Integral Closures

by

Fidele Fouogang Ngwane

A dissertation submitted to the Graduate Faculty of
Auburn University
in partial fulfillment of the
requirements for the Degree of
Doctor of Philosophy

Auburn, Alabama
August 9, 2010

Keywords: Integral closure, Gröbner bases, normalization

Approved by:

Douglas A. Leonard, Chair, Professor of Mathematics
Kevin T. Phelps, Professor of Mathematics
Overtoun M. Jenda, Professor of Mathematics
Geraldo S. De Souza, Professor of Mathematics

Abstract

The q^{th}-power algorithm from Leonard [3], [4], and Leonard and Pellikaan [1] is a recent and efficient method of computing the integral closure of a ring in its field of fractions. Previously, the q^{th}-power algorithm has been used to compute integral closures over finite fields. In this dissertation, we use the q^{th}-power algorithm to compute integral closures over the rationals and number fields.

Acknowledgments

First, I am deeply grateful and indebted to my advisor Professor Douglas Leonard for directing the progress of this dissertation. He spent countless hours guiding my research, teaching me how to ask questions, how to answer them, and he introduced me to various computer algebra packages. His time, advice, regular support and encouragement were invaluable and are very much applauded.

My sincere appreciation is also extended to Professors Jenda, De Souza, Phelps, and Park, for their kindness in serving on my general and final examination committees.

The faculty, staff, and students at the Auburn University, Mathematics Department provided a very cordial and supportive environment. In particular, my gratitude goes to Professors Abebe, Rodger, Slaminka, Hoffman, Harris and Smith for ensuring rounded professional development.

I am also very grateful to my dad Andre Ngwane, to my mum Helen Ngwane, and to my siblings for their financial, material, family and spiritual support. Many relatives and wellwishers have made a strong impact on my life and I owe them gratitude.

My source of inspiration throughout this project has been my wife Axline Sanghapi and my daughter Melissa Ngwane. I thank them for their help, support, kindness and patience.

Finally, this work is joyfully dedicated to the Fountain and Source from which all good things and all true knowledge flow.

Table of Contents

List of Tables

Chapter 1

Introduction

Since integral closures are important in several areas of mathematics, it is not surprising that there are many implementations of the existing integral closure algorithms.

Our main goal is to understand the mathematics necessary to apply the q^{th}-power algorithm to give a highly structured presentation of an integral closure of a ring, and to extend the q^{th}-power algorithm to the rationals and number fields.

Chapter 1 gives the basic background for our work, including several key definitions and useful notation.

Chapter two talks about integral closures and existing algorithms. Given a type I curve, say f, an integral closure algorithm produces an $R-$module basis, $\{f_i\}$ for $0 \leq i \leq m$, where m is the maximum pole order, and all functions have poles at only one point called P_∞. Let $\mathcal{L}(mP_\infty)$ be the vector space consisting of the $\{f_i\}$ for $0 \leq i \leq m$. Note that $\mathcal{L}(mP_\infty)$ has functions with all possible pole orders $0, \ldots, m$ except for g gaps, where g is the genus of the curve, f. Then the generator and/or parity-check functions of a one-point AG code come from the vector space $\mathcal{L}(mP_\infty)$. Most integral closure algorithms compute the integral closure of a ring by repeatedly enlarging the ring until it stabilizes at the integral closure, as in the approach used by de Jong's algorithm, [9].

In the next chapter, we present the q^{th}-power algorithm. Unlike many existing algorithms, the q^{th}-power algorithm uses a different approach, starting with a module that contains the integral closure and repeatedly reducing it to a smaller module until it stabilizes at the integral closure. Here we compute the integral closures of several examples of towers of rings over finite fields.

The q^{th}-power algorithm is currently written for positive characteristic. Can it be extended to the other fields? The answer is yes. The fourth chapter extends the q^{th}-power algorithm to the rational field. This is done with the help of the extended Euclidean algorithm and the Chinese remainder theorem.

Chapter five extends the q^{th}-power algorithm to number fields, and presents some theorems and examples.

In chapter six we present various implementations. We discuss the outputs from various implementations.

Chapter seven presents some speed-up techniques which we use in our computations. Built-in commands in some of the existing computing packages such as Magma, Macaulay2 and Singular are not very efficient. They do unnecessary computations. We have been able write thoughtful and efficient code in place of some of the built-in commands. We end this chapter with some timing illustrations of our techniques compared to built-in commands.

The Final chapter focuses on towers. There are many towers that have very good coding theory properties. Unfortunately, most of these towers in their given form do not allow for evaluation at several points at which some of the variables have poles. We define new variables and transform these towers into type I curves.

1.1 Polynomial rings and monomial orderings

A finite field of order q, where $q = p^t,\ t \geqslant 1$ and p is a prime, will be denoted by $\mathbb{F}_q$, $\mathbb{F}_q^*$ will denote the non-zero elements of $\mathbb{F}_q$. Throughout, $P := \mathbb{F}[x_n, \ldots, x_1]$ (written as $\mathbb{F}[\underline{\mathrm{x}}]$ when convenient) will denote a polynomial ring over $\mathbb{F}$ in n independent variables $x_n, \ldots, x_1$, and $\mathbb{F}$ will be either the rational field , $\mathbb{Q}$, a finite field $\mathbb{F}_q$, or the algebraic closure of one of these fields. Let $\underline{x}^{\underline{\alpha}}$ be shorthand for the monomial $x_n^{\alpha_n} \cdots x_1^{\alpha_1}$, and let I denote an ideal in $\mathbb{F}[\underline{x}]$. Then $R := \mathbb{F}[\underline{x}]/I$ is a quotient ring, and $S := R[\underline{y}]/J$ is a ring extension of R. We are interested in the integral closure $ic(S) := \overline{R}[\underline{z}]/\overline{J}$ of S, and wish to view it as an affine P-algebra.

Given a polynomial ring P, we want a presentation of $ic(S)$ relative to a finite P-module generating set $y_0 := 1, y_1, \ldots, y_{s-1}$, so that $\overline{J}$ has a minimal, reduced Gröbner basis with elements of the form $y_i y_j - \sum_k c_{i,j,,k} y_k,\ c_{i,j,k} \in P$ defining multiplication, and possibly some elements of the form $a_{j,i} y_i - a_{i,j} y_j - \sum_{k \neq i,j} b_{i,j,,k} y_k, \quad a_{j,i}, a_{i,j}, b_{i,j,k} \in P$ if the $P-$module generators are not independent over P. Given a polynomial ring $\mathbb{F}[\underline{x}]$, let $\mathcal{M}on_n := \{\underline{x}^{\underline{\alpha}} : \underline{\alpha} \in \mathbb{N}^n\}$ be the set of all possible monomials in P in the variable $\underline{x}$.

A **global monomial ordering** satisfies the conditions that

1. it is a total ordering on $\mathcal{M}on_n$
2. it is a well-ordering on $\mathcal{M}on_n$
3. $\underline{x}^{\underline{\alpha}} \succ \underline{x}^{\underline{\beta}}$ implies $\underline{x}^{\underline{\gamma}} \underline{x}^{\underline{\alpha}} \succ \underline{x}^{\underline{\gamma}} \underline{x}^{\underline{\beta}}$.

The importance of a monomial ordering on P is that any polynomial has a unique representation (written from highest to lowest terms).

Definition 1.1. *(See Cox et al [13] page 61.) Let $f = \sum_{\underline{\alpha}} a_{\underline{\alpha}} \underline{x}^{\underline{\alpha}}$ a nonzero polynomial in $\mathbb{F}[\underline{x}]$ and let $\succ$ be a monomial order:*

1. *The* **multidegree** *of f is multidegree(f) = max$(\underline{\alpha} \in \mathbb{Z}^n_{\geq 0} : a_{\underline{\alpha}} \neq 0)$ (the maximum is taken with respect to $\succ$).*
2. *The* **leading coefficient** *of f is* $\mathbf{LC}(f) = a_{multideg(f)} \in \mathbb{F}$.
3. *The* **leading monomial** *of f is* $\mathbf{LM}(f) = \underline{x}^{multideg(f)}$.
4. *The* **leading term** *of f is* $\mathbf{LT}(f) = LC(f) \cdot LM(f)$.

We illustrate this with the following; Let $f = -5x^3+7x^2z^2+4xy^2z+4z^2$, and let $\succ$ denote the monomial order. Then multideg$(f) = (3,0,0)$, LC$(f) = -5$, LM$(f) = x^3$, LT$(f) = -5x^3$.

Definition 1.2. *[13]: Let $\underline{\alpha} = (\alpha_n, \ldots, \alpha_1)$ and $\underline{\beta} = (\beta_n, \ldots, \beta_1) \in \mathbb{Z}^n_{\geq 0}$. We say that $\underline{\alpha} \succeq_{\mathbf{lex}} \underline{\beta}$ if, in the vector difference $\underline{\alpha} - \underline{\beta} \in \mathbb{Z}^n$, the leftmost nonzero entry is positive. We* *will write* $\underline{x}^{\underline{\alpha}} \succeq_{lex} \underline{x}^{\underline{\beta}}$ *if* $\underline{\alpha} \succeq_{lex} \underline{\beta}$. *The variables* $x_n, \ldots, x_1$ *are ordered by the lex ordering* $(1,0,\ldots,0) \succeq_{lex} (0,1,0,\ldots,0) \succeq_{lex} \cdots \succeq_{lex} (0,0,\ldots,0,1)$, *so* $x_n \succeq_{lex} \cdots \succeq_{lex} x_1$.

Lexicographic order (*lex*) therefore orders according to the highest power of the most significant indeterminate, using less significant indeterminates to break ties.

Definition 1.3. *[13]: Let* $\underline{\alpha} = (\alpha_n, \ldots, \alpha_1)$ *and* $\underline{\beta} = (\beta_n, \ldots, \beta_1) \in \mathbb{Z}^n_{\geq 0}$. *We say that* $\underline{\alpha} \succeq_{\mathbf{grevlex}} \underline{\beta}$ *if,* $\mid \underline{\alpha} \mid = \sum_{i=1}^{n} \alpha_i > \mid \underline{\beta} \mid = \sum_{i=1}^{n} \beta_i$ *or* $\mid \underline{\alpha} \mid = \mid \underline{\beta} \mid$ *and the rightmost nonzero entry of* $\underline{\alpha} - \underline{\beta} \in \mathbb{Z}^n$ *is negative.*

The variables $x_n, \ldots, x_1$ are ordered by the lex ordering $(1,0,\ldots,0) \succeq_{\text{grevlex}} (0,1,0,\ldots,0) \succeq_{\text{grevlex}}, \ldots, \succeq_{\text{grevlex}} (0,0,\ldots,0,1)$, so $x_n \succeq_{\text{grevlex}}, \ldots, \succeq_{\text{grevlex}} x_1$. Graded reverse lexicographic order **(grevlex)** orders by total degree first, then breaks ties using reverse lexicographic order. The most widely used monomial orderings are the **lex**$(x_n \succ \cdots \succ x_1)$ and the the **grevlex**$(x_n \succ \cdots \succ x_1)$. We note that **lex** and **grevlex** give the same ordering on the variables $x_n, \ldots, x_1$. Let us illustrate both orderings with the following: let $f = 4xy^2z + 4z^2 - 5x^3 + 7x^2z^2 \in \mathbb{F}[x,y,z]$. Then with respect to the **lex** ordering, we have that $f = -5x^3 + 7x^2z^2 + 4xy^2z + 4z^2$, and with respect to the **grevlex** ordering, we have that $f = 4xy^2z + 7x^2z^2 - 5x^3 + 4z^2$. The following is an example from Cox et al [13]. Consider the monomials xy^2z, z^2, x^3, and x^2z^2. Using the indeterminate order $x \succ y \succ z$, here's how some of the monomial orders above would order these four monomials:

$Lex: x^3 \succ x^2z^2 \succ xy^2z \succ z^2$ (power of x dominates).

$Grevlex: xy^2z \succ x^2z^2 \succ x^3 \succ z^2$ (total degree dominates; lower power of z broke tie).

But any global monomial ordering has at least one non-singular matrix A (with entries from $\mathbb{N}$) that defines it in the sense that

$$\underline{x}^{\underline{\alpha}} \succ \underline{x}^{\underline{\beta}} \quad \text{if and only if} \quad A\underline{\alpha}^t \succ_{lex} A\underline{\beta}^t.$$

1.2 Ideals and Gröbner bases

Let I be an ideal of the ring $R := P[\underline{y}]$. I is necessarily finitely generated by some $f_1, f_2, \ldots, f_m$; so let $I := \langle f_1, \ldots, f_m \rangle = \left\{ \sum r_i f_i : r_i \in R \right\}$ with $f_1, \ldots, f_m$ called **generators** of I. $\mathcal{B} := (f_1, \ldots, f_m)$ is an **ordered Gröbner basis** for I if and only if each r in R has a unique remainder, called the **normal form** of f modulo I, (written $NF(f, I)$), after division by elements of $\mathcal{B}$ in any order.

Definition 1.4. *(See page 46 of [15].) Let $\mathcal{G}$ denote the set of all finite elements $G \subset R$. A map*

$$NF : R \times \mathcal{G} \longrightarrow R, \quad (f, G) \mapsto NF(f, G),$$

is called a **normal form** *on R if, for all $G \in \mathcal{G}$:*

(1) $NF(0, G) = 0$, and, for all $f \in R$ and $G \in \mathcal{G}$,

(2) $NF(f, G) \neq 0 \;\Rightarrow\; LM(NF(f, G)) \notin L(G) := \langle LM(g) |\; g \in G \setminus \{0\} \rangle$,

(3) If $G = \{g_1, \ldots, g_s\}$, then $r := f - NF(f, G)$ has a standard representation with respect to G, that is, either $r = 0$, or $r = \sum_{i=1}^{s} a_i g_i$, $\; a_i \in R$, satisfying $LM(f) \succeq LM(a_i g_i)$ for all i such that $a_i g_i \neq 0$. $NF(f, G)$ is called a **reduced normal form***, if, moreover, $NF(f, G)$ is reduced with respect to G.*

Let $L(I) := \{LM(f) : f \in I\}$ be the ideal of **leading monomials** of I. Any monomial not in $L(I)$ is called a **standard monomial**, the set of such is often referred to as the **footprint or Δ-set**, a (vector space) basis for the set of all normal forms $NF(f, I)$. [One of our speed-up techniques involves efficient computation of $NF(f^q, G)$ for large primes q. Such normal forms are used repeatedly in most of our computations.]

Definition 1.5. *[15]: Let $G \subset \mathbb{F}[\underline{x}]$ be any subset.*

(1) G is called **minimal** *if $0 \notin G$ and $LM(g) \nmid LM(f)$ for any two elements $f \neq g$ in G. We note that G is called* **interreduced** *if $LM(g) \nmid$ any monomial of f.*

(2) $f \in R$ is called reduced with respect to G if no monomial of f is contained in the ideal,

$L(G)$, generated by the leading monomials of G. $L(G)$ is called the **leading ideal** *of G.*

(3) Let $I \subset \mathbb{F}[\underline{x}]$ be an ideal and let $\succ$ be a monomial ordering on $\mathcal{M}_n(\underline{x})$. A finite set $G \subset \mathbb{F}[\underline{x}]$ is called a **Gröbner basis** *of I if $G \subset I$, and $LM(I) = LM(G)$. That is, G is a Gröbner basis if the leading monomials of the elements of G generate the leading ideal of I, or, in other words, if for any $f \in I \setminus \{0\}$ there exists a $g \in G$ satisfying $LM(g)|\ LM(f)$.*

Definition 1.6. *[13]: Let $f, g \in R \setminus \{0\}$ with $LM(f) = \underline{x}^{\underline{\alpha}}$ and $LM(g) = \underline{x}^{\underline{\beta}}$, respectively. Set $\underline{\gamma} := lcm(\underline{\alpha}, \underline{\beta}) := (max(\alpha_1, \beta_1), \ldots, max(\alpha_n, \beta_n))$ and let $lcm(\underline{x}^{\underline{\alpha}}, \underline{x}^{\underline{\beta}}) := \underline{x}^{\underline{\gamma}}$ be the least common multiple of $\underline{x}^{\underline{\alpha}}$ and $\underline{x}^{\underline{\beta}}$. We define the s-***polynomial** of f and g (denoted by $spoly(f, g)$), to be*

$$spoly(f, g) := \underline{x}^{\underline{\gamma}-\underline{\alpha}} f - \frac{LC(f)}{LC(g)} \underline{x}^{\underline{\gamma}-\underline{\beta}} g.$$

If $LM(g)$ divides $LM(f)$, say $LM(g) = \underline{x}^{\underline{\beta}}$, $LM(f) = \underline{x}^{\underline{\alpha}}$, then the $s-$polynomial is given by

$$spoly(f, g) := f - \frac{LC(f)}{LC(g)} \underline{x}^{\underline{\alpha}-\underline{\beta}} g,$$

and $LM(spoly(f, g)) \prec LM(f)$.

Buchberger's algorithm, found in most literature on the subject including [13], [27], is suitable for computing Gröbner bases and it does the computations via s-polynomials. Many characterization of Gröbner bases can be found in the literature.

1.3 P-algebras

Definition 1.7. *[14]: A ring R is called a* **domain** *if 0 is prime. Let P be a ring. Some authors define a* **P-algebra** *to be a commutative ring R such that P is a subring of R and the unity of P is also the unity in R. A commutative ring R is called a* **reduced ring** *if it has no non-zero nilpotent elements. A reduced, finitely-generated P-algebra is called an* **affine P-algebra***, or when it is not necessary to refer to the ring P, it is simply called an* **affine ring.** *If the ring is a domain, then it is called an* **affine domain***.*

This is the definition presented in [[14], page 35]. However, we shall consider the following definitions in this study.

Definition 1.8. *$R := P[\underline{y}]/I$ is called a* **quotient ring**. *If there are no zero-divisors, it is also called an* **affine domain** *or* **affine P-algebra**. *It is always possible to adjoin new variables so that there is a Gröbner basis in which all the relations induced are of degree at most 2. We call call such quotient rings* **strictly affine P-algebras** *in the sense that all the P-quadratic relations describe a P-algebra multiplication, and any P-linear relations are called* **P-syzygies** *amongst the dependent variables.*

Definition 1.9. *[13]: Let K be a field, and let $f_1, \dots, f_s$ be polynomials in the polynomial ring $K[x_1, \dots, x_n]$. Then $V(f_1, \dots, f_s) := \{(a_1, \dots, a_n) \in K^n : f_i(a, \dots, a_n) = 0,\ \ 1 \leq i \leq s\}$ is called the* **affine variety** *defined by $f_1, \dots, f_s$. An affine variety $V(f_1, \dots, f_s) \subset K^n$ is thus the set of all solutions of the system of equations $f_i(a, \dots, a_n) = \cdots = f_s(a, \dots, a_n) = 0$. An* **algebraic variety** *is the set of solutions of a system of polynomial equations.*

1.4 Order functions and order domains

Definition 1.10. *(see Geil and Pellikan, [6].) Let $(\Gamma, \prec)$ be a well-order, with its minimal element denoted by 0. An* **order function** *on an P-algebra R is a surjective function*

$$\rho : R \longrightarrow \Gamma \cup \{-\infty\},$$

such that the following conditions hold:

1. $\rho(f) = -\infty$ if and only if $f = 0$;

2. $\rho(af) = \rho(f)$ for all nonzero $a \in \mathbb{F}$;

3. $\rho(f + g) \preceq max\{\rho(f), \rho(g)\}$;

4. if $\rho(f) \prec \rho(g)$ and $h \neq 0$, then $\rho(fh) \prec \rho(gh)$;

5. if f and g are nonzero and $\rho(f) = \rho(g)$, then there exists a nonzero $a \in \mathbb{F}$ such that $\rho(f - ag) \prec \rho(g)$ for all $f, g, h \in R$.

Definition 1.11. *A P-affine algebra, R, on which there is defined an order function is called an* **order domain over** P*, or simply an* **order domain***.*

Definition 1.12. *[4]: Let $S = R/J$ be an affine domain. A function*

$$wt_S := R \longrightarrow \mathbb{N}_0^n \cup \{-\infty\}$$

(with $-\infty \prec \underline{\alpha}$ for all $\underline{\alpha} \in \mathbb{N}_0^n$) is a **weight function** *on S iff:*

1. $wt_S(f) = -\infty$ *iff* $f \in J$*;*

2. $wt_S(f) = \underline{0}$ *iff* $f = c + J, \quad c \in \mathbb{F}\backslash\{0\}$*;*

3. $wt_S(fg) = wt_S(f) + wt_S(g)$ *for all* $f, g \notin J$*;*

4. $wt_S(\alpha f + \beta g) \preceq max\{wt_S(f), wt_S(g)\}$ *for all* $\alpha, \beta \in \mathbb{F}$*;*

5. *if* $wt_S(f) = wt_S(g) \succ \underline{0}$, *then* $wt_S(f - \lambda g) \prec wt_S(g)$ *for a unique* $\lambda \in \mathbb{F}$.

Let A_P be a non-singular n x n **weight-over-grevlex** matrix over $\mathbb{N}_0$ that defines a global monomial ordering on P, the default here being the grevlex ordering, $x_n \succ \cdots \succ x_1$. Let A_{P_k} be a submatrix of A_P, consisting of the first k rows of A_P, where k is the number of the free variables in f, with $J :=< f >$. Then A_P defines a weight function given by $wt_P(\underline{x}^{\underline{\alpha}}) := (A_{P_k}) \cdot \underline{\alpha}^t$, with distinct monomials obviously having distinct weights. Suppose for example that

$$A_R := \begin{pmatrix} 7 & 5 & 3 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

is a weight-over-grevlex matrix that defines a monomial ordering on $R := \mathbb{F}[\underline{y}]$. Then $wt(\underline{y}^{\underline{\gamma}}) = (\begin{array}{ccc} 7 & 5 & 3 \end{array})(\underline{\gamma})^t$. Also $\underline{x}^{\underline{\alpha}} \succ_{A_p} \underline{x}^{\underline{\beta}}$ if and only if $A_p\underline{\alpha}^t \succ_{lex} A_p\underline{\beta}^t$.

An alternative definition of a weight function is found in [[1], page 481]. The conditions of this definition can restated in terms of leading monomials (LM) of normal forms (NF) of elements as follows:

$LM(NF(\lambda f)) = LM(NF(f))$ for $0 \neq \lambda \in \mathbb{F}$.

If $LM(NF(g)) \preceq LM(NF(f))$ and $f \neq g$, then $LM(NF(f-g)) \preceq LM(NF(f))$;
and if $LM(NF(g)) \prec LM(NF(f))$, then $LM(NF(f-g)) = LM(NF(f))$.
$LM(NF(fg)) = LM(NF(LM(f), LM(g)))$.
If $LM(NF(f)) = LM(NF(g))$, then

$$LM\left(\frac{NF(f)}{LC(NF(f))} - \frac{NF(g)}{LC(NF(g))}\right) \prec LM(NF(f)).$$

A weight function, say ρ, can be extended to a function on quotients by defining $\rho(f/g) := \rho(f) - \rho(g) \in \mathbb{Z}^r$. The q^{th}-power map acts on such elements and thus it is important to have the extended definition of a weight function, see [1], page 482. Weight functions are very essential in our integral closure computations, as they are used with the earlier-mentioned monomial orderings to produce new monomial orderings.

1.5 Integral extensions and type I curves

There are several definitions of an integral element. We will present some of them here.

Definition 1.13. *[28]: Let R be a ring and S an R-algebra containing R. An element $x \in S$ is said to be* **integral** *over R if there exists an integer n and elements $r_1, \ldots, r_n$ in R such that*

$$x^n + r_1x^{n-1} + \cdots + r_{n-1}x + r_n = 0.$$

The above equation is called an equation of integral dependence of x over R of degree n. It is important to note here that equations of integral dependence are not unique if the function used to define the integral extension is reducible.
Indeed let S be the ring $\mathbb{Z}[t]/(t^2 - t^3)$, where t is a variable over $\mathbb{Z}$. Let R be the subring of S generated over $\mathbb{Z}$ by t^2. Then $t \in S$ is integral over R and it satisfies the equations
$x^2 - t^2 = 0$ and $x^2 - xt^2 = 0$ in x.
This is not surprising as the function $f(t) = t^2 - t^3$ is reducible. In our definition, we will require $f(t)$ to be irreducible.

Definition 1.14. *[30]: Suppose R is a subring of the commutative ring S with $1 = 1_s \in R$.*

1 *An element $s \in S$ is* **integral** *over R if s is the root of a monic polynomial in $R[x]$.*

2 *The ring S is an* **integral extension** *of R or just* **integral** *over R if every $s \in S$ is integral over R.*

3 *The* **integral closure** *of R in S is the set of all elements of S that are integral over R.*

We will consider the integral closure of an integral domain, R, in its field of fractions, $Q(R)$. We shall consider the following as our definition of an integral element and integral closure.

Definition 1.15. *(Integral element) [1]: Let S be a domain and R a subdomain of S. An element $y \in S$ is said to be* **integral** *over R if and only if there exists a monic polynomial $\phi_y(T) \in R[T]$ such that $\phi_y(y) = 0$.*

Feng and Rao introduced type I curves to be curves that satisfy equations of the form

$$x^a + y^b + g(x, y) = 0, \ gcd(a, b) = 1, \ a > b > \deg(g(x, y)).$$

We shall consider the follow as our definition of type I integral extensions.

Definition 1.16. *[4]: Let $f(T) := \sum_{i=0}^{d} f_i T^i \in P[T]$ be a monic, absolutely irreducible polynomial of degree d. Let the affine domain $S := P[y]/J$ be an integral extension for $J := \langle f(y) \rangle$. To extend wt_P to a weight function wt_S on S, define $wt_S(\underline{x}^{\underline{\alpha}}) := d \cdot wt_P(\underline{x}^{\underline{\alpha}})$, and $wt_S(y) := max\{\frac{wt_S(f_i)}{d-i} : 0 \leq i < d\}$. If the max is taken on at only one value of i, the value is $i = 0$, $LM(f_0) := \underline{x}^{\underline{\alpha}}$, and $gcd\{d, \ gcd\{\alpha_i : 0 \leq i < d\}\} = 1$, then S is said to be a* **type I integral extension.**

Let A_P be a non-singular n x n weight-over-grevlex matrix over $\mathbb{N}_0$ that defines a global monomial ordering on P, with the default here being the grevlex ordering, $x_n \succ \cdots \succ x_1$. The monomial ordering, **weight-over-grevlex**, on the extension S of P above, is given by

$$A_S := \begin{pmatrix} wt_S(y)^t & dA_P \\ 1 & \underline{0} \end{pmatrix}.$$

Definition 1.17. *(Integral closure) [1]: Let S be a domain and R a subdomain of S. The* **integral closure of R in S** *is defined to be $ic_S(R) := \{s \in S | s \text{ is integral over } R\}$. When S is the field of fractions of R, we simply write $ic(R)$ instead of $ic_S(R)$. R is integrally closed in S if and only if $R = ic_S(R)$. Moreover, $ic_S(R)$ is a ring if S is a ring.*

Example 1.1. *Let $P := \mathbb{F}_2[f_3]$ and $R := P[f_5]/\langle f_5^3 + f_3^5 + f_5 f_3 \rangle$. Then* **integral closure of** *R in its field of fractions is given by $ic(R) := \mathbb{F}_2[f_7, f_5; f_3]/\langle f_7^2 + f_5 f_3^3 + f_7, f_7 f_5 + f_3^4 + f_5, f_5^2 + f_7 f_3 \rangle$, where $f_7 := \dfrac{f_5^2}{f_3}$.*

The next chapter presents some theorems about properties of integral elements and integral closures. It also presents a version of de Jong's algorithm that is used by some to compute integral closures.

Chapter 2

Integral Closures

Let $\underline{x} := (x_n, \ldots, x_1)$. Let $\mathbb{F}$ be a field and let $P := \mathbb{F}[\underline{x}]$ be a polynomial ring of free variables. Let $R := P[y]/\langle f(y) \rangle$ be a simple integral extension of P, with $deg(f, y) = m$, and let $Q(R)$ be the quotient ring of R. Let $\overline{u} := (u_r, \ldots, u_1, u_0 := 1)$, $\underline{u} := (u_r, \ldots, u_1)$ and let $ic(R) = \mathbb{F}[\underline{u}; \underline{x}]/\overline{J}$ be the integral closure of R in $Q(R)$, where $\overline{J}$ has a minimal, reduced Gröbner basis consisting of P-quadratic relations defining the P-algebra multiplication and P-linear relations if the P-module generators are not free over P.

The goal of the next theorem is to help show that the integral closure of a ring is a ring.

Theorem 2.1. *[30]: Let R be a subring of the commutative ring S with $1 \in R$ and let $s \in S$. Then the following are equivalent:*

(1) s is integral over R,

(2) $R[s]/ < f(s) >$ is a finitely-generated R-module and

(3) $s \in T$ for some subring T, that is a finitely-generated R-module.

Proof: Suppose first that (1) holds and let s be a root of the monic polynomial

$$f(x) := x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in R[x].$$

Then

$$s^n = -(a_{n-1}s^{n-1} + a_{n-2}s^{n-2} + \cdots + a_0)$$

and so s^n, and hence all higher powers of s, can be expressed as R-linear combinations of $s^{n-1}, \ldots, s, 1$. So $R[s]/ < f(s) >:= R1 + Rs + \cdots + Rs^{n-1}$ is finitely generated as an R-module, which gives (2).

If (2) holds then (3) holds with $T = R[s]/ < f(s) >$.

Suppose that (3) holds and let $v_1, v_2, \ldots, v_n$ be a finite generating set for T. Then for $i = 1, 2, \ldots, n$ the element sv_i is an element of T since T is a ring, and so can be written as an R-linear combination of $v_1, \ldots, v_n$: $\quad sv_i = \sum_{j=1}^{n} a_{ij}v_j,$ for $1 \leq i \leq n$. So $0 = \sum_{j=1}^{n}(\delta_{ij}s - a_{ij})v_j$, where δ_{ij} is the Kronecker delta. If B is the $n \times n$ matrix whose i, j entry is $\delta_{ij}s - a_{ij}$, and v is the $n \times 1$ column vector whose entries are $v_1, \ldots, v_n$, then these equations are simply of the form $B\underline{v} = \underline{0}$. It follows from Cramer's Rule that $det(B)v_i = 0$ for all i. But $B = sI - A$, where A is the matrix (a_{ij}). Thus s is a root of the monic polynomial $\det(xI - A) \in R[x]$ (the characteristic polynomial of A), and so s is a root of a monic polynomial with coefficients in R, which gives (1), completing the proof. □

Corollary 2.1. *Let $R \subseteq S$ be as in Theorem 2.1 above and let $s, t \in S$*

(1) if s and t are integral over R then so are $s \pm t$ and st.

(2) The integral closure of R in S is a subring of S containing R.

(3) Integrality is transitive: let S be a subring of T; if T is integral over S and S is integral over R, then T is integral over R.

Proof: Let s and t be integral over R. By Theorem 2.1 both $R[s]$ and $R[t]$ are finitely-generated R-modules, say

$$R[s]/ < f(s) > := (Rs_1 + Rs_2 + \cdots + Rs_n)$$

$$R[t]/ < f(t) > := (Rt_1 + Rt_2 + \cdots + Rt_m).$$

Then

$$R[s, t]/ < f(s, t) > := (Rs_1t_1 + \cdots + Rs_it_j + \cdots + Rs_nt_m)$$

is a ring containing $s \pm t$ and st that is also a finitely-generated $R-$module. Hence $s \pm t$ and st are also integral over R, which proves (1) and also (2).

To prove (3), let $t \in T$. Since t is integral over S, it is the root of some monic polynomial $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in S[x]$. Since $a_i \in S$ is integral over R, each ring $R[a_i]/ < f(a_i) >$ is a finitely-generated R-module and so the ring $R_1 := R[a_0, a_1, \ldots, a_{n-1}]/ < f(a_0, a_1, \ldots, a_{n-1}) >$ is also a finitely-generated R-module. Since the monic polynomial $p(x)$ has its coefficients in R_1, t is integral over R_1 and it follows that the ring $R_1[t]/ < f(t) >:= R[a_0, a_1, \ldots, a_{n-1}, t]$ is a finitely-generated R-module. By Theorem 2.1, this means that t is integral over R, which gives (3).$\square$

2.1 de Jong's algorithm

de Jong's algorithm has been implemented in Magma, Singular and Macaulay2 to compute integral closures. The approach is to produce a nested sequence of rings $R := R_0 \subset \cdots \subset R_L = R_{L+1} = ic(R)$ with a presentation that is based on elements of the field of fractions, $Q(R)$, used to define the rings involved. Below is a version of de Jong's algorithm:

Algorithm: (See page 275, [9] for details.)

INPUT: A reduced Noetherian ring R.

OUTPUT: The normalization $\widetilde{R}$ of R.

STEP 1: Determine a non-zero ideal I with $NNL \subset V(I)$.

STEP 2: Take a non-zero element $f \in I$, and compute $J := Ann(f)$. If $J = 0$, GOTO STEP 4.

STEP 3: Put $R := R/Ann(J) \oplus R/J$ and GOTO STEP 1.

STEP 4: Compute the radical $\sqrt{I}$ of I. Put $I := \sqrt{I}$.

STEP 5: Compute $Hom_R(I, I)$. If $R = Hom_R(I, I)$ then put $\widetilde{R} := R$ and STOP.

STEP 6: Set $R := Hom_R(I, I)$ and GOTO STEP 1.

In Singular ([15] page 224), the idea to compute $ic(R)$ is to enlarge the ring R to the endomorphism ring $R' = Hom_R(J, J)$ for a suitable ideal J such that $R' \subset ic(R)$, and repeat the process until it stabilizes at the integral closure $ic(R)$.

We now present the theory that is used in SINGULAR to produce the increasing sequence of rings that contains the initial ring and is also contained in the integral closure.

Theorem 2.2. *(See [15], page 192 for details.) Let A, B be rings.*

(1) If $\varphi : A \longrightarrow B$ is a finite extension, then it is integral. More generally, if $I \subset A$ is an ideal and M a finitely-generated B-module then any $b \in B$ with $bM \subset IM$ satisfies a relation

$$b^p + a_1 b^{p-1} + \cdots + a_p = 0, \text{ with } a_i \in \ A.$$

(2) If B is a finitely-generated A-algebra of the form $B = A[b_1, \ldots, b_n]$ with $b_i \in B$ integral over A then B is finite over A.

Theorem 2.3. *(See Lemma 3.6.1 of [15].) Let R be a reduced Noetherian ring and $J \subset A$ an ideal containing a non-zerodivisor x of R. Then there are natural inclusions of rings*

$$R \subset Hom_R(J, J) \cong \frac{1}{x} \cdot (xJ : J) \subset ic(R)$$

Proof: For $a \in R$, let $m_a : J \longrightarrow J$ denote the multiplication by a. If $m_a = 0$, then $m_a(x) = ax = 0$ and, hence, $a = 0$, since x is a non-zerodivisor. Thus $a \mapsto m_a$ defines an inclusion $R \subset Hom_R(J, J)$.

It is easy to see that $\varphi \in Hom_R(J, J)$ the element $\varphi(x)/x \in Q(R)$ is independent of x: for any $a \in J$ we have $\varphi(a) = (1/x) \cdot \varphi(xa) = a \cdot \varphi(x)/x$, since φ is R-linear.

Hence $\varphi \mapsto \varphi(x)/x$ defines an inclusion $Hom_R(J, J) \subset Q(R)$ mapping $x \cdot Hom_R(J, J)$ into $xJ : J = \{b \in R \mid bJ \subset xJ\}$. The latter map is also surjective, since any $b \in xJ : J$ defines, via multiplication by b/x, an element $\varphi \in Hom_R(J, J)$ with $\varphi(x) = b$. Since x is a non-zerodivisor, we obtain the isomorphism $Hom_R(J : J) \cong (1/x) \cdot (xJ : J)$.

It follows from [Theorem 2.2] that any $b \in xJ : J$ satisfies an integral relation $b^p + a_1 b^{p-1} + \cdots + a_0 = 0$ with $a_i \in < x^i >$. Hence, b/x is integral over R, showing $\frac{1}{x} \cdot (xJ : J) \subset ic(R)$.□

Example 2.1. *(See example 3.6.8 of [15].) Let* $R := \mathbb{F}[x,y]/\langle x^2 - y^3 \rangle$ *and* $J := \langle x, y \rangle$*. Then* $x \in J$ *is a non-zerodivisor in* R *with* $xJ : J = x\langle x, y \rangle : \langle x, y \rangle = \langle x, y^2 \rangle$*, therefore,* $Hom_R(J, J) = \langle 1, y^2/x \rangle$*. Thus we have* $R \subset \langle 1, y^2/x \rangle \cong \dfrac{1}{x} \cdot (xJ : J) \subset ic(R)$*.*

Chapter 3

The q^{th}-power algorithm in positive characteristic

In this chapter, we present the q^{th}-power algorithm to compute the integral closure of rings over the finite fields. Most of our rings in this section will be from towers.

3.1 q^{th}-power algorithm

The q^{th}-power algorithm approach is to begin with a dual module $M^{(0)} := \Delta^{-1}R$ and produce a sequence of P-modules $\Delta^{-1}R := M^{(0)} \supset \cdots \supset M^{(L)} = M^{(L+1)} = ic(R)$ where

$$M^{(L+1)} := \left\{\Delta^{-1}f \in M^{(L)} : (\Delta^{-1}f)^q \in M^{(L)}\right\}$$

q^{th}-power algorithm:

Let $f(y,x)$ be a polynomial of degree m in $\mathbf{F}[y,x]$, with y being the dependent variable, x the independent variable, weight$(y) = r$ and weight$(x) = s$. Let $I =$ ideal$< f >$.

(1) (Δ and weights):

(a) Compute the conductor element, Δ, (via computing a Gröbner basis of the ideal generated by minors of the Jacobian matrix of a Gröbner basis of I). [There are other ways to compute Δ.]

(b) $\beta := (q^n)\cdot$Totaldegree(LT(Δ)) $+ 1$

(c) maxweight $:= \displaystyle\sum_{i=0}^{m-1} \mathrm{wt}(y^i)(q-1) + \beta$

(2) (Initialization):

Let G be a list from 0 to maxweight with entries all zeros. set $nextG := G$. Set $G[0] := 1 \in \mathbf{F}[x,y]$, $F[0] := 1 \in \mathbf{F}[x,y]$ and $H[0] := 0 \in \mathbf{F}[x,y]$.

For $i = 1$ to $m-1$, $G[i \cdot r] := G[(i-1)\cdot r]\cdot y$, $F[i\cdot r] := NormalForm(F[(i-1)\cdot r]\cdot y^q, I)$,

$H[i \cdot r] := NormalForm(H[(i-1) \cdot r] \cdot y^q, I)$. $\quad StartG := G$

While $StartG \neq nextG$

(3) (Reduction):

From smallest weight $j = 1$ to maxweight, do (a) (Element of $nextG$): If $F[j] = 0$ then $nextG[j] := G[j]$.

(b) $(F[j]/(StartG[i] \cdot LT(\Delta)),\ i < j)$: If $F[j]$ divides $(StartG[i] \cdot LT(\Delta))$ with quotient say, quo, then

$G[j+s] := G[j] \cdot x, \quad F[j+s] := F[j] \cdot x^q - (\Delta \cdot StartG[i] \cdot quo), \quad H[j+s] := H[j] \cdot x^q + (StartG[i] \cdot quo)$.

(c) ($LM(F[j])$ already exist): If $LM(F[i]) = LM(F[j]),\ i < j$, then

$\alpha := LC(F[j])/LC(F[i]), \quad G[j+s] := G[j] \cdot x - \alpha \cdot G[j], \quad F[j+s] := F[j] \cdot x^q - \alpha \cdot F[j], \quad H[j+s] := H[j] \cdot x^q - \alpha \cdot H[j]$.

(d) (If (a) $-$ (c) fail): If (a) $-$ (c) fail, then

$G[j+s] := G[j] \cdot x, \quad F[j+s] := F[j] \cdot x^q, \quad H[j+s] := H[j] \cdot x^q$.

(4) (Next pass):

$StartG := nextG$ and $nextG := G$, $\quad$ F $:= H \cdot D, \quad H := 0, \quad G := 0$, and repeat steps (a) $-$ (d) in (3) above.

Until $StartG = nextG$

Definition 3.1. *[1]: Let $\overline{R} = R_r := \mathbf{F}[x_r, \ldots, x_1]$ be a ring with field of fractions $F_r := \mathbf{F}(x_r, \ldots, x_1) := \{a/b \mid a, b \in \overline{R},\ b \neq 0\}$. For $r < j \leq n$, recursively define simple field extensions $F_j := F_{j-1}(x_j)$ with $\phi_j(x_j) = 0$ for $\phi_j(T) \in F_{j-1}[T]$ irreducible; and subdomains $R_j := ic_{F_j}(R_{j-1})$. Let $\mathcal{F}_j := ideal\langle \mathcal{F}_{j-1}, \phi_j(x_j)\rangle$. This sequence of domains $(R_j)_{j=r}^n$ (with each R_j integrally closed in the corresponding field of fractions F_j) is called an integral tower (of rank r) if and only if*

1.

$$\phi_j(x_j) := x_j^{m_j} + u_j \prod_{i=1}^{j-1} x_i^{\alpha_{i,j}} + g_j(x_j, \ldots, x_1) \in R_{j-1}[x_j],$$

is (monic) irreducible, with $0 \neq u_j \in \mathbf{F}_q$*;*

2. $gcd(\phi_j(x_j), \phi'_j(x_j)) \in \overline{R} := R_r$*;*

3. The weight functions, given recursively by $W_r := J_r$*, and* $W_j := \binom{\underline{\alpha}_j W j-1}{m_j W_{j-1}}$*, with* $\underline{\alpha}_j := (\alpha_{j-1,j}, \ldots, \alpha_{1,j})$ *satisfy*

$$wt(g_j(x_j, \ldots, x_1)), wt(x_j^{m_j}) = wt\left(\prod_{i=1}^{j-1} x_i^{\alpha_{i,j}}\right);$$

4. $gcd\{m_j, gcd_i\{(\underline{\alpha}_j, W_{j-1})_i\}\} = 1.$

Definition 3.2. *Let* P*,* R *be rings as above, and* $ic(R)$ *be the integral closure of* R *in its field of fractions,* $Q(R)$*. A* ***conductor element,*** Δ*, is an element that satisfies* $\Delta \cdot ic(R) \subseteq R$*.*

It is important to remark here that while we require the *conductor element* to be an element of P, others (see [2], [15], [7], [11], [10], [12], [8], and [9]) allow the *conductor element* to be an element of R. It is important to note that MAGMA's *IntegralClosure* produces a module presentation over a function field, while its *Normalisation* gives a quotient ring. SINGULAR's *Normal* produces an R-module presentation, while its *NormalP* command produces a quotient ring. MACAULAY2 's *integralClosure* gives an extension of R while its *icFracR* command does not give a presentation. Unlike some authors who are interested in a generating set of the integral closure we are interested in a P-module generating set of the integral closure, $ic(R)$, with $ic(R)$ considered as an P-module. Let us look at a common simple example.

Example 3.1. *Let* $P := \mathbb{F}_2[f_3]$ *and* $R := P[f_5]/\langle f_5^3 + f_3^5 + f_5 f_3\rangle$*. Then* q^{th}*-power integral closure computations give us the integral closure of* R *as*

$$ic(R) := \mathbb{F}_2[f_7, f_5; f_3]/\langle f_7^2 + f_5 f_3^3 + f_7, f_7 f_5 + f_3^4 + f_5, f_5^2 + f_7 f_3\rangle, \quad \textit{where } f_7 := \frac{f_5^2}{f_3}.$$

The integral closure, $ic(R)$*, has* R*-module generating set* $\{1, f_7\}$*, meaning,* $ic(R) = R \cdot 1 + R \cdot f_7$*. But* $ic(R)$ *has* P*-module generating set* $\{1, f_5, f_7\}$*, meaning,* $ic(R) = P \cdot 1 + P \cdot f_5 + P \cdot f_7$*.*

In light of the above remark, we will state a corresponding version of a theorem on page 298 from [14]. The proof of this theorem is omitted here but can be found in [14].

Theorem 3.1. *Let P, R, and $ic(R)$ be as above. Then $ic(R)$ is a finitely generated P-module and $ic(R) = \sum_{i=0}^{m-1} Pu_i$, with the u_i's having a common denominator, $\Delta \in P$. That is, $u_i = \dfrac{v_i}{\Delta}$, with $v_i \in R$.*

Corollary 3.1. *Let P and R be as in the above theorem. There exists a* conductor element*, Δ, $\in P$ such that $R \subseteq ic(R) \subseteq \Delta^{-1}R$.*

Proof: We know that $R \subseteq ic(R)$ and from the above theorem, we have that

$$ic(R) = \sum_{i=0}^{m-1} Pu_i = \sum_{i=0}^{m-1} P\frac{v_i}{\Delta} = \frac{1}{\Delta}\sum_{i=0}^{m-1} Pv_i \subseteq \frac{1}{\Delta}R. \quad \square$$

3.2 Examples of integral closures of tower extensions over finite fields via the q^{th}-power algorithm

Example 3.2.

$$x_{i+1}^q + x_{i+1} = \frac{x_i^q}{x_i^{q-1} + 1}, \qquad 1 \le i \le n. \tag{3.1}$$

We compute the integral closure of the above tower of rings. (Details of this tower are found in [16]). Our MAGMA code also computes the corresponding weights. Many useful curves are not usually written as a recursive sequence of integral type I extensions. However, the following change of variables

$$z_{q^m - q^{i+1} + q^i} := x_{m-i} \prod_{j=1}^{m-1} (x_{m-i-j}^{q-1} + 1), \tag{3.2}$$

puts this into type I form. Let us now consider some values of q and n for the above examples.

Example 3.3. *Take $q = 2$ and $n = 2$ in equation 3.3.*

$$\begin{aligned} x_1(x_1+1)(x_2+1) - x_2^2 &= 0 \\ x_2(x_2+1)(x_4+1) - x_4^2 &= 0 \end{aligned}$$

Define x_6 and x_7 respectively by $x_6 := x_2(x_4+1)$ and $x_7 := x_1(x_2+1)(x_4+1)$. Let $\Im := \langle y_6^2 + y_6y_4 + y_6 - y_4^2 - y_4^3,\ \ y_7^2 + y_7y_6 + y_7y_4 + y_7 - y_6y_4^2\rangle$ be the ideal generated by $y_6^2 + y_6y_4 + y_6 - y_4^2 - y_4^3$ and $y_7^2 + y_7y_6 + y_7y_4 + y_7 - y_6y_4^2$. Let $R := \mathbb{F}_2[y_4]\langle 1, y_6, y_7, y_7y_6\rangle/\Im$ and $M_0 := R/\Delta$ The algorithm gives the following edited MAGMA output below;

```
weights and bases for next pass : [ -4, 2, 3, 5 ]
 [  y4,
    y6*y4,
    y7*y4,
    y7*y6   ]
weights and bases for the next pass : [ 0, 5, 6, 7 ]
 [  y4^2,
    y7*y6 + y6*y4,
    y6*y4^2,
    y7*y4^2  ]
```

Thus from the q^{th}-power algorithm, we get

$$\begin{aligned} \Delta M_0 &= \mathbb{F}_2[y_4]\langle 1, y_6, y_7, y_7y_6\rangle/\Im \\ \Delta M_1 &= \mathbb{F}_2[y_4]\langle y_4, y_6y_4, y_7y_4, y_7y_6\rangle/\Im \\ \Delta M_2 &= \mathbb{F}_2[y_4]\langle y_4^2, y_7y_6 + y_6y_4, y_6y_4^2, y_7y_4^2\rangle/\Im \\ \Delta M_3 &= \mathbb{F}_2[y_4]\langle y_4^2, y_7y_6 + y_6y_4, y_6y_4^2, y_7y_4^2\rangle/\Im, \end{aligned}$$

It follows that $ic(R) = M_2$.

Example 3.4. *Take $q = 2$ and $n = 3$ in equation 3.3.*

$$\begin{aligned} x_1(x_1+1)(x_2+1)+x_2^2 &= 0 \\ x_2(x_2+1)(x_4+1)+x_4^2 &= 0 \\ x_4(x_4+1)(x_8+1)+x_8^2 &= 0 \end{aligned}$$

Define $x_{12} := x_4(x_8+1)$, $x_{14} := x_2(x_4+1)(x_8+1)$ and $x_{15} := x_1(x_2+1)(x_4+1)(x_8+1)$. Let $\Im := \langle\, y_{12}^2 + y_{12}y_8 + y_{12} + y_8^2 + y_8^3,\ \ y_{14}^2 + y_{14}y_{12} + y_{14}y_8 + y_{14} + y_{12}y_8^2,\ \ y_{15}^2 + y_{15}y_{14} + y_{15}y_{12} + y_{15}y_8 + y_{15} + y_{14}y_{12} + y_{14}y_8^2\rangle$

Our edited MAGMA output for this example is:

```
 weights and bases for the next pass :[ -16, -4, -2, -1, 2, 5, 9, 11 ]
   M_1
    g_{-16} := y8^2,
    g_{-4} := y12*y8^2,
    g_{-2} := y14*y8^2,
    g_{-1} := y15*y8^2,
    g_2 := y14*y12*y8,
    g_5 := y15*y14*y8,
    g_9 := y15*y14*y12 + y15*y14,
    g_{11} := y15*y12*y8^2
 weights and bases for the next pass : [ -8, 4, 6, 7, 9, 10, 11, 13 ]
  M_2
    g_{-8} := y8^3,
    g_4 := y12*y8^3,
    g_6 := y14*y8^3,
    g_7 := y15*y8^3,
    g_9 := y15*y14*y12 + y15*y14*y8 + y14*y8^2 + y15*y14,
    g_{10} := y14*y12*y8^2 + y14*y8^3,
    g_{11} := y15*y12*y8^2 + y15*y14*y8,
    g_{13} := y15*y14*y8^2 + y15*y8^3
 weights and bases for the next pass :[ 0, 9, 10, 12, 13, 14, 15, 19 ]
   M_3
    g_0 := y8^4,
    g_9 := y15*y14*y12 + y14*y8^3 + y15*y14*y8 + y12*y8^3 + y14*y8^2 + y15*y14,
    g_{10} := y14*y12*y8^2 + y12*y8^3,
    g_{12} := y12*y8^4,
    g_{13} := y15*y14*y8^2,
    g_{14} := y14*y8^4,
    g_{15} := y15*y8^4,
    g_{19} := y15*y12*y8^3 + y15*y14*y8^2
 weights and bases for the next pass :[ 0, 10, 12, 13, 14, 15, 17, 19 ]
    M_4
  g_0 := y8^4,
  g_{10} := y14*y12*y8^2 + y12*y8^3,
  g_{12} := y12*y8^4,
  g_{13} := y15*y14*y8^2 + y15*y14*y12 + y14*y8^3 + y15*y14*y8
  + y12*y8^3 + y14*y8^2 + y15*y14,
  g_{14} := y14*y8^4,
  g_{15} := y15*y8^4,
  g_{17} := y15*y14*y12*y8 + y14*y8^4 + y15*y14*y8^2 + y12*y8^4
  + y14*y8^3 + y15*y14*y8,
  g_{19} := y15*y12*y8^3 + y15*y14*y8^2
```

thus giving

$$\begin{aligned}
\Delta M_0 &= \mathbb{F}_2[y_8]\langle 1, y_{12}, y_{14}, y_{15}, y_{12}y_{14}, y_{12}y_{15}, y_{14}y_{15}, y_{12}y_{14}y_{15}\rangle/\Im \\
\Delta M_1 &= \mathbb{F}_2[y_8]\langle g_{-16}, g_{-4}, g_{-2}, g_{-1}, g_2, g_5, g_9, g_{11}\rangle/\Im \\
\Delta M_2 &= \mathbb{F}_2[y_8]\langle g_{-8}, g_4, g_6, g_7, g_9, g_{10}, g_{11}, g_{13}\rangle/\Im \\
\Delta M_3 &= \mathbb{F}_2[y_8]\langle g_0, g_9, g_{10}, g_{12}, g_{13}, g_{14}, g_{15}, g_{19}\rangle/\Im, \\
\Delta M_4 &= \mathbb{F}_2[y_8]\langle g_0, g_{10}, g_{12}, g_{13}, g_{14}, g_{15}, g_{17}, g_{19}\rangle/\Im, \\
\Delta M_5 &= \mathbb{F}_2[y_8]\langle g_0, g_{10}, g_{12}, g_{13}, g_{14}, g_{15}, g_{17}, g_{19}\rangle/\Im
\end{aligned}$$

and it follows that $ic(R) = M_4$.

Example 3.5. *Take $q = 3$ and $n = 2$ in equation 3.3.*

$$\begin{gathered}
x_1(x_1^2+1)(x_3^2+1) - x_3^3 = 0 \\
x_3(x_3^2+1)(x_9^2+1) - x_9^3 = 0
\end{gathered}$$

By defining $x_{21} := x_3(x_9^2+1)$, and $x_{25} := x_1(x_3^2+1)(x_9^2+1)$, we get the following edited MAGMA output:

```
 weights and GB for pass number 1 new index is  [ -18,
-15, -8, 6, 7, 8, 13, 20, 23 ]
and base is [
    y9^6 + y9^4,
    y21*y9^4,
    y25*y21*y9^2,
    y21^2*y9^4,
    y25*y9^6 + y25*y9^4,
    y25^2*y21*y9,
    y25*y21^2*y9^2 + 2*y25*y9^6 + 2*y25*y9^4,
    y25^2*y21^2,

    y25^2*y9^5 + y25^2*y9^3 + 2*y25^2*y21 ]

weights and GB for pass number 2 new index is

[ 0, 10, 15, 20, 21, 22, 23, 25, 26 ]

and base is [

    y9^8 + y9^6,

    y25*y21*y9^4,

    y21^2*y9^5 + y25*y21*y9^3,

    y25^2*y21^2 + 2*y25*y9^7 + 2*y21^2*y9^4 + 2*y25*y9^5 + y25*y21*y9^2,

    y21*y9^8 + 2*y9^9 + y21*y9^6 + 2*y9^7,

    y25*y21^2*y9^3 + 2*y21*y9^7 + y25*y21*y9^4 + y9^8 + 2*y21*y9^5 + y9^6,

    y25^2*y9^5 + 2*y25^2*y21*y9^2 + y25*y21^2*y9^2

    + y25^2*y9^3 + y21*y9^6 + 2*y25^2*y21 + y21*y9^4,

    y25*y9^8 + y25*y9^6,

    y25^2*y21*y9^3  ]

weights and GB for pass number 3 new index is

[ 0, 19, 20, 21, 22, 23, 24, 25, 26 ]

and base is [

    y9^8 + y9^6,

    y25*y21*y9^5 + y21^2*y9^5 + y25*y21*y9^3,

    y25^2*y21^2 + 2*y25*y9^7 + y25*y21*y9^4 + 2*y21^2*y9^4

    + 2*y25*y9^5 + y25*y21*y9^2,

    y21*y9^8 + 2*y9^9 + y21*y9^6 + 2*y9^7,

    y25*y21^2*y9^3 + 2*y21*y9^7 + y9^8 + 2*y21*y9^5 + y9^6,

    y25^2*y9^5 + 2*y25^2*y21*y9^2 + y25*y21^2*y9^2

    + y25^2*y9^3 + y21*y9^6 +  2*y25^2*y21 + y21*y9^4,

    y21^2*y9^6,
    y25*y9^8 + y25*y9^6,
    y25^2*y21*y9^3  ]
weights and GB for pass number 4 new index is
  [ 0, 19, 20, 21, 22,  23, 24, 25, 26 ]
and base is [
    y9^8 + y9^6,
    y25*y21*y9^5 + y21^2*y9^5 + y25*y21*y9^3,
    y25^2*y21^2 + 2*y25*y9^7 + y25*y21*y9^4 + 2*y21^2*y9^4
        + 2*y25*y9^5 +  y25*y21*y9^2,
    y21*y9^8 + 2*y9^9 + y21*y9^6 + 2*y9^7,
    y25*y21^2*y9^3 + 2*y21*y9^7 + y9^8 + 2*y21*y9^5 + y9^6,
    y25^2*y9^5 + 2*y25^2*y21*y9^2 + y25*y21^2*y9^2 + y25^2*y9^3
     + y21*y9^6 +  2*y25^2*y21 + y21*y9^4,
    y21^2*y9^6,
    y25*y9^8 + y25*y9^6,
    y25^2*y21*y9^3  ]
```

Thus it follows that $ic(R) = M_3$.

Example 3.6. *Consider the tower*

$$z_{n+1}^q + z_{n+1} = x_n^{q+1} \quad \textit{with} \quad x_n = \frac{z_n}{x_{n-1}}, \qquad 1 \leq n \leq m. \tag{3.3}$$

We compute the integral closure of the above tower of rings. (Details of this tower are found in [21]). The following change of variables

$$x_{2q^m + \sum_{j=n}^{m} q^{j-1}} = x_m^2 \prod_{j=n}^{m} x_j$$

puts the curve into type-I form. We will compute the integral closure of the above ring for some values of q and n.

Take $q = 2$ and $n = 2$. We show the weights and the fractions produced during each pass of the q^{th}-power algorithm.

$$y_1^2 y_2 + y_1 + y_2^2 = 0$$
$$y_2^2 y_4 + y_2 + y_4^2 = 0$$

Define $\quad y_{11} := y_1 y_2 y_4^2, \quad y_6 := y_2 y_4$

```
The  computed delta is  y4^6 + y4^3

and your initial weights are [ 1, 12, 23, 34 ]

weights  for pass number 1 are [ -4, 2, 7, 9 ]

and the fractions are [    y4^5 + y4^2,

    y11^2*y4 + y11*y4^3 + y4^2,

    y11*y4^5 + y11*y4^2,

    y11^3 + y11*y4^4 + y11*y4 + y4^3]

weights  for pass number 2 are [ 0, 6, 7, 9 ]

and the fractions are [    y4^6 + y4^3,

    y11^2*y4^2 + y11*y4^4 + y4^3,

    y11*y4^5 + y11*y4^2,

    y11^3 + y11*y4^4 + y11*y4 + y4^3]

weights  for pass number 3  are [ 0, 6, 9, 11 ]

and the fractions are [    y4^6 + y4^3,

    y11^2*y4^2 + y11*y4^4 + y4^3,

    y11^3 + y11*y4^4 + y11*y4 + y4^3,

    y11*y4^6 + y11*y4^3  ]
```

```
weights  for pass number 4 are [ 0, 6, 9, 11 ]

and the fractions are [     y4^6 + y4^3,

    y11^2*y4^2 + y11*y4^4 + y4^3,

    y11^3 + y11*y4^4 + y11*y4 + y4^3,

    y11*y4^6 + y11*y4^3 ]
```

Thus it follows that $ic(R) = M_3$.

Take $q = 2$ and $n = 3$, to get

$$y_1^2 y_2 + y_1 + y_2^2 = 0$$
$$y_2^2 y_4 + y_2 + y_4^2 = 0$$
$$y_4^2 y_8 + y_4 + y_8^2 = 0$$

Define $y_{43} := y_1 y_2 y_4^2 y_8^4, \;\; y_{22} := y_2 y_4 y_8^2, \;\; y_{12} := y_4 y_8$

We note that the fractions produced during each pass of the q^{th}-power algorithm are messy, and will thus be omitted here. However, we will show the weights produced during each pass of the q^{th}-power algorithm.

```
The  computed delta is

y8^82 + y8^76 + y8^70 + y8^64 + y8^55 + y8^46 + y8^43 + y8^40 +

    y8^34 + y8^28

Initial weights are [ 1, 44, 87, 130, 173, 216, 259, 302 ]

weights  for pass number 1

new index is  [ -160, -117, -78, -76, -74, -73, -71, -43 ]

weights  for pass number 2

new index is  [ -80, -37, -33, -28, -26, -22, -3, 1 ]

weights  for pass number 3

new index is  [ -24, -5, -4, -2, 2, 7, 9, 21 ]

weights  for pass number 4
```

```
are  [ -8, 4, 6, 11, 15, 17, 18, 21 ]

weights  for pass number 5

are  [ 0, 11, 12, 14, 15, 18, 21, 25 ]

weights  for pass number 6

are  [ 0, 12, 14, 15, 18, 19, 21, 25 ]

weights  for pass number 7

are  [ 0, 12, 14, 15, 18, 19, 21, 33 ]

weights  for pass number 8

are  [ 0, 12, 14, 15, 18, 19, 21, 33 ]

The fractions  are:

[  y8^82 + y8^76 + y8^70 + y8^64 + y8^55 + y8^46 + y8^43 + y8^40 +

        y8^34 + y8^28,

    y43^4*y8^62 + y43*y8^77 + y43^6*y8^49 + y43^4*y8^59 +

        y43^3*y8^64 + y43^2*y8^69 + y43*y8^74 + y43^4*y8^56 +

        y43^2*y8^66 + y43^7*y8^38 + y43^6*y8^43 + y43^3*y8^58 +

        y43^6*y8^40 + y43^5*y8^45 + y43^2*y8^60 + y43^5*y8^42 +

        y43^4*y8^47 + y8^67 + y43^7*y8^29 + y43^6*y8^34 +

        y43^3*y8^49 + y43^2*y8^54 + y43^7*y8^26 + y43^5*y8^36 +

        y43^3*y8^46 + y43*y8^56 + y43^6*y8^28 + y43^5*y8^33 +

        y43^4*y8^38 + y8^58 + y43^4*y8^35 + y43^3*y8^40 +

        y43^5*y8^27 + y43*y8^47 + y8^52 + y43^5*y8^24 + y43^3*y8^34

        + y43^2*y8^39 + y43^4*y8^26 + y43*y8^41 + y43^4*y8^23 +

        y43^2*y8^33 + y8^40 + y8^37 + y8^31 + y8^28,

    y43^2*y8^73 + y43*y8^75 + y8^80 + y43^6*y8^47 + y43^5*y8^52 +

        y43^3*y8^62 + y43*y8^72 + y43^7*y8^39 + y43^5*y8^49 +

        y43^4*y8^54 + y43^3*y8^59 + y43^2*y8^64 + y43*y8^69 + y8^74

        + y43^7*y8^36 + y43^3*y8^56 + y43^2*y8^61 + y43*y8^66 +
        y8^71 + y43^5*y8^43 + y43*y8^63 + y8^68 + y43^7*y8^30 +
        y43^6*y8^35 + y43^4*y8^45 + y43^3*y8^50 + y8^65 +
        y43^6*y8^32 + y43^3*y8^47 + y43*y8^57 + y43^7*y8^24 +
        y43^5*y8^34 + y43^4*y8^39 + y43^2*y8^49 + y43*y8^54 + y8^59
        + y43^7*y8^21 + y43^6*y8^26 + y43^5*y8^31 + y43^6*y8^23 +
        y43^4*y8^33 + y43*y8^48 + y8^53 + y43^6*y8^20 + y43^4*y8^30
        + y43^3*y8^35 + y43*y8^45 + y8^50 + y43^7*y8^12 +
        y43^6*y8^17 + y43^5*y8^22 + y43^4*y8^27 + y43*y8^42 + y8^47
        + y43^5*y8^19 + y43^3*y8^29 + y43*y8^39 + y43^6*y8^11 +
        y43^5*y8^16 + y43^3*y8^26 + y43*y8^36 + y8^41 + y43*y8^30 +
        y43*y8^27 + y8^32 + y43^2*y8^19 + y43*y8^24 + y8^29 +
        y43^2*y8^16 + y43*y8^21,
    y43^5*y8^57 + y43^4*y8^62 + y43*y8^77 + y43^7*y8^44 +
        y43^6*y8^49 + y43^5*y8^54 + y8^79 + y43^6*y8^46 +
        y43^4*y8^56 + y43^2*y8^66 + y43*y8^71 + y8^76 + y43^7*y8^38
        + y43^6*y8^43 + y43^5*y8^48 + y43^4*y8^53 + y8^73 +
        y43^6*y8^40 + y43^5*y8^45 + y43^3*y8^55 + y43^2*y8^60 +
        y8^70 + y43^6*y8^37 + y43^2*y8^57 + y43*y8^62 + y8^67 +
        y43^7*y8^29 + y43^5*y8^39 + y43^4*y8^44 + y43^2*y8^54 +
        y43*y8^59 + y43^7*y8^26 + y43^6*y8^31 + y43^5*y8^36 +
        y43^4*y8^41 + y43^3*y8^46 + y43^2*y8^51 + y43*y8^56 +
        y43^6*y8^28 + y43^3*y8^43 + y43^7*y8^20 + y43^6*y8^25 +
        y43^4*y8^35 + y43*y8^50 + y43^3*y8^37 + y43^5*y8^24 +
        y43^3*y8^34 + y8^49 + y43^7*y8^11 + y43^6*y8^16 +
        y43^4*y8^26 + y8^46 + y43^4*y8^23 + y43^2*y8^33 + y43*y8^38
        + y43^6*y8^10 + y43^5*y8^15 + y43^3*y8^25 + y43*y8^32 +
        y8^37 + y43*y8^29 + y43^2*y8^18 + y43^2*y8^15 + y43*y8^20,
    y43^6*y8^52 + y43^4*y8^62 + y43^3*y8^67 + y43*y8^77 +
        y43^7*y8^41 + y43^5*y8^51 + y43^4*y8^56 + y43^2*y8^66 +
        y43*y8^71 + y8^76 + y43^7*y8^38 + y43^5*y8^48 + y43^4*y8^53
        + y43*y8^68 + y8^73 + y43^5*y8^45 + y43^4*y8^50 + y8^70 +
        y43^7*y8^32 + y43^4*y8^47 + y43*y8^62 + y8^67 + y43^6*y8^34
        + y43^5*y8^39 + y43^3*y8^49 + y43*y8^59 + y43^7*y8^26 +
        y43^6*y8^31 + y43^5*y8^36 + y43*y8^56 + y8^61 + y43^2*y8^48
        + y43*y8^53 + y43^7*y8^20 + y43^6*y8^25 + y43^4*y8^35 +
        y43^3*y8^40 + y43*y8^50 + y43^7*y8^17 + y43^4*y8^32 +
        y43^2*y8^42 + y43*y8^47 + y43^7*y8^14 + y43^4*y8^29 +
        y43^3*y8^34 + y43*y8^44 + y43^7*y8^11 + y43^3*y8^31 +
        y43^2*y8^36 + y8^46 + y43^6*y8^13 + y43*y8^38 + y8^43 +
        y43^6*y8^10 + y43^5*y8^15 + y43^3*y8^25 + y43^2*y8^30 +
        y43*y8^35 + y43^2*y8^27 + y43*y8^32 + y43^2*y8^24 +
        y43*y8^29 + y8^34 + y43*y8^26 + y8^31 + y8^28 + y43^2*y8^15
        + y43*y8^20,
    y43*y8^79 + y43^6*y8^51 + y43^4*y8^61 + y43^3*y8^66 +
        y43^2*y8^71 + y43*y8^76 + y8^78 + y43^7*y8^40 + y43^6*y8^45
        + y43^4*y8^55 + y43^3*y8^60 + y43^2*y8^65 + y8^75 +
        y43^3*y8^57 + y43^2*y8^62 + y43*y8^67 + y43^7*y8^34 +
        y43^5*y8^44 + y43^4*y8^49 + y43^3*y8^54 + y43^2*y8^59 +
        y43*y8^64 + y43^7*y8^31 + y43^5*y8^41 + y43^4*y8^46 +
        y43*y8^61 + y43^7*y8^28 + y43^5*y8^38 + y43^4*y8^43 +
        y43*y8^58 + y8^63 + y43^7*y8^25 + y43^5*y8^35 + y43^3*y8^45
        + y8^60 + y43^7*y8^22 + y43^5*y8^32 + y43^4*y8^37 +
        y43*y8^52 + y8^57 + y43^5*y8^29 + y43^4*y8^34 + y43^3*y8^39
        + y43*y8^49 + y43^7*y8^16 + y43^6*y8^21 + y43^2*y8^41 +
        y8^51 + y43^7*y8^13 + y43^6*y8^18 + y43*y8^43 + y8^48 +
        y43^6*y8^15 + y43^5*y8^20 + y43^4*y8^25 + y43^3*y8^30 +
        y43^2*y8^35 + y43^6*y8^12 + y43^5*y8^17 + y43^3*y8^27 +
        y43*y8^37 + y8^42 + y43^2*y8^29 + y8^39 + y43^2*y8^26 +
        y43^2*y8^23 + y8^33 + y43*y8^25 + y43^2*y8^17 + y43*y8^22,
    y43^7*y8^47 + y43^6*y8^52 + y43^5*y8^57 + y43^3*y8^67 +
        y43^2*y8^72 + y43*y8^77 + y43^6*y8^49 + y43^4*y8^59 +
        y43^3*y8^64 + y43^2*y8^69 + y43*y8^74 + y8^79 + y43^7*y8^41
        + y43^6*y8^46 + y43^3*y8^61 + y43^2*y8^66 + y8^76 +
        y43^6*y8^43 + y43^4*y8^53 + y43^5*y8^45 + y43^2*y8^60 +
        y43*y8^65 + y43^2*y8^57 + y43*y8^62 + y8^67 + y43^6*y8^34 +
        y43^5*y8^39 + y43^4*y8^44 + y43^3*y8^49 + y43^2*y8^54 +
        y43*y8^59 + y8^64 + y43^7*y8^26 + y43^5*y8^36 + y43^4*y8^41
        + y43^7*y8^23 + y43^6*y8^28 + y43^4*y8^38 + y43^2*y8^48 +
        y43^7*y8^20 + y43^6*y8^25 + y43^5*y8^30 + y43^3*y8^40 +
        y43^2*y8^45 + y43^7*y8^17 + y43^6*y8^22 + y43^5*y8^27 +
        y8^52 + y43^4*y8^29 + y43^2*y8^39 + y43*y8^44 + y43^7*y8^8 +
        y43^6*y8^13 + y43^5*y8^18 + y43^4*y8^23 + y43^3*y8^28 +
        y43^2*y8^33 + y8^43 + y43^7*y8^5 + y43^6*y8^10 + y43^2*y8^30
        + y43*y8^35 + y8^40 + y43^5*y8^12 + y43^2*y8^27 + y8^37 +
        y43^3*y8^19 + y8^34 + y43^4*y8^11 + y43^2*y8^21 + y43*y8^23
        + y8^28 + y43^3*y8^10 + y43^2*y8^15,
    y43^3*y8^70 + y43^2*y8^75 + y43^6*y8^52 + y43^5*y8^57 +
        y43^3*y8^67 + y43*y8^77 + y8^82 + y43*y8^74 + y8^79 +
        y43^6*y8^46 + y43^4*y8^56 + y43^3*y8^61 + y43^2*y8^66 +
        y8^76 + y43^7*y8^38 + y43^6*y8^43 + y43^5*y8^48 +
        y43^3*y8^58 + y8^73 + y43^7*y8^35 + y43^6*y8^40 + y8^70 +
        y43^5*y8^42 + y43^3*y8^52 + y43^2*y8^57 + y43*y8^62 +
        y43^4*y8^44 + y43^3*y8^49 + y43^4*y8^41 + y43^3*y8^46 +
        y43*y8^56 + y43^4*y8^38 + y43^7*y8^20 + y43^6*y8^25 +
        y43^2*y8^45 + y43^4*y8^32 + y43^2*y8^42 + y8^52 +
        y43^4*y8^29 + y43^6*y8^16 + y43^4*y8^26 + y43^3*y8^31 +
        y43*y8^41 + y43^7*y8^8 + y43^4*y8^23 + y43^3*y8^28 +
        y43^2*y8^33 + y43^5*y8^15 + y43^3*y8^25 + y43*y8^35 +
        y43^4*y8^17 + y43^2*y8^27 + y43^4*y8^14 + y43*y8^29 +
        y43^3*y8^16 + y43^2*y8^21 + y43^3*y8^13 + y43*y8^23 ]
```

Example 3.7. *Consider the tower*

$$\frac{y-1}{y^q} = \frac{x^q-1}{x} \tag{3.4}$$

(See [16], page 61, *for more details about this tower).*

The following change of variables

$$x_{2q^m-(q-1)q^{(i-1)}} = x_i(x_m-1)^2 \prod_{j=i+1}^{m-1}(x_j-1),\ 1 \le i \le m. \tag{3.5}$$

puts equation (8.19) into type I form. We will compute the integral closure for some values of q and n.

Take $q = 2,$ and $m = 2$, to get

$$y_1^2 y_2^2 + y_1^2 + y_1 y_2 + y_2 = 0$$
$$y_2^2 y_4^2 + y_2^2 + y_2 y_4 + y_4 = 0$$

Define $y_4 := x_0 + 1, \quad y_6 := y_2 y_4^2 + y_2, \quad y_7 := y_1 y_2 y_4^2 + y_1 y_2 + y_1 y_4^2 + y_1$, The q^{th}-power algorithm then produces:

```
The  computed delta is  x^6 + x^5 + x^4

 and the initial weights are [ 1, 8, 15, 22 ]

weights and GB for pass number 1

are [ -8, -1, 2, 5 ]

and the fractions are

  [ y4^4 + y4^3 + y4^2,

    y7*y4^4 + y7*y4^3 + y7*y4^2,

    y7^2*y4^3 + y7^3*y4 + y7^2*y4^2 + y7^2*y4 + y4^3 + y4^2,

    y7^3*y4^2 + y4^2  ]

weights and GB for pass number 2

are [ -4, 3, 5, 6 ]

and  fractions are

   [ y4^5 + y4^4 + y4^3,

    y7*y4^5 + y7*y4^4 + y7*y4^3,

    y7^3*y4^2 + y7^2*y4^3 + y7^3*y4 + y7*y4^4 + y7^2*y4^2 + y7*y4^3

        + y7^2*y4 + y7*y4^2 + y4^3,

    y7^2*y4^4 + y7^3*y4^2 + y7*y4^5 + y7^2*y4^3 + y7*y4^4 +

        y7^2*y4^2 + y7*y4^3 + y4^4 + y4^3  ]

weights and GB for pass number 3

are  [ 0, 5, 6, 7 ]

and the fractions are

   [ y4^6 + y4^5 + y4^4,

    y7^3*y4^2 + y7*y4^5 + y7^2*y4^3 + y7^3*y4 + y7^2*y4^2 + y4^5 +

        y7^2*y4 + y4^4 + y7*y4^2,

    y7^2*y4^4 + y7^3*y4^2 + y7^2*y4^3 + y7^2*y4^2 + y4^5,

    y7*y4^6 + y7*y4^5 + y7*y4^4   ]

weights and GB for pass number 4
```

```
are [ 0, 5, 6, 7 ]

and the fractions are

    [ y4^6 + y4^5 + y4^4,

    y7^3*y4^2 + y7*y4^5 + y7^2*y4^3 + y7^3*y4 + y7^2*y4^2 + y4^5 +

        y7^2*y4 + y4^4 + y7*y4^2,

    y7^2*y4^4 + y7^3*y4^2 + y7^2*y4^3 + y7^2*y4^2 + y4^5,

    y7*y4^6 + y7*y4^5 + y7*y4^4  ]
```

Take $q = 2$, and $m = 3$, to get

$$y_1^2y_2^2 + y_1^2 + y_1y_2 + y_2 = 0$$

$$y_2^2y_4^2 + y_2^2 + y_2y_4 + y_4 = 0$$

$$y_4^2y_8^2 + y_4^2 + y_4y_8 + y_8 = 0$$

Define $y_8 := x_0 + 1$, $y_{12} := y_4y_8^2 + y_4$, $y_{14} := y_2y_4y_8^2 + y_2y_4 + y_2y_8^2 + y_2$, $y_{15} := y_1y_2y_4y_8^2 + y_1y_2y_4 + y_1y_2y_8^2 + y_1y_2 + y_1y_4y_8^2 + y_1y_4 + y_1y_8^2 + y_1$. The q^{th}-power algorithm then produces:

```
The  computed delta is  x^22 + x^21 + x^20 + x^18 + x^17 + x^16 +

    x^14 + x^13 + x^12

The initial weights are [ 1, 16, 31, 46, 61, 76, 91, 106 ]


weights  for  pass number 1

are  [ -80, -65, -58, -53, -43, -38, -28, -23 ]

weights for pass number 2

are  [ -40, -25, -13, -12, -11, -10, -7, 2 ]

weights  for pass number 3

are  [ -8, 4, 6, 7, 9, 10, 11, 13 ]

weights  for pass number 4
```

```
are  [ 0, 9, 10, 11, 12, 13, 14, 15 ]

weights  for pass number 5

are  [ 0, 10, 12, 13, 14, 15, 17, 19 ]

weights for pass number 6

are  [ 0, 10, 12, 13, 14, 15, 17, 19 ]

and the fractions are [

    y8^22 + y8^21 + y8^20 + y8^18 + y8^17 + y8^16 + y8^14 + y8^13 +

        y8^12,

    y15^6*y8^12 + y15^7*y8^10 + y15*y8^21 + y15^5*y8^13 +

        y15^6*y8^11 + y15^5*y8^12 + y8^21 + y15^2*y8^17 +

        y15^4*y8^13 + y15^6*y8^9 + y15*y8^18 + y15^2*y8^16 +

        y15^4*y8^12 + y15^7*y8^6 + y8^19 + y15*y8^17 + y15^2*y8^15 +

        y15^4*y8^11 + y15^5*y8^9 + y15^6*y8^7 + y15^2*y8^14 +

        y15^4*y8^10 + y15^5*y8^8 + y15^6*y8^6 + y15^2*y8^13 +

        y15^4*y8^9 + y15*y8^14 + y15^2*y8^12 + y8^15 + y15^3*y8^9 +

        y8^14 + y15^2*y8^10 + y15^3*y8^8 + y8^13 + y8^12 +

        y15^2*y8^8,

    y15^4*y8^16 + y15^7*y8^10 + y15*y8^21 + y15^2*y8^19 +

        y15^3*y8^17 + y15^4*y8^15 + y15^5*y8^13 + y15^3*y8^16 +

        y15^4*y8^14 + y15^5*y8^12 + y15^2*y8^17 + y15^4*y8^13 +

        y8^20 + y15*y8^18 + y15^4*y8^12 + y15^2*y8^15 + y15^4*y8^11

        + y8^18 + y15^2*y8^14 + y15^4*y8^10 + y8^17 + y8^16 + y8^15

        + y8^13 + y8^12,

    y15^3*y8^18 + y15^5*y8^14 + y15^6*y8^12 + y15*y8^21 +

        y15^2*y8^19 + y15^3*y8^17 + y15^7*y8^9 + y15^2*y8^18 +

        y15^3*y8^16 + y15^4*y8^14 + y15^5*y8^12 + y15*y8^19 +

        y15^2*y8^17 + y15^3*y8^15 + y15^5*y8^11 + y15^7*y8^7 + y8^20
        + y15^3*y8^14 + y15^4*y8^12 + y15^6*y8^8 + y15*y8^17 +
        y15^5*y8^9 + y15^7*y8^5 + y15*y8^16 + y15^3*y8^12 +
        y15^5*y8^8 + y15^7*y8^4 + y15*y8^15 + y15^2*y8^13 + y8^16 +
        y15*y8^14 + y15^3*y8^10 + y15^6*y8^4 + y15*y8^13 +
        y15^3*y8^9 + y15*y8^12 + y15*y8^11 + y15^2*y8^9 + y15*y8^10
        + y15^2*y8^8 + y15^3*y8^6 + y15*y8^9 + y15^2*y8^7 + y15*y8^8
        + y15^2*y8^6,
    y15^2*y8^20 + y15^3*y8^18 + y15^4*y8^16 + y15^7*y8^10 +
        y15*y8^21 + y15^3*y8^17 + y15^5*y8^13 + y15^7*y8^9 +
        y15*y8^20 + y15^2*y8^17 + y15^3*y8^15 + y15^5*y8^11 +
        y15*y8^18 + y15^3*y8^14 + y15*y8^17 + y8^18 + y15^2*y8^14 +
        y15^2*y8^13 + y15^4*y8^9 + y8^16 + y15^2*y8^12 + y15^3*y8^10
        + y8^15 + y15^2*y8^11 + y8^14 + y15^2*y8^10 + y8^13 + y8^12,
    y15*y8^22 + y15*y8^21 + y15*y8^20 + y15*y8^18 + y15*y8^17 +
        y15*y8^16 + y15*y8^14 + y15*y8^13 + y15*y8^12,
    y15^7*y8^11 + y15*y8^22 + y15^6*y8^12 + y15^4*y8^15 +
        y15^5*y8^13 + y15^7*y8^9 + y8^22 + y15*y8^20 + y15^6*y8^10 +
        y15^7*y8^8 + y8^21 + y15*y8^19 + y15^2*y8^17 + y15^4*y8^13 +
        y15^5*y8^11 + y15^6*y8^9 + y15^7*y8^7 + y15^2*y8^16 +
        y15^3*y8^14 + y15^5*y8^10 + y15^6*y8^8 + y15^7*y8^6 + y8^19
        + y15^2*y8^15 + y15^5*y8^9 + y15^6*y8^7 + y15^7*y8^5 +
        y15*y8^16 + y15^4*y8^10 + y8^17 + y15^2*y8^13 + y15^3*y8^11
        + y15^6*y8^5 + y15*y8^14 + y15^2*y8^11 + y15^3*y8^9 + y8^14
        + y15*y8^12 + y15^2*y8^10 + y8^13 + y15^3*y8^7 + y15*y8^10 +
        y15^2*y8^8 + y15*y8^9 + y15^2*y8^7,
    y15^5*y8^15 + y15^6*y8^13 + y15^7*y8^11 + y15*y8^22 +
        y15^3*y8^18 + y15^5*y8^14 + y15^2*y8^19 + y15^4*y8^15 +
        y15^6*y8^11 + y15^7*y8^9 + y8^22 + y15*y8^20 + y15^3*y8^16 +
        y15^4*y8^14 + y15^6*y8^10 + y15^7*y8^8 + y15^4*y8^13 +
        y15^5*y8^11 + y15^6*y8^9 + y15^7*y8^7 + y15*y8^18 +
        y15^3*y8^14 + y15^4*y8^12 + y15^5*y8^10 + y15^6*y8^8 +
        y15^7*y8^6 + y8^19 + y15*y8^17 + y15^2*y8^15 + y15^4*y8^11 +
        y8^18 + y15*y8^16 + y15^3*y8^12 + y15^6*y8^6 + y15^2*y8^13 +
        y15^3*y8^11 + y8^16 + y15*y8^13 + y15*y8^12 + y15^3*y8^8 +
        y8^13 + y15^2*y8^9 + y15*y8^10 + y15^2*y8^8 ]
```

Chapter 4

The q^{th}-power algorithm over $\mathbb{Q}$

In this chapter, we will represent any $r \in \mathbb{Q}$ in the form $r = \dfrac{a}{b}$ with $b > 0$ and $gcd(a,b) = 1$. For any fixed modulus $M > 0$, we define

$$\mathbb{Q}_M := \left\{ \frac{a}{b}, b > 0, \quad gcd(a,b) = 1 : \quad gcd(M,b) = 1 \right\}.$$

Let $\mathbb{F}[\underline{x}] := \mathbb{F}[x_m, \ldots, x_1]$ and $\underline{x}^{\underline{\alpha}} := \prod_i x_i^{\alpha_i}$. We will consider type I affine domains $S := R/I$ with $R := \mathbb{F}[\underline{x}]$ being a polynomial ring, and $I := \langle G \rangle$ an ideal of R of relations with Gröbner basis G.

Type I affine domains have the property, among others, that relative to a free polynomial subring $P := \mathbb{F}[x_n, \ldots, x_1]$, there is a weight function $wt : R \longrightarrow \mathbb{N}^n$ such that $wt(LM(f)) = wt(LM(NF(f, I)))$.

Given a presentation $S := R/I$ and a presentation of its integral closure $\overline{S} := \overline{R}/\overline{I}$, there is a map $\psi : R \longrightarrow \overline{R}$, necessarily with $\psi(I) \subset \overline{I}$, so that ψ can be viewed as an inclusion map $\overline{\psi} : S \longrightarrow \overline{S}$.

It is possible to use the *extended Euclidean algorithm* to move between fractions $\dfrac{a}{b} \in \mathbb{Q}, \ b > 0$ and representatives $c \in \mathbb{Z}_N$. The fraction reconstruction map (see [26] for details) is

$$E_N(c) := \frac{a}{b}, \quad bc + Nd = a, a^2 + b^2 \ \ min, \quad b \ min.$$

The mod N map is

$$\mu_N\left(\frac{a}{b}\right) := c, \quad bc + Nd = a, \quad |c| \ \ min.$$

These are almost inverse operations in the sense that for $-\dfrac{N}{2} < c < \dfrac{N}{2}$, $(\mu_N \circ E_N)(c) = c$; while, for $a^2 + b^2 < N$, $(E_N \circ \mu_N)\left(\frac{a}{b}\right) = \frac{a}{b}$. Defining $\mu_N(y_j^{(0)}) := y_j^{(0)}$ for $1 \leq j \leq m$, gives a natural extension of μ_N to maps from some elements of $\mathbb{Q}[y_m^{(0)}, \ldots, y_1^{(0)}]$ to elements of $\mathbb{Z}_N[y_m^{(N)}, \ldots, y_1^{(N)}]$; and defining $E_N(Y_j^{(N)}) := Y_j^{(0)}$ for $1 \leq j \leq M$, gives a natural extension of E_N to maps from some elements of $\mathbb{Z}_N[Y_M^{(N)}, \ldots, Y_1^{(N)}]$ to elements of $\mathbb{Q}[Y_m^{(0)}, \ldots, Y_1^{(0)}]$.

Similarly the *Chinese remainder map*

$$C_{q,N}(a^{(q)}, a^{(N)}) := a^{(qN)}(mod\ qN), \quad a^{(qN)} \equiv a^{(q)}(mod\ q), \quad a^{(qN)} \equiv a^{(N)}(mod\ N),$$

can be used to map some pairs of elements from $\mathbb{Z}_q[Y_M^{(q)}, \ldots, Y_1^{(q)}] \times \mathbb{Z}_N[Y_M^{(N)}, \ldots, Y_1^{(N)}]$, to elements of $\mathbb{Z}_{qN}[Y_M^{(qN)}, \ldots, Y_1^{(qN)}]$.

4.1 Lifting maps from coefficient rings to polynomial rings

The *mod M map* $\mu_M : \mathbb{Q}_M \longrightarrow \mathbb{Z}_M$ is defined by $\mu_M(\dfrac{a}{b}) := ab^{-1}(mod\ M)$. This map is naturally extended to the polynomial map $\mu_M^* : \mathbb{Q}_M[\underline{x}] \longrightarrow \mathbb{Z}_M[\underline{x}]$, defined by $\mu_M^*\left(\sum_{\underline{\alpha}} r_{\underline{\alpha}} \underline{x}^{\underline{\alpha}}\right) := \sum_{\underline{\alpha}} \mu_M(r_{\underline{\alpha}}) \underline{x}^{\underline{\alpha}}$.

If $S^{(0)} = R^{(0)}/I^{(0)}$ is type I with $R^{(0)} := \mathbb{Q}[\underline{x}^{(0)}]$, and p is a prime for which $R^{(p)} := \mu_p(R^{(0)}) = \mathbb{Z}_p[\underline{x}^{(p)}]$ and $I^{(p)} := \mu_p(I^{(0)})$, then necessarily $\mu_p(\overline{S}^{(0)}) \subset (\overline{S}^{(p)})$. If equality holds, then we call p a *good* prime.

Choose a sequence $p_1 < p_2 < \cdots$ of good primes, and let $M_s := \prod_{i=1}^{s} p_i$. The Chinese remainder theorem gives a map $CRT_{M_s} := \prod_{l=1}^{s} \mathbb{Z}_{p_l} \longrightarrow \mathbb{Z}_{M_s}$ such that $CRT_{M_s}((a_1, \ldots, a_s)) \equiv a_l\ (mod\ p_l)$ for each l. Extend this naturally to the polynomial map $CRT_{M_s}^* : \prod_{l=1}^{s} \mathbb{Z}_{p_l}[\underline{y}] \longrightarrow \mathbb{Z}_{M_s}[\underline{y}]$ by

$$CRT_{M_s}^*\left(\left(\sum_{\underline{\alpha}} r_{\underline{\alpha}}^{(p_1)} \underline{y}^{\underline{\alpha}}, \cdots, \sum_{\underline{\alpha}} r_{\underline{\alpha}}^{(p_s)} \underline{y}^{\underline{\alpha}}\right)\right) := \sum_{\underline{\alpha}} CRT_{M_s}\left(\left(r_{\underline{\alpha}}^{(p_1)}, \cdots, r_{\underline{\alpha}}^{(p_s)}\right)\right) \underline{y}^{\underline{\alpha}}.$$

The *Euclidean algorithm*, applied to $M_s := r_{-1}$ and any $r_0 > 0$, produces sequences (r_i) and (q_i) such that $r_{i-2} = q_i r_{i-1} + r_i$ with $0 \leq r_i < r_{i-1}$, and $r_n = 0$. It should be noted that part of the *extended Euclidean algorithm* produces a sequence (u_i) with $u_{-1} := 0, \quad u_0 := 1$, and $u_i := q_i u_{i-1} + u_{i-2}$. Then for each i, $(-1)^i r_i/u_i \equiv r_0 \ (mod\ M_s)$. Of these there is necessarily some $i \geq 0$ with $r_i^2 + u_i^2$ minimum, choosing i minimum as well if this is not unique. We use this i to define the map $\epsilon_{M_s} : \mathbb{Z}_{M_s} \longrightarrow \mathbb{Q}$ by $\epsilon_{M_s}(r_0) := (-1)^i r_i/u_i$ for the unique i described above.

Extend this naturally to the polynomial map $\epsilon^*_{M_s} : \mathbb{Z}_{M_s}[\underline{y}] \longrightarrow \mathbb{Q}[\underline{y}]$ defined by

$$\epsilon^*_{M_s}\left(\sum_{\underline{\alpha}} r_{\underline{\alpha}} \underline{y}^{\underline{\alpha}}\right) := \sum_{\underline{\alpha}} \epsilon_{M_s}\left(r_{\underline{\alpha}}\right) \underline{y}^{\underline{\alpha}}.$$

Now define the composition map

$$\psi^{(0,M_s)} := \epsilon^*_{M_s} \circ \overline{CRT}^*_{M_s} \circ \left(\prod_{l=1}^{s} \psi^{(p_l)}\right) \circ \left(\prod_{l=1}^{s} \mu^*_{p_l}\right)$$

mapping $\mathbb{Q}_{M_s}[\underline{x}] \longrightarrow \mathbb{Q}[\underline{y}]$, for $\psi^{(p_l)}$ the inclusion map from R^{p_l} to $\overline{R}^{(p_l)}$.

4.2 Presentations

Let $y_i^{(0)} := f_i^{(0)}/\delta_i^{(0)}$ denote the variables (”fractions”) in the integral closure presentation $S^{(0)}$ by for $f_i^{(0)}$, $\delta_i^{(0)} R^{(0)}$, and let $g_j^{(0)}$ denote the Gröbner basis elements (”relations”) of $\overline{I}^{(0)}$. Let $y_i^{(p)} := f_i^{(p)}/\delta_i^{(p)}$, for $f_i^{(p)} := \mu^*_p\left(f_i^{(0)}\right)$ and $\delta_i^{(p)} := \mu^*_p\left(\delta_i^{(0)}\right)$; and $g_j^{(p)} := \mu^*_p\left(g_j^{(0)}\right)$.

If p is a good prime, then these are variables and (a Gröbner basis of) relations for $\overline{S}^{(p)}$. Here the objective is to go in the reverse direction by reconciling various $\overline{S}^{(p)}$'s and reconstructing $\overline{S}^{(0)}$ from them, using the Chinese remainder map and the extended algorithm map.

The candidates for $\overline{S}^{(0)}$ are $\overline{S}^{(0,M_s)}$ with polynomial ring $\overline{R}^{(0,M_s)}$ having variables

$$y_i^{(0,M_s)} := \epsilon^*_{M_s}\left(CRT^*_{M_s}\left(\prod_{l=1}^{s} y_i^{(p_l)}\right)\right)$$

and ideal $\overline{I}^{(0,M_s)}$ generated by the finite set of images

$$\overline{G}^{(0,M_s)} := \left\{g_j^{(0,M_s)} := \epsilon^*_{M_s}\left(CRT^*_{M_s}\left(\prod_{l=1}^{s} g_i^{(p_l)}\right)\right)\right\}$$

We note that $\overline{S}^{(0)} = \overline{S}^{(0,M_s)}$, then necessarily $\overline{S}^{(0,M_{s+1})} = \overline{S}^{(0,M_s)}$ also. However, as we see from the following example below, the latter is not sufficient to guarantee the former.

Example 4.1.

$$\overline{S}^{(0)} := \mathbb{Q}[x_2; x_1]/\langle x_2^2 + \frac{7}{8}x_1^3\rangle$$

stabilizes after $p_1 := 3,\ p_2 := 5,$ *with* $y_2 := x_2/x_1,\ y_1 := x_1,$

$$\overline{S}^{(0,15)} := \mathbb{Q}[y_2; y_1]/\langle y_2^2 - y_1\rangle$$

rather than the obvious $y_2 := x_2/x_1,\ y_1 := x_1,$

$$\overline{S}^{(0)} := \mathbb{Q}[y_2; y_1]/\langle y_2^2 + \frac{7}{8}y_1\rangle.$$

Theorem 4.1. $\overline{S}^{(0,M)}$ *is a presentation of the integral closure of* $S^{(0)}$ *if*

1. $\overline{G}^{(0,M)}$ *is a Gröbner basis for* $\overline{I}^{(0,M)}$*;*

2. $\psi^{(0,M)}(I^{(0)}) \subseteq \overline{I}^{(0,M)}$.

Proof: $\overline{S}^{(0,M)}$ is necessarily a ring. If $\psi^{(0,M)}(I^{(0)}) \subseteq \overline{I}^{(0,M)}$, then $\overline{\psi}^{(0,M)}(S^{(0)}) \subseteq \overline{S}^{(0,M)}$. So $S^{(0,M)} \subseteq \overline{S}^{(0)}$, because $\overline{S}^{(0)}$ is the largest ring (in the field of fractions of $S^{(0)}$) containing

$\overline{\psi}^{(0,M)}(S^{(0)})$. But if $\overline{G}^{(0,M)}$ is a Gröbner basis for $\overline{I}^{(0,M)}$, then

$$\mu_p^*\left(LM\left(\overline{I}^{(0,M)}\right)\right) = LM\left(\overline{I}^{(p)}\right) = \mu_p^*\left(LM\left(\overline{I}^{(0)}\right)\right).$$

Thus $\overline{S}^{(0,M)} = \overline{S}^{(0)}$, which proves the theorem.□

Note that by the remark preceding the theorem, these conditions need only be checked at the steps at which $y_i^{(0,M_s)} = y_i^{(0,M_{s+1})}$ for each i and $g_j^{(0,M_s)} = g_j^{(0,M_{s+1})}$ for each j.

4.3 Examples

In this section, we present some examples over the rationals.

Example 4.2. *Let* $f = (y^2 - y - \frac{1}{6}x)^3 - yx^4(y^2 - y - \frac{1}{6}x) - x^{11}$
It is immediate that 2 *and* 3 *are possibly "bad" primes, since they both divide* 6.

The first good prime is $q = 5$. *The integral closure and its corresponding weights for this prime are*

$[x^5,$

$y^2x^3 + 4yx^3 + 4x^4,$

$yx^5,$

$y^4x + 3y^3x + 3y^2x^2 + y^2x + 2yx^2 + x^3,$

$y^3x^3 + 4yx^4 + 4yx^3 + 4x^4,$

$y^5 + 2y^4 + 3y^3x + 3y^3 + 4y^2x + yx^2 + 4y^2 + 3yx + 4x^2]$, *and*

$[0, 10, 11, 20, 21, 25]$.

The integral closure over the rationals for the sequence, (5), *of good primes is*

$[x^5,$

$y^2x^3 - yx^3 - x^4,$

$yx^5,$

$y^4x - 2y^3x - 2y^2x^2 + y^2x + 2yx^2 + x^3,$

$y^3x^3 - yx^4 - yx^3 - x^4,$

$y^5 + 2y^4 - 2y^3x - 2y^3 - y^2x + yx^2 - y^2 - 2yx - x^2].$

The next good prime is $q = 7$. *The integral closure and its corresponding weights for this prime are*

$[x^5,$

$y^2x^3 + 6yx^3 + x^4,$

$yx^5,$

$y^4x + 5y^3x + 2y^2x^2 + y^2x + 5yx^2 + x^3,$

$y^3x^3 + yx^4 + 6yx^3 + x^4,$

$y^5 + 4y^4 + 2y^3x + 3y^3 + 3y^2x + yx^2 + 6y^2 + 2yx + 6x^2],$ *and*

$[0, 10, 11, 20, 21, 25].$

The integral closure over the rationals for the sequence, $(5, 7)$, *of good primes is*

$[x^5,$

$y^2x^3 - yx^3 + x^4,$

$yx^5,$

$y^4x - 2y^3x - \frac{1}{3}y^2x^2 + y^2x + \frac{1}{3}yx^2 + x^3,$

$y^3x^3 + yx^4 - yx^3 + x^4,$

$y^5 - 3y^4 - \frac{1}{3}y^3x + 3y^3 + \frac{2}{3}y^2x + yx^2 - y^2 - \frac{1}{3}yx - x^2].$

The next good prime is $q = 11$. *The integral closure and its corresponding weights for this prime are*

$[x^5,$

$y^2x^3 + 10yx^3 + 9x^4,$

$yx^5,$

$y^4x + 9y^3x + 7y^2x^2 + y^2x + 4yx^2 + 4x^3,$

$y^3x^3 + 9yx^4 + 10yx^3 + 9x^4,$

$y^5 + 8y^4 + 7y^3x + 3y^3 + 8y^2x + 4yx^2 + 10y^2 + 7yx + 7x^2],$ *and*

$[0, 10, 11, 20, 21, 25].$

The integral closure over the rationals for the sequence, $(5,7,11)$, *of good primes is*

$[x^5,$

$y^2x^3 - yx^3 - \frac{1}{6}x^4,$

$yx^5,$

$y^4x - 2y^3x - \frac{1}{3}y^2x^2 + y^2x + \frac{1}{3}yx^2 + x^3,$

$y^3x^3 - \frac{1}{6}yx^4 - yx^3 - \frac{1}{6}x^4,$

$y^5 - 3y^4 - \frac{1}{3}y^3x + 3y^3 + \frac{2}{3}y^2x + yx^2 - y^2 - \frac{1}{3}yx - x^2].$

The next good prime is $q = 13$. *The integral closure and its corresponding weights for this prime are*

$[x^5,$

$y^2x^3 + 12yx^3 + 2x^4,$

$yx^5,$

$y^4x + 11y^3x + 4y^2x^2 + y^2x + 9yx^2 + 4x^3,$

$y^3x^3 + 2yx^4 + 12yx^3 + 2x^4,$

$y^5 + 10y^4 + 4y^3x + 3y^3 + 5y^2x + 4yx^2 + 12y^2 + 4yx + 9x^2]$, *and*

$[0, 10, 11, 20, 21, 25].$

The integral closure over the rationals for the sequence, $(5,7,11,13)$, *of good primes is*

$[x^5,$

$y^2x^3 - yx^3 - \frac{1}{6}x^4,$

$yx^5,$

$y^4x - 2y^3x - \frac{1}{3}y^2x^2 + y^2x + \frac{1}{3}yx^2 + \frac{1}{36}x^3,$

$y^3x^3 - \frac{1}{6}yx^4 - yx^3 - \frac{1}{6}x^4,$

$y^5 - 3y^4 - \frac{1}{3}y^3x + 3y^3 + \frac{2}{3}y^2x + \frac{1}{36}yx^2 - y^2 - \frac{1}{3}yx - \frac{1}{36}x^2].$

The next good prime is $q = 17$. *The integral closure and its corresponding weights for this prime are*

$[x^5,$

$y^2x^3 + 16yx^3 + 14x^4,$

$yx^5,$

$y^4x + 15y^3x + 11y^2x^2 + y^2x + 6yx^2 + 9x^3,$

$y^3x^3 + 14yx^4 + 16yx^3 + 14x^4,$

$y^5 + 14y^4 + 11y^3x + 3y^3 + 12y^2x + 9yx^2 + 16y^2 + 11yx + 8x^2]$, *and*

$[0, 10, 11, 20, 21, 25].$

The integral closure over the rationals for the sequence, $(5, 7, 11, 13, 17)$, *of good primes is*

$[x^5,$

$y^2x^3 - yx^3 - \frac{1}{6}x^4,$

$yx^5,$

$y^4x - 2y^3x - \frac{1}{3}y^2x^2 + y^2x + \frac{1}{3}yx^2 + \frac{1}{36}x^3,$

$y^3x^3 - \frac{1}{6}yx^4 - yx^3 - \frac{1}{6}x^4,$

$y^5 - 3y^4 - \frac{1}{3}y^3x + 3y^3 + \frac{2}{3}y^2x + \frac{1}{36}yx^2 - y^2 - \frac{1}{3}yx - \frac{1}{36}x^2],$

which stabilizes as the integral closure over the rationals.

We would want the integral closure produced for each prime to have corresponding weights, $[0, 10, 11, 20, 21, 25]$. *But some primes produce integral closures whose corresponding weights are "smaller", and this is certainly not what we want. Examples of such primes include those in the list,* $[67, 71, 3678929, 162747760338128425024443010 4357]$, *of possibly "bad" primes. Let us consider some of these possibly "bad" primes.*

Take $q = 67$. *The integral closure produced is*

$[x^6 + 43x^5,$

$y^2x^4 + 43y^2x^3 + 66yx^4 + 11x^5 + 24yx^3 + 4x^4,$

$yx^6 + 43yx^5,$

$y^5 + 22y^3x^3 + 24y^4x + 64y^4 + yx^5 + 8y^2x^3 + 41y^3x + 41yx^4 + 59y^2x^2 + 3y^3 + 39x^5 + 37yx^3 +$
$47y^2x + 62x^4 + 62yx^2 + 66y^2 + 23x^3 + 22yx + 13x^2,$

$y^4x^2 + 43y^4x + 65y^3x^2 + 22y^2x^3 + 48y^3x + 9y^2x^2 + 45yx^3 + 43y^2x + 54x^4 + 59yx^2 + 44x^3,$

$y^3x^4 + 43y^3x^3 + 11yx^5 + 3yx^4 + 11x^5 + 24yx^3 + 4x^4],$

and the corresponding weight is $[0, 10, 11, 19, 20, 21]$, *which is "smaller" than* $[0, 10, 11, 20, 21, 25]$.

For $q = 71$*, the integral closure produced is*

$[x^6 + 11x^5,$

$y^2x^4 + 11y^2x^3 + 70yx^4 + 59x^5 + 60yx^3 + 10x^4,$

$yx^6 + 11yx^5,$

$y^5 + 54y^3x^3 + 63y^4x + 68y^4 + 24yx^5 + 40y^2x^3 + 63y^3x + 62yx^4 + 50y^2x^2 + 3y^3 + 29x^5 + 48yx^3 +$
$40y^2x + 8x^4 + 23yx^2 + 70y^2 + 55x^3 + 47yx + 69x^2,$

$y^4x^2 + 11y^4x + 69y^3x^2 + 47y^2x^3 + 49y^3x + 21y^2x^2 + 24yx^3 + 11y^2x + 2x^4 + 51yx^2 + 22x^3,$

$y^3x^4 + 11y^3x^3 + 59yx^5 + 9yx^4 + 59x^5 + 60yx^3 + 10x^4],$

and the corresponding weight is $[0, 10, 11, 19, 20, 21]$*, which is "smaller" than* $[0, 10, 11, 20, 21, 25]$*.*

Hence we will not use the primes $[2, 3, 67, 71, 3678929, 16274776033812842502444301043 57]$*, since they are possibly "bad" primes.*

Example 4.3. *Let* $f = (y^2 - \frac{3}{4}y - \frac{15}{17}x)^3 - 9x^4(y^2 - \frac{3}{4}y - \frac{15}{17}x) - 27x^{11}$
It is immediate that 2 *and* 17 *are possibly "bad" primes. As we shall see, the primes* $(3, 5, 7, 11)$ *are also possibly "bad" primes and we do not use them.*
For $q = 3$*, the integral closure produced is*

$[1,$

$y,$

$y^2,$

$y^3],$

and the corresponding weight is $[0, 11, 22, 33]$*. The number of weights here are fewer than we expect. So* $q = 3$ *is not good.*

For $q = 5$*, the integral closure produced is*

$[x^{14} + 3x^4,$

$y^4x^7 + y^2x^{10} + y^3x^7 + 4y^4x^5 + 3yx^{10} + y^2x^8 + 4x^{11} + 4y^2x^7 + 4y^3x^5 + 2y^4x^3 + 3yx^8 + x^9 +$
$y^2x^5 + 2y^3x^3 + 2y^4x + y^2x^4 + 3x^7 + 3y^2x^3 + 2y^3x + 3yx^4 + 4y^2x^2 + 3x^5 + 3y^2x + 2yx^2,$

$y^2x^{11} + 3y^4x^6 + 3yx^{11} + 3y^2x^9 + 3y^3x^6 + 2y^4x^4 + 4yx^9 + 3y^2x^7 + 2x^{10} + 2y^2x^6 + 2y^3x^4 + y^4x^2 +$
$4yx^7 + 3x^8 + 3y^2x^4y^3x^2 + y^4 + 3y^2x^3 + 4x^6 + 4y^2x^2 + y^3 + 4yx^3 + 4x^4 + 4y^2,$

$yx^{14} + 3yx^4,$

$y^5x^7 + y^3x^{10} + 4y^5x^5 + 2y^2x^{10} + y^3x^8 + 4yx^{11} + 3y^3x^7 + 2y^5x^3 + 2yx^{10} + 2y^2x^8 + x^{11} + yx^9 + y^2x^7 + 2y^3x^5 + 2y^5x + 2yx^8 + y^3x^4 + 4x^9 + 3yx^7 + 4y^2x^5 + y^3x^3 + 2y^2x^4 + 4y^3x^2 + 2x^7 + 3yx^5 + 2y^2x^3 + y^3x + 2yx^4 + 3y^2x^2 + 2x^5 + 2y^2x + 3yx^2,$

$y^3x^{11} + 3y^5x^6 + 3y^3x^9 + 4y^4x^6 + 2y^5x^4 + yx^{11} + 3y^3x^7 + 2yx^{10} + 3y^3x^6 + y^4x^4 + y^5x^2 + 3yx^9 + 4x^{10} + 3yx^8 + 4y^2x^6 + 2y^3x^4 + 3y^4x^2 + y^5 + 3yx^7 + 3y^3x^3 + x^8 + 4yx^6 + y^2x^4 + y^3x^2 + 3y^4 + 3x^6 + 4yx^4 + 3y^2x^2 + y^3 + 3yx^3 + 3x^4 + 3y^2]$, *and the corresponding weight is* $[0, 2, 4, 11, 13, 15]$. *These weights turn out to be "smaller" than what we expect.*

For $q = 7$*, the integral closure produced is*

$[x^5 + 2x^4,$

$y^2x^3 + 2y^2x^2 + yx^3 + 2x^4 + 2yx^2 + 4x^3,$

$yx^5 + 2yx^4,$

$y^4x + 2y^4 + 2y^3x + 4y^2x^2 + 4y^3 + 2y^2x + 4yx^2 + 2y^2 + 4x^3 + yx + x^2,$

$y^3x^3 + 2y^3x^2 + 2yx^4 + 3yx^3 + 5x^4 + 5yx^2 + 3x^3,$

$y^5 + 2y^3x^2 + 6y^4 + 4y^3x + 2yx^4 + 3y^2x^2 + 2y^3 + 4yx^3 + 6y^2x + x^4 + 5yx^2 + 4y^2 + 2x^3 + 2yx + 2x^2]$, *and the corresponding weight is* $[0, 10, 11, 20, 21, 25]$. *These weights turn out to be "smaller" than what we expect.*

For $q = 11$*, the integral closure produced is*

$[x^5 + 4x^4,$

$y^2x^3 + 4y^2x^2 + 2yx^3 + 3x^4 + 8yx^2 + x^3,$

$yx^5 + 4yx^4,$

$y^4x + 4y^4 + 4y^3x + 6y^2x^2 + 5y^3 + 6y^2x + yx^2 + 5y^2 + 9x^3 + 4yx + 3x^2,$

$y^3x^3 + 4y^3x^2 + 3yx^4 + 8yx^3 + 5x^4 + 6yx^2 + 9x^3,$

$y^5 + 4y^3x^2 + 5y^4 + 6y^3x + 7yx^4 + y^2x^2 + 8y^3 + yx^3 + 7y^2x + 7x^4 + 6yx^2 + 4y^2 + x^3 + yx + 9x^2]$, *and the corresponding weight is* $[0, 10, 11, 20, 21, 25]$. *These weights turn out to be "smaller" than what we expect.*

The first good prime is $q = 13$*. The integral closure and its corresponding weights for this prime are*

$[x^4,$

$y^2x^2 + 9yx^2 + 6x^3,$

$yx^4,$

$y^4 + 5y^3 + 12y^2x + 3y^2 + 4yx + 10x^2,$

$y^3x^2 + 6yx^3 + 10yx^2 + 11x^3,$

$y^5 + 12y^3x + 4y^3 + 9y^2x + 10yx^2 + 11y^2 + 6yx + 2x^2]$*, and*

$[0, 10, 11, 20, 21, 31]$.

The integral closure over the rationals for the sequence, (13)*, of good primes is*

$[x^4,$

$y^2x^2 + \frac{1}{3}yx^2 - \frac{1}{2}x^3,$

$yx^4,$

$y^4 - \frac{3}{2}y^3 - y^2x + 3y^2 - \frac{1}{3}yx - 3x^2,$

$y^3x^2 - \frac{1}{2}yx^3 - 3yx^2 - 2x^3,$

$y^5 - y^3x - \frac{1}{3}y^3 + \frac{1}{3}y^2x - 3yx^2 - 2y^2 - \frac{1}{2}yx + 2x^2].$

The next good prime is $q = 19$*. The integral closure and its corresponding weights for this prime are*

$[x^4,$

$y^2x^2 + 4yx^2 + 17x^3,$

$yx^4,$

$y^4 + 8y^3 + 15y^2x + 16y^2 + 3yx + 4x^2,$

$y^3x^2 + 17yx^3 + 3yx^2 + 8x^3,$

$y^5 + 15y^3x + 9y^3 + 16y^2x + 4yx^2 + 5y^2 + 14yx + 6x^2]$*, and*

$[0, 10, 11, 20, 21, 31]$.

The integral closure over the rationals for the sequence, $(13, 19)$*, of good primes is*

$[x^4,$

$y^2x^2 - \frac{3}{4}yx^2 + \frac{11}{4}x^3,$

$yx^4,$

$y^4 - \frac{3}{2}y^3 + \frac{11}{2}y^2x - \frac{7}{15}y^2 + \frac{2}{7}yx + \frac{6}{11}x^2,$

$y^3x^2 + \frac{11}{4}yx^3 + \frac{7}{15}yx^2 - \frac{1}{7}x^3,$

$y^5 + \frac{11}{2}y^3x + \frac{7}{5}y^3 - \frac{2}{7}y^2x + \frac{6}{11}yx^2 - \frac{7}{10}y^2 + \frac{3}{7}yx + \frac{9}{11}x^2].$

The next good prime is $q = 23$. *The integral closure and its corresponding weights for this prime are*

$[x^4,$

$y^2x^2 + 5yx^2 + 14x^3,$

$yx^4,$

$y^4 + 10y^3 + 5y^2x + 2y^2 + 2yx + 12x^2,$

$y^3x^2 + 14yx^3 + 21yx^2 + 22x^3,$

$y^5 + 5y^3x + 17y^3 + 21y^2x + 12yx^2 + 3y^2 + 3yx + 18x^2]$, *and*

$[0, 10, 11, 20, 21, 31].$

The integral closure over the rationals for the sequence, $(13, 19, 23)$, *of good primes is*

$[x^4,$

$y^2x^2 - \frac{3}{4}yx^2 - \frac{15}{17}x^3,$

$yx^4,$

$y^4 - \frac{3}{2}y^3 - \frac{30}{17}y^2x + \frac{9}{16}y^2 + \frac{45}{34}yx + \frac{29}{12}x^2,$

$y^3x^2 - \frac{15}{17}yx^3 - \frac{9}{16}yx^2 + \frac{67}{25}x^3,$

$y^5 - \frac{30}{17}y^3x - \frac{27}{16}y^3 - \frac{45}{34}y^2x + \frac{29}{12}yx^2 + \frac{27}{32}y^2 - \frac{22}{31}yx + \frac{29}{8}x^2].$

The next good prime is $q = 29$. *The integral closure and its corresponding weights for this prime are*

$[x^4,$

$y^2x^2 + 21yx^2 + 23x^3,$

$yx^4,$

$y^4 + 13y^3 + 17y^2x + 6y^2 + 9yx + 7x^2,$

$y^3x^2 + 23yx^3 + 23yx^2 + 10x^3,$

$y^5 + 17y^3x + 11y^3 + 20y^2x + 7yx^2 + 9y^2 + 28yx + 25x^2]$, *and*

$[0, 10, 11, 20, 21, 31].$

The integral closure over the rationals for the sequence, $(13, 19, 23, 29)$, *of good primes is*

$[x^4,$

$y^2x^2 - \frac{3}{4}yx^2 - \frac{15}{17}x^3,$

$yx^4,$

$y^4 - \frac{3}{2}y^3 - \frac{30}{17}y^2x + \frac{9}{16}y^2 + \frac{45}{34}yx + \frac{225}{289}x^2,$

$y^3x^2 - \frac{15}{17}yx^3 - \frac{9}{16}yx^2 - \frac{45}{68}x^3,$

$y^5 - \frac{30}{17}y^3x - \frac{27}{16}y^3 - \frac{45}{34}y^2x + \frac{225}{289}yx^2 + \frac{27}{32}y^2 + \frac{135}{68}yx - \frac{83}{173}x^2].$

The next good prime is $q = 31$. *The integral closure and its corresponding weights for this prime are*

$[x^4,$

$y^2x^2 + 7yx^2 + 21x^3,$

$yx^4,$

$y^4 + 14y^3 + 11y^2x + 18y^2 + 15yx + 7x^2,$

$y^3x^2 + 21yx^3 + 13yx^2 + 8x^3,$

$y^5 + 11y^3x + 8y^3 + 16y^2x + 7yx^2 + 27y^2 + 7yx + 26x^2]$, *and*

$[0, 10, 11, 20, 21, 31].$

The integral closure over the rationals for the sequence, $(13, 19, 23, 29, 31)$, *of good primes is*

$[x^4,$

$y^2x^2 - \frac{3}{4}yx^2 - \frac{15}{17}x^3,$

$yx^4,$

$y^4 - \frac{3}{2}y^3 - \frac{30}{17}y^2x + \frac{9}{16}y^2 + \frac{45}{34}yx + \frac{225}{289}x^2,$

$y^3x^2 - \frac{15}{17}yx^3 - \frac{6}{16}yx^2 - \frac{45}{68}x^3,$

$y^5 - \frac{30}{17}y^3x - \frac{27}{16}y^3 - \frac{45}{34}y^2x + \frac{225}{289}yx^2 + \frac{27}{32}y^2 + \frac{135}{68}yx + \frac{675}{578}x^2].$

The next good prime is $q = 37$. *The integral closure and its corresponding weights for this prime are*

$[x^4,$

$y^2x^2 + 27yx^2 + 10x^3,$

$yx^4,$

$y^4 + 17y^3 + 20y^2x + 26y^2 + 22yx + 26x^2,$

$y^3x^2 + 10yx^3 + 11yx^2 + 26x^3,$

$y^5 + 20y^3x + 33y^3 + 15y^2x + 26yx^2 + 2y^2 + 33yx + 2x^2]$, *and*

$[0, 10, 11, 20, 21, 31]$.

The integral closure over the rationals for the sequence, $(13, 19, 23, 29, 31, 37)$, *of good primes is*

$[x^4,$

$y^2x^2 - \frac{3}{4}yx^2 - \frac{15}{17}x^3,$

$yx^4,$

$y^4 - \frac{3}{2}y^3 - \frac{30}{17}y^2x + \frac{9}{16}y^2 + \frac{45}{34}yx + \frac{225}{289}x^2,$

$y^3x^2 - \frac{15}{17}yx^3 - \frac{9}{16}yx^2 - \frac{45}{68}x^3,$

$y^5 - \frac{30}{17}y^3x - \frac{27}{16}y^3 - \frac{45}{34}y^2x + \frac{225}{289}yx^2 + \frac{27}{32}y^2 + \frac{135}{68}yx + \frac{675}{578}x^2]$.

which stabilizes as the integral closure over the rationals.

Hence we do not use the primes $[2, 3, 5, 7, 11, 17, 7027, 10987, 25303, 61843, 131581, 4818577, 1364771771210789848864664 9543]$.

Example 4.4. *Let* $f = (y^2 - \frac{3}{4}y - \frac{15}{17}x)^3 - 9yx^4(y^2 - \frac{3}{4}y - \frac{15}{17}x) - 27x^{11}$

It is immediate that 2 *and* 17 *are possibly "bad" primes. As we shall see, the primes* $(3, 5, 17)$ *are also possibly "bad" primes and we do not use them.*

For $q = 3$, *the integral closure produced is*

$[1,$

$y,$

$y^2,$

$y^3]$, *and*

the corresponding weight is $[0, 11, 22, 33]$. *The number of weights here are fewer than we expect. So* $q = 3$ *is not good.*

For $q = 5$, *the integral closure produced is*

$[x^7,$

$y^2x^5 + 3yx^5,$

$yx^7,$

$y^5 + y^2x^4 + 4y^4 + 3yx^4 + 2y^3 + 2y^2,$

$y^3x^4 + y^2x^4 + 4yx^4,$

$y^4x^3 + y^3x^3 + 4y^2x^3],$

and the corresponding weight is $[0, 10, 11, 13, 15, 20]$. *These weights turn out to be "smaller" than what we expect.*

The first good prime is $q = 7$. *The integral closure and its corresponding weights for this prime are*

$[x^5,$

$y^2x^3 + yx^3 + 2x^4,$

$yx^5,$

$y^4x + 2y^3x + 4y^2x^2 + y^2x + 4yx^2 + 4x^3,$

$y^3x^3 + 2yx^4 + 6yx^3 + 5x^4,$

$y^5 + 3y^4 + 4y^3x + 3y^3 + y^2x + 4yx^2 + y^2 + 4yx + 4x^2]$, *and*

$[0, 10, 11, 20, 21, 31]$.

The integral closure over the rationals for the sequence, (7), *of good primes is*

$[x^5,$

$y^2x^3 + yx^3 + 2x^4,$

$yx^5,$

$y^4x + 2y^3x + \frac{1}{2}y^2x^2 + y^2x + \frac{1}{2}yx^2 + \frac{1}{2}x^3,$

$y^3x^3 + 2yx^4 - yx^3 - 2x^4,$

$y^5 - \frac{1}{2}y^4 + \frac{1}{2}y^3x - \frac{1}{2}y^3 + y^2x + \frac{1}{2}yx^2 + y^2 + \frac{1}{2}yx + \frac{1}{2}x^2].$

The next good prime is $q = 11$*. The integral closure and its corresponding weights for this prime are*

$[x^5,$

$y^2x^3 + 2yx^3 + 3x^4,$

$yx^5,$

$y^4x + 4y^3x + 6y^2x^2 + 4y^2x + yx^2 + 9x^3,$

$y^3x^3 + 3yx^4 + 7yx^3 + 5x^4,$

$y^5 + 6y^4 + 6y^3x + y^3 + 2y^2x + 9yx^2 + 8y^2 + 2yx + 7x^2],$ *and*

$[0, 10, 11, 20, 21, 31].$

The integral closure over the rationals for the sequence, $(7, 11)$*, of good primes is*

$[x^5,$

$y^2x^3 - \frac{3}{4}yx^3 + \frac{1}{4}x^4,$

$yx^5,$

$y^4x - \frac{3}{2}y^3x + \frac{1}{2}y^2x^2 - \frac{2}{5}y^2x + yx^2 + \frac{5}{3}x^3,$

$y^3x^3 + \frac{1}{4}yx^4 + \frac{2}{5}yx^3 + 5x^4,$

$y^5 + \frac{8}{5}y^4 + \frac{1}{2}y^3x - \frac{6}{5}y^3 - \frac{3}{4}y^2x + \frac{5}{3}yx^2 + 8y^2 - \frac{1}{5}yx - \frac{5}{4}x^2].$

The next good prime is $q = 13$*. The integral closure and its corresponding weights for this prime are*

$[x^5,$

$y^2x^3 + 9yx^3 + 6x^4,$

$yx^5,$

$y^4x + 5y^3x + 12y^2x^2 + 3y^2x + 4yx^2 + 10x^3,$

$y^3x^3 + 6yx^4 + 10yx^3 + 11x^4,$

$y^5 + y^4 + 12y^3x + 9y^3 + 8y^2x + 10yx^2 + y^2 + 10yx + 12x^2],$ *and*

$[0, 10, 11, 20, 21, 31].$

The integral closure over the rationals for the sequence, $(7, 11, 13)$, *of good primes is*

$[x^5,$

$y^2x^3 - \frac{3}{4}yx^3 - \frac{15}{17}x^4,$

$yx^5,$

$y^4x - \frac{3}{2}y^3x + \frac{1}{2}y^2x^2 + \frac{9}{16}y^2x + \frac{1}{23}yx^2 + \frac{16}{25}x^3,$

$y^3x^3 - \frac{15}{17}yx^4 - \frac{9}{16}yx^3 - 2x^4,$

$y^5 - \frac{9}{4}y^4 + \frac{1}{2}y^3x + \frac{27}{16}y^3 + \frac{2}{23}y^2x + \frac{16}{25}yx^2 + y^2 + \frac{10}{27}yx - \frac{12}{25}x^2].$

The next good prime is $q = 19$. *The integral closure and its corresponding weights for this prime are*

$[x^5,$

$y^2x^3 + 4yx^3 + 17x^4,$

$yx^5,$

$y^4x + 8y^3x + 15y^2x^2 + 16y^2x + 3yx^2 + 4x^3,$

$y^3x^3 + 17yx^4 + 3yx^3 + 8x^4,$

$y^5 + 12y^4 + 15y^3x + 10y^3 + 6y^2x + 4yx^2 + 7y^2 + 12yx + 16x^2]$, *and*

$[0, 10, 11, 20, 21, 31].$

The integral closure over the rationals for the sequence, $(7, 11, 13, 19)$, *of good primes is*

$[x^5,$

$y^2x^3 - \frac{3}{4}yx^3 - \frac{15}{17}x^4,$

$yx^5,$

$y^4x - \frac{3}{2}y^3x - \frac{30}{17}y^2x^2 + \frac{9}{16}y^2x + \frac{45}{34}yx^2 - \frac{67}{83}x^3,$

$y^3x^3 - \frac{15}{17}yx^4 - \frac{9}{16}yx^3 - \frac{45}{68}x^4,$

$y^5 - \frac{9}{4}y^4 - \frac{30}{17}y^3x + \frac{27}{16}y^3 + \frac{45}{17}y^2x - \frac{67}{83}yx^2 - \frac{27}{64}y^2 + \frac{17}{3}yx + \frac{10}{3}x^2].$

The next good prime is $q = 23$. *The integral closure and its corresponding weights for this prime are*

$[x^5,$

$y^2x^3 + 5yx^3 + 14x^4,$

$yx^5,$

$y^4x + 10y^3x + 5y^2x^2 + 2y^2x + 2yx^2 + 12x^3,$

$y^3x^3 + 14yx^4 + 21yx^3 + 22x^4,$

$y^5 + 15y^4 + 5y^3x + 6y^3 + 4y^2x + 12yx^2 + 10y^2 + 10yx + 14x^2]$, *and*

$[0, 10, 11, 20, 21, 31].$

The integral closure over the rationals for the sequence, $(7, 11, 13, 19, 23)$, *of good primes is*

$[x^5,$

$y^2x^3 - \frac{3}{4}yx^3 - \frac{15}{17}x^4,$

$yx^5,$

$y^4x - \frac{3}{2}y^3x - \frac{30}{17}y^2x^2 + \frac{9}{16}y^2x + \frac{45}{34}yx^2 + \frac{225}{289}x^3,$

$y^3x^3 - \frac{15}{17}yx^4 - \frac{9}{16}yx^3 - \frac{45}{68}x^4,$

$y^5 - \frac{9}{4}y^4 - \frac{30}{17}y^3x + \frac{27}{16}y^3 + \frac{45}{17}y^2x + \frac{225}{289}yx^2 - \frac{27}{64}y^2 - \frac{135}{136}yx + \frac{4}{43}x^2].$

The next good prime is $q = 29$. *The integral closure and its corresponding weights for this prime are*

$[x^5,$

$y^2x^3 + 21yx^3 + 23x^4,$

$yx^5,$

$y^4x + 13y^3x + 17y^2x^2 + 6y^2x + 9yx^2 + 7x^3,$

$y^3x^3 + 23yx^4 + 23yx^3 + 10x^4,$

$y^5 + 5y^4 + 17y^3x + 18y^3 + 18y^2x + 7yx^2 + 10y^2 + 15yx + 2x^2]$, *and*

$[0, 10, 11, 20, 21, 31].$

The integral closure over the rationals for the sequence, $(7, 11, 13, 19, 23, 29)$, *of good primes is*

$[x^5,$

$y^2x^3 - \frac{3}{4}yx^3 - \frac{15}{17}x^4,$

$yx^5,$

$y^4x - \frac{3}{2}y^3x - \frac{30}{17}y^2x^2 + \frac{9}{16}y^2x + \frac{45}{34}yx^2 + \frac{225}{289}x^3,$

$y^3x^3 - \frac{15}{17}yx^4 - \frac{9}{16}yx^3 - \frac{45}{68}x^4,$

$y^5 - \frac{9}{4}y^4 - \frac{30}{17}y^3x + \frac{27}{16}y^3 + \frac{45}{17}y^2x + \frac{225}{289}yx^2 - \frac{27}{64}y^2 - \frac{135}{136}yx - \frac{675}{1156}x^2].$

The next good prime is $q = 31$*. The integral closure and its corresponding weights for this prime are*

$[x^5,$

$y^2x^3 + 7yx^3 + 21x^4,$

$yx^5,$

$y^4x + 14y^3x + 11y^2x^2 + 18y^2x + 15y^2 + 7x^3,$

$y^3x^3 + 21yx^4 + 13yx^3 + 8x^4,$

$y^5 + 21y^4 + 11y^3x + 23y^3 + 30y^2x + 7yx^2 + 2y^2 + 12yx + 18x^2]$*, and*

$[0, 10, 11, 20, 21, 31].$

The integral closure over the rationals for the sequence, $(7, 11, 13, 19, 23, 29, 31)$*, of good primes is*

$[x^5,$

$y^2x^3 - \frac{3}{4}yx^3 - \frac{15}{17}x^4,$

$yx^5,$

$y^4x - \frac{3}{2}y^3x - \frac{30}{17}y^2x^2 + \frac{9}{16}y^2x + \frac{45}{34}yx^2 + \frac{225}{289}x^3,$

$y^3x^3 - \frac{15}{17}yx^4 - \frac{9}{16}yx^3 - \frac{45}{68}x^4,$

$y^5 - \frac{9}{4}y^4 - \frac{30}{17}y^3x + \frac{27}{16}y^3 + \frac{45}{17}y^2x + \frac{225}{289}yx^2 - \frac{27}{64}y^2 - \frac{135}{136}yx - \frac{675}{1156}x^2].$

Hence we do not use the primes $[2, 3, 5, 17, 521, 1663, 44371, 2290471, 21589481, 144024110264869597351073965556603]$*.*

Chapter 5

Integral closures of maximal order of number fields

Let $f(T) \in \mathbf{Z}[T]$ be a monic polynomial of degree m. Let $I := \langle f(x) \rangle$ be an ideal in $\mathbf{Z}[x]$. Define the *maximal order* $R := \mathbf{Z}[x]/I$ of the *number field* $\mathbf{Q}[x]/I$. There exists a conductor element $\Delta \in \mathbf{Z}^+$ such that

$$R \subseteq ic(R) \subseteq \Delta^{-1}R.$$

5.1 Computation using the q^{th}-power algorithm

$M^{(0)} := \Delta^{-1}R$ is a $\mathbf{Z}$-module with standard basis $\{(\Delta^{-1}x^i),\ 0 \leq i < m\}$. Recursively define sets $S^{(j)} := \{\Delta^{-1}f \in M^{(j-1)} : \Delta^{-n}NF(f^n, I) \in M^{(j-1)} \text{ for all } n\}$, and $\mathbf{Z}$-modules $M^{(j)} := \mathbf{Z}\langle S^{(j)} \rangle$. Clearly $M^{(j)} \subseteq M^{(j-1)}$ for all j. $M^{(j)}$ contains $ic(R)$ and has a basis $\{(\Delta^{-1}f_i^{(j)}),\ 0 \leq i < m\}$, with degree$(f_i^{(j)}) = i$. Indeed, as a $\mathbb{Z}$-module, $ic(R)$ has basis $\{F_i : \text{degree}(F_i) = i\}$ for all i. Hence each $M^{(j)}$ has basis elements of the form

$$f_i^{(j)} = \sum_{k \leq i} q_{i,k}^{(j)} F_k, \text{where } q_{i,k}^{(j)} \neq 0,\ q_{i,k}^{(j)} \in \mathbb{Q}, \text{for each } i.$$

Consider the following example.

Example 5.1. *Let* $f(x) := x^4 - 420x^2 + 40000 \in \mathbf{Z}[x]$. *Then* $\Delta M^{(0)} := \langle 1, x, x^2, x^3 \rangle$.

Below is a *Magma* computation that produces a subset, say, $\overline{S^{(1)}} \subseteq S^{(1)}$ from $S^{(0)}$.

```
F:= RationalField();

P<x>:=PolynomialRing(Integers( ),1);

f1 := (x^4-420*x^2+40000);
```

```
I:=ideal<P|f1>;

G:=GroebnerBasis(I);G;

JM:=JacobianMatrix(G);JM;

M:=Minors(JM,1);M;

J:=ideal<P|G,M>;

B:=GroebnerBasis(J);

delta:=B[#B];

"delta =",delta;

factors_of_delta:= Factorization(delta);  factors_of_delta;

///=====================================================================;

Q:=Integers();

P<x,a3,a2,a1,a0>:=PolynomialRing(Q,5);

f:=x^4-420*x^2+40000;

co:=function(h,i) return Coefficient(h,x,i); end function;

n:=function(g) l:=NormalForm(g^2,[f]); return l;  end function;

del:=   65600000;

Factorization(del);

///===================================================;

g0:=1;

g1:=x;

g2:=x^2;

g3:=x^3;

p:=5;

a1:=2*a1+a3;

a2:=2*a2;

a0:=2*a0; a1:=2*a1; a3:=2*a3;

a0:=2*a0;  a2:=2*a2;
```

```
a0:=2*a0; a1:=2*a1+a2+a3;
a0:=2*a0; a1:=2*a1+a3;   a2:=2*a2;
a0:=2*a0;   a1:=2*a1+a3;
a2:=5*a2;
a0:=5*a0+a2;  a1:=5*a1+2*a3;
a0:=5*a0; a2:=5*a2;
a0:=5*a0;  a1:=5*a1;
a0:=41*a0 - 5*a2;  a1:=41*a1 - 5*a3;
b3:=a3; b2:=a2; b1:=a1; b0:=a0;
h3:=n(b3*g3 + b2*g2 + b1*g1 + b0*g0);
i3:=co(h3,3) div co(g3,3); 3, "i3 =",i3;
h2:=h3 - i3*g3; "h2 =",h2;
i2:=co(h2,2) div co(g2,2); 2, "i2 =",i2;
h1:=h2 - i2*g2; "h1 =",h1;
i1:=co(h1,1) div co(g1,1); 1, "i1 =",i1;
h0:=h1 - i1*g1; "h0 =",h0;
i0:=h0 div g0; 0, "i0 =",i0;
I:=[i3,i2,i1,i0];
k3:=GCD(Coefficients(i3));  3, "k3 =",k3;
k2:=GCD(Coefficients(i2));  2, "k2 =",k2;
k1:=GCD(Coefficients(i1));  1, "k1 =",k1;
k0:=GCD(Coefficients(i0));  0, "k0 =",k0;
k:=[k3,k2,k1,k0];
k:=[GCD(Coefficients(I[l])):l in [1..4]]; "k =",k;
kk:=[del div GCD(k[l],del): l in [1..4]|k[l] ne 0]; "kk =",kk;
R<a0,a1,a2,a3>:=PolynomialRing(GF(p),4);
hPR:=hom<P->R|0,a3,a2,a1,a0>;
```

```
j:=[hPR(I[l] div k[l]): l in [1..4] | (k[l] ne 0)

and (((del div GCD(k[l],del)) mod p) eq 0)];

"j=",j;

J:=ideal<R|j, a3^p -a3, a2^p-a2, a1^p-a1,a0^p-a0>;

RR:=Radical(J);

G:=GroebnerBasis(RR); "G =",G;

h:=b3*g3 + b2*g2 + b1*g1 + b0*g0;

"h=",h;    "b0 =",b0;  "b1 =",b1;  "b2 =",b2;  "b3 =",b3;

/////////////////////////////////
```

give us the following outputs;

```
p = 41

G = [  a0 + 5*a2,        //  linear relation

       a1 + 5*a3,        //  linear relation

       a2^41 + 40*a2,

       a3^41 + 40*a3 ]

h = x^3*a3 + x^2*a2 + x*a1 + a0

G = [ a0^41 + 40*a0,

      a1^41 + 40*a1,

      a2^41 + 40*a2,

      a3^41 + 40*a3  ]

h = x^3*a3 + x^2*a2 - 5*x*a3 + 41*x*a1 - 5*a2 + 41*a0

p = 5

G = [ a0,              //  linear relation

      a1^5 + 4*a1,

      a2,              //  linear relation

      a3^5 + 4*a3  ]

h = x^3*a3 + x^2*a2 - 5*x*a3 + 205*x*a1 - 5*a2 + 205*a0
```

```
G = [ a0 + 4*a2,       //  linear relation

      a1 + 3*a3,       //  linear relation

      a2^5 + 4*a2,

      a3^5 + 4*a3  ]

h = x^3*a3 + 5*x^2*a2 - 5*x*a3 + 205*x*a1 - 25*a2 + 1025*a0

G = [ a0^5 + 4*a0,

      a0*a3,

      a1^5 + 4*a1,

      a2,              //  linear relation

      a3^5 + 4*a3   ]

h = x^3*a3 + 5*x^2*a2 + 405*x*a3 + 1025*x*a1 + 1000*a2 + 5125*a0

G = [ a0^5 + 4*a0,

      a0*a1,

      a0*a3,

      a1^2 + a1*a3,

      a1*a3^4 + 4*a1,

      a2^5 + 4*a2,

      a3^5 + 4*a3  ]

h = x^3*a3 + 25*x^2*a2 + 405*x*a3 + 1025*x*a1 + 5000*a2 + 5125*a0

p = 2

G = [ a0,        //  linear relation

      a1 + a3,   //  linear relation

      a2,        //  linear relation

      a3^2 + a3  ]

h = x^3*a3 + 25*x^2*a2 + 1430*x*a3 + 2050*x*a1 + 5000*a2 + 10250*a0

G = [ a0,

      a1 + a2 + a3,
      a2^2 + a2,
      a3^2 + a3  ]
h = x^3*a3 + 50*x^2*a2 + 3480*x*a3 + 4100*x*a1 + 10000*a2 + 20500*a0
G = [ a0,           //  linear relation
      a1^2 + a1,
      a2,           //  linear relation
      a3^2 + a3  ]
h = x^3*a3 + 50*x^2*a2 + 7580*x*a3 + 4100*x*a2 + 8200*x*a1
      + 10000*a2 + 41000*a0
G = [  a0,            //  linear relation
       a1,            //  linear relation
       a2^2 + a2,
       a3  ]          //  linear relation
h = x^3*a3 + 100*x^2*a2 + 7580*x*a3 + 8200*x*a2 + 8200*x*a1
 + 20000*a2 + 82000*a0
G = [  a0^2 + a0,
       a1^2 + a1,
       a2,             //  linear relation
       a3^2 + a3  ]
h = 2*x^3*a3 + 100*x^2*a2 + 15160*x*a3 + 8200*x*a2
    + 16400*x*a1   + 20000*a2 +  164000*a0
G = [  a0^2 + a0,
       a0*a3,
       a1 + a3,        //  linear relation
       a2^2 + a2,
       a3^2 + a3  ]
h = 2*x^3*a3 + 200*x^2*a2 + 15160*x*a3 + 16400*x*a2
```

```
 +  16400*x*a1 + 40000*a2 + 164000*a0

G = [ a0^2 + a0,

       a0*a3,

       a1^2 + a1,

       a2^2 + a2,

       a3^2 + a3 ]

h = 2*x^3*a3 + 200*x^2*a2 + 31560*x*a3 + 16400*x*a2

 +  32800*x*a1 + 40000*a2 + 164000*a0
```

Let $S^{(j)}$ and $M^{(j)}$ be defined as in above. Let $\overline{S^{(j)}}$ be a subset of $S^{(j)}$, obtained from the linear relations in the Gröbner basis computations generating $S^{(j)}$. Let $\overline{M^{(j)}} := \mathbf{Z}\langle\overline{S^{(j)}}\rangle$. Looking at the above example and considering the linear relations in the Gröbner computations we get that

$\Delta\overline{S^{(1)}} = \{164000, 32800x, 200x^2 + 16400x + 40000, 2x^3 - 1240x\}$, and $\Delta\overline{M^{(1)}} := \mathbf{Z}\langle\overline{S^{(1)}}\rangle$.

Similarly by repeating the process we get

$\Delta\overline{S^{(2)}} = \{3280000, 3280000x, 164000x^2 + 1640000x, 8200x^3 - 5084000x\}$, and $\Delta\overline{M^{(2)}} := \mathbf{Z}\langle\overline{S^{(2)}}\rangle$.

$\Delta\overline{S^{(3)}} = \{32800000, 6560000x, 1640000x^2 + 16400000x, 16400x^3 - 10168000x\}$, and $\Delta\overline{M^{(3)}} := \mathbf{Z}\langle\overline{S^{(3)}}\rangle$.

$\Delta\overline{S^{(4)}} = \{65600000, 32800000x, 1640000x^2 + 16400000x, 82000x^3 - 50840000x + 32800000\}$, and $\Delta\overline{M^{(4)}} := \mathbf{Z}\langle\overline{S^{(4)}}\rangle$.

$\Delta\overline{S^{(5)}} = \{65600000, 32800000x, 1640000x^2 + 16400000x, 82000x^3 - 50840000x + 32800000\}$, and $\Delta\overline{M^{(5)}} := \mathbf{Z}\langle\overline{S^{(5)}}\rangle$.

We compute $\overline{M^{(L)}}$ until $\overline{M^{(L+1)}} = \overline{M^{(L)}}$ for some $L \in \mathbb{N}$. The above example illustrates how we can get $\overline{M^{(1)}}$ from $\overline{M^{(0)}}$. The process is the same to get any other $\overline{M^{(L)}}$ until $\overline{M^{(L+1)}} = \overline{M^{(L)}}$ for some $L \in \mathbb{N}$.

We want to show that $\overline{M^{(L+1)}} = \overline{M^{(L)}}$ for some $L \in \mathbb{N}$.

Lemma 5.1. *Let R, $ic(R)$, $S^{(j)}$, $\overline{S^{(j)}}$ and $M^{(j)}$, $\overline{M^{(j)}}$ be as above. Then any sequence $\Delta^{-1}R = M^{(0)} \supseteq M^{(1)} \supseteq M^{(2)} \supseteq \cdots$ of $\mathbb{Z}$-modules containing $ic(R)$ is finite. That is, $\overline{M^{(L+1)}} = \overline{M^{(L)}}$ for some $L \in \mathbb{N}$.*

Proof: Let $\Delta^{-1}f \in S^{(j)}$ be arbitrary with, $LT(f) = x^i$. It is very important to note here that $S^{(j)}$ is not necessarily closed under linear combinations. However, given any $\Delta^{-1}f \in S^{(j)}$ then $\Delta^{-1}f \in M^{(j-1)}$. But as earlier observed, $M^{(j-1)}$ has a $\mathbb{Z}$-module basis $\{\Delta^{-1}g_k,\ \ 0 \leq k < m\}$. Hence

$$(\Delta^{-1}f)^n \equiv \sum_{k=0}^{m-1} z_{n,k}(\Delta^{-1}g_k)$$

for all $n \in \mathbb{N}$, and some $z_{n,k} \in \mathbb{Z}$, with the above sum in $M^{(j-1)}$.

If the ***leading coefficient***, $LC(f)$, does not divide Δ, then we can add some $(\alpha \cdot \Delta)x^i$ to $(\beta \cdot LC(f))x^i$, with $\alpha,\ \beta \in \mathbf{Z}$, such that $d := (\alpha \cdot \Delta + \beta \cdot LC(f))$ divides Δ. Clearly, Δ has a finite number of factors. Thus the set, $\{LC(f) : \Delta^{-1}f \in S^{(j)}\}$, is finite. Hence we can pick a finite subset $\overline{S^{(j)}}$ of $S^{(j)}$ that generates $\overline{M^{(j)}}$, since for each monomial x^i, there exists a $\Delta^{-1}f \in \overline{S^{(j)}}$ with leading monomial, $LM(f) = x^i$.

Also, we know that $\overline{M^{(j)}} \subseteq \overline{M^{(j-1)}}$ is a finitely generated submodule and there are a finite number of x^i's. Thus $\overline{M^{(j-1)}}$ has a finite number of finitely generated submodules. Hence the process that produces $\overline{M^{(j)}}$ from $\overline{M^{(j-1)}}$ must terminate. Thus there exists $L \in \mathbb{N}$ such that $\overline{M^{(L+1)}} = \overline{M^{(L)}}$. □

Let us write $M^{(L+1)} := \overline{M^{(L+1)}}$ and $S^{(L+1)} := \overline{S^{(L+1)}}$. As a consequence of the above lemma, we have the following corollary.

Corollary 5.1. *Let $S^{(j)}$ and $M^{(j)}$ be as in lemma 5.1 above. Then $M^{(L+n)} = M^{(L)}$ for all $n \in \mathbb{N}$.*

The proof of the above corollary follows immediately by induction on n. □

Corollary 5.2. *Let $S^{(j)}$ and $M^{(j)}$ be as in lemma 5.1 above. Then $\Delta^{-1}f \in M^{(L)} \Rightarrow (\Delta^{-1}f)^n \in M^{(L)}$ for all $n \in \mathbb{N}$.*

Proof:

$$\begin{aligned}
&\Delta^{-1}f \in M^{(L)} = M^{(L+n)}\\
&\Rightarrow (\Delta^{-2}f^2) \in M^{(L+n-1)} = M^{(L)}\\
&\Rightarrow \cdots\\
&\Rightarrow \Delta^{-n}f^n \in M^{(L)}. \ \square
\end{aligned}$$

Our next major goal is to show that when $\overline{M^{(L)}} = \overline{M^{(L+1)}}$ for some $L \in \mathbb{N}$, then every element in $\overline{M^{(L)}}$ is integral. Before proving that the elements in $\overline{M^{(L)}} = \overline{M^{(L+1)}}$ are integral, let us show that this is the case with our last example.

Example 5.2. *We saw in our last example that* $\overline{M^{(4)}} = \overline{M^{(5)}}$ *and that* $\Delta\overline{S^{(5+n)}} = \Delta\overline{S^{(5)}} = \{65600000, 32800000x, 1640000x^2 + 16400000x, 82000x^3 - 50840000x + 32800000\}$, *for any* $n \in \mathbb{N}$. *Hence*

$$\overline{M^{(5)}} = \mathbf{Z}\langle\overline{S^{(5)}}\rangle = \mathbf{Z}\langle f_0 := 1,\ f_1 := \frac{1}{2}x,\ f_2 := \frac{1}{40}\left(x^2 + 10x\right),\ f_3 := \frac{1}{800}\left(x^3 + 180x + 400\right)\rangle.$$

We will show that each element in $\overline{M^{(5)}}$ satisfies an integral equation.

$$\begin{aligned}
&x^4 - 420x^2 + 40000 = 0\\
&\Rightarrow \left(\frac{x}{2}\right)^4 - \frac{420}{4}\left(\frac{x}{2}\right)^2 + \frac{40000}{2^4} = 0\\
&\Rightarrow \left(\frac{x}{2}\right)^4 - 105\left(\frac{x}{2}\right)^2 + 2500 = 0\\
&\Rightarrow f_1^4 - 105f_1^2 + 2500 = 0
\end{aligned}$$

So f_1 satisfies an integral equation.

We are left with showing that f_2 and f_3 each satisfies an integral equation.

Now consider

$$f_2 := \frac{1}{40}(x^2 + 10x);$$

Want to show that f_2 is integral. That is, it satisfies an integral equation. Note

$$\begin{aligned}
NF(f_2^2, I) &= \frac{1}{80}x^3 + \frac{13}{40}x^2 - 25,\\
NF(f_2^4, I) &= \frac{223}{80}x^3 + \frac{1977}{40}x^2 - 650x - 6225,\\
NF(f_2^8, I) &= \frac{3911841}{80}x^3 + \frac{32605377}{40}x^2 - 13951050x - 117026225,\\
NF(f_2^{16}, I) &= \frac{853153602298047}{80}x^3 + \frac{7062391476250257}{40}x^2 - 3112075095880350x\\
&- 25764545727890225.
\end{aligned}$$

and so

$$\begin{aligned}
f_2^2 &= 10f_3 + 13f_2 - 11f_1 - 30f_0,\\
f_2^4 &= 2230f_3 + 1977f_2 - 2642f_1 - 7340f_0,\\
f_2^8 &= 39118410f_3 + 32605377f_2 - 47857023f_1 - 136585430f_0,\\
f_2^{16} &= 8531536022980470f_3 + 7062391476250257f_2\\
&- 10482462044346690f_1 - 30030313739380460f_0.
\end{aligned}$$

Using row-reduction to eliminate f_3 and f_1, we get an integral equation

$$\begin{gathered}
f_2^{16} + 243949426459594f_2^8 - 6230102427638341369f_2^4 + 435020619858623174686f_2^2\\
-1292425639761414271600f_2 + 641634118444033088000 = 0;
\end{gathered}$$

One can check that setting

$y := f_2^{16} + 243949426459594f_2^8 - 6230102427638341369f_2^4 + 435020619858623174686f_2^2$
$- 1292425639761414271600f_2 + 641634118444033088000;$

we get $\mathrm{NF}(y, I) = 0$. Note that y factors into the following minimum polynomials;

$$< f_2^4 - 21f_2^3 + 134f_2^2 - 275f_2 + 125, 1 >,$$
$$< f_2^{12} + 21f_2^{11} + 307f_2^{10} + 3908f_2^9 + 46580f_2^8$$
$$+ 536308f_2^7 + 6057073f_2^6 + 67654261f_2^5 + 243950177213493f_2^4 + 5122946254468954f_2^3$$
$$+ 74892565445027622f_2^2 + 953355366523668176f_2 + 5133072947552264704, 1 >$$

Hence f_2 satisfies an integral equation.

We want to show that f_3 is integral. That is, it satisfies an integral equation. Note

$$NF(f_3^2, I) = 1/800x^3 + 1/2x^2 + 9/20x - 97/2,$$
$$NF(f_3^4, I) = 503/800x^3 + 57x^2 - 2873/20x - 15393/2,$$
$$NF(f_3^8, I) = 9790521/800x^3 + 508326x^2 - 70459911/20x - 147505153/2,$$

and

$$f_3^2 = f_3 + 20f_2 - 10f_1 - 49f_0,$$
$$f_3^4 = 503f_3 + 2280f_2 - 1510f_1 - 7948f_0,$$
$$f_3^8 = 9790521f_3 + 20333040f_2 - 18095250f_1 - 78647837f_0,$$

Using row-reduction to eliminate f_2 and f_1, we get an integral equation

$$f_3^8 - 21429f_3^4 + 1426254f_3^2 - 437988f_3 - 21783409 = 0;$$

One can check that setting

$$y := f_3^8 - 21429f_3^4 + 1426254f_3^2 - 437988f_3 - 21783409;$$

we get $\mathrm{NF}(y, I) = 0$. Note that y factors into the following minimum polynomials

$$< f_3^4 - 2f_3^3 - 111f_3^2 + 112f_3 + 2111, 1 >,$$
$$< f_3^4 + 2f_3^3 + 115f_3^2 + 340f_3 - 10319, 1 >$$

Hence f_3 satisfies an integral equation.

Theorem 5.1. *Let $\overline{M^{(L)}}$ be defined as above such that $\overline{M^{(L)}} = \overline{M^{(L+n)}}$, for any $n \in \mathbb{N}$. Then every element in $\overline{M^{(L)}}$ is integral.*

Proof: The approach here is to show that each element in $\overline{M^{(L)}}$ satisfies an integral equation. Suppose $\Delta^{-n} f^n \in \overline{M^{(L)}}$ for all n. Then any $\mathbb{Z}$-linear combination is as well because $\overline{M^{(L)}}$ is a $\mathbb{Z}$-module. We can thus produce a $\mathbb{Z}$-dependency satisfied by $\Delta^{-1} f$ and then a $\mathbb{Z}$-integral equation satisfied by $\Delta^{-1} f$. Consider the m-tuples $LC((f_i)^n)$. If $\overline{M^{(i)}} \neq \overline{M^{(l)}}$, then their m-tuples are distinct. By construction, $LC((f_i)^n)|\Delta$, so there are only finitely many such distinct m-tuples to consider.

We observed earlier that $\overline{M^{(L)}}$ has a $\mathbb{Z}$-module basis $\{(\Delta^{-1} f_i) \in S^{(L)} : \ 0 \leq i < m\}$, with degree $(f_i) = i$. Hence given each f_i, we can write

$$(\Delta^{-1} f_i)^j \equiv \Delta^{-j} NF((f_i)^j, I) = \sum_{k=0}^{m-1} z_{i,j,k} (\Delta^{-1} f_k),$$

for some integers $z_{i,j,k}$ and for all j. Let f_i, $0 \leq i < m$ be a fixed basis for $\overline{M^{(L)}}$. Let $f := f_i$ for a particular i, and write

$$\Delta^{-n} NF(f^n, I) = \sum_{k=0}^{m-1} z_{n,k} (\Delta^{-1} f_k)$$

for some integers $z_{n,k}$ for all n. To work with polynomials, define

$$g_n := \Delta^{1-n} NF(f^n, I) = \sum_{k=0}^{m-1} z_{n,k} f_k.$$

Let the *leading position* of g_n be denoted by $LP(g_n)$. Then we can "row-reduce" the sequence of m-tuples whenever

$$LP(g_n) = f_k = LP(g_i), \quad n > i.$$

Start with $n = 1$. If $LM(g_n) = LM(g_i)$ for some $i < n$, then

$$d_{n,i} := gcd(LC(g_n), LC(g_i)) = \alpha_{n,i} LC(g_n) + \beta_{n,i} LC(g_i).$$

Let $d := d_{n,i}$. Replace g_i by

$$\overline{g_i} := \alpha_{n,i} g_n + \beta_{n,i} g_i$$

so that $LP(\overline{g_i}) = f_k$, but $LC(\overline{g_i}) = d$; and also replace g_n by

$$\overline{g_n} := \frac{LC(g_i)}{d} g_n - \frac{LC(g_n)}{d} g_i,$$

so that

$$LP(\overline{g_n}) < LP(g_n) \ \text{ and } \ LM(\overline{g}_n) \prec LM(g_n).$$

As mentioned earlier, there are only finitely many such m-tuples. Hence it must be that for some n,

$$g_n \longrightarrow 0,$$

that is

$$\left(\Delta^{-1} f\right)^n - \sum_{k<n} c_{n,k} g_k \left(\Delta^{-1} f\right)^k \equiv 0.$$

Hence $\left(\Delta^{-1} f_i\right)$ is a root of some polynomial,

$$F_i(T) := 1 \cdot T^n - \sum_{k<n} b_{i,n,k} T^k,$$

which is monic of some possibly large degree n. But $\left(\Delta^{-1} f_i\right)^n$, $0 \leq n \leq m$ cannot be $\mathbb{Z}$-independent. So $\left(\Delta^{-1} f_i\right)$ is a root of some $G_i(T)$ not necessarily monic, and with degree(G_i) $\leq m$. However, $\big(\Delta^{-1}f_i\big)$ is a root of

$$E_i(T) := gcd(F_i(T), G_i(T))$$

with degree(E_i) $\leq$ degree(G_i) $\leq m$ and $LC(E_i)|LC(F_i) = 1$. So $E_i(T)$ must be monic and thus $\big(\Delta^{-1}f_i\big)$ satisfies an integral equation of some degree $n \leq m$. □

Remark 5.1. *We see from the above that we could have defined*

$$S^{(L)} := \{\Delta^{-1}f \in M^{(L-1)} : \Delta^{-n}NF(f^n, I) \in M^{(L-1)} \textit{ for all } 0 \leq n \leq m\}.$$

Theorem 5.2. *Let $\overline{M^{(L)}}$ and $ic(R)$ be defined as above such that $\overline{M^{(L)}} = \overline{M^{(L+n)}}$, for any $n \in \mathbb{N}$. Then $\overline{M^{(L)}} = ic(R)$.*

Proof: From the previous theorem, $M := \overline{M^{(L)}}$ consists of integral elements. That is, every element of M is integral. Thus $M \subseteq ic(R)$. But by construction, $ic(R) \subseteq M$. Hence, $M = ic(R)$. □

Example 5.3. *Let $f(x) := x^6 - 200x^3 + 1500 \in \mathbf{Z}[x]$, and $R := \mathbf{Z}[x]/\langle f(x)\rangle$. Then $\Delta = 765000$, and $\Delta\overline{M^{(0)}} = \{1, x, x^2, x^3, x^4, x^5\}$.*
$\Delta\overline{S^{(1)}} = \{5100, 5100x, 5100x^2, 30x^3 + 2100, 6x^4 + 3060x^2 + 4500x, x^5 + 2x^4 + 10x^3 + 1770x^2 + 1500x + 2400\}$, and $\Delta\overline{M^{(1)}} := \mathbf{Z}\langle\overline{S^{(1)}}\rangle$.
$\Delta\overline{S^{(2)}} = \{153000, 153000x, 15300x^2, 2550x^3 + 10200x^2 + 76500, 510x^4 + 10200x^2 + 76500x, 510x^5 + 5100x^3 + 10200x^2\}$, and $\Delta\overline{M^{(2)}} := \mathbf{Z}\langle\overline{S^{(2)}}\rangle$.
$\Delta\overline{S^{(3)}} = \{765000, 153000x, 153000x^2, 7650x^3 + 382500, 7650x^4 + 76500x, 510x^5 + 2550x^4 + 5100x^3 + 76500x^2 + 76500x\}$, and $\Delta\overline{M^{(3)}} := \mathbf{Z}\langle\overline{S^{(3)}}\rangle$.
$\Delta\overline{S^{(4)}} = \{765000, 765000x, 153000x^2, 38250x^3 + 382500, 7650x^4 + 382500x, 2550x^5 + 5100x^4 + 25500x^3 + 76500x^2\}$, and $\Delta\overline{M^{(4)}} := \mathbf{Z}\langle\overline{S^{(4)}}\rangle$.
$\overline{M^{(n+4)}} = \overline{M^{(4)}} = \mathbb{Z}\langle\overline{S^{(4)}}\rangle$. So $\Delta \cdot ic(R) = \mathbf{Z}\langle\overline{S^{(4)}}\rangle$.

5.2 Computation using Magma's built-in function

In this section we present integral closure computations of number fields using Magma built-in commands. The following Magma code is used.

```
pMaximalOverOrder := function(ord, p)
       ovr := MultiplicatorRing(pRadical(ord, p));
       print "index is", Index(ovr, ord);
       return (Index(ovr, ord) eq 1) select ovr else $$(ovr, p);
end function;
Round2 := function(E, K)
       // E should be some order of a number field K
       d := Discriminant(E);
       fact := Factorization(Abs(d));
       print fact;
       M := E;
       for x in fact do
            M := M+pMaximalOverOrder(E, x[1]);
       end for;
       print "index of equation order in maximal order is:", Index(M, E);
       return M;
end function;
R<x> := PolynomialRing(Integers());
          // select an example below by deletting th // at the
          //beginning of the example
// K := NumberField(x^4-420*x^2+40000); // Example  1
// K := NumberField(x^6 - 200*x^3 + 1500); // Example  2
// K := NumberField(x^5 + 5*x^4 - 75*x^3 + 250*x^2 + 65625);  // Example  3
```

```
 // K := NumberField(x^4 + 5*x^3 - 25*x^2 + 125*x + 625); // Example  4
 K := NumberField(x^4-10*x^2+1); // Example  5
 E := EquationOrder(K);
 Round2(E, K);
```

5.2.1 Examples using Magma

Example 5.4. *(Same as example 5.1 done differently). Let* $f(x) := x^4 - 420x^2 + 40000$ *and* $R := \mathbf{Z}[x]/\langle f(x)\rangle$.

```
>[ <2, 18>, <5, 8>, <41, 2> ]
index is 2
index is 4
index is 8
index is 4
index is 2
index is 1
index is 5
index is 25
index is 1
index is 1
index of equation order in maximal order is: 64000
Transformation of E
Transformation Matrix:
[800   0   0   0]
[  0 400   0   0]
[  0 200  20   0]
[400 180   0   1]
```

```
Denominator: 800
```

So $\Delta := 800$ and $\Delta \cdot ic(R) = \mathbf{Z}\langle 800, 400x, 20x^2 + 200, x^3 + 180x + 400\rangle$.

Example 5.5. *(Same as example 5.3 done differently). Let* $f(x) := x^6 - 200x^3 + 1500$ *and* $R := \mathbf{Z}[x]/\langle f(x)\rangle$.

```
[ <2, 16>, <3, 8>, <5, 15>, <17, 3> ]
index is 2
index is 2
index is 2
index is 2
index is 2
index is 2
index is 1
index is 3
index is 1
index is 5
index is 25
index is 5
index is 25
index is 1
index is 1
index of equation order in maximal order is: 3000000
Transformation of E
Transformation Matrix:
[300   0   0   0   0   0]
[  0 300   0   0   0   0]
[  0   0  60   0   0   0]
[150   0   0  15   0   0]
[  0 150   0   0   3   0]
[  0   0  30  10   2   1]
Denominator: 300
```

So $\Delta := 300$ and $\Delta \cdot ic(R) = \mathbf{Z}\langle 300, 300x, 60x^2, 15x^3+150, 3x^4+150x, x^5+2x^4+10x^3+30x^2\rangle$.

Example 5.6. *Let* $f(x) := x^5 + 5x^4 - 75x^3 + 250x^2 + 65625$ *and* $R := \mathbf{Z}[x]/\langle f(x)\rangle$.

```
[ <2, 2>, <3, 1>, <5, 20>, <7, 1>, <37, 1>, <353263, 1> ]
index is 1
index is 1
index is 5
index is 25
index is 125
index is 625
index is 1
index is 1
index is 1
index is 1
index of equation order in maximal order is: 9765625
Transformation of E
Transformation Matrix:
[625   0   0   0   0]
[  0 125   0   0   0]
[  0   0  25   0   0]
[  0   0   0   5   0]
[  0   0   0   0   1]
```

```
Denominator: 625
```

So $\Delta := 625$ and $\Delta \cdot ic(R) = \mathbf{Z}\langle 625, 125x, 25x^2, 5x^3, x^4\rangle$.

Example 5.7. *Let* $f(x) := x^4 + 5x^3 - 25x^2 + 125x + 625$ *and* $R := \mathbf{Z}[x]/\langle f(x)\rangle$.

```
[ <3, 1>, <5, 12>, <13, 2> ]

index is 1

index is 5

index is 25

index is 125

index is 1

index is 1

index of equation order in maximal order is: 15625

Transformation of E

Transformation Matrix:

[125   0   0   0]

[  0  25   0   0]

[  0   0   5   0]

[  0   0   0   1]

Denominator: 125
```

So $\Delta := 125$ and $\Delta \cdot ic(R) = \mathbf{Z}\langle 125, 25x, 5x^2, x^3\rangle$.

Example 5.8. *Let* $f(x) := x^4 - 10x^2 + 1$ *and* $R := \mathbf{Z}[x]/\langle f(x)\rangle$.

```
[ <2, 14>, <3, 2> ]

index is 2

index is 4

index is 1

index is 1
index of equation order in maximal order is: 8

Transformation of E

Transformation Matrix:

[ 4  0  0  0]

[ 0  4  0  0]

[-2  0  2  0]

[-3 -1 -1  1]

Denominator: 4
```

So $\Delta := 4$ and $\Delta \cdot ic(R) = \mathbf{Z}\langle 4, 4x, 2x^2 - 2, x^3 - x^2 - x - 3\rangle$.

Chapter 6

Various implementations

In this chapter, we look at the output from various implementations in computing integral closures. This enables us to see the uniqueness and advantages of the q^{th}-power algorithm approach. By example, we see that the output from other implementations have issues with some key concepts such as weight functions, monomial orderings, and the type of presentation produced. Throughout this chapter, our example will be the following:

Example 6.1. *Let* $\mathbb{F}$ *be the finite field,* $GF(23)$*. Let* $R := \mathbb{F}[y;x]$*,* $f := (y^8 - y^2x^3 + 2yx^6 - x^9)$ *and* $I :=< f >$*.*

We know from the q^{th}-power algorithm that the weights of the P-module basis generating the integral closure are $[0, 4, 5, 10, 14, 15, 19]$, where $\mathbb{F} := GF(23)$ and $P := \mathbb{F}[x]$. We will present outputs from Singular, Macaulay2, Magma and the q^{th}-power algorithm.

6.1 Output from Singular

Using the ”normal” command:

```
> LIB "normal.lib";
> ring r=23,(y,x),wp(9,8);
> ideal i = (y^8 - y^2*x^3  +  2*y*x^6 -x^9);
> list nor=normal(i);
> nor;
[1]:
   [1]:
      //   characteristic : 23
//   number of vars : 7
//        block   1 : ordering dp
//                  : names    T(1) T(2) T(3) T(4) T(5)
//        block   2 : ordering wp
//                  : names    y x
//                  : weights  9 8
//        block   3 : ordering C
[2]:
   [1]:
      _[1]=y5x2
      _[2]=y6x
      _[3]=y3x5-y4x2
      _[4]=y8
      _[5]=yx8-y2x5
      _[6]=yx6-y2x3
> def R=nor[1][1];
> setring R;
> normap;
normap[1]=y
normap[2]=x
> norid;
norid[1]=T(1)*y-T(2)*x
norid[2]=T(4)*y-T(5)*x+y
norid[3]=-T(5)+x^2
norid[4]=-T(3)*x+y^2
norid[5]=T(2)*y^2-T(4)*x
norid[6]=T(1)*x^3-T(2)*x-T(3)*y^2
```

```
norid[7]=T(3)*x^3-T(5)*y^2

norid[8]=T(2)*x^4-T(2)*y*x-T(3)*y^3

norid[9]=T(3)*y^5-T(4)*x^5+T(5)*x^3-T(5)*y

norid[10]=T(4)*x^8-T(5)*y^7-T(5)*x^6+T(5)*y*x^3

norid[11]=T(1)^2-x

norid[12]=T(1)*T(2)-y

norid[13]=T(2)^2-T(3)

norid[14]=T(1)*T(3)-T(2)*y

norid[15]=T(2)*T(3)-T(4)

norid[16]=T(3)^2-T(1)*x^2+T(2)

norid[17]=T(1)*T(4)-T(3)*y

norid[18]=T(2)*T(4)-T(1)*x^2+T(2)

norid[19]=T(3)*T(4)+T(3)-y*x^2

norid[20]=T(4)^2-T(1)*y^2*x+T(4)

norid[21]=T(1)*T(5)-T(1)*x^2

norid[22]=T(2)*T(5)-T(1)*y*x

norid[23]=T(3)*T(5)-y^2*x

norid[24]=T(4)*T(5)-T(1)*y^3

norid[25]=T(5)^2-x^4

norid[26]=-y^8+x^9-2*y*x^6+y^2*x^3

> option(redSB);

> ideal j=std(norid);j;

j[1]=y^8-x^9+2*y*x^6-y^2*x^3

j[2]=T(5)-x^2

j[3]=T(4)*y-x^3+y

j[4]=T(4)*x^6-y^7-x^6+y*x^3

j[5]=T(3)*x-y^2
```

```
j[6]=T(3)*y^5-T(4)*x^5+x^5-y*x^2
j[7]=T(2)*y^2-T(4)*x
j[8]=T(2)*x^4-T(2)*y*x-T(3)*y^3
j[9]=T(1)*y-T(2)*x
j[10]=T(1)*x^3-T(2)*x-T(3)*y^2
j[11]=T(4)^2-T(2)*y*x^2+T(4)
j[12]=T(3)*T(4)+T(3)-y*x^2
j[13]=T(2)*T(4)-T(1)*x^2+T(2)
j[14]=T(1)*T(4)-T(3)*y
j[15]=T(3)^2-T(1)*x^2+T(2)
j[16]=T(2)*T(3)-T(4)
j[17]=T(1)*T(3)-T(2)*y
j[18]=T(2)^2-T(3)
j[19]=T(1)*T(2)-y
j[20]=T(1)^2-x
```

The *normal* command produces an R-module generating set, $\{T(1), T(2), T(3), T(4), T(5)\}$. We see that $nor[1][1]$ gives a *block order, grevlex* on the new variables $\{T(1), T(2), T(3), T(4), T(5)\}$ and the given *order* on the old variables, $\{y, x\}$. The R-module generators are given by

$T(1) := (y^5x^2)/\Delta, \;\; wt(T(1)) = 4$

$T(2) := (y^6x)/\Delta, \;\; wt(T(2)) = 5$

$T(3) := (y^3x^5 - y^4x^2)/\Delta, \;\; wt(T(3)) = 10$

$T(4) := (y^8)/\Delta, \;\; wt(T(4)) = 15$

$T(5) := (yx^8 - y^2x^5)/\Delta, \;\; wt(T(5)) = 16$

where $\Delta := yx^6 - y^2x^3$ is the conductor element used.

Looking at the ideal j above, we see that $j[2] = T(5) - x^2$. That is $T(5) = x^2$ and $T(5)$ does not show up elsewhere in j. So $T(5)$ is an *extra* variable. Also, we notice that the weights 14 and 19 corresponding to $T(2)y$ and $T(3)y$ respectively, are missing. These variables do not show up in the presentation because Singular is producing an R-module presentation, instead of producing a P-module presentation. The relations, *norid*, in the algebra presentation here are linear and quadratic over the input ring.

Using the "normalP" with the "withRing" option command:

```
> LIB "normal.lib";
> ring r=23,(y,x),wp(9,8);
> ideal i =(y^8-y^2*x^3+2*y*x^6-x^9);
> list norp=normalP(i,"withRing");
> norp;
[1]:
   [1]:
      //   characteristic : 23
//   number of vars : 2
//        block   1 : ordering dp
//                  : names    T(1) T(3)
//        block   2 : ordering C
[2]:
   [1]:
      _[1]=y5x
      _[2]=y6
      _[3]=y3x4-y4x
      _[4]=x8-y2x2
      _[5]=yx5-y2x2
[3]:
   [1]:
      22
   [2]:
```

```
   22
> def R=norp[1][1];
> setring R;
> normap;
normap[1]=T(1)^6-T(1)*T(3)^2
normap[2]=T(1)^2
> norid;
norid[1]=T(1)^17-3*T(1)^12*T(3)^2+3*T(1)^7*T(3)^4-T(1)^7*T(3)
-T(1)^2*T(3)^6+T(1)^2*T(3)^3
norid[2]=T(1)^11*T(3)-2*T(1)^6*T(3)^3+T(1)*T(3)^5-T(1)*T(3)^2
norid[3]=T(1)^10-2*T(1)^5*T(3)^2+T(3)^4-T(3)
norid[4]=T(1)^10*T(3)-2*T(1)^5*T(3)^3+T(3)^5-T(3)^2
norid[5]=T(1)^15-3*T(1)^10*T(3)^2+3*T(1)^5*T(3)^4-T(1)^5*T(3)
-T(3)^6+T(3)^3
norid[6]=T(1)^12-2*T(1)^7*T(3)^2+T(1)^2*T(3)^4-T(1)^2*T(3)
norid[7]=T(1)^12*T(3)-2*T(1)^7*T(3)^3+T(1)^2*T(3)^5-T(1)^2*T(3)^2
norid[8]=T(1)^11-2*T(1)^6*T(3)^2+T(1)*T(3)^4-T(1)*T(3)
norid[9]=T(1)^48-8*T(1)^43*T(3)^2+5*T(1)^38*T(3)^4-10*T(1)^33*T(3)^6
+T(1)^28*T(3)^8
-10*T(1)^23*T(3)^10+5*T(1)^18*T(3)^12-8*T(1)^13*T(3)^14
+T(1)^8*T(3)^16-T(1)^8*T(3)^4
> option(redSB);
> ideal j=std(norid);j;
j[1]=T(1)^10-2*T(1)^5*T(3)^2+T(3)^4-T(3)
```

normalP with the "withRing" command does not produce an R-module generating set. The fractions produced are

$T(1) := (y^5x)/\Delta, \quad wt(T(1)) = 4$

$T(2) = (y^6)/\Delta, \;\; wt(T(2)) = 5$

$T(3) := (y^3x^4 - y^4x)/\Delta, \;\; wt(T(3)) = 10$

$T(4) = (x^8 - y^2x^2)/\Delta, \;\; wt(T(4)) = 15$

where $\Delta := yx^5 - y^2x^2$ is the conductor element used.

We see that $nor[1][1]$ gives a *block order, grevlex* on the new variables $\{T1, T3\}$. The old variables y and x are replaced with $(T(1))^6 - T(1)T(3)$ and $(T(1))^2$ respectively.

We know the weights that are produced by the q^{th}-power algorithm. Here we have just $wt(T(1)) := 4$ and $wt(T(3)) := 10$. This is probably because SINGULAR is getting rid of the variables $T(2), T(4), y$ and x. It thinks these variables are unnecessary. There are no y's and x's and the relations do not indicate that R is a subring.

A Gröbner basis of the presentation reduces to a relation which is no longer a presentation over R at all. In fact, the relation is in terms of $T(1)$ and $T(3)$, which is neither linear nor quadratic over R.

Using the "normalP" with "withRing" and "noRed" command:

```
> LIB "normal.lib";
> ring r=23,(y,x),wp(9,8);
> ideal i = (y^8 - y^2*x^3  +  2*y*x^6 -x^9);
> list norp=normalP(i,"withRing","noRed");
> norp;
[1]:
   [1]:
      //   characteristic : 23
//   number of vars : 6
//        block   1 : ordering dp
//                  : names    T(1) T(2) T(3) T(4)
//        block   2 : ordering wp
//                  : names    y x
//                  : weights  9 8
//        block   3 : ordering C
[2]:
   [1]:
      _[1]=y5x
      _[2]=y6
      _[3]=y3x4-y4x
      _[4]=x8-y2x2
      _[5]=yx5-y2x2
[3]:
   [1]:
      22
   [2]:
      22
> def R=norp[1][1];
> setring R;
> normap;
normap[1]=y
normap[2]=x
> norid;
norid[1]=T(1)*y-T(2)*x
norid[2]=-T(3)*x+y^2
norid[3]=T(2)*y^2-T(4)*x+2*x
norid[4]=-T(4)*y+x^3+y
norid[5]=T(1)*x^3-T(2)*x-T(3)*y^2
norid[6]=T(1)^2-x
norid[7]=T(1)*T(2)-y
```

```
norid[8]=T(2)^2-T(3)
norid[9]=T(1)*T(3)-T(2)*y
norid[10]=T(2)*T(3)-T(4)+2
norid[11]=T(3)^2-T(1)*x^2+T(2)
norid[12]=T(1)*T(4)-2*T(1)-T(3)*y
norid[13]=T(2)*T(4)-T(1)*x^2-T(2)
norid[14]=T(3)*T(4)-T(3)-y*x^2
norid[15]=T(4)^2-T(2)*y*x^2-3*T(4)+2
norid[16]=y^8-x^9+2*y*x^6-y^2*x^3
> option(redSB);
> ideal j=std(norid);j;
j[1]=y^8-x^9+2*y*x^6-y^2*x^3
j[2]=T(4)*y-x^3-y
j[3]=T(4)*x^6-y^7-3*x^6+y*x^3
j[4]=T(3)*x-y^2
j[5]=T(3)*y^5-T(4)*x^5+3*x^5-y*x^2
j[6]=T(2)*y^2-T(4)*x+2*x
j[7]=T(2)*x^4-T(2)*y*x-T(3)*y^3
j[8]=T(1)*y-T(2)*x
j[9]=T(1)*x^3-T(2)*x-T(3)*y^2
j[10]=T(4)^2-T(2)*y*x^2-3*T(4)+2
j[11]=T(3)*T(4)-T(3)-y*x^2
j[12]=T(2)*T(4)-T(1)*x^2-T(2)
j[13]=T(1)*T(4)-2*T(1)-T(3)*y
j[14]=T(3)^2-T(1)*x^2+T(2)
j[15]=T(2)*T(3)-T(4)+2
j[16]=T(1)*T(3)-T(2)*y
```

```
j[17]=T(2)^2-T(3)

j[18]=T(1)*T(2)-y

j[19]=T(1)^2-x
```

normalP with "withRing" and "noRed" command produces an R-module generating set, $\{T(1), T(2), T(3), T(4)\}$, with fewer variables. We see that $nor[1][1]$ gives a *block order, grevlex* on the new variables $\{T(1), T(2), T(3), T(4)\}$ and the given *order* on the old variables, $\{y, x\}$. The R-module generators are given by

$T(1) := (y^5x)/\Delta, \quad wt(T(1)) = 4$

$T(2) := (y^6)/\Delta, \quad wt(T(2)) = 5$

$T(3) := (y^3x^4 - y^4x)/\Delta, \quad wt(T(3)) = 10$

$T(4) := (x^8 - y^2x^2)/\Delta, \quad wt(T(4)) = 15$

where $\Delta := yx^5 - y^2x^2$ is the conductor element used.

We notice that the weights 14 and 19 corresponding to $T(2)y$ and $T(3)y$ respectively, are missing. These variables do not show up in the presentation because SINGULAR is producing an R-module presentation, instead of producing a P-module presentation. The relations, *norid*, in the algebra presentation here are linear and quadratic over the input ring, R.

Looking at the outputs from SINGULAR, the outputs gotten by using *normalP(i,"withRing","noRed")* and *normal* commands are radically different from the output gotten by using the *normalP(i,"withRing")* command, which produces a presentation over $\mathbb{F}_{23}[T(3)]$, instead of a presentation over $\mathbb{F}_{23}[T(2)]$. Indeed, a presentation using T(2) instead of T(3) would have probably matched the output of MAGMA's Normalisation.

The presentation from *normalP(i,"withRing")* command, has a Gröbner basis having only one relation $j[1] = (T(1))^{10} - 2(T(1))^5(T(3))^2 + 9(T(3))^4 - T(3)$. This presentation is not quite *type I* because $gcd(wt(T(1)), wt(T(3))) \neq 1$.

It is important to note that the theory in the SINGULAR book (see [15]) is that the presentation is to be a strict affine R-algebra. But the presentation from *normalP(i,"withRing")* is contrary to this theory. In fact *normalP(i,"withRing")* tries to get a minimized presentation, suggesting that such an affine R- algebra presentation may not be the best. The attempt by *normalP(i,"withRing")* to get a minimized presentation is unsuccessful as $T(2)$ is removed instead of $T(3)$. *normalP(i,"withRing","noRed")* and *normal* produce an affine R-algebra presentation, which matches the theory in the book.

In order the salvage the output from SINGULAR, it is vital to process the input so as to identify the free and independent variables in the input ring. We think that the presentation over the input ring, R, is not a good approach. The presentation should be over the ring of free variables, P, as in the case of the q^{th}-power algorithm. In fact using the q^{th}-power algorithm, we produce a strictly P-affine algebra presentation, with only linear and quadratic relations over the ring of free variable, P. It is also important to note the input ring is no longer important in the output, since the integral closure always contain the input ring. Unfortunately, SINGULAR thinks that the input ring is more important in the output.

6.2 Output from MACAULAY2

The *integralClosure* and *icFracP* commands in MACAULAY2 give

```
i1 :  load "IntegralClosure.m2";

i2 : R=ZZ/23[y,x,MonomialOrder=>{Weights=>{9,8}}];

i3 :  I=ideal(y^8 - y^2*x^3  +  2*y*x^6 -x^9);

o3 : Ideal of R

i4 : S=R/I;

i5 : time P=presentation(integralClosure(S))

     -- used 2.12 seconds

o5 = | w_(10,0)^3y-x3+y w_(12,0)x2-w_(10,0)^4-w_(10,0)

     ---------------------------------------------------------------

     w_(12,0)w_(10,0)x-yx w_(12,0)y-w_(10,0)x w_(12,0)w_(10,0)-y

     ---------------------------------------------------------------
     w_(12,0)^2x-x2 w_(12,0)^2-x |

             ZZ                      1       ZZ                      7
o5 : Matrix (--[w    , w    , y, x])  <--- (--[w    , w    , y, x])
             23  12,0   10,0                 23  12,0   10,0

i6 : time G=gens gb P
     -- used 0. seconds

o6 = | x9-y8-2yx6+y2x3 w_(10,0)y3-x4+yx w_(10,0)x5-w_(10,0)yx2-y5
     ---------------------------------------------------------------
     w_(10,0)^2x-y2 w_(10,0)^3y-x3+y w_(10,0)^5+w_(10,0)^2-yx2
     ---------------------------------------------------------------
     w_(12,0)y-w_(10,0)x w_(12,0)x2-w_(10,0)^4-w_(10,0)
     ---------------------------------------------------------------
     w_(12,0)w_(10,0)-y w_(12,0)^2-x |

             ZZ                      1       ZZ                      10
o6 : Matrix (--[w    , w    , y, x])  <--- (--[w    , w    , y, x])
             23  12,0   10,0                 23  12,0   10,0

i7 : time F=icFracP(S)
     -- used 432.23 seconds

          5      2   4         2   3
         x  - y*x   x  - y*x  y   x  - 6y
o7 = {1, ---------, --------, --, -------}
              4         3      x     y
             y         y
```

Macaulay2's *integralClosure* command produces an R-module generating set, $\{w\_(10,0), w\_(12,0)\}$, with $w\_(10,0) := \frac{x^4-yx}{y^3}$, having weight $wt(w\_(10,0)) = 5$ and $w\_(12,0) := \frac{w\_(10,0)x}{y} = \frac{x^5-yx^2}{y^4}$, having weight $wt(w\_(12,0)) = 4$. Though *integralClosure* produces a presentation that is not quadratic-and-linear over R, *icFracP* does not produce a presentation at all, but only fractions. Though *icFracP* does not produce weights, we see that the weights of the fractions produced are $[0, 4, 5, 10, 15]$.

Again the output here from Macaulay2, using either the *integralClosure* or the *icFracP* command, produces fewer variables. The weights 14 and 19 corresponding to $y((x^4 - yx)/y^3)$ and $y((y^2)/x))$ respectively, are missing. These variables do not show up in the presentation because Macaulay2 is producing an R-module presentation over the input ring,R, instead of producing a P-module presentation.

6.3 Output from Magma

The *IntegralClosure* command in Magma gives a module presentation over the function field $\mathbb{Q}(x)$.

```
Q:=GF(23);
F<x>:=FunctionField(Q);
P<y>:=PolynomialRing(F);
f:=(y^8 - y^2*x^3  +  2*y*x^6 -x^9);
Ff<Y>:=RationalExtensionRepresentation(FunctionField(f));
C<X>:=CoefficientRing(Ff);
INT:=Integers(C);
IC:=IntegralClosure(INT,Ff);
B:=Basis(IC);
for i in [1..#B] do
i,B[i];
end for;
"time for char=0 is",Cputime(t23);
==================================
 [ 1    1
   2    Y
```

```
    3    1/X*Y^2
    4    1/X*Y^3
    5    1/X^2*Y^4
    6    1/X^2*Y^5
    7    1/X^3*Y^6
    8    1/X^13*Y^7 + 1/X^10*Y^6 + 1/X^7*Y^5 + 1/X^4*Y^4 + 18/X^10*Y + 1/X^7  ]
```

which is an $\mathbb{F}_{23}[x]$-module basis. Though MAGMA does not produce weights, we see that the weights of the fractions are $[0, 9, 10, 19, 20, 29, 30, 4]$.

MAGMA's *IntegralClosure* treats the output as a subring of $\mathbb{F}_{23}(X)[Y]$, allowing for operations to be performed on elements there, which means producing other elements of $\mathbb{F}_{23}(X)[Y]$ not necessarily immediately recognizable in terms of the basis elements produced.

The *Normalisation* command in MAGMA gives

```
t:=Cputime();
F:=Rationals();
P<y,x>:=PolynomialRing(F,2,"weight",[1,0,9,8]);
f:=(y^8 - y^2*x^3  +  2*y*x^6 -x^9);
I:=ideal<P|f>;
N:=Normalisation(I);
J:=N[1][1];J;
"Normalisation time=",Cputime(t);
G:=GroebnerBasis(J);G;
"total time=",Cputime(t);
======
Ideal of Polynomial ring of rank 2 over Rational Field
Order: Lexicographical
Variables: $.1, $.2
Basis:
```

```
[
    -$.1^21 + $.1^16*$.2^4 + $.1^11*$.2^5 + $.1^6*$.2^6 + $.1^6
    +  $.1*$.2^7 - $.1*$.2,
    -$.1^7 + $.1^2*$.2^4 + $.1^2*$.2,
    -$.1^10 + 2*$.1^5*$.2 + $.2^8 - $.2^2,
    -$.1^11 + $.1^6*$.2^4 + $.1*$.2^5 + $.1*$.2^2,
    -$.1^12 + 2*$.1^7*$.2 + $.1^2*$.2^8 - $.1^2*$.2^2,
    -$.1^11*$.2 + 2*$.1^6*$.2^2 + $.1*$.2^9 - $.1*$.2^3,
    -$.1^17 + $.1^12*$.2^4 + $.1^7*$.2^5 + $.1^2*$.2^6 +
        $.1^2*$.2^3,
    -$.1^10*$.2^2 + 2*$.1^5*$.2^3 + $.2^10 - $.2^4,
    -$.1^6 + $.1*$.2^4 + $.1*$.2,
    -$.1^12*$.2^2 + 2*$.1^7*$.2^3 + $.1^2*$.2^10 - $.1^2*$.2^4,
    -$.1^11*$.2^3 + 2*$.1^6*$.2^4 + $.1*$.2^11 - $.1*$.2^5,
    -$.1^7*$.2 + $.1^2*$.2^5 + $.1^2*$.2^2,
    -$.1^10*$.2^4 + 2*$.1^5*$.2^5 + $.2^12 - $.2^6,
    -$.1^6*$.2^2 + $.1*$.2^6 + $.1*$.2^3,
    -$.1^5 + $.2^4 + $.2 ]
> "Normalisation time=",Cputime(t);
Normalisation time= 0.770
> G:=GroebnerBasis(J);G;
[     $.1^5 - $.2^4 - $.2   ]
> "total time=",Cputime(t);
```

A Gröbner basis of Magma's *Normalisation* produces a single relation $(J.1)^5 - (J.2)^4 - J.2$, which is what which is what *normalP* with the ”withRing” command should have produced.

6.4 Output from the q^{th}-power algorithm

The q^{th}-power algorithm gives a $\mathbb{F}_{23}[x]$-module presentation with the following $\mathbb{F}_{23}[x]$-module basis, and $\Delta := x^{13}$.

1 y^3x^{12},

2 $y^7x^7 - yx^{10}$,

3 $y^6x^8 + y^7x^5 + x^{11} - yx^8$,

4 y^2x^{12},

5 yx^{13},

6 $y^5x^8 + y^6x^5 + y^7x^2 + x^8 - yx^5$,

7 $y^4x^9 + y^5x^6 + y^6x^3 + y^7 + x^6 - yx^3$,

8 x^{13}

with weights $[19, 15, 14, 10, 9, 5, 4, 0]$

and the following strictly $\mathbb{F}_{23}[x]$-affine algebra presentation

$[\ f_4^2 - f_8$,

$f_5^2 - f_{10}$,

$f_5f_4 - f_9$,

$f_9^2 - f_{10}f_8$,

$f_9f_5 - f_{14}$,

$f_9f_4 - f_5f_8$,

$f_{10}^2 - f_4f_8^2 + f_5$,

$f_{10}f_9 - f_{19}$,

$f_{10}f_5 - f_{15} - 1$,

$f_{10}f_4 - f_{14}$,

$f_{14}^2 - f_4f_8^3 + f_5f_8$,

$f_{14}f_{10} - f_8^3 + f_9$,

$f_{14}f_9 - f_{15}f_8 - f_8$,

$f_{14}f_5 - f_{19}$,

$f_{14}f_4 - f_{10}f_8,$

$f_{15}^2 - f_{14}f_8^2 + 3f_{15} + 2,$

$f_{15}f_{14} - f_5f_8^3 + 2f_{14},$

$f_{15}f_{10} - f_9f_8^2 + 2f_{10},$

$f_{15}f_9 - f_8^3 + 2f_9,$

$f_{15}f_5 - f_4f_8^2 + 2f_5,$

$f_{15}f_4 - f_{19} + f_4,$

$f_{19}^2 - f_{14}f_8^3 + f_{15}f_8 + f_8,$

$f_{19}f_{15} - f_{10}f_8^3 + 2f_{19},$

$f_{19}f_{14} - f_9f_8^3 + f_{10}f_8,$

$f_{19}f_{10} - f_5f_8^3 + f_{14},$

$f_{19}f_9 - f_4f_8^3 + f_5f_8,$

$f_{19}f_5 - f_8^3 + f_9,$

$f_{19}f_4 - f_{15}f_8 - f_8$]

where $f_4 := (1/x^{13})y^4x^9, f_5 := (1/x^{13})y^5x^8, f_9 := y, f_{10} := (1/x^{13})y^2x^{12}, f_{14} := (1/x^{13})y^6x^8,$ $f_{15} := (1/x^{13})y^7x^7, f_{19} := (1/x^{13})y^3x^{12}, f_8 := x.$

It is important to note here that if we look at the weights, $[19, 15, 14, 10, 9, 5, 4, 0]$, it is possible to extract a minimized answer using f_4, f_5, f_{10}, and f_{15}, a weighted $\mathbb{F}_{23}[f_4]$-module version of what *Normalisation* produced, what *normalP(i,"withRing")* and *icFracP* should have produced.

Chapter 7
Speed-up techniques

In this chapter, we present some approaches in doing computations that are very time efficient. It is not standard for computer algebra systems to have code to compute $NF(f^q, I)$ efficiently. So while computing f^q in characteristic q may be easy, reducing it mod I may be very dense and costly in terms of time and/or storage.

Therefore it is wise to write code for repeatedly squaring and reducing mod I, a well-known strategy for dealing with exponentiating and reducing large objects in general. The following code and examples show the computational necessity of this approach. The first technique speeds up some necessary normal form computations in some existing computational algebra packages.

7.1 Normal Form, $NF(f^q, I)$

Let f be an element in a polynomial ring P. Let I be an ideal in P, and q be a prime. We want to compute the normal form of f^q modulo the ideal I . That is, we want to compute $NF(f^q, I)$, using the built-in Magma command.

(a) Less efficient approach: An inefficient approach to compute $NF(f^q, I)$ is to mindlessly raise f to the q and then take its normal form modulo I. The approach is very slow and very inefficient, since we may be taking the normal form of a polynomial of very large degree.

(b) Efficient approach and why it works: We note that the normal form operation is very dense and takes much time for polynomials of very large degree. A more efficient approach considered here is to start with the normal form of f modulo the ideal I and then repeatedly square and reduce the resulting normal form modulo the ideal I. This means we are only taking the normal form of a polynomial of very small degree every time.

Below are two pieces of code that implement the above approaches.

Code for approach (a).

```
METHOD ONE

////////////  normal form function ///////////////

slow_normal_form:=function(q,f,I)

   nf_time:=Cputime();

   b:= NormalForm(f^q,I);

   bb:= Cputime(nf_time);

   return    q,b,f,I, bb;  /////////////

end function;

/////////////////////////////////////////////////////
```

Code for approach (b).

```
METHOD TWO

//////////////////////////////////////////////

fast_normal_form:=function(q,f,I)

nfg_time:=Cputime();

 if g eq 0 then

   return 0;

 else

     t:=q;

     prd:=1;

     temp:=NormalForm(f,I);

     repeat

        rem:=t mod 2;

        t div:=2;
        if rem eq 1 then
           prd *:=temp;
        end if;
        if t ne 0 then
           temp:=NormalForm(temp^2,I);
        end if;
     until t eq 0;
    a:= NormalForm(prd,I);
     aa:=Cputime(nfg_time);
 return  q, a, f, I,  aa;
  end if;
end function;
//////////////////////////////////////////////////
```

Here are timings for the two different approaches over a polynomial ring $\mathbb{F}_q[y, x]$, $y \succeq_{grevlex} x$, and a polynomial $f = y^5$, for various primes q, and ideals I_q generated by the polynomial $g_q(y, x) = q_1y^6 + q_2x^{11} + q_3y^3x^4 + q_4y^5 + q_5y^4x + q_6y^2x^4 + q_7y^4 + q_8yx^5 + q_9y^3x + q_{10}y^2x^2 + q_{11}y^3 + q_{12}y^2x + q_{13}yx^2 + q_{14}x^3$ with each $q_i \in \mathbb{F}_q$. The timings clearly indicate that approach (b) is more efficient.

Table 7.1: Timing normal forms

prime, q	Method#2	Method#1
5	0.000	0.000
7	0.000	0.000
11	0.000	0.010
13	0.010	0.020
17	0.020	0.040
19	0.030	0.060
23	0.080	0.110
29	0.130	0.260
31	0.210	0.330
37	0.140	0.560
41	0.180	0.780
43	0.280	0.920
47	0.450	1.210
53	0.430	1.790
59	0.770	2.540
61	0.840	2.840
73	0.540	5.040
79	1.180	6.490
83	1.010	7.560
89	1.210	9.460
97	0.900	12.350
101	1.500	13.850
113	1.930	19.340
193	3.600	102.280
257	5.140	245.670
307	17.800	395.830
353	17.680	600.370
541	53.160	2194.400
547	39.020	2275.170

7.2 Extended Euclidean algorithm

Below is our extended Euclidean division algorithm code.

```
////////////////////  EXTENDED DIVISION   FUNCTION      ///////

///////////////////////////////////////////////////////////////

EEDXGCD:= function(F,n,P,f,g,i)
```

```
FF:=FunctionField(F,n);
hP:=hom<P->FF|[FF.j:j in [1..n]]>;
R:=PolynomialRing(FF);
ff:=&+[Coefficient(f,P.i,j)@hP*R.1^j: j in [0..Degree(f,P.i)]];
gg:=&+[Coefficient(g,P.i,j)@hP*R.1^j: j in [0..Degree(g,P.i)]];
dd1,aa1,bb1:=XGCD(ff,gg);
C:=Lcm([Denominator(x) : x in Eltseq(aa1) cat Eltseq(bb1)]);
D:=dd1*C;A:=aa1*C;B:=bb1*C;
hR:=hom<R->P|hom<FF->P|[P.j: j in [1..n]]>, P.i>;
return D@hR,A@hR,B@hR;
end function;
////////////////////////////////////////////////////////////////////////
```

Some of the algebraic packages do not have a direct implementation of the extended Euclidean algorithm. And those that do have one, rely on resultant computations, which often turn out to be computationally wasteful. Also, those packages that do have the extended Euclidean algorithm are generally written for a univariate polynomial. The above extended Euclidean algorithm improves the mentioned deficiencies. It is a fast approach in doing elimination of polynomial variables, similar to the Magma built-in resultant command. It is also used for computing a special polynomial called conductor element, denoted Δ, with Δ in the polynomial ring P of free variables. We will compute some timings below to show how efficient this extended Euclidean algorithm function is in eliminating or inverting and in computing Δ. We note that, the Δ computed using the extended Euclidean function may have higher degree than the one computed using the Magma built-in commands.

7.2.1 Inverting and eliminating

The extended Euclidean function takes as input a function field F, the number n, of variables in a polynomial ring P, two polynomials f and g in P and the i^{th} variable in P to be eliminated from g, relative to f. It is very useful in inverting polynomial ring elements. We will show a small example by hand and by using the above code. Consider the the curve $f(y) = y^3 + yx + x^5 \ \in \mathbb{F}_2[y,x]$. Then $f'(y) = y^2 + x$. We want to write $\dfrac{1}{f'(y)} = \dfrac{g(y)}{D(x)}$, for some $g(y), D(x) \in \mathbb{F}_2[y,x]$.

$$\frac{1}{f'(y)} = \frac{1}{y^2 + x} = \frac{y}{y^3 + yx} = \frac{y}{x^5}.$$

We have thus inverted y in the denominator of $\dfrac{1}{y^2 + x}$. Using the extended Euclidean function, EEDXGCD, above we get

$q := 2;$

$n := 2;$

$P < y, x > := PolynomialRing(GF(q), 2);$

$f := y^3 + xy + x^5;$

$h := y^2 + x;$

$D, b, g := EEDXGCD(GF(q), n, P, f, h, 1);$

$D, b, g = x^5, 1, y$

which is exactly what we got earlier.

Standard techniques for eliminating variables often rely on computing resultants. Consider the above example

$f := y^3 + yx + x^5 \in \mathbb{F}_2[y,x], \quad h := y^2 + x \in \mathbb{F}_2[y,x]$. Then standard techniques will invert y in $h := y^2 + x \in \mathbb{F}_2[y,x]$ to produce

$$\begin{vmatrix} 0 & 0 & 0 & x^5 & \\ & 0 & 0 & 0 & x^5 \\ 1 & 0 & x & & \\ & 1 & 0 & x & \\ & & 1 & 0 & x \end{vmatrix} = x^{10}.$$

This is done by computing the resultant of f and h with respect to the variable y, denoted $Res(f, h, y)$. However, this is generally computationally wasteful, when a straightforward extended Euclidean algorithm above gives a much better answer.

$$(y^3 + yx + x^5) \cdot 1 + (y^2 + x) \cdot y = x^5$$

As mentioned earlier, the extended Euclidean function, EEDXCGD, can be used to eliminate variables. Let us consider the tower example

$$x_{i+1}^q + x_{i+1} = \frac{x_i^q}{x_i^{q-1} + 1}, \qquad 1 \leq i \leq n. \tag{7.1}$$

by Stichtenoch *et al* [16]. Then for $q = 2$ and $n = 3$ we get the equations

$$\begin{aligned} x_1(x_1+1)(x_2+1) + x_2^2 &= 0 \\ x_2(x_2+1)(x_4+1) + x_4^2 &= 0 \\ x_4(x_4+1)(x_8+1) + x_8^2 &= 0 \end{aligned} \tag{7.2}$$

Now define

$$\begin{aligned} x_{12} &:= x_4(x_8+1), \\ x_{14} &:= x_2(x_4+1)(x_8+1) \\ \text{and } \ x_{15} &:= x_1(x_2+1)(x_4+1)(x_8+1) \end{aligned} \tag{7.3}$$

Using the extended Euclidean function, EEDXGCD, and (7.2) to eliminate the variables x_1, x_2 and x_4 from the equation (7.3) we get

$$\begin{gathered} x_{12}^2 + x_{12}x_8 + x_{12} + x_8^2 + x_8^3 = 0 \\ x_{14}^2 + x_{14}x_{12} + x_{14}x_8 + x_{14} + x_{12}x_8^2 = 0 \\ x_{15}^2 + x_{15}x_{14} + x_{15}x_{12} + x_{15}x_8 + x_{15} + x_{14}x_{12} + x_{14}x_8^2 = 0 \end{gathered} \tag{7.4}$$

which does not have x_1, x_2 and x_4

MAGMA has built-in commands that do elimination of variables. However, these built-in commands are very inefficient. Below are some timings of the above example 7.1, for various q and n, using both the extended Euclidean function, EEDXGCD, and MAGMA built-in commands.

Table 7.2: Timing elimination via MAGMA commands versus EEDXGCD command

values of q and n	*Timing elimination via* MAGMA *commands /sec*	*Timing elimination via EEDXGCD /sec*
$q = 2, n = 2$	0.000	0.130
$q = 2, n = 3$	0.010	0.150
$q = 2, n = 4$	0.040	0.140
$q = 2, n = 5$	0.200	0.150
$q = 2, n = 6$	1.890	0.180
$q = 2, n = 7$	26.730	0.300
$q = 2, n = 8$	979.230	1.560
$q = 2, n = 9$	$---$	11.770
$q = 3, n = 2$	0.020	0.150
$q = 3, n = 3$	0.080	0.150
$q = 3, n = 4$	7.630	0.170
$q = 3, n = 5$	40631.220	0.310

7.2.2 $n \times n$ minors of the jacobian and conductor element computations

A typical approach to compute a suitable Δ from the polynomial ring of free variables will be to compute all $n \times n$ minors of the a Jacobian matrix and then compute a Gröbner basis. This approach is good for very small prime numbers and it also produces a Δ of smaller degree that works faster with the q^{th}-power algorithm. However, this approach is best for very small primes. Our approach computes Δ by taking products of the nonzero leading diagonal entries of the Jacobian matrix. Our example here will be the tower above in equation 7.1, by Stichtenoch *et al* [16]. (Details of this tower are found in [16]).

Magma commands: Using Magma built-in commands to do the elimination and to compute Δ, we get the following timings.

Table 7.3: Timing Magma commands for elimination and Δ computation

values of q and n	*Timing elimination /sec*	*Timing* Δ */sec*	*Timing* q^{th} *power*	*Computed* Δ
$q = 2, n = 2$	0.000	0.030	0.030	x_4^2
$q = 2, n = 3$	0.010	0.000	0.030	x_8^4
$q = 2, n = 4$	0.040	0.020	0.070	x_{16}^8
$q = 2, n = 5$	0.200	0.150	0.340	x_{32}^{16}
$q = 2, n = 6$	1.890	1.030	2.040	x_{64}^{32}
$q = 2, n = 7$	26.730	8.320	13.800	x_{128}^{64}
$q = 2, n = 8$	979.230	84.370	86.870	x_{256}^{128}
$q = 3, n = 2$	0.020	0.000	0.090	$x_9^8 + x_9^6$
$q = 3, n = 3$	0.080	0.100	36.310	$x_{27}^{20} + x_{27}^{18}$
$q = 3, n = 4$	7.630	8.160	131.880	$x_{81}^{56} + x_{81}^{54}$
$q = 3, n = 5$	40631.220	2530.180	7141.200	$x_{243}^{164} + x_{243}^{162}$

EEGCD function and Magma commands: Using our extended Euclidean division greatest common divisor function (EEGCD) to do the elimination and using Magma built-in commands to compute Δ, we get the following timings.

Table 7.4: Timing EEGCD to do elimination andMagma commands for Δ computation

values of q and n	*Timing elimination /sec*	*Timing* Δ */sec*	*Timing* q^{th} *power*	*Computed* Δ
$q = 2, n = 2$	0.130	0.010	0.010	x_4^2
$q = 2, n = 3$	0.150	0.000	0.030	x_8^4
$q = 2, n = 4$	0.140	0.020	0.060	x_{16}^8
$q = 2, n = 5$	0.150	0.150	0.350	x_{32}^{16}
$q = 2, n = 6$	0.180	1.060	2.040	x_{64}^{32}
$q = 2, n = 7$	0.300	8.380	12.800	x_{128}^{64}
$q = 2, n = 8$	1.560	80.210	85.470	x_{256}^{128}
$q = 2, n = 9$	11.770	5573.280	640.620	x_{512}^{265}
$q = 3, n = 2$	0.150	0.000	0.090	$x_9^8 + x_9^6$
$q = 3, n = 3$	0.150	0.100	101.640	$x_{27}^{20} + x_{27}^{18}$
$q = 3, n = 4$	0.170	8.510	133.740	$x_{81}^{56} + x_{81}^{54}$
$q = 3, n = 5$	0.310	2120.570	7181.200	$x_{243}^{164} + x_{243}^{162}$

EEGCD function: Using our extended Euclidean division greatest common divisor function (EEGCD) to do the elimination and to compute Δ, we get the following timings.

Table 7.5: Timing EEGCD function for elimination and Δ computation

values of q and n	*Timing* *elimination /sec*	*Timing* Δ */sec*	*Timing* q^{th} *power*	*Computed* Δ
$q = 2, n = 2$	0.130	0.010	0.010	$x_4^3 + x_4^2$
$q = 2, n = 3$	0.130	0.000	0.090	$x_8^8 + x_8^6$
$q = 2, n = 4$	0.150	0.010	0.130	$x_{16}^{17} + x_{16}^{16} + x_{16}^{15} + x_{16}^{14}$
$q = 2, n = 5$	0.140	0.010	0.880	$x_{32}^{34} + x_{32}^{30}$
$q = 2, n = 6$	0.190	0.010	5.930	$x_{64}^{67} + x_{64}^{66} + x_{64}^{63} + x_{64}^{62}$
$q = 2, n = 7$	0.300	0.090	40.770	$x_{128}^{132} + x_{128}^{130} + x_{128}^{128} + \cdots$
$q = 2, n = 8$	1.550	1.740	294.150	$x_{256}^{261} + x_{256}^{260} + x_{256}^{260} + \cdots$
$q = 2, n = 9$	11.860	139.470	2265.610	$x_{512}^{518} + x_{512}^{510}$
$q = 3, n = 2$	0.150	0.000	0.250	$x_9^{12} + x_9^6$
$q = 3, n = 3$	0.150	0.100	425.050	$x_{27}^{52} + 2x_{27}^{50} + x_{27}^{48} + \cdots$
$q = 3, n = 4$	0.170	0.140	481.460	$x_{81}^{200} + x_{81}^{198} + 2x_{81}^{194} + \cdots$
$q = 3, n = 5$	0.310	53.860	30226.170	$x_{243}^{672} + x_{243}^{654}$

Chapter 8

Towers

In this chapter we will consider some asymptotically good towers by Stichenoth el al, and Noam Elkies. We will transform some of the towers that are not type I form into curves that are type I. This will be done by finding the divisors of the curves. We will also compute a formula for the genus of some of the towers. We begin by defining what we mean by a tower of function fields and asymptotically good towers.

Definition 8.1 ([17], page 439)**.** *A* **tower** *of function fields over* $\mathbb{F}_q$ *is an infinite sequence* $\mathcal{F} = (\mathbf{F}_0, \mathbf{F}_1, \mathbf{F}_2, \ldots)$ *of function fields* $\mathbf{F}_i/\mathbb{F}_q$ *having the properties:*
$(i)\mathbf{F}_0 \subseteq \mathbf{F}_1 \subseteq \mathbf{F}_2 \subseteq \ldots,$ *and for each* $n \geq 1$ *the extension* $\mathbf{F}_n/\mathbf{F}_{n-1}$ *is separable of degree* $[\mathbf{F}_n : \mathbf{F}_{n-1}] > 1.$
$(ii)g(\mathbf{F}_j) > 1$ *for some* $j \geq 0.$

Definition 8.2 ([17], page 440)**.** *The tower* $\mathcal{F} = (\mathbf{F}_i)_{i\geq 0}$ *of functions fields over* $\mathbb{F}_q$ *is said to be* **asymptotically good***, if* $\lambda(\mathcal{F}) > 0,$ *where* $\lambda(\mathcal{F}) := \lim\limits_{i\to\infty} \dfrac{N(\mathbf{F}_i)}{g(\mathbf{F}_i)}.$ *Here* $N(\mathbf{F}_i),$ (*respectively* $g(\mathbf{F}_i)$) *is the number of* $\mathbb{F}_q-$ *rational points (respectively the genus) of* $\mathbf{F}_i.$

Let us now consider some towers and try to put them into type I curves.

8.1 Stichenoth towers

8.1.1 Example 1

Consider the first tower

$$z_{n+1}^q + z_{n+1} = x_n^{q+1} \text{ with } x_n := \frac{z_n}{x_{n-1}},\ 1 \leq n \leq m \tag{8.1}$$

(See [21] for more about this tower and see [3] for more details on the one point description of this tower). So we have that

$$x_n^q x_{n-1}^{q-1} + x_n = x_{n-1}^q, \ 1 \leq n \leq m \tag{8.2}$$

Let P_0 be the unique point at which all the x_{q^n} have zeros and P_∞ be the point at which all have poles. Then from Leonard [3] page 2572, we have the divisors of x_{q^n} to be given by

$$\begin{aligned}(x_{q^n}) = (-q^n).P_\infty \ &+ \sum_{1\leq i\leq (m+1)/2} \sum_j (-q^n).P_{i,j} \ + \sum_{(m+1)/2<i<(m-n+1)} \sum_j (-q^{2i+n-m-1}).P_{i,j} \\ &+ \sum_{(m-n+1)<i\leq m} \sum_j (q^{m-n}).P_{i,j} \ + (q^{m-n}).P_0\end{aligned} \tag{8.3}$$

for $0 \leq n < (m+1)/2$ and

$$\begin{aligned}(x_{q^n}) = (-q^n).P_\infty \ &+ \sum_{1\leq i<m-n+1} \sum_j (-q^n).P_{i,j} \ + \sum_{m-n+1\leq i\leq (m+1)/2} \sum_j (-q^{2(m-i)-n+1}).P_{i,j} \\ &+ \sum_{(m+1)/2<i\leq m} \sum_j (q^{m-n}).P_{i,j} \ + (q^{m-n}).P_0\end{aligned} \tag{8.4}$$

for $(m+1)/2 \leq n \leq m$.

The choices for local parameters are $t_P := 1/x_{q^0}$ for $P = P_\infty$ or $P = P_{i,j}$ with $i < (m + 1)/2,$ and $t_P := x_{q^m}$ for $P = P_0$ and $P = P_i, j$ for $i \geq (m+1)/2$. Now the following change of variables

$$x_{2q^m + \sum_{j=n}^m q^{j-1}} = x_m^2 \prod_{j=n}^m x_j \tag{8.5}$$

puts equation (8.2) into type I form.

Now take $q = 2,$ and $m = 2$, and with respect to the pole orders, define

$$y_1 := x_0, \quad y_2 := x_1, \quad y_4 := x_2, \quad y_{11} := y_1 y_2 y_4^2, \quad y_6 := y_2 y_4$$

Then we get the following equations

$$y_1^2y_2 + y_1 + y_2^2 = 0,$$
$$y_2^2y_4 + y_2 + y_4^2 = 0,$$

From which we have the following type I integral equations.

$$\begin{aligned} y_6^2 + y_6 + y_4^3 &= 0 \\ y_{11}^2 + y_{11}y_4^2 + y_6y_4^4 + y_6y_4 + y_4^4 &= 0 \end{aligned} \tag{8.6}$$

Now take $q = 3,$ and $m = 2$, and with respect to the pole orders, define

$$y_1 := x_0, \quad y_3 := x_1, \quad y_9 := x_2, \quad y_{22} := y_1y_3y_9^2, \quad y_{12} := y_3y_9$$

Then we get the following equations

$$\begin{aligned} y_1^3y_3^2 + y_1 + 2y_3^3 &= 0 \\ y_3^3y_9^2 + y_3 + 2y_9^3 &= 0 \end{aligned} \tag{8.7}$$

From which we have the following type I integral equations.

$$\begin{aligned} y_{12}^3 + y_{12} + 2y_9^4 &= 0 \\ y_{22}^3 + y_{22}y_9^4 + y_{12}^2y_9^2 + 2y_{12}y_9^6 &= 0. \end{aligned} \tag{8.8}$$

Now take $q = 3,$ and $m = 3$, and with respect to the pole orders, define

$y_1 := x_0,\ y_3 := x_1,\ y_9 := x_2,\ y_{27} := x_3,\ y_{36} := y_9y_{27},\ y_{66} := y_3y_9y_{27}^2,\ y_{67} := y_1y_3y_9y_{27}^2.$

Then we get the following equations

$$\begin{aligned} y_1^3y_3^2 + y_1 + 2y_3^3 &= 0, \\ y_3^3y_9^2 + y_3 + 2y_9^3 &= 0, \\ y_9^3y_{27}^2 + y_9 + 2y_{27}^3 &= 0. \end{aligned} \tag{8.9}$$

From which we have the following type I integral equations.

$$\begin{aligned} y_{36}^3 + 2y_{27}^4 + y_{36} &= 0, \\ y_{66}^3 + 2y_{36}y_{27}^6 + y_{66}y_{27}^4 + y_{36}^2y_{27}^2 &= 0, \\ y_{67}^6 + 2y_{66}^2y_{27}^{10} + 2y_{67}y_{66}y_{36}^2y_{27}^7 + 2y_{67}^2y_{36}y_{27}^8 + 2y_{27}^{14} + y_{67}y_{66}^2y_{36}y_{27}^5 + y_{67}y_{66}y_{27}^7 & \\ +y_{67}^2y_{36}^2y_{27}^4 + 2y_{36}y_{27}^{10} + 2y_{67}y_{66}y_{36}y_{27}^3 + 2y_{36}^2y_{27}^6 + y_{66}^2y_{27}^2 &= 0. \end{aligned} \tag{8.10}$$

Remark 8.1. *We note that the equation*

$$\begin{aligned} y_{67}^6 \quad + & \quad 2y_{66}^2y_{27}^{10} + 2y_{67}y_{66}y_{36}^2y_{27}^7 + 2y_{67}^2y_{36}y_{27}^8 + 2y_{27}^{14} + y_{67}y_{66}^2y_{36}y_{27}^5 + y_{67}y_{66}y_{27}^7 \\ + & \quad y_{67}^2y_{36}^2y_{27}^4 + 2y_{36}y_{27}^{10} + 2y_{67}y_{66}y_{36}y_{27}^3 + 2y_{36}^2y_{27}^6 + y_{66}^2y_{27}^2 = 0 \end{aligned}$$

is not a cubic type I integral equation. But we know that $y_{67} = y_{27}^2y_9y_3y_1$. *So*

$$\begin{aligned} y_{67}^3 &= y_{27}^6y_9^3y_3^3y_1^3 \\ &= y_{27}^6y_9^3y_3(y_3^3 - y_1) \\ &= y_{27}^6y_9^3y_3^4 + 2y_{27}^6y_9^3y_3y_1 \\ &= y_{27}^6y_9y_3(y_9^3 - y_3) + 2y_{27}^4y_9^2y_{67} \\ &= y_{27}^6y_9^4y_3 - y_{27}^6y_9y_3^2 + 2y_{27}^2y_{36}^2y_{67} \\ &= y_{27}^4y_9y_3(y_{27}^3 - y_9) + 2y_{27}^6y_9y_3^2 + 2y_{27}^2y_{36}^2y_{67} \\ &= y_{27}^7y_9y_3 + 2y_{27}^4y_9^2y_3 + 2y_{27}^6y_9y_3^2 + 2y_{27}^2y_{36}^2y_{67} \end{aligned}$$

Hence defining

$$y_{201} := y_{27}^7 y_9 y_3, \quad y_{129} := y_{27}^4 y_9^2 y_3, \quad y_{177} := y_{27}^6 y_9 y_3^2,$$

we get

$$y_{67}^3 + 2y_{201} + y_{177} + y_{129} + y_{67} y_{27}^2 y_{36}^2 = 0$$

which is a cubic type I integral equation. However, in order to obtain this cubic equation, we had to define some new variables.

This observation is expressed in the following conjecture.

Conjecture 8.1. *Given the tower*

$$x_n^q x_{n-1}^{q-1} + x_n = x_{n-1}^q, \ 1 \leq n \leq m$$

and the following change of variables

$$x_{2q^m + \sum_{j=n}^m q^{j-1}} = x_m^2 \prod_{j=n}^m x_j$$

we can eliminate the first m variables to get type I integral equations that may (or may not) be q^{th}-extensions of the previous tower. However, if the equations are are not q^{th}-extensions of the previous tower, we can introduce new variables, defined in terms of the initial variables $x_n, \ 1 \leq n \leq m$, to get q^{th}-extensions of the previous tower that are type I integral equations. Hence the extensions gotten this may contain additional variables.

8.1.2 Example 2

Consider the second tower

$$x_{i+1}^q + x_{i+1} = \frac{x_i^q}{x_i^{q-1} + 1}, \ 1 \leq i \leq m \tag{8.11}$$

(See [16], page 61, for more about this tower and see [3] for more details on the one point description of this tower).

Let P_0 be the unique point at which all the x_{q^n} have zeros and P_∞ be the point at which all have poles. Then from Leonard [3] page 2572, we have the divisors of x_{q^n} to be given by

$$(x_{q^n}) = (-q^n).P_\infty \ + \sum_{1\leq i\leq (m+2)/2} \sum_j (-q^n).P_{i,j} + \sum_{(m+2)/2<i<(m-n+1)} \sum_j (-q^{2(i-1)+n-m}).P_{i,j}$$
$$+ \sum_{(m-n+1)<i\leq m+1} \sum_j (q^{m-n}).P_{i,j} \ + (q^{m-n}).P_0 \tag{8.12}$$

for $0 \leq n < m/2$ and

$$(x_{q^n}) = (-q^n).P_\infty \ + \sum_{1\leq i<m-n+1} \sum_j (-q^n).P_{i,j} + \sum_{m-n+1\leq i\leq (m+2)/2} \sum_j (-q^{2(m-i+1)-n}).P_{i,j}$$
$$+ \sum_{(m+2)/2<i\leq m+1} \sum_j (q^{m-n}).P_{i,j} \ + (q^{m-n}).P_0 \tag{8.13}$$

for $m/2 \leq n \leq m+1$.

The choices for local parameters are $t_P := 1/x_{q^0}$ for $P = P_\infty$ or $P = P_{i,j}$ with $i < (m+1)/2$, and $t_P := x_{q^m}$ for $P = P_0$ and $P = P_i, j$ for $i \geq (m+1)/2$. Now the following change of variables

$$x_{q^{(i-1)}+\sum_{j=i+1}^{m}(q-1)q^{j-1}} = x_i \prod_{j=i+1}^{m} x_j^{(q-1)} + 1, \ 1 \leq i \leq m. \tag{8.14}$$

puts equation (8.11) into type I form.

Now take $q = 2$, and $m = 2$, and with respect to the pole orders, define

$$y_1 := x_0, \quad y_2 := x_1, \quad y_4 := x_2, \quad y_6 := y_2(y_4+1), \quad y_7 := y_1(y_2+1)(y_4+1)$$

Then we get the following equations

$$\begin{aligned} y_1^2y_2 + y_1^2 + y_1y_2 + y_1 + y_2^2 &= 0 \\ y_2^2y_4 + y_2^2 + y_2y_4 + y_2 + y_4^2 &= 0, \end{aligned}$$

from which we have the following type I integral equations.

$$\begin{aligned} y_6^2 + y_6y_4 + y_6 + y_4^3 + y_4^2 &= 0 \\ y_7^2 + y_7y_6 + y_7y_4 + y_7 + y_6y_4^2 &= 0. \end{aligned} \tag{8.15}$$

Now take $q = 3,$ and $m = 2$, and with respect to the pole orders, define

$$y_1 := x_0, \quad y_3 := x_1, \quad y_9 := x_2, \quad y_{21} := y_3(y_9^2 + 1), \quad y_{25} := y_1(y_3^2 + 1)(y_9^2 + 1)$$

Then we get the following equations

$$\begin{aligned} y_1^3y_3^2 + y_1^3 + y_1y_3^2 + y_1 + 2y_3^3 &= 0 \\ y_3^3y_9^2 + y_3^3 + y_3y_9^2 + y_3 + 2y_9^3 &= 0 \end{aligned} \tag{8.16}$$

from which we have the following type I integral equations.

$$\begin{aligned} y_{21}^3 + y_{21}y_9^4 + 2y_{21}y_9^2 + y_{21} + 2y_9^7 + y_9^5 + 2y_9^3 &= 0 \\ y_{25}^3 + y_{25}y_{21}^2 + y_{25}y_{21}y_9^3 + y_{25}y_9^4 + 2y_{25}y_9^2 + y_{25} + 2y_{21}y_9^6 &= 0 \end{aligned} \tag{8.17}$$

Now take $q = 3,$ and $m = 3$, and with respect to the pole orders, define

$y_1 := x_0, \quad y_3 := x_1, \quad y_9 := x_2, \quad y_{27} := x_3, \quad y_{63} := y_9(y_{27}^2 + 1),$

$y_{75} := y_3(y_9^2 + 1)(y_{27}^2 + 1), \quad y_{79} := y_1(y_3^2 + 1)(y_9^2 + 1)(y_{27}^2 + 1)$

Then we get the following equations

$$
\begin{aligned}
y_1^3y_3^2 + y_1^3 + y_1y_3^2 + y_1 + 2y_3^3 &= 0 \\
y_3^3y_9^2 + y_3^3 + y_3y_9^2 + y_3 + 2y_9^3 &= 0 \\
y_9^3y_{27}^2 + y_9^3 + y_9y_{27}^2 + y_9 + 2y_{27}^3 &= 0, \qquad (8.18)
\end{aligned}
$$

from which we have the following type I integral equations.

$$
\begin{aligned}
y_{63}^3 + y_{63}y_{27}^4 + 2y_{63}y_{27}^2 + y_{63} + 2y_{27}^7 + y_{27}^5 + 2y_{27}^3 &= 0 \\
y_{75}^3 + y_{75}y_{63}^2 + y_{75}y_{63}y_{27}^3 + y_{75}y_{27}^4 + 2y_{75}y_{27}^2 + y_{75} + 2y_{63}y_{27}^6 &= 0 \\
y_{79}^3 + y_{79}y_{75}^2 + 2y_{79}y_{75}y_{63} + y_{79}y_{75}y_{27}^3 + y_{79}y_{63}^2 + y_{79}y_{63}y_{27}^3 + y_{79}y_{27}^4 & \\
+2y_{79}y_{27}^2 + y_{79} + 2y_{75}y_{63}^2 + 2y_{75}y_{63}y_{27}^3 + 2y_{75}y_{27}^6 &= 0
\end{aligned}
$$

8.1.3 Example 3

Consider the tower

$$
\frac{y-1}{y^q} = \frac{x^q-1}{x} \tag{8.19}
$$

See [16], page 61, for more about this tower. We can write the divisors for the first level of the tower with $q = 2$ as follows

$$
\begin{array}{rlll}
\mathrm{div}(y) & = -2\mathrm{P}_1 & +2\mathrm{P}_2 + & 0\mathrm{P}_3 + 0\mathrm{P}_4 \\
\mathrm{div}(y-1) & = -2\mathrm{P}_1 & +0\mathrm{P}_2 + & 1\mathrm{P}_3 + 1\mathrm{P}_4 \\
\mathrm{div}(x) & = 1\mathrm{P}_1 & +1\mathrm{P}_2 + & -2\mathrm{P}_3 + 0\mathrm{P}_4 \\
\mathrm{div}(x-1) & = 0\mathrm{P}_1 & +0\mathrm{P}_2 + & -2\mathrm{P}_3 + 2\mathrm{P}_4
\end{array}
$$

For $q = 3$, and considering the first level of the tower, we get

$$\begin{aligned}
\mathrm{div}(y) &= -3\mathrm{P}_1 && +0\mathrm{P}_2 + \ 3\mathrm{P}_3 + 0\mathrm{P}_4 \\
\mathrm{div}(y-1) &= -3\mathrm{P}_1 && +2\mathrm{P}_2 + \ 0\mathrm{P}_3 + 1\mathrm{P}_4 \\
\mathrm{div}(x) &= 2\mathrm{P}_1 && + - 3\mathrm{P}_2 + 1\mathrm{P}_3 + 0\mathrm{P}_4 \\
\mathrm{div}(x-1) &= 0\mathrm{P}_1 && + - 3\mathrm{P}_2 + 0\mathrm{P}_3 + 3\mathrm{P}_4
\end{aligned}$$

In general for the first level and any q, we can write

$$\begin{array}{rccccc}
 & & P_1 & P_2 & P_3 & P_4 \\
\text{div(y)} & = & -q & q & 0 & 0 \\
\text{div(y-1)} & = & -q & 0 & 1 & q-1 \\
\text{div(x)} & = & q-1 & 1 & 0 & -q \\
\text{div(x-1)} & = & 0 & 0 & q & -q
\end{array}$$

In general for the second level and any q, we can write

$$\begin{array}{rcccccc}
 & & P_1 & P_2 & P_3 & P_4 & P_5 \\
\mathrm{div}(x_2) & = & -q^2 & q^2 & 0 & 0 & 0 \\
\mathrm{div}(x_2-1) & = & -q^2 & 0 & 1 & q(q-1) & q-1 \\
\mathrm{div}(x_1) & = & q(q-1) & q & 0 & -q^2 & 0 \\
\mathrm{div}(x_1-1) & = & 0 & 0 & q & -q^2 & q(q-1) \\
\mathrm{div}(x_0) & = & q-1 & 1 & 0 & q(q-1) & -q^2 \\
\mathrm{div}(x_0-1) & = & 0 & 0 & q^2 & 0 & -q^2
\end{array}$$

We now generalize the above for any level, n, of the tower and any q.

		P_1	P_2	P_3	P_4	$\dots$	P_n	P_{n+1}	P_{n+2}	P_{n+3}
(x_n)	$=$	q^n	$-q^n$	0	0	$\dots$	0	0	0	0
$(x_n - 1)$	$=$	0	$-q^n$	$q^{n-1}(q-1)$	$q^{n-2}(q-1)$	$\dots$	$q^2(q-1)$	$q(q-1)$	$(q-1)$	1
$(x_{(n-1)})$	$=$	q^{n-1}	$q^{n-1}(q-1)$	$-q^n$	0	$\dots$	0	0	0	0
$(x_{(n-1)} - 1)$	$=$	0	0	$-q^n$	$q^{n-1}(q-1)$	$\dots$	$q^3(q-1)$	$q^2(q-1)$	$q(q-1)$	q
$(x_{(n-2)})$	$=$	q^{n-2}	$q^{n-2}(q-1)$	$q^{n-1}(q-1)$	$-q^n$	$\dots$	0	0	0	0
$(x_{(n-2)} - 1)$	$=$	0	0	0	$-q^n$	$\dots$	$q^4(q-1)$	$q^3(q-1)$	$q^2(q-1)$	q^2
$\vdots$	$=$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
(x_2)	$=$	q^2	$q^2(q-1)$	$q^3(q-1)$	$q^4(q-1)$	$\dots$	$-q^n$	0	0	0
$(x_2 - 1)$	$=$	0	0	0	0	$\dots$	$-q^n$	$q^{n-1}(q-1)$	$q^{n-2}(q-1)$	q^{n-2}
(x_1)	$=$	q	$q(q-1)$	$q^2(q-1)$	$q^3(q-1)$	$\dots$	$q^{n-1}(q-1)$	$-q^n$	0	0
$(x_1 - 1)$	$=$	0	0	0	0	$\dots$	0	$-q^n$	$q^{n-1}(q-1)$	q^{n-1}
(x_0)	$=$	1	$(q-1)$	$q(q-1)$	$q^2(q-1)$	$\dots$	$q^{n-2}(q-1)$	$q^{n-1}(q-1)$	$-q^n$	0
$(x_0 - 1)$	$=$	0	0	0	0	$\dots$	0	0	$-q^n$	q^n

The following change of variables

$$x_{2q^m-(q-1)q^{(i-1)}} = x_i(x_m - 1)^2 \prod_{j=i+1}^{m-1} (x_j - 1), \ 1 \leq i \leq m. \tag{8.20}$$

puts equation (8.19) into type I form.

For example take $q = 2,$ and $m = 2$, and with respect to the pole orders, define

$$y_4 := x_0 + 1, \quad y_6 := x_1(x_0 + 1)^2, \quad y_7 := x_2(x_1 + 1)(x_0 + 1)^2.$$

Then we have the following from (8.19)

$$y_6^2 + y_6 y_4 + y_6 + y_4^3 + y_4^2 = 0$$
$$y_7^2 y_6 + y_7^2 y_4^2 + y_7 y_6 y_4^2 + y_6 y_4^4 + y_6 y_4^3 + y_6 y_4^2 + y_4^5 + y_4^4 = 0$$

From which we have the following type I integral equations.

$$y_6^2 + y_6 y_4 + y_6 + y_4^3 + y_4^2 = 0$$
$$y_7^2 + y_7 y_6 + y_7 y_4 + y_7 + y_6 y_4^2 = 0$$

Take $q = 2,$ and $m = 3$, and with respect to the pole orders, define

$$y_8 := x_0{+}1, \quad y_{12} := x_1(x_0{+}1)^2, \quad y_{14} := x_2(x_1{+}1)(x_0{+}1)^2, \quad y_{15} := x_3(x_2{+}1)(x_1{+}1)(x_0{+}1)^2.$$

Then we have the following from (8.19)

$$\begin{aligned}
y_{12}^2 + y_{12}y_8 + y_{12} + y_8^3 + y_8^2 &= 0\\
y_{14}^2y_{12} + y_{14}^2y_8^2 + y_{14}y_{12}y_8^2 + y_{12}y_8^4 + y_{12}y_8^3 + y_{12}y_8^2 + y_8^5 + y_8^4 &= 0\\
y_{15}^2y_{14} + y_{15}^2y_{12} + y_{15}^2y_8^2 + y_{15}y_{14}y_{12} + y_{15}y_{14}y_8^2 + y_{14}y_{12}y_8^2 + y_{14}y_{12}y_8 + y_{14}y_{12}&\\
+y_{14}y_8^4 + y_{14}y_8^3 + y_{14}y_8^2 + y_{12}y_8^4 + y_{12}y_8^3 + y_{12}y_8^2 + y_8^5 + y_8^4 &= 0
\end{aligned}$$

from which we get the following type I integral equations.

$$\begin{aligned}
y_{12}^2 + y_{12}y_8 + y_{12} + y_8^3 + y_8^2 &= 0\\
y_{14}^2 + y_{14}y_{12} + y_{14}y_8 + y_{14} + y_{12}y_8^2 &= 0\\
y_{15}^2 + y_{15}y_{14} + y_{15}y_{12} + y_{15}y_8 + y_{15} + y_{14}y_{12} + y_{14}y_8^2 &= 0
\end{aligned}$$

Take $q = 3,$ and $m = 2$, and with respect to the pole orders, define

$$y_9 := x_0 - 1, \quad y_{12} := x_1(x_0 - 1)^2, \quad y_{16} := x_2(x_1 - 1)(x_0 - 1)^2.$$

Then we have the following from (8.19)

$$\begin{aligned}
y_{12}^3 + 2y_{12}y_9^2 + 2y_{12}y_9 + y_9^4 + y_9^3 &= 0\\
2y_{16}^3y_{12} + y_{16}^3y_9^2 + y_{16}y_{12}y_9^4 + 2y_{12}^2y_9^4 + y_{12}y_9^6 &= 0,
\end{aligned}$$

from which we get the following type I integral equations.

$$
\begin{aligned}
y_{12}^3 + 2y_{12}y_9^2 + 2y_{12}y_9 + y_9^4 + y_9^3 &= 0 \\
y_{16}^3 + y_{16}y_{12}^2 + y_{16}y_{12}y_9^2 + 2y_{16}y_9^2 + 2y_{16}y_9 + 2y_{12}^4 + y_{12}^2y_9^2 + y_{12}^2y_9 + 2y_{12}y_9^3 &= 0.
\end{aligned}
$$

Take $q = 3,$ and $m = 3$, and with respect to the pole orders, define

$$y_{27} := x_0-1, \quad y_{36} := x_1(x_0-1)^2, \quad y_{48} := x_2(x_1-1)(x_0-1)^2, \quad y_{52} := x_3(x_2-1)(x_1-1)(x_0-1)^2.$$

Then we have the following from (8.19)

$$
\begin{aligned}
y_{36}^3 + 2y_{36}y_{27}^2 + 2y_{36}y_{27} + y_{27}^4 + y_{27}^3 &= 0 \\
2y_{48}^3y_{36} + y_{48}^3y_{27}^2 + y_{48}y_{36}y_{27}^4 + 2y_{36}^2y_{27}^4 + y_{36}y_{27}^6 &= 0 \\
y_{52}^3y_{48} + 2y_{52}^3y_{36} + y_{52}^3y_{27}^2 + 2y_{52}y_{48}y_{36}^2 + 2y_{52}y_{48}y_{36}y_{27}^2 + 2y_{52}y_{48}y_{27}^4 + y_{48}^2y_{36}^2 & \\
+y_{48}^2y_{36}y_{27}^2 + y_{48}^2y_{27}^4 + 2y_{48}y_{36}y_{27}^2 + 2y_{48}y_{36}y_{27} + y_{48}y_{27}^6 + y_{48}y_{27}^4 + y_{48}y_{27}^3 &= 0
\end{aligned}
$$

from which we get the following type I integral equations.

$$
\begin{aligned}
y_{36}^3 + 2y_{36}y_{27}^2 + 2y_{36}y_{27} + y_{27}^4 + y_{27}^3 &= 0 \\
y_{48}^3 + y_{48}y_{36}^2 + y_{48}y_{36}y_{27}^2 + 2y_{48}y_{27}^2 + 2y_{48}y_{27} + 2y_{36}^4 + y_{36}^2y_{27}^2 + y_{36}^2y_{27} + 2y_{36}y_{27}^3 &= 0 \\
y_{52}^3 + y_{52}y_{48}^2 + y_{52}y_{48}y_{36} + 2y_{52}y_{48}y_{27}^2 + y_{52}y_{36}^2 + y_{52}y_{36}y_{27}^2 + y_{52}y_{27}^2 + 2y_{52}y_{27} + 2y_{48}y_{36}^3 & \\
+y_{48}y_{36}^2 + 2y_{48}y_{36}y_{27}^2 + y_{48}y_{36}y_{27} + 2y_{48}y_{27}^3 &= 0
\end{aligned}
$$

8.1.4 Example 4

Consider the tower

$$(x_j^2 - 1)(z_{j+1}^2 - 1) = 1 \quad (j = 1, \ldots, n-2), \tag{8.21}$$

where

$$z_j := \frac{x_j + 3}{x_j - 1} \tag{8.22}$$

See N.D.Elkies [25], page 4, for more about this tower. From the above two equations we get that

$$8(x_j^2 - 1)(x_{j+1} + 1) - (x_{j+1} - 1)^2 = 0 \quad (j = 1, \ldots, n-2). \tag{8.23}$$

We can write the divisors for the first level of the tower over any field of positive characteristic $q > 0$ as follows;

$$\begin{array}{rcrrrr}
 & & P_1 & P_2 & P_3 & P_4 \\
\operatorname{div}(x_2 - 1) & = & -2 & 0 & 1 & 1 \\
\operatorname{div}(x_2 + 1) & = & -2 & 2 & 0 & 0 \\
\operatorname{div}(x_1 - 1) & = & -1 & -1 & 2 & 0 \\
\operatorname{div}(x_1 + 1) & = & -1 & -1 & 0 & 2
\end{array}$$

For the second level the divisors are

$$\begin{array}{rcrrrrr}
\operatorname{div}(x_3 - 1) & = & -4 & 0 & 2 & 1 & 1 \\
\operatorname{div}(x_3 + 1) & = & -4 & 4 & 0 & 0 & 0 \\
\operatorname{div}(x_2 - 1) & = & -2 & -2 & 0 & 2 & 2 \\
\operatorname{div}(x_2 + 1) & = & -2 & -2 & 4 & 0 & 0 \\
\operatorname{div}(x_1 - 1) & = & -1 & -1 & -2 & 4 & 0 \\
\operatorname{div}(x_1 + 1) & = & -1 & -2 & -1 & 0 & 4
\end{array}$$

We now generalize the above for any level, n, of the tower.

		P_1	P_2	P_3	P_4	$\dots$	P_n	P_{n+1}	P_{n+2}	P_{n+3}
$(x_{n+1}-1)$	$=$	-2^n	0	2^{n-1}	2^{n-2}	$\dots$	4	2	1	1
$(x_{n+1}+1)$	$=$	-2^n	2^n	0	0	$\dots$	0	0	0	0
(x_n-1)	$=$	-2^{n-1}	-2^{n-1}	0	2^{n-1}	$\dots$	8	4	2	2
(x_n+1)	$=$	-2^{n-1}	-2^{n-1}	2^n	0	$\dots$	0	0	0	0
(x_{n-1-1})	$=$	-2^{n-2}	-2^{n-2}	-2^{n-1}	0	$\dots$	16	8	4	4
$(x_{n-1}+1)$	$=$	-2^{n-2}	-2^{n-2}	-2^{n-1}	2^n	$\dots$	0	0	0	0
$\vdots$	$=$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
(x_3-1)	$=$	-4	-4	-8	-16	$\dots$	2^n	0	0	0
(x_3+1)	$=$	-4	-4	-8	-16	$\dots$	0	2^{n-1}	2^{n-2}	2^{n-2}
(x_2-1)	$=$	-2	-2	-4	-8	$\dots$	-2^{n-1}	2^n	0	0
(x_2+1)	$=$	-2	-2	-4	-8	$\dots$	-2^{n-1}	0	2^{n-1}	2^{n-1}
(x_1-1)	$=$	-1	-1	-2	-4	$\dots$	-2^{n-2}	-2^{n-1}	2^n	0
(x_1+1)	$=$	-1	-1	-2	-4	$\dots$	-2^{n-2}	-2^{n-1}	0	2^n

The following change of variables

$$x_{2q^m+\sum_{j=i}^{m}2^{(j-1)}} = (x_{m+1}+1)\prod_{j=i}^{m-1}(x_j+1),\ 1 \leq i \leq m, \tag{8.24}$$

puts equation (8.23) into type I form. Let GF[3] represent the finite field of characteristic 3.

Take $m = 2$, and with respect to the pole orders, define

$$y_4 := x_3+1, \quad y_6 := x_2+1(x_1+1), \quad y_7 := (x_1+1)(x_2+1)(x_3+1).$$

From equation (8.23) we have the following type I integral equations.

$$y_6^2 + y_6y_4 + y_4^3 + 2y_4^2 + y_4 = 0$$
$$y_7^2 + y_7y_6 + 2y_6y_4^2 + y_6y_4 + 2y_6 + 2y_4^3 + y_4^2 + 2y_4 = 0$$

Take $m = 3$, and with respect to the pole orders, define $y_8 := x_4 + 1, \quad y_{12} := (x_3 + 1)(x_4 + 1), \quad y_{14} := (x_2 + 1)(x_3 + 1)(x_4 + 1)$,
$y_{15} := (x_1 + 1)(x_2 + 1)(x_3 + 1)(x_4 + 1)$. From equation (8.23) we have the following type I integral equations.

$$y_{12}^2 + y_{12}y_8 + y_8^3 + 2y_8^2 + y_8 = 0$$
$$y_{14}^2 + y_{14}y_{12} + 2y_{12}y_8^2 + y_{12}y_8 + 2y_{12} + 2y_8^3 + y_8^2 + 2y_8 = 0$$
$$y_{15}^2 + y_{15}y_{14} + 2y_{14}y_{12} + y_{14}y_8^2 + y_{14}y_8 + y_{14} + y_{12}y_8^2 + 2y_{12}y_8 + y_{12} + y_8^3 + 2y_8^2 + y_8 = 0$$

Bibliography

[1] D. A. Leonard and R. Pellikaan, "Integral Closures and weight functions over finite Fields", Finite Fields and Their Applications, 9:479-504, 2003.

[2] A. Taylor, "Methods for Computing Normalisations of Affine Rings", Advances in algebra and geometry, (Hyderabad, 2001), 279-295, Hindustan Book Agency, New Delhi, 2003.

[3] D. A. Leonard, "Finding the defining functions for one-point algebraic-geometry codes", IEEE Transactions on information theory, VOL.47, NO.6, 2566-2573, 2001.

[4] D. A. Leonard, "A weighted module view of integral closures of affine domians of type I", Advances in mathematics of communications, volume 3, No.1, 1-11, 2009.

[5] D. A. Leonard, " Addentum to A weighted module view of integral closures of affine domians of type I", http://www.dms.auburn.edu/ leonada/downloads/addendum02102009.pdf.

[6] P. Olav, and R. Pellikan, "On the structure of order domains", Finite Fields and Their Applications, 8:369-396, 2002.

[7] G-M. Greuel, S. Laplagne, and F. Seelisch, "Normalization of Rings", arXiv:0904.3561v1 [math.AC], Submitted on 22 Apr 2009.

[8] A. K. Singh, and I. Swanson, "An algorithm for computing the integral closure", Commutative Algebra (math.AC) arXiv:0901.0871v1 [math.AC] Submitted on 7 Jan 2009

[9] T. De Jong, "An Algorithm for computing the integral closure", J. Symbolic computation, 26: 273-277, 1998.

[10] "The MAGMA Computational Algebra System for Algebra, Number Theory and Geometry", The University of Sydney Computational Algebra Group, http://magma.maths.usyd.edu.au/magma.

[11] D. R. Grayson, and M. E. Stillman, "MACAULAY 2, a software system for research in algebraic geometry", Available at http://www.math.uiuc.edu/Macaulay2/.

[12] G. M. Greuel, G. Pfister, and H. Schönemann, " SINGULAR 3-1-0. A computer algebra system for polynomial computations", Center for computer algebra, University of Kaiserslautern, (2009), http://www.singular.uni-kl.de.

[13] D. Cox, J. Little, and D. O'Shea, "Ideals, varieties, and algorithms. An introduction to computational algebraic geometry and commutative algebra", Springer, third edition (2007).

[14] D. Eisenbud, "Commutative algebra with a view toward algebraic geometry", Springer-Verlag, (1995).

[15] G. M. Greuel, and G. Pfister, "A Singular Introduction to commutative algebra", Springer-Verlag Berlin Heidelberg New York, (2002).

[16] P. Beelen, A. Garcia, and H. Stichenoth, "Towrads a classification of recursive towers of function fields over finite fields", Finite Fields and Their Applications, 12: 56-77, 2006.

[17] A. Garcia, and H. Stichenoth, "Asymtotics for the genus and the number of rational places in towers of function fields over a finite field", Finite Fields and Their Applications, 11: 434-450, 2005.

[18] P. Beelen, A. Garcia, and H. Stichenoth "On towers of fields of Artin-Schreier type", Bull Braz Math Soc, new series 35(2) : 151-164, 2004.

[19] S. Ling, H. Stichenoth, and S. Yang, "A class of Artin-Schreier towers with finite genus", Bull Braz Math Soc, new series 36(3) : 393-401, 2005.

[20] A. Bassa, and H. Stichenoth, "A simplified proof for the limit of a tower over a cubic finite filed", Journal of number theory, vol 123, : 154-169, 2007.

[21] A. Garcia, and H. Stichenoth, "On the asymptotic behaviour of some towers of function fields over finite fileds", Journal of number theory, vol 61, : 248-273, 1996.

[22] A. Garcia, H. Stichenoth, and M. Thomas, "On towers and composita of towers of function fields over finite fields", Finite Fields and Their Applications, 3: 257-274, 1997.

[23] G.L. Feng, T.R.N. Rao, "A simple approach for the construction of algebraic-geometric codes from affine plane curves", IEEE Trans. Inform. Theory, 40 (3): 1003-1012, 1994.

[24] K. Saints, C. Heegard, "Algebraic-Geometric codes and multidimensional cyclic codes: a unified theory and algorithms for decoding using Gröbner bases", IEEE Trans. Inform. Theory, 41 (6): 1753-1761, 1995.

[25] N. Elkies, "Explicit modular towers", Proceedings of the Thirty-Fifth [1997] Annual Allerton Conference on Communication, Control and Computing, math/0103107v1 [math.NT] 16 Mar 2001.

[26] J. V. Z. Gathen, J. Gerhard, "Introduction to finite fields and their applications", Cambridge University Press, 2 edition, 2003.

[27] B. Buchberger, F. Winkler, "Gröbner bases and Applicationsociety", London Mathematical Society. Lecture Note Series 251, Cambridge University Press, 1^{st} edition, 1998.

[28] C. Huneke, I. Swanson, “Integral closure of ideals, rings, and modules”, London Mathematical Society. Lecture Note Series 336, Cambridge University Press, 2006.

[29] H. Niederreiter, C. Xing, “Rational points on curves over finite fields. Theory and applications”, London Mathematical Society. Lecture Note Series 285, Cambridge University Press, 1^{st} edition, 2001.

[30] D. Dummit, R. M. Foote, “Abstract Algebra” John Wiley and Sons, Inc, 3^{rd} edition, 2004.

[31] R. Lidl, H. Niederreiter, “Introduction to finite fields and their applications”, Cambridge University Press, 1986.

[32] M. Nagata, “Theory commutative fields”, Translations Mathematical monographs, volume 125, 1993.

[33] H. Stichtenoth, “Algebraic function fields and codes”, Springer-Verlag Berlinn Heidelberg, 1993.

[34] R. Lidl, H. Niederreiter, “Finite fields”, Encyclopedia of Mathematics and its application, Addison-Wesley Publishing Company, 20, Algebra, 1986.