Part I
Order Domains, and their Application in Coding Theory

Preface to part I

This material can be used as an introduction to the relatively new branch of order domains and their application in coding theory. Well-known as well as new results are presented.
It is assumed that the reader is familiar with the most basic Gröbner basis theory. A review of the relevant Gröbner basis theory can be found in appendix I.A. See also [4] for a nice introduction to Gröbner basis theory.
The theory of order domains is very much related to the theory of algebraic function fields and the theory of algebraic geometry. It is the authors policy that this material should be readable also for readers without any experience with these two theories. However, as the connection between the theories is interesting in itself, a continuous discussion of the connection is present throughout the material. This discussion can be skipped.
The references made, refer to the bibliography on pp. 152-155. Also a list of symbols as well as an index of terms can be found on pp. 158-162.

Contents of part I

I.1
A historical survey

The concept of order domains and order functions is rather new. The first references on the subject are [20], [21] and [33]. Independently of this work by van Lint, Høholdt and Pellikaan a similar concept is defined in [30] and [31] by O'Sullivan. Although a new subject, the ideas behind the theory can be found in the theory of algebraic geometry and in the theory of algebraic function field theory. To be more precise, the order function can be viewed as a generalization of the discrete valuation on a function field of transcendence degree 1.

The introduction of this new theory was motivated by the papers [8], [6] and [7] where Feng, Wei, Rao and Tzeng showed, that a large class of algebraic geometry codes can be described without the rather heavy theory of algebraic geometry / algebraic function field theory (in particular without the Riemann-Roch theorem). And that improved constructions of codes can be made from this new descriptions. So the idea has been to build a new theory that is more simple than the algebraic geometry / algebraic function field theory, but still contains enough information to describe a very large class of algebraic geometry codes.

In [8], [6] and [7] Feng, Wei, Rao and Tzeng state lower bounds on the minimum distance of codes defined from so-called well-behaving sequences. However they do it on the level of the code words, instead of on the level of the elements in a related algebraic structure (the order domain). (See also [23], [32] and [39]). In the language of order domain theory this result today is known as the order bound.

The by far largest class of algebraic geometry codes considered, up to the birth of the order domain theory, consists of the following two types of codes. The codes defined from algebraic curves, that is codes defined from function fields of transcendence degree 1. And the Reed-Muller codes, that are codes defined from polynomial rings $\mathbb{F}_q[X_1, \ldots, X_m]$. Note that the quotient field of a polynomial ring in m variables constitutes the simplest example of a function field of transcendence degree m. Beside giving new and more simple descriptions of

many of the algebraic geometry codes that have been considered up to the birth of order domain theory, it has been the hope, that the new theory would make it possible to describe codes defined from a much larger class of function fields of transcendence degree $m > 1$. In [31] O'Sullivan gives examples of nontrivial order domains of transcendence degree greater than 1. However he develops his order domains using methods from algebraic geometry. In [13] Pellikaan and the author of this thesis develop tools, and modify (and generalize slightly) the notion of an order function, such that order domains of arbitrary transcendence degree can easily be constructed. The codes related to order domains of transcendence degree more than 1 are treated in the last chapters of the present thesis.

Already in [8], [6] and [7] Feng, Wei, Rao and Tzeng describes a decoding algorithms for their codes. In [21] it is described how one can decode the dual of an evaluation code coming from an arbitrary order domain. The decoding algorithm uses majority voting and is based on Sakata's extension of the classical Berlekamp-Massey algorithm. Høholdt et. al.'s description is an adaption of a decoding procedure described in [29] by O'Sullivan. The decoding algorithm decodes up to half of the Feng-Rao distance which is a lower bound on the minimum distance given by the order bound.

I.2
Some important definitions

The definition, and in particular the actual construction of order domains, requires some knowledge about certain orderings on different structures. For later reference we will in this chapter discuss different structures and characterize some interesting orderings on these.

I.2.1 Monoids and orderings

We have the following definitions.

Definition I.2.1
Let Λ be a set, and let $+$ be a binary operation on Λ, and 0 an element in Λ. Then $(\Lambda, +, 0)$ is called a commutative monoid if the following conditions hold for any $\alpha, \beta, \gamma \in \Lambda$

$$\begin{array}{ll} (1) & \alpha + 0 = 0 + \alpha = \alpha \\ (2) & (\alpha + \beta) + \gamma = \alpha + (\beta + \gamma) \\ (3) & \alpha + \beta = \beta + \alpha. \end{array}$$

Definition I.2.2
A commutative monoid $(\Lambda, +, 0)$ is called a semigroup if the following condition holds for any $\alpha, \beta, \gamma \in \Lambda$

$$(1) \quad \alpha + \gamma = \beta + \gamma \text{ implies } \alpha = \beta.$$

A semigroup is called inverse free if

$$(2) \quad \alpha + \beta = 0, \text{ implies } \alpha = \beta = 0.$$

And a semigroup is called torsion free if

$$(3) \quad \overbrace{\alpha + \alpha + \cdots + \alpha}^{n \text{ times}} = 0 \text{ for some } n \in \mathbb{N} \text{ implies } \alpha = 0.$$

Any commutative monoid defines a commutative group in the following way.

Definition I.2.3
Given a commutative monoid $(\Lambda, +, 0)$ *then define the relation* $\sim$ *on* $\Lambda \times \Lambda$ *by* $(\alpha, \beta) \sim (\gamma, \delta)$ *if and only if there exists* $\varepsilon \in \Lambda$ *such that* $\alpha + \delta + \varepsilon = \gamma + \beta + \varepsilon$. *Clearly* $\sim$ *is an equivalence relation. The equivalence class of* (α, β) *is denoted by* $[\alpha, \beta]$ *and the set of equivalence classes is denoted by* $D(\Lambda)$. *Define* $[\alpha, \beta] + [\gamma, \delta] = [\alpha + \gamma, \beta + \delta]$. *Then this operation* $+$ *is well-defined and gives* $D(\Lambda)$ *the structure of a commutative group which is called the group of differences of* Λ.

Next we will be concerned with classifying orderings.

Definition I.2.4
Let $\prec$ *be an ordering on the set* Λ. $(\Lambda, \prec)$ *is called a well-order (and* $\prec$ *a well-ordering) if the following condition hold*

(1) *any non empty subset of* Λ *has a smallest element under* $\prec$.

In particular a well-ordering is a total ordering.

Definition I.2.5
Let $(\Lambda, \prec)$ *be a well-order. If a surjective map* $N : \Lambda \to \mathbb{N}$ *exists such that* $N(\alpha) < N(\beta)$ *whenever* $\alpha \prec \beta$, $\alpha, \beta \in \Lambda$ *then we say that* $(\Lambda, \prec)$ *is isomorphic with* $(\mathbb{N}, <)$. *Or we say a little less correct that the ordering* $\prec$ *is isomorphic with the ordering on* $\mathbb{N}$.

Saying that $(\Lambda, \prec)$ is isomorphic to $(\mathbb{N}, <)$ is of course equivalent to saying that the elements of Λ can be ordered in a sequence $(\lambda_1, \lambda_2, \ldots)$ such that $\lambda_i \prec \lambda_{i+1}$ for $i = 1, \ldots$.

Definition I.2.6
Let $(\Lambda, +, 0)$ *be a commutative monoid. A partial ordering* $\prec$ *on* Λ *is called admissible (with respect to* $+$ *and* 0*) if the following conditions hold for any* $\alpha, \beta, \gamma \in \Lambda$.

(1) $0 \prec \alpha$ *whenever* $\alpha \neq 0$
(2) $\alpha \prec \beta$ *implies* $\alpha + \gamma \prec \beta + \gamma$.

Remark I.2.7
Let $(\Lambda, +, 0)$ *be a commutative monoid that possesses a total admissible ordering (with respect to* $+$ *and* 0*). Part (2) of definition I.2.6 ensures that* $(\Lambda, +, 0)$ *is a semigroup.*

Definition I.2.8
Let $\prec$ be an ordering on a semigroup $(\Lambda, +, 0)$. We call $(\Lambda, +, 0, \prec)$ a well-ordered semigroup if $\prec$ is admissible (with respect to $+$ and 0) and $\prec$ is a well-ordering.

Remark I.2.9
A well-ordered semigroup is inverse free and hence torsion free.

I.2.2 Monomial orderings

Of particular importans in the theory of order domains are the following two well-known semigroups $(\mathbb{N}_0^r, +, \mathbf{0} = (0, \ldots, 0))$ and $(\mathcal{M}_r, \cdot, 1)$, where $\mathcal{M}_r$ is the set of monomials in the variables $X_1, X_2, \ldots, X_r$, and where $+$ and $\cdot$ are as usual. We will sometimes use different labels for the indeterminates, say $\cdots$ instead of $X_1, \ldots, X_m$. In this case we write $\mathcal{M}(\cdots)$ for the set of monomials in the indeterminates $\cdots$. For instance the set of monomials in X, Y is denoted $\mathcal{M}(X, Y)$. We will often use the multi index notation $\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \ldots, \alpha_r)$ and $\boldsymbol{X}^{\boldsymbol{\alpha}} = X_1^{\alpha_1} X_2^{\alpha_2} \cdots X_r^{\alpha_r}$.

Using the natural map $\mathbb{N}_0^r \mapsto \mathcal{M}_r$ given by $\boldsymbol{\alpha} \mapsto \boldsymbol{X}^{\boldsymbol{\alpha}}$, an ordering on $\mathbb{N}_0^r$ corresponds to a unique ordering on $\mathcal{M}_r$. Now one gives a special name to orderings $\prec$ on $(\mathbb{N}_0^r, +, \mathbf{0})$ (or equivalent on $(\mathcal{M}_r, \cdot, 1)$), such that $(\mathbb{N}_0^r, +, \mathbf{0}, \prec)$ (or equivalent $(\mathcal{M}_r, \cdot, 1, \prec)$) is a well-ordered semigroup.

Definition I.2.10
An ordering $\prec$ on $(\mathbb{N}_0^r, +, \mathbf{0})$ (or equivalent on $(\mathcal{M}_r, \cdot, 1)$) that is an admissible well-ordering is called a monomial ordering.

Remark I.2.11
If $\prec$ is a monomial ordering on $(\mathbb{N}_0^r, +, \mathbf{0})$ (or equivalent on $(\mathcal{M}_r, \cdot, 1)$) then $\mathbf{0}$ is the smallets element of $\mathbb{N}_0^r$ under $\prec$ (or equivalent 1 is the smallest element of $\mathcal{M}_r$) (see [4, Ch. 2 §4, Cor. 6]).

In the following we will whenever the binary operation $+$ and the neutral element 0 is given by the context, use abbreviated notation and write Λ in the place of $(\Lambda, +, 0)$. In this thesis we will often consider sub semigroups $\Lambda \subseteq \mathbb{N}_0^r$. And we will adjoin an element $-\infty$ to Λ to give $\Lambda_{-\infty} := \Lambda \cup \{-\infty\}$. We will use the convention

$$\lambda + (-\infty) = (-\infty) + (-\infty) = -\infty$$

for any $\lambda \in \Lambda$. To ease the notation we state the following definition.

Definition I.2.12
Let $\prec_{\mathbb{N}_0^r}$ be a monomial ordering on $\mathbb{N}_0^r$. And let $\Lambda \in \mathbb{N}_0^r$ be a semigroup. The restriction $\prec_\Lambda$ of $\prec_{\mathbb{N}_0^r}$ to Λ is said to be a monomial ordering on Λ. Extend $\prec_\Lambda$ to an ordering on $\Lambda_{-\infty}$ by the rule $-\infty \prec_\Lambda \lambda$ for any $\lambda \in \Lambda$. Also this extension is called a monomial ordering.

In the following we describe some important monomial orderings. We mainly describe them on the level of $\mathcal{M}_m$.

Definition I.2.13
Consider indices

$$\{i_1, i_2, \ldots, i_m\} = \{1, 2, \ldots, m\}.$$

The sequence $(X_{i_1}, X_{i_2}, \ldots, X_{i_m})$ defines a so-called lexicographic ordering $\prec_{lex}$ on $\mathcal{M}_m$ by the following rule

$$X_{i_1}^{\alpha_{i_1}} X_{i_2}^{\alpha_{i_2}} \cdots X_{i_m}^{\alpha_{i_m}} \prec_{lex} X_{i_1}^{\beta_{i_1}} X_{i_2}^{\beta_{i_2}} \cdots X_{i_m}^{\beta_{i_m}}$$

if and only if there exists a value $j \in \{1, \ldots, m\}$ such that $\alpha_{i_s} = \beta_{i_s}$ for $s = 1, \ldots, j-1$ and $\alpha_{i_j} < \beta_{i_j}$. We say that the lexicographic ordering is defined by

$$X_{i_m} \prec_{lex} X_{i_{m-1}} \prec_{lex} \cdots \prec_{lex} X_{i_1}.$$

When the lexicographic ordering is not composed with other monomial orderings, then we will sometimes call it the pure lexicographic ordering.

Note that definition I.2.13 gives us $m!$ different lexicographic orderings on $\mathcal{M}_m$ corresponding to the $m!$ different choices of assignments to $j_1, \ldots, j_m$.

Definition I.2.14
Consider so-called weights $w(X_1), w(X_2), \ldots, w(X_m) \in \mathbb{R}_+$, where $\mathbb{R}_+$ is the set of positive real numbers. If these are linearly dependent over $\mathbb{Z}$ then consider also a lexicographic ordering $\prec_{lex}$ on $\mathcal{M}_m$. The weights $w(X_i)$ extends to a monomial function on $\mathcal{M}_m$, that is

$$w : \begin{cases} \mathcal{M}_m & \to & \mathbb{R}_+ \\ \boldsymbol{X^\alpha} & \mapsto & \sum_{i=1}^m \alpha_i w(X_i). \end{cases}$$

In general we will call $w(\boldsymbol{X^\alpha})$ the weight of $\boldsymbol{X^\alpha}$. Now the function w together with the ordering $\prec_{lex}$ defines a monomial ordering $\prec_w$ on $\mathcal{M}_m$ by the following rule

$$M_1 \prec_w M_2$$

if and only if one of the following two conditions holds

$$\begin{array}{ll}(1) & w(M_1) < w(M_2) \\ (2) & w(M_1) = w(M_2) \text{ and } \boldsymbol{X}^{\boldsymbol{\alpha}} \prec_{lex} \boldsymbol{X}^{\boldsymbol{\beta}}.\end{array}$$

We will call this particular ordering a one-dimensional weighted degree lexicographic ordering as the weights belongs to the space $\mathbb{R}_+$*. When* $w(X_1) = \cdots = w(X_m)$ *then we call* $\prec_w$ *a graded lexicographic ordering. The particular graded lexicographic ordering with lexpart given by*

$$X_m \prec_{lex} X_{m-1} \prec_{lex} \cdots \prec_{lex} X_1$$

will be called the standard weighted degree lexicographic ordering (or simply the standard ordering) on $\mathcal{M}_m$*. We will denote it by* $\prec_{st}$*.*

Note that the monomial orderings that we choose to call one-dimensional weighted degree lexicographic orderings are the orderings that in the literature are often called weighted graded lexicographic orderings. The reason why we include the words "one-dimensional" is, that we will define a monomial ordering below where the weights belongs to $\mathbb{N}_0^r \setminus \{0\}$ for arbitrary fixed natural number r. These monomial orderings will contain the orderings from definition I.2.14 as a special case (however not necessarily with $r = 1$).

The following definition very much related to definition I.2.14 is essential when we later in this material construct examples of order domains.

Definition I.2.15
Consider weights $w(X_1), \ldots, w(X_m) \in \mathbb{N}_0^r \setminus \{\mathbf{0}\}$*. Order* $\mathbb{N}_0^r$ *by a monomial ordering* $\prec_{\mathbb{N}_0^r}$ *and order* $\mathcal{M}_m$ *by a lexicographic ordering* $\prec_{lex}$*. We will refer to* $\prec_{\mathbb{N}_0^r}$ *as the inner ordering. The weights extends to a monomial function on* $\mathcal{M}_m$*, that is*

$$w : \begin{cases} \mathcal{M}_m & \to \quad \mathbb{N}_0^r \\ \boldsymbol{X}^{\boldsymbol{\alpha}} & \mapsto \quad \sum_{i=1}^m \alpha_i w(X_i). \end{cases}$$

We will call $w(\boldsymbol{X}^{\boldsymbol{\alpha}})$ *the weight of* $\boldsymbol{X}^{\boldsymbol{\alpha}}$*. Now the weighted degree lexicographic ordering* $\prec_w$ *(on* $\mathcal{M}_m$*) induced by* $w, \prec_{\mathbb{N}_0^r}$ *and* $\prec_{lex}$ *is the monomial ordering defined as follows. Given* $M_1, M_2 \in \mathcal{M}_m$ *then* $M_1 \prec_w M_2$ *if and only if one of the following two conditions holds.*

$$\begin{array}{ll}(1) & w(M_1) \prec_{\mathbb{N}_0^r} w(M_2) \\ (2) & w(M_1) = w(M_2) \text{ and } M_1 \prec_{lex} M_2.\end{array}$$

This definition surely is very general, as actually all monomial orderings can be viewed as weighted degree lexicographic orderings in the following way. Given a monomial ordering $\prec$ on $\mathcal{M}_m$, then simply choose the weights to be the unit vectors in $\mathbb{N}_0^m$, and the ordering on $\mathbb{N}_0^m$ to be $\prec$ (note that in particular, $m = r$ in this case). In this thesis we will often study cases where $m > r$. And we will study families of orderings on $\mathcal{M}_m$ consisting of weighted degree lexicographic orderings that are defined from the same weights in $\mathbb{N}_0^r$, by the same lexicographic ordering on $\mathcal{M}_m$, but by different choices of monomial orderings on $\mathbb{N}_0^r$.

I.3

Order domains

In this chapter we give the definition of an order function and of some important related concepts. We give some simple examples and discuss different aspects of the structures. In later chapters we will construct various examples of order domains.

I.3.1 Order functions, order domains and well-behaving bases

The definition of an order function uses the concept of a k-algebra.

Definition I.3.1
Let k be a field. A k-algebra is a commutative ring R that satisfies the following conditions

(1) *k is a subring of R*
(2) *the unity of k is also a unity in R.*

In the remaining part of this thesis the smallest element of a well-order $(\Lambda, \prec_\Lambda)$ will always be denoted by 0. We will often adjoin an extra element $-\infty$ to Λ to get the set $\Lambda_{-\infty} := \Lambda \cup \{-\infty\}$. We extend the ordering $\prec_\Lambda$ to an ordering on $\Lambda_{-\infty}$ by the rule that $-\infty \prec_\Lambda \alpha$ for any $\alpha \neq -\infty$. This extended ordering will also be denoted by $\prec_\Lambda$. We are now ready to define an order function. The following definition is from [13].

Definition I.3.2
Let R be a k-algebra. An order function on R is a surjective map $\rho : R \mapsto \Lambda_{-\infty}$

where $(\Lambda, \prec_\Lambda)$ is a well-order, such that the following conditions hold

$(O.1)$ $\rho(f) = -\infty$ *if and only if* $f = 0$
$(O.2)$ $\rho(\lambda f) = \rho(f)$ *for all nonzero* $\lambda \in k$
$(O.3)$ $\rho(f+g) \preceq \max_{\prec}\{\rho(f), \rho(g)\}$ *and equality holds whenever* $\rho(f) \prec \rho(g)$
$(O.4)$ *if* $\rho(f) \prec \rho(g)$ *and* $h \neq 0$ *then* $\rho(fh) \prec \rho(gh)$
$(O.5)$ *if* $\rho(f) = \rho(g)$, *then there exists a nonzero* $\lambda \in k$ *such that* $\rho(f - \lambda g) \prec \rho(g)$.

In [20], [21] and [33] Høholdt, van Lint and Pellikaan requires that Λ is a subset of $\mathbb{N}_0$. So in their original set-up the well-ordering of Λ is always the restriction of the usual (and unique) monomial ordering $<$ on $\mathbb{N}_0$ to Λ. However whenever an order function ρ with respect to definition I.3.2 is given, where $(\Lambda, \prec_\Lambda)$ is isomorphic with $(\mathbb{N}_0, <)$, then also this function can be understood as an order function with respect to the definition given by Høholdt et. al. O'Sullivan's definition of an order function is nearly similar to the one given by Høholdt, van Lint and Pellikaan. We will discuss this at the end of this section.
From [21] we have the following result.

Proposition I.3.3
Let R be a k-algebra with an order function ρ. Then R is an integral domain.

Proof:
Assume that $fg = 0$, where neither f nor g equals 0. From part (O.1) of definition I.3.2 we have $\rho(f) \succ -\infty$, which again by part (O.4) implies $\rho(fg) \succ -\infty$. But $\rho(0) = -\infty$, and we have reached a contradiction. □

This proposition suggests the following definition (from [13])

Definition I.3.4
A k-algebra R on which there is defined an order function is called an order domain over k, or simply an order domain.

The fact that an order domain R is an integral domain of course implies, that one can define the quotient field $\mathrm{Quot}(R)$.

Definition I.3.5
Let R be an order domain over k. The transcendence degree $\mathrm{trdg}(R)$ of R is the maximal number r of elements $f_1, \ldots, f_r \in R$ that are algebraically

independent over k, meaning that there exists no nonzero polynomial P of r variables with coefficients in k, s.t. $P(f_1, \ldots, f_r) = 0$ in R. The transcendence degree of $\mathrm{Quot}(R)$ is defined similarly.

Remark I.3.6
If R is an order domain then obviously $\mathrm{trdg}(R) \leq \mathrm{trdg}(\mathrm{Quot}(R))$.
If $\mathrm{trdg}(\mathrm{Quot}(R)) = 1$ then also $\mathrm{trdg}(R) = 1$.

We now give some simple examples of order domains.

Example I.3.7
The k-algebra $R := k$ is an order domain with an order function given by $\Lambda := \{0\}$ and

$$\rho : \begin{cases} k & \to & \Lambda_{-\infty} \\ 0 & \mapsto & -\infty \\ c & \mapsto & 0 \ \text{for } c \in k \backslash \{0\}. \end{cases}$$

We will call this order domain the trivial order domain .

Example I.3.8
The k-algebra $R := k[X]$ is an order domain with an order function given by $\Lambda := \mathbb{N}_0$ and

$$\rho : \begin{cases} k[X] & \to & \Lambda_{-\infty} \\ 0 & \mapsto & -\infty \\ F(X) & \mapsto & \deg(F(X)), \quad \text{for } F(X) \neq 0. \end{cases} \tag{I.3.2}$$

Example I.3.9
The k-algebra $R := k[X_1, \ldots, X_m]$, $m \geq 2$, is an order domain that possesses a whole range of basically different order functions. In this example we describe the simplest one. Denote by $\boldsymbol{e}_i$, $i = 1, \ldots, m$ the unit vector in $\mathbb{N}_0^m$ with a 1 in position i. Consider weights $w(X_i) = \boldsymbol{e}_i$, $i = 1, \ldots, m$. Extend w to a monomial function $w : \mathcal{M}_m \to \mathbb{N}_0^m$ (recall, that $\mathcal{M}_m$ is the set of monomials in $X_1, \ldots, X_m$). Consider the standard ordering $\prec_{st}$ on $\mathbb{N}_0^m$. Denote $\boldsymbol{X} := (X_1, \ldots, X_m)$. The function $w : \mathcal{M}_m \to \mathbb{N}_0^m$ is extended to an order function on $k[\boldsymbol{X}]$ in the following way. Let $\Lambda := \mathbb{N}_0^m$, and define

$$\rho : \begin{cases} k[\boldsymbol{X}] & \to & \Lambda_{-\infty} \\ 0 & \mapsto & -\infty \\ F(\boldsymbol{X}) & \mapsto & \max_{\prec_{st}}\{w(M) \mid M \in \mathrm{Supp}(F(\boldsymbol{X}))\}, \\ & & \qquad \text{for } F(\boldsymbol{X}) \neq 0 \end{cases}$$

(where $\mathrm{Supp}(F(\boldsymbol{X})$ denotes the set of monomials in $F(\boldsymbol{X})$).

The following results are mainly simple generalizations of results shown in [21].

Proposition I.3.10
Let ρ be an order function on R. We have

(1) *if $\rho(f) = \rho(g)$, then $\rho(fh) = \rho(gh)$ for all $h \in R$*
(2) *if $f \in R$ and $f \neq 0$, then $\rho(1) \preceq_\Lambda \rho(f)$*
(3) $k = \{f \in R \mid \rho(f) \preceq_\Lambda \rho(1)\}$
(4) *if $\rho(f) = \rho(g)$, then there exists a unique nonzero $\lambda \in k$ such that $\rho(f - \lambda g) \prec_\Lambda \rho(g)$.*

Proof:
See [21, Lem. 3.9]. □

Remark I.3.11
Note that (1) in proposition I.3.10 implies

$(1')$ *if $\rho(f) = \rho(g)$ and $\rho(h) = \rho(i)$ then $\rho(fh) = \rho(gi)$.*

Note also that the only case where Λ is a finite set is the case $\Lambda = \{0\}$ corresponding to the k-algebra $R = k$ (the trivial order domain).

Proposition I.3.12
Let R be a k-algebra that possesses an order function $\rho : R \to \Lambda_{-\infty}$. Consider any sub k-algebra $S \subseteq R$. Let Λ_S be the image of S under ρ. The restriction of ρ to S, that is $\rho : S \to \Lambda_S$, is an order function.

Proof:
A simple proof can be found in [30] and [31]. □

Two concepts strongly related to order domains are the concept of a well-behaving basis, and when Λ is ordered isomorphic with $\mathbb{N}$, the concept of a well-behaving sequence. The first appearance of the word well-behaving sequence is in the paper [7] of Feng and Rao. In the previous papers [6] and [8] the authors introduce a related concept of a well-behaving matrix. [1] In this material we will use the definition of a well-behaving sequence given by Høholdt, van Lint and Pellikaan in [20], [21] and [33]. Their definition is a strongly modified version of the one

[1] Feng and Rao's definition of a well-behaving sequence is related to a quotient ring $\mathbb{F}_q[X_1, \ldots, X_m]/I$. Denote

$$n := \#\{\boldsymbol{a} \in \mathbb{F}_q^m \mid P(\boldsymbol{a}) = 0 \,\forall\, P \in I\}.$$

given by Feng et. al[2]. In [13] the definition of Høholdt et. al. of a well-behaving sequence, is generalized to a definition of a well-behaving basis. We will introduce this definition first, and then afterwards explain what a well-behaving sequence is. We will need the following definitions.

Definition I.3.13
Let R be a k-algebra and $\mathcal{B}$ a basis for R as a vector space over k. Let $(\Lambda, \prec_\Lambda)$ be a well-order and assume that a bijective map $\rho : \mathcal{B} \to \Lambda$ is given (note that in this general set-up ρ need not be related to an order function). We index the elements of $\mathcal{B}$ by writing for every $\lambda \in \Lambda$, $f_\lambda := f$ where f is the unique element in $\mathcal{B}$ with $\rho(f) = \lambda$. We call ρ an index map. The indexed basis is denoted by $(f_\lambda \mid \lambda \in \Lambda)$ or simply by $\mathcal{B}_\rho$. The index map ρ together with the well-ordering $\prec_\Lambda$ on Λ induce a well-ordering $\prec_\mathcal{B}$ on $\mathcal{B}$, by the following rule: $f_\lambda \prec_\mathcal{B} f_\gamma$ if and only if $\lambda \prec_\Lambda \gamma$. The in this way well-ordered indexed basis is denoted by $(f_\lambda \mid \lambda \in \Lambda)_{\prec_\Lambda}$ or simply by $\mathcal{B}_{\rho,\prec_\Lambda}$.

Definition I.3.14
Let $\mathcal{B}_{\rho,\prec_\Lambda} = (f_\lambda \mid \lambda \in \Lambda)_{\prec_\Lambda}$ be a well-ordered indexed basis for a k-algebra R. For any $\lambda \in \Lambda$ let $R_\lambda \subseteq R$ be defined by

$$R_\lambda := \mathrm{span}_k\{f_{\lambda'} \mid \lambda' \preceq_\Lambda \lambda\}.$$

The l-function corresponding to $\mathcal{B}_{\rho,\prec_\Lambda}$ is the map

$$l_\Lambda : \left\{ \begin{array}{lcl} \Lambda \times \Lambda & \to & \Lambda \\ (\alpha, \beta) & \mapsto & \min_{\prec_\Lambda}\{\lambda \in \Lambda \mid f_\alpha f_\beta \in R_\lambda\}. \end{array} \right.$$

Definition I.3.15
Let $\mathcal{B}_{\rho,\prec_\Lambda} = (f_\lambda \mid \lambda \in \Lambda)_{\prec_\Lambda}$ be a well-ordered indexed basis according to definition I.3.13. We will say that $\mathcal{B}_{\rho,\prec_\Lambda}$ is well-behaving if and only if $l_\Lambda(\alpha, \beta) \prec_\Lambda l_\Lambda(\gamma, \beta)$ for all $\alpha, \beta, \gamma \in \Lambda$ such that $\alpha \prec_\Lambda \gamma$. A well-behaving basis is a well-behaving well-ordered indexed basis.

In many of the applications that we will present in this thesis the ordering $\prec_\Lambda$ on Λ will be isomorphic with the unique admissible ordering on $\mathbb{N}$ by an isomorphism

$$N : (\Lambda, \prec_\Lambda) \to (\mathbb{N}, <).$$

Their definition involves an evaluation map

$$ev : \mathbb{F}_q[X_1, \ldots, X_m]/I \to \mathbb{F}_q^n$$

(we will define this evaluation map properly in chapter I.11).

[2]As we will see, no map $\varphi : R \to \mathbb{F}_q^n$ is involved in the definition given by Høholdt et. al.'s

Define in this special case $g_i := f_\lambda$ if $N(\lambda) = i$, $i = 1, 2, \ldots$ giving

$$\{f_\lambda \mid \lambda \in \Lambda\} = \{g_i \mid i \in \mathbb{N}\}. \tag{I.3.5}$$

Definition I.3.16
If Λ is ordered isomorphic with the ordering on $\mathbb{N}$ and $(f_\lambda \mid \lambda \in \Lambda)_{\prec_\Lambda}$ is a well-behaving basis, then we will call $(g_1, g_2, \ldots)$ a well-behaving sequence. We define

$$L_i := R_\lambda \quad \textit{if} \quad N(\lambda) = i$$

(that is $L_i = \operatorname{span}_k\{g_1, \ldots, g_i\}$) and we define the map

$$l : \begin{cases} \mathbb{N} \times \mathbb{N} & \to & \mathbb{N} \\ (i, j) & \mapsto & \min_<\{l \in \mathbb{N} \mid g_i g_j \in L_l\}. \end{cases}$$

The maps l_Λ and l are related by

$$l(N(\alpha), N(\beta)) = N(l_\Lambda(\alpha, \beta))$$

for $\alpha, \beta \in \Lambda$.

Now it might at a first glance seem cumbersome to use special notation when an isomorphism $N : (\Lambda, \prec_\Lambda) \to (\mathbb{N}, <)$ exists. Beside the historical reason for doing this (until recently only order functions with well-behaving sequences were considered) we will later learn, that it can actually be an advantage in many situations, especially when we, in the last part of this thesis, construct codes. Whenever it does not cause any confusion, we will take the freedom to write $(f_1, f_2, \ldots)$ instead of $(g_1, g_2, \ldots)$.

The connection between well-behaving bases and order domains is described by the following two propositions.

Proposition I.3.17
Let R be a k-algebra with an order function $\rho \to \Lambda_{-\infty}$, where Λ is ordered by $\prec_\Lambda$. Let $\mathcal{B} \subseteq R \backslash \{0\}$ be a set such that the restriction of ρ to $\mathcal{B}$, that is $\rho : \mathcal{B} \to \Lambda$, is a bijective map. Then $\mathcal{B}$ is a basis for R. If we index the elements of $\mathcal{B}$ by $f_\lambda := f$ if and only if $\rho(f) = \lambda$, then $\mathcal{B}_{\rho,\prec_\Lambda} := (f_\lambda \mid \lambda \in \Lambda)_{\prec_\lambda}$ is well-behaving. We will say that $\mathcal{B}_{\rho,\prec_\Lambda}$ is a well-behaving basis corresponding to the order function ρ.

Proof:
This proof is from [21, Pro, 3.12]. The fact that $\mathcal{B}$ is a basis for R is proved by induction using part (4) of proposition I.3.10. The well-behaving property of the indexed and ordered basis follows immediately from part (O.4) of definition I.3.2. □

Proposition I.3.18
Let $(f_\lambda \mid \lambda \in \Lambda)_{\prec_\Lambda}$ be a well-behaving basis of a k-algebra R. Define $\rho(f) = -\infty$ if $f = 0$, and $\rho(f) = \lambda$ where $\lambda := \min_{\prec_\Lambda}\{\lambda' \mid f \in R_{\lambda'}\}$ for $f \neq 0$. Then $\rho : R \to \Lambda_{-\infty}$ is an order function. And it is the only order function with $\rho(f_\lambda) = \lambda$ for all $\lambda \in \Lambda$. We will say that ρ is the order function corresponding to the well-behaving basis $(f_\lambda \mid \lambda \in \Lambda)_{\prec_\Lambda}$.

Proof:
This proof is a slightly modification of the proof from [21, Pro. 3.14]. Property (O.1), (O.2), (O.3) and (O.5) from definition I.3.2 follows easily. To see that also (O.4) holds, note the following. Let f, g be nonzero elements in R. Write

$$f = \sum_{\lambda \preceq_\Lambda \rho(f)} \alpha_\lambda f_\lambda$$

$$g = \sum_{\lambda \preceq_\Lambda \rho(g)} \beta_\lambda f_\lambda.$$

Note that $\alpha_{\rho(f)}, \beta_{\rho(g)} \neq 0$. We get

$$fg = \sum_{\lambda \preceq_\Lambda l(\rho(f),\rho(g))} \mu_\lambda f_\lambda$$

where $\mu_{l(\rho(f),\rho(g))} \neq 0$. So $\rho(fg) = l(\rho(f), \rho(g))$ and property (O.4) in definition I.3.2 follows. The uniqueness follows from condition (O.3) in definition I.3.2. □

Definition I.3.19
Let $\mathcal{B}_{\rho,\prec_\Lambda} = (f_\lambda \mid \lambda \in \Lambda)_{\prec_\Lambda}$ be a well-behaving basis for a k-algebra R. Then $\mathcal{B} := \{f_\lambda \mid \lambda \in \Lambda\}$ is said to be an order basis for the order function $\rho : R \to \Lambda_{-\infty}$ described in proposition I.3.18. Similar $\mathcal{B}_\rho := (f_\lambda \mid \lambda \in \Lambda)$ is said to be an indexed order basis for the order function $\rho : R \to \Lambda_{-\infty}$ described in proposition I.3.18. In general a subset $\mathcal{B} \subseteq R\backslash\{0\}$ is said to be an order basis if there exists a well-behaving basis $\mathcal{B}_{\rho,\prec_\Lambda} = (f_\lambda \mid \lambda \in \Lambda)_{\prec_\Lambda}$ st. $\mathcal{B} = \{f_\lambda \mid \lambda \in \Lambda\}$.

Remark I.3.20
Let $(f_\lambda \mid \lambda \in \Lambda)_{\prec_\Lambda}$ be a well-behaving basis corresponding to an order function ρ. Replacing for every $\lambda \in \Lambda$ (in turn) f_λ by

$$\sum_{\lambda' \preceq_\Lambda \lambda} \alpha_{\lambda'} f_{\lambda'}$$

where $\alpha_{\lambda'} \in k$, only finitely many $\alpha_{\lambda'}$'s are nonzero and α_λ is nonzero, we get a new well-behaving basis (with respect to ρ). It is clear that every well-behaving basis for R with respect to ρ can be found from $(f_\lambda \mid \lambda \in \Lambda)_{\prec_\Lambda}$ in this way.

Remark I.3.21
Let R be an order domain with an order function $\rho : R \to \Lambda_{-\infty}$. Then R_λ and l_Λ are independent of the choice of order basis. In particular it follows from remark I.3.11 that $l_\Lambda(\alpha, \beta) = \rho(fg)$ where $f, g \in R$ are any elements such that $\rho(f) = \alpha$ and $\rho(g) = \beta$.

We conclude this section with a discussion of O'Sullivan's version of an order function. From [30] and [31] we have the following definition.

Definition I.3.22
Let R be a finitely generated domain[3] *over k. An order function on k is a map $o : R \to \mathbb{N}_0 \cup \{-1\}$ which satisfies the following conditions*

$(O'.1)$ *the set $L_a := \{r \in R$ such that $o(r) \leq a\}$ is an $a+1$ dimensional vector space over k*

$(O'.2)$ *if $f, g, z \in R$ and z is nonzero then $o(f) > o(g)$ implies $o(zf) > o(zg)$.*

If we replace -1 with $-\infty$ then it is clear (as also noted in [30] and [31]) that this definition is more or less equivalent to the one from [20], [21] and [33]. The only difference is that O'Sullivan requires surjectivity on $\mathbb{N}_0$, requires R to be finitely generated and exclude the case $R = k$. Now using the notation from this thesis, and [13], any order function $\rho : R \to \Lambda_{-\infty}$ where $(\Lambda, \prec_\Lambda)$ is isomorphic to $(\mathbb{N}, <)$, can be translated to an order function of O'Sullivan's type. So in the case of Λ being ordered isomorphic with $\mathbb{N}$, the difference in definition is again only a matter of point of view.

[3] That is, a finitely generated integral domain

I.3.2 Weight functions

Remark I.3.21 ensures that we can define a binary operation $\boxplus$ on $\Lambda_{-\infty}$ in the following way.

Definition I.3.23
Let $\rho : R \mapsto \Lambda_{-\infty}$ be an order function. Define $\boxplus$ by the following rule. For any $\alpha, \beta \in \Lambda_{-\infty}$ then $\alpha \boxplus \beta := \gamma$ if and only if there exist $f, g, h \in R$ such that $\rho(f) = \alpha$, $\rho(g) = \beta$, $\rho(h) = \gamma$ and $\rho(fg) = \rho(h)$.

This was also observed in [30] and in [31]. It is clear that $(\Lambda, \boxplus, 0, \prec_\Lambda)$ is a well-ordered semigroup. From [37] we have the following result concerning torsion free semigroups $(\Lambda, \boxplus, 0)$ (recall from definition I.2.3 that $D(\Lambda)$ denotes the corresponding group of differences).

Lemma I.3.24
If $(\Lambda, \boxplus, 0)$ is a torsion free semigroup generated by n elements, then for some $r \leq n$ the group $(D(\Lambda), \boxplus, [0, 0])$ is isomorphic to $(\mathbb{Z}^r, +, \mathbf{0})$, where $+$ is the usual addition.

Remark I.3.25
Let $\rho : R \mapsto \Lambda_{-\infty}$ be any order function. From lemma I.3.24 we conclude that whenever Λ is finitely generated, then $(\Lambda, \boxplus, 0)$ is isomorphic to $(N, +, \mathbf{0})$ where N is a subset of $\mathbb{N}_0^r$ for some r.

In [20], [21] and [33] a weight function is an order function

$$\rho : R \mapsto \Lambda_{-\infty} \subseteq \mathbb{N}_0 \cup \{-\infty\}$$

such that

$$\rho(fg) = \rho(f) + \rho(g) \tag{I.3.8}$$

whenever $f, g \in R$ (here $+$ is the usual addition on $\mathbb{N}_0$).
In our case Λ does not possess a binary operation from the beginning. However with the operation $\boxplus$ on Λ induced by the order function all order functions will satisfy requirement (I.3.8). The operation $\boxplus$ is not really practical in use, as it requires knowledge about the order function to use it. Actually it is specified by the infinite indexed order basis. This is the motivation for the following definition from [13].

Definition I.3.26
Let R be a k-algebra. A weight function is a surjective map $\rho : R \mapsto \Lambda_{-\infty}$ where $(\Lambda, +, 0, \prec_\Lambda)$ is a well-ordered semigroup, such that the conditions $(O.1)$,

$\ldots, (O.5)$ *from definition I.3.2 hold, and such that*

$$(O.6) \quad \rho(fg) = \rho(f) + \rho(g) \text{ whenever } f, g \in R$$

holds. We call $(\Lambda, +, 0, \prec_\Lambda)$ *the value semigroup of* ρ*. And when* $+, 0, \prec_\Lambda$ *is clear from the context, then we take the freedom to talk about the value semigroup* Λ*.*

Clearly condition $(O.4)$ is superfluous. Note that the definition in [20], [21] and [33] covers a special case of definition I.3.26. A thorough treatment of weight functions with value semigroup contained in $\mathbb{N}_0$ can be found in [21].

In all of the examples of weight functions that are considered in this thesis, the well-ordered semigroup will be

$$(\Lambda \subseteq \mathbb{N}_0^r, \mathbf{0}, +, \prec_\Lambda) \tag{I.3.9}$$

(for some r) where $+$ is the usual addition on $\mathbb{N}_0^r$, and $\prec_\Lambda$ is the restriction of a monomial ordering $\prec_{\mathbb{N}_0^r}$ on $\mathbb{N}_0^r$. Rather than specifying the well-ordered semigroup (I.3.9) every time, we will simply speak about a weight function

$$\rho : R \mapsto \Lambda_{-\infty} (\subseteq \mathbb{N}_0^r \cup \{-\infty\}),$$

where Λ is ordered by $\prec_\Lambda$.

Remark I.3.27
One of the main advantages of using definition I.3.2 of an order function, instead of the definitions of an order function given by Høholdt et. al., and by O'Sullivan, is the following. By using definition I.3.2 one can understand any order function as a weight function. And whenever an order function $\rho : R \to \Lambda_{-\infty}$ *is given, where* Λ *is finitely generated, then the isomorphism from lemma I.3.24 describes a weight function* $\rho' : R \to \Lambda'_{-\infty}$*, where* $\Lambda' \subseteq \mathbb{N}_0^r$ *for some* r*. The order funtions* ρ *and* ρ' *are basically the same, but the later is much easier to work with in practice.*

Example I.3.28
The order functions in example I.3.7, I.3.8 and I.3.9 are all weight functions. We will call the weight function from example I.3.7 a trivial weight function. According to proposition I.3.10 the order domain from example I.3.7 is the only order domain over k *that possesses a trivial weight function.*

Consider a weight function $\rho : R \to \Lambda_{-\infty} \subseteq \mathbb{N}_0^r \cup \{-\infty\}$ where $\mathbb{N}_0^r$ is ordered by a monomial ordering $\prec_{\mathbb{N}_0^r}$ that is isomorphic with the admissible ordering

on $\mathbb{N}_0$. Consider a (not necessarily surjective) map $N_0 : \Lambda_{-\infty} \to \mathbb{N}_0 \cup \{-\infty\}$ where $N_0(-\infty) = -\infty$ and $N_0(\alpha) < N_0(\beta)$ whenever $\alpha \prec_{\mathbb{N}_0^r} \beta$, $\alpha, \beta \in \Lambda$. It is easily seen that the composite map

$$N_0(\rho) : R \to N_0(\Lambda_{-\infty}) \subseteq \mathbb{N}_0 \cup \{-\infty\}$$

is an order function. However it will only in very special cases be possible to choose the map N_0 in a way s.t. $N_0(\rho)$ becomes a weight function also. What is required for $N_0(\rho)$ to be a weight function is that N_0 is an isomorphism wrt. $+$.

Example I.3.29
Consider the order function ρ from example I.3.9. There does not exist any map $N_0 : \mathbb{N}_0^2 \to \mathbb{N}_0$ such that

$$N_0(\rho) : k[X, Y] \to N_0(\mathbb{N}_0^2 \cup \{-\infty\})$$

is a weight function.

I.3.3 Permutation equivalent well-behaving bases

In this section we will introduce the concepts of permutation equivalent well-behaving bases and equivalent order functions.

Definition I.3.30
Let a k-algebra R be given. Two well-behaving bases for R

$$(f_\lambda \mid \lambda \in \Lambda)_{\prec_\Lambda}$$

and

$$\left(\tilde{f}_{\tilde{\lambda}} \mid \tilde{\lambda} \in \tilde{\Lambda}\right)_{\prec_{\tilde{\Lambda}}}$$

are said to be permutation equivalent if there exists a map $\alpha : \tilde{\Lambda} \to k\backslash\{0\}$ such that

$$\{f_\lambda \mid \lambda \in \Lambda\} = \{\alpha(\tilde{\lambda})\tilde{f}_{\tilde{\lambda}} \mid \tilde{\lambda} \in \tilde{\Lambda}\}.$$

The most trivial example of permutation equivalent well-behaving bases are obviously the following.

Example I.3.31
If two well-behaving bases for R defines the same order basis, then they are permutation equivalent (the α-map from definition I.3.30 is simply identical 1, in this case).

Remark I.3.32
The permutation equivalence is an equivalence relation on the set of well-behaving bases corresponding to R. Note that every single order function defines (infinitely) many of these equivalence classes.

Definition I.3.33
Let $(f_\lambda \mid \lambda \in \Lambda)_{\prec_\Lambda}$ and $\left(\tilde{f}_{\tilde{\lambda}} \mid \tilde{\lambda} \in \tilde{\Lambda}\right)_{\prec_{\tilde{\Lambda}}}$ be permutation equivalent well-behaving bases (notation as in definition I.3.30). Assume that if

$$\lambda_1, \lambda_2 \in \Lambda \text{ and } \tilde{\lambda}_1, \tilde{\lambda}_2 \in \tilde{\Lambda}$$

are any elements such that

$$f_{\lambda_1} = \alpha(\tilde{\lambda}_1)\tilde{f}_{\tilde{\lambda}_1}, \quad f_{\lambda_2} = \alpha(\tilde{\lambda}_2)\tilde{f}_{\tilde{\lambda}_2}, \quad \text{and } \lambda_1 \prec_\Lambda \lambda_2$$

then necessarily

$$\tilde{\lambda}_1 \prec_{\tilde{\Lambda}} \tilde{\lambda}_2.$$

Then we will say that the well-behaving bases are equivalent.

Remark I.3.34
The equivalence from definition I.3.33 is an equivalence relation on the set of well-behaving bases corresponding to R.

Proposition I.3.35
Let $\rho : R \to \Lambda$ (Λ ordered by $\prec_\Lambda$) and $\tilde{\rho} : R \to \tilde{\Lambda}$ ($\tilde{\Lambda}$ ordered by $\prec_{\tilde{\Lambda}}$) be order functions with corresponding well-behaving bases

$$\mathcal{B}_{\rho,\prec_\Lambda} = (f_\lambda \mid \lambda \in \Lambda)_{\prec_\Lambda} \quad \text{and} \quad \tilde{\mathcal{B}}_{\tilde{\rho},\prec_{\tilde{\Lambda}}} = \left(\tilde{f}_{\tilde{\lambda}} \mid \tilde{\lambda} \in \tilde{\Lambda}\right)_{\prec_{\tilde{\Lambda}}}$$

respectively. If $\mathcal{B}_{\rho,\prec_\Lambda}$ is equivalent to $\tilde{\mathcal{B}}_{\tilde{\rho},\prec_{\tilde{\Lambda}}}$, then for every order basis with respect to ρ there exists an equivalent order basis with respect to $\tilde{\rho}$.

Proof:
Using the notation from definition I.3.30 we have by assumption a map $\alpha : \tilde{\Lambda} \to k\backslash\{0\}$ such that

$$\{f_\lambda \mid \lambda \in \Lambda\} = \{\alpha(\tilde{\lambda})\tilde{f}_{\tilde{\lambda}} \mid \tilde{\lambda} \in \tilde{\Lambda}\}. \tag{I.3.15}$$

By remark I.3.20

$$\left(\alpha(\tilde{\lambda})\tilde{f}_{\tilde{\lambda}} \mid \tilde{\lambda} \in \tilde{\Lambda}\right)_{\prec_{\tilde{\Lambda}}} \tag{I.3.16}$$

is again a well-behaving basis for $\tilde{\rho}$. Now also from remark I.3.20 any well-behaving basis related to ρ say $\mathcal{B}^1_{\rho,\prec_\Lambda}$ can be constructed from $\mathcal{B}_{\rho,\prec_\Lambda}$ by replacing for any $\lambda \in \Lambda$, f_λ by a finite linear combination

$$\sum_{\lambda' \preceq_\Lambda \lambda} \beta_{\lambda'} f_{\lambda'} \quad (\text{where } \beta_{\lambda'} \in k)$$

such that $\rho(f_\lambda) = \rho(\sum_{\lambda' \preceq_\Lambda \lambda} \beta_{\lambda'} f_{\lambda'})$. Now let $\beta_{\tilde{\lambda}'} := \beta_{\lambda'}$ if and only if $f_{\lambda'} = \tilde{\alpha}_{\lambda'} \tilde{f}_{\tilde{\lambda}'}$. Define

$$\tilde{f}^{(1)}_{\tilde{\lambda}} := \sum_{\lambda' \preceq_\Lambda \lambda} \beta_{\tilde{\lambda}'} \alpha_{\tilde{\lambda}'} \tilde{f}_{\tilde{\lambda}'}.$$

By definition I.3.33 we have $\rho(f_{\tilde{\lambda}}) = \rho(\tilde{f}^{(1)}_{\tilde{\lambda}})$. So

$$\tilde{\mathcal{B}}^1_{\tilde{\rho},\prec_{\tilde{\Lambda}}} := \{\tilde{f}^{(1)}_{\tilde{\lambda}} \mid \tilde{\lambda} \in \tilde{\Lambda}\}$$

is a well-behaving basis for $\tilde{\rho}$. Clearly $\mathcal{B}^1_{\rho,\prec_\Lambda}$ is equivalent to $\tilde{\mathcal{B}}^1_{\tilde{\rho},\prec_{\tilde{\Lambda}}}$. □

Definition I.3.36
Let $\rho : R \to \Lambda_{-\infty}$ and $\tilde{\rho} : R \to \tilde{\Lambda}_{-\infty}$ be order functions. If there exists a well-behaving basis for ρ that is equivalent to a well-behaving basis for $\tilde{\rho}$, then we will say that ρ is equivalent to $\tilde{\rho}$.

Remark I.3.37
Proposition I.3.35 ensures that the equivalence from definition I.3.36 is an equivalence relation on the set of order functions on R[4]. We will in general not distinguish two equivalent order functions from each other.

We illustrate the concepts introduced above with a discussion of the set of order functions on $k[X, Y]$ for which the set of monomials in X, Y constitutes an order basis. It may seem in the following, as if we use much to heavy machinery to describe something, that is really not very complicated. The reason for doing this is, that the chosen machinery will be very suitable, when we are to consider more complicated k-algebras later in this material.

[4] A natural question is, if also the permutation equivalence on the set of well-behaving bases of a given order domain R, imposes an equivalence relation on the set of order functions on R. A strategy to construct such an equivalence relation, could be to choose for every order function a unique related well-behaving basis. However it is not at all clear how one should choose these related well-behaving bases in a systematic way.

Example I.3.38
Define the ordering $\prec_i$ on $\mathbb{N}_0 \oplus \mathbb{R}_+$, $i = 1, 2$ to be the graded lexicographic ordering with lexpart given by

$$\begin{array}{ll} (0,1) \prec_{lex} (1,0) & \text{for} \quad i = 1, \\ (1,0) \prec_{lex} (0,1) & \text{for} \quad i = 2. \end{array} \tag{I.3.17}$$

For any $a \in \mathbb{R}_+$ and $i \in \{1, 2\}$ we define a weight function

$$\rho_{a,i} : k[X, Y] \to \mathbb{N}_0 \oplus \mathbb{R}_+ XS \cup \{-\infty\}, \quad i = 1, 2$$

as follows. Order $\mathbb{N}_0^2$ by $\prec_i$ and define

$$\begin{aligned} \rho_{a,i}(X) &= (1, 0), \\ \rho_{a,i}(Y) &= (0, a). \end{aligned}$$

It is clear that the set

$$\mathcal{B} := \{X^\alpha Y^\beta \mid \alpha, \beta \in \mathbb{N}_0\}$$

in each of the above cases constitutes an order basis. The corresponding well-behaving bases are obviously pairwise permutation equivalent. And $\rho_{a,i}$ is equivalent to $\rho_{\tilde{a},\tilde{i}}$ only if $a = \tilde{a}$ and $i = \tilde{i}$.

In the following we will, for each positive number a and $i \in \{1, 2\}$, construct a new order function equivalent to $\rho_{a,i}$. We fix one of the above order functions, say $\rho := \rho_{1,1}$. That is ρ is induced by $\rho(X) = (1, 0)$ and $\rho(Y) = (0, 1)$, and $\mathbb{N}_0^2$ is ordered by $\prec_1$. Next we change the ordering on $\mathbb{N}_0^2$. For each a, i we order $\mathbb{N}_0^2$ by the weighted degree lexicographic ordering $\prec_{a,i}$ with weights

$$w((1, 0)) = 1, \ w((0, 1)) = a$$

and with lexpart as in (I.3.17). Now using this ordering on $\mathbb{N}_0^2$ we get a weight function

$$\rho'_{a,i} : \left\{ \begin{array}{ccl} k[X, Y] & \to & \mathbb{N}_0^2 \cup \{-\infty\} \\ F & \mapsto & \rho(F) \text{ whenever } F \text{ is in } \mathcal{B} \end{array} \right. \tag{I.3.20}$$

that is equivalent to $\rho_{a,i}$.
Next we introduce two order functions that are not captured by the above descriptions but can be described very similar to (I.3.20). In particular these two order functions will possess order bases consisting of the monomials in X, Y.
First order $\mathbb{N}_0^2$ by the (pure) lexicographic ordering where $(0, 1) \prec_{lex} (1, 0)$ and define

$$\rho'_\infty(F) := \rho(F) \ \text{ whenever } F \in \mathcal{B}.$$

Next order $\mathbb{N}_0^2$ *by the (pure) lexicographic ordering where* $(1,0) \prec_{lex} (0,1)$ *and define*

$$\rho_0'(F) := \rho(F) \quad \textit{whenever } F \in \mathcal{B}.$$

Note that ρ_∞' *and* ρ_0' *do not possess well-behaving sequences.*
Altogether we can consider $\rho_{a,i}'$, $a \in \mathbb{R}_+$, $i = 1, 2$, ρ_∞' *and* ρ_0' *as being defined from* ρ *by changing the ordering on* $\mathbb{N}_0^2$. *Geometrically the process of ordering* $\mathbb{N}_0^2$ *can be understood as follows. We first describe the case* $\rho_{a,i}'$. *Let* l_a *be the line through* $(0,0)$ *with slope* $\alpha = a$. *Given two different points* (c_1, d_1) *and* $c_2, d_2)$ *in* $\mathbb{N}_0^2$ *then we can decide which is the smallest (wrt.* $\prec_{a,i}$*) by projecting the points onto* P_1 *and* P_2 *on* l_a. *If they are not projected to the same point then*

$$(c_1, d_1) \prec_{a,i} (c_2, d_2)$$

if and only if

$$\operatorname{dist}((0,0), P_1) < \operatorname{dist}((0,0), P_2)$$

and vice versa. If on the other hand $P_1 = P_2$ *(this can only happen if* $a \in \mathbb{Q}$*) then we use the lexpart of* $\prec_{a,i}$ *on* (c_1, d_1) *and* (c_2, d_2).
Turning our attention to the order functions ρ_∞' *and* ρ_0' *then we can give a simi-*

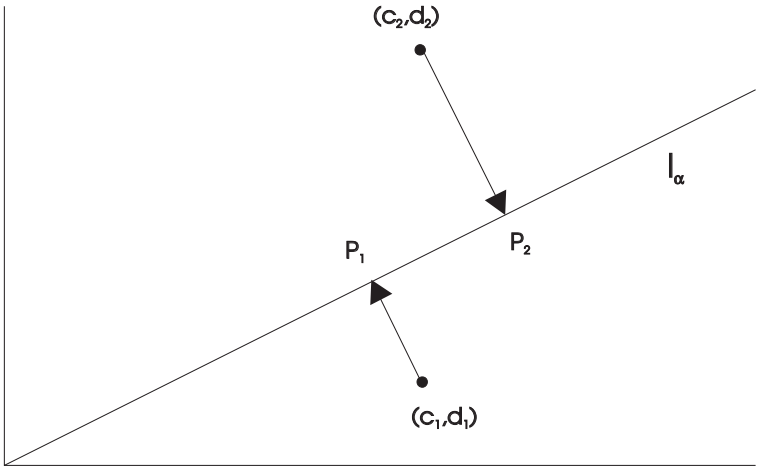

Figure I.3.1: The situation for $\alpha = \dfrac{1}{2}$

lar description where l_∞ *is the vertical line through origo and* l_0 *is the horizontal line through origo. We will take the freedom to say that* l_∞ *has slope* $\alpha = \infty$.

Inspired of example I.3.38 we have the following definition.

Definition I.3.39
Let $\mathcal{B}_\rho = (f_\lambda \mid \lambda \in \Lambda)$ be an indexed basis for a k-algebra R. We will say that an ordering $\prec_\Lambda$ on Λ is a legal ordering wrt. $\mathcal{B}_\rho$ if $\mathcal{B}_{\rho,\prec_\Lambda}$ is a well-behaving basis (in this case of course ρ can be extended to an order function $\rho : R \to \Lambda_{-\infty}$).

Remark I.3.40
In the special case of an indexed basis $\mathcal{B}_\rho = (f_\lambda \mid \lambda \in \Lambda)$ where $\Lambda \subseteq \mathbb{N}_0^2$, we will some times say that a slope $\alpha \in \mathbb{R}_+$ is legal (using the notation from example I.3.38) if there exists an $i \in \{1, 2\}$ such that $\prec_{a,i}$ is legal. We use similar notation in the case of $\alpha = \infty$ or $\alpha = 0$.

Example I.3.41
In example I.3.38 all the considered orderings on $\mathbb{N}_0^2$ were legal wrt. $\mathcal{B}_\rho$. In particular all positive slopes α and also the slopes 0 and $-\infty$ were legal wrt. $\mathcal{B}_\rho$ (giving us the one half of the set of considered order functions namely the ones corresponding to $i = 1$).

In the case of $\Lambda \subseteq \mathbb{N}_0$ there are only one possible ordering namely $<$. This fact is strongly related to the following lemma from [21, Lem. 5.16].

Lemma I.3.42
Let f be a nonzero element of a non trivial order domain R over k with a weight-function[5]

$$\rho : R \to \Lambda_{-\infty} \subseteq \mathbb{N}_0 \cup \{-\infty\}.$$

Then $\dim_k(R/\langle f \rangle) = \rho(f)$ (where $\dim_k(W)$ denotes the dimension of W as a vector space over k).

A natural question is the following. Given a well-behaving basis $\mathcal{B}_{\rho,\prec_\Lambda}$, can every other well-behaving basis permutation equivalent to $\mathcal{B}_{\rho,\prec_\Lambda}$ be found from $\mathcal{B}_{\rho,\prec_\Lambda}$ by considering all possible choices of legal orderings $\prec'_\Lambda$ on $\mathcal{B}_\rho$? It turns out that the answer to this question is in general negative. We illustrate this by an example.

Example I.3.43
Consider the order domain $R := k[X, Y]$ with weight functions ρ_1 and ρ_2 defined as follows

$$\rho_1(X) = (3, 3), \quad \rho_1(Y) = (0, 1)$$

and $\mathbb{N}_0^2$ is ordered by any ordering say $\prec^{(1)}$.

$$\rho_2(X) = (3, 3), \quad \rho_2(Y) = (1, 2)$$

[5] That is, a (non trivial) weight function according to the definition in [21].

and $\mathbb{N}_0^2$ is ordered by any ordering say $\prec^{(2)}$.
Clearly ρ_1 and ρ_2 possess permutation equivalent well-behaving bases but

$$\rho_1(Y^3) \prec^{(1)} \rho_1(X) \text{ and } \rho_2(X) \prec^{(2)} \rho_2(Y^3)$$

no matter how we choose $\prec^{(1)}$ and $\prec^{(2)}$.

Example I.3.44
In example I.3.38 and I.3.43 we treated some order functions on $k[X,Y]$ that had

$$\{X^\alpha Y^\beta \mid \alpha, \beta \in \mathbb{N}_0\} \tag{I.3.28}$$

as an order basis. Two very natural questions arise. First, are there other weight functions than the ones captured by our description in examples I.3.38 and I.3.43 that has (I.3.28) as an order basis? Second, what is the relation between the order functions from example I.3.38 and example I.3.43? In the following we will see that, up to equivalence, the set of weight functions described in example I.3.38 is the full set of weight functions with order basis (I.3.28). That is, the answer to the first question is negative. And the two disjoint sets described in example I.3.43 are contained (by equivalence) in the set from example I.3.38.
Let $\rho : k[X,Y] \to \Lambda$ be any order function with order basis (I.3.28). The ordering of the set $\{\rho(X^\alpha Y^\beta) \mid \alpha, \beta \geq 0\}$ induces a unique monomial ordering on $\mathcal{M}(X,Y)$. Conversely, up to equivalence a monomial ordering $\prec_{\mathcal{M}(X,Y)}$ on $\mathcal{M}(X,Y)$ describes an order function completely. In [31, Ex. 1.3, Ex. 1.4] O'Sullivan is concerned with detecting which monomial orderings on $\mathcal{M}(X_1,\ldots,X_m)$, there defines order functions (of his type) on $k[X_1,\ldots,X_m]$. He notes the following. Describing a monomial ordering on $\mathcal{M}(X_1,\ldots,X_m)$ of course corresponds to describing a monomial ordering on $\mathbb{N}_0^m$. We may extend this ordering to a total ordering $\prec_T$ on $\mathbb{Z}^m$. The reason for making this extension is, that one has a very nice procedure, due to Robbiano, that describes all total orderings on $\mathbb{Z}^m$. Let $\prec_T$ be any total ordering on $\mathbb{Z}^m$. According to [36, §2] there exist $\boldsymbol{r}_1,\ldots,\boldsymbol{r}_m \in \mathbb{R}^m$ such that $\boldsymbol{v} \prec_T \boldsymbol{w}$ if and only if there exists a $k \in [1,\ldots,m]$ such that

$$\begin{cases} \boldsymbol{v}\cdot\boldsymbol{r}_i = \boldsymbol{w}\cdot\boldsymbol{r}_i & \text{for } i<k \\ \boldsymbol{v}\cdot\boldsymbol{r}_k < \boldsymbol{w}\cdot\boldsymbol{r}_k. \end{cases}$$

Obviously, $\boldsymbol{r}_1,\ldots,\boldsymbol{r}_m$ must be linearly independent over $\mathbb{Z}$. In the particular case, where the restriction of $\prec_T$ to $\mathbb{N}_0^m$ is a monomial ordering, further all the coordinates of $\boldsymbol{r}_i$, $i=1,\ldots,m$ must be non negative. We conclude, that the following choices of $\boldsymbol{r}_1$ and $\boldsymbol{r}_2$ covers all possible choices of monomial

orderings on $\mathcal{M}(X,Y)$. Either $\boldsymbol{r}_1 = (1,a)$ and $\boldsymbol{r}_2 = (1,0)$ (with $a > 0$), or $\boldsymbol{r}_1 = (1,a)$ and $\boldsymbol{r}_2 = (0,1)$ (with $a \geq 0$), or $\boldsymbol{r}_1 = (0,1)$ and $\boldsymbol{r}_2 = (1,0)$. The connection to our example I.3.38 is as follows. The unique monomial ordering on (I.3.28) corresponding to $\rho_{a,i}$ (or $\rho'_{a,i}$) is the ordering given by

$$\boldsymbol{r}_1 = (1,a), \quad \boldsymbol{r}_2 = \begin{cases} (1,0) & \text{if} \quad i = 1 \\ (0,1) & \text{if} \quad i = 2. \end{cases}$$

Finally the unique monomial ordering on(I.3.28) corresponding to ρ'_∞ and ρ'_0 are given by

$$\begin{aligned} \rho'_\infty : \quad & \boldsymbol{r}_1 = (1,0) \quad \boldsymbol{r}_2 = (0,1), \\ \rho'_0 : \quad & \boldsymbol{r}_1 = (0,1) \quad \boldsymbol{r}_2 = (1,0). \end{aligned} \tag{I.3.29}$$

We conclude, that up to equivalence, there are no other order functions than the ones from example I.3.38 that has order basis equal to (I.3.28).

I.4
Sub domains of polynomial rings

In this section we will be concerned with subalgebras of polynomial rings. We start with an example.

Example I.4.1
Let $\mathbb{N}_0^m$ be ordered by any monomial ordering $\prec_{\mathbb{N}_0^m}$. Consider the weighted degree lexicographic ordering $\prec_w$ on $\mathcal{M}(X_1, \ldots, X_m)$ (see definition I.2.15) given by weights

$$w(X_1), \ldots, w(X_m) \in \mathbb{N}_0^m$$

that are linearly independent over $\mathbb{Z}$, and by $\prec_{\mathbb{N}_0^m}$. We will not need a lexicographic part of $\prec_w$ in this case. Extend the weights to a monomial function on $\mathcal{M}(X_1, \ldots, X_m)$. Now no two different elements in

$$\{M \mid M \in \mathcal{M}(X_1, \ldots, X_m)\} \tag{I.4.1}$$

are of the same weight. Implying that we can index (I.4.1) by the weights. The nice thing now is that the indexed basis is obviously well-behaving. From proposition I.3.18 we conclude that the function

$$w : \mathcal{M}(X_1, \ldots, X_m) \to \langle w(X_1), \ldots, w(X_m) \rangle$$

can be extended to a weight function

$$\rho : \begin{cases} k[\boldsymbol{X}] & \to & \langle w(X_1), \ldots, w(X_m) \rangle \cup \{-\infty\} \\ F & \mapsto & \max_{\prec_{\mathbb{N}_0^m}} \{w(M) \,|M \in \mathrm{Supp}(F)\} \quad \text{for } F \neq 0 \\ 0 & \mapsto & -\infty. \end{cases}$$

and that (I.4.1) is a corresponding order basis.

We have the following simple but also very general result.

Proposition I.4.2
Let $\Lambda \subseteq \mathbb{N}_0^r$ be any semigroup, and let $\prec_\Lambda$ be any monomial ordering on Λ. Then there exists an order domain R with a weight function $\rho : R \to \Lambda_{-\infty}$.

Proof:
Let Λ be generated by $\Lambda = \langle \boldsymbol{\lambda} \mid \boldsymbol{\lambda} \in S \rangle$. By the very definition of a monomial ordering on a sub semigroup of $\mathbb{N}_0^r$, $\prec_\Lambda$ is the restriction to $\Lambda_{-\infty}$ of a monomial ordering $\prec_{\mathbb{N}_0^r}$ on $\mathbb{N}_0^r \cup \{-\infty\}$. Consider the order domain $k[T_1, \ldots, T_r]$ with weight function

$$\rho : k[T_1, \ldots, T_r] \to \mathbb{N}_0^r \cup \{-\infty\}$$

induced by

$$\begin{aligned} \rho(T_1) &= (1, 0, 0, \ldots, 0) \\ \rho(T_2) &= (0, 1, 0, \ldots, 0) \\ &\vdots \\ \rho(T_r) &= (0, 0, \ldots, 0, 1) \end{aligned}$$

and by the ordering $\prec_{\mathbb{N}_0^r}$ of $\mathbb{N}_0^r$. To see that ρ is a weight function, just consult example I.4.1 above. By proposition I.3.12 the restriction of ρ to the subring $k[\boldsymbol{T}^{\boldsymbol{\lambda}} \mid \boldsymbol{\lambda} \in S]$ is a weight function with value semigroup equal to $\Lambda_{-\infty}$. □

In chapter I.6 we will see how to describe the order domains from the above proof as quotient rings whenever Λ is finitely generated. The next example demonstrates that infinitely generated order domains exist.

Example I.4.3
Order $\mathbb{N}_0^2$ by some monomial ordering $\prec_{\mathbb{N}_0^2}$, and consider the weight function $\rho : k[T_1, T_2] \to \mathbb{N}_0^2 \cup \{-\infty\}$ induced by $\rho(T_1) = (1, 0)$ and $\rho(T_2) = (0, 1)$. Now

$$R := k[T_1T_2, T_1T_2^2, T_1T_2^3, \ldots] \subseteq k[T_1, T_2]$$

is a sub order domain with a weight function with value semigroup

$$\Lambda = \langle (1, a) \mid a \in \mathbb{N} \rangle \cup \{-\infty\}.$$

R is not finitely generated and neither is Λ.

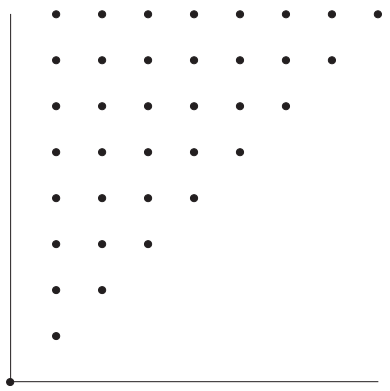

Figure I.4.1: The value semigroup Λ from example I.4.3

I.5
Quotient rings

Almost all the examples of order domains in this thesis are quotient rings. That is, they are of the form $R = k[X_1, \ldots, X_m]/I$ where $I \subseteq k[X_1, \ldots, X_m]$ is an ideal. Up to now I has always been the zero ideal, but we will in the following chapters see several examples where I is not the zero ideal. Before giving these examples, we will in this chapter consider some general properties of quotient rings that are order domains.

Proposition I.5.1
Let $I \subsetneq k[X_1, \ldots, X_m]$ be an ideal such that $R := k[X_1, \ldots, X_m]/I$ is an order domain. Then I is a prime ideal. Let $\rho : R \to \Lambda_{-\infty}$ be an order function on R, where Λ is ordered by $\prec_\Lambda$, and let F be any element in I. Say $F = \sum_{i=1}^{s} a_i X^{\boldsymbol{\alpha}^{(i)}}$, $a_i \in k\backslash\{0\}$, and $\boldsymbol{\alpha}^{(k)} \neq \boldsymbol{\alpha}^{(l)}$, for $k \neq l$. There are two possibilities

(1) $X^{\boldsymbol{\alpha}^{(1)}}, \ldots, X^{\boldsymbol{\alpha}^{(s)}} \in I$

(2) *if an enumeration of the $\boldsymbol{\alpha}^{(i)}$'s is chosen such that*
$\rho(X^{\boldsymbol{\alpha}^{(1)}} + I) \succeq_\lambda \rho(X^{\boldsymbol{\alpha}^{(2)}} + I) \succeq_\Lambda \ldots \succeq_\Lambda \rho(X^{\boldsymbol{\alpha}^{(s)}} + I)$,
then $\rho(X^{\boldsymbol{\alpha}^{(1)}} + I) = \rho(X^{\boldsymbol{\alpha}^{(2)}} + I) \succeq_\Lambda 0$.

Proof:
That I is a prime ideal follows immediately from the fact that an order domain is an integral domain (see proposition I.3.3). Possibility (1) corresponds to the case $\rho(X^{\boldsymbol{\alpha}^{(i)}} + I) = -\infty$, $i = 1, \ldots, s$. Assume that we are not in this case, and let an enumeration as described in (2) be chosen. By assumption, $\rho((X^{\boldsymbol{\alpha}^{(1)}} + I) \succeq_\Lambda 0$. Now if $\rho((X^{\boldsymbol{\alpha}^{(1)}} + I) \succ_\Lambda \rho((X^{\boldsymbol{\alpha}^{(2)}} + I)$ then necessarily $\rho(F + I) = \rho(X^{\boldsymbol{\alpha}^{(1)}} + I) \succeq_\Lambda 0$. This is a contradiction, as $F \in I$ implies $\rho(F+I) = -\infty$. We conclude $\rho(X^{\boldsymbol{\alpha}^{(1)}}+I) = \rho(X^{\boldsymbol{\alpha}^{(2)}}+I) \succeq_\Lambda 0$. □

Proposition I.5.4, at the end of this chapter, states that we wlog. may assume that only possibility (2) from the above proposition occurs. Further it states that

we may assume that the inequality in

$$\rho(X^{\boldsymbol{\alpha}^{(1)}} + I) = \rho(X^{\boldsymbol{\alpha}^{(2)}} + I) \succeq_\Lambda 0$$

is strict. To derive this proposition we will need a few lemmas.

Lemma I.5.2
Let $R = k[X_1, \ldots, X_m]/I$ be an order domain with an order function ρ. Consider a vector $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_m)$ s.t. $\rho(\boldsymbol{X}^{\boldsymbol{\alpha}} + I) = 0$.[1] For any index i, s.t. $\alpha_i \neq 0$, we have $X_i - c_i \in I$ for some $c_i \in k\backslash\{0\}$.

Proof:
We first show that $\rho(X_i + I) = 0$, whenever i is an index s.t. $\alpha_i \neq 0$. Consider a decomposition

$$\boldsymbol{X}^{\boldsymbol{\alpha}} + I = (\boldsymbol{X}^{\boldsymbol{\beta}} + I)(\boldsymbol{X}^{\boldsymbol{\gamma}} + I).$$

On the one hand neither $\rho(\boldsymbol{X}^{\boldsymbol{\beta}} + I)$ nor $\rho(\boldsymbol{X}^{\boldsymbol{\gamma}} + I)$ can be equal to $-\infty$, as this would imply $\boldsymbol{X}^{\boldsymbol{\alpha}} + I = I$. On the other hand neither $\rho(\boldsymbol{X}^{\boldsymbol{\beta}} + I)$ nor $\rho(\boldsymbol{X}^{\boldsymbol{\gamma}} + I)$ can exceed 0. Assume namely that $\rho(\boldsymbol{X}^{\boldsymbol{\beta}} + I) \succ_\Lambda 0$. But then from part (O.4) of definition I.3.2 and from part (3) of proposition I.3.10 we would have $\rho(\boldsymbol{X}^{\boldsymbol{\alpha}} + I) \succ_\Lambda \rho(\boldsymbol{X}^{\boldsymbol{\gamma}} + I) \succeq_\Lambda 0$, a contradiction.
To complete the proof we observe from part (3) of proposition I.3.10 and part (O.1) from definition I.3.2 that $\rho(X_i + I) = 0$ implies $X_i + I = c_i + I$ for some $c_i \in k\backslash\{0\}$. That is $X_i - c_i \in I$. □

Lemma I.5.3
Consider indeterminates $X_1, \ldots, X_r, Y_1, \ldots, Y_s$ and constants $c_1, \ldots, c_r \in k\backslash\{0\}$. Denote $\boldsymbol{X} = (X_1, \ldots, X_r)$, $\boldsymbol{Y} = (Y_1, \ldots, Y_s)$ and $\boldsymbol{c} = (c_1, \ldots, c_r)$. The quotient ring

$$k[\boldsymbol{X}, \boldsymbol{Y}]/\langle X_1 - c_1, \ldots, X_r - c_r, F_1(\boldsymbol{X}, \boldsymbol{Y}), \ldots, F_t(\boldsymbol{X}, \boldsymbol{Y})\rangle$$

is isomorphic with the quotient ring

$$k[\boldsymbol{Y}]/\langle F_1(\boldsymbol{c}, \boldsymbol{Y}), \ldots, F_t(\boldsymbol{c}, \boldsymbol{Y})\rangle.$$

Proof:
Denote $I := \langle F_1(\boldsymbol{c}, \boldsymbol{Y}), \ldots, F_t(\boldsymbol{c}, \boldsymbol{Y})\rangle \subseteq k[\boldsymbol{Y}]$. Consider the homomorphism

$$\varphi : \begin{cases} k[\boldsymbol{X}, \boldsymbol{Y}] & \to \quad k[\boldsymbol{Y}]/I \\ G(\boldsymbol{X}, \boldsymbol{Y}) & \mapsto \quad G(\boldsymbol{c}, \boldsymbol{Y}) + I. \end{cases}$$

[1] The equality for instance holds for $\boldsymbol{\alpha} = \mathbf{0}$

We want to show that

$$\begin{aligned}\ker(\varphi) &= \langle X_1 - c_1, \ldots, X_r - c_r, F_1(\boldsymbol{X}, \boldsymbol{Y}), \ldots, F_t(\boldsymbol{X}, \boldsymbol{Y}) \\ &=: J.\end{aligned} \tag{I.5.2}$$

The rhs. of (I.5.2) is obviously contained in the lhs. We need to show that also the lhs. is contained in the rhs. From the following calculations

$$\begin{aligned} & X_i P(\boldsymbol{X}, \boldsymbol{Y}) + (Q(\boldsymbol{X}, \boldsymbol{Y}) + J) \\ = \; & -(X_i - c_i)((\boldsymbol{X}, \boldsymbol{Y}) + X_i P(\boldsymbol{X}, \boldsymbol{Y}) + (Q(\boldsymbol{X}, \boldsymbol{Y}) + J \\ = \; & c_i P(\boldsymbol{X}, \boldsymbol{Y}) + (Q(\boldsymbol{X}, \boldsymbol{Y}) + J) \end{aligned}$$

we conclude, that $H(\boldsymbol{X}, \boldsymbol{Y}) \in J$ if and only if $H(\boldsymbol{c}, \boldsymbol{Y}) \in J$. In particular $I \subseteq J$. Let $G(\boldsymbol{X}, \boldsymbol{Y}) \in \ker(\varphi)$. We have

$$G(\boldsymbol{c}, \boldsymbol{Y}) \in I \Rightarrow G(\boldsymbol{c}, \boldsymbol{Y}) \in J \Rightarrow G(\boldsymbol{X}, \boldsymbol{Y}) \in J.$$

And (I.5.2) is shown to hold. The lemma now follows from The Fundamental Homomorphism Theorem (see [9, Th. 5.7]). □

Proposition I.5.4
Consider an order domain that can be described as a quotient ring $R = k[X_1, \ldots, X_m]/I$. *Then one may wlog. assume that the following holds. If* $P(\boldsymbol{X}) \in I$ *then there are two monomials* $\boldsymbol{X}^{\boldsymbol{\alpha_1}}, \boldsymbol{X}^{\boldsymbol{\alpha_2}} \in \mathrm{Supp}(P)$ $(\boldsymbol{\alpha_1} \neq \boldsymbol{\alpha_2})$ *s.t.*

$$\rho(\boldsymbol{X}^{\boldsymbol{\alpha_1}} + I) = \rho(\boldsymbol{X}^{\boldsymbol{\alpha_2}} + I) \succ_\Lambda 0,$$

and s.t. $\rho(\boldsymbol{X}^{\boldsymbol{\gamma}} + I) \preceq_\Lambda \rho(\boldsymbol{X}^{\boldsymbol{\alpha_1}} + I)$ *for all* $\boldsymbol{X}^{\boldsymbol{\gamma}} \in \mathrm{Supp}(P)$.

Proof:
The proposition follows by combining proposition I.5.1, lemma I.5.2 and lemma I.5.3. □

I.6
Toric rings

Consider any semigroup $\Lambda \subseteq \mathbb{N}_0^r$ ordered by a monomial ordering $\prec_\Lambda$. In the proof of proposition I.4.2 we showed how one can find a sub order domain R of a polynomial ring $k[X_1, \ldots, X_r]$, such that R possesses a weight function with value semigroup equal to $\Lambda_{-\infty}$. In this section we will be concerned with the special case where Λ is finitely generated. Say $\Lambda = \langle \boldsymbol{\lambda}_1, \ldots, \boldsymbol{\lambda}_m \rangle$. We will describe a method to detect a quotient ring $k[X_1, \ldots, X_m]/I$ which is an order domain with a weight function with value semigroup equal to Λ.

I.6.1 Toric order domains

The ideals we will consider are examples of what is known in the literature as toric ideals. An introduction to toric ideals can be found in [40]. In general a toric ideal is defined from a set $\mathcal{A} = \{\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m\} \subseteq \mathbb{Z}^r$. However we will only be concerned with the toric ideals generated by sets $\{\boldsymbol{\lambda}_1, \ldots, \boldsymbol{\lambda}_m\} \subseteq \mathbb{N}_0^r$. These can be defined as follows.

Definition I.6.1
Consider a set $\{\boldsymbol{\lambda}_1, \ldots, \boldsymbol{\lambda}_m\} \subseteq \mathbb{N}_0^r$. Define a monomial function $w : \mathcal{M}_m \to \mathbb{N}_0^r$ by $w(X_1) = \boldsymbol{\lambda}_1, \ldots, w(X_m) = \boldsymbol{\lambda}_m$. The ideal

$$I := \langle \boldsymbol{X}^{\boldsymbol{u}} - \boldsymbol{X}^{\boldsymbol{v}} \mid w\left(\boldsymbol{X}^{\boldsymbol{u}}\right) = w\left(\boldsymbol{X}^{\boldsymbol{v}}\right) \rangle \subseteq k[X_1, \ldots, X_m]$$

is called the toric ideal related to $\Lambda := \langle \boldsymbol{\lambda}_1, \ldots, \boldsymbol{\lambda}_m \rangle$.

A result similar to the last part of the following proposition can be found in [40]. However our proof differs from the one given there.

Proposition I.6.2
Let a semigroup $\Lambda = \langle \boldsymbol{\lambda}_1, \ldots, \boldsymbol{\lambda}_m \rangle \subseteq \mathbb{N}_0^r$ be given. Let $\prec_{\mathbb{N}_0^r}$ be any monomoial ordering on $\mathbb{N}_0^r$, and let $\prec_\Lambda$ be the restriction of $\prec_{\mathbb{N}_0^r}$ to Λ. Let I be the toric ideal related to Λ. We have

(1) *$k[X_1, \ldots, X_m]/I$ is an order domain with a weight function with value semigroup equal to $\Lambda_{-\infty}$.*

(2) *The following procedure finds generators of I.*
Procedure: Write $\boldsymbol{T} := (T_1, \ldots, T_r)$ and $\boldsymbol{X} = (X_1, \ldots, X_m)$. Consider the lexicographic ordering $\prec_{lex}$ on $k[\boldsymbol{T}, \boldsymbol{X}]$ given by $X_m \prec_{lex} \cdots \prec_{lex} X_1 \prec_{lex} T_r \prec_{lex} \cdots \prec_{lex} T_1$. Expand

$$\{\boldsymbol{T}^{\boldsymbol{\lambda}_1} - X_1, \boldsymbol{T}^{\boldsymbol{\lambda}_2} - X_2, \ldots, \boldsymbol{T}^{\boldsymbol{\lambda}_m} - X_m\}$$

to a Gröbner basis $\mathcal{G}$ wrt. $\prec_{lex}$. Let $\mathcal{G}_X := \mathcal{G} \cap k[\boldsymbol{X}]$, we have $I = \langle \mathcal{G}_X \rangle \subseteq k[\boldsymbol{X}]$.

Proof:
(1): Following the lines of the proof of proposition I.4.2, we consider the order domain $k[\boldsymbol{T}]$ with weight function $\rho : k[\boldsymbol{T}] \to \mathbb{N}_0^r \cup \{-\infty\}$ induced by

$$\begin{aligned} \rho(T_1) &= (1, 0, 0, \ldots, 0) \\ \rho(T_2) &= (0, 1, 0, \ldots, 0) \\ &\vdots \\ \rho(T_r) &= (0, 0, \ldots, 0, 1) \end{aligned}$$

and by the ordering $\prec_{\mathbb{N}_0^r}$ on $\mathbb{N}_0^r$. As noted in the proof of proposition I.4.2 the restriction of ρ to $k[\boldsymbol{T}^{\boldsymbol{\lambda_1}}, \ldots, \boldsymbol{T}^{\boldsymbol{\lambda_m}}]$ is a weight function with value semigroup equal to $\Lambda_{-\infty}$.

Consider the map

$$\varphi : \begin{cases} k[X_1, \ldots, X_m] & \to & k[\boldsymbol{T}^{\boldsymbol{\lambda_1}}, \ldots, \boldsymbol{T}^{\boldsymbol{\lambda_m}}] \\ F(X_1, \ldots, X_m) & \mapsto & F(\boldsymbol{T}^{\boldsymbol{\lambda_1}}, \ldots, \boldsymbol{T}^{\boldsymbol{\lambda_m}}). \end{cases}$$

Clearly φ is a homomorphism. So according to the Fundamental Homomorphism Theorem $\ker(\varphi)$ is an ideal and

$$\Phi : \begin{cases} k[X_1, \ldots, X_m]/\ker(\varphi) & \to & k[\boldsymbol{T}^{\boldsymbol{\lambda_1}}, \ldots, \boldsymbol{T}^{\boldsymbol{\lambda_m}}] \\ F(X_1, \ldots, X_m) + \ker(\varphi) & \mapsto & F(\boldsymbol{T}^{\boldsymbol{\lambda_1}}, \ldots, \boldsymbol{T}^{\boldsymbol{\lambda_m}}). \end{cases}$$

is an isomorphism. Note that $\varphi(a) = a$ for any $a \in k$. We conclude that $R := k[X_1, \ldots, X_m]/\ker(\varphi)$ is an order domain with a weight function

$$\rho_\varphi : \begin{cases} R & \to & \langle \boldsymbol{\lambda_1}, \ldots, \boldsymbol{\lambda_m} \rangle \\ f = F(X_1, \ldots, X_m) + \ker(\varphi) & \mapsto & \rho(\Phi(f)) \\ & = & \rho(F(\boldsymbol{T}^{\boldsymbol{\lambda_1}}, \ldots, \boldsymbol{T}^{\boldsymbol{\lambda_m}})). \end{cases}$$

In the following we will determine $\ker(\varphi)$. Consider the toric ideal

$$\begin{aligned} I &:= \langle \boldsymbol{X^u} - \boldsymbol{X^v} \mid w\left(\boldsymbol{X^u}\right) = w\left(\boldsymbol{X^v}\right)\rangle \\ &= \langle \boldsymbol{X^u} - \boldsymbol{X^v} \mid \varphi(\boldsymbol{X^u}) = \varphi(\boldsymbol{X^v})\rangle \subseteq k[X_1, \ldots, X_m]. \end{aligned}$$

We claim that $\ker(\varphi) = I$. It is obvious that $I \subseteq \ker(\varphi)$. It remains to prove $\ker(\varphi) \subseteq I$. To this end, consider a polynomial

$$F = \sum_{i=1}^{s} k_i \boldsymbol{X^{\alpha_i}} \in \ker(\varphi) \tag{I.6.4}$$

where $k_i \neq 0$ for $i = 1, \ldots, s$. Now

$$\begin{array}{c} \varphi(F) = 0 \\ \Downarrow \\ \displaystyle\sum_{i=1}^{s} k_i \varphi(\boldsymbol{X^{\alpha_i}}) = 0. \end{array}$$

Note that in general, monomials in $X_1, \ldots, X_m$ is mapped to monomials in $T_1, \ldots, T_r$ under φ. And recall that the monomials in $k[\boldsymbol{T}]$ are linearly independent. From these facts we conclude that there exist indices, say $1 \leq j_1 < \cdots < j_u < s$ such that

$$\varphi(\boldsymbol{X^{\alpha_{j_1}}}) = \cdots = \varphi(\boldsymbol{X^{\alpha_{j_u}}}) = \varphi(\boldsymbol{X^{\alpha_s}})$$

and such that $k_s + (k_{j_1} + \cdots + k_{j_u}) = 0$. Now replace k_s with

$$(-k_{j_1} - \cdots - k_{j_u})$$

in (I.6.4) to get

$$F = \sum_{\substack{i \in \{i, \ldots, s-1\} \\ i \neq j_1, \ldots, j_u}} k_i \boldsymbol{X^{\alpha_i}} + \sum_{v=1}^{u} k_{j_v}(\boldsymbol{X^{\alpha_{j_v}}} - \boldsymbol{X^{\alpha_s}}).$$

The last sum clearly is contained in I, and the first sum is mapped to zero under φ. Observe that the first sum contains fewer monomials than F does. We now repeat the above procedure on the first sum. Continuing this way, we will finaly end up with a left sum equal to 0. So F is a sum of elements in I. We have shown $\ker(\varphi) \subseteq I$. All together $I = \ker(\varphi)$.

(2): Consider

$$\tilde{I} := \langle X_1 - \boldsymbol{T}^{\boldsymbol{\lambda_1}}, \ldots, X_m - \boldsymbol{T}^{\boldsymbol{\lambda_m}} \rangle \subseteq k[\boldsymbol{T}, \boldsymbol{X}].$$

We claim that $I = \tilde{I} \cap k[\boldsymbol{X}]$, that is I is an elimination ideal. To prove this consider the map

$$\psi : \begin{cases} k[T_1, .., T_r, X_1, .., X_m] & \to k[T_1, .., T_r] \\ F(T_1, .., T_r, X_1, .., X_m) & \mapsto F(T_1, .., T_r, \varphi(X_1), .., \varphi(X_m)). \end{cases}$$

Now clearly $I = \ker(\psi) \cap k[\boldsymbol{X}]$, so to prove our claim it suffices to show that $\ker(\psi) = \tilde{I}$. The inclusion $\tilde{I} \subseteq \ker(\psi)$ is obvious. To see that $\ker(\psi) \subseteq \tilde{I}$, note that any polynomial $F(\boldsymbol{T}, \boldsymbol{X}) \in k[\boldsymbol{T}, \boldsymbol{X}]$ can be written

$$F(\boldsymbol{T}, \boldsymbol{X}) = G(\boldsymbol{T}) + \sum_{i=1}^{m} (X_i - \boldsymbol{T}^{\boldsymbol{\lambda_i}}) H_i(\boldsymbol{T}, \boldsymbol{X}). \tag{I.6.8}$$

Now if $F(\boldsymbol{T}, \boldsymbol{X}) \in \ker(\psi)$ then by using ψ on the rhs. of (I.6.8) we see that $\psi(G(\boldsymbol{T})) = 0$. But $\psi(G(\boldsymbol{T})) = G(\boldsymbol{T})$, that is

$$F(\boldsymbol{T}, \boldsymbol{X}) = \sum_{i=1}^{m} (X_i - \boldsymbol{T}^{\boldsymbol{\lambda_i}}) H_i(\boldsymbol{T}, \boldsymbol{X}) \in I. \tag{I.6.9}$$

Finally, the procedure described in (2) is just a well-known procedure from elimination theory to find a Gröbner basis for an elimination ideal (see [4, Ch. 3 §3 Th. 2]). □

Proposition I.6.2 suggests the following definition.

Definition I.6.3
Let $I \subseteq k[X_1, \ldots, X_m]$ be a toric ideal according to definition I.6.1. We say that $k[X_1, \ldots, X_m]/I$ is a toric order domain.

Example I.6.4
Consider the semigroup

$$\Lambda := \langle (0,2), (0,3), (1,1), (2,0) \rangle \subseteq \mathbb{N}_0^2.$$

and consider any monomial ordering $\prec_{\mathbb{N}_0^2}$ on $\mathbb{N}_0^2$. If we expand $\{T_2^2 - X_1, T_2^3 - X_2, T_1T_2 - X_3, T_1^2 - X_4\}$ to a Gröbner basis as described in proposition I.6.2

we get

$$\begin{aligned}\mathcal{G} \;=\; \{&T_2^2 - X_1, T_2^3 - X_2, T_1T_2 - X_3, T_1^2 - X_4, T_2X_1 - X_2,\\ &T_1X_1 - T_2X_3, T_2X_2 - X_1^2, T_1X_2 - X_1X_3, X_1^3 - X_2^2,\\ &T_1X_3 - T_2X_4, X_1X_4 - X_3^2, T_2X_3^2 - X_2X_4, X_1^2X_3^2 - X_2^2X_4,\\ &X_1X_3^4 - X_2^2X_4^2, X_2^2X_4^3 - X_3^6\}.\end{aligned}$$

Now

$$\begin{aligned}I \;=\; \langle &X_1^3 - X_2^2, X_1X_4 - X_3^2, X_1^2X_3^2 - X_2^2X_4,\\ &X_1X_3^4 - X_2^2X_4^2, X_2^2X_4^3 - X_3^6\rangle\end{aligned}$$

and $k[\boldsymbol{X}]/I$ is an order domain with a weight function $\rho : k[\boldsymbol{X}]/I \longrightarrow \Lambda_{-\infty}$ induced by $\rho(X_1 + I) = (0, 2)$, $\rho(X_2 + I) = (0, 3)$, $\rho(X_3 + I) = (1, 1)$ and $\rho(X_4 + I) = (2, 0)$ and by the restriction of $\prec_{\mathbb{N}_0^2}$ to Λ.

The next example shows the necessity of the procedure from proposition I.6.2.

Example I.6.5
Consider the semigroup $\Lambda = \langle 7, 9, 13\rangle$. Using the procedure from proposition I.6.2 one can construct an order domain $R = k[X_1, X_2, X_3]/I$ with a weight function $\rho : R \to \Lambda_{-\infty}$ induced by $\rho(X_1 + I) = 7$, $\rho(X_2 + I) = 9$, $\rho(X_3 + I) = 13$. In this example we will see what happens if one tries to construct the toric ideal I without using the procedure from proposition I.6.2. The polynomials

$$F_1 := X_2^7 - X_1^9 \quad F_2 := X_3^7 - X_1^{13} \quad F_3 := X_3^9 - X_2^{13}$$

are obviously contained in the toric ideal I. So we could hope that they actually generates I. To investigate if this is the case we expand $\{F_1, F_2, F_3\}$ to a Gröbner basis. We do this with respect to the weighted degree lexicographic ordering given by weights $w(X_1) = 7$, $w(X_2) = 9$, $w(X_3) = 13$ and with lexicographic part given by $X_1 \prec_{lex} X_2 \prec_{lex} X_3$. After a following reduction we get a Gröbner basis $\{F_1', F_2', F_3', F_4', F_5'\}$ where

$$\begin{aligned}F_1' := F_1 \quad F_2' := F_2 \quad F_3' := X_3X_2^4 - X_1^7\\ F_4' := X_3X_1^2 - X_2^3 \quad F_5' := X_3^6X_2^3 - X_1^{15}.\end{aligned}$$

The corresponding footprint is

$$\begin{aligned}\{X_1^\alpha X_2^\beta \mid \beta < 7\} \cup \{X_1^\alpha X_2^\beta X_3^\gamma \mid 0 < \gamma < 6,\ \alpha < 2,\ \beta < 4\}\\ \cup \{X_1^\alpha X_2^\beta X_3^6 \mid \alpha < 2,\ \beta < 3\}.\end{aligned}$$

Now $w\left(X_1^3X_2^2\right) = w\left(X_3^3\right) = 39$ *and both* $X_1^3X_2^2$ *and* X_3^3 *are elements in the footprint, that is*

$$X_3^3 - X_1^3X_2^2 \notin \langle F_1, F_2, F_3\rangle.$$

To construct the desired ideal we will have at least to add $F_6' := X_3^3 - X_2^2X_1^3$ *as a generator. Expanding next* $\{F_1', \ldots, F_6'\}$ *to a Gröbner basis we get after reduction a Gröbner basis* $\{F_1'', F_2'', \ldots, F_5''\}$ *where*

$$F_1'' := X_2^7 - X_1^9,\ \ F_2'' := X_3X_2^4 - X_1^7,\ \ F_3'' := X_3X_1^2 - X_2^3$$
$$F_4'' := X_3^3 - X_2^2X_1^3,\ \ F_5'' := X_3^2X_2 - X_1^5.$$

The footprint of $\langle F_1'', \ldots, F_5''\rangle$ *is given by*

$$\{X_1^\alpha X_2^\beta \mid \beta < 7\} \cup \{X_1^\alpha X_2^\beta X_3 \mid \alpha < 2,\ \beta < 4\} \cup \{X_1^\alpha X_3^2 \mid \alpha < 2\}.$$

Now, no two different monomials in this footprint has the same weight. From this fact it is an easy task to show that actually $\langle F_1'', \ldots, F_5''\rangle = I$*. That is we have found the desired toric ideal.*

Example I.6.6
For $n \geq 2$ *consider the* $2 \times n$ *matrix* $[X]_{ij}$ *of variables* X_{ij}*. As usual we write* $\boldsymbol{X} := (X_{11}, X_{12}, \ldots, X_{2n})$*. Denote by* $\mathcal{F}$ *the set of all* 2×2 *minors in* $(X)_{ij}$*, and let* I *be the ideal in* $k[\boldsymbol{X}]$ *generated by* $\mathcal{F}$*. We will show that* I *is a toric ideal, and it will follow from proposition I.6.2 that* $k[\boldsymbol{X}]/I$ *is an order domain. Let weight vectors,* $w(X_{ij}) \in \mathbb{N}_0^{n+1}\backslash\{\mathbf{0}\}$*, be given as in figure I.6.1 and let* $\mathbb{N}_0^{n+1}$ *be ordered by any monomial ordering.*

$$\begin{bmatrix} I_{2\times 2} & I_{2\times 2} & I_{2\times 2} & \cdots & I_{2\times 2} \\ & J_{1\times 2} & & & \\ & & J_{1\times 2} & & \\ & & & \ddots & \\ & & & & J_{1\times 2} \end{bmatrix}$$

Figure I.6.1: $I_{2\times 2}$ denotes the 2 times 2 identity matix, whereas $J_{1\times 2}$ denotes the 1 times 2 matrix with a 1 in both entries. The first two columns correspond to $w(X_{11})$, $w(X_{21})$. The next two columns to $w(X_{12})$, $w(X_{22})$ and so on.

Every 2×2 *minor, of course contains, precisely two terms, and it is seen from figure I.6.1 that these two terms are of the same weight. It is also seen, that if*

two monomials are of the same weight, then either they are equal or there exists a minor $M_1 - M_2$, such that M_1 divides the one of them and M_2 divides the other. We have shown that I is a toric ideal.

I.6.2 The variety of a toric ideal

We adopt the definition of a variety from [4].

Definition I.6.7
Given a field k and an ideal $I \subseteq k[X_1, \ldots, X_m]$ then the variety of I is

$$\mathcal{V}_k(I) := \{\boldsymbol{a} \in k^m \mid P(\boldsymbol{a}) = 0 \; \forall \; P \in I\}.$$

We note that some authors refer to the set in definition I.6.7 as an algebraic set, and use the word variety in another meaning than the one from the above definition.

In the following we will be concerned with the size of the variety $\mathcal{V}_{\mathbb{F}_q}(I)$ of a toric ideal. The reason for this interest will become clear in chapter I.11, where we describe how one, from an order domain $k[\boldsymbol{X}]/I$, can easily construct codes over $\mathbb{F}_q$ of length up to $\#\mathcal{V}_{\mathbb{F}_q}(I)$.

We first investigate the special case $\Lambda \subseteq \mathbb{N}_0$, that is the case where $\boldsymbol{T} = T_1$. In this special case it turns out that

$$\#\mathcal{V}_{\mathbb{F}_q}(I) = q \tag{I.6.11}$$

for any toric ideal. This result can be derived using arguments from algebraic function field theory. However we will prefer to show the result using simpler machinery. Our proof only relies on simple combinatorics and some results from elimination theory, that we are going to introduce anyway. The following result known as The Extension Theorem, will be essential for the discussions below. For a proof see [4].

Theorem I.6.8
Consider an ideal $I = \langle F_1, \ldots, F_s \rangle \subseteq k[Z_1, \ldots, Z_m]$ where k is algebraically closed. Denote the first elimination ideal by $I_1 := I \cap k[Z_2, \ldots, Z_m]$. For each i, $1 \leq i \leq s$, write F_i on the form

$$F_i = G_i(Z_2, \ldots, Z_m) Z_1^{N_i} + R(Z_1, \ldots, Z_m), \tag{I.6.12}$$

where $\deg_{Z_1}(R) < N_i$, $N_i \geq 0$ *and* $G_i \in k[Z_2, \ldots, Z_m]$ *is nonzero. Suppose that a solution* $(a_2, \ldots, a_m) \in \mathcal{V}_k(I_1)$ *is given. If* $(a_2, \ldots, a_m) \notin \mathcal{V}_k(G_1, \ldots, G_s)$ *then there exists* $a_1 \in k$ *such that* $(a_1, a_2, \ldots, a_m) \in \mathcal{V}_k(I)$.

We will also need the following obvious lemma.

Lemma I.6.9
With the notation from proposition I.6.8 define the map

$$\pi : \left\{ \begin{array}{ccc} \mathcal{V}_k(I) & \to & \mathcal{V}_k(I_1) \\ (a_1, \ldots, a_m) & \mapsto & (a_2, \ldots, a_m). \end{array} \right. \tag{I.6.13}$$

Then $\pi(\mathcal{V}_k(I)) \subseteq \mathcal{V}_k(I_1)$.

We now have the machinery to prove (I.6.11).

Proposition I.6.10
Let $a_1, \ldots, a_m \in \mathbb{N}$ *be given with* $\gcd(a_1, \ldots, a_m) = 1$. *Let* I_1 *be the corresponding toric ideal, that is define*

$$I := \langle X_1 - T^{a_1}, X_2 - T^{a_2}, \ldots, X_m - T^{a_m} \rangle \subseteq \mathbb{F}_q[T, X_1, \ldots, X_m],$$

and

$$I_1 := I \cap \mathbb{F}_q[X_1, \ldots, X_m].$$

We have $\#\mathcal{V}_{\mathbb{F}_q}(I_1) = q$.

Proof:
The proof consists of three parts. In the first part we show that

$$\pi(\mathcal{V}_{\bar{\mathbb{F}}_q}(I)) = \mathcal{V}_{\bar{\mathbb{F}}_q}(I_1). \tag{I.6.15}$$

In the second part we show that if $(t, t^{a_1}, t^{a_2}, \ldots, t^{a_m}) \in \mathcal{V}_{\bar{\mathbb{F}}_q}(I)$ with $t^{a_1}, t^{a_2}, \ldots, t^{a_m} \in \mathbb{F}_q$ then also $t \in \mathbb{F}_q$. Part one and two together establish

$$\pi(\mathcal{V}_{\mathbb{F}_q}(I)) = \mathcal{V}_{\mathbb{F}_q}(I_1). \tag{I.6.16}$$

Finally in the third part we show that there does not exist $t \neq t'$ such that

$$(t^{a_1}, t^{a_2}, \ldots, t^{a_m}) = (t'^{a_1}, t'^{a_2}, \ldots, t'^{a_m}).$$

Comparing with (I.6.16) we get $\#\mathcal{V}_{\mathbb{F}_q}(I) = \#\mathcal{V}_{\mathbb{F}_q}(I_1)$. The proposition now follows from the fact, that $\#\pi(\mathcal{V}_{\mathbb{F}_q}(I)) = q$.

Part 1:
Using the notation from theorem I.6.8 we have $G_1 = G_2 = \ldots = G_m = 1$. So $\mathcal{V}_{\mathbb{F}_q}(\langle G_1, \ldots, G_m \rangle) = \emptyset$. From theorem I.6.8 we conclude that (I.6.15) is satisfied.

Part 2:
Assume $(t, t^{a_1}, \ldots, t^{a_m}) \in \mathcal{V}_{\mathbb{F}_q}(I)$ and that $t^{a_1}, \ldots, t^{a_m} \in \mathbb{F}_q$. From the assumption that $\gcd(a_1, \ldots, a_m) = 1$ we have that there exist $k_1, \ldots, k_m \in \mathbb{Z}$ such that

$$a_1 k_1 + a_2 k_2 + \cdots a_m k_m = 1.$$

So we can write

$$\begin{aligned} t &= t^{a_1 k_1 + a_2 k_2 + \cdots + a_m k_m} \\ &= \left(t^{a_1}\right)^{k_1} \left(t^{a_2}\right)^{k_2} \cdots \left(t^{a_m}\right)^{k_m} \in \mathbb{F}_q. \end{aligned}$$

Part 3:
Assume

$$\left(t^{a_1}, t^{a_2}, \ldots, t^{a_m}\right) = \left(t'^{a_1}, t'^{a_2}, \ldots, t'^{a_m}\right).$$

From the proof of part 2 we have

$$t = \left(t^{a_1}\right)^{k_1} \left(t^{a_2}\right)^{k_2} \cdots \left(t^{a_m}\right)^{k_m}$$

and

$$t' = \left(t'^{a_1}\right)^{k_1} \left(t'^{a_2}\right)^{k_2} \cdots \left(t'^{a_m}\right)^{k_m}.$$

It follows that $t = t'$. □

The following examples show that a result equivalent to proposition I.6.10 does not hold when $\Lambda \subseteq \mathbb{N}_0^r$, $\Lambda \not\subseteq \mathbb{N}_0^{r-1}$ with $r > 1$.

Example I.6.11
Consider the ideal $I \subseteq \mathbb{F}_q[X_{11}, X_{21}, X_{12}, X_{22}, X_{13}, X_{23}]$ generated by the 2×2 minors of the 2×3 matrix $[X_{ij}]$ of indeterminates. Order $\mathbb{N}_0^4$ by any monomial ordering. In example I.6.6 we saw that I is a toric ideal, and that $\mathbb{F}_q[X_{11}, \ldots, X_{23}]/I$ is an order domain with a weight function

$$\rho : \mathbb{F}_q[X_{11}, \ldots, X_{23}]/I \to \Lambda_{-\infty}$$

induced by

$$\begin{aligned} &\rho(X_{11}) = (1,0,0,0), \quad \rho(X_{21}) = (0,1,0,0) \\ &\rho(X_{12}) = (1,0,1,0), \quad \rho(X_{22}) = (0,1,1,0) \\ &\rho(X_{13}) = (1,0,0,1), \quad \rho(X_{23}) = (0,1,0,1). \end{aligned} \tag{I.6.17}$$

One might, from proposition I.6.10, and from the fact that $\Lambda \subseteq \mathbb{N}_0^4$ but $\Lambda \not\subseteq \mathbb{N}_0^3$, get the idea, that the variety $\mathcal{V}_{\mathbb{F}_q}(I)$ contains precisely q^4 points. This is however not the case. Assume for instance that $q = 2$, by inspection we find $\#\mathcal{V}_{\mathbb{F}_2}(I) = 22 > 2^4 = 16$.

The following example explains why a result equivalent to proposition I.6.10 does not hold when $\Lambda \subseteq \mathbb{N}_0^r$, $\Lambda \not\subseteq \mathbb{N}_0^{r-1}$ with $r > 1$.

Example I.6.12
Let $\Lambda \subset \mathbb{N}_0^3$ be generated as a semigroup by

$$\Lambda := \langle (1,0,0), (1,0,1), (0,1,0), (0,1,1) \rangle.$$

Now the corresponding toric ideal $I \subseteq \mathbb{F}_q[X_1, \ldots, X_4]$ is found in the following way. Expand

$$\mathcal{H} := \{X_1 - T_1, X_2 - T_1T_3, X_3 - T_2, X_4 - T_2T_3\}$$

to a minimal Gröbner basis $\mathcal{G}$ with respect to the lexicographic ordering given by

$$X_4 \prec_{lex} X_3 \prec_{lex} X_2 \prec_{lex} X_1 \prec_{lex} T_3 \prec_{lex} T_2 \prec_{lex} T_1.$$

We get

$$\mathcal{G} = \{T_1 - X_1, T_2 - X_3, T_3X_3 - X_4, T_3X_1 - X_2, X_1X_4 - X_2X_3\}.$$

Consider the elimination ideals

$$\begin{aligned} I_0 &:= \langle \mathcal{H} \rangle \\ I_1 &:= \langle \mathcal{H} \rangle \cap \mathbb{F}_q[T_2, T_3, X_1, \ldots, X_4] \\ I_2 &:= \langle \mathcal{H} \rangle \cap \mathbb{F}_q[T_3, X_1, \ldots, X_4] \\ I_3 &:= \langle \mathcal{H} \rangle \cap \mathbb{F}_q[X_1, \ldots, X_4]. \end{aligned}$$

We know from proposition I.6.2 that $R := \mathbb{F}_q[X_1, \ldots, X_4]/I_3$ is an order domain with a weight function $\rho : R \to \Lambda_{-\infty}$. Actually this is again a special case of example I.6.6.

Let π_1, π_2 π_3 and π^* be the projections given by

$$\pi_1 : \begin{cases} \mathcal{V}_{\bar{\mathbb{F}}_q}(I_0) & \to & \bar{\mathbb{F}}_q^6 \\ (t_1, t_2, t_3, x_1, \ldots, x_4) & \mapsto & (t_2, t_3, x_1, \ldots, x_4) \end{cases}$$

$$\pi_2 : \begin{cases} \mathcal{V}_{\bar{\mathbb{F}}_q}(I_1) & \to & \bar{\mathbb{F}}_q^5 \\ (t_2, t_3, x_1, \ldots, x_4) & \mapsto & (t_3, x_1, \ldots, x_4) \end{cases}$$

$$\pi_3 : \begin{cases} \mathcal{V}_{\bar{\mathbb{F}}_q}(I_2) & \to & \bar{\mathbb{F}}_q^4 \\ (t_3, x_1, \ldots, x_4) & \mapsto & (x_1, \ldots, x_4) \end{cases}$$

$$\pi^* : \begin{cases} \mathcal{V}_{\bar{\mathbb{F}}_q}(I_0) & \to & \bar{\mathbb{F}}_q^4 \\ (\boldsymbol{t}, \boldsymbol{x}) & \mapsto & (\boldsymbol{x}). \end{cases}$$

In the following we will investigate the connection between $\pi^*(\mathcal{V}_{\mathbb{F}_q}(I_0))$ and $\mathcal{V}_{\mathbb{F}_q}(I_3)$.
From lemma I.6.9 we know that

$$\pi^*(\mathcal{V}_{\bar{\mathbb{F}}_q}(I_0)) \subseteq \mathcal{V}_{\bar{\mathbb{F}}_q}(I_3). \tag{I.6.20}$$

Our first concern will be to investigate if two different points in $\mathcal{V}_{\mathbb{F}_q}(I_0)$ can be projected to the same point under π^*. That this actually can be the case is seen by the following example. Let namely $q = 2$. Now both $(\boldsymbol{t}, \boldsymbol{x}) = (0, \ldots, 0)$ and $(\boldsymbol{t}', \boldsymbol{x}') = (0, 0, 1, 0, 0, 0, 0)$ are contained in $\mathcal{V}_{\mathbb{F}_q}(I_0)$ but $\pi^*(\boldsymbol{t}, \boldsymbol{x}) = \pi^*(\boldsymbol{t}', \boldsymbol{x}')$. In this particular example it is further easily shown that $\pi^*(\mathcal{V}_{\bar{\mathbb{F}}_2}(I_0)) \cap \mathbb{F}_2^4 = \pi^*(\mathcal{V}_{\mathbb{F}_2}(I_0))$. We note that we can not expect that a similar result holds in general. By inspection we find that

$$\#\pi^*(\mathcal{V}_{\bar{\mathbb{F}}_2}(I_0)) \cap \mathbb{F}_2^4 = \#\pi^*(\mathcal{V}_{\mathbb{F}_2}(I_0)) = 7.$$

Next we will show that the inclusion in (I.6.20) can be proper. From proposition I.6.8 we know that $\pi_1(\mathcal{V}_{\bar{\mathbb{F}}_q}(I_0)) = \mathcal{V}_{\bar{\mathbb{F}}_q}(I_1)$, because the coefficient to the highest power of T_1 in the polynomial $T_1 - X_1 \in I_0$, viewed as a polynomial in T_1, is equal to 1, a constant. In the same way we see that $\pi_2(\mathcal{V}_{\bar{\mathbb{F}}_q}(I_1)) = \mathcal{V}_{\bar{\mathbb{F}}_q}(I_2)$. But under the final mapping π_3 completely different things happen. Now

$$I_2 = \langle T_3X_3 - X_4, T_3X_1 - X_2, X_1X_4 - X_2X_3 \rangle.$$

We investigate the coefficients to the highest power of T_3 namely X_3, X_1 , $(X_1X_4 - X_2X_3)$. Let us again consider the situation where $\mathbb{F}_q = \mathbb{F}_2$. We have the following four elements in $\mathcal{V}_{\mathbb{F}_2}(\langle X_3, X_1, X_1X_4 - X_2X_3 \rangle)$, namely $(0, 0, 0, 0)$, $(0, 1, 0, 0)$, $(0, 1, 0, 1)$ and $(0, 0, 0, 1)$. The extension theorem tells us that these four points are candidates for points lying in $\mathcal{V}_{\mathbb{F}_2}(I_3)$ but not in $\pi^*(\mathcal{V}_{\bar{\mathbb{F}}_2}(I_2))$. Inspection shows that the last three points are not contained in

$\pi^*(\mathcal{V}_{\bar{\mathbb{F}}_2}(I_2))$.
All together we have located the 10 *points that constitute* $\mathcal{V}_{\mathbb{F}_2}(I_3)$.

I.7
Pellikaan's factor ring theorem

In this chapter we will introduce a very important theorem by Pellikaan. Using this theorem one can recognize a very large class of quotient rings as order domains.

I.7.1 The theorem

In example I.4.1 we considered the weighted degree lexicographic ordering on $\mathcal{M}(X_1, \ldots, X_m)$, given by weights

$$w(X_1), \ldots, w(X_m) \in \mathbb{N}_0^m$$

that are linearly independent over $\mathbb{Z}$, and by a monomial ordering $\prec_{\mathbb{N}_0^m}$ on $\mathbb{N}_0^m$. We extended the weights to a monomial function w on $\mathcal{M}(X_1, \ldots, X_m)$. And as a first step in constructing a weight function on $k[X_1, \ldots, X_m]$, we considered the basis of $k[X_1, \ldots, X_m]$ consisting of the monomials. We noted, that one can index the elements $\boldsymbol{X}^{\boldsymbol{\alpha}} \in \mathcal{M}(X_1, \ldots, X_m)$ by their corresponding values $w\left(\boldsymbol{X}^{\boldsymbol{\alpha}}\right)$.

Consider next the following more complicated situation. Let $r < m$, and assume that $\mathbb{N}_0^r$ is ordered by the monomial ordering $\prec_{\mathbb{N}_0^r}$. Consider a weighted degree lexicographic ordering on $\mathcal{M}(X_1, \ldots, X_m)$ given by weights

$$w(X_1), \ldots, w(X_m) \in \mathbb{N}_0^r$$

by $\prec_{\mathbb{N}_0^r}$ and by some lexicographic ordering $\prec_{lex}$ of $\mathcal{M}(X_1, \ldots, X_m)$. Now we can not, as before, index the monomials in $\mathcal{M}(X_1, \ldots, X_m)$ by their weights, as there will be pairs of monomials $M_1 \neq M_2$ with $w(M_1) = w(M_2)$. The idea in this chapter is to find an ideal $I \subseteq k[X_1, \ldots, X_m]$ such that no two different elements in the footprint $\Delta(I)$ corresponding to $\prec_w$ are of the same weight. This will enable us to index the basis

$$\{M + I \mid M \in \Delta(I)\} \tag{I.7.1}$$

for $k[\boldsymbol{X}]/I$ in an obvious way. As we will soon see, Pellikaan's factor ring theorem (recall that another word for quotient ring is factor ring) gives a condition under which the ordered basis (I.7.1) is well-behaving. Pellikaan's factor ring theorem was originally stated in [33][1] in the special case of $r = 1$. In [13] the theorem is generalized to any $r \in \mathbb{N}$.

Theorem I.7.1
Let I be an ideal in $k[X_1, \ldots, X_m]$ with Gröbner basis $\mathcal{G}$ with respect to a weighted degree lexicographic ordering $\prec_w$. Suppose that the elements of the corresponding footprint $\Delta(I)$ have mutually distinct weights and that every element of $\mathcal{G}$ has exactly two monomials of highest weight in its support. Denote

$$\Lambda := \langle w(M) \mid M \in \Delta(I) \rangle \subseteq \mathbb{N}_0^r.$$

And denote by F the remainder of a polynomial in f after division with $\mathcal{G}$[2]. Then $R = k[X_1, \ldots, X_m]/I$ is an order domain with a weight function ρ defined by

$$\rho : \begin{cases} R & \to & \Lambda_{-\infty} \\ f & \mapsto & \max_{\prec_{\mathbb{N}_0^r}} \{w(M) \,|\, M \in \mathrm{Supp}(F)\} \ \textit{for } f \neq 0 \\ 0 & \mapsto & -\infty. \end{cases} \tag{I.7.2}$$

Proof:
Clearly $\mathcal{B} := \{M + I \mid M \in \Delta(I)\}$ is a basis for R as a vector space over k. And by assumption we can index the elements in $\mathcal{B}$ by the weights of their representatives in $\Delta(I)$. That is we can write

$$\mathcal{B}_w = (f_\lambda = F_\lambda + I \mid F_\lambda \in \Delta(I) \text{ and } w(F_\lambda) = \lambda \in \Lambda)\,.$$

Denote by $\prec_\Lambda$ the restriction of $\prec_{N_0^r}$ to Λ. It remains to be shown that the indexed and ordered basis $\mathcal{B}_{w.\prec_\Lambda}$ is well-behaving. Consider two elements in $\mathcal{B}$, say $f_\lambda = F_\lambda + I$ and $f_\gamma = F_\gamma + I$. Now $F_\lambda F_\gamma$ is a monomial but it need not be an element in $\Delta(I)$. However to write $f_\lambda f_\gamma = F_\lambda F_\gamma + I$ as a linear combination of the elements in the basis $\mathcal{B}$ one need only find the residue of $F_\lambda F_\gamma$ modulo the Gröbner basis $\mathcal{G}$. Say $F_\lambda F_\gamma$ is reduced modulo $\mathcal{G}$ to $\sum k_\alpha F_\alpha$ (recall that the reduction is unique). We get $f_\lambda f_\gamma = \sum k_\alpha f_\alpha$. As the elements in the footprint have mutually distinct weights there is precisely one monomial in $\mathrm{Supp}(\sum k_\alpha F_\alpha)$ of highest weight. From the assumption that every element

[1] Note added the second edition: "[33]" should be replaced by "[27] and [33].

[2] Given a residue class f, recall from appendix I.A that the remainder of any two polynomials $P_1, P_2 \in f$ after division with $\mathcal{G}$ is the same.

in $\mathcal{B}$ has two monomials of highest weight in its support, and from the nature of the division algorithm producing the residue $\sum k_\alpha F_\alpha$, it follows that the monomial of highest weight in $\mathrm{Supp}(\sum k_\alpha F_\alpha)$ is of weight equal to $w(F_\lambda F_\gamma)$. The well-behaving property of the indexed and ordered basis $\mathcal{B}_{w,\prec_\Lambda}$ is ensured by the fact that $w(F_\lambda F_\gamma) = w(F_\lambda) + w(F_\gamma)$, and by the assumption that $\prec_\Lambda$ is a monomial ordering. So $\mathcal{B}$ is an order basis, and the corresponding order function is a weight function. □

Remark I.7.2
In the proof of theorem I.7.1 we did not use the structure of the lexicographic part $\prec_{lex}$ of $\prec_w$. Let $\prec_w$ on $\mathcal{M}_m$ be an ordering definded as in definition I.2.15 but with $\prec_{lex}$ replaced by any monomial ordering $\prec_{\mathcal{M}_m}$ on $\mathcal{M}_m$. One easily verifies that $\prec_w$ is a monomial ordering, and that theorem I.7.1 holds in this more general set-up as well.

Remark I.7.3
Assume that an order domain $R = k[X_1, \ldots, X_m]/I$ is constructed using theorem I.7.1. The requirement, that every polynomial in the Gröbner basis for I has precisely two monomials of highest weight in its support, ensures that every polynomial in I has precisely an even number of monomials of highest weight in its support. Further any polynomial in $k[X_1, \ldots, X_m]$ can be written as the sum of two polynomials, the first being a linear combination of monomials in $\Delta(I)$ (in particular a linear combination of monomials of different weights), and the second being a polynomial in I. So we have an easy way to check if a polynomial F is a residue modulo $\mathcal{G}$. That is namely precisely the case, when F contains no two monomials in its support of the same weight.

Remark I.7.4
In the case of a toric ideal $I = \langle \mathcal{G}_X \rangle$ (the notation as in proposition I.6.2) the conditions in proposition I.7.1 are satisfied if we choose $\mathcal{B} := \mathcal{G}_X$.

Proposition I.7.5
Let $\tilde{k} \supseteq k$ be a field extension. If $k[\boldsymbol{X}]/I$, where

$$I = \langle F_1(\boldsymbol{X}), \ldots, F_s(\boldsymbol{X}) \rangle \subseteq k[\boldsymbol{X}],$$

can be understood as an order domain by using Pellikaan's factor ring theorem, then can also $\tilde{k}[\boldsymbol{X}]/\tilde{I}$, where

$$\tilde{I} := \langle F_1(\boldsymbol{X}), \ldots, F_s(\boldsymbol{X}) \rangle \subseteq \tilde{k}[\boldsymbol{X}].$$

Proof:
A Gröbner basis for I wrt. $\prec_w$ is also a Gröbner basis for $\tilde{I}$ wrt. $\prec_w$. □

Remark I.7.6
Of particular interest is the special case where $\tilde{k}$ in proposition I.7.5 is the algebraic closure of k. We then write $\tilde{k} = \bar{k}$ and $\tilde{I} = \bar{I}$. Now the fact that $\bar{I}$ is prime (proposition I.5.1) together with $\bar{k}$ being algebraically closed implies that $\bar{I} = \mathcal{I}(V)$ for some irreducible variety V (see [4, Ch. 4 §5, Cor. 4]). If in particular I has only one generator $F_1(\boldsymbol{X})$ then F_1 must be absolutely irreducible over k. Now $\bar{k}[\boldsymbol{X}]/\mathcal{I}(V)$ is isomorphic to the coordinate ring $\bar{k}[V]$ (the collection of polynomial functions $\varphi : V \to \bar{k}$) (the isomorphism is described in [4, Ch. 5 §2]).

I.7.2 Some examples

The following examples illustrate how easily one can construct weight functions using Pellikaan's factor ring theorem.

Example I.7.7
Consider $R := k[X, Y, Z]/I$ where $I := Y^2 - X^2Z + YZ^2 + Z^{35}$. Define weights $w(X) = (1, 0), w(Y) = (1, 1), w(Z) = (0, 2)$. Order the elements of $\mathbb{N}_0^2$ by $\prec_{lex}$ where $(0, 1) \prec_{lex} (1, 0)$. Now $w(Y^2) = w(X^2Z) = (2, 2)$, $w(YZ^2) = (1, 5)$ and $w(Z^{35}) = (0, 35)$. With respect to the chosen ordering on $\mathbb{N}_0^2$, $(2, 2)$ is the largest among these three values. The conditions in Pellikaan's factor ring theorem are satisfied. So we have a weight function

$$\rho : R \to \langle (1, 0), (1, 1), (0, 2) \rangle \cup \{-\infty\}$$

induced by $\rho(X + I) = (1, 0)$, $\rho(Y + I) = (1, 1)$ and $\rho(Z + I) = (0, 2)$. Beside the ordering $\prec_{lex}$ on $\mathbb{N}_0^2$ (corresponding to slope $\alpha = 0$) the legal orderings on $\mathbb{N}_0^2$ are the ones with slope $\alpha \in]0, \frac{2}{33}[$ and the one with slope $\alpha = \frac{2}{33}$ and with lexpart given by $(0, 1) \prec'_{lex} (1, 0)$.

Using Pellikaans factor ring theorem, we can often describe more families of order functions corresponding to a given order domain.

Example I.7.8
In this example any ordering $\prec_{\mathbb{N}_0^2}$ on $\mathbb{N}_0^2$ is assumed to be monomial. Consider the order domain $\mathbb{F}_q[X, Y, Z]/\langle X^3 + Y^4 + Z \rangle$. We list a few classes of weight

functions.

$$\begin{array}{ll}(1) & \rho(X+I)=(4,0),\ \rho(Y+I)=(3,0),\ \rho(Z+I)=(0,1)\\ (2) & \rho(X+I)=(4,4),\ \rho(Y+I)=(3,3),\ \rho(Z+I)=(1,2)\\ (3) & \rho(X+I)=(4,4),\ \rho(Y+I)=(3,3),\ \rho(Z+I)=(0,1)\\ (4) & \rho(X+I)=(2,0),\ \rho(Y+I)=(0,1),\ \rho(Z+I)=(6,0)\\ (5) & \rho(X+I)=(0,1),\ \rho(Y+I)=(1,0),\ \rho(Z+I)=(4,0).\end{array}$$

For class (1), (2) and(3) the legal choices of $\prec_{\mathbb{N}_0^2}$ *are the ones that satisfies* $\rho(X^3+I)\succ_{\mathbb{N}_0^2}\rho(Z+I)$. *For class (4) the legal choices of* $\prec_{\mathbb{N}_0^2}$ *are the ones that satisfies* $\rho(X^3+I)\succ_{\mathbb{N}_0^2}\rho(Y^4+I)$ *and finally for class (5) the legal choices are the ones that satisfies* $\rho(Y^4+I)\succ_{\mathbb{N}_0^2}\rho(X^3+I)$. *We have the following characteristicas.*

$(1)-(3)$ $\rho(X^3+I)=\rho(Y^4+I),\ \rho(X^3+I)\neq\rho(Z+I),$
$\rho(Y^4+I)\neq\rho(Z+I)$

(1) *whether* $\rho(Z^3+I)\succ_{\mathbb{N}_0^2}\rho(Y+I)$
or $\rho(Z^3+I)\prec_{\mathbb{N}_0^2}\rho(Y+I)$ *depends on the choice of* $\prec_{\mathbb{N}_0^2}$ *(both things can happen)*

(2) $\rho(Z^3+I)\succ_{\mathbb{N}_0^2}\rho(Y+I)$

(3) $\rho(Z^3+I)\prec_{\mathbb{N}_0^2}\rho(Y+I)$

(4) $\rho(X^3+I)\neq\rho(Y^4+I),\ \rho(X^3+I)=\rho(Z+I),$
$\rho(Y^4+I)\neq\rho(Z+I)$

(5) $\rho(X^3+I)\neq\rho(Y^4+I),\ \rho(X^3+I)\neq\rho(Z+I),$
$\rho(Y^4+I)=\rho(Z+I).$

It is clear that for instance the classes (1), (4) and (5) are disjoint and so are the classes (2),(3),(4) and (5). It is also clear that no two classes are the same.

The order functions corresponding to the same class are in general very different from each other. We illustrate this with a few examples in the case of class (1). In the following we use the notation $f=F+I$. *The legal choices of* $\prec_{\mathbb{N}_0^2}$ *correspond to the slopes* $\alpha\in[0,12]$. *If* $\alpha=12$ *then we must have* $(0,1)\prec_{\mathbb{N}_0^2}(1,0)$. *The well behaving sequence corresponding to the footprint*

$$\Delta(I)=\{X^\alpha Y^\beta Z^\gamma\,|\,\alpha<3\}$$

starts with

$$(1, y, x, y^2, xy, x^2, y^3, x^2y, z, y^4, xy^3, x^2y^2, y^5, \ldots).$$

If instead $\alpha = \sqrt{2}$ *then the well behaving sequence corresponding to* $\Delta(I)$ *starts with*

$$(1, z, z^2, y, x, z^3, yz, xz, z^4, yz^2, y^2, xz^2, xy, z^5, \ldots).$$

If $\alpha = 1$ *then there are two possible choices. Either* $(0,1) \prec_{\mathbb{N}_0^2} (1,0)$ *or* $(0,1) \succ_{\mathbb{N}_0^2} (1,0)$*. In both cases the well behaving sequence corresponding to* $\Delta(I)$ *starts with*

$$(1, z, z^2, z^3, y, z^4, yz, x, z^5, yz^2, xz, z^6, yz^3, xz^2, y^2, \ldots). \tag{I.7.3}$$

Finally if $\alpha = 0$ *then we do not have a well-behaving sequence but only a well-behaving basis. We list some of the elements in this basis after increasing order, to get a picture of the structure of this well-behaving basis.*

$$1, z, z^2, z^3, \ldots, y, yz, yz^2, yz^3, \ldots, x, xz, xz^2, xz^3, \ldots,$$
$$xy, xyz, xyz^2, xyz^3, \ldots\ldots\ldots$$

As noted before, in this material we do not always describe, all the legal orderings on a given value semigroup Λ. In this way we consider in the following two examples only the standard orderings on $\mathbb{N}_0^r$.

Recall that in example I.6.6 we considered a determinantal ring coming from a $2 \times n$ matrix $[X]_{ij}$ of variables X_{ij}. We showed that the quotient ring $k[X_{11}, X_{12}, \ldots, X_{2n}]/I$, where I is the ideal generated by the 2×2 minors, is an order domain. With Pellikaan's factor ring theorem we now have the tool for giving some more examples of determinantal rings that are order domains.

Example I.7.9
For $m \geq 2$ *consider a* $m \times m$ *matrix* $[X]_{ij}$ *of variables* X_{ij}*. As usual we use the notation* $\boldsymbol{X} := (X_{11}, X_{12}, \ldots, X_{mm})$ *and we will write* $\mathcal{M}$ *for the set of monomials in* $X_{11}, \ldots, X_{mm}$*. Let* I *be the ideal in* $k[\boldsymbol{X}]$ *generated by the determinant* $F(\boldsymbol{X})$ *of* $[X]_{ij}$*. We will show that* $k[\boldsymbol{X}]/I$ *is an order domain.*
Let weight vectors, $w(X_{ij}) \in \mathbb{N}_0^{m^2-1} \backslash \{\mathbf{0}\}$ *be given as in figure I.7.1 and let* $\mathbb{N}_0^{m^2-1}$ *be ordered by the standard ordering* $\prec_{st}$*. Let* $\prec_w$ *be the weighted degree lexicographic ordering on* $\mathcal{M}$ *induced by these weights, by* $\prec_{st}$ *on* $\mathbb{N}_0^{m^2-1}$*, and by some lexicographic ordering* $\prec_{lex}$ *on* $\mathcal{M}$*. One easily checks that* $X_{11}X_{22}\cdots X_{mm}$

and $X_{1m}\left(X_{21}X_{32}\cdots X_{m(m-1)}\right)$ *are the only terms of* F *of the highest weight. Wlog. we may assume that the leading monomial of* F *wrt.* $\prec_w$ *is* $\mathrm{lm}(F) = X_{11}\cdots X_{mm}$*. Now*

$$\Delta(I) = \{M \in \mathcal{M} \mid X_{11}\cdots X_{mm} \nmid M\}\,.$$

From figure I.7.1 one easily concludes that no two different monomials in $\Delta(I)$ *have the same weight. As* $\{F\}$ *of course is a Gröbner basis we conclude that all the conditions in theorem I.7.1 are satisfied.*

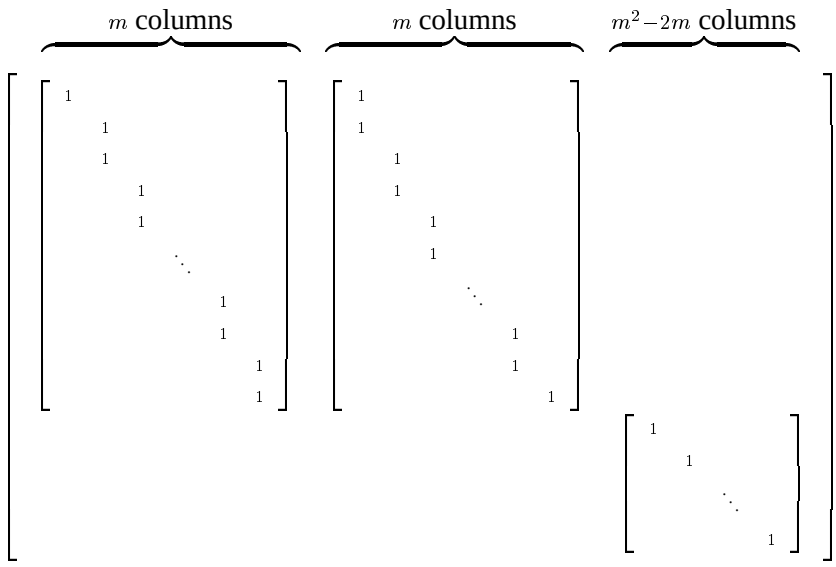

Figure I.7.1: The first m columns are the weights $w(X_{11})$, $w(X_{22}),\ldots,w(X_{mm})$. The next m columns are the weigths $w(X_{1m})$, $w(X_{21})$, $w(X_{32}),\ldots,w(X_{m(m-1)})$. The remaining last m^2-2m columns consist of the weights of the remaining variables in some unspecified order.

Given $m < n$ consider the following determinantal ring comming from an $m\times n$ matrix of indeterminates. Namely the ring $k[X_{11},\ldots,X_{mn}]/I$ where I is the ideal that is generated by all $m\times m$ minors. In a class of experiments the author tried to find weight functions on these structures, but without any luck. In the next example we leave out some of the $m\times m$ minors defining I, and we are then able to find weight functions on the corresponding structures.

Example I.7.10
For $m \geq 3$ consider a $m \times (m+2)$ matrix $[X]_{ij}$ of variables X_{ij}. As usual we use the notation $\boldsymbol{X} := \left(X_{11}, X_{12}, \ldots, X_{m(m+2)}\right)$ and we will write $\mathcal{M}$ for the set of monomials in $X_{11}, \ldots, X_{m(m+2)}$. Let I be the ideal in $k\left[\boldsymbol{X}\right]$ generated by F_1 and F_2, where F_1 and F_2 are given in the following way. F_1 is the determinant of the matrix consisting of the first m columns in $[X]_{ij}$ and F_2 is the determinant of the matrix consisting of the last m columns in $[X]_{ij}$. We will show that in the case $m = 3, 4, 5$ the domain $k\left[\boldsymbol{X}\right]/I$ is an order domain. The result can be generalized to any value $m \geq 3$.

Case I, $m = 3$:
Let weight vectors, $w(X_{ij}) \in \mathbb{N}_0^{13} \setminus \{\mathbf{0}\}$, be given as in figure I.7.2, and let $\mathbb{N}_0^{13}$ be ordered by the standard ordering $\prec_{st}$. Let $\prec_w$ be the weighted degree lexicographic ordering on $\mathcal{M}$ induced by these weights, by the ordering on $\mathbb{N}_0^{13}$, and by a lexicographic ordering $\prec_{lex}$ on $\mathcal{M}$ such that $X_{31}X_{12}X_{23} \prec_{lex} X_{11}X_{22}X_{33}$ and $X_{23}X_{34}X_{15} \prec_{lex} X_{13}X_{24}X_{35}$.

$$\begin{bmatrix}
1 & & 1 & & & & & & & & & & \\
1 & & & 1 & & & & & & & & & \\
 & 1 & & 1 & & & & & & & & & \\
 & 1 & & & 1 & & 1 & & & & & & \\
 & & 1 & & 1 & & 1 & & & & & & \\
 & & 1 & & 1 & & & 1 & & & & & \\
 & & & & & 1 & & 1 & & & & & \\
 & & & & & 1 & & & 1 & & & & \\
 & & & & & & 1 & & 1 & & & & \\
 & & & & & & & & & 1 & & & \\
 & & & & & & & & & & 1 & & \\
 & & & & & & & & & & & 1 & \\
 & & & & & & & & & & & & 1
\end{bmatrix}$$

Figure I.7.2: Case I: Each column corresponds to a weight of a variable. The weights are listed in the following way. The first 11 columns state the value of $w(X_{11})$, $w(X_{22})$, $w(X_{33})$, $w(X_{31})$, $w(X_{12})$, $w(X_{23})$, $w(X_{34})$, $w(X_{15})$, $w(X_{13})$, $w(X_{24})$, $w(X_{35})$. The last 4 columns (unit vectors) give the weights of the remaining variables in some order.

It is easily checked that $X_{31}X_{12}X_{23}$ and $X_{11}X_{22}X_{33}$ are the only terms in F_1 of the highest weight with respect to the ordering just mentioned. In particular $\mathrm{lm}(F_1) = X_{11}X_{22}X_{33}$. Also $X_{23}X_{34}X_{15}$ and $X_{13}X_{24}X_{35}$ are the only terms in F_2 of the highest weight. In particular $\mathrm{lm}(F_2) = X_{13}X_{24}X_{35}$. As the leading monomials are relatively prime we conclude that $\{F_1, F_2\}$ constitutes a Gröbner basis for I with respect to $\prec_w$. In particular this means that

$$\Delta(I) = \{M \in \mathcal{M} \mid X_{11}X_{22}X_{33} \nmid M, X_{13}X_{24}X_{35} \nmid M\}.$$

Studying the nullspace of the matrix in figure I.7.2 we see that there do not exist two different elements in the footprint with the same weighted degree. All the conditions in theorem I.7.1 are satisfied.

Case II, m=4:
Let weight vectors, $w(X_{ij}) \in \mathbb{N}_0^{22} \setminus \{\mathbf{0}\}$ be given as in figure I.7.3, and let $\mathbb{N}_0^{22}$ be ordered by the standard ordering $\prec_{st}$. Let $\prec_w$ be the weighted degreee lexicographic ordering on $\mathcal{M}$ induced by these weights, by $\prec_{st}$ on $\mathbb{N}_0^{22}$ and by a lexicographic ordering $\prec_{lex}$ on $\mathcal{M}$ such that

$$X_{41}X_{12}X_{23}X_{34} \prec_{lex} X_{11}X_{22}X_{33}X_{44}$$

$$X_{23}X_{34}X_{45}X_{16} \prec_{lex} X_{13}X_{24}X_{35}X_{46}.$$

Now $X_{41}X_{12}X_{23}X_{34}$ and $X_{11}X_{22}X_{33}X_{44}$ are the only terms in F_1 of the highest weight and $X_{23}X_{34}X_{45}X_{16}$ and $X_{13}X_{24}X_{35}X_{46}$ are the only terms in F_2 of the highest weight. Just as in case 1 the conditions in theorem I.7.1 are seen to be satisfied.

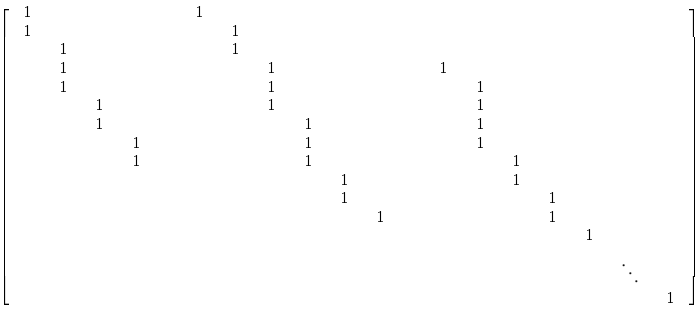

Figure I.7.3: Case II: Each column corresponds to a weight of a variable. The weights are listed in the following way. The first 14 columns state the value of $w(X_{11})$, $w(X_{22})$, $w(X_{33})$, $w(X_{44})$, $w(X_{41})$, $w(X_{12})$, $w(X_{23})$, $w(X_{34})$, $w(X_{45})$, $w(X_{16})$, $w(X_{13})$, $w(X_{24})$, $w(X_{35})$, $w(X_{46})$. The remaining last 10 columns (unit vectors) gives the weights of the remaining variables in some order.

Case III, $m = 5$:
Let weight vectors $w(X_{ij}) \in \mathbb{N}_0^{33} \setminus \{\mathbf{0}\}$ be given as in figure I.7.4, and let $\mathbb{N}_0^{33}$ be ordered by the standard ordering $\prec_{st}$. Let $\prec_w$ be the ordering on $\mathcal{M}$ induced by these weights, by $\prec_{st}$ on $\mathbb{N}_0^{33}$, and by a lexicographic ordering $\prec_{lex}$ on $\mathcal{M}$ such

that

$$X_{51}X_{12}X_{23}X_{34}X_{45} \prec_{lex} X_{11}X_{22}X_{33}X_{44}X_{55}$$

$$X_{23}X_{34}X_{45}X_{56}X_{17} \prec_{lex} X_{13}X_{24}X_{35}X_{46}X_{57}.$$

Now $X_{51}X_{12}X_{23}X_{34}X_{45}$ and $X_{11}X_{22}X_{33}X_{44}X_{55}$ are the only terms in F_1 of the highest weight. And $X_{23}X_{34}X_{45}X_{56}X_{17}$ and $X_{13}X_{24}X_{35}X_{46}X_{57}$ are the only terms in F_2 of the highest weight. Just as in case I and II we find that the conditions in theorem I.7.1 are satisfied.

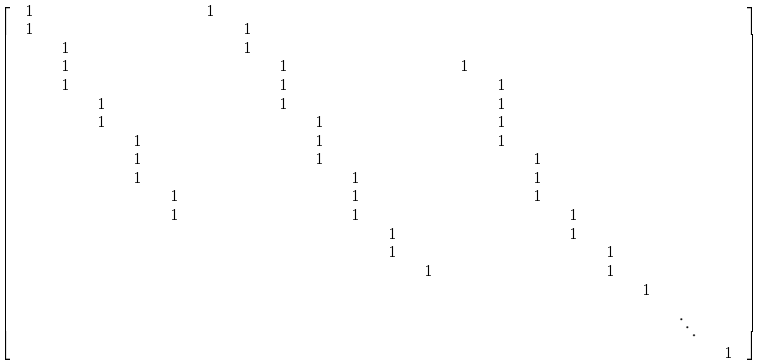

Figure I.7.4: Case III: Each column corresponds to the weight of a variable. The weights are listed in the following way. The first 17 columns state the value of $w(X_{11})$, $w(X_{22})$, $w(X_{33})$, $w(X_{44})$, $w(X_{55})$, $w(X_{51})$, $w(X_{12})$, $w(X_{23})$, $w(X_{34})$, $w(X_{45})$, $w(X_{56})$, $w(X_{17})$, $w(X_{13})$, $w(X_{24})$, $w(X_{35})$, $w(X_{46})$, $w(X_{57})$. The remaining last 18 columns (unit vectors) give the weights of the remaining variables in some order.

I.7.3 The effect of different choices of lex-part of $\prec_w$

Let $I \subseteq k[X_1, \ldots, X_m]$ be an ideal with a Gröbner basis $\mathcal{G}$ with respect to a weighted degree lexicographic ordering $\prec_w$. Denote the lexicographic part of $\prec_w$ by $\prec_{lex}$. Assume now that $I, \mathcal{G}, \prec_w$ satisfies the conditions in Pellikaan's theorem. A natural question then is what happens if we interchange the lex-part of $\prec_w$ with another lexicographic ordering $\prec'_{lex}$ to give us $\prec'_w$. Will the conditions in Pellikaan's theorem still be satisfied? (eventually with a new Gröbner basis). And if they are, will the corresponding weight function on $k[X_1, \ldots, X_m]/I$ be the same? We will show that the answer to the last question is positive. And we will give a condition under which the answer to the first

question is also positive.

To state the condition we will need some notation. Denote

$$\mathcal{G} = \{F^{(1)} = M_1^{(1)} + \alpha^{(1)} M_2^{(1)} + G^{(1)}, \ldots, \\ F^{(s)} = M_1^{(s)} + \alpha^{(s)} M_2^{(s)} + G^{(s)}\}$$

where $M_1^{(t)}, M_2^{(t)}$, $t = 1, \ldots, s$ are the monomials in $F^{(t)}$ of highest weight. The condition is as follows.

Condition I:
Given any two monomials $N_1 \neq N_2$ *such that* $w(N_1) = w(N_2)$ *then there exists an index* $t \in \{1, \ldots, s\}$ *such that*

$$M_1^{(t)} | N_1, M_2^{(t)} | N_2 \quad \textit{or} \quad M_2^{(t)} | N_1, M_1^{(t)} | N_2.$$

We first show that under this condition, $\mathcal{G}$ is also a Gröbner basis with respect to $\prec'_w$. Assume by contrary that it is necessary to adjoin more polynomials to $\mathcal{G}$ to get a Gröbner basis $\mathcal{G}'$ wrt. $\prec'_w$. Let H be any of these polynomials. By proposition I.5.4 we may wlog. assume, that H can be written

$$H = N_1 + \alpha N_2 + I, \ \alpha \neq 0$$

where

$$w(N_1) = w(N_2) = \mathrm{wdeg}(H),$$

and where N_1 is the leading monomial of H wrt. $\prec'_w$. Further wlog. we may assume, that wrt. $\prec'_w$, we have $\mathrm{lm}(F^{(l)}) = M_1^{(l)}$, for $l = 1, \ldots, s$. By condition I, a t, $1 \leq t \leq s$, exists, such that either $M_1^{(t)} \mid N_1$ and $M_2^{(t)} \mid N_2$ holds, or $M_2^{(t)} \mid N_1$ and $M_1^{(t)} \mid N_2$ holds. In the first case, by the very definition of a Gröbner basis (see definition I.A.2 in the appendix), the set $\mathcal{G}' \backslash \{H\}$ is also a Gröbner basis of I wrt. $\prec'_w$. So $M_2^{(t)} \mid N_1$ and $M_1^{(t)} \mid N_2$ must hold. Consider

$$H_1 := H - \alpha \frac{N_2}{M_1^{(t)}} F^{(t)}.$$

As $\mathrm{lm}(H) = N_1$, we must have $N_1 \in \mathrm{Supp}(H_1)$. And in particular $\mathrm{lm}(H_1) = N_1$. As $H_1 \in I$, we can conclude that

$$H_1 = N_1 + \beta Q_2 + J, \ \beta \neq 0$$

where

$$w(N_1) = w(Q_2) = \mathrm{wdeg}(H_1).$$

That is, H_1 is of a form similar to H. Getting from H to H_1, is the first step in the division algorithm, that finds the residue of H modulo $\{F^{(1)}, \ldots, F^{(s)}\}$. So wlog. we may assume that H is its own residue modulo $\{F^{(1)}, \ldots, F^{(s)}\}$. But this is in contradiction with condition I. We have proved that $\mathcal{G}$ is also a Gröbner basis wrt $\prec'_w$.

Although $\Delta_{\prec'_w}(I)$ will not equal $\Delta_{\prec_w}(I)$, condition I ensures that no two monomials in $\Delta_{\prec'_w}(I)$ will be of the same weight. We conclude that $I, \mathcal{G}, \prec'_w$ satisfies the conditions in Pellikaan's factor ring theorem.

Finally to see that $\prec'_w$ and $\prec_w$ gives the same weight function whenever both $I, \mathcal{G}', \prec'_w$ and $I, \mathcal{G}, \prec_w$ satisfies the conditions in Pellikaan's theorem note the following. Consider any residue class $f = F + I$ where F is the residue of any polynomial in f modulo $\mathcal{G}$ (wrt. $\prec_w$). By assumption F has precisely one monomial of highest weight in its support. Now reduce F modulo $\mathcal{G}'$ (wrt. $\prec'_w$) to get the unique residue $F' \in F + I$. As F has precisely one monomial in its support of highest weight, so has also F', and $\mathrm{wdeg}(F') = \mathrm{wdeg}(F)$. By construction the weight functions are the same.

Note that all the weight functions considered in this material satisfies condition I. We leave it as an open problem to decide if it is at all possible to construct a weight function such that condition I is not satisfied.

I.8
Constructing new order domains from old ones

In this chapter we will study three different ways to construct new order domains from old ones. First we discuss how to construct new order domains from toric order domains. Next we study the tensor products of order domains, and finally we will be concerned with constructing new order domains by a certain kind of substitution.

I.8.1 New order domains from toric order domains

For coding theoretical purposes one of the interesting parameters of an order domain $\mathbb{F}_q[\boldsymbol{X}]/I$ is the number of zeros $n = \#\mathcal{V}_{\mathbb{F}_q}(I)$. As we will see in chapter I.11 there exist simple methods to construct codes over $\mathbb{F}_q$ of length $n = \#\mathcal{V}_{\mathbb{F}_q}$ from an order domain $\mathbb{F}_q[\boldsymbol{X}]/I$. A motivation for constructing a new order domain $\mathbb{F}_q[\boldsymbol{X}]/I'$ by modifying the defining polynomials of a toric order domain $\mathbb{F}_q[\boldsymbol{X}]/I$ could be to try to obtain $\#\mathcal{V}_{\mathbb{F}_q}(I') > \#\mathcal{V}_{\mathbb{F}_q}(I)$. This will allow us to construct longer codes. If we modify the defining polynomials of the toric order domain carefully, we may achieve that a value semigroup Λ survives the modification in the sense, that there exist both a weight function $\rho : k[\boldsymbol{X}]/I \to \Lambda_{-\infty}$ and a weight function $\rho' : k[\boldsymbol{X}]/I' \to \Lambda_{-\infty}$. That this can actually be desirable relies on the fact that the structure of the value semigroup contains information about the minimum distances of the codes corresponding to the order domain. The implication of the structure of Λ on the minimum distances of the corresponding codes is described in chapter I.11.

Example I.8.1
Consider the toric ideal I in $\mathbb{F}_2[X_1, X_2, X_3]$ corresponding to the weights

$$w(X_1) = (2, 0) \quad w(X_2) = (0, 2) \quad w(X_3) = (1, 1). \tag{I.8.1}$$

One easily verifies that $I = \langle X_1, X_2 + X_3^2 \rangle$. Let $\prec_{\mathbb{N}_0^2}$ be a monomial ordering on $\mathbb{N}_0^2$. An order function on $R := \mathbb{F}_2[X_1, X_2, X_3]/I$ is induced as a weight

function by

$$\begin{aligned} \rho(X_1 + I) = (2,0), \rho(X_2 + I) = (0,2), \\ \rho(X_3 + I) = (1,1). \end{aligned} \tag{I.8.2}$$

Order next $\mathcal{M}_3$ by the lexicographic ordering $\prec_{lex}$, where $X_1 \prec_{lex} X_2 \prec_{lex} X_3$. And denote by $\prec_w$ the weighted degree lexicographic ordering given by (I.8.1), $\prec_{\mathbb{N}_0^2}$ and $\prec_{lex}$. Now clearly ρ can be understood as a weight function from Pellikaan's factor ring theorem by the use of $\prec_w$. In particular $\{X_1X_2 + X_3^2\}$ is a Gröbner basis wrt. $\prec_w$.
We will now add terms to the defining polynomial $X_1X_2 + X_3^2$ in a way such that X_1X_2, X_3^2 is still the unique pair of monomials of highest weight in our defining polynomial. That is we will add terms of weight less than $(2,2)$ (with respect to $\prec_{\mathbb{N}_0^2}$). It is clear that the conditions in Pellikaan's factor ring theorem will still be satisfied if we replace $X_1X_2 + X_3^2$ with the new defining polynomial. And the weight function will still be induced by (I.8.2) if we interchange I with the ideal generated by the new defining polynomial. What might change, when we in this way replace I with a new ideal, is the size of the corresponding variety. Working with this process in practice, one often experience that the size of the variety is either unchanged or raised. However it can happen that the size of the variety is lowered. If we choose $\prec_{\mathbb{N}_0^2}$ to be $\prec_{st}$ then adding $X_1 + X_3$ or $X_1 + X_2 + X_3$ will be legal. We get

$$\mathcal{V}_{\mathbb{F}_2}(\langle X_1X_2 + X_3^2 \rangle) = \{(0,0,0),(1,0,0),(0,1,0),(1,1,1)\}$$

$$\begin{aligned} \mathcal{V}_{\mathbb{F}_2}(\langle X_1X_2 + X_3^2 + X_1 + X_3 \rangle) = \{&(0,1,0),(0,1,1),(0,0,0), \\ &(0,0,1),(1,1,0),(1,1,1)\} \end{aligned}$$

$$\mathcal{V}_{\mathbb{F}_2}(\langle X_1X_2 + X_3^2 + X_1 + X_2 + X_3 \rangle) = \{(0,0,0),(0,0,1)\}.$$

Example I.8.2
Consider the toric ideal I in $\mathbb{F}_2[X_1, X_2, X_3, X_4]$ corresponding to the weights

$$\begin{aligned} w(X_1) = (2,0), \quad w(X_2) = (0,2), \\ w(X_3) = (1,1), \quad w(X_4) = (1,2). \end{aligned} \tag{I.8.3}$$

We have $I = \langle X_3^2 - X_2X_1, X_4^2 - X_2^2X_1 \rangle$. Order $\mathbb{N}_0^2$ by some monomial ordering $\prec_{\mathbb{N}_0^2}$. We will define two orderings on $\mathcal{M}_4$. Let the weighted degree

lexicographic ordering $\prec_w$ be defined by the weights (I.8.3), by the ordering $\prec_{\mathbb{N}_0^2}$, and by the lexicographic ordering

$$X_1 \prec_{lex} X_2 \prec_{lex} X_3 \prec_{lex} X_4.$$

Further let $\prec'_w$ be the similar ordering where $\prec_{lex}$ is replaced with the lexicographic ordering $\prec'_{lex}$ defined by

$$X_4 \prec'_{lex} X_3 \prec'_{lex} X_2 \prec'_{lex} X_1.$$

Now

$$\mathcal{G}^{(\prec_w)} = \{X_3^2 - X_2X_1, X_4^2 - X_2^2X_1\} \tag{I.8.4}$$

is a Gröbner basis with respect to $\prec_w$. And

$$\mathcal{G}^{(\prec'_w)} = \{X_2X_3^2 - X_4^2, X_1X_4^2 - X_3^4, X_1X_2 - X_3^2\} \tag{I.8.5}$$

is a Gröbner basis with respect to $\prec'_w$.
The leading monomials of the polynomials in $\mathcal{G}^{(\prec_w)}$ are X_3^2 and X_4^2. That is the leading monomials are relatively prime. From Gröbner basis theory (see lemma I.A.16 in the appendix) we know that the S-polynomial of two polynomials with relatively prime leading monomials will always be zero. We conclude that we can add any terms we like to the first polynomial in $\mathcal{G}^{(\prec_w)}$, as long as these are of lower weight than $w(X_3^2) = (2, 2)$, and add as well any terms we like to the second polynomial in $\mathcal{G}^{(\prec_w)}$, as long as these are of lower weight than $w(X_4^2) = (2, 4)$. The new basis generated in this way will again be a Gröbner basis. As the footprint is unaffected by the adding of terms, the conditions in Pellikaan's factor ring theorem will still be satisfied. Note that different choices of $\prec_{\mathbb{N}_0^2}$ will give us different opportunities of adding terms.
However the situation is much more complicated in the case of $\prec'_w$. We can not repeat the argument from above as $X_2X_3^2$ is not relatively prime to X_1X_2 and neither is $X_1X_4^2$ to X_1X_2. If we for instance try to modify $\mathcal{G}^{(\prec'_w)}$ by simply adding the term X_4 to the first polynomial, then the following thing happen. Applying Buchberger's algorithm we get after reduction, the new Gröbner basis

$$\tilde{\mathcal{G}}^{(\prec'_w)} = \{X_2X_3^2 - X_4^2 - X_4, X_1X_2 - X_3^2, X_1X_4, X_3^4, X_3^2X_4, X_4^3 - X_4^2\}$$

and clearly this does not generate a prime ideal and therefore neither an order domain.

I.8.2 The tensor product construction

In this section we introduce a particular simple method to construct new order domains from old ones. We start with two examples.

Example I.8.3
Consider the order domains $R_1 := k[X_1]$ and $R_2 := k[X_2]$ with weight functions

$$\rho_i : \begin{cases} R_i & \to & \mathbb{N}_0 \cup \{-\infty\} \\ 0 & \mapsto & -\infty \\ F(X_i) & \mapsto & \deg F,\ F \neq 0 \end{cases} \qquad i = 1, 2.$$

Let $\mathbb{N}_0^2$ be ordered by $\prec_{st}$. Now with respect to this ordering $R := k[X_1, X_2]$ is an order domain with a weight function

$$\rho : \begin{cases} R & \to & \mathbb{N}_0^2 \cup \{-\infty\} \\ 0 & \mapsto & -\infty \\ F(X_1, X_2) & \mapsto & \max_{\prec_{st}}\{(\deg_{X_1} M, \deg_{X_2} M) \mid \\ & & \qquad M \in \mathrm{Supp}(F)\},\ F \neq 0. \end{cases}$$

Example I.8.4
Consider the order domain $R_1 := \mathbb{F}_4[X_1^{(1)}, X_2^{(1)}]/I_1$ where

$$I_1 := \langle (X_1^{(1)})^3 + (X_2^{(1)})^2 + X_2^{(1)} \rangle.$$

And similar $R_2 := \mathbb{F}_4[X_1^{(2)}, X_2^{(2)}]/I_2$ where

$$I_2 := \langle (X_1^{(2)})^5 + (X_2^{(2)})^3 \rangle.$$

Now R_1 can be understood as an order domain from Pellikaan's factor ring theorem by using weights

$$w_1(X_1^{(1)}) = 2, w_1(X_2^{(1)}) = 3$$

and by considering the footprint

$$\Delta(I_1) = \{(X_1^{(1)})^\alpha (X_2^{(1)})^\beta \mid \beta < 2\}.$$

The same story holds for R_2, by using weights

$$w_2(X_1^{(2)}) = 3, w_2(X_2^{(2)}) = 5$$

and by considering the footprint

$$\Delta(I_2) = \{(X_1^{(2)})^\alpha (X_2^{(2)})^\beta \mid \beta < 3\}.$$

Consider now

$$R := \mathbb{F}_4[X_1^{(1)}, X_2^{(1)}, X_1^{(2)}, X_2^{(2)}]/I$$

where

$$I := \langle (X_1^{(1)})^3 + (X_2^{(1)})^2 + X_2^{(1)}, (X_1^{(2)})^5 + (X_2^{(2)})^3 \rangle.$$

The crucial observation is that also R can be understood from Pellikaan's factor ring theorem to be an order domain. Just consider the weights

$$\begin{array}{ll} w(X_1^{(1)}) = (w_1(X_1^{(1)}), 0) = (2,0) & w(X_2^{(1)}) = (w_1(X_2^{(1)}), 0) = (3,0) \\ w(X_1^{(2)}) = (0, w_2(X_1^{(2)})) = (0,3) & w(X_2^{(2)}) = (0, w_2(X_2^{(2)})) = (0,5) \end{array}$$

and the footprint

$$\Delta(I) = \{M_1 M_2 \mid M_1 \in \Delta(I_1),\ M_2 \in \Delta(I_2)\}. \tag{I.8.8}$$

Using for instance the $\prec_{st}$ ordering on $\mathbb{N}_0^2$ the theorem is satisfied. Note that (I.8.8) follows from the fact that if $\mathcal{G}_i$ is a Gröbner basis for I_i, $i = 1, 2$, then $\mathcal{G} := \{F \mid F \in \mathcal{G}_1$ or $F \in \mathcal{G}_2\}$ is a Gröbner basis for I.

The construction in example I.8.3 and example I.8.4 is a special case of the so-called tensor product between k-algebras. We refer to [22] and [46] for the general definition of a tensor product. In [13] it is shown that the tensor product between any two order domains is again an order domain. In this material we consider only the case of a tensor product between quotient rings. This restriction makes it possible to develop the theory we need, using only already introduced concepts.

Consider two quotient rings, say

$$R = k[X_1, \ldots, X_m]/I$$

where

$$I = \langle F_1(\boldsymbol{X}), \ldots, F_r(\boldsymbol{X}) \rangle$$

and

$$S = k[Y_1, \ldots, Y_n]/J$$

where

$$J = \langle G_1(\boldsymbol{Y}), \ldots, G_s(\boldsymbol{Y}) \rangle.$$

Let

$$\{p_\lambda = P_\lambda(\boldsymbol{X}) + I \mid \lambda \in \Lambda\} \tag{I.8.9}$$

be a basis for R as a vector space over k, and

$$\{q_\gamma = Q_\gamma(\boldsymbol{Y}) + J \mid \gamma \in \Gamma\} \tag{I.8.10}$$

be a basis for S as a vector space over k.

Definition I.8.5
The tensor product over k between R and S is the quotient ring

$$\begin{aligned} R \otimes_k S &:= k[\boldsymbol{X}, \boldsymbol{Y}]/\langle F_1(\boldsymbol{X}), \ldots, F_r(\boldsymbol{X}), G_1(\boldsymbol{Y}), \ldots, G_s(\boldsymbol{Y})\rangle \\ &=: k[\boldsymbol{X}, \boldsymbol{Y}]/(I + J). \end{aligned}$$

Note that this definition is independent of the choice of generators $F_1, \ldots, F_r$ for I and $G_1, \ldots, G_s$ for J. We have the following (well-known) lemma.

Lemma I.8.6

$$\mathcal{B} := \{P_\lambda Q_\gamma + (I + J) \mid \lambda \in \Lambda, \gamma \in \Gamma\} \tag{I.8.11}$$

is a basis for $R \otimes_k S$.

Proof:
We may wlog. assume that

$$\{F_1(\boldsymbol{X}), \ldots, F_r(\boldsymbol{X})\} \tag{I.8.12}$$

is either equal to $\{0\}$ or is a Gröbner basis say wrt. the pure lexicographic ordering $\prec^X_{lex}$ on $\mathcal{M}(X_1, \ldots, X_m)$ defined by $X_m \prec^X_{lex} \cdots \prec^X_{lex} X_1$. And we assume that the representative P_λ of p_λ, $\lambda \in \Lambda$ is chosen as the residue modulo (I.8.12) of a(ny) polynomial in the residue class p_λ. Similar we assume that

$$\{G_1(\boldsymbol{Y}), \ldots, G_s(\boldsymbol{Y})\} \tag{I.8.13}$$

is either equal to $\{0\}$ or is a Gröbner basis say wrt. the pure lexicographic ordering $\prec^Y_{lex}$ on $\mathcal{M}(Y_1, \ldots, Y_n)$ defined by $Y_n \prec^Y_{lex} \cdots \prec^Y_{lex} Y_1$. And that Q_γ is the unique residue of a(ny) polynomial in q_γ. Note that the set $\mathcal{B}$ is defined independent of these assumptions.
To show that $\mathcal{B}$ is a basis for $R \otimes_k S$, we must show

(i) the elements of $\mathcal{B}$ are linearly independent over k

(ii) every residue class in $R \otimes_k S$ can be written as a linear combination of the elements in $\mathcal{B}$.

As a preparation to show (i) and (ii) we extend $\prec_{lex}^X$ and $\prec_{lex}^Y$ to the pure lexicographic ordering $\prec_{lex}$ on $\mathcal{M}(X_1, \ldots, X_m, Y_1, \ldots, Y_n)$ defined by

$$Y_n \prec_{lex} \cdots \prec_{lex} Y_1 \prec_{lex} X_m \prec_{lex} \cdots \prec_{lex} X_1.$$

Now

$$\{F_1(\boldsymbol{X}), \ldots, F_r(\boldsymbol{X}), G_1(\boldsymbol{Y}), \ldots, G_s(\boldsymbol{Y})\} \tag{I.8.14}$$

is either equal to $\{0\}$ or is a Gröbner basis wrt. $\prec_{lex}$. To see this consult Buchberger's algorithm and lemma I.A.16 in section I.A.4 of the appendix.

Proof of (i):
Assume that (i) does not hold. That is assume a linear combination exists

$$\begin{aligned} \sum_{\substack{\lambda \in \Lambda \\ \gamma \in \Gamma}} \alpha_{\lambda\gamma}(P_\lambda Q_\gamma + (I+J)) &= \left(\sum \alpha_{\lambda\gamma} P_\lambda Q_\gamma\right) + (I+J) \\ &= (I+J) \end{aligned} \tag{I.8.15}$$

where not all $\alpha_{\lambda\gamma}$ equals zero. As no term of $P_\lambda Q_\gamma$ is divisible by any of the leading terms in (I.8.14) whenever (I.8.14) does not equal $\{0\}$, then neither is any of the terms in $\sum \alpha_{\lambda\gamma} P_\lambda Q_\gamma$. So if $\sum \alpha_{\lambda\gamma} P_\lambda Q_\gamma$ is to be a polynomial in $I + J$ (assumption (I.8.15)), then we must have

$$\sum_{\substack{\lambda \in \Lambda \\ \gamma \in \Gamma}} \alpha_{\lambda\gamma} P_\lambda Q_\gamma = 0. \tag{I.8.16}$$

It remains to show that (I.8.16) leads to a contradiction. We have

$$\begin{aligned} &\sum_{\substack{\lambda \in \Lambda \\ \gamma \in \Gamma}} \alpha_{\lambda\gamma} P_\lambda Q_\gamma = 0 \\ \Downarrow \\ &\sum_{\lambda \in \Lambda} \left(\sum_{\gamma \in \Gamma} \alpha_{\lambda\gamma} Q_\gamma \right) P_\lambda = 0 \\ \Downarrow \\ &\sum_{\lambda \in \Lambda} R_\lambda(\boldsymbol{Y}) P_\lambda(\boldsymbol{X}) = 0 \end{aligned} \tag{I.8.17}$$

where

$$R_\lambda(\boldsymbol{Y}) = \sum_{\gamma\in\Gamma} \alpha_{\lambda\gamma} Q_\gamma(\boldsymbol{Y}) = \sum_{\boldsymbol{\delta}\in\mathbb{N}_0^n} c_{\lambda\boldsymbol{\delta}} \boldsymbol{Y}^{\boldsymbol{\delta}}.$$

Continuing from (I.8.17) we get

$$\begin{aligned}
&\sum_{\lambda\in\Lambda}\left(\sum_{\boldsymbol{\delta}\in\mathbb{N}_0^n} c_{\lambda\boldsymbol{\delta}}\boldsymbol{Y}^{\boldsymbol{\delta}}\right) P_\lambda(\boldsymbol{X}) = 0\\
\Downarrow\\
&\sum_{\boldsymbol{\delta}\in\mathbb{N}_0^n}\left(\sum_{\lambda} c_{\lambda\boldsymbol{\delta}} P_\lambda(\boldsymbol{X})\right)\boldsymbol{Y}^{\boldsymbol{\delta}} = 0\\
\Downarrow\\
&\sum_{\lambda\in\Lambda} c_{\lambda\boldsymbol{\delta}} P_\lambda(\boldsymbol{X}) = 0 \quad \text{for all } \boldsymbol{\delta}\in\mathbb{N}_0^n\\
\Downarrow\\
&c_{\lambda\boldsymbol{\delta}} = 0 \quad \text{for all } \lambda\in\Lambda, \boldsymbol{\delta}\in\mathbb{N}_0^n\\
\Downarrow\\
&\alpha_{\lambda\gamma} = 0 \quad \text{for all } \lambda\in\Lambda, \gamma\in\Gamma
\end{aligned}$$

and we have reached our contradiction.

Proof of (ii):
We have by assumption

$$\begin{aligned}
\operatorname{span}_k\{P_\lambda \mid \lambda\in\Lambda\} &= \{P \mid P \text{ a residue modulo } \{F_1(\boldsymbol{X}),\dots,F_r(\boldsymbol{X})\}\}\\
\operatorname{span}_k\{Q_\gamma \mid \gamma\in\Gamma\} &= \{Q \mid Q \text{ a residue modulo } \{G_1(\boldsymbol{Y}),\dots,G_s(\boldsymbol{Y})\}\}.
\end{aligned}$$

We conclude that

$$\begin{aligned}
\operatorname{span}_k\{P_\lambda Q_\gamma \mid \lambda\in\Lambda,\gamma\in\Gamma\} = \{T \mid T \text{ a residue modulo}\\
\{F_1(\boldsymbol{X}),\dots,F_r(\boldsymbol{X}),G_1(\boldsymbol{Y}),\dots,G_s(\boldsymbol{Y})\}\}.
\end{aligned}$$

□

Now assume that R and S are order domains with order functions $\rho_R : R\to\Lambda_{-\infty}$ and $\rho_S : S\to\Gamma_{-\infty}$ where Λ is ordered by $\prec_\Lambda$ and Γ is ordered by $\prec_\Gamma$. We may assume that (I.8.9) and (I.8.10) are order bases. We claim that $R\otimes_k S$ is an order domain. To show this define the map

$$\rho_{R\otimes_k S} : \left\{\begin{array}{rcl} \mathcal{B} & \to & \Lambda\oplus\Gamma\\ P_\lambda Q_\gamma + (I+J) & \mapsto & (\rho_R(P_\lambda+I),\rho_S(Q_\gamma+J)).\end{array}\right. \tag{I.8.18}$$

Define an ordering $\prec_{\Lambda\oplus\Gamma}$ on $\Lambda\oplus\Gamma$ by the rule, that $(\lambda_1,\gamma_1)\prec_{\Lambda\oplus\Gamma}(\lambda_2,\gamma_2)$ if and only if one of the following two conditions holds

$$\begin{array}{ll}(1) & \lambda_1\prec_\Lambda\lambda_2\\ (2) & \lambda_1=\lambda_2 \text{ and } \gamma_1\prec_\Gamma\gamma_2.\end{array}$$

The function $\rho_{R\otimes_k S}$ gives an indexing of $\mathcal{B}$. If we can show that the indexed and ordered basis $\mathcal{B}_{\rho_{R\otimes_k S},\prec_{\Lambda\oplus\Gamma}}$ is well-behaving, then it will follow by theorem I.3.18 that $\rho_{R\otimes_k S}$ can be extended to an order function on $R\otimes_k S$. Consider the l-functions l_Λ and l_Γ corresponding to ρ_Λ and ρ_Γ respectively. We will show that the l-function corresponding to $\rho_{R\otimes_k S}$ is

$$l_{\Lambda\oplus\Gamma}:\left\{\begin{array}{lcl}(\Lambda\oplus\Gamma)\times(\Lambda\oplus\Gamma) & \to & (\Lambda\oplus\Gamma)\\ ((\lambda_1,\gamma_1),(\lambda_2,\gamma_2)) & \mapsto & (l_\Lambda(\lambda_1,\lambda_2),l_\Gamma(\gamma_1,\gamma_2))\end{array}\right. \tag{I.8.19}$$

and it will easily follow that $\mathcal{B}_{\rho_{R\otimes_k S},\prec_{\Lambda\oplus\Gamma}}$ is well-behaving, implying that $\rho_{R\otimes_k S}$ can be extended to an order function on $R\otimes_k S$.

To show that $l_{\Lambda\oplus\Gamma}$ truly is the desired l-function, consider the product of two elements in $\mathcal{B}$, say

$$\begin{array}{rl}&\big(P_{\lambda'}Q_{\gamma'}+(I+J)\big)\,\big(P_\lambda Q_\gamma+(I+J)\big)\\ =&(P_{\lambda'}P_\lambda)(Q_{\gamma'}Q_\gamma)+(I+J)\\ =&\Big(\sum\alpha_u P_u\Big)\Big(\sum\beta_v Q_v\Big)+(I+J)\end{array}$$

where $(\sum\alpha_u P_u)(\sum\beta_v Q_v)$ is the unique residue of $(P_{\lambda'}P_\lambda)(Q_{\gamma'}Q_\gamma)$ modulo the Gröbner basis (I.8.14) (or if $I+J=0$ then $(\sum\cdots)(\sum\cdots)=(P_{\lambda'}P_\lambda)(Q_{\gamma'}Q_\gamma)$). But $\sum\alpha_u P_u$ is also the unique residue of $P_{\lambda'}P_\lambda$ modulo the Gröbner basis (I.8.12) (or if $I=0$ then $\sum\cdots=P_{\lambda'}P_\lambda$). And similar $\sum\beta_V Q_v$ is the unique residue of $Q_{\gamma'}Q_\gamma$ modulo the Gröbner basis (I.8.13) (or if $J=0$ then $\sum\cdots=Q_{\gamma'}Q_\gamma$). We conclude that (I.8.19) describes the l-function corresponding to $\rho_{R\otimes_k S}$.

We note that there are many other ways, beside the one described here, to extend the set $\prec_\Lambda$, $\prec_\Gamma$ to an ordering on $\Lambda\oplus\Gamma$, that would lead to order functions on $R\oplus_k S$ (see [13]).

The above construction of a tensor product between two order domains over k is easily generalized to a tensor product between $n\geq 1$ order domains over k. When k is understood from the context we will denote such a product by

$$\otimes_{i=1}^n R_i=R_1\otimes R_2\otimes\cdots\otimes R_n.$$

We note that in this way we have found an easy method to construct sequences

$$(D_1 := R_1 =: \mathbb{F}_q[\boldsymbol{X}^{(1)}]/I^{(1)},\ D_2 := R_1 \otimes R_2 =: \mathbb{F}_q[\boldsymbol{X}^{(1)}, \boldsymbol{X}^{(2)}]/I^{(2)},$$
$$D_3 := R_1 \otimes R_2 \otimes R_3 =: \mathbb{F}_q[\boldsymbol{X}^{(1)}, \boldsymbol{X}^{(2)}, \boldsymbol{X}^{(3)}]/I^{(3)}, \ldots)$$

of order domains, such that $\#\mathcal{V}_{\mathbb{F}_q}(I^{(i)})$ tends to infinity as i tends to infinity. These sequences are interesting as they give rise to infinite sequences of codes of increasing length. We will return to this subject in chapter I.15.

I.8.3 Constructing new order domains by substitution

Given a non algebraically closed field k and an irreducible polynomial $P(T)$ of degree n. Let α be a root of $P(T)$, and consider the field extension $k(\alpha)/k$. Let $F(\boldsymbol{X})$ be a polynomial in $k(\alpha)[X_1, \ldots, X_m]$, and consider elements $\boldsymbol{x} = (x_1, \ldots, x_m) \in \mathcal{V}_{k(\alpha)}(\langle F(\boldsymbol{X})\rangle$. The nature of a field extension $k(\alpha)/k$ ensures that we can write

$$x_i = y_1^{(i)} + y_2^{(i)}\alpha + \cdots + y_n^{(i)}\alpha^{n-1} \tag{I.8.20}$$

uniquely. Expanding the equality $F(x_1, \ldots, x_m) = 0$ by use of the rhs. of (I.8.20), we derive

$$F_1(\boldsymbol{y}) + F_2(\boldsymbol{y})\alpha + \cdots + F_n(\boldsymbol{y})\alpha^{n-1} = 0, \tag{I.8.21}$$

where we have used the notation

$$\boldsymbol{y} = \left(y_1^{(1)}, \ldots, y_n^{(1)}, \ldots, y_1^{(m)}, \ldots, y_n^{(m)}\right).$$

The linearly independence of $1, \alpha, \ldots, \alpha^{n-1}$ implies that

$$F_1(\boldsymbol{y}) = F_2(\boldsymbol{y}) = \cdots = F_n(\boldsymbol{y}) = 0. \tag{I.8.23}$$

Now the idea in this section is to take an order domain $k(\alpha)[X_1, \ldots, X_m]/I$ where

$$I = \langle F^{(1)}(X_1, \ldots, X_m), \ldots, F^{(s)}(X_1, \ldots, X_m)\rangle.$$

Then substitute every X_i with

$$Y_1^{(i)} + Y_2^{(i)}\alpha + \cdots + Y_n^{(i)}\alpha^{n-1}$$

in the defining polynomials to get a new set of polynomials according to (I.8.21) and (I.8.23)

$$F_1^{(1)}(\boldsymbol{Y}), \ldots, F_n^{(1)}(\boldsymbol{Y}), \ldots, F_1^{(s)}(\boldsymbol{Y}), \ldots, F_n^{(s)}(\boldsymbol{Y}).$$

Let $\tilde{I}$ be the ideal in $k[\boldsymbol{Y}]$ defined by these polynomials. Now the hope is that also $k[\boldsymbol{Y}]/\tilde{I}$ is an order domain. We give no arguments why this should actually be the case in general; but only consider two examples.

Example I.8.7
Consider the Hermitian polynomial $H(X_1, X_2) = X_1^{q+1} - X_2^q - X_2$ *over* $\mathbb{F}_{q^2}$. *In the following we will transform the Hermitian order domain* $\mathbb{F}_{q^2}[X_1, X_2]/\langle H\rangle$ *to a new order domain, by introducing new variables related to the field extension* $\mathbb{F}_{q^2}/\mathbb{F}_q$.
Let $P(T) \in \mathbb{F}_q[T]$ *be an irreducible polynomial of degree* 2, *and let* α *be a root of* $P(T)$. *We identify the elements of* $\mathbb{F}_{q^2}$ *with the polynomials in* $\mathbb{F}_q[T]$ *of degree at most* 1 *evaluated in* α. *In the following we will need the fact that* $\alpha^q \notin \mathbb{F}_q \subseteq \mathbb{F}_{q^2}$, *or in other words that* $\alpha^q = a + b\alpha$ *where* $a, b \in \mathbb{F}_q$ *and* b *is nonzero. To see this assume by contrary that* $\alpha^q \in \mathbb{F}_q$. *We have*

$$\begin{array}{c} (\alpha^q)^{q-1} = 1 \\ \Downarrow \\ \alpha^{q^2-q} = 1. \end{array}$$

But at the same time we also have $\alpha^{q^2-1} = 1$. *We conclude that* $\alpha^{q-1} = 1 \Rightarrow \alpha^q = \alpha$. *But* $\alpha \notin \mathbb{F}_q$ *and we have reached a contradiction. We will also need the fact that* $c := \alpha^{q+1} \in \mathbb{F}_q \backslash \{0\}$.

We now introduce new variables X, Y, Z, W *and substitute* X_1 *with* $X + Y\alpha$ *and* X_2 *with* $Z + W\alpha$ *in the defining polynomial* H. *This gives us*

$$\begin{aligned} X_1^{q+1} - X_2^q - X_2 &= \left(X^{q+1} + aXY^q + cY^{q+1} - Z^q - aW^q - Z\right) \\ &\quad + \left(bXY^q + X^qY - bW^q - W\right)\alpha \\ &=: H_1(X, Y, Z, W) + H_2(X, Y, Z, W)\alpha. \end{aligned}$$

From the discussion above we know that $a \in \mathbb{F}_q$ *and* $b, c \in \mathbb{F}_q \backslash \{0\}$. *We will show that* $\mathbb{F}_q[X, Y, Z, W]/\langle H_1, H_2\rangle$ *is an order domain. Let weight vectors be given by*

$$w(X) = (q, 0),\ w(Z) = (q+1, 0),\ w(Y) = (0, q),\ w(W) = (q, 1)$$

and let $\mathbb{N}_0^2$ *be ordered by the standard ordering* $\prec_{st}$. *Now there are precisely two terms in* H_1 *of highest weight, namely*

$$w\left(X^{q+1}\right) = w\left(Z^q\right) = (q^2 + q, 0)$$

and there are also precisely two terms in H_2 *of the highest weight namely*

$$w\left(X^qY\right) = w\left(W^q\right) = (q^2, q).$$

Note that it is crucial here that $b \neq 0$. *We now choose a lexicographic ordering* $\prec_{lex}$ *on* $\mathcal{M}(X, Y, Z, W)$ *with* $X \prec_{lex} Z$ *and* $X, Y \prec_{lex} W$. *Combining*

this with the weights, we get a weighted degree lexicographic ordering $\prec_w$ *on* $\mathcal{M}(X,Y,Z,W)$ *for which* $\mathrm{lm}(H_1) = Z^q$ *and* $\mathrm{lm}(H_2) = W^q$*. As these two leading monomials are relatively prime,* $\{H_1, H_2\}$ *constitute a Gröbner basis with respect to* $\prec_w$*. The footprint is given by*

$$\Delta(I) = \{M \in \mathcal{M}(X,Y,Z,W) \mid \deg_Z(M), \deg_W(M) < q\}.$$

It is easy to see that there is no pair of monomials in $\Delta(I)$ *with the same weight. For the special case* $q = 3$ *the value semigroup* Λ *is illustrated in figure I.8.1. We have shown that* $\mathbb{F}_q[X,Y,Z,W]/\langle H_1, H_2\rangle$ *is an order domain. But so is also* $k[X,Y,Z,W]/\langle H_1, H_2\rangle$ *where* k *is an extension of* $\mathbb{F}_q$*. In particular* $\mathbb{F}_{q^2}[X,Y,Z,W]/\langle H_1, H_2\rangle$ *is an order domain.*

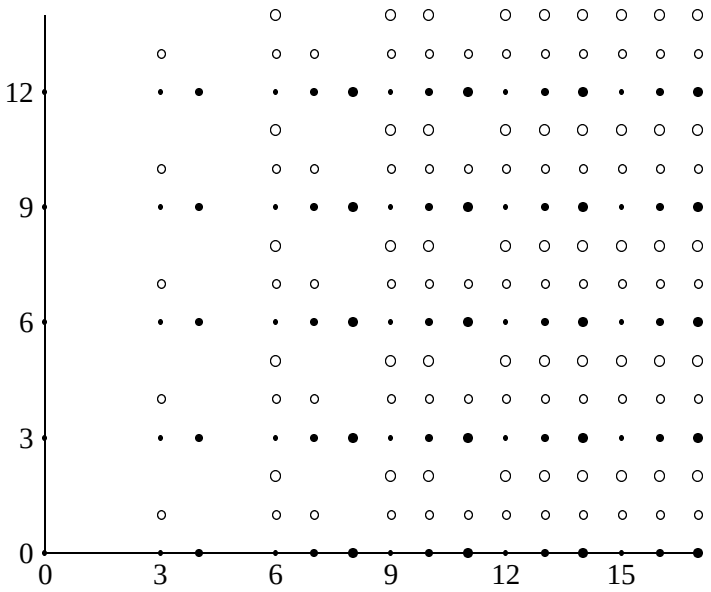

Figure I.8.1: The value semigroup $\Lambda \subseteq \mathbb{N}_0^2$ in the case $q = 3$. Massive small dots correspond to weights of monomials with $\deg_Z = \deg_W = 0$, massive medium dots to $\deg_Z = 1$, $\deg_W = 0$, massive large dots to $\deg_Z = 2$, $\deg_W = 0$, open medium dots to $\deg_W = 1$ and finally open large dots to $\deg_W = 2$.

Example I.8.8
Now assume that we consider $H(X_1, X_2) = X_1^3 - X_2^2 - X_2$ *as a polynomial over the complex numbers* $\mathbb{C}$*. As before* $\mathbb{C}[X_1, X_2]/\langle H\rangle$ *is an order domain.*

Let $\mathbb{C}/\mathbb{R}$ define our substitution, that is substitute X_1 with $X + Yi$ and X_2 with $Z + Wi$, where $i = \sqrt{-1}$. By inserting we get

$$\begin{aligned} X_1^3 - X_2^2 - X_2 &= (X^3 - 3XY^2 - Z^2 + W^2 - Z) \\ &\quad +(3X^2Y - Y^3 + 2ZW - W)i \\ &=: H_1(X, Y, Z, W) + H_2(X, Y, Z, W)i. \end{aligned}$$

We will show that the situation is more complicated than in example I.8.7. That is, we will show that there does not exist a weighted degree lexicographic ordering on $\mathcal{M}(X, Y, Z, W)$, such that $\{H_1, H_2\}$ is a Gröbner basis that satisfies the conditions in theorem I.7.1.
Assume that such one did exist. Then the set of monomials of highest weight in H_1 could be either $\{X^3, Z^2\}$, $\{X^3, W^2\}$, $\{XY^2, Z^2\}$ or $\{XY^2, W^2\}$. And the set of monomials of highest weight in H_2 could be either $\{X^2Y, ZW\}$ or $\{Y^3, ZW\}$. This gives us eight combinations to check.
Case I: Assume that the sets are $\{X^3, Z^2\}$ for H_1 and $\{X^2Y, ZW\}$ for H_2. Then $w(XY^2) = w(W^2)$. But this by assumption does not hold as both XY^2 and W^2 are in the footprint no matter which lexicographic ordering is chosen.
Case II: Assume that the sets are $\{X^3, Z^2\}$ for H_1 and $\{Y^3, ZW\}$ for H_2. Now from H_1 we get $w(y) < w(x)$ and from H_2 we get $w(x) < w(y)$, a contradiction.
Case III: Assume that the sets are $\{XY^2, Z^2\}$ for H_1 and $\{Y^3, ZW\}$ for H_2. We must have $w(W) < w(Z)$ and also $w(X) < w(Y)$. This gives us $w(XY^2) < w(Y^3) < w(Z^2)$, a contradiction.
Going through the remaining five cases one finds contradictions like the ones described above. We conclude that we must look for a weighted lexicographic ordering for which $\{H_1, H_2\}$ is not a Gröbner basis. Especially we must look for an ordering such that $\mathrm{lm}(H_1)$ and $\mathrm{lm}(H_2)$ are not relatively prime. Given all the possible sets of such leading monomials one could, in each case try, to add new polynomials to the basis using Buchberger's algorithm. However the complexity of such a search algorithm is relatively high, if it is to be done by hand.

I.9

The nature of the value semigroup of a weight function

Consider a weight function

$$\rho : R \to \Lambda_{-\infty} \subseteq \mathbb{N}_0^r \cup \{-\infty\}$$

(Λ ordered by some monomial ordering). We may assume that ρ is chosen from the set of weight functions, in a given equivalence class of order functions in a way s.t. r is minimal. In all the examples of weight functions that we have considered up to now we have had $r = \mathrm{trdg}(R)$. This result may very well hold in general whenever Λ is finitely generated. However at this moment only the following result is proved to hold. Namely that the value semigroup of a weight function can not be contained in $\mathbb{N}_0 \cup \{-\infty\}$, whenever the transcendence degree of the related order domain exceeds 1.

Theorem I.9.1
Given an order domain R of transcendence degree at least 2, with a weight function $\rho : R \to \Lambda_{-\infty}$. Then Λ is not isomorphic to a subspace of $\mathbb{N}_0$.

Proof:
Let x_1, x_2 be two elements in a transcendence basis for R. We have $k[x_1, x_2] \subseteq R$. Consider the restriction of ρ and Λ, that is consider $\rho' : k[x_1, x_2] \to \Lambda'$. Assume in the rest of this proof that $\Lambda' \subset \mathbb{N}_0$. We will show that this assumption leads to a contradiction, and the theorem will be proved. The contradiction is a consequence of the following fact (which we are going to prove).

Fact:
Consider the weighted degree function wdeg *on* $k[x_1, x_2]$ *induced by the weights* $w(x_1) = \rho(x_1)$ *and* $w(x_2) = \rho(x_2)$. *Under the assumption* $\Lambda' \subseteq \mathbb{N}_0$ *there exists an infinite sequence* $(x_1, f_1 := x_2, f_2, f_3, \ldots)$ *of elements in* $k[x_1, x_2]$ *such that*

$$\frac{\rho(f_i)}{\mathrm{wdeg}(f_i)} > \frac{\rho(f_{i+1})}{\mathrm{wdeg}(f_{i+1})}, \qquad i \geq 1 \tag{I.9.1}$$

$$\rho(f_i) \notin \langle \rho(x_1), \rho(f_1), \rho(f_2), \ldots, \rho(f_{i-1}) \rangle, \qquad i \geq 2. \tag{I.9.2}$$

Before proving this fact, let us investigate the contradiction. It goes as follows. From (I.9.2) we conclude that Λ' can not be finitely generated, but on the other hand every semigroup of $\mathbb{N}_0$ is known to be finitely generated.

Now let us turn to the proof of the fact. We show by an induction proof, that (I.9.1) and (I.9.2) are satisfied for every sub sequence $(x_1, f_1 := x_2, f_2, f_3, \ldots, f_n)$, $n \geq 2$.

Initial step (n=2):
Define $a_0 := \rho(x_1)$, $a_1 := \rho(x_2)$. Now $\rho(x_1^{a_1}) = \rho(x_2^{a_0})$, so a $\lambda_1^{(1)} \in k\backslash\{0\}$ exists, such that $g_2^{(1)} := x_1^{a_1} + \lambda_1^{(1)} x_2^{a_0}$ satisfies $0 < \rho(g_2^{(1)}) < \rho(x_1^{a_1})$. Note that $\mathrm{wdeg}(g_2^{(1)}) = \mathrm{wdeg}(x_1^{a_1})$. Now if $\rho(g_2^{(1)}) \notin \Lambda_1' := \langle a_0, a_1\rangle$ then we choose $f_2 := g_2^{(1)}$. If on the other hand $\rho(g_2^{(1)})$ is already contained in Λ_1', then it is because there exist $\alpha_1^{(2)}, \alpha_2^{(2)} \geq 0$, not both zero, such that $\rho(g_2^{(1)}) = \rho(x_1^{\alpha_1^{(2)}} x_2^{\alpha_2^{(2)}})$. But then for some $\lambda_1^{(2)} \in k\backslash\{0\}$, $g_2^{(2)} := g_2^{(1)} + \lambda_1^{(2)} x_1^{\alpha_1^{(2)}} x_2^{\alpha_2^{(2)}}$ satisfies $0 < \rho(g_2^{(2)}) < \rho(g_2^{(1)})$. Note that again $\mathrm{wdeg}(g_2^{(2)}) = \mathrm{wdeg}(x_1^{a_1})$. If $\rho(g_2^{(2)})$ is not contained in Λ_1', we chose $f_2 := g_2^{(2)}$. If this is however not the case, we continue the process as above, by finding new $\alpha_1^{(i)}, \alpha_2^{(i)}$ and $\lambda_1^{(i)}$, and define new $g_2^{(i)}$ from the old ones, as long as possible. In every run the order of the candidate for f_2 (that is the order of $g_2^{(i)}$) discrease strictly, but never attains zero, as the weighted degree of every candidate will be equal to $\mathrm{wdeg}(x_1^{a_1})$. This means especially that the process will eventually stop. That is an $s \geq 1$ exists, such that $f_2 := g_2^{(s)}$ satisfies (I.9.2). Combining $\rho(f_2) < \rho(x_2^{a_0})$ with $\mathrm{wdeg}(f_2) = \mathrm{wdeg}(x_2^{a_0})$ we see that (I.9.1) is satisfied as well.

Induction step:
Assume a subset

$$\{x_1, f_1 := x_2, f_2, \ldots, f_n\} \subseteq k[x_1, x_2] \tag{I.9.3}$$

is given such that (I.9.1) and (I.9.2) holds. We will show that an element $f_{n+1} \in k[x_1, x_2]$ exists, such that

$$\rho(f_{n+1}) \notin \Lambda_n' := \langle \rho(x_1), \rho(x_2), \rho(f_2), \ldots, \rho(f_n)\rangle \tag{I.9.4}$$

and such that

$$\frac{\rho(f_n)}{\mathrm{wdeg}(f_n)} > \frac{\rho(f_{n+1})}{\mathrm{wdeg}(f_{n+1})}. \tag{I.9.5}$$

Denote $a_n := \rho(f_n)$. Now $\rho(f_n^{a_1}) = \rho(x_1^{a_n})$ and there exists $\lambda_n^{(1)} \in k\backslash\{0\}$ such that $g_n^{(1)} := f_n^{a_1} + \lambda_n^{(1)} x_1^{a_n}$ satisfies $0 < \rho(g_n^{(1)}) < \rho(f_n^{a_1})$. Note that $\mathrm{wdeg}(g_n^{(1)}) = \mathrm{wdeg}(f_n^{a_1})$, follows from the induction hypothesis that (I.9.1) holds in (I.9.3). If $\rho(g_n^{(1)}) \notin \Lambda'_n$, then we define $f_{n+1} := g_n^{(1)}$, and (I.9.4) is satisfied. If this is not the case, then it is because there exist $\beta_1^{(2)}, \beta_2^{(2)}, \gamma_2^{(2)}, \ldots, \gamma_n^{(2)} \geq 0$, not all zero, such that

$$\rho(x_1^{\beta_1^{(2)}} x_2^{\beta_2^{(2)}} f_2^{\gamma_2^{(2)}} \ldots f_n^{\gamma_n^{(2)}}) = \rho(g_n^{(1)}).$$

But then also a $\lambda_n^{(2)} \in k\backslash\{0\}$ exists such that

$$g_n^{(2)} := g_n^{(1)} + \lambda_n^{(2)} x_1^{\beta_1^{(2)}} x_2^{\beta_2^{(2)}} f_2^{\gamma_2^{(2)}} \ldots f_n^{\gamma_n^{(2)}}$$

satisfies $0 < \rho(g_n^{(2)}) < \rho(g_n^{(1)})$. Note again that $\mathrm{wdeg}(g_n^{(2)}) = \mathrm{wdeg}(f_n^{a_1})$. If $\rho(g_n^{(2)}) \notin \Lambda'_n$, then we chose $f_{n+1} := g_n^{(2)}$. If not we continue the process (just as in the initial step), by finding new $\beta_1^{(i)}, \beta_2^{(i)}, \gamma_2^{(i)}, \ldots, \gamma_n^{(i)}$ and $\lambda_n^{(i)}$ and defining new $g_n^{(i)}$ from the old ones, as long as possible. In every run the order of the candidate for f_{n+1} (that is the order of $g_n^{(i)}$) discrease strictly, but never attains zero, as the weighted degree of every candidate will be equal to $\mathrm{wdeg}(f_n^{a_1})$. Just as in the initial step there exists a s such that $f_{n+1} := g_n^{(s)}$ satisfies (I.9.4) and (I.9.5). This concludes the proof of the fact, and thereby the proof of the theorem. □

In particular we have the following result.

Proposition I.9.2
A nontrivial order domain R, that possesses a weight function ρ with value semigroup contained in $\mathbb{N}_0 \cup \{-\infty\}$, must be of transcendence degree 1. Up to equivalence R does not possess any other weight function with value semigroup contained in $\mathbb{N}_0 \cup \{-\infty\}$. If ρ' is a weight function not equivalent to ρ, then the value semigroup Λ' of ρ' cannot be finitely generated.

Proof:
The first part is a consequence of theorem I.9.1 and remark I.3.11. The second is a consequence of lemma I.3.42. To see the last part note the following. Assume that ρ' is a weight function that is not equivalent to ρ. Given any two elements $X, Y \in R$ then a nonzero polynomial $P \in k[T_1, T_2]$ exists, s.t. $P(X, Y) = 0$ in R. Now $P(X, Y)$ viewed as a polynomial in X, Y must contain two different monomials, say $X^a Y^b$ and $X^c Y^d$, st. $\rho'(X^a Y^b) = \rho'(X^c Y^d)$. If Λ'

is finitely generated, then we have $\Lambda' \subseteq \mathbb{N}_0 \cup \{-\infty\}$, which is impossible by part two of the proposition. We conclude that Λ' cannot be finitely generated. $\square$

The proof of theorem I.9.1 was developed before (and thereby independently of) the appearance of [31] and [26]. Theorem I.9.1 corresponds to the result in [31], that a discrete valuation on a field K/k of transcendence degree 2 does not correspond to an order function (see section I.10.1). And it corresponds to the result in [26] that if an order domain R possesses a weight function $\rho : R \to \Lambda_{-\infty}$, with $\Lambda \subseteq \mathbb{N}_0$, then the transcendence degree of $\mathrm{Quot}(R)$ is 1.

The following surprisingly example of a weight function on $k[X_1, X_2]$ is strongly related to the proof of theorem I.9.1. Actually it has been used as inspiration to develop the proof of theorem I.9.1. It was first presented at the Winter School of Coding Theory in Ebeltoft dec. 1998. In this material we will present the weight function using Pellikaan's factor ring theorem, although it was not from that it was developed in the first place.

Example I.9.3
Consider the order domain $k[X_1, X_2]$. The well-known weight function induced by $\rho'(X_1) = (1, 0)$, $\rho'(X_2) = (0, 1)$, and by some monomial ordering $\prec_{\mathbb{N}_0^2}$ on $\mathbb{N}_0^2$ has the property that no pair of different monomials has the same order. In the following we will give examples of order functions on $k[X_1, X_2]$, with the remarkable property that there exist pairs of different monomials that are of the same order. To develop these order functions, we first consider the order domain $k[Y_1, Y_2, Y_3]/I$, where $I := \langle Y_1^2 - Y_2^3 - Y_3 \rangle$. We will use the isomorphism

$$k[Y_1, Y_2, Y_3]/I \simeq k[X_1, X_2] \tag{I.9.8}$$

given by $Y_1 + I \mapsto X_1$, $Y_2 + I \mapsto X_2$ and $Y_3 + I \mapsto X_1^2 - X_2^3$. That is, we will construct an order function on $k[Y_1, Y_2, Y_3]/I$, and then use the isomorphism to translate it to an order function on $k[X_1, X_2]$.
Let weights be given by $w(Y_1) = (3, 0)$, $w(Y_2) = (2, 0)$, $w(Y_3) = (0, 1)$ and let $\mathbb{N}_0^2$ be ordered by $\prec_{st}$. Choose lexicographic ordering $Y_3 \prec_{lex} Y_2 \prec_{lex} Y_1$. As usual we define $\prec_w$ to be the induced weighted degree lexicographic ordering on $k[Y_1, Y_2, Y_3]$. This gives us $\mathrm{lm}(Y_1^2 - Y_2^3 - Y_3) = Y_1^2$ and $\Delta(\langle Y_1^2 - Y_2^3 - Y_3 \rangle) = \{\boldsymbol{Y}^{\boldsymbol{\alpha}} \mid \alpha_1 < 2\}$. We easily see that the conditions in theorem I.7.1 are satisfied. Let ρ be the corresponding weight function, with order basis $\{\boldsymbol{Y}^{\boldsymbol{\alpha}} + I \mid \alpha_1 < 2\}$. The isomorphism (I.9.8) now corresponds to the fact that $\{X_1^{\alpha_1} X_2^{\alpha_2} (X_1^2 - X_2^3)^{\alpha_3} \mid \alpha_1 < 2\}$ is a basis for $k[X_1, X_2]$. The isomorphism immediately gives us an order function ρ on $k[X_1, X_2]$ that is induced by $\rho(X_1) = (3, 0)$, $\rho(X_2) = (2, 0)$ and $\rho(X_1^2 - X_2^3) = (0, 1)$. This order function has the property $\rho(X_1^2) =$

$\rho(X_2^3)$.
In the above case $\rho(X_1^2 - X_2^3) \prec_{st} \rho(X_1), \rho(X_2)$. *But if we instead from the beginning choose* $w(Y_3 + I) = (0, 6)$, *we will get an order function* ρ *on* $k[X_1, X_2]$ *with* $\rho(X_1) \prec_{st} \rho(X_2) \prec_{st} \rho(X_1^2) \prec_{st} \rho(X_1X_2) \prec_{st} \rho(X_1^3 + X_2^2) \prec_{st} \rho(X_1^3), \rho(X_2^2) \prec_{st} \ldots$. *By choosing in turn* $w(Y_3 + I) = (0, 1)$, $(0, 2)$, $(0, 3)$, $(0, 4)$, $(0, 5)$, $(0, 6)$ *we get basically different order functions.*
Now let us restrict ρ *to the subring* $k[Z_1 := X_1, Z_2 := X_1^2 - X_2^3] \subsetneq k[X_1, X_2]$. *Of course no pair of monomials in* Z_1 *and* Z_2 *has the same order. So* $k[X_1, X_2]$ *contains two (*$= \operatorname{trdg}(k[X_1, X_2])$*) relatively transcendental elements with the considered property, but it is not* X_1, X_2.

Example I.9.4
This is a continuation of example I.9.3. Order $\mathbb{N}_0^2$ *by* $\prec_{st}$ *and consider the weight function induced by*

$$\rho(X) = (2, 0), \quad \rho(Y) = (3, 0), \quad \rho(X^3 + Y^2) = (0, 6).$$

The first three elements of any well-behaving sequence for $k[X, Y]$ *wrt.* ρ *is of the form*

$$\begin{aligned} f_1 &= a_1, \\ f_2 &= b_2X + b_1, \\ f_3 &= c_3Y + c_2X + c_1, \end{aligned}$$

where $a_i, b_i, c_i \in k$ *and* a_1, b_2, c_3 *are all nonzero. Now* $\rho(f_2^3) = \rho(f_3^2)$ *independently of the actual values of the coefficients* a_i, b_i, c_i. *Assume there exists an order basis* $\mathcal{B}$ *with respect to* ρ *that is closed under multiplication. But then we must have*

$$f_2^3 = f_3^2 \in \mathcal{B}. \tag{I.9.9}$$

However f_3^2 *contains the nonzero term* $c_3^2Y^2$ *whereas* f_2^3 *contains no term with with* Y^2. *Therefore* $k[X, Y]$ *does not possess any order basis with respect to* ρ *that is closed under multiplication. Or in other words,* ρ *does not possess any order basis* $\mathcal{B}$ *such that* $(\mathcal{B}, \cdot, 1)$ *is a semigroup. This example fills in a gap, we had in section I.3.3.*

From [31] we have the following definition.

Definition I.9.5
Assume R *is an order domain of transcendence degree* r *with an order function* ρ. *Then* ρ *is said to be monomial if there exists a transcendence basis* $\{z_1, \ldots, z_r\}$ *for* R *such that any two different monomials in* $z_1, \ldots, z_r$ *are of different orders.*

Example I.9.6
The weight functions from example I.9.3 are monomial.

The following conjecture is due to Ruud Pellikaan.

Conjecture I.9.7
Let R be an order domain of transcendence degree r. If $\rho : R \to \Lambda_{-\infty}$ is a weight function and Λ is finitely generated, then Λ is isomorphic to a subspace of $\mathbb{N}_0^r$ but not to a subspace of $\mathbb{N}_0^{r-1}$.

If conjecture I.9.7 holds, then an immediate consequence will be the following proposition.

Proposition I.9.8
If $\rho : R \to \Lambda_{-\infty}$ is an order function and Λ is finitely generated then ρ is monomial.

In [31, Ex. 5.2] O'Sullivan uses algebraic geometry techniques to give an example of a non monomial order function corresponding to a valuation

$$v : k(X, Y)\backslash\{0\} \to \Gamma \subseteq \mathbb{Q}.$$

In the structure this example resembles example I.9.3 very much. However the proof needed to show [31, Ex. 5.2] is very different from the proof in example I.9.3. From the appearance of O'Sullivan's example we conclude that the condition in conjecture I.9.7, that Λ is finitely generated, is crucial. However example I.4.3 shows that it is not in general a necessary condition.

I.10
Every weight function is a valuation

In this chapter we first treat the general concept of valuations and corresponding valuation rings. It will become clear that there is a strong connection between order domain theory and valuation theory. Actually all weight functions are valuations. However not all valuations are weight functions. In the second part of this chapter we concentrate on the valuations corresponding to order domains of transcendence degree 1.

I.10.1 Valuations in general

The definitions in this section are from [46]. In the following K and k will always be fields and by K/k we will as usual denote a field K that contains k as a subfield. We have the following definition of a valuation on K/k.

Definition I.10.1
Let v be a map from $K\backslash\{0\}$ to an additive abelian group Γ that is ordered totally by $\prec$. If $k \subset K$ and if for every $f, g \in K\backslash\{0\}$ and every $c \in k\backslash\{0\}$ one has

$$\begin{aligned} v(fg) &= v(f) + v(g) && \text{(I.10.1)} \\ v(f+g) &\succeq \min\{v(f), v(g)\} && \text{(I.10.2)} \\ v(c) &= 0 && \text{(I.10.3)} \end{aligned}$$

then v is called a valuation on K/k.

We will say that two valuations $v : K\backslash\{0\} \to \Gamma$ and $v' : K\backslash\{0\} \to \Gamma'$ are equivalent if an order preserving isomorphism $\varphi : \Gamma \to \Gamma'$ exists, such that $v'(f) = \varphi(v(f))$. The set of valuations on K/k is nonempty as it will always contain the trivial valuation corresponding to $\Gamma = \{0\}$. Condition (I.10.1) ensures that $v(1) = 0$, and it follows that condition (I.10.3) can be skipped when k is a finite field. We can wlog. assume that the map v is surjective.

We next list some important consequences of (I.10.1)-(I.10.3). Given $f, g \in K\backslash\{0\}$ and $c \in k\backslash\{0\}$ then

$$\begin{aligned} v(f) &= v(cf) && \text{(I.10.4)} \\ v(f) &= -v(f^{-1}) && \text{(I.10.5)} \\ v(f+g) &= v(f) \text{ if } v(f) \prec v(g). && \text{(I.10.6)} \end{aligned}$$

A valuation defines a so-called valuation ring.

Definition I.10.2
Let v be a valuation on K/k. The substructure of K/k given by

$$\mathcal{O}_v := \{f \in K\backslash\{0\} \mid v(f) \succeq 0\} \cup \{0\} \qquad \text{(I.10.7)}$$

is called a valuation ring.

Note that surely $\mathcal{O}_v$ is a ring, and that if $f \in K\backslash\mathcal{O}_v$ then necessarily $f^{-1} \in \mathcal{O}_v$. $\mathcal{O}_v$ has a unique maximal ideal, namely the set

$$P_v := \{f \in K\backslash\{0\} \mid v(f) \succ 0\} \cup \{0\} \qquad \text{(I.10.8)}$$

of all non units in $\mathcal{O}_v$. As P_v is a maximal ideal, $\mathcal{O}_v/P_v$ is a field. It is clear from (I.10.6) that $\mathcal{O}_v/P_v$ contains k as a subfield.

As mentioned above $\mathcal{O}_v$ has the property that if $f \in K\backslash\mathcal{O}_v$ then $f^{-1} \in \mathcal{O}_v$. The next theorem states that this property actually is a sufficient condition for a subring R, $k \subseteq R \subseteq K$, to be a valuation ring.

Theorem I.10.3
Let R be a ring, $k \subseteq R \subseteq K$, such that $f \in K\backslash R$ implies $f^{-1} \in R$. Then there exists a valuation v on K/k such that $R = \mathcal{O}_v$.

Proof:
See [46]. □

Recall that O'Sullivan only considers order functions where $\Lambda \subseteq \mathbb{N}_0$. In [30] O'Sullivan shows the following very important theorem.

Theorem I.10.4
Let R be a finitely generated domain over k with order function o (of O'Sullivan's type), and let K be the quotient field of R. Then there exists a valuation on K/k such that if $f, g \in R\backslash\{0\}$ are any elements s.t. $o(f) < o(g)$ then necessarily $v(f) \succ v(g)$.

The fact that the value set, Λ of o, is ordered isomorphic to $\mathbb{N}_0$ is not used in O'Sullivan's proof, so his result generalizes to the more general set-up from [13]. In the language of [13] and of this thesis, theorem I.10.4 becomes.

Theorem I.10.5
Let R be a finitely generated order domain over k with a weight function $\rho : R \to \Lambda_{-\infty}$. Let $\Gamma := D(\Lambda)$ be the group of differences according to definition I.2.3. And denote $K := \mathrm{Quot}(R)$. There exists an, up to equivalence unique, valuation $v : K\backslash\{0\} \to D(\Lambda)$ such that if $f \in R \subseteq K$ is non zero then $\rho(f) = -v(f)$.

So an order function defines a valuation. However the opposite is not true in general. In [31] O'Sullivan notes that there exist valuations on $k(X, Y)$ with $\Gamma \subseteq \mathbb{Z}_0$. And he shows that such a valuation does not define any order function (alternatively consult theorem I.9.1 for this fact). Clearly the equivalence relation from this section on the set of valuations corresponds to the equivalence relation from section I.3.3 on the set of order functions.

As already noted in section I.3.3, O'Sullivan in his papers, treats the order functions on the polynomial ring $k[X_1, \ldots, X_m]$, that has the set of monomials in $X_1, \ldots, X_m$ as an order basis. Beside these order functions, he also describes several other order functions on k-algebras of transcendence degree more than 1. All of these descriptions involves more or less complicated methods from the theory of algebraic geometry.

I.10.2 Algebraic function fields of one variable

In this section we will see that certain well-studied structures related to algebraic function fields of one variable are order domains. To be more precise we will see, that the union of the so-called $\mathcal{L}$-spaces, corresponding to a single rational place, is an order domain. The treatment of these structures has been postponed to this relatively late point of the thesis, as it is the authors policy, that order domain theory should be understandable also for readers without knowledge of algebraic geometry and algebraic function field theory. Historically however, these structures play a significant role as one of the major motivation to introduce the concept of order functions (see [6], [20], [21] and [33]). It is beyond the scope of this thesis to give an introduction to the theory of algebraic function fields of one variable. So the purpose of this section is, to give an overview of the connection between order domain theory and the theory of algebraic function fields of one variable, for the reader that has some experience with the later.

We refer to [38] for a nice and general description of the theory of algebraic function fields of one variable. In the following we state some of the, for our purpose, most important results from [38].

Definition I.10.6
An algebraic function field $\mathcal{F}$ of one variable over the field k is an extension field $\mathcal{F} \supseteq k$, such that $\mathcal{F}$ is a finite algebraic extension of $k(x)$ for some element $x \in \mathcal{F}$ which is transcendental over k.

We will sometimes refer to an algebraic function field simply as a function field. The reader familiar with [4] should be careful, as the definition of a function field given there, does not match the above definition. In the remaining part of this section all considered algebraic function fields are assumed to be of one variable.

The valuations on the function fields of the above type are so-called discrete valuations. That is, the abelian group $(\Gamma, +)$ from definition I.10.1 is a subgroup of $(\mathbb{Z}, +)$ (here $+$ is the usual plus). We extend the valuations v to all of K by the assignment $v(0) = \infty$. A valuation is uniquely specified by its valuation ring or equivalent by the maximal ideal of the valuation ring, the last being called a place. This justifies why we speak about the valuation v_P corresponding to the place P, and why we use the following notation for a valuation ring and its maximal ideal

$$\begin{aligned} \mathcal{O}_P &:= \{f \in \mathcal{F} \mid v_P \geq 0\} \\ P &:= \{f \in \mathcal{F} \mid v_P > 0\}. \end{aligned}$$

Now $\mathcal{O}_P/P$ is a finite dimensional vector space over k and the degree of the place P is defined to be

$$\deg(P) := \dim_k(\mathcal{O}_P/P).$$

If $\deg(P) = 1$ then we call P a rational place. We denote by $\boldsymbol{P}_{\mathcal{F}}$ the set of places in the function field $\mathcal{F}$. A divisor is by definition a linear combination

$$A = \sum_{\substack{n_P \in \mathbb{Z} \\ P \in \boldsymbol{P}_{\mathcal{F}}}} n_P P \tag{I.10.9}$$

where only finitely many of the n_P's are nonzero. The degree of a divisor is defined by $\deg(A) := \sum n_P \deg(P)$. To every divisor corresponds a so-called $\mathcal{L}$-space defined by

$$\mathcal{L}(A) := \{x \in \mathcal{F} \mid v_P(x) \geq -n_P, \text{ for all } P \in \boldsymbol{P}_{\mathcal{F}}\}.$$

The name $\mathcal{L}$-space is motivated by the fact that $\mathcal{L}(A)$ is a finite dimensional vector space over k. We denote by $\dim(A)$ the dimension of this vector space. As for any place P, $v_P(x) = 0$ whenever $x \in k\backslash\{0\}$, we see that k is contained in $\mathcal{L}(A)$, precisely when all the n_P's in the linear combination (I.10.9) are non-negative. One of the most important parameters of an algebraic function field is the genus g. The genus is a non negative integer, that is equal to zero if and only if $\mathcal{F}$ is isomorphic to the quotient field $k(x)$.

A celebrated result is the so-called Riemann-Roch theorem that relates the degree of A with the dimension of $\mathcal{L}(A)$. It uses the notion of a canonical divisor W. We will not explain what a canonical divisor W is, but only mention the important result that $\dim(W - A) = 0$ whenever $\deg(A) \geq 2g - 1$. We now state the Riemann-Roch theorem.

Theorem I.10.7
Let W be a canonical divisor, then for any divisor A we have

$$\dim(A) = \deg(A) + 1 - g + \dim(W - A).$$

Combining the Riemann-Roch theorem with the following lemma one gets the important Weierstrass Gap theorem.

Lemma I.10.8
Let $A = \sum n_P P$ and $B = \sum n'_P P$ be divisors of $\mathcal{F}$ with $n_P \leq n'_P$ for all P. Then

$$\dim(B) - \dim(A) \leq \deg(B) - \deg(A).$$

Before stating Weierstrass Gap theorem, we must introduce the so-called pole numbers related to a place. Let P be a place. An integer $n \geq 0$ is called a pole number of P if and only if there exists an element $x \in \mathcal{F}$ with $v_P(x) = n$ and $v_Q(x) \geq 0$ for all $Q \in \boldsymbol{P}_{\mathcal{F}}\backslash\{P\}$. The numbers in $\mathbb{N}_0$, that are not pole numbers, are called gaps. The set of gaps defines a semigroup, this semigroup is called the Weierstrass semigroup corresponding to P. We now state Weierstrass Gap theorem.

Theorem I.10.9
Let $\mathcal{F}$ be a function field with genus $g > 0$, and let P be a rational place in $\boldsymbol{P}_{\mathcal{F}}$. Then there are exactly g gap numbers $i_1 < \cdots < i_g$ of P. We have $i_1 = 1$ and $i_g \leq 2g - 1$.

So if P is a rational place with gap numbers $\{i_1, \ldots, i_g\}$ then

$$\dim(mP) = \dim((m-1)P)$$

whenever m is a gap number. And

$$\dim(mP) = \dim((m-1)P) + 1$$

whenever $m \geq 0$ is not a gap number. So the first part of the following proposition is obvious.

Proposition I.10.10
Let P be a rational place in a function field $\mathcal{F}$. Then $R := \cup_{m=0}^{\infty} \mathcal{L}(mP)$ is an order domain with a weight function

$$\rho : \begin{cases} R & \to & \mathbb{N}_0 \setminus \{i_1, \ldots, i_g\} \cup \{-\infty\} \\ x & \mapsto & -v_P(x). \end{cases} \tag{I.10.11}$$

Conversely let R/k be any order domain with a weight function

$$\rho : R \to \Lambda_{-\infty} \subseteq \mathbb{N}_0 \cup \{-\infty\}$$

then there exists a description $R = k[X_1, \ldots, X_m]/I$, such that the quotient field $\mathcal{F} := \mathrm{Quot}(R)$ is an algebraic function field (of one variable), with a unique place P at infinity, and this place satisfies (I.10.11).

Proof:
For a proof of the last part see [26, Th. 1]. □

Consider an algebraic function field

$$\mathrm{Quot}\left(k[X_1, \ldots, X_m]/I\right). \tag{I.10.12}$$

Denote $x_i = X_i + I$, $i = 1, \ldots, m$. Of particular interest is the situation where a place P satisfies $v_P(x_i) < 0$, $i = 1, \ldots, m$, and $v_Q(x_i) \geq 0$ for all $Q \neq P$ and $i = 1, \ldots, m$. We say that P is the only place at infinity, and denote it by $P = P_\infty$. Now any polynomial $f(x_1, \ldots, x_m)$ satisfies $v_{P_\infty}(f(x_1, \ldots, x_m)) \leq 0$ and $v_Q(f(x_1, \ldots, x_m) \geq 0$ for $Q \neq P_\infty$. So

$$k[X_1, \ldots, X_m]/I \subseteq \bigcup_{m=0}^{\infty} \mathcal{L}(mP_\infty). \tag{I.10.13}$$

Although we often have equality in (I.10.13) in our examples, it also sometimes happens that (I.10.13) is satisfied with a strict inclusion.

Example I.10.11
Consider the algebraic function field $\mathrm{Quot}\left(k[X,Y]/\langle X^3 - Y^2\rangle\right)$. *There is only one place at infinity, it is rational and* $v_{P_\infty}(x) = -2$, $v_{P_\infty}(y) = -3$. *Now* $v_{P_\infty}(y/x) \geq 0$ *for all* $Q \neq P_\infty$. *So*

$$k[X,Y]/\langle X^3 - Y^2\rangle \subsetneq \bigcup_{m=0}^{\infty} \mathcal{L}(mP_\infty)$$

that is the quotient ring is a strict sub order domain of the union of the $\mathcal{L}$*-spaces. Note that the considered algebraic function field is isomorphic to the rational function field. A similar situation, as the one described above, occurs whenever* $\mathrm{Quot}\left(k[X_1,\ldots,X_m]/I\right)$ *is of transcendence degree* 1*, and* I *is a toric ideal.*

So far we have taken the algebraic point of view on algebraic function fields. We now discuss some more geometric features that will be important, when we are to construct codes. In the following $\mathbb{A}_k^m$ denotes the m-dimensional affine space over k, and $\mathbb{P}_k^m$ the m-dimensional projective space over k. As usual $\bar{k}$ denotes the algebraic closure of k. If $I = \langle F_1(\boldsymbol{X}),\ldots,F_s(\boldsymbol{X})\rangle \subseteq k[\boldsymbol{X}]$ is an ideal, then we denote $\bar{I} := \langle F_1(\boldsymbol{X}),\ldots,F_s(\boldsymbol{X})\rangle \subseteq \bar{k}[\boldsymbol{X}]$. The irreducible affine variety $\bar{V} := \mathcal{V}_{\bar{k}}(\bar{I}) \subseteq \mathbb{A}_{\bar{k}}^m$ corresponding to a function field of one variable is called an affine curve (or simply a curve). Now homogenizing the defining polynomials $F_1,\ldots,F_s$ we get a projective variety $\bar{V}^{\mathbb{P}} \subseteq \mathbb{P}_{\bar{k}}^m$, that contains (the image) of $\bar{V}$. We call $\bar{V}^{\mathbb{P}}$ a projective curve (or the projective curve corresponding to $\bar{V}$). In the following we will, when we a little incorrectly talk about a curve $F(X,Y)$, mean the corresponding projective variety. A point $p \in \bar{V}$ ($p \in \bar{V}^{\mathbb{P}}$) is called nonsingular, if the slope of $\bar{V}$ (or equivalent of $\bar{V}^{\mathbb{P}}$) at p is well-defined. If not, then it is called singular. Consider the following three cases.

Case I
$p \in \bar{V} = \bar{V}^{\mathbb{P}} \cap \mathbb{A}_k^m$ is nonsingular. Now

$$\mathcal{O}_P = \{f \in \mathcal{F} \mid f = g/h \text{ with } g,h \in k[\boldsymbol{X}]/I \text{ and } h(p) \neq 0\} \quad \text{(I.10.15)}$$

is a valuation ring with maximal ideal (place)

$$P = \{f \in \mathcal{F} \mid f = g/h \text{ with } g,h \in k[\boldsymbol{X}]/I \text{ and } h(p) \neq 0 \text{ and } g(p) = 0\}. \quad \text{(I.10.16)}$$

Important facts are that P is rational and that $k[\boldsymbol{X}]/I \subseteq \mathcal{O}_P$.

Case II
$p \in \bar{V}^{\mathbb{P}} \cap (\mathbb{P}_k^m \backslash \mathbb{A}_k^m)$ is nonsingular. We call p a point at infinity. A generalization of (I.10.15) and (I.10.16) defines a unique valuation ring with corresponding

place. But in this case there exist elements $f \in k[\boldsymbol{X}]/I$ such that $v_P(f) < 0$.

Case III
$p \in \bar{V}^{\mathbb{P}}$ is singular. The blow-up algorithm (see [24]) gives us the places that corresponds to p. We can not say in advance, how many and of which degrees these places will be.

The very important fact is, that the cases I,II and III together, gives us all the rational places of $\boldsymbol{P}_{\mathcal{F}}$, and that a rational place corresponds to exactly one (not more) point. The situation is particular simple for curves that contains no singular points. These curves are called smooth curves.

Now let P be any rational place. That is

$$\mathcal{O}_P/P = \{c + P \mid c \in k\}.$$

For $x \in \mathcal{O}_P$ we define $x(P) \in k$ to be the residue of x modulo P. The function defined in this way is called the residue map corresponding to P. Now let P be any place from case I (in particular P is rational). A very nice thing now happens, namely that we for any $f = F + I \in \mathcal{O}_P$ can find $f(P)$ simply as $f(P) = F(p)$. This result is of great importance when one constructs the so-called geometric Goppa codes. We will discuss these codes in chapter I.11.

Remark I.10.12
Let P be any rational place of a given algebraic function field $\mathcal{F}$. According to [26] and [31] there exists a description like (I.10.12) of $\mathcal{F}$, such that P in this description becomes a unique place of $\mathcal{F}$ at infinity. However this particular description is in general not easy to find.

We have the following example.

Example I.10.13
Let k be any field. The polynomial $T^3 + Y^3T + Y$ is absolutely irreducible over $k(Y)[T]$, so $\mathrm{Quot}\left(k[X,Y]/\langle X^3 + Y^3X + Y\rangle\right)$ is a function field. This function field is known as the function field of the Klein Quartic. Homogenizing $X^3 + Y^3X + Y$, we get $X^3Z + Y^3X + YZ^3$, that has the zeros $(0:1:0)$ and $(1:0:0)$ at infinity. As there are more than one zero at infinity, we have more than one Q, for which at least one of the values $v_Q(x)$, $v_Q(y)$ is negative. So the coordinate ring $R := k[X,Y]/\langle X^3 + Y^3X + Y\rangle$ is not contained in $\cup_{m=0}^{\infty}\mathcal{L}(mQ)$ for any place Q of the function field.

The following proposition is in [21, §3.2] proved on the level of order functions only. It contains the result from example I.10.13 as a special case.

Proposition I.10.14
Let $F(X,Y) \in k[X,Y]$ be of the form $F(X,Y) = X^aY^c + uY^{b+c} + G(X,Y)$ with $u \in k\backslash\{0\}$, $\deg_X(G) = d < a$, $\deg(G) < b+c$ and $\gcd(a,b) = 1$. Define $I := \langle F(X,Y)\rangle$ and consider

$$\mathcal{B} := \left\{ X^\alpha Y^\beta + I \mid \alpha,\beta \in \mathbb{N}_0, \alpha < a, c\alpha \leq (a-d)\beta \right\}.$$

A weight function can be developed from $\mathcal{B}$ by defining $\rho(X^\alpha Y^\beta + I) := \alpha a + \beta b$ (clearly this makes $\mathcal{B}$ into an order basis). If $c > 0$ then $k[X,Y]/I$ possesses no weight function.

Note that $\mathcal{B}$ generates all of $k[X,Y]/I$ when $c = 0$. That is $k[X,Y]/I$ is an order domain in this case. In [2] Beelen extends

$$\operatorname{span}_k \left\{ X^\alpha Y^\beta + I \mid \alpha,\beta \in \mathbb{N}_0, \alpha < a, c\alpha \leq (a-d)\beta \right\}$$

to various rings that possess weight functions with values in $\mathbb{N}_0$. He does this using algebraic geometry techniques.

Example I.10.15
In this example we use ramification theory. For an introduction to this theory see [38, Ch. III]. Define a weighted degree function wdeg *on $k[X,Y]$ by $w(X) = b$ and $w(Y) = a$. We consider curves of the form*

$$F(X,Y) = X^a + uY^b + G(X,Y) \in \mathbb{F}_q[X,Y] \tag{I.10.17}$$

where $u \in \mathbb{F}_q\backslash\{0\}$, $\gcd(a,b) = 1$ and $\operatorname{wdeg}(G) < ab$. In particular (I.10.17) includes the curves Feng and Rao calls type-I curves (see [6]). In the remaining part of this thesis, a type-I curve is a curve of the form (I.10.17). Now

$$R := \mathbb{F}_q[X,Y]/\langle F(X,Y)\rangle$$

is an order domain with an order function ρ induced as a weight function by $\rho(x = X + I) = b$ and $\rho(y = Y + I) = a$. To see this simply apply Pellikaan's factor ring theorem. Alternatively, a direct proof that ρ satisfies the conditions for being a weight function, can be found in [21]. Let us see how we can understand the structure R in an algebraic function field theoretical set-up. Consider the function field

$$\mathcal{F} := \operatorname{Quot}(\mathbb{F}_q[X,Y]/\langle F(X,Y)\rangle).$$

We first show that there is only one place in $\boldsymbol{P}_\mathcal{F}$ that is a pole for x, and that this place is at the same time the only place that is a pole for y (a pole for f is a

place such that $v_P(f) < 0$).
By assumption we have $\gcd(a, b) = 1$ so the place at infinity in $\boldsymbol{P}_{\mathbb{F}_q(X)}$ is fully ramified in the extension $\mathcal{F}/\mathbb{F}_q(X)$. This shows the uniqueness of a pole of x. Now denote this pole by P_∞. It is easily seen that P_∞ is also a pole for y. We have $\nu_{P_\infty}(x) = -b$ and $\nu_{P_\infty}(y) = -a$. Finally the place at infinity in $\boldsymbol{P}_{\mathbb{F}_q(Y)}$ is fully ramified in the extension $\mathcal{F}/\mathbb{F}_q(Y)$ and we are through. Actually we have also shown that P_∞ is a rational place. We now investigate the vector space $\cup_{m=0}^{\infty}\mathcal{L}(mP_\infty)$. From the above discussion, we know that for $\alpha, \beta \geq 0$ one has $v_{P_\infty}(x^\alpha y^\beta) = -(b\alpha + a\beta)$ and $v_Q(x^\alpha y^\beta) \geq 0$ for all $Q \neq P_\infty$. In particular $R \subseteq \cup_{m=0}^{\infty}\mathcal{L}(mP_\infty)$. And we have the following connection between the order function ρ and the valuation ν_{P_∞}, namely

$$\rho(f) = -\nu_{P_\infty}(f) \text{ for } f \in D.$$

If the monomials in x and y are the only elements in $\mathcal{F}$ with pole divisor of the form mP_∞ for some m, then $R = \cup_{m=0}^{\infty}\mathcal{L}(mP_\infty)$. If however there are rational expressions r such that

$$v_{P_\infty}(r) = -m \quad \text{and} \quad v_Q(r) \geq 0 \text{ for all } Q \neq P_\infty$$

then $R \subsetneq \cup_{m=0}^{\infty}\mathcal{L}(mP_\infty)$. If $F(X, Y)$ from (I.10.17) is equal to

$$F(X, Y) = H(X) - Y^b - uY, \quad u \in \mathbb{F}_q \backslash \{0\}$$

where b is equal to some power of the characteristic of $\mathbb{F}_q$, and where all the solutions to in $T^b + uT = 0$ are in $\mathbb{F}_q$, then according to [38, Prop. VI.4.1], the first condition is satisfied. In particular it is satisfied for the Hermitian curve

$$F(X, Y) = X^{q+1} - Y^q - Y \in \mathbb{F}_{q^2}[X, Y].$$

I.11
The codes related to order domains

As noted in the very beginning of this material, the whole purpose of introducing order domains and order functions is to construct codes. More specific the concept of order domains and order functions can be seen as a generalization of the algebraic structures, that gives us Reed-Muller codes and 1-point geometric Goppa codes. To understand the construction of geometric Goppa codes, some knowledge about algebraic function field theory or algebraic geometry is required. However it is the authors policy, that the main part of this thesis should be readable, also for readers that do not have experience with algebraic function field theory or algebraic geometry. Therefore the connection to the 1-point geometric Goppa codes will not be treated before chapter I.12, although they constitute a very important subclass of the codes that we are going to construct.

The code constructions E_l, C_l, $\tilde{C}(d)$ and $\tilde{C}_\varphi(d)$ that we describe in the following have their origins in the papers [8], [6] and [7] by Feng et. al. However with the invention of the concept of order functions by Høholdt et. al. in [20], [21] and [33] the codes were described in a more un-complicated way. We follow the tradition for the description of the codes initiated by Høholdt et. al.

I.11.1 The evaluation code and its dual

In this section the so-called evaluation codes and their duals are introduced. The very important order bound that is a bound on the minimum distance of the dual codes is treated. Instead of introducing the evaluation codes and their duals in general from the beginning, we will do it in two steps. In subsection I.11.1.1 we will consider the evaluation codes and their duals, in a special case where the notation becomes rather simple. In subsection I.11.1.2 we will treat the codes in general.
Recall that the order functions fall into two classes. The one being the order functions where the value set Λ is ordered isomorphic to $\mathbb{N}$, and the other being the order functions such that Λ is not ordered isomorphic to $\mathbb{N}$. Up til recently only order-domains/order-functions of the first kind were treated. Especially

only the codes coming from the order functions of the first kind are treated in [21]. However the order bound not only holds for the dual codes coming from order functions where Λ is ordered isomorphic to $\mathbb{N}$. It holds for any order function. As the notation of the codes is much simpler, when a well behaving sequence exists, we start by considering order functions where Λ is ordered isomorphic with $\mathbb{N}$. We follow the lines of [21]. In the following we use extensively the definitions from section I.3.1. The reader might want to consult this section before proceeding.

I.11.1.1 The codes E_l and C_l

In this subsection we will always assume, that an order domain R with a well-behaving sequence $(f_1, f_2, \ldots)$ is given. We start with a definition of a multiplication between the elements in $\mathbb{F}_q^n$.

Definition I.11.1
Define the coordinate wise multiplication $*$ on $\mathbb{F}_q^n$ by

$$(a_1, \ldots, a_n) * (b_1, \ldots, b_n) = (a_1 b_1, \ldots, a_n b_n).$$

Note that the vector space $\mathbb{F}_q^n$ with the multiplication $*$ becomes a commutative ring with $(1, \ldots, 1)$ as the unity. Identifying $\{(a, \ldots, a) \mid a \in \mathbb{F}_q\}$ with $\mathbb{F}_q$ we see that $\mathbb{F}_q^n$ is an $\mathbb{F}_q$-algebra.

Definition I.11.2
Let R be an $\mathbb{F}_q$-algebra. A map $\varphi : R \to \mathbb{F}_q^n$ that is $\mathbb{F}_q$-linear and satisfies

$$\varphi(fg) = \varphi(f) * \varphi(g)$$

for any $f, g \in R$ is called a morphism of the $\mathbb{F}_q$-algebras.

We are now in the position to give a first definition of the codes. Recall that we at this stage assume, that the order domain R possesses a well-behaving sequence $(f_1, f_2, \ldots)$. We define the evaluation code E_l in the following way.

Definition I.11.3
Let φ be a morphism on R and denote $\boldsymbol{h}_i := \varphi(f_i)$. For a given $l \geq 1$ the evaluation code (corresponding to φ) is given by

$$E_l := \varphi(L_l) = \operatorname{span}_{\mathbb{F}_q}\{\boldsymbol{h}_1, \ldots, \boldsymbol{h}_l\}.$$

The dual code is denoted by C_l, that is.

Definition I.11.4

$$C_l := \{\boldsymbol{c} \in \mathbb{F}_q^n \mid \boldsymbol{c} \cdot \boldsymbol{h}_i = 0 \text{ for all } i \leq l\}.$$

Remark I.11.5
Given an order function, then it is from remark I.3.20 clear, that the codes E_l and C_l do not depend on the choice of order basis.

In all of the examples that are given in this material (and in all examples that are given in [21] as well), the morphism φ is a so-called evaluation map.

Definition I.11.6
Given a quotient ring $R := \mathbb{F}_q[X_1, \ldots, X_m]/I$. Let $\mathcal{V}_{\mathbb{F}_q}(I) = \{P_1, \ldots, P_n\}$. The evaluation map is given by.

$$ev : \begin{cases} R & \to & \mathbb{F}_q^n \\ F + I & \mapsto & (F(P_1), \ldots, F(P_n)) \,. \end{cases}$$

Remark I.11.7
It is well known that ev is surjective (see [19]). It is easily verified that ev satisfies the conditions in definition I.11.2, that is ev is a morphism of $\mathbb{F}_q$-algebras.

Example I.11.8
Consider the order domain $\mathbb{F}_2[X, Y]$ with weight function $\rho : \mathbb{F}_2[X, Y] \to \mathbb{N}_0^2 \cup \{-\infty\}$ induced by $\rho(X) = (1, 0)$, $\rho(Y) = (0, 1)$ and where $\mathbb{N}_0^2$ is ordered by $\prec_{st}$. A well-behaving sequence is given by

$$(f_1 = 1, f_2 = Y, f_3 = X, f_4 = Y^2, f_5 = XY, f_6 = X^2, f_7 = Y^3, \ldots).$$

Consider the evaluation map

$$ev : \begin{cases} \mathbb{F}_2[X, Y] & \to & \mathbb{F}_2^4 \\ F & \mapsto & (F(0,0), F(0,1), F(1,0), F(1,1)) \,. \end{cases}$$

The evaluation codes are

$$\begin{aligned} E_1 &= \operatorname{span}_{\mathbb{F}_2}\{(1,1,1,1)\} \\ E_2 &= \operatorname{span}_{\mathbb{F}_2}\{(1,1,1,1),(0,1,0,1)\} \\ E_3 &= \operatorname{span}_{\mathbb{F}_2}\{(1,1,1,1),(0,1,0,1),(0,0,1,1)\} \\ &= E_4 \\ E_5 &= \operatorname{span}_{\mathbb{F}_2}\{(1,1,1,1),(0,1,0,1),(0,0,1,1),(0,0,1,1)\} \\ &= \mathbb{F}_2^4 = E_6 = E_7 = \cdots . \end{aligned}$$

And the dual codes are

$$\begin{aligned}
C_1 &= \{\boldsymbol{c} \in \mathbb{F}_2^4 \mid \boldsymbol{c} \cdot (1,1,1,1) = 0\} \\
C_2 &= \{\boldsymbol{c} \in \mathbb{F}_2^4 \mid \boldsymbol{c} \cdot (1,1,1,1) = \boldsymbol{c} \cdot (0,1,0,1) = 0\} \\
C_3 &= \{\boldsymbol{c} \in \mathbb{F}_2^4 \mid \boldsymbol{c} \cdot (1,1,1,1) = \boldsymbol{c} \cdot (0,1,0,1) = \boldsymbol{c} \cdot (0,0,1,1) = 0\} \\
&= C_4 \\
C_5 &= \{\boldsymbol{c} \in \mathbb{F}_2^4 \mid \boldsymbol{c} \cdot (1,1,1,1) = \boldsymbol{c} \cdot (0,1,0,1) = \boldsymbol{c} \cdot (0,0,1,1) \\
&\qquad\qquad = \boldsymbol{c} \cdot (0,0,0,1) = 0\} \\
&= \{(0,0,0,0)\} = C_6 = C_7 = \cdots .
\end{aligned}$$

Example I.11.9
Denote $I := \langle X^3 - Y^2 - Y \rangle \subseteq \mathbb{F}_4[X,Y]$. *Consider the order domain* $R := \mathbb{F}_4[X,Y]/I$ *with weight function* $\rho : R \to \Lambda_{-\infty} := \langle 2,3 \rangle \cup \{-\infty\}$ *induced by* $\rho(X+I) = 2$, $\rho(Y+I) = 3$. *A well-behaving sequence is given by*

$$\begin{aligned}
&(f_1 = 1 + I, f_2 = X + I, f_3 = Y + I, f_4 = X^2 + I, f_5 = XY + I, \\
&\ f_6 = X^3 + I, f_7 = X^2Y + I, f_8 = X^4 + I, f_9 = X^3Y + I, \\
&\ f_{10} = X^5 + I, f_{11} = X^4Y + I, \ldots).
\end{aligned}$$

Let the elements of $\mathbb{F}_4$ *be* $\{0, 1, \alpha, \alpha^2\}$ *where* $\alpha^2 + \alpha + 1 = 0$. *Now*

$$\mathcal{V}_{\mathbb{F}_4}(I) = \{(0,0),(0,1),(1,\alpha),(1,\alpha^2),(\alpha,\alpha),(\alpha,\alpha^2),(\alpha^2,\alpha),(\alpha^2,\alpha^2)\}.$$

So our evaluation map is

$$ev : \left\{ \begin{array}{rcl} R & \to & \mathbb{F}_4^8 \\ F + I & \mapsto & \big(F(0,0), F(0,1), F(1,\alpha), F(1,\alpha^2), \\ & & \ F(\alpha,\alpha), F(\alpha,\alpha^2), F(\alpha^2,\alpha), F(\alpha^2,\alpha^2)\big) . \end{array} \right.$$

For instance

$$\begin{aligned}
E_5 = \operatorname{span}_{\mathbb{F}_4}\{&(1,1,1,1,1,1,1,1), (0,0,1,1,\alpha,\alpha,\alpha^2,\alpha^2), \\
&(0,1,\alpha,\alpha^2,\alpha,\alpha^2,\alpha,\alpha^2), (0,0,1,1,\alpha^2,\alpha^2,\alpha,\alpha), \\
&(0,0,\alpha,\alpha^2,\alpha^2,1,1,\alpha)\}
\end{aligned}$$

and we have

$$\begin{aligned}
E_1 \subsetneq E_2 \subsetneq E_3 \subsetneq E_4 \subsetneq E_5 \subsetneq E_6 \subsetneq E_7 = E_8 \\
\subsetneq E_9 = \mathbb{F}_4^8 = E_{10} = E_{11} = \cdots .
\end{aligned} \tag{I.11.9}$$

The order bound

One of the nice things about the present description of codes is the so-called order bound on the minimum distance of C_l. It holds in any case, where φ is surjective. Note that according to remark I.11.7, the bound holds especially, when φ is of the type ev. In the following we will always assume that φ is surjective.

Still following the lines of [21] we introduce the order bound by first studying the so-called matrix of syndromes. Our assumption that $\varphi : R \to \mathbb{F}_q^n$ is surjective corresponds to the assumption that an $N \in \mathbb{N}$ exists such that $C_l = 0$ for $l \geq N$. Consider the $N \times n$ matrix

$$H := \begin{bmatrix} \boldsymbol{h}_1 \\ \vdots \\ \boldsymbol{h}_N \end{bmatrix}$$

(here $\boldsymbol{h}_i$ is a row vector).

Definition I.11.10
Given $\boldsymbol{y} \in \mathbb{F}_q^n$. Define the so-called syndromes by

$$s_{ij}(\boldsymbol{y}) := \boldsymbol{y} \cdot (\boldsymbol{h}_i * \boldsymbol{h}_j).$$

We call

$$S(\boldsymbol{y}) := (s_{ij}(\boldsymbol{y}) \mid 1 \leq i, j \leq N)$$

the matrix of syndromes of $\boldsymbol{y}$.

We have the following lemmas (all from [21]).

Lemma I.11.11
Given a nonzero $\boldsymbol{y} = (y_1, \ldots, y_n) \in \mathbb{F}_q^n$ let $D(\boldsymbol{y})$ be the diagonal $n \times n$ matrix $(D(\boldsymbol{y}))_{ii} := y_i$, $i = 1, \ldots, n$. Then

$$S(\boldsymbol{y}) = HD(\boldsymbol{y})H^T \quad \text{and} \quad \operatorname{rank}(S(\boldsymbol{y})) = wt(\boldsymbol{y}).$$

Proof:
We have

$$\begin{aligned} s_{ij}(\boldsymbol{y}) &= \boldsymbol{y} \cdot (\boldsymbol{h}_i * \boldsymbol{h}_j) \\ &= \sum_{s=1}^{n} y_s (\boldsymbol{h}_i)_s (\boldsymbol{h}_j)_s \\ &= \boldsymbol{h}_i \cdot \boldsymbol{y} * \boldsymbol{h}_j \\ &= (HD(\boldsymbol{y})H^T)_{ij}. \end{aligned}$$

Now $\mathrm{rank}(D(\boldsymbol{y})) = wt(\boldsymbol{y})$. As H (and H^T) by assumption have full rank equal to n, we get that

$$\mathrm{rank}(S(\boldsymbol{y})) = \mathrm{rank}(D(\boldsymbol{y})) = wt(\boldsymbol{y}).$$

□

Lemma I.11.12

(1) *If* $\boldsymbol{y} \in C_{l-1}$ *and* $l(i,j) < l$ *then* $s_{ij}(\boldsymbol{y}) = 0$
(2) *if* $\boldsymbol{y} \in C_{l-1} \backslash C_l$ *and* $l(i,j) = l$ *then* $s_{ij}(\boldsymbol{y}) \neq 0$.

Proof:
(1): Let $\boldsymbol{y} \in C_{l-1}$ and $l(i,j) < l$. Now the last assumption means that $f_i f_j \in L_{l-1}$. By the definition of a morphism we have

$$\boldsymbol{h}_i * \boldsymbol{h}_j = \varphi(f_i f_j) \in \varphi(L_{l-1}) = E_{l-1} = C_{l-1}^{\perp}$$

that is

$$s_{ij}(\boldsymbol{y}) = \boldsymbol{y} \cdot \boldsymbol{h}_i * \boldsymbol{h}_j = 0.$$

(2): Let $\boldsymbol{y} \in C_{l-1} \backslash C_l$ and assume $l(i,j) = l$. The last assumption implies $f_i f_j \in L_l \backslash L_{l-1}$, or in other words $f_i f_j = \sum_{s=1}^{l} \alpha_s f_s$, where $\alpha_s \in \mathbb{F}_q$ and $\alpha_l \neq 0$. It follows that

$$s_{ij}(\boldsymbol{y}) = \boldsymbol{y} \cdot \varphi(f_i f_j) = \boldsymbol{y} \cdot \alpha_l \varphi(f_l) \neq 0.$$

□

To state the next lemma we will need some notation.

Definition I.11.13
For $l \in \mathbb{N}$ *define*

$$N_l := \{(i,j) \in \mathbb{N}^2 \mid l(i,j) = l\}.$$

Let μ_l *be the number of elements of* N_l.

Remark I.11.14
We differ in notation from [21]. Our N_l *corresponds to their* N_{l-1} *and our* μ_l *to their* ν_{l-1}. *It is the authors opinion, that the above introduced notation is easier to work with in practice. Especially when one works with the improved codes* $\tilde{C}(d)$ *and* $\tilde{C}_{\varphi}(d)$ *(not introduced yet). More importantly, the* μ*-notation becomes indispensable, when we in the next subsection extend the* C_l *construction to general order-domains/order-functions.*

To ease the notation we sometimes consider μ as a function on R in the following way.

Definition I.11.15
Let

$$\mu : \begin{cases} R & \to & \mathbb{N} \\ f & \mapsto & \mu_l \ \text{if } f \in L_l \backslash L_{l-1}. \end{cases}$$

We have the following lemma.

Lemma I.11.16
If $t = \mu_l$ then the elements of N_l can be enumerated $(i_1, j_1), \ldots, (i_t, j_t)$ such that $i_1 < \cdots < i_t$ and $j_1 > \cdots > j_t$.

Proof:
We can enumerate the elements such that $i_1 \leq \cdots \leq i_t$ and $j_u < j_{u+1}$ if $i_u = i_{u+1}$. But then

$$l = l(i_u, j_u) < l(i_u, j_{u+1}) = l(i_{u+1}, j_{u+1}) = l$$

a contradiction (note that the first inequality follows from the assumption, that $(f_1, f_2, \ldots)$ is well-behaving). The equality $i_u = i_{u+1}$ must be false. That is we have $i_1 < \cdots < i_t$. A similar argument shows that $j_1 > \cdots > j_t$. □

The last lemma is.

Lemma I.11.17
Let $N_l = \{(i_1, j_1), \ldots, (i_t, j_t)\}$ be enumerated as in lemma I.11.16. If $\boldsymbol{y} \in C_{l-1} \backslash C_l$ then

$$s_{i_u j_v}(\boldsymbol{y}) = \begin{cases} 0 & \text{if } u < v \\ \text{not zero} & \text{if } u = v. \end{cases} \tag{I.11.19}$$

Proof:
The assumption $\boldsymbol{y} \in C_{l-1} \backslash C_l$ implies that

$$\varphi(f_{i_1}), \ldots, \varphi(f_{i_t}), \varphi(f_{j_1}), \ldots, \varphi(f_{j_t})$$

are contained as row vectors in H. If $u < v$ then by lemma I.11.16 we have $l(i_u, j_v) < l(i_v, j_v) = l$. Lemma I.11.12 part (1) then implies that $s_{i_u j_v}(\boldsymbol{y}) = 0$. If $u = v$ then lemma I.11.12 part (2) states that $s_{i_u j_v}(\boldsymbol{y}) \neq 0$. □

We are now almost in the position to state the important order bound. We will just need the following definition.

Definition I.11.18
Denote

$$\begin{aligned} d(l) &:= \min\{\mu_s \mid s > l\} \\ d_\varphi(l) &:= \min\{\mu_s \mid s > l, C_{s-1} \neq C_s\}. \end{aligned}$$

The order bound can now be formulated as follows.

Theorem I.11.19
Let C_l be defined from a surjective morphism φ. The minimum distance of C_l is bounded by

$$d(C_l) \geq d_\varphi(l) \geq d(l).$$

Proof:
Consider any $\boldsymbol{y} \in C_l \backslash \{\mathbf{0}\}$. There exists an index $s > l$ such that $\boldsymbol{y} \in C_{s-1} \backslash C_s$. By lemma I.11.17 the syndrome matrix $S(\boldsymbol{y})$ contains a submatrix of rank at least μ_s and by lemma I.11.11 this means that $wt(\boldsymbol{y}) \geq \mu_s$. We have proved the first inequality. The last inequality is obvious. □

In [6] a result similar to theorem I.11.19 was presented without the notion of an order function. One therefore refers to $d_\varphi(l)$ as the Feng-Rao distance.

Remark I.11.20
The parameter $d(l)$ depends only on the order function. Especially in the case of a weight function only on the value set Λ. The Feng-Rao distance $d_\varphi(l)$ however, also depends on the nature of the isomorphism φ. Neither $d(l)$ nor $d_\varphi(l)$ depends on the choice of the order basis.

Example I.11.21
This is a continuation of example I.11.8. Now $C_1 \neq C_2$, $C_2 \neq C_3$ and $C_4 \neq C_5$. So to determine the Feng-Rao distances we need only consider

$$\left\{ \begin{array}{lcl} \mu_2 & = & 2 \\ \mu_3 & = & 2 \\ \mu_5 & = & 4 \end{array} \right. \quad \textit{giving} \quad \left\{ \begin{array}{lcl} d_\varphi(1) & = & 2 \\ d_\varphi(2) & = & 2 \\ d_\varphi(3) & = & 4. \end{array} \right.$$

We conclude that C_1 is a $[n = 4, k = 3, d \geq 2]$ code, C_2 is a $[n = 4, k = 2, d \geq 2]$ code, and C_3 is a $[n = 4, k = 1, d \geq 4]$ code. Inspection shows that the order bound is tight for all three codes.

Example I.11.22
This is a continuation of example I.11.9. From (I.11.9) we have

$$\begin{aligned} C_1 \supsetneq C_2 \supsetneq C_3 \supsetneq C_4 \supsetneq C_5 \supsetneq C_6 \\ \supsetneq C_7 = C_8 \supsetneq C_9 = C_{10} = C_{11} = \cdots . \end{aligned}$$

So to determine the Feng-Rao distances we need only consider

$$\begin{cases} \mu_2 = 2 \\ \mu_3 = 2 \\ \mu_4 = 3 \\ \mu_5 = 4 \\ \mu_6 = 5 \\ \mu_7 = 6 \\ \mu_9 = 8 \end{cases} \quad \textit{giving} \quad \begin{cases} d_\varphi(1) = 2 \\ d_\varphi(2) = 2 \\ d_\varphi(3) = 3 \\ d_\varphi(4) = 4 \\ d_\varphi(5) = 5 \\ d_\varphi(6) = 6 \\ d_\varphi(7) = 8. \end{cases}$$

The parameters of E_l

As described above, the order bound holds for any C_l code. A counterpart that states a lower bound on the minimum distance of the E_l code is however known only in the case of an order domain of transcendence degree 1.

Theorem I.11.23
Let $R = \mathbb{F}_q[X_1, \ldots, X_m]/I$ be an order domain over $\mathbb{F}_q$ with a weight function $\rho : R \to \Lambda_{-\infty} \subseteq \mathbb{N}_0 \cup \{-\infty\}$. And let $ev : R \to \mathbb{F}_q^n$ be an evaluation map. The minimum distance of the related code E_l is at least $n - \rho_l$, where ρ_l is the order of the l.th element in an order sequence for R. If $\rho_l < n$ then $\dim(E_l) = l$.

Proof:
The proof uses the order bound. It relies heavily on the assumption $\Lambda \subseteq \mathbb{N}_0$. See [21, Sec. 5]. □

Decoding of the C_l codes

One of the main arguments for the importance of the theory of order domains and related codes, is the very nice fact, that an efficient decoding algorithm for the C_l codes is known. We will not describe this decoding algorithm, but just repeat the following facts already mentioned in chapter I.1. Namely that a decoding algorithm, that detects up to $\lfloor (d(l) - 1)/2 \rfloor$ errors, has been known more or less as long as the codes has been known. In [21] it is described how to decode the C_l codes using majority voting. The algorithm is based on Sakata's extension of the classical Berlekamp-Massey algorithm.

I.11.1.2 The codes E_λ and C_λ, $\lambda \in \Lambda$

We now generalize the E_l and C_l construction to the general case, where a well-behaving basis exists, but where a well-behaving sequence does not necessarily exist. That is to the general case where Λ is not necessarily ordered isomorphic with $\mathbb{N}$. Let

$$(f_\lambda \,|\, \rho(f_\lambda) = \lambda \in \Lambda)_{\prec_\Lambda}$$

be a well-behaving basis for an order domain R. The codes are defined as follows.

Definition I.11.24
Let φ be a morphism on R and denote $\boldsymbol{h}_\lambda := \varphi(f_\lambda)$. For a given $\lambda \in \Lambda$ the evaluation code (corresponding to φ) is given by

$$E_\lambda := \varphi(L_\lambda) = \operatorname{span}_{\mathbb{F}_q}\{\boldsymbol{h}_{\lambda'} \,|\, \lambda' \preceq_\Lambda \lambda\}.$$

The dual code is denoted by C_λ, that is.

Definition I.11.25

$$C_\lambda := \{\boldsymbol{c} \in \mathbb{F}_q^n \,|\, \boldsymbol{c} \cdot \boldsymbol{h}_{\lambda'} = 0 \text{ for all } \lambda' \preceq_\Lambda \lambda\}.$$

Remark I.11.26
We note that our notation is not consistent in the special case $\Lambda \subseteq \mathbb{N}_0$. We get around this problem by the following convention. If Λ is ordered isomorphic to $\mathbb{N}$ then we will use the notation from the previous subsection. Only when Λ is not ordered isomorphic to $\mathbb{N}$ (in this case Λ can not be contained in $\mathbb{N}_0$), we will use the notation from the present subsection.

Example I.11.27
Consider the order domain $\mathbb{F}_2[X,Y]$ with weight function $\rho : \mathbb{F}_2[X,Y] \to \mathbb{N}_0^2 \cup \{-\infty\}$ induced by $\rho(X) = (1,0)$, $\rho(Y) = (0,1)$ and where $\mathbb{N}_0^2$ is ordered by the pure lexicograhpic ordering $\prec_\Lambda := \prec_{lex}$ where $(0,1) \prec_{lex} (1,0)$. Consider the evaluation map (as in example I.11.8)

$$ev : \begin{cases} \mathbb{F}_2[X,Y] & \to & \mathbb{F}_2^4 \\ F & \mapsto & (F((0,0)), F((0,1)), F((1,0)), F((1,1))) \,. \end{cases}$$

Now

$$\begin{aligned}
C_{(0,0)} &= \{\boldsymbol{c} \in \mathbb{F}_2^4 \,|\, \boldsymbol{c} \cdot (1,1,1,1) = 0)\} \\
C_{(0,1)} &= \{\boldsymbol{c} \in \mathbb{F}_2^4 \,|\, \boldsymbol{c} \cdot (1,1,1,1) = \boldsymbol{c} \cdot (0,1,0,1) = 0\} \\
&= C_{(0,2)} = C_{(0,3)} = \cdots \\
C_{(1,0)} &= \{\boldsymbol{c} \in \mathbb{F}_2^4 \,|\, \boldsymbol{c} \cdot (1,1,1,1) = \boldsymbol{c} \cdot (0,1,0,1) = \boldsymbol{c} \cdot (0,0,1,1) = 0\} \\
C_{(1,1)} &= \{\boldsymbol{c} \in \mathbb{F}_2^4 \,|\, \boldsymbol{c} \cdot (1,1,1,1) = \boldsymbol{c} \cdot (0,1,0,1) = \boldsymbol{c} \cdot (0,0,1,1) = \\
&\qquad\qquad = \boldsymbol{c} \cdot (0,0,0,1) = 0\} \\
&= \{(0,0,0,0)\} \\
&= C_{(a,b)} \text{ for any } (a,b) \succ_\Lambda (1,1).
\end{aligned}$$

Example I.11.28
In this example we compare the codes from the above example with the codes from example I.11.8. We immediately see that

$$C_1 = C_{(0,0)}, C_2 = C_{(0,1)}, C_3 = C_{(1,0)} \text{ and } C_5 = C_{(1,1)}. \tag{I.11.28}$$

Now let $\rho : \mathbb{F}_2[X,Y] \to \mathbb{N}_0^2$ be any weight function induced by $\rho(X) = (1,0)$, $\rho(Y) = (0,1)$ and with $\mathbb{N}_0^2$ ordered by $\prec_{\mathbb{N}_0^2}$. Regardless of the actual definition of $\prec_{\mathbb{N}_0^2}$ we will have

- $ev(Y) \neq ev(F(X,Y))$ *for any* $F(X,Y)$ *such that* $\rho(F(X,Y)) \prec_{\mathbb{N}_0^2} \rho(Y)$
- $ev(X) \neq ev(F(X,Y))$ *for any* $F(X,Y)$ *such that* $\rho(F(X,Y)) \prec_{\mathbb{N}_0^2} \rho(X)$
- $ev(XY) \neq ev(F(X,Y))$ *for any* $F(X,Y)$ *such that* $\rho(F(X,Y)) \prec_{\mathbb{N}_0^2} \rho(XY)$.

So the reason for the equalities in (I.11.28) is that both $1 \prec_{st} Y \prec_{st} X \prec_{st} XY$ and $1 \prec_{lex} Y \prec_{lex} X \prec_{lex} XY$. We may think of $\prec_{st}$ from example I.11.8, as an approximation of $\prec_{lex}$ from example I.11.27.

Remark I.11.29
Consider the codes defined from a well-behaving basis to which there does not correspond a well-behaving sequence. A natural question in the light of example I.11.28 is, if one can always find a well-behaving sequence, that approximates the well-behaving basis in the sense, that it defines the same set of codes by the same set of basis elements. We will not try to answer this question, but

only note, that the description of an approximating well-behaving sequence, in some cases may be more complicated, than the description of the well-behaving basis it approximates.

The order bound

We next show how to generalize the proof of the order bound given in subsection I.11.1.1, to the general case considered in this subsection. In the remaining part of this subsection φ is always assumed to be surjective. This corresponds to assuming that a $\lambda \in \Lambda$ exists such that $C_{\tilde{\lambda}} = 0$ for all $\tilde{\lambda} \succeq_\Lambda \lambda$. It might not, as in the previous subsection, be possible to choose λ such that both $C_\lambda = 0$, and such that there are finitely many indices $\lambda' \prec_\Lambda \lambda$. So we do not have an $N \times n$ matrix H as in the previous subsection. To prove the order bound we will, instead of considering a fixed matrix H, consider n different matrices. One for each $\lambda \in \Lambda$ such that $C_\lambda \neq C_{\lambda'}$ for any $\lambda' \prec_\Lambda \lambda$.

To describe these matrices we must first introduce some notation and state a lemma.

Definition I.11.30
Given $\lambda \in \Lambda$ then

$$N_\lambda := \{(\alpha, \beta) \in \Lambda^2 \mid l_\Lambda(\alpha, \beta) = \lambda\}.$$

Define $\mu_\lambda := \#N_\lambda$ if N_λ is a finite set, and $\mu_\lambda := \infty$ if not.

In consistency with definition I.11.15 we have.

Definition I.11.31
Let

$$\mu : \begin{cases} R & \to & \mathbb{N} & \\ f & \mapsto & \mu_\lambda & \text{if } f \in L_\lambda \text{ but} \\ & & & f \notin L_{\lambda'} \text{ for any } \lambda' \prec_\Lambda \lambda. \end{cases}$$

Lemma I.11.32
Let $r \leq \mu_\lambda$ be finite. Given r elements $(\alpha_1, \beta_1), \ldots, (\alpha_r, \beta_r) \in N_\lambda$ then the enumeration can be chosen such that $\alpha_1 \prec_\Lambda \cdots \prec_\Lambda \alpha_r$ and $\beta_1 \succ_\Lambda \cdots \succ_\Lambda \beta_r$.

Proof:
As the proof of lemma I.11.16. □

Now let $\lambda \in \Lambda$ be an element such that $C_\lambda \neq C_{\lambda'}$ for any $\lambda' \prec_\Lambda \lambda$. Define for this λ, $r := \min\{\mu_\lambda, n\}$, where n is the length of the codes. The matrix M

corresponding to λ (or equivalent the matrix M corresponding to $\boldsymbol{y} \in \mathbb{F}_q^n$, where $\boldsymbol{y} \notin C_\lambda$ but $\boldsymbol{y} \in C_{\lambda'}$ for any $\lambda' \prec_\Lambda \lambda$) is defined as follows. Let $\alpha_1, \ldots, \alpha_r \in \Lambda$ be chosen such that $(\alpha_1, \alpha_r), (\alpha_2, \alpha_{r-1}), \ldots, (\alpha_r, \alpha_1) \in N_\lambda$ and $\alpha_1 \prec_\Lambda \cdots \prec_\Lambda \alpha_r$. This is possible by lemma I.11.32. The first rows of M are $\boldsymbol{m}_1 := \varphi(f_{\alpha_1}), \ldots, \boldsymbol{m}_r := \varphi(f_{\alpha_r})$. Now fill in with extra rows of the form $\varphi(f_\lambda)$ where the λ's are some elements in Λ to get a, say $N \times n$ matrix

$$M := \begin{bmatrix} \boldsymbol{m}_1 \\ \vdots \\ \boldsymbol{m}_N \end{bmatrix}$$

of full rank equal to n.

Definition I.11.33
Given $\boldsymbol{y} \in \mathbb{F}_q^n$ let M be the corresponding matrix. Define

$$t_{ij}(\boldsymbol{y}) := \boldsymbol{y} \cdot (\boldsymbol{m}_i * \boldsymbol{m}_j)$$

and

$$T(\boldsymbol{y}) := (t_{ij}(\boldsymbol{y}) \mid 1 \leq i, j \leq N)\,.$$

We have the following lemmas.

Lemma I.11.34
Let $\boldsymbol{y} = (y_1, \ldots, y_n) \in \mathbb{F}_q^n \backslash \{\mathbf{0}\}$ and let M be the corresponding matrix. Let $D(\boldsymbol{y})$ be the $n \times n$ diagonal matrix with $(D(\boldsymbol{y}))_{ii} = y_i$, $i = 1, \ldots, n$. Then

$$T(\boldsymbol{y}) = M D(\boldsymbol{y}) M^T \qquad \textit{and} \qquad \mathrm{rank}(T(\boldsymbol{y})) = wt(\boldsymbol{y}).$$

Proof:
As the proof of lemma I.11.11. □

Lemma I.11.35

(1) *If $\boldsymbol{y} \in C_{\lambda'}$ for all $\lambda' \prec_\Lambda \lambda$ and $l_\Lambda(\gamma_i, \gamma_j) \prec_\Lambda \lambda$ then $t_{ij}(\boldsymbol{y}) = \boldsymbol{y} \cdot \varphi(f_{\gamma_i}) * \varphi(f_{\gamma_j}) = 0$.*

(2) *if $\boldsymbol{y} \in C_{\lambda'}$ for all $\lambda' \prec_\Lambda \lambda$ but $\boldsymbol{y} \notin C_\lambda$ and $l_\Lambda(\gamma_i, \gamma_j) = \lambda$ then $t_{ij}(\boldsymbol{y}) = \boldsymbol{y} \cdot \varphi(f_{\gamma_i}) * \varphi(f_{\gamma_j}) \neq 0$.*

Proof:
As the proof of lemma I.11.12. □

Lemma I.11.36
For $\boldsymbol{y} \in \mathbb{F}_q^n$ let M be the corresponding matrix. We get

$$t_{uv}(\boldsymbol{y}) = \begin{cases} 0 & \text{if } u+v < r+1 \\ \text{not zero} & \text{if } u+v = r+1. \end{cases} \tag{I.11.33}$$

Proof:
Note that $u, v \leq r$ for all the entries considered in (I.11.33), that is we only work with the first r vectors of M. The proof follows the lines of the proof of lemma I.11.17. □

The natural generalization of definition I.11.18 is:

Definition I.11.37
Denote

$$\begin{aligned} d(\lambda) &:= \min\{\mu_\eta \,|\, \eta \succ_\Lambda \lambda\} \\ d_\varphi(\lambda) &:= \min\{\mu_\eta \,|\, \eta \succ_\Lambda \lambda, C_{\eta'} \neq C_\eta \text{ for any } \eta' \prec_\Lambda \eta\}. \end{aligned}$$

We will refer to $d_\varphi(\lambda)$ as the Feng-Rao distance.

The general version of the order bound is.

Theorem I.11.38
Let C_λ be defined from a surjective morphism φ. The minimum distance of C_λ is bounded by

$$d(C_\lambda) \geq d_\varphi(\lambda) \geq d(\lambda).$$

Proof:
The proof follows the lines of the proof of I.11.19. □

Remark I.11.39
The contents of remark I.11.5 and remark I.11.20 is of course still valid in this more general setting.

Remark I.11.40
If we label the n matrices M by $M_1, \ldots, M_n$ and the corresponding r-values by $r_1, \cdots, r_n$. Then we can construct a matrix H that contains, as the only rows, the first r_1 rows of M_1, the first r_2 rows of M_2, ..., the first r_n rows of M_n. This matrix will be of rank equal to n. That is, we could rewrite the above proof for the order bound using only one matrix.

Example I.11.41
This is a continuation of example I.11.27. By example I.11.28 and example I.11.21 the parameters of the C_λ codes are of course already known. However if we want to determine the Feng-Rao distances in the language of example I.11.27, then the derivation looks as follows

$$\begin{cases} \mu_{(0,1)} = 2 \\ \mu_{(1,0)} = 2 \\ \mu_{(1,1)} = 4 \end{cases} \quad \textit{giving} \quad \begin{cases} d_\varphi((0,0)) = 2 \\ d_\varphi((0,1)) = 2 \\ d_\varphi((1,0)) = 4. \end{cases}$$

I.11.2 Improved dual codes

In this section we shall see how to improve the construction of the dual codes of the evaluation codes. Again the first reference on the subject is [6]. This improvement is described in [21] in the case of C_l codes. The definitions of the improved codes and the bounds on their minimum distances described there, is immediately generalized to the general case C_λ, $\lambda \in \Lambda$ (where Λ is not necessarily ordered isomorphic to $\mathbb{N}$). We have the following general definition.

Definition I.11.42
Let $(f_\lambda \mid \lambda \in \Lambda)_{\prec_\Lambda}$ be a well-behaving basis. For any positive integer d define

$$\begin{aligned} \tilde{C}(d) &:= \{\boldsymbol{c} \in \mathbb{F}_q^n \mid \boldsymbol{c} \cdot \boldsymbol{h}_\lambda = 0 \textit{ for all } \lambda \in \Lambda \textit{ such that } \mu_\lambda < d\} \\ \tilde{C}_\varphi(d) &:= \{\boldsymbol{c} \in \mathbb{F}_q^n \mid \boldsymbol{c} \cdot \boldsymbol{h}_\lambda = 0 \textit{ for all } \lambda \in \Lambda \textit{ such that } \mu_\lambda < d \\ &\qquad \textit{and such that } C_{\lambda'} \neq C_\lambda \textit{ for any } \lambda' \prec_\Lambda \lambda\}. \end{aligned}$$

Of course the definitions simplify to

$$\begin{aligned} \tilde{C}(d) &:= \{\boldsymbol{c} \in \mathbb{F}_q^n \mid \boldsymbol{c} \cdot \boldsymbol{h}_l = 0 \text{ for all } l \in \mathbb{N} \text{ such that } \mu_l < d\} \\ \tilde{C}_\varphi(d) &:= \{\boldsymbol{c} \in \mathbb{F}_q^n \mid \boldsymbol{c} \cdot \boldsymbol{h}_l = 0 \text{ for all } l \in \mathbb{N} \text{ such that } \mu_l < d \\ &\qquad \text{and such that } C_{l-1} \neq C_l\} \end{aligned}$$

in the case of Λ being ordered isomorphic to $\mathbb{N}$.

Remark I.11.43
Again we get around the inconsistency in notation by the convention that we use the later notation whenever a well-behaving sequence exists.

From [21] we have the following counterpart to the order bound.

Theorem I.11.44
Let $\tilde{C}(d)$ and $\tilde{C}_\varphi(d)$ be constructed from a surjective morphism. The minimum distances is bounded by

$$d\left(\tilde{C}(d)\right) \geq d\left(\tilde{C}_\varphi(d)\right) \geq d$$

(here we use the convention $d(\{\mathbf{0}\}) = \infty$).

Proof:
The code $\tilde{C}(d)$ is contained in $\tilde{C}_\varphi(d)$. So it is enough to prove $d\left(\tilde{C}_\varphi(d)\right) \geq d$. The above convention ensures that the theorem holds in the case $\tilde{C}_\varphi(d) = \{\mathbf{0}\}$. Assume a nonzero $\boldsymbol{y} \in \tilde{C}_\varphi(d)$ is given. Let $\lambda \in \Lambda$ be the value such that $\boldsymbol{y} \in C_\lambda$ but $\boldsymbol{y} \notin C_{\lambda'}$ for any $\lambda' \prec_\Lambda \lambda$. Especially

$$\boldsymbol{y} \cdot \boldsymbol{h}_\lambda \neq 0. \tag{I.11.36}$$

From the proof of theorem I.11.38 we have $wt(\boldsymbol{y}) \geq \mu_\lambda$. Assume that theorem I.11.44 does not hold, implying that $\mu_\lambda < d$. But then by definition of $\tilde{C}_\varphi(d)$ we must have $\boldsymbol{y} \cdot \boldsymbol{h}_\lambda = 0$ contradicting (I.11.36). □

We will sometimes refer to theorem I.11.44 as the order bound for the $\tilde{C}(d)$ and the $\tilde{C}_\varphi(d)$ codes.

Remark I.11.45
To construct the $\tilde{C}_\varphi(d)$ code we need to know the set

$$S_d := \{\lambda \in \Lambda \mid \mu_\lambda < d, C_{\lambda'} \neq C_\lambda \text{ for any } \lambda' \prec_\Lambda \lambda\}.$$

The dimension of $\tilde{C}_\varphi(d)$ is easily found as $k = n - \#S_d$.

Example I.11.46
Consider the order domain $\mathbb{F}_3[X,Y]$ with weight function $\rho : \mathbb{F}_3[X,Y] \to \mathbb{N}_0^2 \cup \{-\infty\}$ induced by $\rho(X) = (1,0)$, $\rho(Y) = (0,1)$ and where $\mathbb{N}_0^2$ is ordered by $\prec_{st}$. A well-behaving sequence is given by

$$\begin{aligned}(f_1 = 1, f_2 = Y, f_3 = X, f_4 = Y^2, f_5 = XY, f_6 = X^2,\\ f_7 = Y^3, f_8 = XY^2, f_9 = X^2Y, f_{10} = X^3, f_{11} = Y^4,\\ f_{12} = XY^3, f_{13} = X^2Y^2, f_{14} = X^3Y, \ldots).\end{aligned} \tag{I.11.37}$$

The 9 points in $\mathbb{F}_3^2$ defines an evaluation map $ev : \mathbb{F}_3[X,Y] \to \mathbb{F}_3^2$. The indices l for which $C_l \neq C_{l-1}$ are $1,2,3,4,5,6,8,9,13$. And the corresponding μ-values are

$$\begin{aligned}\mu_1 = 1, \mu_2 = 2, \mu_3 = 2, \mu_4 = 3, \mu_5 = 4,\\ \mu_6 = 3, \mu_7 = 4, \mu_8 = 6, \mu_9 = 6, \mu_{13} = 9.\end{aligned}$$

So

$$\begin{aligned}\tilde{C}_\varphi(4) &= \{\boldsymbol{c} \in \mathbb{F}_3^9 \mid \boldsymbol{c}\cdot\boldsymbol{h_1} = \boldsymbol{c}\cdot\boldsymbol{h_2} = \boldsymbol{c}\cdot\boldsymbol{h_3} \\ &\qquad = \boldsymbol{c}\cdot\boldsymbol{h_4} = \boldsymbol{c}\cdot\boldsymbol{h_6} = 0\}\end{aligned}$$

has minimum distance at least 4 *and dimension* $k = 9 - 5 = 4$*. Whereas*

$$C_6 = \{\boldsymbol{c} \in \mathbb{F}_3^9 \mid \boldsymbol{c}\cdot\boldsymbol{h_1} = \cdots = \boldsymbol{c}\cdot\boldsymbol{h_6} = 0\}$$

has also minimum distance at least 4 *but only dimension* $k = 9 - 6 = 3$*. Note that* $\tilde{C}(4) = \tilde{C}_\varphi(4)$*.*

Example I.11.47
This is a continuation of example I.11.8 and example I.11.9. In both examples the sequence $(\mu_l \mid C_l \neq C_{l-1})$ *is non discreasing. We conclude that every* $\tilde{C}_\varphi(d)$ *code, constructed from the order sequences in examples I.11.8 and I.11.9, is also a* C_l *code.*

Example I.11.48
This is a continuation of example I.11.46. If we replace f_6 *in the order sequence (I.11.37) by* $f_6' := f_6 + f_5 = X^2 + XY$*, then we get a new order sequence for the same order function. The* $\tilde{C}_\varphi(4)$ *and* $\tilde{C}(4)$ *codes with respect to this order sequence are again equal. But they are different from the code from example I.11.46.*

Remark I.11.49
The $\tilde{C}(d)$ *and* $\tilde{C}_\varphi(d)$ *constructions rely on the choice of order basis. The dimension of the* $\tilde{C}_\varphi(d)$ *code is unaffected by the choice of order basis.*

I.11.3 Generalized Hamming weights

In the previous sections we saw how to estimate the minimum distances of a large class of the codes coming from order domains. In this section we mention how theorem I.11.38 can be generalized to work, not only for minimum distances, but for the so-called generalized Hamming weights. The generalized Hamming weights are parameters related to linear codes. We have the following definitions. Consider a set $D \subseteq \mathbb{F}_q^n$ and define

$$\mathrm{Supp}(D) := \{i \mid \exists \boldsymbol{v} = (v_1, \ldots, v_n) \in D \text{ such that } v_i \neq 0\}.$$

Given a linear code of dimension k then k parameters are defined as follows.

Definition I.11.50
Let C be a linear code of dimension k. The r.th generalized Hamming weight, $r \in \{1, \ldots, k\}$, is defined by

$$d^r(C) := \min\{\#\mathrm{Supp}(D) \mid D \text{ is a linear subspace of } C \text{ of dimension } r\}.$$

It is clear that $d^1(C)$ is the minimum distance of C. That is, the generalized Hamming weights can be understood as a generalization of the minimum distance of linear codes. The concept of generalized Hamming weights was originally studied in [18] and was later used for cryptographical purposes by Wei in [45] in 1991. Since 1991 a lot of research have been done on this area and many results have been achieved, although the area is still quite open. What is interesting to us here is, that some of the important achievements have been done using order domain theory. In [17] Heijnen and Pellikaan describe the following generalization of theorem I.11.19. First we need to extend definition I.11.13.

Definition I.11.51
Let R be an order domain that possesses a well-behaving sequence $(f_1, f_2, \ldots)$. Given numbers $l_1 < \cdots < l_r$ then

$$\mu^r_{l_1,\cdots,l_r} := \#\{(i,j) \in \mathbb{N}^2 \mid \exists\, s \in \{l_1, \ldots, l_r\} \text{ such that } l(i,j) = s\}.$$

Clearly $\mu^1_{l_1} = \mu_{l_1}$ (definition I.11.13).

Definition I.11.52
Let $(C_1, C_2, \ldots)$ be defined from a surjective morphism φ. Let N be a number such that $C_N = \{\mathbf{0}\}$. Denote

$$d^r_\varphi(l) := \min\{\mu^r_{l_1,\ldots,l_r} \mid l < l_1 < \cdots \leq N \text{ and } C_{l_i - 1} \neq C_{l_i},\ \forall i = 1, \ldots, r\}.$$

Clearly $d^1_\varphi(l) = d_\varphi(l)$ (definition I.11.18). The order bound for generalized Hamming weights can now be formulated as follows.

Theorem I.11.53
Let C_l be defined from a surjective morphism φ. The r.th generalized Hamming weight is bounded by

$$d^r(C_l) \geq d^r_\varphi(l).$$

It is shown in [17] that this bound is tight in the important case of Reed-Muller codes. Theorem I.11.53 is also used in [1] to find the generalized Hamming weights of the Hermitian codes.

Turning to the codes C_λ, coming from order bases that can not necessarily be ordered to become order sequences, we have the following modification of the above definitions and theorem I.11.53.

Definition I.11.54
Let $\{F_\lambda \mid \lambda \in \Lambda\}$ be an order basis for an order domain R (with respect to the ordering $\prec_\Lambda$ on Λ). Given elements $\lambda_1 \prec_\Lambda \cdots \prec_\Lambda \lambda_r$ then

$$\mu^r_{\lambda_1,\ldots,\lambda_r} := \#\left\{(\alpha,\beta) \in \Lambda^2 \mid \exists \sigma \in \{\lambda_1,\ldots,\lambda_r\} \text{ such that } l_\Lambda(\alpha,\beta) = \sigma\right\}.$$

Definition I.11.55
Let $\lambda_1,\ldots,\lambda_n$ be the unique elements in Λ such that $C_{\lambda_i} \neq C_{\lambda'}$ for any $\lambda' \prec_\Lambda \lambda_i$, $i = 1,\ldots,n$. Denote

$$d^r_\varphi(\lambda) := \min\left\{\mu^r_{\lambda_{j_1},\ldots,\lambda_{j_r}} \mid \lambda \prec_\Lambda \lambda_{j_1} \prec_\Lambda \cdots \prec_\Lambda \lambda_{j_r}, \ \lambda_{j_i} \in \{\lambda_1,\ldots,\lambda_n\},\ i = 1,\ldots,r\right\}.$$

Theorem I.11.56
Let C_λ be defined from a surjective morphism φ. The r.th generalized Hamming weight is bounded by

$$d^r(C_\lambda) \geq d^r_\varphi(\lambda).$$

A rough outline of a proof:
In exactly the same way as we modified the proof of theorem I.11.19 to give a proof of theorem I.11.38, we can modify the proof of theorem I.11.53 from [17], to give a proof of theorem I.11.56. Especially we keep the definitions of M and $T(\boldsymbol{y})$. We notice that the choice of M is even more natural in the later case. □

I.12
New codes and new descriptions of old codes

In this chapter we will compare the constructions of codes from order domains, with previous known constructions of codes. In this connection we will consider Feng and Rao's codes from [7] as codes constructed from order domains, although the concept of an order domain was not invented then. We will illustrate how the codes from order domains can be seen as a generalization of the Reed-Muller codes and the 1-point geometric Goppa codes. A description of this can also be found in [7] and [21]. We are in this chapter only concerned with codes defined from order sequences, as we have not demonstrated that the generalization from section I.11.1.2 actually gives more codes than can already be constructed using the techniques from section I.11.1.1.

I.12.1 Reed-Muller codes

In this section we will, from an order domain theoretical point of view, discuss the well-known Reed-Muller codes and an important generalization of these. We will only be concerned with the affine ones, that is, we do not consider projective Reed-Muller codes.

Consider the affine space $\mathbb{A}^m_{\mathbb{F}_q} = \mathbb{F}^m_q$. Denote $n := q^m$ and let $\{P_1, \ldots, P_n\}$ be the points in $\mathbb{F}^m_q$. By φ we denote the surjective evaluation map

$$\varphi : \begin{cases} \mathbb{F}_q[X_1, \ldots, X_m] & \to & \mathbb{F}^m_q \\ F & \mapsto & (F(P_1), \ldots, F(P_n)) \,. \end{cases}$$

Define

$$\begin{aligned} \Delta_q \;\; := \;\; & \{M \mid M \;\text{ a monomial,} \\ & \quad \text{and } \deg_{X_i}(M) < q, \; i = 1, \ldots, m\} \end{aligned} \tag{I.12.2}$$

and note that

$$\varphi(\Delta_q) = \{\varphi(M) \mid M \in \Delta_q\}$$

is a basis for $\mathbb{F}_q^m$. We have the following definition of a Reed-Muller code $RM_q(r,m)$.

Definition I.12.1
Let r be a nonnegative integer, m a positive integer and q a prime power. The r.th order q-ary Reed-Muller code (abbreviated RM-code) of length $n = q^m$ is the vector space

$$RM_q(r,m) := \mathrm{span}_{\mathbb{F}_q}\{\varphi(M) \mid M \text{ a monomial in } X_1,\ldots,X_m \text{ and } \deg(M) \leq r\}.$$

It is a well-known fact that $RM_q(r,m)^\perp = RM_q(m(q-1)-r-1,m)$. If we define an appropriate weight function ρ on $R := \mathbb{F}_q[X_1,\ldots,X_m]$ then $RM_q(r,m)$ becomes a code of type E_l. One such choice is the weight function $\rho : R \to \mathbb{N}_0^m$ induced by the weights

$$\begin{array}{rcl} \rho(X_1) & = & (1,0,0,\ldots,0) \\ \rho(X_2) & = & (0,1,0,\ldots,0) \\ & \vdots & \\ \rho(X_m) & = & (0,0,\ldots,0,1) \end{array} \tag{I.12.4}$$

and where $\mathbb{N}_0^0$ is ordered by $\prec_{st}$. We get a well-behaving sequence

$$(1, X_m, X_{m-1}, \ldots, X_1, X_m^2, \ldots, X_2X_1, X_1^2, X_m^3, \ldots). \tag{I.12.5}$$

And $RM_q(r,m) = E_l$ where l is the index such that $f_l = X_1^r$. In [21, Sec. 4] it was first shown that the order bound gives the right value of the minimum distance of any $RM_q^\perp(r,m)$ code (and thereby of any $RM_q(r,m)$ code). In [17] it is (as noted in the previous chapter) shown, that even the generalization of the order bound to case of generalized Hamming weights, is tight in the case of a RM-code.

Example I.12.2
This is a continuation of example I.11.8. We have

$$E_1 = RM_2(0,2) = C_3$$
$$E_3 = RM_2(1,2) = C_1.$$

Example I.12.3
This is a continuation of example I.11.46. We have

$$E_1 = RM_3(0,2) = C_{13}$$
$$E_3 = RM_3(1,2) = C_6$$
$$E_6 = RM_3(2,2) = C_3$$
$$E_{13} = RM_3(3,2) = C_1.$$

From [41] we have the following definition of what we will call a weighted Reed-Muller code, or abbreviated a WRM-code. The definition calls for a set of weights $W = \{w(X_1), \ldots, w(X_m) \in \mathbb{N}\}$. By wdeg we denote the corresponding weighted degree function on $\mathbb{F}_q[X_1, \ldots, X_m]$.

Definition I.12.4
Let r be a nonnegative integer, m a positive integer and q a prime power. The r.th order q-ary Reed-Muller code of length $n = q^m$ defined from the set W of weights is the vector space

$$WRM_q(r, m, W) := \mathrm{span}_{\mathbb{F}_q}\{\varphi(M) \mid M \textit{ a monomial in } X_1, \ldots, X_m \textit{ and } \mathrm{wdeg}(M) \leq r\}.$$

According to [41] the dual of a weighted Reed-Muller code is again a weighted Reed-Muller code. By [41, Rem. 1] the parameters of the WRM codes are worse or equal to the parameters of the RM codes. Again it is obvious that a weight function on R can be defined such that $WRM_q(r, m, W)$ becomes a code of type E_l. Simply define a weight function by

$$\begin{array}{rcl} \rho(X_1) & = & (w(X_1), 0, 0, \ldots, 0) \\ \rho(X_2) & = & (0, w(X_2), 0, \ldots, 0) \\ & \vdots & \\ \rho(X_m) & = & (0, 0, \ldots, 0, w(X_m)) \end{array} \tag{I.12.6}$$

and order $\mathbb{N}_0^m$ by $\prec_{st}$.

Recall that only for certain choices of l, the code E_l, corresponding to the order sequence (I.12.5), is a RM code. However it is a WRM code. This is seen as follows. We first note that if $M \notin \Delta_q$ then there exists a $M' \in \Delta_q$ such that $\varphi(M) = \varphi(M')$ and such that $M' \mid M$. We now choose weights $w(X_1), \ldots, w(X_m)$ such that $\mathrm{wdeg}(M_1) < \mathrm{wdeg}(M_2)$ for $M_1, M_2 \in \Delta_q$ if and only if M_1 comes before M_2 in the order sequence (I.12.5). The result follows. A similar result clearly holds for the E_l codes related to the order function defined by (I.12.6).

Consider now any order function ρ on $\mathbb{F}_q[X_1, \ldots, X_m]$ for which the set of monomials constitutes an order basis $\mathcal{B}$. If $m = 2$ then we have, from section I.3.3, a complete picture of the monomial orderings that gives order functions. It is clear that when $m = 2$, then for any of these monomial orderings $\prec_{\mathbb{N}_0^r}$ one can find a weighted degree lexicographic ordering $\prec_w$ with weights $w(X_1), \ldots, w(X_m) \in \mathbb{N}_0$, that approximate the monomial ordering in the sense,

that if $M_1, M_2 \in \Delta_q$ satisfies $M_1 \prec_{\mathbb{N}_0^r} M_2$ then $w(M_1) < w(M_2)$. It follows that for $m = 2$ any E_l code corresponding to the order basis $\mathcal{B}$ can be described as a WRM code. However when $m > 2$ then the situation is not so clear. We leave it as an open problem to decide whether the result holds for arbitrary m.

Recall that, in example I.9.3 and example I.9.4, we showed that there are order functions on $k[X_1, X_2]$ that does not correspond to monomial orderings on $k[X_1, X_2]$. We can conclude that the set of E_l codes defined from a polynomial ring $\mathbb{F}_q[X_1, \ldots, X_m]$ ($m \geq 2$) is larger that the set of WRM codes defined from $\mathbb{F}_q[X_1, \ldots, X_m]$.

Finally we discuss the codes of type $\tilde{C}_\varphi(d)$. We claim that if ρ and ρ' are two order functions on $\mathbb{F}_q[X_1, \ldots, X_m]$, such that both have the set of monomials as an order basis, then the codes $\tilde{C}_\varphi(d)$ are the same. To see this let M be a monomial in $\mathbb{F}_q[X_1, \ldots, X_m]$, say $M = f_i$ with respect to ρ and $M = f_{i'}$ with respect to ρ'. We must convince our selves that $C_i \neq C_{i-1}$ (with respect to ρ) if and only if $C_{i'} \neq C_{i'-1}$ (with respect to ρ'). The result follows from the following already mentioned facts. First $\varphi(\Delta_q)$ is a basis for $\mathbb{F}_q^m$. And second, if a monomial $M \notin \Delta_q$ is considered, then there exists an $M' \in \Delta_q$, such that $\varphi(M) = \varphi(M')$, and such that $M' \mid M$.

Finally a $\tilde{C}_\varphi(d)$ code of the above type can not in general be described as an E_l code coming from a monomial ordering on $\mathcal{M}_m$. Simply note that the μ-value corresponding to X_1^2 and X_2^2 is 3, and that the μ-value corresponding to X_1X_2 is 4. If a monomial ordering $\prec$ on $\mathbb{F}_q[X_1, X_2]$ was to respect $X_1^2, X_2^2 \prec X_1X_2$ then we would have $X_1 \prec X_2 \prec X_1$, a contradiction. We have once again demonstrated that the order domain methods give new classes of codes coming from polynomial rings.

I.12.2 Geometric Goppa codes

An important motivation for introducing the concept of order domains in the first place was, that one wanted to simplify the description of the so-called 1-point geometric Goppa codes. We have the following general definition of geometric Goppa codes.

Definition I.12.5
Consider an algebraic function field $\mathcal{F}$ over $\mathbb{F}_q$ of one variable. Let $P_1, \ldots, P_n$ be rational places and denote $D = P_1, \ldots, P_n$. Let $G = \sum n_P P$ be a divisor such that $n_{P_i} = 0$ for $i = 1, \ldots, n$. The geometric Goppa code $C_{\mathcal{L}}(D, G)$ is the

code

$$C_{\mathcal{L}}(D,G) := \{(f(P_1),\ldots,f(P_n)) \mid f \in \mathcal{L}(G)\}.$$

If $G = mQ$ and Q is rational, then $C_{\mathcal{L}}(D,G)$ is said to be a 1-point geometric Goppa code.

Clearly $C_{\mathcal{L}}(D,G)$ is $\mathbb{F}_q$ linear, and if $\{f_1,\ldots,f_s\}$ is a basis for $\mathcal{L}(G)$, then

$$\{(f_1(P_1),\ldots,f_1(P_n)),\ldots,(f_s(P_1),\ldots f_s(P_n))\}$$

is a basis for $C_{\mathcal{L}}(D,G)$. The following well-known theorem describes the parameters of the code.

Theorem I.12.6
Let $C_{\mathcal{L}}(D,G)$ be a geometric Goppa code with $\deg(G) < n$. The parameters of $C_{\mathcal{L}}(D,G)$ are described by

$$d \geq n - \deg(G) \tag{I.12.8}$$

$$k = \dim(G) \geq \deg(G) + 1 - g \tag{I.12.9}$$

where g is the genus of $\mathcal{F}$. If in particular $2g-2 < \deg(G) < n$ then equality holds in (I.12.9).

Proof:
The proof relies heavily on the Riemann-Roch Theorem, see [38]. □

It is clear that the set of E_l codes related to order domains of transcendence degree 1 contains the 1-point geometric Goppa codes as a subset, simply because $\cup_{m=0}^{\infty}\mathcal{L}(mQ)$ is an order domain when Q is rational (the first part of proposition I.10.10), and because the residue map is an $\mathbb{F}_q$ morphism. Similar it is clear that the set of C_l codes related to R contains the set of duals of 1-point geometric Goppa codes as a subset. Now from the second part of proposition I.10.10 we know that any order domain R with a weight function

$$\rho : R \to \Lambda_{-\infty} \subseteq \mathbb{N}_0 \cup \{-\infty\}$$

can be described on the form $R = k[X_1,\ldots,X_m]/I$, such that the quotient field $\mathcal{F} := \mathrm{Quot}(R)$ is an algebraic function field (of one variable) with a unique place P at infinity, and such that this place satisfies $\rho(f) = -v_P(f)$ for any $f \in R$. Regarding the nature of the surjective morphisms $\varphi : R \to \mathbb{F}_q^n$, Matsumoto shows in [26], that any surjective morphism $\varphi : R \to \mathbb{F}_q^n$ is of the form $\varphi(f) = (f(P_1),\ldots,f(P_n))$ where $P_1,\ldots,P_n$ are rational places in $\mathcal{F}$ (this result also holds for non finite constant fields k). From this fact it is (as noted

in [26]) clear that every E_l code related to an order domain of transcendence degree 1 can be understood as a 1-point geometric Goppa code. And it is clear that a similar result holds for the C_l codes. Finally of course also the $\tilde{C}_\varphi(d)$ codes can be understood in the language of geometric Goppa codes. Matsumoto notes that they corresponds to what he calls Miura's generalization of 1-point geometric Goppa codes (the references are [27] and [28]).

Regarding the estimation of the minimum distance, it is clear that the bound in theorem I.11.23 equals the bound in theorem I.12.6. Matsumoto notes that the bounds on the minimum distance of C_l and $\tilde{C}_\varphi(d)$, that we treated earlier in this thesis, equals the bounds stated by Miura.

The advantage of using order domain theory to describe 1-point geometric Goppa codes should be obvious. Note that from an order domain point of view singular points are no more difficult to handle that nonsingular ones.

I.12.3 The new constructions versus previous constructions

As demonstrated in section I.12.1 and section I.12.2, the set of codes constructed from order domains contains as important special cases the following codes. Namely the 1-point geometric Goppa codes, the duals of 1-point geometric Goppa codes and the WRM-codes. Further in the case of an order domain R of transcendence degree 1 the $\tilde{C}_\varphi(d)$ construction can be viewed as an improvement of the duals of 1-point geometric Goppa codes.
Beside these codes we get a new large class of descriptions of codes coming from order domains of transcendence degree larger than 1. Whenever these codes are of type C_l, $\tilde{C}(d)$ or $\tilde{C}_\varphi(d)$, the description includes an estimation of their minimum distances. One can think of the C_l-codes as generalizations of the duals of the 1-point geometric Goppa codes. That is a generalization to the case of function fields of arbitrary high transcendence degree. We mention that J. P. Hansen in [15] and S. H. Hansen in [16] succeed in constructing generalizations of geometric Goppa codes, to the case of higher dimensional function fields by use of algebraic geometry.

All together the application of order domain theory in coding theory has three important advantages.

- The descriptions are simplified for many of the already known codes
- We get new classes of codes coming from $\mathbb{F}_q$-algebras of transcendence degree larger than 1

- We get improvements by the $\tilde{C}_{\varphi}(d)$ construction.

In figure I.12.1 an overview of the different constructions is given. It is important to notice that the figure gives a picture of the relationship between the different classes of constructions; not a clear picture of the relationship between the different classes of codes. To see why this is so, just notice, that actually all linear codes can be described as geometric Goppa codes (see [34]), and that some 1-point geometric Goppa codes can also be described as duals of 1-point geometric Goppa codes (see [1] for an example).

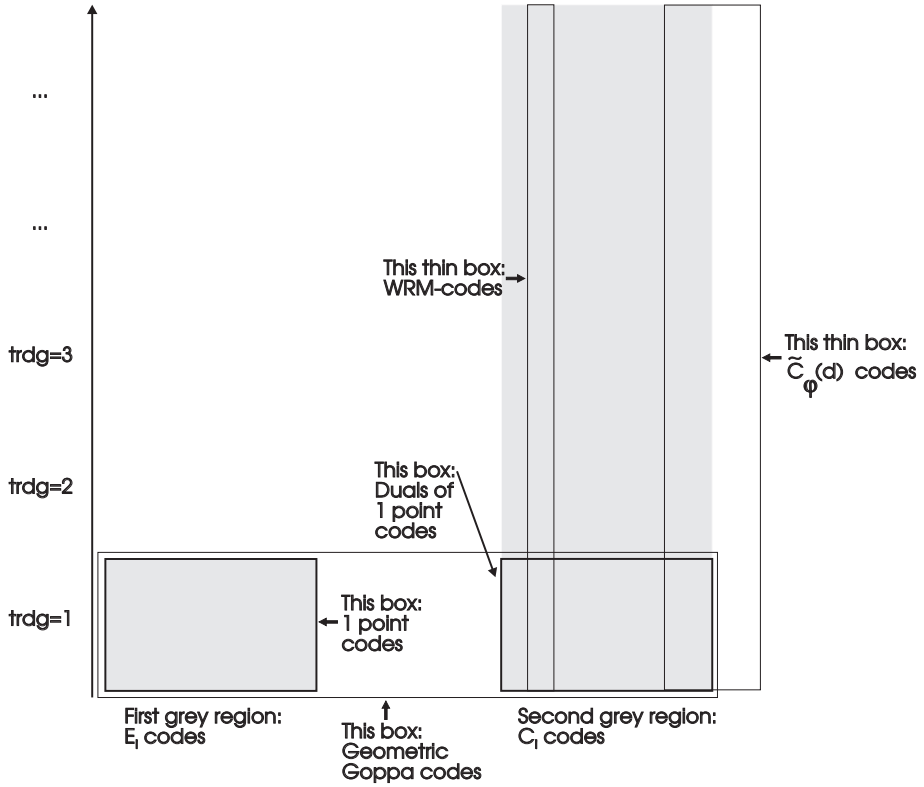

Figure I.12.1: The relationship between the different classes of constructions. The E_l codes are left out for $\mathbb{F}_q$-algebras of transcendence degree larger than 1, as no estimation of their minimum distances is known.

I.13

Changing the parameters of $\tilde{C}_{\varphi}(d)$ by changing $\prec_{\Lambda}$

Every order domain R of transcendence degree at least 2 presented in this thesis, possesses infinitely large families of weight functions, such that if ρ and ρ' are weight functions in the family then the following holds. Both ρ and ρ' has value semigroup Λ but the corresponding monomial orderings on Λ are different. Further there exists a basis for R that is an order basis for both ρ and ρ'. And ρ and ρ' are identical on this basis. In other words, the indexed order bases are the same.
While the $\tilde{C}(d)$ construction is unaffected by this change of ordering on the indexed order basis, this is clearly in general not the case for the C_l construction. Regarding the $\tilde{C}_{\varphi}(d)$ construction, we will see in the following, that it is in some cases unaffected, and in other cases affected by a change of ordering on Λ.

In the following example we show that $\tilde{C}_{\varphi}(d)$ might be independent of the choice of ordering on Λ, although infinitely many choices of proper ordering on Λ exist.

Example I.13.1
Consider the toric ideal

$$I := \langle X_1X_2 + X_3^2 \rangle \subseteq \mathbb{F}_2[X_1, X_2, X_3].$$

We have a weight function

$$\rho : R := \mathbb{F}_2[X_1, X_2, X_3]/I \to \Lambda_{-\infty} := \langle (2,0), (0,2), (1,1) \rangle \cup \{-\infty\}$$

induced by

$$\begin{aligned} \rho(x_1 := X_1 + I) &= (2,0) \\ \rho(x_2 := X_2 + I) &= (0,2) \\ \rho(x_3 := X_3 + I) &= (1,1) \end{aligned}$$

and by some arbitrary monomial ordering $\prec_\Lambda$ on Λ. Let $\Delta(I)$ be one of the two possibilities of a footprint of I, and

$$\mathcal{B} := \{M + I \mid M \in \Delta(I)\}$$

the corresponding basis for R. Now if we index the elements of $\mathcal{B}$ according to their orders and if we then order the elements in $\mathcal{B}_\rho$ according to $\prec_\Lambda$ (used on the indices), then we get a well behaving basis. For any monomial ordering $\prec_\Lambda$ on $\Lambda_{-\infty}$ we know in advance that

- *x_i is of lower index than x_i^a for $a > 1$ and $i = 1, \ldots, 3$*
- *x_3 is of lower index than x_1x_3, x_3x_3 and x_1x_2*

(to see that x_3 is of lower index than x_1x_2 just note that $\rho(x_3) = (1,1)$ and $\rho(x_1x_2) = (2,2)$).
Now the variety corresponding to I is

$$\mathcal{V}_{\mathbb{F}_2}(I) = \{(0,0,0), (1,0,0), (0,1,0), (1,1,1)\}$$

giving us the evaluation map ev. We have

$$\begin{aligned} ev(x_i) &= ev(x_i^a) \quad \text{for } a > 1, i = 1, \ldots, 3 \\ ev(x_3) &= ev(x_1x_2) = ev(x_1x_3) = ev(x_2x_3). \end{aligned}$$

So no matter which ordering $\prec_\Lambda$ we choose then a basis element f_λ in $\mathcal{B}$ such that

$$ev(f_\lambda) \notin \operatorname{span}_{\mathbb{F}_2}\{ev(f_{\lambda'}) \mid \lambda' \prec_{\mathbb{N}_0^2}\} \tag{I.13.4}$$

must be either $1, x_1, x_2$ or x_3. As the number of possible choices of f_λ such that (I.13.4) is satisfied equals $\#\mathcal{V}_{\mathbb{F}_2}(I)$, we conclude the following. Different choices of $\prec_\Lambda$ might give different codes C_l, but the codes $\tilde{C}_\varphi(d)$ will be independent of the choice of $\prec_\Lambda$.

In the next example we will see that there exist order domains such that different legal choices of ordering on Λ give different $\tilde{C}_\varphi(d)$ codes. In the example, actually even the parameters of the codes, will be dependent on the choice of the ordering on Λ.

Example I.13.2
Consider the toric ideal

$$I := \langle X_1X_2^2 - X_3^3 \rangle \subseteq \mathbb{F}_3[X_1, X_2, X_3].$$

We have a weight function

$$\rho : R := \mathbb{F}_3[X_1, X_2, X_3]/I \to \Lambda_{-\infty} := \langle (0,6), (3,0), (2,2) \rangle \cup \{-\infty\}$$

induced by

$$\begin{aligned} \rho(x_1 := X_1 + I) &= (0,6) \\ \rho(x_2 := X_2 + I) &= (3,0) \\ \rho(x_3 := X_3 + I) &= (2,2) \end{aligned}$$

and by some arbitrary monomial ordering $\prec_\Lambda$ on Λ. Consider the footprint

$$\Delta(I) = \{X_1^\alpha X_2^\beta X_3^\gamma \mid \gamma < 3\}$$

and the corresponding indexed order basis for R

$$\mathcal{B}_\rho := \{f_{\rho(M+I)} := M + I \mid M \in \Delta(I)\}.$$

In the following we will construct codes of the type $\tilde{C}_\varphi(d)$ corresponding to two different orderings $\prec_\Lambda$.
The variety of I is

$$\begin{aligned} \mathcal{V}_{\mathbb{F}_3}(I) &= \{(0,0,0), (1,0,0), (2,0,0), (0,1,0), (0,2,0), \\ &\quad (1,1,1), (1,2,1), (2,1,2), (2,2,2)\} \end{aligned}$$

defining our ev map. So the codes will be of length 9. In the following we use the notation $f := F + I$.

Case I:
Assume $\prec_{\mathbb{N}_0^2}$ is the standard ordering $\prec_{st}$. One can show that the basis elements f_i in $\mathcal{B}$ such that $C_i \neq C_{i-1}$ are

$$\{1, x_2, x_3, x_1, x_2^2, x_2x_3, x_3^2, x_2x_3^2, x_1^2\}$$

(ordered with respect to $\prec_{\mathbb{N}_0^2}$). The corresponding set of μ values is

$$\{1, 2, 2, 2, 3, 4, 3, 6, 3\}.$$

Now $\tilde{C}_\varphi(3)$ has parity check matrix

$$\tilde{H}_\varphi(3) = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 2 & 1 & 2 & 1 & 2 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 2 & 2 \\ 0 & 1 & 2 & 0 & 0 & 1 & 1 & 2 & 2 \end{bmatrix} \tag{I.13.5}$$

and the order bound is tight as

$$(1,1,1,0,0,0,0,0,0) \in \tilde{C}_\varphi(3).$$

Of course the dimension is $k = 9 - 4 = 5$.
Turning to the code $\tilde{C}_\varphi(4)$ *we have parity check matrix*

$$\tilde{H}_\varphi(4) = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 2 & 1 & 2 & 1 & 2 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 2 & 2 \\ 0 & 1 & 2 & 0 & 0 & 1 & 1 & 2 & 2 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}. \tag{I.13.6}$$

The order bound is tight as

$$(0,0,0,1,2,2,1,0,0) \in \tilde{C}_\varphi(4)$$

and the dimension is $k = 9 - 7 = 2$.

Case II
We choose $\prec_{\mathbb{N}_0^2}$ *to be the weighted degree lexicographic ordering composed by* $w((1,0)) = 2$, $w((0,1)) = 1$ *and* $(1,0) \succ_{lex} (0,1)$. *And* $\prec_\Lambda$ *to be the restriction of this. One can show that the basis elements* f_i *in* $\mathcal{B}$ *such that* $C_i \neq C_{i-1}$ *are*

$$\{1, x_1, x_3, x_2, x_1^2, x_1x_3, x_1x_2, x_2^2, x_1^2x_2\}$$

(ordered with respect to $\prec_{\mathbb{N}_0^2}$*). The corresponding set of* μ *values is*

$$\{1,2,2,2,3,4,4,3,6\}.$$

Now the $\tilde{C}_\varphi(3)$ *code is exactly the same as in case I. However the* $\tilde{C}_\varphi(4)$ *code is improved as the row*

$$ev(x_3^2) = (0,0,0,0,0,1,1,1,1)$$

is to be removed from (I.13.6) to establish the new $\tilde{H}_\varphi(4)$. *The order bound is again tight as of course still* $(0,0,0,1,2,2,1,0,0) \in \tilde{C}_\varphi(4)$. *The dimension is larger than before namely* $k = 9 - 6 = 3$. *So the code is indeed improved.*

I.14
Some tools for constructing the codes

In this chapter we will describe some tools that are nice to have, both when one construct codes in practice, and when one constructs codes on a theoretical level. First we will be concerned with the length n of the codes. We will derive an upper bound on n in the cases of φ being an evaluation map ev. Next we will be concerned with narrowing the set of elements f_λ in the order basis $\{f_\lambda \mid \lambda \in \Lambda\}$ that need to be considered when the codes are constructed. Finally we will derive some bounds on the values $\mu(f_\lambda)$ in certain special cases.

I.14.1 The restricted footprint bound

Assume $\varphi : \mathbb{F}_q[\boldsymbol{X}]/I \to \mathbb{F}_q^n$ is an evaluation map, that is φ is of the form

$$ev : \begin{cases} \mathbb{F}_q[\boldsymbol{X}]/I & \to & \mathbb{F}_q^n \\ F + I & \mapsto & (F(P_1), \ldots, F(P_n)) \end{cases} \tag{I.14.1}$$

where

$$\{P_1, \ldots, P_n\} \subseteq \mathcal{V}_{\mathbb{F}_q}(I). \tag{I.14.2}$$

In the rest of this section we choose

$$n := \#\mathcal{V}_{\mathbb{F}_q}(I),$$

that is we use all the points from $\mathcal{V}_{\mathbb{F}_q}(I)$.

Given any ideal $J \subseteq k[\boldsymbol{X}]$, then the footprint bound (see appendix I.A) states that

$$\#\mathcal{V}_k(J) \leq \#\Delta(J) \tag{I.14.3}$$

where $\Delta(J)$ is the footprint of J with respect to some monomial ordering on $\mathcal{M}(\boldsymbol{X})$. And equality holds in (I.14.3) precisely when $J = \mathcal{I}(\mathcal{V}_k(J))$.
So a way to determine n without actually evaluating all the points of $\mathbb{F}_q^m$ in the generators $F_1, \ldots, F_s$ of $I \subseteq \mathbb{F}_q[X_1, \ldots, X_m]$, would be to find $I'' := \mathcal{I}(\mathcal{V}_{\mathbb{F}_q}(I))$. The footprint bound then tells us that $n = \#\Delta(I'')$, where the

footprint is taken with respect to any monomial ordering on $\mathbb{F}_q[X_1, \ldots, X_m]$. Unfortunately there apparently is no general method to find I''. However I'' must contain[1]

$$\begin{aligned} I' &:= I + \langle X_1^q - X_1, \ldots, X_m^q - X_m \rangle \\ &= \langle F_1, \ldots, F_s, X_1^q - X_1, \ldots, X_m^q - X_m \rangle. \end{aligned}$$

That is $\Delta(I'') \subseteq \Delta(I')$ giving us the bound

$$n \leq \#\Delta(I').$$

Note that in the case $n = \#\Delta(I')$ we have $I' = I''$.

Example I.14.1
Assume we want to study type-I curves $X^a + uY^b + G(X, Y)$ where $a > b$ is known, but $u \neq 0$ and $G(X, Y)$ is not. The only thing that is known about $G(X, Y)$ is, that it contains no monomials $X^\alpha Y^\beta$ such that $\alpha b + \beta a \geq ab$. In this general setting we will not be able to calculate a Gröbner basis for

$$I' = \langle X^a + uY^b + G(X, Y), X^q - X, Y^q - Y \rangle,$$

meaning that we will not be able to determine $\Delta(I')$. However

$$\Delta(I') \subseteq \{M \in \Delta(I) \mid \deg_X M < q, \deg_Y M < q\} =: \Delta_q(I).$$

Giving us $n \leq \#\Delta_q(I)$. Now different choices of monomial ordering on $\mathcal{M}(X, Y)$, may (and will in many cases) lead to different values of $\#\Delta_q(I)$. In the case of $a < q$ the most narrow bound is found by choosing Y^b as the leading monomial. We get $n \leq aq$. Choosing instead X^a to be the leading monomial gives the weaker bound $n \leq \min\{bq, q^2\}$.

In general we have the following definition.

Definition I.14.2
Given a monomial ordering on $\mathcal{M}(X_1, \ldots, X_m)$, define the restricted footprint to be

$$\Delta_q(I) := \{M \in \Delta(I) \mid \deg_{X_i} M < q,\ i = 1, \ldots, m\}.$$

We have the general result.

[1] Note added in the second edition: In the manuscript "On the construction of codes from order domains", june 2000 by Olav Geil, it is shown that $I' = I''$.

Theorem I.14.3
The number of points in a variety $\mathcal{V}_{\mathbb{F}_q}(I)$ is bounded by

$$n = \#\mathcal{V}_{\mathbb{F}_q}(I) \leq \min\{\#\Delta_q(I) \,|\, \Delta(I) \text{ a footprint of } I\}. \tag{I.14.7}$$

We will refer to this result as the restricted footprint bound.

Example I.14.4
Consider the order ideal $I := \langle X^4 - Y^3 \rangle \subseteq \mathbb{F}_4[X,Y]$. The following calculations are with respect to the weighted degree lexicographic ordering given by $w(X) = 3$, $W(Y) = 4$ and $Y \succ_{lex} X$. The footprint is given by $\Delta(I) = \{X^\alpha Y^\beta \,|\, \beta < 3\}$ and the restricted footprint equals $\Delta_4(I) = \{X^\alpha Y^\beta \,|\, \alpha < 4, \beta < 3\}$. To find $\Delta(I')$ we use Buchberger's algorithm on $\{Y^3 - X^4, X^4 - X, Y^4 - Y\}$ to get the reduced Gröbner basis $\{Y^3 - X^4, YX + Y, X^2 + X\}$. We conclude that $\Delta(I') = \{1, X, Y, Y^2\}$. Now I is a toric ideal. From proposition I.6.10 we have $\#\mathcal{V}_{\mathbb{F}_4}(I) = q = 4$. And we conclude that $I'' = I'$. The situation is illustrated in figure I.14.1.

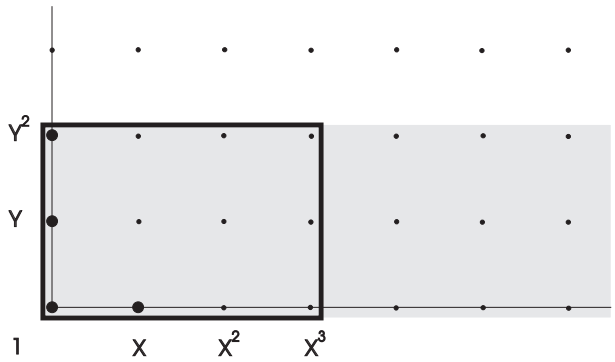

Figure I.14.1: The shadowed region is $\Delta(I)$, the framed region $\Delta_q(I)$ and the boldet dots constitutes $\Delta(I') = \Delta(I'')$.

Note that the restricted footprint is a footprint in the special case where $n = \Delta_q(I)$. That the restricted footprint bound can actually be attained, is seen in the following example.

Example I.14.5
Consider the Hermitian curve $\mathcal{V}_{\mathbb{F}_{q^2}}(I)$ where

$$I := \langle X^{q+1} - Y^q - Y \rangle \subseteq \mathbb{F}_{q^2}[X,Y].$$

From (I.14.7) we have $n \leq q^3$ (there are only two possible restricted footprints to consider). It is well known (and easily seen) that actually $n = q^3$ holds.

Example I.14.6
This example is a continuation of example I.10.15 and example I.14.1. We will discuss the restricted footprint bound versus the so-called Hasse-Weil bound in the case of a type-I curve, that is a curve

$$F(X,Y) = X^a + uY^b + G(X,Y) \in \mathbb{F}_q[X,Y]$$

where $\gcd(a,b) = 1$ and $\mathrm{wdeg}(G) < ab$ (wlog. we assume $a > b$). Let $\mathcal{F}$ be an algebraic function field of one variable over $\mathbb{F}_q$, and denote by N_P the number of rational places of $\mathcal{F}$. The Hasse-Weil bound gives the following bound on N_P

$$|N_P - (q+1)| \leq 2gq^{1/2} \tag{I.14.9}$$

where g is the genus of $\mathcal{F}$ (for a proof see [38, Sec. V.2]). Recall that the function field $\mathcal{F}$ corresponding to a type-I curve has precisely one place at infinity, and that this place is rational. According to the discussion on page 86, any other rational place must correspond to a nonsingular affine point on the curve, or to a singular eventually projective point on the curve. And no two different points correspond to the same place. Beside these points there may be singular points that does not correspond to rational places. From (I.14.9) we get that the number n_{nons} of nonsingular points in $\mathcal{V}_{\mathbb{F}_q}(\langle F(X,Y)\rangle)$ is bounded by

$$n_{nons} \leq 2gq^{1/2} + q. \tag{I.14.10}$$

To translate (I.14.10) into something useful we must have a picture of the size of the genus g. According to Weierstrass Gap theorem (theorem I.10.9) the genus equals

$$\begin{aligned} g \;=\; \{\gamma \mid \gamma \in \mathbb{N},\;\; &\text{there exist no element } f \in \mathcal{F} \\ &\text{such that } v_{P_\infty}(f) = \gamma \text{ and } v_Q(f) \geq 0 \;\forall\, Q \neq P_\infty\}. \end{aligned}$$

We have

$$\begin{aligned} g &\leq \#(\mathbb{N}_0 \setminus \langle a,b\rangle) && \text{(I.14.11)} \\ &= (a-1)(b-1)/2 && \text{(I.14.12)} \end{aligned}$$

and equality holds in (I.14.11) if $R \simeq \mathcal{L}(P_\infty)$ (the equality in (I.14.12) can be found in [21, Prop. 5.11]). Combining (I.14.10) and (I.14.12) we get

$$n_{nons} \leq (a-1)(b-1)q^{1/2} + q. \tag{I.14.13}$$

Using instead the restricted footprint bound we get

$$n_{nons} \leq n \leq \min\{q^2, bq\}. \tag{I.14.14}$$

If $a = q^{1/2} + 1$ and $b \leq q$ then the bounds (I.14.13) and (I.14.14) are equal. For some choices of a, b, q (I.14.13) constitutes the narrowest bound, for other choices (I.14.14) does.

Example I.14.7
This is a continuation of example I.6.11 and example I.6.12. In the first example we studied the toric ideal $I \subseteq \mathbb{F}_2[X_{11}, X_{21}, X_{12}, X_{22}, X_{13}, X_{23}]$ generated by the 2×2 minors of the 2×3 matrix $[X_{ij}]$ of indeterminates. We noted that the variety $\mathcal{V}_{\mathbb{F}_2}(I)$ contains 22 points. That is, considerable more than our first guess, that was 16 points. By inspection on the generators of the ideal, we see that the restricted footprint bound states $\#\mathcal{V}_{\mathbb{F}_2}(I) \leq 32$. So we can not conclude that $\#\mathcal{V}_{\mathbb{F}_2}(I)$ is nearly maximal in that sense. Repeating for the second example, that is for the toric ideal $I := \langle X_{11}X_{22} - X_{21}X_{12} \rangle \subseteq \mathbb{F}_2[X_{11}, X_{21}, X_{12}, X_{22}]$, we saw that $\#\mathcal{V}_{\mathbb{F}_2}(I) = 10$. In this case the restricted footprint bound tells us $\#\mathcal{V}_{\mathbb{F}_2}(I) \leq 12$.

I.14.2 Detection of the f_λ's that are superfluous

In the previous subsection we invented the notion of the restricted footprint to give an upper bound on n. In this section we will see that the concept is relevant for more purposes. Let $R = \mathbb{F}_q[X_1, \ldots, X_m]/I$ be an order domain that can be understood from Pellikaan's factor ring theorem. Let $\{f_\lambda = F_\lambda + I \mid \lambda \in \Lambda\}$ be a corresponding order basis, where $\{F_\lambda \mid \lambda \in \Lambda\}$ is a footprint of I. Denote this footprint by $\Delta(I)$. In the following, we will be concerned with detecting, which f_λ's we need to consider, when we are to construct codes of the types E_λ, C_λ, $\tilde{C}(d)$ and $\tilde{C}_\varphi(d)$ using a surjective morphism φ. Take any $F_\gamma \in \Delta(I) \backslash \Delta_q(I)$. Now there exists a X_i such that F_γ / X_i^{q-1} is a monomial (and thereby contained in $\Delta(I)$). Let γ' be the value such that $F_{\gamma'} = F_\gamma / X_i^{q-1}$. We have

$$\begin{array}{ccc} \rho(f_{\gamma'}) & \prec_\Lambda & \rho(f_\gamma) \\ \mu(f_{\gamma'}) & < & \mu(f_\gamma) \\ \varphi(f_{\gamma'}) & = & \varphi(f_\gamma) \end{array}$$

We conclude the following.

Remark I.14.8
When we are to construct codes of one of the following types E_λ, C_λ, $\tilde{C}(d)$ or $\tilde{C}_\varphi(d)$, then we need only include the f_λ's, where $F_\lambda \in \Delta_q(I)$, in our description. Also the problem of determining the values $d_\varphi(\lambda)$ is considerable simplified, and so is the problem of finding the dimension of the above codes.

We suggest the following definition[2]

Definition I.14.9
Assume that R is an $\mathbb{F}_q$-algebra with an order basis $\{f_\lambda = F_\lambda + I \mid \lambda \in \Lambda\}$, defined from a footprint $\Delta(I) = \{F_\lambda \mid \lambda \in \Lambda\}$. We define

$$d_q(\lambda) := \min\{\mu(f_{\lambda'}) \mid F_{\lambda'} \in \Delta_q(I), \lambda \prec_\Lambda \lambda'\}. \tag{I.14.15}$$

Clearly $d_\varphi(\lambda) \geq d_q(\lambda) \geq d(\lambda)$ (see definition I.11.37)

Example I.14.10
In this example we construct codes from the order domain in example I.7.7 in the case $k = \mathbb{F}_3$. Recall that $R := \mathbb{F}_3[X, Y, Z]/I$ where

$$I := Y^2 - X^2Z + YZ^2 + Z^{35}$$

is shown to be an order domain, by use of Pellikaan's factor ring theorem. The considered weights are $w(X) = (1, 0)$, $w(Y) = (1, 1)$ and $w(Z) = (0, 2)$, and the considered ordering on $\mathbb{N}_0^2$ is $\prec_{lex}$ where $(0, 1) \prec_{lex} (1, 0)$. We get a weight function

$$\rho : R \to \Lambda_{-\infty} := \langle (1, 0), (1, 1), (0, 2) \rangle \cup \{-\infty\}$$

induced by $\rho(x := X + I) = (1, 0)$, $\rho(y := Y + I) = (1, 1)$ and $\rho(z := Z + I) = (0, 2)$. Consider the weighted degree lexicographic ordering $\prec_w$ on $\mathcal{M}(X, Y, Z)$ given by the above weights, by the above specified ordering $\prec_{lex}$ on Λ, and by the lexicographic ordering $\prec'_{lex}$ on $\mathcal{M}(X, Y, Z)$ where $Z \prec'_{lex} X \prec'_{lex} Y$. Denote by $\Delta(I)$ the corresponding footprint. We get an order basis

$$\mathcal{B} := \{F + I \mid F \in \Delta(I)\}.$$

As the involved ordering on Λ is not isomorphic with the ordering on $\mathbb{N}_0$, the indices, we are going to use, are not the natural numbers but the elements of Λ. We know that we need only consider the basis vectors corresponding to the

[2] This definition is a very natural consequence of remark I.14.8. It was suggested in the spring 1999 by Johnny Weile and Søren Raunsbæk Jørgensen (both students at Dept. of Math., Aalb. Uni. at that time) while they were studying a previous version (that included remark I.14.8) of this thesis.

elements of the restricted footprint $\Delta_3(I)$. *These are (the indices increasing with respect to* $\prec_{lex}$*)*

$$\begin{aligned}\{&f_{(0,0)}=1, f_{(0,2)}=z, f_{(0,4)}=z^2, f_{(1,0)}=x, f_{(1,1)}=y,\\ &f_{(1,2)}=xz, f_{(1,3)}=yz, f_{(1,4)}=xz^2, f_{(1,5)}=yz^2, f_{(2,0)}=x^2,\\ &f_{(2,1)}=xy, f_{(2,2)}=x^2z, f_{(2,3)}=xyz, f_{(2,4)}=x^2z^2,\\ &f_{(2,5)}=xyz^2, f_{(3,1)}=x^2y, f_{(3,3)}=x^2yz, f_{(3,5)}=x^2yz^2\}. \quad \text{(I.14.16)}\end{aligned}$$

By inspection we find that $\mathcal{V}_{\mathbb{F}_3}(I)$ *consists of the 12 points*

$$\begin{aligned}\{&(0,0,0),(1,0,0),(2,0,0),(1,0,1),(2,0,1),(0,1,1),\\ &(1,2,1),(2,2,1),(1,0,2),(2,0,2),(1,2,2),(2,2,2)\}.\end{aligned}$$

As morphism we choose the evaluation map defined from these points. So among the 18 elements of (I.14.16), the 6 are superfluous when we are to construct codes. For instance $C_{(1,5)}=C_{(1,4)}$ *as* $ev(f_{(1,5)})=ev(f_{(1,1)})$. *To sort out the remaining 5 superfluous elements, or in other words to detect the 12 indices* (a,b) *such that*

$$C_{(a,b)} \neq C_{(c,d)} \quad \text{for any } (c,d) \prec_{lex} (a,b) \qquad \text{(I.14.17)}$$

we do the following. Consider the 18×12 *matrix*

$$\begin{bmatrix} \boldsymbol{r}_1 \\ \boldsymbol{r}_2 \\ \vdots \\ \boldsymbol{r}_{18} \end{bmatrix} := \begin{bmatrix} ev(f_{(0,0)}) \\ ev(f_{(0,2)}) \\ \vdots \\ ev(f_{(3,5)}) \end{bmatrix}.$$

On this matrix we perform Gaussian elimination in a certain restricted way. The only row operations that we allow, are the ones where a row $\boldsymbol{r}_i$ *is substituted by*

a linear combination $\boldsymbol{r}_i + \sum_{j<i} \alpha_j \boldsymbol{r}_j$. We get

$$\begin{bmatrix} \boldsymbol{r}_1 \\ \boldsymbol{r}_2 \\ \vdots \\ \boldsymbol{r}_{18} \end{bmatrix} = \begin{bmatrix} 1&1&1&1&1&1&1&1&1&1&1&1 \\ 0&0&0&1&1&1&1&1&2&2&2&2 \\ 0&0&0&1&1&1&1&1&1&1&1&1 \\ 0&1&2&1&2&0&1&2&1&2&1&2 \\ 0&0&0&0&0&1&2&2&0&0&2&2 \\ 0&0&0&1&2&0&1&2&2&1&2&1 \\ 0&0&0&0&0&1&2&2&0&0&1&1 \\ 0&0&0&1&2&0&1&2&1&2&1&2 \\ 0&0&0&0&0&1&2&2&0&0&2&2 \\ 0&1&1&1&1&0&1&1&1&1&1&1 \\ 0&0&0&0&0&0&2&1&0&0&2&1 \\ 0&0&0&1&1&0&1&1&2&2&2&2 \\ 0&0&0&0&0&0&2&1&0&0&1&2 \\ 0&0&0&1&1&0&1&1&1&1&1&1 \\ 0&0&0&0&0&0&2&1&0&0&2&1 \\ 0&0&0&0&0&0&2&2&0&0&2&2 \\ 0&0&0&0&0&0&2&2&0&0&1&1 \\ 0&0&0&0&0&0&2&2&0&0&2&2 \end{bmatrix}$$

$$\sim \begin{bmatrix} \underline{1}&1&1&1&1&1&1&1&1&1&1&1 \\ 0&0&0&\underline{1}&1&1&1&1&2&2&2&2 \\ 0&0&0&0&0&0&0&0&\underline{1}&1&1&1 \\ 0&\underline{1}&2&1&2&0&1&2&1&2&1&2 \\ 0&0&0&0&0&\underline{1}&2&2&0&0&2&2 \\ 0&0&0&0&\underline{1}&2&0&1&0&2&0&2 \\ 0&0&0&0&0&0&0&0&0&0&\underline{1}&1 \\ 0&0&0&0&0&0&0&0&0&\underline{1}&0&1 \\ 0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&\underline{2}&0&2&0&0&2&0&2&0&2 \\ 0&0&0&0&0&0&\underline{2}&1&0&0&2&1 \\ 0&0&0&0&0&0&0&\underline{2}&2&2&2&1 \\ 0&0&0&0&0&0&0&0&0&0&0&\underline{1} \\ 0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0 \end{bmatrix}.$$

Now the 12 pivots correspond to the 12 basis vectors (and thereby indices) such

that (I.14.17) is satisfied. That is, the interesting μ-values are the ones in table I.14.1. The parameters related to the $C_{(a,b)}$ codes and the $\tilde{C}_\varphi(d)$ codes are stated in table I.14.2 and table I.14.3.

(a,b)	$(0,0)$	$(0,2)$	$(0,4)$	$(1,0)$	$(1,1)$	$(1,2)$
$\mu(f_{(a,b)})$	1	2	3	2	2	4

(a,b)	$(1,3)$	$(1,4)$	$(2,0)$	$(2,1)$	$(2,2)$	$(2,3)$
$\mu(f_{(a,b)})$	4	6	3	4	7	8

Table I.14.1: The μ values that need to be considered.

(a,b)	(0,0)	(0,2)	(0,4)	(1,0)	(1,1)	(1,2)
$k(a,b)$	11	10	9	8	7	6
$d_\varphi(a,b)$	2	2	2	2	3	3

(a,b)	(1,3)	(1,4)	(2,0)	(2,1)	(2,2)	(2,3)
$k(a,b)$	5	4	3	2	1	0
$d_\varphi(a,b)$	3	3	4	7	8	∞

Table I.14.2: The parameters related to the codes $C_{(a,b)}$ from example I.14.10.

$k(d)$	11	8	6	3	2	1	0
d	2	3	4	6	7	8	∞

Table I.14.3: The parameters related to the codes $\tilde{C}_\varphi(d)$ from example I.14.10.

We note that one can also detect the desired pivots in the following way. First transpose the initial matrix, then perform Gaussian elimination without any restrictions, and finally transpose back again.

In the case $n = \#\Delta_q(I)$ the situation is particular simple. This is illustrated in the following two examples.

Example I.14.11
In this example we will construct codes over $\mathbb{F}_4$ from an order domain of the type described in example I.8.7. Let $p(T) := T^2 + T + 1$ and let α be a root in $p(T)$. We identify the elements of $\mathbb{F}_4$ with the polynomials in $\mathbb{F}_2[T]$ of degree at most one evaluated in α. Starting with the Hermitian polynomial

$H(X_1, X_2) = X_1^3 + X_2^2 + X_2$ over $\mathbb{F}_4$, we get, by following the construction in example I.8.7,

$$\begin{aligned} H_1 &= X^3 + XY^2 + Y^3 + Z^2 + W^2 + Z \\ H_2 &= XY^2 + X^2Y + W^2 + W. \end{aligned}$$

Now with $I := \langle H_1, H_2 \rangle$ we know that $R := \mathbb{F}_4[X, Y, Z, W]/I$ is an order domain with a weight function

$$\rho : R \to \Lambda_{-\infty} := \langle (2,0), (0,2), (3,0), (2,1) \rangle \cup \{-\infty\}$$

induced by $\rho(X + I) = (2, 0)$, $\rho(Y + I) = (0, 2)$, $\rho(Z + I) = (3, 0)$, $\rho(W + I) = (2, 1)$ and by using the standard ordering $\prec_{st}$ on $\mathbb{N}_0^2$.
Let $\prec_w$ be the weighted degree lexicographic ordering on $\mathcal{M}(X, Y, Z, W)$, induced by the weights $w(X) = \rho(X + I)$, $w(Y) = \rho(Y + I)$, $w(Z) = \rho(Z + I)$, $w(W) = \rho(W + I)$, by the ordering $\prec_{st}$ on $\mathbb{N}_0^2$, and by the lexicographic ordering $\prec_{lex}$ on $\mathcal{M}(X, Y, Z, W)$, where $W \prec_{lex} X \prec_{lex} Y \prec_{lex} Z$. We have $\mathrm{lm}(H_1) = Z^2$ and $\mathrm{lm}(H_2) = W^2$. We denote by $\Delta(I)$ the footprint of I with respect to $\prec_w$. The important fact is that

$$\mathcal{B} := \{F + I \mid F \in \Delta(I)\}$$

is an order basis for R. Let $(f_1 = F_1 + I, f_2 = F_2 + I, \ldots)$ be the corresponding well-behaving sequence. Consider the restricted footprint with respect to $\prec_w$, that is consider

$$\begin{aligned} \Delta_4(I) = \{F \text{ a monomial} \mid & \deg_X(F), \deg_Y(F) < 4, \\ & \deg_Z(F), \deg_W(F) < 2\}. \end{aligned}$$

We label $\Delta_4(I)$ by

$$\Delta_4(I) =: \{F_{i_1}, F_{i_2}, \ldots F_{i_{64}}\},$$

where $i_j < i_{j+1}$ for $j = 1, \ldots, 63$. We know that the set

$$\{F_m \mid C_{m-1} \neq C_m\} \tag{I.14.19}$$

is contained in $\Delta_4(I)$. That is we can forget about the F_i outside $\Delta_4(I)$. By inspection we next find, that the number of common roots in $\mathbb{F}_4^4$ of H_1 and H_2 equals $\#\Delta_4(I) = 64$. And we choose as morphism the evaluation map $ev : R \to \mathbb{F}_4^{64}$ that corresponds to these points. So our codes are of length $n = 64$. The very nice consequence of $n = \#\Delta_4(I)$ is that $\{ev(F) \mid F \in \Delta_4(I)\}$ is a

basis for $\mathbb{F}_4^n$. So the codes are particular simple to construct, and we get the following nice expression for the dimension of the code C_{i_l}

$$k_{i_l} = n - l, \tag{I.14.20}$$

and the following nice expression for the dimension of the code $\tilde{C}_\varphi(d)$

$$k(d) = n - \#\{F_j \in \Delta_q(I) \,|\, \mu_j < d\}. \tag{I.14.21}$$

To estimate the minimum distances we need a list of the μ values corresponding to the elements in the restricted footprint. This is contained in figure I.14.2.

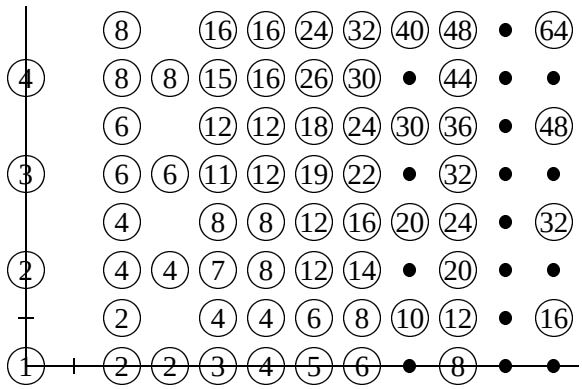

Figure I.14.2: The figure describes the situation in example I.14.11. A number μ with a circle around in the position (s,t), means that there is a monomial F_j in $\Delta_4(I)$ with $\rho(f_j) = (s,t)$ and that $\mu_j = \mu$. A $\bullet$ in position (s,t) denotes that there exists a $F_i \in \Delta(I)\backslash\Delta_4(I)$ with $\rho(f_i) = (s,t)$.

From (I.14.20) and figure I.14.2 (and the knowledge, that $\mathbb{N}_0^2$ is ordered by $\prec_{st}$) we get table I.14.4 of the parameters related to the codes C_l. The value d_{rec} is the best known achieved minimum distance for any linear code over $\mathbb{F}_4$ of length $n = 64$, and dimension k according to Brouwer's table of linear codes at "http://www.win.tue.nl/math/dw/personalpages/aeb/voorlincod.html".
Note that the codes in certain nontrivial cases reach the best known result. From (I.14.21) and figure I.14.2 we get table I.14.5 of the parameters related to the codes $\tilde{C}_\varphi(d)$. Again some of the codes are as good as the best known.

i_l	i_1	i_5	i_8	i_{16}	i_{17}	i_{23}	i_{36}	i_{41}
k_{i_l}	63	59	56	48	47	41	28	23
$d_\varphi(i_l)$	2	3	4	5	6	8	12	16
d_{rec}	2	3	5	8	8	11	18	24

i_l	i_{52}	i_{53}	i_{55}	i_{59}	i_{60}	i_{61}	i_{63}
k_{i_l}	12	11	9	5	4	3	1
$d_\varphi(i_l)$	24	30	32	40	44	48	64
d_{rec}	33	35	38	45	48	48	64

Table I.14.4: Parameters related to the codes C_{i_l} from example I.14.11.

$k(d)$	63	59	57	50	49	44	43	35	34	33	27	26	25
d	2	3	4	5	6	7	8	10	11	12	14	15	16
d_{rec}	2	3	4	7	7	10	10	14	14	15	22	23	23

$k(d)$	20	19	18	16	15	12	11	9	6	5	4	3	1
d	18	19	20	22	24	26	30	32	36	40	44	48	64
d_{rec}	27	27	27	28	30	33	35	38	44	45	48	48	64

Table I.14.5: Parameters related to the codes $\tilde{C}_\varphi(d)$ from example I.14.11.

Example I.14.12
Consider the tensor product of the Hermitian order domain

$$D_H^{(1)} := \mathbb{F}_4[X,Y]/\langle X^3+Y^2+Y\rangle$$

with itself. That is define $I := \langle X^3+Y^2+Y, Z^3+W^2+W\rangle \subseteq \mathbb{F}_4[X,Y,Z,W]$, *and consider the order domain* $D_H^{(2)} := \mathbb{F}_4[X,Y,Z,W]/I$ *with weight function*

$$\rho : D_H^{(2)} \to \Lambda_{-\infty} := \langle (2,0),(3,0),(0,2),(0,3)\rangle \cup \{-\infty\}$$

induced by $\rho(X+I) = (2,0)$, $\rho(Y+I) = (3,0)$, $\rho(Z+I) = (0,2)$, $\rho(W+I) = (0,3)$ *and by using the standard ordering* $\prec_{st}$ *on* Λ. *Consider the weighted degree lexicographic ordering* $\prec_w$ *on* $\mathcal{M}(X,Y,Z,W)$ *given by the weights* $w(X) = \rho(X+I), \ldots, w(W) = \rho(W+I)$, *by the ordering* $\prec_{st}$ *on* Λ *and by the lexicographic ordering* $\prec_{lex}$ *on* $\mathcal{M}(X,Y,Z,W)$ *where* $X \prec_{lex} Y \prec_{lex} Z \prec_{lex} W$. *With respect to this ordering the footprint of* I *is*

$$\Delta(I) = \{M \text{ a monomial} \mid \deg_Y(M), \deg_W(M) < 2\}.$$

And

$$\mathcal{B} := \{M + I \mid M \in \Delta(I)\}$$

is an order basis for $D_H^{(2)}$*. As in the previous example we have*

$$\#\Delta_4(I) = \#\mathcal{V}_{\mathbb{F}_4}(I) = 64 =: n.$$

So if we as morphism choose the evaluation map corresponding to the 64 *points in* $\mathcal{V}_{\mathbb{F}_4}(I)$*, then we are in a situation exactly as simple as the situation in example I.14.11. In particular (I.14.20) and (I.14.21) still holds. To estimate the minimum distances, we need a list of the* μ*-values corresponding to the elements in the restricted footprint. These are stated in figure I.14.3.*

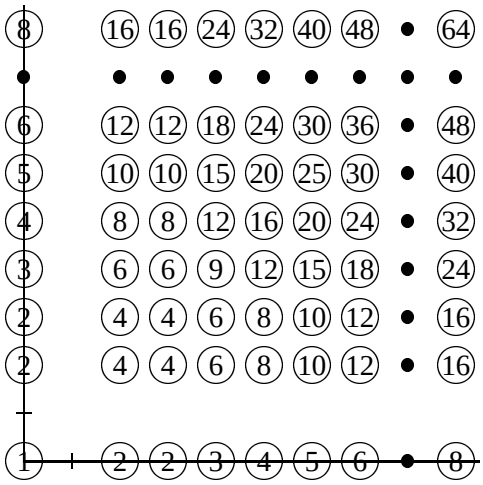

Figure I.14.3: A number μ with a circle around in the position (s,t) means that there is a monomial F_j in the restricted footprint with $\rho(F_j+I) = (s,t)$ and that $\mu f_j = \mu$. A filled circle in position (s,t) denotes that there exists a $F_i \in \Delta(I)\backslash\Delta_q(I)$ with $\rho(F_i + I) = (s,t)$.

From (I.14.20) and figure I.14.3 (and the knowledge, that $\mathbb{N}_0^2$ *is ordered by* $\prec_{st}$*) we get table I.14.6 of the parameters related to the codes* C_l*. And from (I.14.21) and figure I.14.3 we get table I.14.7 of the parameters related to the codes* $\tilde{C}_\varphi(d)$*.*

i_l	i_1	i_5	i_8	i_{15}	i_{17}	i_{23}	i_{36}
k_{i_l}	63	59	56	49	47	41	28
$d_\varphi(i_l)$	2	3	4	5	6	8	12

i_l	i_{41}	i_{52}	i_{56}	i_{59}	i_{61}	i_{63}
k_{i_l}	23	12	8	5	3	1
$d_\varphi(i_l)$	16	24	32	40	48	64

Table I.14.6: Parameters related to the codes C_{i_l} from example I.14.12.

$k(d)$	63	59	57	51	49	43	37	36	32	26	24
d	2	3	4	5	6	8	9	10	12	15	16

$k(d)$	19	17	15	11	10	8	6	5	3	1
d	18	20	24	25	30	32	36	40	48	64

Table I.14.7: Parameters related to the codes $\tilde{C}_\varphi(d)$ from example I.14.12.

Example I.14.13
In example I.14.11 and I.14.12 we considered codes over $\mathbb{F}_4$ of length $n = 64$. It is natural to compare the C_l codes from these examples with the Reed-Muller codes over $\mathbb{F}_4$ of length $n = 64$. Using the results from section I.12.1 one gets the results described in table I.14.8. For five dimensions the Reed-Muller

i	0	1	2	3	4	5	6	7	8
k	63	60	54	44	32	20	10	4	1
d	2	3	4	8	12	16	32	48	64

Table I.14.8: The parameters of the $RM_4^\perp(i, 3)$ codes, $i = 0, \ldots, 8$.

codes are the best, for two dimensions they are equally good as the codes from example I.14.11 and I.14.12, and finally for two dimensions they are worse.

The technique described in this section holds in an apparently more general setting. Let R be an order domain with an order basis $\mathcal{B} = \{f_\lambda \mid \lambda \in \Lambda\}$ that is multiplicatively finitely generated and closed in the following sense. There exists a set $\{f_{\lambda_1}, \ldots, f_{\lambda_s}\}$ such that whenever f_λ is an element in $\mathcal{B}$ then one

can find $\alpha_1^{(\lambda)}, \ldots, \alpha_s^{(\lambda)} \in \mathbb{N}_0$ such that

$$f_\lambda = \prod_{i=1}^{s} f_{\lambda_i}^{\alpha_i^{(\lambda)}}$$

and contrary every

$$\prod_{i=1}^{s} f_{\lambda_i}^{\alpha_i^{(\lambda)}}, \quad \alpha_1^{(\lambda)}, \ldots, \alpha_s^{(\lambda)} \in \mathbb{N}_0$$

is an element in $\mathcal{B}$. When constructing codes over $\mathbb{F}_q$ one need only consider the elements in

$$\{f_\lambda = \prod_{i=1}^{s} f_{\lambda_i}^{\alpha_i^{(\lambda)}} \in \mathcal{B} \mid \alpha_i^{(\lambda)} < q,\ i = 1, \ldots, s\}.$$

We leave it as an open problem to decide if this setting is actually more general than the ones considered above.

I.14.3 Bounds on $\mu(f_\lambda)$

Assume that we are given an order domain $R = k[X_1, \ldots, X_m]/I$ that possesses an order basis $\{f_\lambda = F_\lambda + I \mid \lambda \in \Lambda\}$ such that $\{F_\lambda \mid \lambda \in \Lambda\}$ is a footprint. Consider an arbitrary $F_\lambda = X_1^{\alpha_1} X_2^{\alpha_2} \cdots X_m^{\alpha_m}$. Any factor of F_λ will be a new element in $\Delta(I)$, and by assumption no two different factors M_1 and M_2 satisfy $\rho(M_1 + I) = \rho(M_2 + I)$. We conclude that

$$\mu(f_\lambda) \geq \#\{M \text{ divides } F_\lambda\} = \prod_{j=1}^{m} (\alpha_j + 1). \tag{I.14.22}$$

We next give an example where the bound (I.14.22) is attained for all the elements f_i that are of interest when constructing codes.

Example I.14.14
Consider a type-I curve $X^a + uY^b + G(X, Y) \in \mathbb{F}_q[X, Y]$, where $a > b$ and $a \geq q$. Denote $I := \langle X^a + uY^b + G(X, Y) \rangle$, and let

$$\rho : \mathbb{F}_q[X, Y]/I \to \Lambda_{-\infty} := \langle a, b \rangle \cup \{-\infty\}$$

be the weight function induced by $\rho(X + I) = b$, $\rho(Y + I) = a$. Assume

$$\rho(X^\alpha Y^\beta + I) = \rho(X^{\alpha'} Y^{\beta'} + I). \tag{I.14.23}$$

Then $\alpha \equiv \alpha' \mod a$ and $\beta \equiv \beta' \mod b$. Further if $\alpha > \alpha'$ then $\beta < \beta'$ and vice versa. We conclude that if $(\alpha, \beta) \neq (\alpha', \beta')$ satisfy (I.14.23) then

$$\alpha \geq a \quad \text{or} \quad \beta \geq b. \tag{I.14.24}$$

Consider the weighted degree lexicographic ordering on $\mathcal{M}(X, Y)$ given by $w(X) = b$, $w(Y) = a$ and $X \prec_{lex} Y$. The corresponding footprint is

$$\Delta(I) = \{X^\alpha Y^\beta \mid \beta < b\}$$

and

$$\mathcal{B} := \{M + I \mid M \in \Delta(I)\}$$

is an order basis. Let $(f_1 = F_1 + I, f_2 = F_2 + I, \ldots)$ be the corresponding well-behaving sequence. As noted in section I.14.2, the only $\mu(f_i)$-values that we are interested in knowing, are the ones corresponding to the F_i's in the restricted footprint

$$\Delta_q(I) = \{X^\alpha Y^\beta \mid \alpha < q, \beta < b\}. \tag{I.14.25}$$

Take an arbitrary element $X^\alpha Y^\beta \in \Delta_q(I)$. By comparing (I.14.24) with (I.14.25), and by using the assumption $a \geq q$, we get that an identity $\rho(X^\alpha Y^\beta + I) = \rho(X^{\alpha'} Y^{\beta'} + I)$ will imply $(\alpha, \beta) = (\alpha', \beta')$. We have shown that

$$\mu(X^\alpha Y^\beta + I) = \#\{M \mid M \text{ a factor of } X^\alpha Y^\beta\} = (\alpha + 1)(\beta + 1) \tag{I.14.26}$$

for $X^\alpha Y^\beta \in \Delta_q(I)$.

For later use let us pursue the investigations a little further. Consider $B \subseteq \Delta_q(I)$, where either B equals $\Delta_q(I)$, or is a footprint that is strictly contained in $\Delta_q(I)$. For instance B can be the set $\Delta(I'')$ where $I'' := \mathcal{I}(\mathcal{V}_{\mathbb{F}_q}(I))$. Denote $n_B := \#B$ and consider the μ-values corresponding to elements in B. Assume these are denoted

$$\{\mu_1, \ldots, \mu_{n_B}\} \tag{I.14.27}$$

such that $\mu_i \leq \mu_{i+1}$ for $i = 1, \ldots, n_B - 1$. We claim that (I.14.27) is dominated by $\{1, 2, \ldots, n_B\}$ in the sense that

$$\mu_i \leq i, \ i = 1, \ldots, n_B. \tag{I.14.28}$$

Assume for a moment that this was not the case. That is assume there exists an $i \in \{1, \ldots, n_B\}$ such that $\mu_i > i$. But then according to the structure of B and to the first equality in (I.14.26), there will exist $\mu_i - 1 \geq i$, μ-values in (I.14.27) that are strictly smaller than μ_i, a contradiction. The inequalities (I.14.28) will be important when we investigate the asymptotic behaviour of the codes corresponding to the repeated tensor products of type-I curves of the above type.

Example I.14.15
Assume that we are given an order domain $R = k[X_1, \ldots, X_m]/I$ *that possesses an order basis* $\{f_\lambda = F_\lambda + I \mid \lambda \in \Lambda\}$ *such that* $\{F_\lambda \mid \lambda \in \Lambda\}$ *is a footprint. Assume further that the restricted footprint* $\Delta_q(I)$ *contains precisely* $n = \#\mathcal{V}_{\mathbb{F}_q}(I)$ *elements. We have seen that the assumptions for instance are satisfied for the ideals* $\langle 0\rangle \subseteq \mathbb{F}_q[X_1, \ldots, X_m]$, $\langle X^{q+1} - Y^q - Y\rangle \subseteq \mathbb{F}_q[X, Y]$, *and* $\langle X^3 + XY^2 + Y^3 + Z^2 + W^2 + Z, XY^2 + X^2Y + W^2 + W\rangle \subseteq \mathbb{F}_4[X, Y, Z, W]$. *We claim that*

$$\{\mu(f_\lambda = F_\lambda + I) \,|\, F_\lambda \in \Delta_q(I)\} \tag{I.14.29}$$

is dominated by $\{1, 2, \ldots, n\}$ *in the sense that if (I.14.29) is written* $\{\mu_1, \ldots, \mu_n\}$ *where* $\mu_i \leq \mu_{i+1}$ *for* $i = 1, \ldots, n-1$, *then* $\mu_i \leq i$. *To see this, we consider the codes* $\tilde{C}_\varphi(d) = \tilde{C}(d)$ *defined from* $\mathbb{F}_q[X_1, \ldots, X_m]/I$. *Now on the one hand* $\tilde{C}(\mu_i)$, $i \geq 2$ *has of course minimum distance* $d \geq \mu_i$. *On the other hand the dimension is bounded by* $k \geq n - (i-1)$ *(equality holds if* $\mu_{i-1} \neq \mu_i$*), and the Singleton bound states that* $n - k \geq d - 1$. *So* $d \leq i$. *All together* $\mu_i \leq i$. *We have proved our claim.*

I.15
The asymptotic behaviour of some classes of codes

In this chapter we will be concerned with the asymptotic behaviour of the codes coming from certain classes of order domains. In the first part we investigate sequences of codes coming from repeated tensor products of certain order domains. In the last part we will discuss the tower of Garcia and Stichtenoth from an order domain point of view.

I.15.1 Codes coming from the tensor products of order domains

In section I.8.2 we introduced the tensor products of order domains, and in example I.14.12 we investigated the codes related to the product of two Hermitian order domains. In the following the notation from section I.8.2 will be used heavily. The reader might want to consult this section before proceeding.

Now let a sequence of order domains be given

$$(R_1 = \mathbb{F}_q[\boldsymbol{X}_1]/I_1,\ R_2 = \mathbb{F}_q[\boldsymbol{X}_2]/I_2,\ R_3 = \mathbb{F}_q[\boldsymbol{X}_3]/I_3, \ldots) \qquad \text{(I.15.1)}$$

where each R_i can be understood from Pellikaan's factor ring theorem, by studying the footprints $\Delta(I_i)$, $i = 1, \ldots$. Eventually $R_i = R_1$ for $i = 1, 2, \ldots$. Now from the sequence (I.15.1) we construct a new sequence of order domains namely

$$\begin{aligned}(D^{(1)} := R_1 =: \mathbb{F}_q[\boldsymbol{X}_1]/I^{(1)},\ D^{(2)} := R_1 \otimes R_2 =: \mathbb{F}_q[\boldsymbol{X}_1, \boldsymbol{X}_2]/I^{(2)},\\ D^{(3)} := R_1 \otimes R_2 \otimes R_3 =: \mathbb{F}_q[\boldsymbol{X}_1, \boldsymbol{X}_2, \boldsymbol{X}_3]/I^{(3)}, \ldots).\end{aligned} \qquad \text{(I.15.2)}$$

If we denote $n_j := \#\mathcal{V}_{\mathbb{F}_q}(I_j)$ then the number of zeros of $I^{(i)}$ is given by $n^{(i)} = \prod_{j=1}^{i} n_j$. We may assume $n_j \geq 2$. So $n^{(i)}$ tends to infinity as i tends to infinity. A natural question now is if there exists a sequence of type (I.15.2) from which we can construct a good sequence of codes. That is a sequence

$$(C^{(1)}, C^{(2)}, \ldots)$$

with corresponding parameters

$$\left((n^{(1)}, k^{(1)}, d^{(1)}), (n^{(2)}, k^{(2)}, d^{(2)}), \ldots\right)$$

such that both

$$R := \liminf_{i\to\infty} \frac{k^{(i)}}{n^{(i)}} > 0 \tag{I.15.5}$$

and

$$\delta := \liminf_{i\to\infty} \frac{d^{(i)}}{n^{(i)}} > 0. \tag{I.15.6}$$

We will not answer this question completely, but describe some important cases where the sequences of codes are bad, at least with respect to the order bound.

Consider $D^{(i)}$ from the sequence (I.15.2). A footprint for $I^{(i)}$ satisfying the conditions in Pellikaan's factor ring theorem is given by

$$\Delta(I^{(i)}) = \{M_1 M_2 \cdots M_i \mid M_j \in \Delta(I_j),\ j = 1, \ldots, i\} \tag{I.15.7}$$

and the corresponding restricted footprint is given by

$$\Delta_q(I^{(i)}) = \{M_1 M_2 \cdots M_i \mid M_j \in \Delta_q(I_j),\ j = 1, \ldots, i\}. \tag{I.15.8}$$

Next we consider the μ-values. We note that

$$\mu(M_j + I_j) = \mu(M_j + I^{(i)}),\ i \geq j$$

(here the first μ-value is with respect to the order domain R_j, and the second μ-value is with respect to the order domain $D^{(i)}$). Further for $M_j \in I_j$, $j = 1, \ldots, i$, we have

$$\begin{aligned} \mu(M_1 M_2 \cdots M_i + I^{(i)}) &= \prod_{j=1}^{i} \mu(M_j + I^{(i)}) \\ &= \prod_{j=1}^{i} \mu(M_j + I_j). \end{aligned}$$

We are now ready to give some conclusions on the asymptotic behaviour of codes corresponding to certain classes of sequences (I.15.2). We will study three cases.

Case I

The assumptions are as follows. Assume $n_j = \#\Delta_q(I_j)$ for any R_j in the sequence (I.15.1), and assume that there exists a value n_{max} such that

$$n_j \leq n_{max} \text{ for } j = 1, \ldots . \tag{I.15.10}$$

According to (I.15.8) we have $n^{(i)} = \#\Delta_q(I^{(i)})$, $i = 1, \ldots$. Referring to section I.14.2 we will need precisely the elements of $\Delta_q(I^{(i)})$, when we construct the parity check matrices of the codes of types C_l, $\tilde{C}(d)$ and $\tilde{C}_\varphi(d)$. In this special case of course $\tilde{C}(d) = \tilde{C}_\varphi(d)$ for any d. We now show that every sequence of $\tilde{C}(d)$-codes/$\tilde{C}_\varphi(d)$-codes is bad (at least with respect to the order bound). Of course then also every sequence of C_l-codes is bad (at least with respect to the order bound).

First consider any R_j in (I.15.1). Write the set of μ-values corresponding to elements in $\Delta_q(I_j)$ as

$$U_j = \{\mu_1(j), \ldots, \mu_{n_j}(j)\} \tag{I.15.11}$$

where $\mu_s(j) \leq \mu_{s+1}(j)$, $s = 1, \ldots, n_j - 1$. From example I.14.15 we know that the sequence (I.15.11) is dominated by $\{1, 2, \ldots, n_j\}$ in the sense that $\mu_s(j) \leq s$, $s = 1, \ldots, n_j$. Turning our attention to $R^{(i)}$ the set of μ-values corresponding to elements in $\Delta_q(I^{(i)})$ is

$$U^{(i)} = \{\prod_{j=1}^{i} \mu(j) \,|\, \mu(j) \in U(j),\ j = 1, \ldots, i\}.$$

Therefore the set of μ-values corresponding to elements in $\Delta_q(I^{(i)})$ is dominated by

$$\{\prod_{j=1}^{i} \mu(j) \,|\, \mu(j) \in \{1, 2, \ldots, n_j\}\}. \tag{I.15.13}$$

Assume now that a good sequence

$$\left(\tilde{C}(d^{(1)}), \tilde{C}(d^{(2)}), \ldots\right)$$

exists (good wrt. the order bound). Then there exist $R' > 0$, $\delta' > 0$ and an N such that

$$\frac{d^{(i)}}{n^{(i)}} > \delta', \quad \frac{k^{(i)}}{n^{(i)}} > R' \quad \text{for } i > N. \tag{I.15.14}$$

Consider a fixed $i > N$. We will calculate a lower bound on the mean value of the μ-values corresponding to elements in $\Delta_q(I^{(i)})$. From (I.15.14) we have $d^{(i)} > \delta' n^{(i)}$ and $k^{(i)} > R' n^{(i)}$. That is there are at least $k^{(i)}$ μ-values in $U^{(i)}$ greater than $\delta' n^{(i)}$. So the mean value of the elements in $U^{(i)}$ is bounded by

$$\begin{aligned} \text{mean value} &> \frac{k^{(i)}\delta' n^{(i)}}{n^{(i)}} \\ &> R'\delta' n^{(i)} \\ &= R'\delta' \prod_{j=1}^{i} n_j. \end{aligned} \tag{I.15.15}$$

On the other hand we can conclude from (I.15.13) that the mean value is upper bounded by

$$\text{mean value } \leq \prod_{j=1}^{i} \frac{n_j + 1}{2} \leq \prod_{j=1}^{i} (n_j - \frac{1}{2}) \tag{I.15.16}$$

(here we used $n_j \geq 2$). Using the assumption (I.15.10) we see that the upper bound on the mean value is smaller than the lower bound, for i sufficiently large. We have reached a contradiction.

Note that the set of codes that we have investigated above contains the Reed-Muller codes (the case $I^{(i)} = \langle 0 \rangle$, $i = 1, \ldots$). These codes are known to have minimum distance equal to the Feng-Rao bound, giving us the well-known fact, that Reed-Muller codes are asymptotic bad.

Some general results

Before proceeding to case II and case III, we discuss some general results. As in previous sections we will use the notation $I'' := \mathcal{I}(\mathcal{V}_{\mathbb{F}_q}(I))$. In particular $(I^{(i)})'' := \mathcal{I}(\mathcal{V}_{\mathbb{F}_q}(I^{(i)}))$. We have $\Delta((I^{(i)})'') \subseteq \Delta_q(I^{(i)})$, $\#\Delta((I^{(i)})'') = \#\mathcal{V}_{\mathbb{F}_q}(I^{(i)})$ and that $\{ev(M) \mid M \in \Delta((I^{(i)})'')\}$ is a basis for $\mathbb{F}_q^{n^{(i)}}$. Let the μ-values corresponding to the elements in $\Delta((I^{(i)})'')$ be enumerated $\{\mu_1^{(i)}, \ldots, \mu_{n^{(i)}}^{(i)}\}$ such that $\mu_j^{(i)} \leq \mu_{j+1}^{(i)}$, $j = 1, \ldots, n^{(i)} - 1$. The first important observation is that the dimension of $\tilde{C}(\mu_s^{(i)} + 1)$ is bounded by

$$k \leq n^{(i)} - s \tag{I.15.17}$$

(note that this observation need not hold for $\tilde{C}_\varphi(d)$-codes). The other important observation is, that we can easily find $\Delta((I^{(i)})'')$ ones we know the $\Delta(I_j'')$,

$j = 1, \ldots i$. Just note that

$$\{M_1 M_2 \cdots M_i \mid M_j \in \Delta(I_j''),\ j = 1, \ldots, i\} \subseteq \Delta((I^{(i)})'') \tag{I.15.18}$$

and that the cardinality of both sides equals $\prod_{j=1}^{i} n_j$. That is we have equality in (I.15.18).

Case II

The assumptions are as follows. Assume the maximal μ-value corresponding to an element in $\Delta(I_j'')$ is bounded by $\mu_{n_j}(j) < n_j$ for $j = 1, \ldots$. Assume further that a value n_{max} exists, such that $n_j \leq n_{max}$ for $j = 1, \ldots$.
Now the maximal μ-value corresponding to $\Delta((I^{(i)})'')$ is bounded by

$$\mu_{n^{(i)}}^{(i)} = \prod_{j=1}^{i} \mu_{n_j}(j) \leq \prod_{j=1}^{i} (n_j - 1),$$

giving us the bound

$$\frac{\mu_{n^{(i)}}^{(i)}}{n^{(i)}} \leq \prod_{j=1}^{i} \frac{n_j - 1}{n_j}. \tag{I.15.20}$$

But the rhs. of (I.15.20) tends to zero as i tends to infinity (here we used the fact that n_j is bounded). So even a sequence of $\tilde{C}(d)$ codes all of dimension at most one, will satisfy

$$\liminf_{i \to \infty} \frac{d^{(i)}}{n^{(i)}} = 0.$$

It follows that the codes $\tilde{C}(d)$ are (with respect to the order bound) asymptotic bad. But then are so the codes C_l.

That the assumptions corresponding to case II can actually take place is seen by the following example.

Example I.15.1
Consider the order domain

$$R := \mathbb{F}_4[X, Y]/\langle X_1^3 + Y^2 \rangle.$$

There are two choices of weighted degree lexicographic ordering on $\mathcal{M}(X, Y)$ that satisfies the conditions in Pellikaan's factor ring theorem. In both cases $w(X) = 2$ and $w(Y) = 3$. For the one choice $X \prec_{lex} Y$ and for the other $Y \prec_{lex} X$. Now $X^3 - Y^2$ has the roots $(0, 0), (1, 1), (\alpha, 1), (\alpha^2, 1)$ where $\alpha^2 +$

$\alpha+1=0$. *Calculating a Gröbner basis for* $I' := \langle X^3-Y^2, X^4-X, Y^4-Y\rangle$ *we get for both orderings the footprint* $\Delta(I') = \{1, X, X^2, Y\}$. *The corresponding* μ*-values are* $\{1,2,3,2\}$. *By inspection the code*

$$C_3 = \{\boldsymbol{c} \in \mathbb{F}_4^4 \mid \boldsymbol{c}\cdot ev(1) = \boldsymbol{c}\cdot ev(X) = \boldsymbol{c}\cdot ev(Y) = 0\}$$

actually has minimum distance equal to 3.

Case III

The assumptions are as follows. Assume that

$$R_j = \mathbb{F}_q[X_1^{(j)}, X_2^{(j)}]/\langle (X_1^{(j)})^{a_j} + u_j (X_2^{(j)})^{b_j} + G_j(X_1^{(j)}, X_2^{(j)})\rangle,$$

$j = 1, \ldots$ is a type-I curve with $a_j \geq q$, $j = 1, \ldots$ (see example I.10.15 for a definition of a type-I curve).
Recall that in example I.14.22 we showed that for such curves the set of μ-values corresponding to elements in $\Delta(I_j'')$ is dominated by $\{1, \ldots, n_j\}$. Recall also that

$$\Delta((I^{(i)})'') = \{M_1 M_2 \cdots M_i \mid M_j \in \Delta(I_j''),\ j = 1, \ldots, i\}.$$

Assume that a good sequence of codes of type $\tilde{C}(d)$ exists. As a best case we may assume equality holds in (I.15.17). But now we can make similar calculations as in case I, which we remember lead to a contradiction. So (with respect to the order bound) no good sequence of $\tilde{C}(d)$-codes exists, and then does neither any good sequence of C_l-codes exist.

I.15.2 The tower of Garcia and Stichtenoth

In [10] Garcia and Stichtenoth gave a description of a tower

$$\mathcal{F}_1 \subseteq \mathcal{F}_2 \subseteq \mathcal{F}_3 \subseteq \cdots$$

of algebraic function fields over $\mathbb{F}_{q^2}$ (for any prime power q) of one variable, that has some very nice properties. Their tower is defined recursively by

$$\begin{aligned} \mathcal{F}_1 &:= \mathbb{F}_{q^2}(x_1) \\ \mathcal{F}_{i+1} &:= \mathcal{F}_i(z_{i+1}) \end{aligned}$$

where z_{i+1} satisfies the equation

$$z_{i+1}^q + z_{i+1} = x_i^{q+1}$$

and where x_i for $i > 1$ is given by

$$x_i := \frac{z_i}{x_{i-1}} \in \mathcal{F}_i.$$

Denote by N_i the number of rational places in $\boldsymbol{P}_{\mathcal{F}_i}$, and by g_i the genus of $\mathcal{F}_i$, The nice properties of the tower are

- $N_i \to \infty$ for $i \to \infty$
- $\liminf_{i\to\infty} \frac{N_i}{g_i} = q - 1.$

The second property is rather impressing as the Drinfeld-Vlăduţ bound states that $q - 1$ is the highest possible attainable value (see [38, Ch. V]).

Using theorem I.12.6 one can conclude, that there to the tower corresponds good sequences of geometric Goppa codes. One way of constructing a good sequence of codes

$$(C_{\mathcal{L}}(D_1, G_1), C_{\mathcal{L}}(D_2, G_2), \ldots)$$

(where $C_{\mathcal{L}}(D_i, G_i)$ is a geometric Goppa code constructed from the function field $\mathcal{F}_i$) is by for each $\mathcal{F}_i$ to choose one rational place P_i. Then define D_i to be the sum of the remaining rational places and G_i to be $G_i := m_i P_i$, where m_i is a natural number satisfying a certain criterion. Choosing the m_i's in the right way, one gets sequences of codes that attains the so-called Tsfasman-Vlăduţ-Zink bound. A rather impressing result as there for $q^2 \geq 49$ is a region where the Tsfasman-Vlăduţ-Zink bound is better than the important Gilbert-Varshamov bound.

Although this very nice tower is given, it is certainly not clear how one should construct the corresponding good sequences of codes in practice. Many researchers have tried (and still try) to find bases for the $\mathcal{L}$-spaces involved in the construction. However the problem is not at all solved yet. There are algorithms for finding the bases for these $\mathcal{L}$-spaces (see [14] and [24]) but they are of rather high complexity. Also in [44] Voß and Høholdt succeed in giving general descriptions of bases for many choices of $\mathcal{L}$-spaces for the first three function fields in the tower.

As shown already in [10] the unique pole P_1^∞ of x_1 in $\mathcal{F}_1$ is totally ramified in the extension $\mathcal{F}_i/\mathcal{F}_1$, $i \geq 1$. Denote by P_i^∞ the unique place in $\boldsymbol{P}_{\mathcal{F}_i}$ that lies over P_1^∞, and note that P_i^∞ is rational. Now an obvious choice of a sequence of $\mathcal{L}$-spaces corresponding to a good sequence of codes is the following

$$(\mathcal{L}(m_1 P_1^\infty), \mathcal{L}(m_2 P_2^\infty), \mathcal{L}(m_3 P_3^\infty), \ldots)$$

where m_i, $i \geq 1$, is to be chosen properly s.t. the codes attains the Tsfasman-Vlăduţ-Zink bound. In [35] Pellikaan, Stichtenoth and Torres takes the first step to determine a basis for the vector space $\mathcal{L}(m_i P_i^{\infty})$, $i \geq 1$, as they determine the Weierstrass semigroup Λ_i for P_i^{∞}. According to [35] the Weierstrass semigroup Λ_i can be found by the following recursive formula

$$c_m = \begin{cases} q^m - q^{m/2} & \text{if} \quad m \equiv 0 \mod 2 \\ q^m - q^{(m+1)/2} & \text{if} \quad m \equiv 1 \mod 2 \end{cases}$$

$$\Lambda_1 = \mathbb{N}_0$$

$$\Lambda_i = q\Lambda_{i-1} \cup \{a \in \mathbb{N}_0 \mid a \geq c_i\} \quad \text{for } i > 1. \tag{I.15.25}$$

As already noted in section I.10.2, for any algebraic function field over k, and for any rational place P in $\boldsymbol{P}_{\mathcal{F}}$, there exists an index m and an ideal $I \subseteq k[X_1, \ldots, X_m]$ such that

$$\mathcal{F} \simeq \mathrm{Quot}(k[X_1, \ldots, X_m]/I) \tag{I.15.26}$$

and such that the place in $\mathrm{Quot}(k[X_1, \ldots, X_m]/I)$ isomorphic with P is the only place at infinity. If a description similar to the rhs. of (I.15.26) could be found for each $\mathcal{F}_i$, then we would more or less have solved our problem with finding bases for certain $\mathcal{L}$-spaces. This suggests the following strategy for finding a sequence of well-described order domains to which there corresponds good sequences of codes attaining the Tsfasman-Vlăduţ-Zink bound. For $i = 1, \ldots$ do the following.

Step 1 Extract the generators for the Weierstrass semigroup Λ_i.
Consider them as weights. Construct the toric ideal say
$I_{toric}^{(i)} = \langle G_1^{(i)}, \ldots, G_{s_i}^{(i)} \rangle \subseteq \mathbb{F}_{q^2}[X_1, \ldots, X_{m_i}]$
corresponding to these weights.

Step 2 Add terms to the defining polynomials $G_1^{(i)}, \ldots, G_{s_i}^{(i)}$ to get
$\tilde{G}_1^{(i)}, \ldots, \tilde{G}_{s_i}^{(i)}$ that satisfies that $\#\mathcal{V}_{\mathbb{F}_{q^2}}(\langle \tilde{G}_1^{(i)}, \ldots, \tilde{G}_{s_i}^{(i)} \rangle)$
is near the value $N_i - 1$.

Implementing the algorithm from theorem I.6.2 in a computer program (MapleV), the author calculated a reduced Gröbner basis $\mathcal{B}_i$ for $I_{toric}^{(i)}$, $i = 1, \ldots, 5$, in the case of $\mathbb{F}_{q^2} = \mathbb{F}_4$. The following high values explain why the results are not listed. We have $\#\mathcal{B}_1 = 0$, $\#\mathcal{B}_2 = 1$, $\#\mathcal{B}_3 = 11$, $\#\mathcal{B}_4 = 57$, and $\#\mathcal{B}_5 = 238$.

The high value of $\#\mathcal{B}_5$ suggests that it might not be an easy task to describe $I^{(i)}_{toric}$ in general. We propose the following research problem. Find a nice description of the sequence

$$\left(I^{(1)}_{toric}, I^{(2)}_{toric}, \ldots\right)$$

of toric ideals related to the semigroups in (I.15.25).

Appendix I.A

Gröbner basis theory

This appendix contains a survey of the Gröbner basis theory that is needed in the present thesis. All the results listed below can be found in [4]. See also [19].

I.A.1 Gröbner bases

The definition of a Gröbner basis for an ideal $I \subseteq k[X_1, \ldots, X_m]$ with respect to a given monomial ordering $\prec$ on $\mathcal{M}_m$, uses the well-known concept of the leading monomial of a polynomial.

Definition I.A.1
Let $I \subseteq k[X_1, \ldots, X_m]$ be an ideal and $\prec$ a monomial ordering on $\mathcal{M}_m$. Consider a nonzero polynomial $P(\boldsymbol{X}) = \sum_{i=1}^{n} c_i \boldsymbol{X}^{\boldsymbol{\alpha}_i}$ where $c_i \neq 0$ for $i = 1, \ldots, n$, and $\boldsymbol{\alpha}_i \neq \boldsymbol{\alpha}_j$ for $i \neq j$, $1 \leq i, j \leq n$. The unique monomial $\boldsymbol{X}^{\boldsymbol{\alpha}_k}$ such that $\boldsymbol{X}^{\boldsymbol{\alpha}_k} \succ \boldsymbol{X}^{\boldsymbol{\alpha}_i}$ for all $1 \leq i \leq n$, $i \neq k$ is called the leading monomial of $P(\boldsymbol{X})$ and is denoted $\mathrm{lm}(P)$. The term $c_k \boldsymbol{X}^{\boldsymbol{\alpha}_k}$ is called the leading term of $P(\boldsymbol{X})$ and is denoted $\mathrm{lt}(P)$.

Definition I.A.2
Let $I \subseteq k[X_1, \ldots, X_m]$ be a nonzero ideal and $\prec$ a monomial ordering on $\mathcal{M}_m$. A finite subset $\mathcal{G} = \{G_1, \ldots, G_s\} \subseteq I$, $G_i \neq 0$ for $i = 1, \ldots, s$ is said to be a Gröbner basis for I wrt. $\prec$, if there for any $P(\boldsymbol{X}) \in I$ exists an index $t \in \{1, \ldots, s\}$ s.t. $\mathrm{lm}(G_t) | \mathrm{lm}(P)$.

Theorem I.A.3
Let $\prec$ be any monomial ordering on $\mathcal{M}_m$. Every nonzero ideal $I \subseteq k[X_1, \ldots, X_m]$ possesses a Gröbner basis wrt. $\prec$.

The following theorem justifies the name "Gröbner basis".

Theorem I.A.4
If $\mathcal{G} = \{G_1, \ldots, G_s\}$ is a Gröbner basis for I wrt. $\prec$, then $\mathcal{G}$ is a basis (that is a generating set) for I.

It may very well happen that a given Gröbner basis contains more polynomials than necessary. Assume G_i, G_j are two elements in a given Gröbner basis $\mathcal{G}$ for I wrt. $\prec$. From the very definition of a Gröbner basis, we see, that if $\mathrm{lm}(G_i) \mid \mathrm{lm}(G_j)$, then also $\mathcal{G}\backslash\{G_j\}$ is a Gröbner basis for I wrt. $\prec$. The process of removing superfluous elements from the Gröbner basis is called reduction.

Definition I.A.5
Let $\mathcal{G} = \{G_1, \ldots, G_s\}$ be a Gröbner basis wrt. $\prec$. We will say that $\mathcal{G}$ is a minimal Gröbner basis wrt. $\prec$ if the following two conditions are satisfied.

$$
\begin{aligned}
&(1) \quad \mathrm{lt}(G_i) = \mathrm{lm}(G_i),\ i = 1, \ldots, s \\
&(2) \quad \textit{there does not exist indices} \\
&\qquad i, j \in \{1, \ldots, s\}, i \neq j \\
&\qquad \textit{s.t.}\ \mathrm{lm}(G_i) | \mathrm{lm}(G_j).
\end{aligned}
$$

Another interesting type of a Gröbner basis is the following one.

Definition I.A.6
Let $I \subseteq k[X_1, \ldots, X_m]$ be a nonzero ideal. Assume that $\mathcal{G} = \{G_1, \ldots, G_s\}$ is a Gröbner basis for I wrt. any possible monomial ordering $\prec$ on $\mathcal{M}_m$. Then $\mathcal{G}$ is said to be a universal Gröbner basis.

We have the following surprisingly result.

Proposition I.A.7
Any nonzero ideal $I \subseteq k[X_1, \ldots, X_m]$ possesses a universal Gröbner basis.

I.A.2 The division algorithm

In the following we describe the so-called division algorithm that gives a particular informative result when a Gröbner basis is used. Consider a polynomial $P(\boldsymbol{X}) = \sum_{i=1}^{n} c_i \boldsymbol{X}^{\boldsymbol{\alpha}_i} \in k[X_1, \ldots, X_m]$, where $c_i \neq 0$ for $i = 1, \ldots, n$. And consider a set of nonzero polynomials $\{G_1(\boldsymbol{X}), \ldots, G_s(\boldsymbol{X})\} \subseteq k[X_1, \ldots, X_m]$. Assume that there exist indices $u^{(1)} \in \{1, \ldots, n\}$ and $v^{(1)} \in \{1, \ldots, s\}$ s.t. $\mathrm{lm}(G_{v^{(1)}}) | \boldsymbol{X}^{\boldsymbol{\alpha}_{u^{(1)}}}$. Consider the polynomial

$$
P_1(\boldsymbol{X}) := P(\boldsymbol{X}) - \frac{c_{u^{(1)}} \boldsymbol{X}^{\boldsymbol{\alpha}_{u^{(1)}}}}{\mathrm{lt}(G_{v^{(1)}}(\boldsymbol{X}))} G_{v^{(1)}}(\boldsymbol{X}).
$$

We will say that P is reduced modulo $G_{v^{(1)}}$ to P_1. Note that $\mathrm{lm}(P_1) \preceq \mathrm{lm}(P)$. Continuing the process P_1 possible may be reduced modulo say $G_{v^{(2)}}$ to P_2.

And P_2 possible may be reduced to P_3 and so forth. Until finally a P_δ is attained that can not be reduced modulo any of the polynomials $G_1, \ldots, G_s$. Given any polynomial P_d in a sequence $(P_1, \ldots, P_\delta)$ as above, then we will say that P can be reduced modulo $\{G_1, \ldots, G_s\}$ to P_d. Note that in general the sequence $(P_1, \ldots, P_\delta)$ is not unique, but is dependent on the choice of the $v^{(j)}$'s. The procedure described above is known as the division algorithm. It gives us a way to describe $P(\boldsymbol{X})$ as a linear combination $P(\boldsymbol{X}) = \sum_{i=1}^{s} a_i(\boldsymbol{X})G_i(\boldsymbol{X}) + P_\delta(\boldsymbol{X})$ where $\mathrm{lm}(a_i G_i) \preceq \mathrm{lm}(P)$, and no of the monomials in P_δ are divisible by any of the leading monomials of $G_1, \ldots, G_s$.

Definition I.A.8
The polynomial P_δ from above is called a residue of P modulo $\{G_1, \ldots, G_s\}$, or a remainder of P after division with $\{G_1, \ldots, G_s\}$.

Remark I.A.9
In general P may have many different residues modulo $\{G_1, \ldots, G_s\}$ according to the choice of the $u^{(j)}$'s.

However if $\{G_1, \ldots, G_s\}$ is a Gröbner basis, then the situation is simplified dramatically.

Theorem I.A.10
If $\mathcal{G} = \{G_1, \ldots, G_s\} \subseteq k[X_1, \ldots, X_m]$ is a Gröbner basis wrt. $\prec$, and if the division algorithm is used on $P(\boldsymbol{X})$ wrt. $\prec$. Then the remainder of P after division with $\mathcal{G}$ is unique.

In particular we have the following theorem.

Theorem I.A.11
Let $I \subseteq k[X_1, \ldots, X_m]$ be a nonzero ideal with Gröbner basis $\mathcal{G} = \{G_1(\boldsymbol{X}), \ldots, G_s(\boldsymbol{X})\}$ wrt. $\prec$. The following two statements are equivalent

(1) $P(\boldsymbol{X}) \in I$
(2) *the remainder of P after division with $\mathcal{G}$ is zero.*

I.A.3 A basis for $k[X_1, \ldots, X_m]/I$

One of the most important reasons for using Gröbner basis theory in this thesis, is that it gives us an easy way to find a basis for the k-vector space $k[X_1, \ldots, X_m]/I$. To explain how this works we will need the concept of a footprint.

Definition I.A.12
Let $I \subseteq k[X_1, \ldots, X_m]$ be any ideal, and $\prec$ a monomial ordering on $\mathcal{M}_m$. Consider the set

$$\Delta_\prec(I) := \{M(\boldsymbol{X}) \in \mathcal{M}_m \mid M(\boldsymbol{X}) \text{ is not a leading monomial of any polynomial in } I\}.$$

We call $\Delta_\prec(I)$ the footprint of I wrt. $\prec$, and use the abbreviated notion $\Delta(I)$, when $\prec$ is clear from the context.

Remark I.A.13
Note that $\Delta_\prec(I)$ is easily read from any Gröbner basis $\mathcal{G}$ for I wrt. $\prec$.

We have the following important result.

Theorem I.A.14
Let $I \subseteq k[X_1, \ldots, X_m]$ be an ideal, and $\Delta_\prec(I)$ the footprint of I wrt. some monomial ordering $\prec$ on $\mathcal{M}_m$. Then

$$\mathcal{B} := \{M(\boldsymbol{X}) + I \mid M(\boldsymbol{X}) \in \Delta_\prec(I)\}$$

is a basis for the k-vector space $k[X_1, \ldots, X_m]/I$.

We conclude the following. If we can develop a Gröbner basis for a given ideal I, then we will have a method to find a basis for the k-vector space $k[X_1, \ldots, X_m]/I$. As we will see in the following, the so-called Buchberger's algorithm is the right tool to develop a Gröbner basis for I wrt. any given $\prec$.

I.A.4 Buchberger's algorithm

To describe Buchberger's algorithm we will need the concept of an S-polynomial.

Definition I.A.15
Consider polynomials $G_1(\boldsymbol{X}), G_2(\boldsymbol{X}) \in k[X_1, \ldots, X_m]$ and a monomial ordering $\prec$ on $\mathcal{M}_m$. Denote by $\boldsymbol{X}^\gamma$ the smallest monomial (wrt. $\prec$) that is divisible both by $\mathrm{lm}(G_1)$ and by $\mathrm{lm}(G_2)$. The S-polynomial of G_1 and G_2 is the polynomial

$$S(G_1, G_2) := \frac{\boldsymbol{X}^\gamma}{\mathrm{lt}(G_1)} G_1 - \frac{\boldsymbol{X}^\gamma}{\mathrm{lt}(G_2)} G_2.$$

A particular nice thing happens if $\mathrm{lm}(G_1)$ and $\mathrm{lm}(G_2)$ are relatively prime.

Lemma I.A.16
If $\mathrm{lm}(G_1)$ and $\mathrm{lm}(G_2)$ are relatively prime, then the S-polynomial $S(G_1, G_2)$ reduces to zero modulo $\{G_1, G_2\}$.

We have the following important theorem.

Theorem I.A.17
Let $I \subseteq k[X_1, \ldots, X_m]$ be a nonzero ideal and $\prec$ a monomial ordering on $\mathcal{M}_m$. Then a basis $\mathcal{G} = \{G_1, \ldots, G_s\}$ for I is a Gröbner basis for I if and only if for all pairs $i \neq j$, $S(G_i, G_j)$ reduces modulo $\{G_1, \ldots, G_s\}$ to zero.

Now assume that a basis $\{G_1, \ldots, G_s\}$ for I is given that is not a Gröbner basis wrt. $\prec$. One easily verifies that a residue of $S(G_i, G_j)$ modulo $\{G_1, \ldots, G_s\}$ is contained again in I. By assumption (at least) one of these residues is nonzero. Denote it by G_{s+1}. If all the S-polynomials $S(G_i, G_j)$, $1 \leq i, j \leq s+1$ reduces modulo $\{G_1, \ldots, G_s, G_{s+1}\}$ to zero, then of course $\{G_1, \ldots, G_s, G_{s+1}\}$ is a Gröbner basis. If this is not the case we continue the process by adding a nonzero residue to the Gröbner basis to get $\{G_1, \ldots, G_{s+2}\}$. We continue this way. The very nice thing now is, that after finitely many steps, say n steps, we will end up with a set $\{G_1, \ldots, G_{s+n}\}$ that is a Gröbner basis. That is we have a simple method to extend a basis to a Gröbner basis. The above procedure is known as Buchberger's algorithm.

Theorem I.A.18
With a basis for I as the input Buchberger's algorithm returns a Gröbner basis for I wrt. $\prec$.

I.A.5 The footprint bound

Another result frequently used in the present material is the so-called footprint bound. As discussed in [12] it represents an alternative to the generalized Bezout's theorem.

Theorem I.A.19
Let $I \subseteq k[X_1, \ldots, X_m]$ be an ideal. If $\Delta(I)_\prec$ is finite then

$$\#\mathcal{V}_{\bar{k}}(I) \leq \#\Delta_\prec(I).$$

And equality holds if I is a radical ideal.

Remark I.A.20
In particular of course

$$\#\mathcal{V}_k(I) \leq \#\Delta_\prec(I). \tag{I.A.1}$$

holds. And one can verify, that equality holds in (I.A.1) precisely when $I = \mathcal{I}(\mathcal{V}_k(I))$*. Note that according to theorem I.A.14, the number* $\#\Delta_\prec(I)$ *is independent of the choice of monomial ordering* $\prec$*.*

Bibliography of part I

[1] A.I. Barbero, C. Munuera. *The weight hierarchy of Hermitian codes.* Preprint University of Valladolid , june 1998.

[2] Peter Beelen. *Error-correcting codes and algebraic geometry*. Master thesis, The University of Utrecht, 1997.

[3] Winfried Bruns, Udo Vetter. *Determinantal rings*. Lecture Notes in Mathematics 1327 (A. Dold, B. Eckmann eds.), Springer Verlag, 1988.

[4] David Cox, John Little and Donal O'Shea. *Ideals, Varieties, and Algorithms, Second Edition.* Springer, 1997.

[5] David Cox, John Little and Donal O'Shea. *Using Algebraic Geometry.* Springer, 1998.

[6] G.-L. Feng and T.R.N. Rao, *A Simple Approach for Construction of Algebraic-Geometric Codes from Affine Plane Curves*. IEEE Trans. Inf. Theory, vol. 40, pp. 1003-1012, july 1994.

[7] G.-L. Feng and T.R.N. Rao, *Improved Geometric Goppa Codes, Part I:Basic theory.* IEEE Trans. Inf. Theory, vol. 41, pp. 1678-1693, nov. 1995.

[8] G.-L. Feng, V. Wei, T.R.N. Rao and K.K. Tzeng, *Simplified Understanding and Efficient Decoding of a Class of Algebraic-Geometric Codes.* IEEE Trans. Inf. Theory, vol. 40, pp. 981-1002, july 1994.

[9] John B. Fraleigh. *A First Course of Abstract Algebra, Fourth Edition.* Addison-Wesley Publishing Company, 1989.

[10] Arnaldo Garcia and Henning Stichtenoth. *A Tower of Artin-Schreier Extensions of Function Fields Attaining the Drinfeld-Vladut Bound.* Invent. Math **121**, pp. 211-222, 1995.

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

[12] Olav Geil and Tom Høholdt. *Footprints or Generalized Bezout's Theorem*. Submitted to IEEE Trans. Inf. Theory, 1999.

[13] Olav Geil and Ruud Pellikaan. *On the structure of order domains*. Under construction. Preleminary version 1999.

[14] Gaétan Haché. *Construction Effective des Codes Géométriques*. PhD-thesis, Univesité Paris 6, 1996.

[15] Johan P. Hansen. *Toric Surfaces and Error-correcting Codes*. Preprint Series No. 9, Department of Mathematics, University of Aarhus, August 1998.

[16] Søren Have Hansen. *The geometry of Deligne-Lusztig varieties; Higher-Dimensional AG codes*. PhD-thesis, University of Aarhus, 1999.

[17] Petra Heijnen and Ruud Pellikaan. *Generalized Hamming weights of q-ary Reed-Muller codes*. IEEE Trans. Inf. Theory, vol. 44, pp. 181-196, jan. 1998.

[18] T. Helleseth, T. Kløve, and J. Mykkeltveit. *The weight distribution of irreducible cyclic codes with block lengths $n_1((q^l-1)/N)$*. Discr. Math. vol. 18, pp. 179-211, 1977.

[19] Tom Høholdt. *On (or in) Dick Blahut's "footprint"*. In *Codes, Curves and Signals* (A. Vardy ed.), pp. 3-9 , Kluwer 1998.

[20] Tom Høholdt, Jacobus H. van Lint and Ruud Pellikaan. *Order Functions and Evaluation Codes*. Proc AAECC-12, Toulouse 23-27 June, 1997, (T. Mora and H. Mattson eds.), Lect. Notes Comp. Sc., vol. 1255, pp. 138-150, Springer, Berlin 1997.

[21] Tom Høholdt, Jacobus H. van Lint and Ruud Pellikaan *Algebraic Geometry Codes.* Chapter 10 in *Handbook of Coding Theory* (V.S. Pless, and W.C. Huffman, eds.), vol. 1, pp. 871-961, Elsevier, Amsterdam 1998.

[22] Nathan Jacobsen. *Theory of Fields and Galois Theory*. Vol. III in *Lectures in Abstract Algebra.* D. Van Nostrand Company, USA 1953.

[23] C. Kirfel and R. Pellikaan. *The minimum distance of codes in an array coming from telescopic semigroups*. IEEE Trans. Inf. Theory, vol. 41, pp. 1720-1731, nov. 1995.

[24] Kaj Søndergaard Laursen. *Constructing Geometric Goppa Codes*. PhD-thesis, Aalborg University, 1998.

[25] Florence Jessie MacWilliams and Neil James Alexander Sloane. *The Theory of Error-Correcting Codes.* North-Holland, 1993.

[26] Ryutaroh Matsumoto. *Høholdt, van Lint and Pellikaan's Generalization of One-Point AG Codes is Equivalent to Miura's Generalization*. IEICE Trans. Fundamentals of Electronics, Communications and Computer Sciences, vol. E82-A, no.10, pp. 2007-2010, oct. 1999

[27] Shinji Miura. *PhD-thesis*. University of Tokyo, 1997 (japanese).

[28] Shinji Miura. *Linear codes on affine algebraic curves.* Trans. IEICE **j81-A**, no. 10, pp. 1398-1421, 1998 (japanese).

[29] Michael E. O'Sullivan. *Decoding of codes defined by a single point on a curve*. IEEE Trans. Inf. Theory, vol. 41, pp. 1709-1719, nov. 1995.

[30] Michael E. O'Sullivan. *Grobner Basis and Decoding of Algebraic Geometry Codes*. Preleminary version of [31], oct. 24, 1997.

[31] Michael E. O'Sullivan. *New Codes for the Berlekamp-Massey-Sakata Algorithm*, to appear in Finite Fields and their Applications.

[32] Ruud Pellikaan. *On the efficient decoding of algebraic-geometric codes*. Eurocode 92, CISM Courses and Lectures, vol. 339, pp. 231-253, Springer, New York 1993.

[33] Ruud Pellikaan. *On the existense of order functions*. To appear in Journal of Statistical Planning and Inference.

[34] Ruud Pellikaan, B.-Z. Shen and G.J.M. van Wee. *Which linear codes are algebraic-geometric?*. IEEE Trans. Inf. Theory, vol. 37, pp. 583-602, march 1991.

[35] Ruud Pellikaan, Henning Stichtenoth and Fernando Torres. *Weierstrass semigroups in an asymptotically good tower of function fields.* Finite Fields Appl., vol. 4, pp. 381-392, 1998.

[36] L. Robbiano. *On the theory of graded structures.* J. Symb. Comp. **2**, pp. 139-170, 1986.

[37] G. Schiffels. *Orderings and algorithms in commutative algebra*. Afrika Mathematika, Series 3, vol. 2, pp. 79-101, 1993.

[38] Henning Stichtenoth. *Algebraic Function Fields and Codes.* Universitext, Springer-Verlag, 1993.

[39] B.-Z. Shen and K.K. Tzeng. *Generation of matrices for determining minimum distance and decoding of algebraic-geometric codes*. IEEE Trans. Inf. Theory, vol. 41, pp. 1703-1708, nov. 1995.

[40] Bernd Sturmfels. *Gröbner Bases and Convex Polutopes*. AMS, Providence RI, 1996.

[41] Anders Bjært Sørensen. *Weighted Reed-Muller Codes and Algebraic-Geometric Codes*. IEEE Trans. Inf. Theory, vol. 38, pp. 1821-1827, nov. 1992.

[42] Michael A. Tsfasman and Serge G. Vlăduţ. *Geometric Approach to Higher Weights*. IEEE Trans. Inf. Theory, vol. 41, pp. 1564-1588, nov. 1995.

[43] Jacobus Hendricus van Lint. *Introduction to Coding Theory.* Springer-Verlag, 1981.

[44] Conny Voß and Tom Høholdt. *An explicit construction of a sequence of codes attaining the Tsfasman-Vladut-Zink bound. The first steps.* IEEE Trans. Inf. Theory, vol. 43, pp. 128-135, jan. 1997.

[45] V. K. Wei. *Generalized Hamming weights for linear codes.* IEEE Trans. Inf. Theory, vol. 37, pp. 1412-1418, sept. 1991.

[46] O. Zariski and P. Samuel. *Commutative Algebra, Vol.I.* Springer-Verlag, 1975.

List of symbols in part I

Index of part I