve, therefore $(g) \geq \mathcal{C}$. Thus the function g belongs in the conductor of C i.e., $g \in \mathcal{C}$.

□

The following examples illustrate the procedure of finding adjoint curves using the second statement of theorem 3.2.

Example 3.4 Consider the curve $C : F = Y^2Z^3 + YZ^4 + X^5 = 0$, described in example 3.1, defined over the finite field $\mathbf{k} = \mathbf{F}_{2^4}$.

The singular point of the curve is P_1 of multiplicity $m_{P_1}(C) = 3$.

We first calculate the integer α_{P_1} and then we find adjoint curves of C. The image of the blown-up point in the normalized surface is $\pi'^*(P_1) = \pi_2^*(E_1)$ where $\pi_2^*(E_1) = E_1' + m_{P_1}(E_1)$, i.e., $E_2 = E_1' + E_2'$. Looking at the description of the integer α_{P_1} in the third statement of theorem 3.2, we conclude that $n_1 = n_2 = 1$. Let us recall that $\tilde{E}_1 = \pi_2'^*(E_1) \bullet \tilde{C}$ where $\pi_2'^*(E_1) = E_1' + E_2'$. Therefore since $\pi_2'^*(E_1) \bullet \tilde{C} = (E_1' + E_2') \bullet \tilde{C}$, we can conclude that $m_{11} = m_{12} = 1$. Similarly, we have that $\tilde{E}_2 = E_2' \bullet \tilde{C}$ from where we conclude that $m_{22} = 1$. Returning to the definition of the integer α_{P_1}, which is the sup of the set $\{ 1/n_1 m_{11}(r_1 - 1), \quad 1/n_2[m_{12}(r_1 - 1) + m_{22}(r_2 - 1)] \}$, we conclude that $\alpha_{P_1} = 3$.

We claim that the curve $C_a : Y^2Z^5 = 0$ is an adjoint curve of C since it is going through the singular point P_1, the local equation of C_a around P_1 is $t^5 = 0$ of multiplicity $m_{P_1}(C_a) = m_{P_1}(t^5) = 5 > \alpha_{P_1}$. Note that the curves $G_0 = YZ^5$ and $G_1 = YZ^3$ are also adjoint curves of C since they both go through the singular point P_1 and their multiplicities $m_{P_1}(G_0) = m_{P_1}(t^5) = 5$ and $m_{P_1}(G_1) = m_{P_1}(t^3) = 3$ are greater than the integer α_{P_1}.

Example 3.5 Consider the curve $C : F = Y^5Z^4 - X^9 - XZ^8$, described in example 3.2, defined over the finite field $\mathbf{k} = \mathbf{F}_8$.

Let us first estimate the integer α_{P_1}. The image $\pi^{-1}(P_1)$ of the singular point P_1 in the normalized surface is described as follows:

$$\begin{aligned} \pi^{-1}(P_1) &= (\pi_2 \circ \pi_3)^*(E_1) = \pi_3^*(\pi_2^*(E_1)) \\ &= \pi_3^*(E_1' + E_2) = \pi_3^*(E_1') + \pi_3^*(E_2) \\ &= E_3 + E_1'' + E_3 + E_2' = E_1'' + E_2' + 2E_3' \end{aligned}$$

Returning to the description of the integer α_i we conclude that the coefficients are $n_1 = n_2 = 1$, $n_3 = 2$. Similarly,

$$\begin{aligned} \tilde{E}_1 &= \pi_1'^*(E_1) \bullet \tilde{C} \\ &= \pi_3^*(\pi_2(E_1)) \bullet \tilde{C} \\ &= (E_1'' + E_2' + 2E_3') \bullet \tilde{C} \end{aligned}$$

From the definition of the integer α we estimate the integers $m_{11} = m_{12} = 1$, $m_{13} = 2$. We continue with the divisor $\tilde{E}_2 = \pi_2'^*(E_2) \bullet \tilde{C}$. Since $\pi_2'^*(E_2) = E_2' + E_3$ then $m_{22} = m_{23} = 1$. Finally, the intersection divisor $\tilde{E}_3 = \pi_3'^*(E_3) \bullet \tilde{C}$ is the divisor $E_3' \bullet \tilde{C}$ i.e., $m_{33} = 1$. From the definition of the integer α we conclude that $\alpha_{P_1} = 6$.

We will now compute the integer α_{P_2} similarly. Since $\pi^{-1}(P_2) = \pi_2^*(E_1) = E_1' + E_2'$ therefore we can compute the integers $n_1 = n_2 = 1$. Since $\tilde{E}_2 = E_2' \bullet \tilde{C}$ we estimate the coefficient $m_{22} = 1$; thus $\alpha_{P_2} = 6$. Therefore, the curve C_a associated with the form $G_0 : X^6Y^6 = 0$ is an adjoint curve of C. Note that C_a goes through P_1 with multiplicity $m_{P_1}(C_a) = m_{P_1}(y^6) = 6$ which is greater than the integer α_{P_1}. The curve C_a also goes through the singular point P_2 with multiplicity $m_{P_2}(C_a) = m_{P_2}(u^6) = 6$ greater than α_{P_2}.

3.3 Discriminants of Algebraic Curves

Our results in this section are inspired by Abhyankar's aphorism [2] stated as follows: " The discriminant locus (totality of roots) of a polynomial is the sum of the branch locus and the projection of the singular locus." The polynomial under consideration is an affine representation of a plane smooth curve defined over an algebraically closed field.

Our contribution in this section is to translate the aphorism as a statement on the points which appear in the divisor described by the discriminant of a polynomial. In our case the polynomial is an affine representation of a plane singular absolutely irreducible curve. In contrast to Abhyankar, we assume that the plane curve is defined over a finite field. We compute the discriminant divisor using two methods.

The first method is based on a geometric approach. We view the discriminant divisor as cycle (Fulton [21]).

The second method is based on an algebraic approach. It is defined as the product of two divisors, the branch divisor and the image of the adjoint divisor in the initial curve.

Both methods show that the points which appear in the discriminant divisor are the singular points and the simple different points of the curve. We present examples where we compute the discriminant of absolutely irreducible curves using each method.

Consider the plane curve C and let $f(x, y)$ be its affine representation in some fixed affine neighborhood. We fix the *projection* ρ as $\rho(x, y) = x$ which projects the curve C onto the affine line $\mathbf{A}^1(\mathbf{k})$. The *discriminant* $d_f = \prod g_i^{r_i}$ of the polynomial f is a polynomial in $\mathbf{k}[x]$ where $g_i \in \mathbf{k}[x]$ are irreducible linear factors which correspond to the closed points on the affine line.
With d_f we associate a divisor in $\mathrm{Div}(\mathbf{A}^1)$ given by

$$(d_f)_0 = \sum_i r_i P_i$$

where P_i are the zeros of g_i. Let $\rho^*(d_f)_0$ be the inverse image of $(d_f)_0$ in $\mathbf{A}^2$. We now denote by

$$D_f = C \bullet \rho^*(d_f)_0$$

the intersection of C and $\rho^*(d_f)_0$ considered as a divisor in $\mathrm{Div}(\mathbf{A}^2)$. This will be called the *discriminant divisor of the polynomial* f.

3.3.1 Geometric Approach

With notation as in previous section we compute the discriminant divisor D_f of the plane curve $C : f(x,y) = 0$ using a geometric approach. It is based on the naive view of divisors as *cycles* (Fulton [21]).

Consider an absolutely irreducible plane curve C defined over a finite field $\mathbf{k}$. Let P be a $\mathbf{k}$-rational point on the curve. We fix one of the affine neighborhoods of C which contains the point P. Let $f(x,y) = 0$ be the affine representation of the curve in that affine neighborhood. Let us fix a projection ρ from the affine plane $\mathbf{A}^2(\mathbf{k})$ on the affine line $\mathbf{A}^1(\mathbf{k})$ as $\rho(x,y) = x$.

We want to examine how the points P which appear in the discriminant divisor D_f are related to the curve C. Let us first describe the points on the curve C (Abyankar [2], sec. 43).

Definition 3.7 *If the point P is a singular (res. simple) point on the curve C : $f(x,y) = 0$ and C has a vertical tangent at P then P is called singular (res. simple) different point. The projection of a different point on the x-axis is a branch point.*

Remark. Let us stress the fact that a point is simple or singular independently of the choice of the coordinate patch (affine neighborhood) which contains the point where the different points depend on the direction of the projection ρ and the affine neighborhood.

We will now show that the points which appear in the support of the divisor D_f are the singular points and the simple different points of the curve C: $f(x,y) = 0$.

Notation. By i_R we denote the number of times the point R appears in a given cycle.

Theorem 3.3 *Consider the discriminant divisor D_f. The following equation holds*

$$D_f = \sum_P i_P P + \sum_Q i_Q Q$$

where the first sum is taken over the singular points of C. The second sum runs through the points Q in the set of the simple different points of C. The integer i_P (resp. i_Q) is the number of times the point P (resp. Q) appears in D_f.

Proof. Let us recall that d_f is the resultant of the polynomial f and $\partial f/\partial y$, i.e., the locus (totality of roots) of the discriminant polynomial d_f is the set of common roots of f and $\partial f/\partial y$. A point R is in the set of common roots of f and $\partial f/\partial y$ if and only

if it is either a singular (different or not-different) point or a simple different point. Therefore the locus of the discriminant polynomial d_f is the union of two disjoint sets. The first set contains the projections of the singular points and the other set contains the projections of the simple different points of C. Therefore we can rewrite the discriminant polynomial as the product $d_f = g_P g_Q$ where g_P (resp. g_Q) in $\mathbf{k}[x]$ is the product of those linear factors g_i that vanish at the projections of the singular (resp. the simple different) points of the curve C. Thus the divisor $(d_f)_0$ can be written as the sum of divisors

$$(d_{g_P})_0 + (d_{g_Q})_0$$

Thus D_f can be written as

$$D_f = C \bullet ((d_{g_P})_0 + (d_{g_Q})_0)$$

and can be replaced by

$$D_f = C \bullet (d_{g_P})_0 + C \bullet (d_{g_Q})_0$$

Therefore the equation described in the theorem becomes obvious.
□

Example 3.6 Consider the curve $C : Y^2Z^3 + YZ^4 + X^5 = 0$ defined over the finite field $\mathbf{k} = \mathbf{F}_{16}$.

The point $P_1 = [0,1,0]$ is a non-ordinary point of the curve of multiplicity $m_{P_1}(C) = 3$. The affine equation of the curve around the point P_1 is $f(s,t) = t^3 + t^4 + s^5 = 0$ where the local coordinates are defined as the quotients $s = X/Y$ and $t = Z/Y$. The three non-distinct tangents of the curve C at the singular point P_1 are given by the local equation $t = 0$. Fix the projection from an affine neighborhood of the plane to the affine line $\rho(s,t) = t$. The tangents of C at P_1 are not distinct and vertical given by the equation $t = 0$. Therefore P_1 is a singular different point.

The point $Q_1 = [0,1,1]$ is a simple point since $f(Q_1) = 0$ and $\partial f/\partial t(Q_1) \neq 0$. The unique tangent $t + 1 = 0$ of the curve at Q_1 is vertical. Therefore Q_1 is a simple different point.

The points $t = 1$ and $t = 0$ are branch points since they are the projection of the simple different point Q_1 and the singular different point P_1 on the t-axis.

The discriminant polynomial, $d_f = \mathrm{Res}(f, \partial f/\partial s, s) = t^{12}(1+t)^4$.

The discriminant divisor $D_f = 12(t) + 4(1+t) = 12(5P_1) + 4(5Q_1) = 60P_1 + 20Q_1$.

The following example demonstrates that theorem 3.3 can be applied when the field of constants is of characteristic zero.

Example 3.7 Consider the curve $C : Y^2Z + X^2Z + X^3$ defined over the real numbers.

The point $P = (0,0)$ is a singular double point. The affine representation of C around P is $f(x,y) = y^2 + x^2 + x^3$. Fix the projection from an affine neighborhood of the plane to the affine line $\rho(x,y) = x$. The distinct tangents of C at P are $y = x$ and $y = -x$ and they are not vertical.

The point $P_1 = (-1,0)$ is a simple different point since it has a vertical tangent $x + 1 = 0$.

The point $x = 0$ is the projection of the singular point P on the y-axis and $x = -1$ is a branch point.

The discriminant polynomial is $d_f = \text{Res}(f, \partial f/\partial y, y) = (2x)^2(-x-1)$.

The discriminant divisor is $D_f = 2(2P) + 1(2P_1) = 4P + 2P_1$.

Example 3.8 Consider the plane curve $C : Y^5Z^4 - X^9 - XZ^8 = 0$ over the finite field $\mathbf{k} = \mathbf{F}_8$ (see also ex. 2.3, 3.2).

The point $P_1 = [1,0,1]$ with multiplicity $m_{P_1}(C) = 5$ and the point $P_2 = [0,1,0]$ with multiplicity $m_{P_2}(C) = 4$ are non-ordinary singular points.

The affine representation of the curve C around P_1 is given by the polynomial equation $f_1(y,z) = y^5z^4 + y^5 + z^8$. The five nondistinct tangents of C at P_1 are given by the local equation $y = 0$. Fix the projection from an affine neighborhood of the plane the affine line $\rho(y,z) = z$. Since the tangents are not vertical we conclude that P_1 is just a singular point.

The discriminant polynomial is $D_{f_1} = \text{Res}(f_1, \partial f_1/\partial y, y) = (z^4+1)^4 z^{32}$.

The discriminant divisor $D_{f_1} = 160P_1$.

The affine representation of C around P_2 is given by the polynomial equation $f_2(u,v) = v^4 - u^9 - uv^8$. The four nondistinct tangents of C at P_2 are given by the local equations $v = 0$. Fix the projection from an affine neighborhood of the plane to the affine line $\rho(u,v) = v$. Since the tangents are vertical we conclude that P_2 is a different singular point.

The discriminant polynomial is $D_{f_2} = \text{Res}(f_2, \partial f_2/\partial u, u) = v^{32}$.

The discriminant divisor is $D_{f_2} = 288P_2$.

3.3.2 Algebraic Approach

In this section we view the discriminant divisor algebraically. It is the divisor consisting of: the branch divisor and the image of the adjoint divisor in the initial curve

Let us recall that the *different* (ramification) divisor $\mathcal{D}$ is a divisor in the normalized curve $\tilde{C}$ (Serre [59]). The image of the different divisor under the morphism $\tilde{\pi}_* : \mathrm{Div}\tilde{C} \longrightarrow \mathrm{Div}C$ is the *branch divisor* (δ) i.e., $\tilde{\pi}_*(\mathcal{D}) = (\delta_P)$.

We start with a singular absolutely irreducible plane curve $C : f(x,y) = 0$ over an arbitrary field $\mathbf{k}$. The polynomial $f(x,y) \in \mathbf{k}[x,y]$ is an affine representation of the curve C around one of its singular point P. We find an affine non-singular model $\tilde{C}$ of the curve C by considering the morphism $\tilde{\pi}: \tilde{C} \longrightarrow C$.

Theorem 3.4 *Let $C : f(x,y) = 0$ be an absolutely irreducible singular plane curve defined over the finite field $\mathbf{k}$. The discriminant divisor D_f is related to the adjoint divisor Δ_P and the branch divisor δ_R by the equation*

$$D_f = \sum_P \tilde{\pi}_*(\Delta_P)\delta_P + \sum_R \delta_R$$

where the first sum is taken over the singular points of the curve. The second sum is taken over the simple points of the curve whose images under the morphism $\tilde{\pi}^*$ belong in the different (ramification) divisor.

Proof. Fix a projection ρ from an affine neighborhood of the plane to the affine line. Let us recall the identity $(\partial f/\partial x) = \Delta\mathcal{D}$ (Hecke [31], pg.145) where Δ and $\mathcal{D}$ is the adjoint divisor and the different of the curve respectively.
We translate the identity $(\partial f/\partial x) = \Delta\mathcal{D}$ as an identity on divisors on the normalization $\tilde{C}$.

The image of the divisor $\tilde{\pi}^*(\partial f/\partial x)$ under the morphism $\tilde{\pi}_*$ yields the discriminant divisor D_f. The image of the different divisor $\mathcal{D}$ under the morphism $\tilde{\pi}_*$ yields the branch divisor δ. Recall that the adjoint divisor Δ is the sum of the adjoint divisors Δ_P of the points of the curve C (sec. 3.1). (When the points are simple then the conductor at those points is zero). Similarly the different divisor $\mathcal{D}$ of the curve C is the sum of the different divisors $\mathcal{D}_P$. Therefore the translated identity can be rewritten as

$$D_f = \sum_P \tilde{\pi}_*(\Delta_P)\delta_P + \sum_R \delta_R$$

where the first sum is taken over the singular points of the curve. The second sum is taken over the simple points of the curve whose images under the morphism $\tilde{\pi}^*$ belongs in the different (ramification) divisor .
□

We use notation from section 2.2 in the next example.

Example 3.9 Consider the curve of example 3.1.

Recall that the point P_1 is a singular different point and the affine representation of C around P_1 is the polynomial equation: $t^3 + t^4 + s^5 = 0$. The point Q_1 is a simple different point of the curve and the affine representation of C around Q_1 is the polynomial equation: $\tilde{t} + \tilde{t}^2 + \tilde{t}^3 + \tilde{t}^5 + s^5 = 0$.

From ex.3.6 we recall that $C_2 : f(s',t') = s'^2 + t' + t'^3$ is a local non-singular affine model of C around P_1. The point P_3 is the point lying above P_1.

The local parameter s' is a local uniformizing parameter around the point P_3 i.e., $\text{ord}_{P_3} s' = 1$. It follows that $\text{ord}_{P_3} t' = 2$. Similarly $\text{ord}_{Q_1} \tilde{t} = 5$ and $\text{ord}_{Q_1} s = 1$.

The adjoint divisor of C around P_3 is $\Delta_{P_1} = 8P_3$ (ex. 3.1).

The different (ramification) divisors are $\mathcal{D}_{P_1} = (d\pi^*(t)) = 4P_3$ and $\mathcal{D}_{Q_1} = (d\pi^*(\tilde{t})) = 4Q_1$.

The discriminant divisor is

$$\begin{aligned} D_f &= \delta_{P_1}\pi_*(\Delta_{P_1}) + \delta_{Q_1} \\ &= 8\pi_*(P_3) + 4\pi_*(P_3) + 20Q_1 \\ &= 8f(P_3)P_1 + 4f(P_3)P_1 + 20Q_1 \\ &= 8 \times 5P_1 + 4 \times 5P_1 + 20Q_1 \\ &= 60P_1 + 20Q_1 \end{aligned}$$

The discriminant divisor is the same as in example 3.6.

Example 3.10 We use the curve of example 3.7.

Recall that P_1 is a simple different point where P is a double singular point.

We desingularize C by blowing it up around its singular point P.
The blown up curve C_1 is given by the affine equation $f_1(x,\tilde{y}) = \tilde{y}^2 - 1 - x = 0$. The points lying above the point P are the points $P' = (0,1)$ and $P'' = (0,-1)$ whose multiplicities at C_1 are one. Therefore C_1 is an affine non-singular model of C.

The adjoint divisor of C is $\Delta_P = P' + P''$.

The different $\mathcal{D}_P = (\pi^* dx) = 0$.

The adjoint divisor Δ_{P_1} is zero since P_1 is a non-singular point.

The different $\mathcal{D}_{P_1} = (dx) = P_1$.

Thus the discriminant divisor is $D_f = \tilde{\pi}^*(\Delta_P)\delta_P + \delta_{P_1} = 4P + 2P_1$. Thus we attained the same answer as in example 3.7.

Example 3.11 We use the curve of examples 2.3, 3.2 and 3.8.

Recall that P_1 is a singular point where P_2 is a singular different point of the curve . We desingularize C by blowing up the curve around its singular points P_1 and P_2.

After three successive blowing ups around P_1 we attain a local nonsingular model is given by the polynomial equation $y_1^2 + z_1^8 y_1^6 + z_1 = 0$. The point lying above P_1 is the point P_1''' (ex. 2.3).

The adjoint divisor of the curve C at the point P_1 is $\Delta_{P_1} = 28P_1'''$ (ex. 3.2).

The different $\mathcal{D}_{P_1} = (\pi^* dz) = 4P_1'''$.

The discriminant divisor is $D_{f_1} = \delta_{P_1} + \pi_*(\Delta_{P_1}) = 160P_1$. Recall from example 2.3 that f_1 is the affine representation of C around its singular point P_1.

After two successive blowing ups around P_2 we attain a nonsingular model of the original curve. The local representation of the nonsingular model is given by the polynomial equation $v'^4 + u + u^9 v^8 = 0$. The point lying above P_2 is P_2''.

The adjoint divisor of the curve C at the point P_2 is $\Delta_{P_2} = 24P_2''$.

The different $\mathcal{D}_{P_2} = (\pi^* dv) = 8P_2''$.

The discriminant divisor is $D_{f_2} = \delta_{P_2} + \pi_*(\Delta_{P_2}) = 288P_2$. Recall that f_2 is the affine representation of the curve C around its singular point P_2.

Chapter 4

Brill-Noether Theorem and Applications

The two main topics of this chapter are, the Brill-Noether theorem and its application to the theory of algebraic geometric Goppa codes.

In the first section of this chapter, we prove the Brill-Noether theorem when the field of constants is finite.

The Brill-Noether theorem implies an algorithmic construction of a basis for the vector space $\mathcal{L}(G)$ first realized by Goppa, [23],[22],[24],[25], [26]. In his book, [26],this algorithm is applied to plane curves having only ordinary singularities. However, is not considered the case where the curves are singular with nonordinary singularities defined over finite fields. Throughout the second section, we present the algorithm EVG which is an extended version of the one described by Goppa. In the algorithm EVG, we consider singular curves defined over finite fields. The time complexity of the algorithm EVG is proven to be polynomial in the degree of the curve (lemma 4.2).

Le Brigand and Risler [43], also approached the Brill-Noether theorem algorithmically in their recent work in coding theory. While studying their algorithm, the following questions are raised: What methods can be used to compute the adjoint divisors? Is the adjoint curve of Le Brigand and Risler [43] unique and how do we calculate it? Taking under consideration the above mentioned questions we develop the algorithm MBR which serves as an effective modification to the one described by Le Brigand and Risler. The algorithm MBR is a composition of algorithms which appear in the earlier chapters of this thesis. We demonstrate the algorithm MBR through example 4.1 .The time complexity of the algorithm MBR is computed in lemma 4.1.

The last section is an introduction to the theory of algebraic geometric Goppa codes. For further reading on this topic we suggest the books by Goppa [26], Tsfasman and Vladut [64] ,van Lint [65], [66], [67] and Moreno [45]. In this part we emphasize the natural application of the algorithms MBR and EVG to the construction of algebraic geometric Goppa codes.

4.1 Brill-Noether theorem

In this section we will prove the Brill-Noether theorem when the field of constants is finite. We base our proof on a corollary of Noether's Fundamental theorem proved by Gorenstein ([27], th.7) .

Notation. (Gorestein [27]) Note that if a curve C': $G[X,Y,Z] = 0$ does not contain the curve C as a component then the intersection divisor $C \bullet C'$ can be represented as:

$$C \bullet C' = \sum_P \mathrm{ord}_P(g(x,y))P$$

where the sum is taken over the closed points (Moreno [45] pg. 155) in the function field of the curve $k(C)$ and $g(x,y)$ is the dehomogenization of $G[X,Y,Z]$ with respect to one homogeneous coordinate and is considered as an element in $k(C)$.
For notational convenience we denote the above by writing

$$C \bullet C' = (G)$$

and stress the fact that this is not in general a principal divisor.

Corollary 4.0.1 *Let C: $F[X,Y,Z] = 0$ be an irreducible plane projective curve defined over an arbitrary ground field k, and let Δ be its adjoint divisor. Suppose C': $G[X,Y,Z] = 0$ is another curve which does not contain C as a component. If C'': $H[X,Y,Z] = 0$ is an adjoint curve of C which satisfies*

$$C \bullet C'' \geq C \bullet C' + \Delta$$

where $C \bullet C'$ (resp. $C \bullet C''$) is the complete intersection divisor of C and C' (resp. C and C''), then there exist homogeneous forms A and B such that

$$H = BG + AF$$

The proof of the corollary becomes obvious if we consider the definition of the adjoint curve (def. 3.6).

Theorem 4.1 (Brill-Noether Theorem) *Let C: $F[X,Y,Z] = 0$ be an absolutely irreducible singular plane curve defined over a finite field* k. *Let G be an effective divisor on the nonsingular model $\tilde{C}$. Consider a homogeneous form G_0 of degree l such that $(G_0) \geq \Delta + G$ where Δ is the adjoint divisor of C. Then as G_1 runs through a complete system of* k*-linearly independent forms of degree l which are not multiples of F and which satisfy $(G_1) \geq (G_0) - G$, the quotients $\phi = G_1/G_0$ form a basis for the linear system $\mathcal{L}(G) - \{0\}$.*

Proof.
We first assume that the rational function $\phi = G_1/G_0$ satisfies the inequalities: $(G_0) \geq \Delta + G$ and $(G_1) \geq (G_0) - G$. We need to show that ϕ belongs in the finite vector space $\mathcal{L}(G)$..

From the second inequality we conclude that $(\phi) = (G_1) - (G_0) \geq -G$. Therefore the rational function ϕ belongs in the finite vector space $\mathcal{L}(G)$.
Since the homogeneous form G_1 is not divisible by F we conclude that $\phi \neq M \cdot F/G_0$, for some homogeneous form M. Since the quotient $M \cdot F/G_0$ evaluated at any point of the curve is zero, we conclude that $\phi \neq 0$, i.e., $\phi \in \mathcal{L}(G) - \{0\}$.

Next, we show that given a non zero function f in the vector space $\mathcal{L}(G)$ there exists a homogeneous form G_1 of degree l non divisible by F such that $(G_1) \geq (G_0) - G$. Also we show that the rational function f is the quotient G_1/G_0 and belongs in the vector space $\mathcal{L}(G)$.
Let f be the nonzero rational function in $\mathcal{L}(G)$ designated by the quotient H/H_0 where H and H_0 are homogeneous forms of the same degree. We want to show that $G_1/G_0 = H/H_0$, i.e., $G_0H = H_0G_1 + BF$ for some homogeneous form, B. From corollary 4.0.1 we conclude that it suffices to show the inequality, $(G_0H) \geq (H_0) + \Delta$, i.e., $(G_0) + (H) - (H_0) \geq \Delta$. Thus it suffices to show that $(G_0) + (f) \geq \Delta$:

The sum $(f) + G$ is greater or equal to zero since the rational function f belongs in the vector space $\mathcal{L}(G)$ which implies that $(G_0) + (f) + G \geq (G_0)$. But since $(G_0) \geq \Delta + G$ we conclude that $(G_0) + (f) \geq \Delta$.
□

Remark. Le Brigand and Risler [43] prove the above theorem utilizing the theorem of residues.

4.2 Two new versions of the Brill-Noether algorithm

The Brill-Noether theorem provides an algorithmic construction of a basis of the k-vector space $\mathcal{L}(G)$. Recent developments in this direction are:

- Goppa, [26], has applied the algorithm on plane curves having ordinary singularities, however all the curves that he used in the examples of [26] are nonsingular. The divisors on the curve are intersection divisors or part of intersection divisors. The curves are plane curves, so the machinery in Fulton [21] can be applied in order to execute the algorithm.

- Manin and Vladut [69] use modular curves of elliptic modules of V.G Drienfel'd. The singularities are resolved using the normalization process.

- Le Brigand and Risler [43] have applied the algorithm on an irreducible singular plane curve; the singularities are resolved using the normalization process. The divisors are defined over the nonsingular projective model of the curve. The nonsingular model of the curve is in $\mathbf{P}^n(\mathbf{k})$ where $n > 2$, thus more machinery from algebraic geometry is needed in order to apply the algorithm.

- Le Brigand [42] generalizes the Brill Noether algorithm, by applying it to reducible curves in order to find their factors.

Our contribution in this section is to present two new versions of the Brill-Noether algorithm. The first version is the algorithm EVG, which is an extended version of Goppa's [26] algorithmic construction. In our case the curve is any absolutely irreducible, singular, plane curve.

The second version is the algorithm MBR which is a modified version of the algorithmic construction which appears in Le Brigand and Risler [43]. Both algorithms require the Rationality assumption (sec. 2.1).

4.2.1 Algorithm MBR

The algorithm MBR inputs an absolutely irreducible singular curve defined over a finite field and a divisor D in the normalization of the curve. It outputs a basis for the vector space $\mathcal{L}(G)$. The algorithm MBR detects the rational singularities of the curve by applying the algorithmic construction SM described in the second chapter of this thesis (sec. 2.1). It resolves the singularities using successive blowing ups, i.e., we apply the algorithm NOR described in the second chapter of this thesis (sec. 2.2). It finds the adjoint divisor of the curve utilizing the algorithm AD described in the third chapter of this thesis (sec. 3.1). Finally we calculate the time complexity needed to execute the algorithm.

Let C be an absolutely irreducible, singular, plane curve defined over the finite field $\mathbf{k} = \mathbf{F}_q$ where $q = p^b$. Let $\tilde{C}$ be the nonsingular model of C obtained by the birational morphism $\tilde{\pi} : \tilde{C} \longrightarrow C$.

Notation. If A and B are homogeneous forms in X, Y and Z of the same degree, then $\overline{A}/\overline{B}$ denotes the associated rational function on $\mathbf{P}^2$ or any restriction to a curve on $\mathbf{P}^2$.

Algorithm MBR
Input: An absolutely irreducible, plane curve $C : F[X, Y, Z] = 0$ defined over $\mathbf{k} = \mathbf{F}_q$ where $q = p^b$. An effective divisor G on $\tilde{C}$ such that the image $\tilde{\pi}(G)$ does not contain any point which belongs in the singular locus of C i.e., $G = m\,Q_0$ where Q_0 is a nonsingular point of the curve C.
Output: A basis of the k-vector space $\mathcal{L}(G)$.
Method:

Step 1: Find the rational singularities of C and their multiplicities (algorithm SM).

Step 2: Find the local representations of the normalized curve $\tilde{C}$ (algorithm NOR).

Step 3: Calculate the integers α_{P_i} (theorem 3.2).

Step 4: Calculate the adjoint divisor $\tilde{\Delta}$ of the curve C (algorithm AD).

Step 5: Find the adjoint curve $C_a : G_0 = 0$ i.e., the following facts should be satisfied.

i. The homogeneous form G_0 is of degree l not divisible by F.

ii. The divisor (G_0) is greater or equal to the zero divisor (0).

iii. The divisor $(G_0) \geq \tilde{\Delta} + G$

iv. The homogeneous form G_0 goes through every rational singular point of C with multiplicity greater or equal to a_P.

Step 6: Find a basis for all those homogeneous forms G_i which satisfies the following conditions.

i. The homogeneous form G_i is of degree l not divisible by F.

ii. The divisor (G_i) is greater or equal to the zero divisor.

iii. The inequality $(G_i) \geq (G_0) - G$ holds.

Step 7: If $\{G_0, ..., G_n\}$ is the set which contains the forms found in the previous step, then the set

$$\{1, \overline{G_{1*}}/\overline{G_{0*}}, \cdots, \overline{G_{n*}}/\overline{G_{0*}}\}$$

forms a basis for $\mathcal{L}(G)$ over $\mathbf{k}$.

Lemma 4.1 *The algorithm MBR terminates and its complexity is polynomial in the degree of the curve.*

Proof. Let $C(i)$ denote the time complexity of the i-th step. In the first step, we apply algorithm SM hence $C(1) = O(q^2n^4\log^3 q)$.

For the second step we need to construct all the singularity trees, i.e., we apply the algorithm NOR; thus $C(2) = O(n^8q^2r\log^3 q)$ where r is the highest multiplicity of the curve C at any of the singular points (worst singularity). The estimate of the third step $C(3)$ is also contained in $C(2)$.

In the fourth step, we apply the algorithm AD , thus $C(4) = O(q^4n^4\log^3 q)$

In the fifth step, we input a monomial $G_0 = X^aY^bZ^c$ such that $a+b+c = l$ which goes through the singular points of C and the points in the support of the divisor D. We decide if the curve C_a represented by the form G_0 is a candidate for an adjoint of C by checking the multiplicities of all the singular points of the curve C and by finding the divisor (G_0). In order to compute the multiplicities we need $O(n^4\log^3 q)$ time. The computation of the divisor (G_0) requires the computation of the orders of G_0 at all the $O(q^2)$ simple infinitely near points in the singularity trees. Therefore we need $O(q^2)$ power expansions where each requires $O(n^2b^2(\log p + 1))$ time. The overall bound of this step is $C(5) = O(n^4q^2\log^2 q)$.

In the sixth step, we repeat the procedure of the fifth step with $l(G) - 1$ different forms. The integer $l(G)$ is the dimension of the vector space $\mathcal{L}(G)$ over the finite field $\mathbf{k}$ and $l(G) = O(n^2)$. Therefore the sixth step requires $C(6) = O(n^6q^2r(\log^3 q))$ bit operations.

Hence the time complexity of the algorithm MBR is

$$O(n^8q^2r\log^3 q)$$

□

Example 4.1 We will use examples 3.1 and 3.4 where the curve $C : F = Y^2Z^3 + YZ^4 + X^5 = 0$ is over the finite field $\mathbf{k} = \mathbf{F}_{2^4}$.

The effective divisor on the curve is $G = 5Q_0$ where $Q_0 = [0, 0, 1]$ is a simple point of C. The local coordinates of Q_0 are the rational functions $u = X/Z$ and $v = Y/Z$. The order of the function u at the point Q_0 is $\text{ord}_{Q_0} u = 1$. The order of the function v at the point Q_0 is $\text{ord}_{Q_0} v = 5$.

Step1: The point $P_1 = [0, 1, 0]$ is a non-ordinary point of C of multiplicity $m_P(C) = 3$.

Step2: The affine representation of the nonsingular model of C around P_1 is given by the polynomial $f(s', t') = (s')^2 + t' + (t')^3 s'$.

Step3: The integer $a_{P_1} = 3$ (ex.3.4).

Step4: The adjoint divisor of the curve is $\Delta = 8P_3$ where P_3 is the point lying over P_1 (ex. 3.1).

Step5: We claim that the adjoint curve of C is $C_a : G_0 = Y^2Z^5 = 0$ since it meets the following requirements:

i. The homogeneous form G_0 is of degree $l = 7$ and is not divisible by F.

ii. The divisor described by the homogeneous form G_0 is $(G_0) = 25P_3 + 10Q_0 > 5Q_0 + 8P_3 = G + \Delta$. This is clear since $\text{ord}_{P_1} t^5 = 25$ where t^5 is the image of the homogeneous form G_0 in the local ring $\mathcal{O}_P(C)$. Indeed $\text{ord}_{P_1} t^5 = \text{ord}_{P_3}((t')^2(s'))^5$. Similarly the local affine equation of G_0 around the point Q_0 is $v^2 = 0$ and $\text{ord}_{Q_0}(G_0) = \text{ord}_{Q_0} v^2 = 10$.

iii. The homogeneous form G_0 goes through the points P_1 and Q_0. The multiplicity of G_0 around the point P_1 is $m_{P_1}(G_0) = 5 > a_{P_1}$.

Step6: The homogeneous forms G_i, $i = 1, ..., 4$ are:

Forms	$g(u,v)$	$f(s,t)$	$\text{ord}_{P_3} f$	$\text{ord}_{Q_0} g$
$G_1 = Y^2Z^5$	v^2	t^5	$\text{ord}_{P_3}((t')^2s')^5 = 25$	$\text{ord}_{Q_0} v^2 = 10$
$G_2 = YZ^6$	v	t^6	$\text{ord}_{P_3}((t')^2s')^6 = 30$	$\text{ord}_{Q_0} v = 5$
$G_3 = Z^5XY$	uv	st^5	28	6
$G_4 = Z^4X^2Y$	u^2v	s^2t^4	26	7

It is obvious that the divisors described by the forms G_i are greater than the difference $(G_0) - D$. In addition, their multiplicities at the singular point P_1 of the curve C are $m_{P_1}(YZ^6) = 6$, $m_{P_1}(Z^5XY) = 6$ and $m_{P_1}(Z^4X^2Y) = 6$ and they are greater than the integer a_{P_1}. The above forms are linear independent since they vanish in different orders.

Step7: A basis of the vector space $\mathcal{L}(G)$ over the finite field $\mathbf{k}$ is the set $\{1, 1/v, u/v, u^2/v\} = \{1, t, s, s^2/t\}$.

Remark. Unlike Le Brigand and Risler [43], we compute the adjoint divisor of the curve which appears in the above example by using two methods (ex. 3.1). In example 3.4 we showed that the curves with homogeneous equations $G_0 = YZ^5$ and $G_1 = YZ^3$ can also serve as adjoints to the curve C therefore we do not restrict ourselves to the one adjoint curve chosen by Le Brigand and Risler .

4.2.2 Algorithm EVG

Goppa, [22], [26], has suggested an algorithmic construction based on the Brill-Noether theorem for the case where the curve is a singular curve with only ordinary singularities. In this section we consider the case where C is any singular curve defined over a finite field. In the algorithm EVG we use the Cremona transformations in order to find a birational equivalent curve having only ordinary rational singularities, i.e. we apply the algorithmic construction RC described in the second chapter of this thesis. We use intersection divisors or part of intersection divisors defined in the plane. The advantage of algorithm EVG versus algorithm MBR is that we are always on the plane and we can use the simple concepts on plane curves which appear in Fulton [21]. Finally we calculate the time complexity needed to execute the algorithm.

Algorithm EVG (* Extended Version of Goppa *)
Input: A singular, absolutely irreducible plane curve $C : F = 0$ of degree n defined over a finite field $\mathbf{k} = \mathbf{F}_q$ with $q = 2^m$ elements. An intersection divisor -or part of an intersection divisor- G .
Otput: A basis of the k-vector space $\mathcal{L}(G)$.

Step1: Find the rational singularities of C and their multiplicities (algorithm SM).

Step2: Find a curve $C' : F'[X, Y, Z] = 0$ which is birational equivalent to C and has at worst ordinary singularities (algorithm RC). Resolve the ordinary singularities (algorithm BU).

Step3: Find the adjoint divisor $(E') = \sum(E'_P)$ of the curve C' where the sum is taken over all the ordinary singular points $P \in \mathrm{Sing}C'$ and $(E'_P) = \sum_{Q_i \in \pi^*(P)}(r-1)Q_i$.

Step4: Find an arbitrary adjoint curve $C_a : G_0 = 0$ which satisfies the following conditions:

i. The homogeneous form G_0 is of degree l not divisible by F'.

ii. The divisor (G_0) is greater or equal to the zero divisor (0).

iii. The inequality $(G_0) \geq (E') + G$, holds.

iv. The curve $C_a : G_0[X, Y, Z] = 0$ is an adjoint curve of C' and goes through every ordinary singular point P of the curve C' with multiplicity greater or equal to $r - 1$.

Step5: Find a basis for all those forms G_i which satisfy the following conditions:

i. The homogeneous form G_i is a form of degree l not divisible by F'.

ii. The divisor (G_i) is greater or equal to the zero divisor (0).

iii. The inequality $(G_i) \geq (G_0) - G$ holds.

Step6: The quotients $\overline{G_{i*}}/\overline{G_{0*}}$'s form a basis for the vector space $\mathcal{L}(G)$.

Lemma 4.2 *The algorithm EVG terminates and its complexity is polynomial in the degree of the curve.*

Proof. Let $C(i)$ denote the time complexity of the i-th step. In the first step, we apply algorithm SM hence $C(1) = O(q^2n^4\log^3 q)$.

The algorithm RC is applied in the second step, hence $C(2) = O(q^{12}rn^{12}\log^3 q)$. The estimate of the time complexity of the third step $C(3)$is contained in $C(2)$.

Let G_0 be some homogeneous form of degree l. In the fourth step we need to compute the intersection divisor $F \bullet G$ i.e., we need to evaluate the homogeneous forms F and G at the $q^2 + q + 1$ projective points. Each evaluation requires to rise $O(q^2)$ elements from the finite field in some power which is at worst the degree of F (or G); this process requires the overall time bound $O(q^2\log n\log^3 q)$. Thus the overall time complexity of the fourth step is $C(4) = O(q^4\log n\log^3 q)$.

In the fifth step we need to repeat the previous step $l(G)$ number of times where $l(G) = O(n^2)$ is the dimension of the vector space $\mathcal{L}(G)$ over the finite field $\mathbf{k}$.

Thus the overall time bound for the algorithm EVG is

$$O(q^{12}rn^{14}\log n^3\log^3 q)$$

□

Remark. Goppa ([26] ,pg.92) computes the adjoint divisor E of the curve as $E = \sum(r-1)r\,P$ where the sum runs through all the ordinary singular points of the curve C of multiplicity r. What Goppa describes, is the projection of the adjoint divisor on the set of divisors of C, i.e., $E = \pi_*\Delta$ where $\pi_* : \mathrm{Div}(\tilde{C}) \longrightarrow \mathrm{Div}(C)$ and C is defined over an *algebraically closed field.*

Example 4.2 Consider the singular curve $C = Y^2Z + X^3 + XYZ = 0$ defined over the finite field $\mathbf{k} = \mathbf{F}_{2^5}$.

The intersection divisor is $D = Z \bullet F = 3P_2$ where the point $P_2 = [0, 1, 0]$.

Step 1: The point $P_1 = [0, 0, 1]$ is an ordinary point of multiplicity $m_{P_1}(C) = 2$. The local equation of C around P_1 is $f(u, v) = v^2 + u^3 + uv = 0$.

Step 2: The blowing up of the curve C around each singular point P_1 yields the infinitely simple points P_1' and P_1''. The adjoint divisor is $E = P_1' + P_1''$.

Step 3: The adjoint curve C_a is given by the homogeneous form $G_0 = X^3Y$. It satisfies the required conditions.

i. The homogeneous form G_0 is of degree 4.

ii. The divisor (G_0) is:

$$\begin{aligned}(G_0) &= (X^3Y) \bullet F \\ &= X^3 \bullet F + Y \bullet F \\ &= 3(X \bullet F) + Y \bullet F \\ &= 3(2P_1 + P_2) + 3P_1 = 9P_1 + 3P_2\end{aligned}$$

Thus $(G_0) = 3P_2 + 2P_1 + 7P_1$ i.e., $(G_0) \geq \Delta + D$ as expected.

iii. The adjoint curve $C_a : G_0 = 0$ goes through the singular point $P_1 = [0, 0, 1]$ with multiplicity $m_{P_1}(G_0) = m_{P_1}(X^3Y) = m_{P_1}(u^3v) = 4$.

Step 4: A basis for the required forms G_i of degree $l = 4$ are:

G	$I(P_1, G \cap F)$
$G_1 = X^3Y$	9
$G_2 = X^2Y^2$	10
$G_3 = XY^3$	11
$G_4 = Y^4$	12

The divisors (G_i) can easily be computed as follows:

$$\begin{aligned}(G_1) = (X^3Y) \bullet F &= 9P_1 + 3P_2 \\ (G_2) = (X^2Y^2) \bullet F &= 10P_1 + 2P_2 \\ (G_3) = (XY^3) \bullet F &= 11P_1 + P_2 \\ (G_4) = (Y^4) \bullet F &= 12P_1\end{aligned}$$

From where we conclude that the inequality $(G_i) \geq (G_0) - D$ holds for every $i = 1, ..., 4$.

Step 5: Therefore the set $\{1, Y/X, Y^2/X^2, Y^3/X^3\} = \{1, y, y^2, y^3\}$ is a basis of $\mathcal{L}(G)$. The genus of the curve C is $g = 0$ and the dimension of the vector space $\mathcal{L}(G)$ is $l(G) = 4$.

Remark. The curve C in example 4.2 has exactly 32 rational points over the finite field $\mathbf{F}_{2^5}$.

4.3 Applications to A. G. Goppa Codes

Recent developments in the field of algebraic codes pioneered by Goppa [22], [26] seem to suggest that a unified approach to the study of some of the most important codes is best achieved from the point of view of algebraic geometry. For further reading on

this topic we suggest, Goppa [26], Tsfasman-Vladut [64], van Lint [67] , Moreno [45], Wolfmann [72] and Lachaud [41].

Let C be an absolutely irreducible smooth curve defined over the finite field $\mathbf{k} = \mathbf{F}_q$ with $q = p^r$ elements where p is a prime number. Consider the divisor $D = P_1 + \cdots + P_n$ of the curve C with P_i distinct rational points over $\mathbf{k}$ and $G = \sum_Q m_Q Q$ be another divisor whose support is disjoint from the support of D.
There are two equivalent constructions of Algebraic Geometric Goppa Codes.

Construction 1: Consider the linear map $\Phi\colon \mathcal{L}(G) \longrightarrow \mathbf{k}^n$ defined by $\Phi(\phi) = (\phi(P_1) \cdots \phi(P_n))$

where ϕ is an element of $\mathcal{L}(G)$ and $\phi(P_i) \in \mathbf{k}$. The image $\Phi(\mathcal{L}(G))$ of Φ in $\mathbf{k}^n$ is a linear code of length n called the *algebraic geometric Goppa code* of length n. It is denoted by $C_{\mathcal{L}}(D, G)$.

Construction 2: Consider the map $\Psi\colon \Omega(G-D) \longrightarrow \mathbf{k}^n$ defined as $\Psi(\omega) = (\mathrm{Res}_{P_1}\omega, \mathrm{Res}_{P_2}\omega, \cdots$ $\mathbf{k}^n$. The image $\Psi(\Omega(G-D))$ in $\mathbf{k}^n$ is an *algebraic geometric Goppa code* of length n. It is denoted by $C_{\Omega}(D, G)$.

The two codes $C_{\mathcal{L}}(D,G)$ and $C_{\Omega}(D,G)$ are duals. Every code is characterized by the parameters $[n, k, d]$ where n is the length of the code k the dimension and d the minimum distance of the code.

The algorithms MBR and EVG are the main tools for the construction of algebraic geometric Goppa codes built from a singular curve of degree n over a finite field $\mathbf{k} = \mathbf{F}_q$. Therefore the time needed to construct an a.g. Goppa code is the time to run either of these algorithms, i.e., $O(n^8 q^2 r \log^3 q$ and $O(q^{12} r n^{14} \log n^3 \log^3 q)$ where r is the multiplicity of the curve at each worse singularity .

Example 4.3 (Klein Quartic) This example also appears in Hansen [29].
Consider the Klein Quartic curve $C : F = X^3Y + Y^3Z + Z^3X = 0$ over the finite field $\mathbf{k} = \mathbf{F}_8$.

The curve C is a nonsingular curve and is of degree $m = \deg F = 4$.

The adjoint divisor Δ of the curve is zero since the curve is nonsingular.

Every curve is an adjoint curve of the Klein Quartic curve.

The genus of the curve is $g = 3$.

The number of rational points of the curve over the finite field $\mathbf{k}$ is $N(g) \leq 24$. Actually the curve has exactly 24 rational points and they are: $Q_0 = [1,0,0]$, $Q_1 = [0,1,0]$, $Q_2 = [0,0,1]$ and P_{ij} where $P_{ij} = B^i \mathbf{A}^j P_{00}$, $i = 0,1,2$, $j = 0, \cdots, 6$, and

$$A = \begin{pmatrix} a & 0 & 0 \\ 0 & a^4 & 0 \\ 0 & 0 & a^2 \end{pmatrix}$$

and

$$B = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

The points P_{ij} are:

$$\begin{aligned} P_{00} &= [1, a^2, a+a^2] & P_{01} &= [1, a^2+a+1, a^2+a+1] \\ P_{02} &= [1, a, a^2+1] & P_{03} &= [1, a^2+a, 1] \\ P_{04} &= [1, 1, a] & P_{05} &= [1, a+1, a^2] \\ P_{06} &= [1, a^2+1, a+1] & P_{10} &= [a^2+a, 1, a^2] \\ P_{11} &= [a^2+a+1, 1, a^2+a+1] & P_{12} &= [a^2+1, 1, a] \\ P_{13} &= [1, 1, a^2+a] & P_{14} &= [a, 1, 1] \\ P_{15} &= [a^2, 1, a+1] & P_{16} &= [a+1, 1, a^2+1] \\ P_{20} &= [a^2, a^2+a, 1] & P_{21} &= [a^2+a, a^2+a+1, 1] \\ P_{22} &= [a, a^2+1, 1] & P_{23} &= [a^2+a+1, 1, 1] \\ P_{24} &= [a+1, a^2+1, 1] & P_{25} &= [a^2+a, a^2, 1] \\ P_{26} &= [a^2, a, 1] \end{aligned}$$

Since the above points are distinct, we conclude that the Frobenius group generated by the matrices A and B acts transitively on the Klein Quartic curve.

The divisors are $G = 4(Q_0 + Q_1 + Q_2)$ of degree $\deg(G) = 12$ and $D = \sum P_{ij}$ of degree $\deg D = 21$.

Consider the map Φ: $\mathcal{L}(G) \longrightarrow (\mathbf{F}_8)^{21}$, defined by $f \longrightarrow (f(P_{ij}))$ $i = 0, \cdots, 2$, $j = 0 \cdots, 6$. The rational function f belongs in the base of $\mathcal{L}(G)$. The code $C_{\mathcal{L}}(D, G)$ described by the Klein Quartic curve is the image of $\Phi(\mathcal{L}(G))$ in $(\mathbf{F}_8)^{21}$.

The parameters $[n, k, d]$ of the code are: $n = 21$, $k = l(G) = \deg G + 1 - g + l(W - G) = 10$ and $d = n - \deg G = 9$ (we denote by W the canonical divisor). Thus the code over $\mathbf{k} = \mathbf{F}_8$ has parameters $[n, k, d] = [21, 10, 9]$.

The curve with homogeneous equation $G_0 = XYZ$ is an adjoint curve of the Klein curve.

A base of the vector space $\mathcal{L}(G)$ is the set

$$\{\frac{XYZ}{XYZ}, \frac{X^3}{XYZ}, \frac{X^2Y}{XYZ}, \frac{X^2Z}{XYZ}, \frac{XY^2}{XYZ}, \frac{XZ^2}{XYZ}, \frac{Y^3}{XYZ}, \frac{Y^2Z}{XYZ}, \frac{YZ^2}{XYZ}, \frac{Z^3}{XYZ}\}$$

Example 4.4 Consider the singular curve $C : F = Y^2Z^3 + YZ^4 + X^5 = 0$ over the finite field $\mathbf{k} = \mathbf{F}_{2^4} \cong Z_2[a]/(a^4 + a + 1)$.

In examples 3.1, 3.4, and 4.1 we computed the following:

The divisor $G = 5Q_0$ where $Q_0 = [0, 0, 1]$.

The base of $\mathcal{L}(G)$ over k is the set $\{1, t, s, s^2/t\}$.

The genus of the curve is $g = (5-1)(5-2)/2 - 3(2)/2 - 2(1)/2 - 1(0)/2 = 2$.

Using Weil's bound we can have an upper bound for the number N of the rational points on the curve, i.e., $N \leq q + 1 + 2g\sqrt{q} = 16 + 1 + 2(2)\sqrt{16} = 33$. There are actually exactly 33 rational points on C i.e., $Q_0 = [0, 0, 1]$, $Q_1 = [0, 1, 0]$, $Q_2 = [0, 1, 1]$ and

$$\begin{aligned}
Q_3, ..., Q_7 &: [\alpha, a, 1] && \alpha = a, a^4, a^7, a^{10}, a^{13} \\
Q_8, ..., Q_{12} &: [\alpha, a^2, 1] && \alpha = a^2, a^5, a^8, a^{11}, a^{14} \\
Q_{13}, ..., Q_{17} &: [\alpha, a^4, 1] && \alpha = a, a^4, a^7, a^{10}, a^{13} \\
Q_{18}, ..., Q_{22} &: [\alpha, a^5, 1] && \alpha = 1, a^3, a^6, a^9, a^{12} \\
Q_{23}, ..., Q_{27} &: [\alpha, a^8, 1] && \alpha = a^2, a^5, a^8, a^{11}, a^{14} \\
Q_{28}, ..., Q_{32} &: [\alpha, a^{10}, 1] && \alpha = 1, a^3, a^6, a^9, a^{12}
\end{aligned}$$

Consider the injection $\Phi: \mathcal{L}(G) \longrightarrow (\mathbf{F}_{16})^{32}$ defined as $\Phi(f) = (f(P_3), f(Q_2), ..., f(Q_{32}))$ where f is in the basis of $\mathcal{L}(G)$. The image of Φ in $(\mathbf{F}_{16})^{32}$ is an a.g. Goppa code of length $n = 32$.

The length of the code is $n = 32$ the dimension k is the $\dim_{\mathbf{k}}\mathcal{L}(G)$ i.e., $k = 4$. The distance $d \geq n - \deg(G) = 27$. Thus the code defined by the curve C is a $[32, 4, 27]$ code. The transmission rate is $R = k/n = 1/8$ and the relative Hamming distance is $\delta = d/n = 27/32$.

The above generating matrix defined as $H = (f_i(P_3), f_i(Q_2), ..., f_i(Q_{32}))$ where $i = 1, ..., 4$ is the 4×32 matrix:

15	0	0	0	15	8	6	10	4	10	9	8	11	11	15	3	5	5	3	7	15	1	3	5	3	4	12	10	7	1	15	3
0	15	0	0	11	4	2	8	3	8	12	9	0	0	8	1	14	10	6	13	7	9	2	12	2	6	3	5	1	8	2	4
0	0	15	0	9	11	8	10	11	11	7	6	12	0	6	8	5	11	5	13	3	13	4	5	5	1	15	6	15	8	13	8
0	0	0	15	2	14	6	2	2	13	12	1	0	12	14	11	3	11	4	9	4	2	11	11	7	6	10	6	14	1	4	12

Chapter 5

Exponential Sums

Our main objective in this chapter is to show the interrelation which exists between the theory of exponential sums, algebraic geometry and the theory of algebraic geometric Goppa codes.

In a preliminary section we provide some basic material from the theory of exponential sums, which is necessary in order to comprehend the results of this chapter.

In the second section of this chapter, our objective is to prove the existence of a relation between the exponential sums, built from singular curves and those built from the desingularization of these curves. We reduce the singularities of the curves by the use of two methods: the blowing up method and the one based on the Cremona transformations.
The above mentioned relation is described by two formulas. The first formula links the exponential sum built from a singular projective curve to the exponential sum built from the birational equivalent curve (pr. 5.1, 5.2). The second one, relates the exponential sum built from a singular affine plane curve to the exponential sum built from the blown up curve (pr. 5.3-5.6).
The above formulas are utilized in examples 5.1 through 5.7. where computations are been performed by the use of the computer language, Mathematica.

The last section of this chapter describes the existing relation between the exponential sum and the theory of a.g. Goppa codes. Our contribution in this section is theorem 5.2 where we prove a new bound on the minimum distance of the dual of a Goppa binary subfield subcode constructed from a singular curve .
We derive the new estimates for exponential sums built from certain rational functions, i.e., the functions which belong to the vector space $\mathcal{L}(G)$ (th. 5.1). In example 5.8, we compute the minimum distance of the dual of a Goppa binary subfield subcode generated by a singular curve.

5.1 Basic Definitions

A major portion of this section is taken by a presentation of some of the fundamental concepts of the theory of exponential sums along with some theorems on the bounds

of exponential sums. This section will provide the basic tools for the development in the following sections. A fuller presentation of the theory of exponential sums in one variable is given in the fourth chapter of Moreno's book [45]. A report on recent work in the theory of exponential sums and their applications was given by C.Moreno and O. Moreno [48]. Katz in the two important monographs, [35] and [36], also deals with the recent advanced work on exponential sums.

Definition 5.1 *Let* $\mathbf{k} = \mathbf{F}_q$ *be a finite field of* $q = p^a$ *elements and* $\mathbf{k}_m$ *its extension of degree* m. *Fix a nontrivial character* ψ *of* $\mathbf{k}$. *For any Laurent polynomial* $f \in \mathbf{k}[x_1, x_1^{-1}, ..., x_n, x_n^{-1}]$ *we may form the exponential sums*

$$S^*(f) = \sum \psi(\mathrm{Tr}_m(f(x_1, ..., x_n))) \tag{5.1}$$

where $\mathrm{Tr}_m: \mathbf{k}_m \longrightarrow \mathbf{k}$ *is the trace map from* $\mathbf{k}_m$ *to* $\mathbf{k}$ *and the sum is over all the points* $(x_1, ..., x_n) \in (\mathbf{k}_m^*)^n$. *When* f *is actually a polynomial, we can also define* $S(f)$ *by taking the sum on the right hand side of (5.1) over all the points* $(x_1, ..., x_n) \in (\mathbf{k}_m)^n$.

The sums $S(f)$ and $S^*(f)$ are related in the following way. For any subset (including the empty set) $A \subset \{1, 2, .., n\}$ let f_A be the polynomial obtained from f by setting $x_i = 0$ for $i \in A$. Let $|A|$ denote the cardinality of A. Then

$$S(f) = \sum_A S^*(f_A) \tag{5.2}$$

$$S^*(f) = \sum_A (-1)^{|A|} S(f_A) \tag{5.3}$$

If $\mathbf{k}_m$ is a finite extension of $\mathbf{k} = \mathbf{F}_q$ of $q = p^e$ elements with absolute trace $\mathrm{Tr} = \mathrm{Trace}_{\mathbf{k}_m/\mathbf{F}_p}$ then we define a character $\psi_{\mathbf{k}_m}(x) = \exp\{2\pi i \mathrm{Tr}(x)/p\}$. The exponential sums that we will use in this chapter are defined over a finite field $\mathbf{k} = \mathbf{F}_q$ of $q = 2^e$ elements and thus are of the form

$$S_m(f(x_1, ..., x_n)) = \sum_{(x_1,...,x_n) \in (\mathbf{k}_m)^n} (-1)^{\mathrm{Tr}(f(x_1,...,x_n))}$$

where $\mathbf{k}_m$ is a finite extension of the finite field $\mathbf{k}$ of degree m.

There is a connection between exponential sums and the numbers of rational points on curves defined over a finite field. In particular let C be a plane nonsingular curve defined over the finite field $\mathbf{k} = \mathbf{F}_q$ with $q = 2^m$ elements.

Consider the exponential sum $S(F)$ defined as follows:

$$S(F) = \sum_{(X,Y,Z) \in (\mathbf{F}_q)^3} (-1)^{\mathrm{Tr}(F(X,Y,Z))} \tag{5.4}$$

The exponential sum can be rewritten as follows:

$$S(F) = Z_+ - Z_- \tag{5.5}$$

where $Z_+ = \#\{(X,Y,Z) : \mathrm{Tr}(F) = 0\}$ and $Z_- = \#\{(X,Y,Z) : \mathrm{Tr}(F) = 1\}$. Equation 5.5 implies that $q^3 = Z_+ + Z_-$ and consequently $Z_+ = 1/2(q^3 + S(F))$. On the other hand we note that the set Z_+ contains the projective points which satisfy the curve.

Let C' be the curve defined by the equation $C' : y^2 - y = f(x)$ where $f(x)$ is a rational function in the field of rational functions of C. The map $\pi : C' \longrightarrow C$ is a Galois covering. If $\tilde{C}$ denotes the normalization of C' then the map $\tilde{\pi} : \tilde{C} \longrightarrow C$ gives the Artin-Scheier covering associated with the rational function $f(x)$. Let $N(C)$ indicate the rational points of the curve C let $N(\tilde{C})$ and $N(\mathbf{P}^1)$ denote the number of rational points of $\tilde{C}$ and the rational points of the projective line $\mathbf{P}^1$ respectively. Then we have the fundamental equation, cf Moreno [45], [47],

$$N(\tilde{C}) - N(\mathbf{P}^1) = \sum_{x \in N(C) - \{\text{poles}\}} (-1)^{\mathrm{Tr} f(x)}$$

where the sum runs through all the rational points of the curve C which are not poles of $f(x)$. Since $N(\mathbf{P}^1) = q + 1$ we attain the equality

$$N(\tilde{C}) - (q+1) = \sum_{x \in N(C) - \{\text{poles}\}} (-1)^{\mathrm{Tr} f(x)}$$

5.2 Computing with Exponential Sums

Our main objective in this section is to show a relation between the exponential sums built from singular curves and their birational equivalents. For applications to coding theory we treat only the case associated with absolutely irreducible plane curves over a finite field of characteristic two. Throught this section we consider the Basic Rationality assumption (sec. 2.1).

The significance of the results of this section is that often a complicated exponential sum can be reduced to a simpler exponential sum which is easier to compute. In this part we reduce the singularities of a singular curve utilizing quadratic transformations. For a detailed analysis on this topic and for the notation of this section, we refer the reader to the second chapter of this thesis (sec. 2.3).

Let p be a prime and let $\mathrm{k} = \mathbf{F}_q$ denote a finite field of $q = 2^n$ elements. Let $\mathrm{Tr}_{\mathbf{F}_q/\mathbf{F}_2}$ be the *trace map*

$$\mathrm{Tr}_{\mathbf{F}_q/\mathbf{F}_2}(x) = x^{2^0} + x^{2^1} + \ldots + x^{2^{n-1}}$$

from the field $\mathbf{F}_q$ to the field $\mathbf{F}_2$. Consider the homogeneous form $F[X,Y,Z]$ in $\mathrm{k}[X,Y,Z]$. The *trace of the form* F is denoted by $\mathrm{Tr}(F)$ and is defined as follows:

$$\mathrm{Tr}(F) = F^{2^0} + \ldots + F^{2^{n-1}}$$

Consider an absolutely irreducible curve C represented by the homogeneous equation $F = 0$ with a non-ordinary singular point which is one of the fundamental points.

The curve C is defined over a finite field $\mathbf{k} = \mathbf{F}_q$ where $q = 2^n$. Consider the nontrivial additive character $\psi(x) = (-1)^x$ of the finite field $\mathbf{k}$. We define the *exponential sum* built from the form $F[X, Y, Z]$ to be

$$S(F[X,Y,Z]) = \sum_{(X,Y,Z)\in(\mathbf{F}_{2^n})^3} (-1)^{\mathrm{Tr}(F[X,Y,Z])}$$

where the sum is taken over all the affine points $(X, Y, Z) \in (\mathbf{F}_{2^n})^3$.

Let us apply the quadratic transformation Q on the curve C. The transformed curve C^Q is given by the form $F^Q[X, Y, Z] = Z^r Y^{r'} X^{r''} F_1[X, Y, Z]$ where r, r' and r'' are the multiplicities of the fundamental points P, P' and P'' respectively (Fulton [21], pg. 172). The birational equivalent curve which lies above the original curve C is the curve C_1 represented by the homogeneous equation $F_1[X, Y, Z] = 0$. The exponential sum built from the algebraic transform F_1 is described similarly, i.e.,

$$S(F_1[X,Y,Z]) = \sum_{(X,Y,Z)\in(\mathbf{F}_{2^n})^3} (-1)^{\mathrm{Tr}(F_1[X,Y,Z])}$$

The exponential sum constructed from the transformed curve C^Q is

$$S(F^Q[X,Y,Z]) = \sum_{(X,Y,Z)\in(\mathbf{F}_{2^n})^3} (-1)^{\mathrm{Tr}(F[YZ,XZ,XY])}$$

Our goal is to find a relation among the two exponential sums $S(F[X, Y, Z])$ and $S(F^Q[X, Y, Z])$. This leads us to the relation of the exponential sums constructed from the original curve, and its algebraic transform, i.e., the exponential sums $S(F[X, Y, Z])$ and $S(F_1[X, Y, Z])$. Keeping the above notation, the main results are described in the next two propositions. Let q denote the cardinality of the finite field $\mathbf{F}_{2^n}$. We indicate by $S^*[X, Y, Z]$ the exponential sum where the sum is taken over the affine points (X, Y, Z) in $(\mathbf{F}^*_{2^n})^3$ where $\mathbf{F}^*_{2^n} = \mathbf{F}^*_{2^n} - \{0\}$.

Proposition 5.1 *With notation as above, we have*

$$\begin{aligned} S(F^Q) - S(F) \;=\; & (q^2 - 2q)[S^*(F[X,0,0]) + S^*(F[0,Y,0]) + S^*(F[0,0,Z])] \\ & +3(q-1) - \\ & -[S^*(F[X,Y,0]) + S^*(F[X,0,Z]) + S^*(F[0,Y,Z])] \end{aligned}$$

Proof. In order to reduce the singularities of the curve $C : F[X, Y, Z] = 0$ we have to apply the Quadratic transformation Q i.e., $F^Q[X, Y, Z] = F[YZ, XZ, XY]$. Let us now take a closer look at this transformation and see how the q^3 affine points with coordinates (X, Y, Z) get transformed to the affine points with local coordinates YZ, XZ and XY. The nonzero points with any two coordinates zero, i.e., the points $[X, 0, 0]$, $[0, Y, 0]$ and $[0, 0, Z]$ are mapped to the zero point $[0, 0, 0]$ where X, Y, $Z \in \mathbf{F}_{2^n} - \{0\}$. There are $3(q - 1)$ such points.

The affine points with one coordinate zero, i.e., $[0, Y, Z]$, $[X, 0, Z]$ and $[X, Y, 0]$ are mapped to points with two coordinates zero, i.e., the points $[X, 0, 0]$, $[0, Y, 0]$ and $[0, 0, Z]$ where X, Y, $Z \in \mathbf{F}_{2^n} - \{0\}$. There are $3(q - 1)^2$ such points.

The $(q-1)^3$ remaining points with nonzero coordinates are mapped to points with nonzero coordinates. The zero point $[0,0,0]$ is mapped into itself.

Evaluating the exponential sum built from the transformed form F^Q is the same as evaluating the exponential sum built from the original form F but we have to substitute all the exponential sums evaluated from the forms $F[X,0,0]$ $F[0,Y,0]$ and $F[0,0,Z]$ where X, Y $Z \in \mathbf{F}_{2^n} - \{0\}$ with the number $3(q-1)(-1)^{\mathrm{Tr}(F[0,0,0])}$. The exponential sums evaluated by the homogeneous forms $F[0,Y,Z]$ $F[X,0,Z]$ and $F[X,Y,0]$ will be replaced by $(q-1)^2$ multiplied by the exponential sums constructed from the forms $F[X,0,0]$, $F[0,Y,0]$ and $F[0,0,Z]$ where X, Y, $Z \in \mathbf{F}_{2^n} - \{0\}$. Thus we have the following relation

$$\begin{aligned} S(F^Q) &= S(F) - [S^*(F[X,0,0] + S^*(F[0,Y,0]) + S^*(F[0,0,Z])] \\ &\quad +3(q-1)(-1)^{\mathrm{Tr}(F[0,0,0])} - \\ &\quad -[S^*(F[X,Y,0]) + S^*(F[X,0,Z]) + S^*(F[0,Y,Z])] \\ &\quad +(q-1)^2[S^*(F[X,0,0]) + S^*(F[0,Y,0])S^*(F[0,0,Z])] \end{aligned}$$

The desired relation is now obvious.
□

The following proposition relates the exponential sums built by the original curve $C : F[X,Y,Z] = 0$ and the birational equivalent curve $C_1 : F_1[X,Y,Z] = 0$. Recall that the multiplicities of the curve at the fundamental points are r, r' and r''. Using proposition 5.1 we attain the result of the next proposition.

Proposition 5.2 *With notation as above, we have*

$$\begin{aligned} S(F) - S(X^r Y^{r'} Z^{r''} F_1) &= [S^*(F[X,Y,0]) + S^*(F[X,0,Z]) + S^*(F[0,Y,Z])] \\ &\quad -(q^2-2q)[S^*(F[X,0,0]) + S^*(F[0,Y,0])S^*(F[0,0,Z])] \\ &\quad -3(q-1) \end{aligned}$$

Proof. The exponential sum built from the transformed form $S(F^Q)$ is $S(F^Q) = S(X^r Y^{r'} Z^{r''} F_1)$.
□

the next part of this section, we use the *blowing-up* method in order to reduce the singularities of a singular curve. We refer the reader to the second chapter of this thesis (sec. 2.2) for the notation which appears in this section.

Let p be a prime and let $\mathbf{k} = \mathbf{F}_q$ denote a finite field of $q = 2^n$ elements. Let $\mathrm{Tr}_{\mathbf{F}_q/\mathbf{F}_2}$ be the *trace* of an element x be defined as:

$$\mathrm{Tr}_{\mathbf{F}_q/\mathbf{F}_2}(x) = x^{2^0} + x^{2^1} + ... + x^{2^{n-1}}$$

from the field $\mathbf{F}_q$ to the field $\mathbf{F}_2$. Consider the polynomial $f(x,y)$ in $\mathbf{k}[x,y]$. The *trace polynomial* $\mathrm{Tr}(f)$ defined as $\mathrm{Tr}(f) = f^{2^0} + ... + f^{2^{n-1}}$ is a polynomial in the

field $\mathbf{F}_2[x,y]$. Let $f_0(u,v)$ be an affine local representation around a singular point, P of an absolutely irreducible curve C with multiplicity $m_P(C) = r_1$. The curve C is defined over a finite field $\mathbf{k} = \mathbf{F}_q$ where $q = 2^n$. Consider the nontrivial additive character $\psi(x) = (-1)^x$ of the finite field $\mathbf{k}$. We define the *exponential sum* built from the polynomial $f_0(u,v)$ to be

$$S(f_0(u,v)) = \sum (-1)^{\mathrm{Tr}(f_0(u,v))}$$

where the sum is taken over the affine points $(u,v) \in (\mathbf{F}_{2^n})^2$. The blowing up of the curve C around its singular point P is obtained by applying the birational morphism $\tilde{\pi}_1 : C_1 \longrightarrow C$ and

$$\tilde{\pi}_1^*(C) = f_0(u,us) = u^{r_1}[f_{r_1}(1,s) + uf_{r_1+1}(1,s) + ... + u^{n-r_1}f_n(1,s)]$$

The curve which lies above the original curve C is the curve C_1 and is given by the local equation $f_1(u,s) = f_{r_1}(1,s) + uf_{r_1+1}(1,s) + ... + u^{n-r_1}f_n(1,s) = 0$. The exponential sum built from the new polynomial $f_1(u,s)$ is:

$$S(f_1(u,s)) = \sum_{(u,s)\in(\mathbf{F}_{2^n})^2} (-1)^{\mathrm{Tr}(f_1(u,s))}$$

The exponential sum built from the polynomial $f_0(u,us)$ is defined similarly, i.e.,

$$S(f_0(u,us)) = \sum (-1)^{\mathrm{Tr}(f_0(u,us))}$$

where the sum is taken over the affine points $(u,s) \in (\mathbf{F}_{2^n})^2$. Our goal is to find a relation among the two exponential sums $S(f_1(u,s))$ and $S(f_0(u,us))$ which yields a new connection of the exponential sums $S(f_0(u,v))$ and $S(u^{r_1}f_1(u,s))$. Actually these relations hold for any birational morphism $\tilde{\pi}_i : C_i \longrightarrow C$. Following the existing notation we have the following propositions:

Proposition 5.3 *Let C be an absolutely irreducible singular plane curve defined over the finite field $\mathbf{F}_q$ with $q = 2^n$ elements. Let $f_0(u,v)$ be the affine polynomial around one of the singular points of the curve. Let $v = us$ be the change of variable required for the first blowing up. Then the exponential sums built from the polynomials $f_0(u,v)$ and $f_0(u,us)$ are related as follows:*

$$S(f_0(u,v)) - S(f_0(u,us)) = S(f_0(0,v)) - q(-1)^{\mathrm{Tr}f_0(0,0)} \tag{5.6}$$

Proof. At every step i of the blowing up process, where we apply the birational morphism $\tilde{\pi}_i$, we make the affine quadratic transformation $Q : \mathbf{A}^2(\mathbf{k}) \longrightarrow \mathbf{A}^2(\mathbf{k})$ defined as $Q(u,v) = (u,us)$. Let us now take a closer look at this transformation. In particular we want to examine how the $(q)^2$ affine points with coordinates (u,v) get transformed to the affine points with local coordinates (u,us). Note that the rational points of the functions u, v and s are the elements in the finite field $\mathbf{F}_{2^n}$. All the q points with first coordinate zero are mapped to zero, i.e., $(0,v) \longrightarrow (0.0)$

for all v in $\mathbf{F}_{2^n}$. The $q-1$ points whose second coordinates are zero are mapped to the same points, i.e., $(x,0) \longrightarrow (x,0)$ for all $x \in \mathbf{F}_{2^n} - \{0\}$. The remaining points with nonzero coordinates are mapped to different points with nonzero coordinates, i.e, $(u,v) \longrightarrow (u,s)$ for all u, v and s in $\mathbf{F}_{2^n} - \{0\}$. We need to evaluate the trace polynomial $\mathrm{Tr}(f_0(u,us)) \in \mathbf{F}_{2^n}[u,s]$ at the affine points with coordinates $(u,s) \in (\mathbf{F}_{2^n})^2$. This is the same as evaluating $\mathrm{Tr}(f_0(u,v))$ at the points with local coordinates $(u,v) \in (\mathbf{F}_{2^n})^2$. We exclude all those values of the trace polynomial $\mathrm{Tr}(f_0(u,v))$ evaluated at the points with coordinates $(0,v)$ where $v \in \mathbf{F}_{2^n}$. We replace these values with the product $q\mathrm{Tr}(f_0(0,0))$. Therefore the exponential sum $\sum(-1)^{\mathrm{Tr}(f_0(u,us)}$ where the sum is over all pairs $(u,s) \in (\mathbf{F}_{2^n})^2$ is

$$\sum_{(u,v)\in(\mathbf{F}_{2^n})^2} (-1)^{\mathrm{Tr}(f_0(u,v)} - \sum_{v\in(\mathbf{F}_{2^n}^2)} (-1)^{\mathrm{Tr}(f_0(0,v))} + q(-1)^{\mathrm{Tr}(f_0(0,0))}$$

Consequently the desired equation is obvious.
□

An analogous formula is described in the next proposition if the blowing up requires the change of the other variable, i.e., $u = vs$.

Proposition 5.4 *With notation as above, we have*

$$S(f_0(u,v)) - S(f_0(vs,v)) = S(f_0(u,0)) - q(-1)^{\mathrm{Tr}f_0(0,0)} \tag{5.7}$$

Proof. The affine quadratic transformation Q: $\mathbf{A}^2(\mathbf{k}) \longrightarrow \mathbf{A}^2(\mathbf{k})$ defined as $Q(u,v) = (vs,v)$ can also be applied at the blowing up process. Thus, the proof of this proposition becomes obvious if we follow the steps of the proof of proposition 5.3.
□

In the first four examples, we compare the calculations of the exponential sums obtained by Mathemetica and by the formula in proposition 5.3. In the next three examples we compare the calculations computed by Mathematica and by the formula in proposition 5.4.

Example 5.1 Consider the curve C with the affine equation $f(u,v) = v^2 + v^3 + u^4$ around its non-ordinary singular point $P = (0,0)$ of multiplicity, $m_P(C) = 2$. The curve is defined over the finite field $\mathbf{k} = \mathbf{F}_{2^2}$.

The exponential sum constructed from the polynomial $f(u,v)$ is

$$S(f(u,v)) = \sum_{(u,v)\in(\mathbf{F}_{2^2})^2} (-1)^{\mathrm{Tr}(v^2+v^3+u^4)} = 0$$

The blowing up of P yields the blown-up curve $\tilde{\pi}_1^*(C) : f(u,us) = u^2s^2 + u^3s^3 + u^4 = 0$.

The exponential sum built from the polynomial $f(u,us)$ is

$$S(f(u,us)) = \sum(-1)^{\mathrm{Tr}(u^2s^2+u^3s^3+u^4)} = 4$$

where the sum is taken over all the pairs $(u,s) \in (\mathbf{F}_{2^2})^2$.

Proposition 5.3 yields the exponential sum $S(f(u,us)) = 0-[2(-1)^0+2(-1)^1]+4(-1)^0 = 4$.

Example 5.2 Consider the curve C with the affine equation $f(u,v) = v^4+u^9+uv^8$ around its non-ordinary singular point $P = (0,0)$ of multiplicity, $m_P(C) = 4$. The curve is defined over the finite field $\mathbf{k} = \mathbf{F}_{2^2}$.

The exponential sum constructed from the polynomial $f(u,v)$ is

$$S(f(u,v)) = \sum(-1)^{\mathrm{Tr}(v^4+u^9+uv^8)} = 0$$

where the sum is taken over all the pairs $(u,v) \in (\mathbf{F}_{2^2})^2$.

The blowing up of P yields $\tilde{\pi}_1^*(C) = f(u,us) = u^4s^4+u^9+u^9s^8$.

The exponential sum defined by the polynomial $f(u,us)$ is

$$S(f(u,us)) = \sum(-1)^{\mathrm{Tr}(u^4s^4+u^9+u^9s^8)} = 8$$

where the sum is taken over the pairs $(u,s) \in (\mathbf{F}_{2^2})^2$.

Using proposition 5.3 we calculate the exponential sum $S(f(u,us)) = 4 - [2(-1)^0+2(-1)^1]+4(-1)^0 = 8$.

Example 5.3 Consider the same curve as in example 5.1. The curve is defined over the finite field $\mathbf{k} = \mathbf{F}_{2^3}$.

The exponential sum constructed from the polynomial $f(u,v)$ is

$$S(f(u,v)) = \sum(-1)^{\mathrm{Tr}(v^2+v^3+u^4)} = 0$$

where the sum is taken over the pairs $(u,v) \in (\mathbf{F}_{2^3})^2$.

The blowing up of P yields the blown-up curve $\tilde{\pi}_1^*(C) : f(u,us) = u^2s^2+u^3s^3+u^4 = 0$.

The exponential sum built from the polynomial $f(u,us)$ is

$$S(f(u,us)) = \sum(-1)^{\mathrm{Tr}(u^2s^2+u^3s^3+u^4)} = 12$$

where the sum is over the pairs $(u,s) \in (\mathbf{F}_{2^3})^2$.

Using proposition 5.3 we calculate the exponential sum $S(f(u,us))$ in order to attain $S(f(u,us)) = 0-[2(-1)^0+6(-1)^1]+8(-1)^0 = 12$.

Example 5.4 Consider the same curve as in example 5.2. The curve is defined over the finite field $\mathbf{k} = \mathbf{F}_{2^3}$.

The exponential sum constructed from the polynomial $f(u,v)$ is

$$S(f(u,v)) = \sum(-1)^{\mathrm{Tr}(v^4+u^9+uv^8)} = -8$$

where the sum is taken over $(u,v) \in (\mathbf{F}_{2^3})^2$

The blowing up of P yields the blown-up curve $\tilde{\pi}_1^*(C) = f(u,us) = u^4s^4 + u^9 + u^9s^8$.

The exponential sum is

$$S(f(u,us)) = \sum(-1)^{\mathrm{Tr}(u^4s^4+u^9+u^9s^8)} = 12$$

where the sum is taken over $(u,s) \in (\mathbf{F}_{2^3})^2$.

Using proposition 5.3 we calculate the exponential sum $S(f(u,us)) = -8 - [4(-1)^0 + 4(-1)^1] + 8(-1)^0 = 0$.

Example 5.5 Consider the curve C with the affine equation $f(u,v) = v^3 + uv^4 + u^2$ around its non-ordinary singular point $P = (0,0)$ of multiplicity $m_P(C) = 2$. The curve is defined over the finite field $\mathbf{k} = \mathbf{F}_{2^2}$.

The exponential sum constructed from the polynomial $f(u,v)$ is

$$S(f(u,v)) = \sum(-1)^{\mathrm{Tr}(v^3+uv^4+u^2)} = 8$$

where the sum is taken over $(u,v) \in (\mathbf{F}_{2^2})^2$.

The blowing up of P yields $\tilde{\pi}_1^*(C) = f(vs,v) = v^3 + sv^5 + s^2v^2$.

The exponential sum

$$S(f(vs,v)) = \sum(-1)^{\mathrm{Tr}(v^3+sv^5+s^2v^2)} = 8$$

where the sum is taken $(s,v) \in (\mathbf{F}_{2^2})^2$.

Using proposition 5.4 we calculate the exponential sum $S(f(vs,v))$ in order to attain $S(f(vs,v)) = 4 - [2(-1)^0 + 2(-1)^1] + 4(-1)^0 = 8$.

Example 5.6 Consider the same curve as in example 5.5, defined over the finite field $\mathbf{F}_{2^3}$.

The exponential sum constructed from the polynomial $f(u,v)$ is

$$S(f(u,v)) = \sum(-1)^{\mathrm{Tr}(v^3+uv^4+u^2)} = -8$$

The blowing up of P yields $\tilde{\pi}_1^*(C) = f(vs,v) = v^3 + sv^5 + s^2v^2$.

The exponential sum built from the polynomial $f(vs, v)$ is

$$S(f(vs,v)) = \sum (-1)^{\mathrm{Tr}(v^3+sv^5+s^2v^2)} = 0$$

Using proposition 5.4 we calculate the exponential sum $S(f(vs, v))$ in order to yield $S(f(vs, v)) = -8 - [4(-1)^0 + 4(-1)^1] + 8(-1)^0 = 0$.

Example 5.7 Consider the same curve as in example 5.5, defined over the finite field $\mathbf{F}_q$ with $q = 2^4$ elements.

The exponential sum constructed from the polynomial $f(u, v)$ is

$$S(f(u,v)) = \sum (-1)^{\mathrm{Tr}(v^3+uv^4+u^2)} = 16$$

where the pairs $(u, v) \in (\mathbf{F}_{2^4})^2$.

The blown up curve around its singular point P is $\tilde{\pi}_1^*(C) = f(vs, v) = v^3 + sv^5 + s^2v^2$.

The exponential sum is

$$S(f(vs,v)) = \sum (-1)^{\mathrm{Tr}(v^3+sv^5+s^2v^2)} = 32$$

where the sum is over $(s, v) \in (\mathbf{F}_{2^4})^2$.

Using proposition 5.4 we calculate the exponential sum $S(f(vs, v)) = 16 - [8(-1)^0 + 8(-1)^1] + 16(-1)^0 = 32$.

The following proposition relates the exponential sums built by the original curve $C : f_0(u, v) = 0$ and the blown-up curve $C_1 : f_1(u, s) = 0$. The polynomial $f_0(u, v)$ describes the original curve around its singular point of multiplicity r_1.

Proposition 5.5 *The exponential sums of $f_0(u, v)$, $f_1(u, s)$ and $f_0(0, v)$ are related by the formulas*

$$S(f_0(u,v)) - S(u^{r_1} f_1(u,s)) = S(f_0(0,v)) - q(-1)^{\mathrm{Tr} f_0(0,0)} \tag{5.8}$$

Proof. Let us apply the birational morphism $\tilde{\pi}_1 : C_1 \longrightarrow C$ to the original curve C. The blown up curve $\tilde{\pi}_1^*(C)$ is described by the polynomial equation $f_0(u, us) = u^{r_1} f_1(u, s)$. The polynomial equation $f_1(u, s) = 0$ represents the affine equation of the curve C_1 which lies above the original curve. Therefore $S(f_0(u, us)) = S(u^{r_1} f_1(u, s))$ and from proposition 5.3 we conclude that $S(f_0(u, v)) - S(f_0(0, v)) + q(-1)^{\mathrm{Tr}(f_0(0,0))} = S(u^{r_1} f_1(u, s))$. The last equation yields the desired result, i.e.,

$$S(f_0(u,us)) - S(u^{r_1} f_1(u,s)) = S(f_0(0,v)) - q(-1)^{\mathrm{Tr} f_0(0,0)}$$

□

When we apply the affine quadratic transformation $Q : (u, v) \longrightarrow (vs, v)$ we have the following proposition:

Proposition 5.6 *With notation as above, we have*

$$S(f_0(u,v)) - S(v^{r_1} f_1(s,v)) = S(f_0(u,0)) - q(-1)^{\mathrm{Tr} f_0(0,0)} \tag{5.9}$$

Remark. The above four formulas established in propositions 5.3, 5.4, 5.5, 5.6 can be applied at any birational morphism $\tilde{\pi}_i: C_{i+1} \longrightarrow C_i$. Consequently, we can apply the propositions to the normalization process where we have the birational morphism $\tilde{\pi}: \tilde{C} = C_N \longrightarrow C_0$ where $\tilde{\pi} = \tilde{\pi}_N \circ ... \circ \tilde{\pi}_i \circ ... \tilde{\pi}_1$.

5.3 Exponential Sums and A.G. Goppa Codes

The goal in this section is to estimate the minimum distance of the dual of a Goppa binary subfield subcode generated from a singular curve. The new estimate is obtained using exponential sums techniques.

Our contribution is theorem5.1 where we find a bound for the exponential sum formed from rational functions which belong in the vector space $\mathcal{L}(G)$. The curve C is a singular, absolutely irreducible plane curve of genus g and degree d_1 over a finite field $\mathbf{k} = \mathbf{F}_{2^m}$.

Our next main theorem is theorem 5.2 where we derive a new lower bound on the minimum distance of the dual of a binary algebraic geometric Goppa code generated from a singular curve.

Let π be the birational morphism from the normalization of the curve $\tilde{C}$ to the curve C. The morphism π induces k-isomorphisms in the field of the rational functions of the curve, i.e., $\mathbf{k}(\tilde{C}) \cong \mathbf{k}(C)$.

Remark. The field of rational functions $\mathbf{k}(C)$ can be realized as an algebraic extension of the pure transcendental extension $\mathbf{k}(x)$.

The adjoint divisor $\mathcal{E}_P$ is a divisor on the normalized curve $\tilde{C}$ (sec. 3.1). Consider the divisor $G = \sum_{j=1}^{s} a_j Q_j$ in the set of divisors of $\tilde{C}$. The points $\{Q_j\}_{j=1}^{s}$ are k-rational simple points of C. Consider the vector space $\mathcal{L}(G)$ of dimension k over the finite field $\mathbf{k}$. Begin by selecting a nonzero homogeneous rational function R in $\mathbf{P}^2(\mathbf{k})$ such that $R = G_1/G_0$ where G_1 and G_0 are homogeneous forms of same degree d_2. The affine representation of R is a rational function $r = g_1(x,y)/g_0(x,y)$. The rational function r is a function from some affine piece of the curve to the affine line, i.e., $r : C \longrightarrow \mathbf{A}^1$ defined as $r(Q) = g_1(Q)/g_0(Q)$ for any rational point Q of the curve C. (By $r(Q)$ we denote the value of $r(x,y)$ at the rational point Q of the curve C; this is an element of the residue class field $\mathbf{k}_Q(C)$.) The composition $\pi \circ r$ yields the rational function f i.e., $f = \pi \circ r$. The rational function f is a function in $\mathbf{k}(\tilde{C})$ and maps an affine piece of the nonsingular model $\tilde{C}$ to the affine line , i.e., $f : \tilde{C} \longrightarrow \mathbf{A}^1$ defined as $f(Q') = r(\pi(Q'))$ for some point Q' in $\tilde{C}$.

We proceed by estimating the exponential sum

$$S(r, C) = \sum_{i=1}^{n} (-1)^{\mathrm{Tr}(f(P_i))}$$

where the trace function is $\mathrm{Tr}: \mathbf{F}_{2^m} \longrightarrow \mathbf{F}_2$ the rational function r is in the vector space $\mathcal{L}G - \{0\}$ and the sum $\sum$ is restricted to those rational points $\{P_i\}$ where $i = 1, ..., n$ of the curve which are not poles of r.

We want to use Bombieri's theorem ([11]th.5) so we need the following hypothesis: $r \neq h^2 - h$ for any rational function h in $\overline{\mathbf{k}}(\tilde{C})$ where $\overline{\mathbf{k}}$ is the algebraic closure of $\mathbf{k}$. The following lemma which appears in Moreno [49] gives a condition when the above hypothesis is satisfied.

Lemma 5.1 *If the divisor $G = \sum_{j=1}^{s} a_j Q_j$ with $a_j = 1$ then for $r \in \mathcal{L}(G)$ and r nonconstant we have that $r \neq h^2 - h$ for any rational function in $\overline{\mathbf{k}}(C)$.*

Bombieri [11](th.6) has estimated the exponential sum built by a singular curve with respect to the degree d_1 of the curve C. On page 98 of the same paper, Bombieri mentions that the number of points of $\tilde{C}$ such that $\pi^{-1}(\pi(x))$ is not defined in at most $(d_1 - 1)(d_1 - 2) - 2g$ where g is the genus of the curve.

We note that the number $(d_1 - 1)(d_1 - 2) - 2g$ is the degree of the adjoint divisor of the curve. In the third chapter of this thesis we described computational methods in order to calculate the adjoint divisor of the curve. Our objective in the next theorem is to modify Bombieri's theorem (th.6) utilizing those computational methods. We also reconsider his theorem in the special case where the rational function $r \in \mathcal{L}(G)$.

Theorem 5.1 *Let r be a nonconstant rational function in the finite dimensional vector space $\mathcal{L}(G)$. Let $G = \sum_{j=1}^{s} Q_j$ be a divisor on* $\mathrm{Div}(\tilde{C})$. *Then*

$$|S(r, C)| \leq (\, d_1^2 - 3d_1 + \deg(\mathcal{E}) + 2\deg G\,)2^{m/2} + \deg(\mathcal{E}) \tag{5.10}$$

where $(\mathcal{E})$ is the adjoint divisor of the curve C and d_1 is the degree of C.

Proof. Let $R = G_1/G_0$ be the homogeneous rational function in $\mathbf{P}^2(\mathbf{k})$ such that the affine representation $r = g_1/g_0$ of R belongs in the finite vector space $\mathcal{L}(G)$ and $f = \pi \circ r$ is the corresponding rational function in $\mathbf{k}(\tilde{C})$.

Since the divisor G is of the form $G = \sum_{j=1}^{s} a_j Q_j$ with $a_j = 1$ the function f satisfies $f \neq h^2(x) + h(x)$. The total number of points of $\tilde{C}$ such that $\pi^{-1}(\pi(x))$ is not defined, is at most the degree of the adjoint divisor of the curve, i.e., $\deg(\mathcal{E})$. Therefore we have

$$|S(r, C)| - \left|S(f, \tilde{C})\right| \leq \deg(\mathcal{E}) \tag{5.11}$$

Let us now apply Bombieri's estimate ([11](th.5)) on the normalized curve $\tilde{C}$ i.e.,

$$\left|S(f, \tilde{C})\right| \leq (\, 2g - 2 + t + \deg(f)_\infty\,)2^{m/2} \tag{5.12}$$

Recall Plucker's formula and rewrite the genus as $g = (d_1 - 1)(d_1 - 2)/2 - 1/2\deg(\mathcal{E})$ where $(\mathcal{E})$ is the adjoint divisor (Gorenstein [27], th.11). From the above equation we can conclude that $2g - 2 = d_1^2 - 3d_1 - \deg(\mathcal{E})$. On the other hand note that the divisor of poles, $(f)_\infty$ is the divisor associated with the homogeneous form G_0. Therefore

the degree $\deg(f)_\infty = \deg(G_0)$. We have assumed that the rational function f is in $\mathcal{L}(G) - \{0\}$. Therefore from the Brill-Noether theorem (th. 4.8), we conclude that the divisor $(G_0) \geq (\mathcal{E}) + G$. Thus $\deg(G_0) \geq \deg(\mathcal{E}) + \deg G$. Also note that if the divisor $(G_0) = \sum_{i=1}^{t} b_i Q_i$ where b_i is the intersection multiplicity of G_0 at Q_i , then the integer $t \leq \deg(G_0)$. Therefore the Bombieri's estimate can be rewritten as follows:

$$\left|S(f, \tilde{C})\right| \leq (d_1^2 - 3d_1 + \deg(\mathcal{E}) + 2\deg G)2^{m/2} \tag{5.13}$$

□

Corollary 5.1.1 *Let C be a nonsingular absolutely irreducible plane curve of degree d_1 defined over the field $\mathbf{F}_{2^n}$. Let $G = \sum_{j=1}^{s} Q_j$ be a divisor on C and r a rational function in $\mathcal{L}(G) - \{0\}$. We then have*

$$|S(r, C)| \leq (\, d_1^2 - 3d_1 + 2\deg G\,)2^{m/2} \tag{5.14}$$

Proof. The proof becomes obvious if we recall that the adjoint divisor of a nonsingular curve is zero. Therefore the genus g is the product $1/2(d_1-1)(d_1-1)$ and consequently $2g - 2 = d_1^2 - 3d_1$.
□

Remark. Theorem 5.1 holds for any finite field of prime characteristic. Note that theorem 5.1 can be stated for the general case where the rational function r is any rational function in $k(C)$. The proof of theorem 5.1 for the case where the curve is reducible or irreducible follows the same lines as the proof of theorem 6 in Bombieri [11].

5.3.1 Minimum Distance of the Dual

The fundamental result of this section is described in theorem 5.2 where we find a new bound on the minimum distance of the dual of a Goppa binary subfield subcode.

We recall the definition of a.g. Goppa codes. For further reading on this topic we suggest Goppa [26], van Lint [67], Tsfasman [64] and the fourth Gchapter of this thesis.

Let C be an absolutely irreducible plane curve defined over a finite field k of characteristic two. Consider two divisors $G = \sum_{j=1}^{s} a_j Q_j$ and $D = \sum_{i=1}^{n} P_i$ on the nonsingular model of the curve C with disjoint supports. The points $\{P_i\}$ and $\{Q_j\}$ are k-rational points of the nonsingular model of the curve C. By means of the map ψ: $\mathcal{L}(G) \longrightarrow \mathrm{k}^n$ defined as $\psi(f) = (f(P_1), ..., f(P_n))$ we define the *algebraic geometric Goppa code*, $C(D, G)$ as the image $\psi(\mathcal{L}(G))$.

The parity check matrix of $C(D, G)$ is $|f_i(P_j)|$ for $j = 1, ..., n$. The rational functions f_i run through a basis of the linear system $\mathcal{L}(G)$ i.e., $i = 1, ..., k$ where $k = \dim_{\mathrm{k}} \mathcal{L}(G)$. The Brill-Noether theorem describes the rational functions f_i.

The codes $C(D, G)$ are characterized by the parameters $[n, k, d]$ where n indicates the length of the code k the dimension and d the minimum distance.

The *binary subfield subcode of the a.g. Goppa code* is denoted by $C_2(D,G)$ and is the intersection $C(D,G) \cap (\mathbf{F}_2)^n$. Based on Delsarte [18] we can characterize the *dual of a Goppa binary subfield subcode* $C_2^{\perp}(D,G)$ as the trace of the a.g. Goppa code, i.e.,

$$C_2^{\perp}(D,G) = \mathrm{Tr}(C(D,G)) = \{ (\mathrm{Tr}(f_i(P_1)), ..., \mathrm{Tr}(f_i(P_n))) \}$$

where the trace map is $\mathrm{Tr} : \mathbf{F}_{2^m} \longrightarrow \mathbf{F}_2$ and the rational functions f_i belong in the basis of the vector space $\mathcal{L}(G)$.

We proceed by using the bound described in theorem 5.1 to estimate the minimum distance of $C_2^{\perp}(D,G)$. Recall that the *minimum distance* is the minimum number of the nonzero elements of the code which appears in any of the codewords, i.e., the minimum weight.

Theorem 5.2 *Consider the dual of a Goppa binary subfield subcode $C_2^{\perp}(D,G)$ generated from a singular curve C. Let D and G be divisors in $\tilde{C}$ described as above. Then the minimum distance of $C_2^{\perp}(D,G)$ is at least* $1/2[n-(d_1^2-3d_1+\deg(\mathcal{E})+2\deg G)2^{m/2}]$.

Proof.
Let $\mathbf{x}$ be a codeword of $C_2^{\perp}(D,G)$ then $\mathbf{x} = (\mathrm{Tr}(f(P_1)), ..., \mathrm{Tr}(f(P_n)))$ where f is a rational function in the vector space $\mathcal{L}(G) - \{0\}$. The weight w of the codeword $\mathbf{x}$ is the number of nonzero components of $\mathbf{x}$. Let z be the number of zero components. Then $z + w = n$ where n is the length of the codeword. The exponential sum $S(f,\tilde{C}) = \sum_{i=1}^{n}(-1)^{\mathrm{Tr}(f(P_i))}$ is the difference $z - w$. In particular $S(f,\tilde{C}) = n - 2w$. The bound estimated in theorem 5.12

$$\left|S(f,\tilde{C})\right| \leq (d_1^2 - 3d_1 + \deg(\mathcal{E}) + 2\deg G)2^{m/2}$$

yields a bound on the weight of the code. In particular the weight is $w \geq 1/2[n - (d_1^2 - 3d_1 + \deg(\mathcal{E}) + 2\deg G)]2^{m/2}$. Therefore the minimum distance is at least $1/2[n - (d_1^2 - 3d_1 + \deg(\mathcal{E}) + 2\deg G)]2^{m/2}$.
□

Corollary 5.2.1 *Consider the dual of the binary a. g. Goppa code, $C_2^{\perp}(D,G)$ generated from a nonsingular curve C. The minimum distance of $C_2^{\perp}(D,G)$ where D and G are divisors in C is at least* $1/2[n - (d_1^2 - 3d_1 + 2\deg G)]2^{m/2}$.

Remark. The estimation of the covering radius, the number of information symbols can be done similarly using the machinery in Moreno [49].

Examples 3.1, 3.4, 4.1 are used for the results of the next example.

Example 5.8 Consider the plane singular curve C_1 described by the homogeneous equation $Y^2Z^3 + YZ^4 + X^5 = 0$ defined over the finite field $\mathbf{k} = \mathbf{F}_{2^4}$ of degree d_1. The point, $P_1 = [0,1,0]$ is a non-ordinary singular point of multiplicity $m_{P_1}(C) = 3$.

Let $G = 5Q_0$ and $D = \sum_{i=1}^{32} P_i$ be the divisors in the set of divisors in the normalization of C with disjoint supports .

The algebraic geometric Goppa $C(D,G)$ that evolves from the curve C has parameters $[n = 32,\ k = 4,\ d = 27]$.

The binary algebraic geometric Goppa $C_2(D,G)$ is the intersection $C(D,G) \cap (\mathbf{F}_2)^{32}$.

The dual of the binary algebraic geometric Goppa $C_2^{\perp}(D,G)$ is the trace $\mathrm{Tr}(C(D,G))$.

The parity check matrix of $C_2^{\perp}(D,G)$ is the matrix, $H = |(\mathrm{Tr}(f_i(P_j))|$ where $j = 1,...,n = 32$ and $i = 1,...,k = 4$. The rational functions f_i are the elements in the basis of $\mathcal{L}(G) - \{0\}$. Note that f_i are the images of the homogeneous rational functions of $\mathbf{P}^2(\mathbf{k})$ in the local ring of the curve $\tilde{C}$ at the point P_3 . Recall that the point P_3 is the point lying above the singular point P_1.

The exponential sum $\left|S(f_i,\tilde{C}\right| \leq 80$. Therefore the weight $w \geq 24$. Thus the minimum distance of $C_2^{\perp}(D,G)$ is at least 24.

Remark. Using the improved Bombieri bound achieved by Moreno in [47], we have obtained a new bound for the minimum distance of $C_2^{\perp}(D,G)$ constructed of singular curves .

Bibliography

[1] S. Abhyankar and C. Bajaj, Computations with albebraic curves, *Lecture Notes in Computer Science, Springer Verlag*, 358, July 1988.

[2] S. S. Abhyankar, Ramblings in Algebraic Geometry and Related Algebra, *AMS Monthly*, 83:409–448, 1976.

[3] S. S. Abhyankar, Desingularization of Plane Curves, *American Mathematical Society Proc. of the Symp. in Pure Mathematics*, 40, Part 1:1–45, 1983.

[4] S. S. Abhyankar, *Algebraic geometry for scientists and engineers*, American Mathematical Society, Providence, Rhode Island, 1990.

[5] Aho, Hopcroft, and Ullman, *The Design and Analysis of Computer Algorithms*, Addison- Wesley Publishing Company, New York, 1974.

[6] Arbarello, Cornalba, Griffiths, and Harris, *Geometry of Algebraic Curves*, Grundlehren der mathematischen Wissenschaften 267 Springer Verlag, Basel, 1985.

[7] A. Averbuch, Z. Galil, and S. Winograd, Classification of all the minimal bilinear algorithms for computing the coefficients of the product of the polynomials modulo a polynomial, part I: The Algebra $G[u]/ < Q(u)^l >$, $l > 1$, *Theoretical Computer Science*, 58:17–56, 1988.

[8] L. Bertini, *Rendiconti*, 21:326, 1888.

[9] G.A Bliss, The reduction of singularities of plane curves by birational transformation, *Bull. of Amer. Math. Soc.*, XXIX:161–183, 1923.

[10] G.A Bliss, *Algebraic Functions*, Dover, New York, 1966.

[11] E. Bombieri, On Exponential Sums in Finite Fields, *American Jour. of Math.*, 88:71–105, 1966.

[12] A. Borodin and I. Munro, *Computational complexity of algebraic and numeric problems*, American Elsevier, New York, 1975.

[13] Von A. Brill and M. Noether, Die Entwicklung der Theorie der algebraischen Functionen in älterer und neuerer Zeit, *Jahresberichte der Deutschen Mathematiker-Vereinigung*, III:111–566, 1892-1893.

[14] Von A. Brill and M. Nöther, Über die algebraischen Functionen und ihre Anwendung in der Geometrie, *Mathematische Annalen*, 7:269–310, 1874.

[15] Bronstein, Hassner, Williamson, and Vasquez, Computer Algebra Algorithms for the Construction of Error Correcting Codes on Algebraic Curves, *presented in 1991 IEEE International Symposium on Information Theory*, June 1991.

[16] D.V. Chudnovsky and G.V. Chudnovsky, Algebraic Complexities and Algebraic Curves over Finite Fields, *Proc. Natl. Acad. Sci. USA*, 84:1739–1743, April 1987.

[17] P. Cull and E.F. Jr Ecklund, Towers of Hanoi and analysis of algorithms, *Monthly of the M.A.M.*, page 407, 1985.

[18] P. Delsarte, On Subfield Subcodes of Reed-Solomon codes, *IEEE Trans. Info. Theory*, 21:575–576, 1975.

[19] Van der Waerden, *Modern Algebra*, N.Y. Ungar, New York, 1949, translated by Fred Blum.

[20] D.J. Ford, *On the Computation of the Maximal Order in a Dedekind Domain*, PhD thesis, Ohio State University, 1978.

[21] W. Fulton, *Algebraic Curves: An Introduction to Algebraic Geometry*, W.A.Benjamin Inc., New York, 1969.

[22] V.D. Goppa, Decoding and Diophantine Approximation, *Problems of Control and Information Theory*, 5:195–206, 1976.

[23] V.D. Goppa, Codes on Algebraic Curves, *Soviet Math. Doklady*, 24:170–172, 1981.

[24] V.D. Goppa, Algebraic Geometric Codes, *Mathematics of the USSR Izvestiya*, 21, no.1:75–91, 1983.

[25] V.D. Goppa, Codes and Information, *Russian Mathematical Surveys*, 39, no.1:87–141, 1984.

[26] V.D. Goppa, *Geometry and Codes*, Kluwer Academic Publishers, The Netherlands, 1988.

[27] D. Gorenstein, An Aritmetic Theory Of Adjoint Plane Curves, *Trans.Amer.Math.Soc.*, 72:414–436, 1952.

[28] D. Yu. Grigor'ev, *Computational Complexity in Polynomial Algebra*, Proceedings of the International Congress of Mathematicians, Berkeley, California, 1986.

[29] J.P Hansen, Codes on the Klein Quartic Ideals and Decoding, *IEEE Transactions on Information Theory*, 1T-33, no 6, 1987.

[30] R. Hartshorne, *Algebraic Geometry*, Springer Verlag, New York, 1977.

[31] E. Hecke, *Lectures on the Theory of Algebraic Numbers*, Springer Verlag, New York, 1981.

[32] T. Hungerford, *Algebra*, Springer Verlag, New York, 1974.

[33] Y. Ihara, Some remarks on the number of rational points of algebraic curves over finite fields, *J. Fac. Sci. Univ. Tokyo*, 28:721–724, 1981.

[34] R. Kannan, Solving Systems of Linear Equations over Polynomials, *Theoretical Computer Science*, 39:69–88, 1985.

[35] N. Katz, Sommes exponentielles, *Asterisque*, 79:1–209, 1980.

[36] N. Katz, *Gauss sums, Kloosterman sums and monodromy groups*, Annals of Math. Studies, No.116, Princeton University Press, Princeton, 1988.

[37] O. Keller, *Vorlesungen uber algebraische Geometrie*, Leipzig, 1874.

[38] D. Knuth, *The Art Of Computer Programming*, volume 2, Addison Wesley, Reading, MA, 1981.

[39] N. Koblitz, *A course in Number Theory and Cryptography*, Springer Verlag, New York, 1987.

[40] K. Kodaira, The theorem of Riemann-Roch on compact analytic surfaces, *Amer. J. Math.*, 73:813–875, 1951.

[41] G. Lachaud, Les codes géometrique de Goppa, *Asterisque, Seminaire Bourbaki*, 133-134, 1986.

[42] D. Le Brigand, Polynomial factorization using Brill Noether algorithm, *Lecture Notes In Computer Science*, 388:37–46, 1989.

[43] D. Le Brigand and J.J. Risler, Algorithm de Brill-Noether et Codes de Goppa, *Bull. Soc. math. France*, 116:231–253, 1988.

[44] A. Macdonald, *Introduction to Commutative Algebra*, Addison Wesley, Reading, Mass, 1969.

[45] C. Moreno, *Algebraic Curves over Finite Fields*, Cambridge University Press, New York, 1990.

[46] C. J. Moreno and O. Moreno, Exponential Sums and Goppa Codes: I, *Proc. of the AMS*, 111(2), 1991.

[47] C. J. Moreno and O. Moreno, Exponential Sums and Goppa Codes: I, *Proc. of the AMS*, 111(2), 1991.

[48] C.J. Moreno and O Moreno, *A report on exponential sums*, (preprint).

[49] C.J. Moreno and O. Moreno, Exponential Sums and Goppa Codes: II, *IEEE Trans. Info. Theory*, 1991, (to appear).

[50] C.J. Moreno and O. Moreno, Exponential Sums and Goppa Codes: II, *IEEE Trans. Info. Theory*, 1991, (to appear).

[51] C.J Moreno and O. Moreno, On the Number of Information Symbols and Covering Radius of Long Goppa Codes, *Presented at International Workshop on Algebraic and Combinatorial Coding Theory*, September 1988.

[52] D. Mumford, *Algebraic Geometry I, Complex Projective Varieties*, Springer Verlag, New York, 1976.

[53] M. Noether, *Göttinger Nachrighten*, page 267, 1871.

[54] M. Noether, Rationale Ausführungen der Operationen in der Theorie der algebräischen Functionen, *Mathematische Annalen*, 23:311–358, 1883.

[55] E. Picard and G. Simart, *Théorie des fonctions algébriques de deux variables indépendantes*, Gauthier-Villars, Paris, 1906.

[56] P. Samuel, Singularités des variétés algébriques, *Bull. Soc. Math. France*, 79:121–129, 1951.

[57] A. Schonhage, *Equation solving in terms of computational complexity*, Proceedings of the International Congress of Mathematicians, Berkeley, California, 1986.

[58] J.P. Serre, *Groupes Algebriques et Corps de Classes*, Hermann, Paris, 1959.

[59] J.P. Serre, *Local Fields*, Springer Verlag, New York, 1979.

[60] I.R Shafarevich, *Basic Algebraic Geometry*, Springer Verlag, New York, 1974.

[61] J. Teitelbaum, The Computational Complexity of the Resolution of Plane Curve Singularities, *Lecture Notes in Computer Science*, 358, July 1988.

[62] B.M. Trager, *Integration of Algebraic Functions*, PhD thesis, Massachusetts Institute of Technology, 1984.

[63] Tsfasman, Vladut, and Zink, Modular curves, Shimura curves and Goppa codes better than Varshamov-Gilbert bound, *Math. Nachr.*, 109:21–28, 1982.

[64] M. Tsfasman and S. Vladut, *Algebraic Geometric Codes*, Kluwer Academic Publishers, The Netherlands, 1991.

[65] J.H. van Lint, *Introduction to Coding Theory*, Springer Verlag, New York, 1982.

[66] J.H van Lint, Algebraic Geometric Codes, *Preprint*, 1988.

[67] J.H. van Lint and G.van der Geer, *Introduction to Coding theory and Algebraic Geometry*, Birkhauser Verlag, Basel, 1988.

[68] A. Vasquez, Rational desingularization of a curve defined over a finite field, *NYC Number Theory Seminar*, 1991, (to appear).

[69] S. Vladut and Manin Y., Linear Codes and Modular Curves, *Journal of Soviet Mathematics*, 30, no. 6:2611–2643, 1985.

[70] R.J. Walker, Reduction of the singularities of an algebraic surface, *Ann. of Math.*, 36:336–365, 1935.

[71] S. Winograd, *Arithmetic complexity of computations*, SIAM, 1980.

[72] J. Wolfmann, Recent results on coding and algebraic geometry, *Lecture Notes in Computer Science, Algebraic Algorithms and Error Correcting codes*, 229, 1985.

[73] O. Zariski, The reduction of the singularities of an algebraic surface, *Annals of Math.*, 40:639–689, 1939.