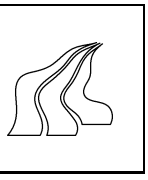
AALBORG UNIVERSITY

Codes Based on an $\mathbb{F}_q$-Algebra

Order Domains and their Application in Coding Theory
The Generalized Hamming Weights of the Dual of an Evaluation Code

Olav Geil

DEPARTMENT OF MATHEMATICAL SCIENCES
Fredrik Bajers Vej 7E — DK 9220 Aalborg Øst — Denmark
Tel.: +45 96 35 80 80



Codes Based on an $\mathbb{F}_q$-Algebra

Order Domains and their Application in Coding Theory
The Generalized Hamming Weights of the Dual of an Evaluation Code

PhD-thesis,
The Faculty of Technology and Science at Aalborg University,
Second edition

Olav Geil

Department of Mathematical Sciences
Aalborg University

DEPARTMENT OF MATHEMATICAL SCIENCES
Fredrik Bajers Vej 7E — DK 9220 Aalborg Øst — Denmark
Tel.: +45 96 35 80 80

Preface to the first edition

This thesis is the result of my PhD-study at Department of Mathematical Sciences, Aalborg University, Denmark. It concerns two topics from what could be called the theory of codes based on an $\mathbb{F}_q$-algebra. The thesis is organized in two self-contained parts, that can be read independently of each other. Each part contains its own bibliography, and part I contains its own list of symbols and list of index terms.

In part I order domains and their application in coding theory are treated. Part I is written as a general introduction to this new research area. Both well-known as well as new results are treated. Most of these new results have been developed through a co work between Dr. Ruud Pellikaan, Department of Mathematics and Computing Science, Technical University of Eindhoven, The Netherlands, and myself.

Part II is a reproduction of a paper by Professor Tom Høholdt, Department of Mathematics, Technical University of Denmark, and myself. This paper is concerned with the problem of how to determine/estimate the generalized Hamming weights of the dual of an evaluation code.

What links together the two parts is mainly the fact that the same relatively simple tools from Gröbner basis theory are used throughout the thesis. To read this thesis knowledge about the most basic Gröbner basis theory therefore is required. Appendix I.A in part I contains a review of some of this theory. For a nice and general introduction to the subject, see David Cox, John Little and Donal O'Shea's book *Ideals, Varieties, and Algorithms, Second Edition*, Springer, 1997.

Another thing that is common for the two parts is the fact that a great deal of the concerned results can be seen as developments of results given by Feng, Rao, and co-authors.

Acknowledgements

I am grateful to Associate Professor Christian Thommesen who has been my advisor through the PhD-study. Christian Thommesen has always been ready for a good discussion on mathematical topics (as well as other topics). I am grateful to Dr. Ruud Pellikaan who shared his ideas with me under my three month long stay in the spring 1998 at Department of Mathematics and Computing Science, Technical University of Eindhoven, The Netherlands. Visiting the department was a nice experience. In particular my thanks go to Ruud Pellikaan, his wife Marion, Peter Beelen, Jeroen Keuning, and Eric Verheul for their hospitality. I am also grateful to Professor Tom Høholdt who shared his ideas with me under more short stays at Department of Mathematics, Technical University of Denmark. And who has introduced me to the topic of order domains. Also thanks to Tom Høholdt for hospitality under my stays there. My thanks further go to Jens Peter Pedersen who so to speak got me started, being my advisor when I was writing my master thesis. I also thank Johnny Weile and Søren Raunsbæk Jørgensen for many good discussions on order domain theory, during the period where they were writing their master thesis. It was really a good experience discussing with them. Finally I am most of all very grateful to my wife Kirsten for being such a good support under my study. Without her encorregment I would probably still have been a postman today. As a mathematician I am only able to work properly when I am happy. I thank Kirsten for making me a happy man, and thereby able to write this thesis.

Aalborg University, December, 1999. Olav Geil.

Preface to the second edition

The present thesis was defended on april 7 2000 with the result that the author has been awarded the PhD-degree.

Some misprints in the first edition has been corrected. And some new comments are included. The theory described in part I, has been developed further after the thesis was originally submitted. See the manuscripts “On the structure of order domains”, june 2000, by Olav Geil and Ruud Pellikaan, and “On the construction of codes from order domains”, june 2000, by Olav Geil.

Aalborg University, June, 2000. Olav Geil.

Contents of the thesis

Summary

This thesis contains two parts. Part I is a general introduction to the new research area: Order domains, and their application in coding theory. Both well-known as well as new results are included. Many of the new results have been developed in co-work between Dr. Ruud Pellikaan and the author of this thesis. Part II is a reproduction of a paper by Professor Tom Høholdt and the author of this thesis. It is concerned with the problem of how to find/estimate the generalized Hamming weights of the dual of an evaluation code. In the following I[n] means item n in the bibliography on pp. 152-155 in part I, and II[n] means item n in the bibliography on pp. 183-184 in part II.

Summary of part I

Chapter I.1 in part I gives an overview of the historical development of the theory of order domains, including their application in coding theory. In chapter I.2 some well-known results and definitions are stated concerning monoids, orderings on these, and in particular monomial orderings. A new and very general definition is given of a so-called weighted degree lexicographic ordering on $k[X_1, \ldots, X_m]$. As demonstrated in later chapters, this concept is a nice tool when one wants to construct order domains and order functions by use of Gröbner basis theory. In chapter I.3 the basic definitions from order domain theory is given. In agreement with I[13] an order function is defined to be a function ρ from a k-algebra R to $\Lambda \cup \{-\infty\}$, where $(\Lambda, \prec_\Lambda)$ is a well-order. The order function is to satisfy five certain criterions. A k-algebra that possesses an order function is called an order domain. The structure of the order function ensures that an order domain R possesses a so-called well-behaving basis. The elements in the well-behaving basis is called an order basis. The order basis constitutes a basis for R as a vector space over k, and the knowledge of how ρ acts on the order basis together with knowledge of $\prec_\Lambda$ describes the order

function ρ completely. The definition from I[13] is a slightly generalization of the previous given definitions in I[21], I[30], and I[31]. In I[21] for instance $(\Lambda, \prec_\Lambda) = (\mathbb{N}_0, <)$. Besides given a few new order functions, the advantage of the general definition from I[13] is merely that it gives a new point of view on order functions. In particular the class of weight functions, that are order functions satisfying a certain sixth criterion, is enlarged considerably using this new definition. This enlargement makes it easy to give non trivial examples of order functions on k-algebras of transcendence degree more than 1. Something that has been difficult until now. In I[31] examples are given of order functions on order domains of transcendence degree more than 1. However these examples use relatively difficult valuation theory and algebraic geometry, something that is not needed in this thesis. In chapter I.3 further some terminology is introduced, that makes it possible to classify the order functions related to any given order domain. An ordering $\prec'_\Lambda$ on Λ is said to be legal wrt. a given order basis for R, if the order basis together with $\prec'_\Lambda$ describes an order function. In chapter I.4 it is shown that given any semigroup $\Lambda \subseteq \mathbb{N}_0^r$ (finitely or not finitely generated) then there exists an order domain R with a weight function $\rho : R \to \Lambda \cup \{-\infty\}$. Chapter I.5 gives some general results on order domains that are quotient rings of the form $R = k[\boldsymbol{X}]/I$, where $I \subseteq k[\boldsymbol{X}]$ is an ideal. It is shown that an order domain that is a quotient ring always can be described in a particular nice way. One may assume that if $f = F + I$, where $F \in k[\boldsymbol{X}]$, and $f \neq I$, then the support $M_1, \ldots, M_s$ of F contains two different monomials, say M_{i_1} and M_{i_2} such that $\rho(M_{i_1} + I) = \rho(M_{i_2} + I) \succeq \rho(M_t + I)$ for $t = 1, \ldots, s$. In chapter I.6 we consider any finitely generated semigroup $\Lambda \subseteq \mathbb{N}_0^r$ and show how to construct a so-called toric ideal $I \subseteq k[\boldsymbol{X}]$ with the property that a weight function $\rho : k[\boldsymbol{X}]/I \to \Lambda \cup \{-\infty\}$ exists. The theory of toric ideals is well-known, however their application in order domain theory is new. The corresponding varieties $\mathcal{V}_k(I)$ are studied in the case of $k = \mathbb{F}_q$. It is shown using only simple techniques that $\#\mathcal{V}_{\mathbb{F}_q}(I) = q$ whenever I is a toric ideal corresponding to a semigroup $\Lambda \subseteq \mathbb{N}_0$. By examples it is shown that in the general case $\Lambda \subseteq \mathbb{N}_0^r$, $r > 1$, however it can happen that $\#\mathcal{V}_{\mathbb{F}_q}(I) > q^r$. An explanation of this phenomenon is given on the basis of elimination theory. Chapter I.7 is concerned with what we call Pellikaan's Factor Ring Theorem. In the original version from I[33], Pellikaan's Factor Ring Theorem describes, by use of Gröbner basis theory, a very large class of order domains R that possesses a weight function $\rho : R \to \Lambda \cup \{-\infty\}$ where $\Lambda \subseteq \mathbb{N}_0$. In the version presented in I[13] and in this thesis, the theorem is generalized to deal with the case $\Lambda \subseteq \mathbb{N}_0^r$, where r can be arbitrary large. The definition from chapter I.2 of the weighted degree lexicographic ordering is crucial for this generalization. Several examples of order domains constructed using the generalized version

of Pellikaan's Factor Ring Theorem are considered. In particular certain determinantal rings are studied. Chapter I.8 is concerned with different techniques to construct new order domains from old ones. Three techniques from I[13] are considered. It is first described how one can transform an order domain $R = k[\boldsymbol{X}]/I$ where I is toric, to a new order domain $R' = k[\boldsymbol{X}]/I'$, where I' is not toric, by adding appropriate terms to the generators of I. Next the very general tensor product construction is treated. Finally some results are given on how to construct new order domains from old ones by certain substitutions. Chapter I.9 deals with the nature of Λ in the case of a weight function. Using only pure order domain theory it is shown, that Λ can not be contained in $\mathbb{N}_0$ when the transcendence degree of R exceeds 1. A similar result has lately been shown in I[31] and I[26] using different techniques (that is before the result from this thesis has been published). Chapter I.9 further contains a very unexpected example of a set of weight functions on $k[X_1, X_2]$. Chapter I.10 describes the connection between order domain theory and valuation theory, as investigated by other authors. In particular the strong connection between order domains of transcendence degree 1, and algebraic function fields of transcendence degree 1 is described. The rest of part I is concerned with the application of order domains in coding theory. Chapter I.11 starts with a treatment of the simplest construction of codes related to those of the order functions, that are also order functions with respect to the definition in I[21]. The evaluation code E_l and its dual C_l are treated following the lines of I[21]. The order bound from I[21] (and I[6]) that is a bound on the minimum distance of C_l, is stated and proved following again the lines of I[21]. The order bound is next shown to hold, also when the more general class of order functions, as defined in I[13] and in this thesis, is used. The generalization of E_l is denoted by E_λ and the generalization of C_l by C_λ. In I[Heinen] it is shown how to extend the order bound on the minimum distance of the C_l codes to a bound on every generalized Hamming weight of the C_l codes. Also this result can be generalized to work in the case of any C_λ code. A rough outline of a proof for this fact is given. Also the improved codes $\tilde{C}(d)$ and $\tilde{C}_\varphi(d)$ from I[6] (and I[21]) is generalized. Finally from I[21] we have a bound on the minimum distance of the E_l code in the special case of a weight function $\rho : R \to \Lambda \cup \{-\infty\}$, where $\Lambda \subseteq \mathbb{N}_0$. This bound is unfortunately not immediately generalized to work also in the case of a weight function where $\Lambda \not\subseteq \mathbb{N}_0$. In chapter I.12 the construction of codes from order domains are compared to previous known constructions. We describe the well-known fact that one, by using the theory of order domains, gets an easy way to describe and handle the so-called 1-point geometric Goppa codes and their duals. Also the well-known fact that the weighted Reed-Muller codes can be understood by use of order domain theory is described. Chapter I.12 present an

overview of the connection between the codes constructed from order domains and the codes constructed using other techniques. It becomes clear, that a very large class of new codes can be described using the definition of a weight function from I[13] and from this thesis. In chapter I.13 we are concerned with the following problem. Assume we are given an order domain R and two order functions $\rho : R \to \Lambda \cup \{-\infty\}$ and $\rho' : R \to \Lambda \cup \{-\infty\}$ where ρ and ρ' are identical on a given common order basis, but where Λ is ordered by $\prec_\Lambda$ in the case of ρ and is ordered by $\prec'_\Lambda$ in the case of ρ'. Does the different choices of ordering on Λ have any effect on the parameters of the corresponding $\tilde{C}_\varphi(d)$ codes? By an example we show that this (surprisingly) can actually happen to be the case. Chapter I.14 deals with different techniques for the construction and estimation of the codes. The notion of the restricted footprint is introduced as follows. Given a footprint $\Delta(I)$ for $I \subseteq \mathbb{F}_q[X_1, \ldots, X_m]$ then the restricted footprint is given by

$$\Delta_q(I) := \{M \in \Delta(I) \mid \deg_{X_i}(M) < q, i = 1, \ldots, m\}.$$

In particular we get the restricted footprint bound $n := \#\mathcal{V}_{\mathbb{F}_q}(I) \leq \#\Delta_q(I)$, implying that the codes investigated in part I, can at most be $\Delta_q(I)$ long. The bound $n \leq \#\Delta_q(I)$ is compared with the so-called Hasse-Weil bound from algebraic function field theory in the case of a type-I curve. Also the restricted footprint turns out to be a very practical tool in the actual construction of the codes, and in the practical use of the order bound. Chapter I.14 contains various examples of codes constructed from order domains that are studied in the earlier chapters. These codes are relatively good, however not better than previous known codes. Chapter I.15 deals with the asymptotic behaviour of some classes of codes coming from order domains. The codes related to repeated tensor products of order domains are treated in three important cases. Wrt. the order bound, all three cases are shown to give asymptotic bad codes. Finally we treat a famous tower of function fields given by Garcia and Stichtenoth. This tower is known to correspond to good sequences of geometric Goppa codes. Sequences that are so good, that they reach the Tsfasman-Vlăduţ-Zink bound. However no-one have succeeded in actual constructing the sequences of codes related to the tower. We suggest a method to attack the problem from an order domain theory point of view. We do in no way succeed in solving this problem ourselves.

Summary of part II

Part II contains a reproduction of the paper *Footprints or Generalized Bezout's Theorem* by Olav Geil and Tom Høholdt. This paper is been accepted by *IEEE Transactions on Information Theory*, where it will appear as a correspondence. The paper is a natural continuation of the recent papers II[2], II[3] and II[4] by Feng, Rao et. al. In these three papers the authors described methods to estimate the generalized Hamming weights of the dual of an evaluation code, using a generalization of Bezout's theorem. In the paper reproduced in part II, we show that Feng, Rao et. al.'s method can be extended to give not only estimated values of the generalized Hamming weights, but to give the actual values of these weights. More important we show that it is much more natural to use the footprint bound from Gröbner basis theory instead of their generalization of Bezout's theorem, when estimating/calculating the generalized Hamming weights of the dual of an evaluation code. Consider any k-dimensional code $\mathcal{C}$ with parity check matrix $H := [\boldsymbol{h_1}, \ldots, \boldsymbol{h_r}]^T$. Define

$$[\boldsymbol{h_i}] := \{\boldsymbol{h_i} + \sum_{j=1}^{i-1} \alpha_j \boldsymbol{h_j} \mid \alpha_j \in \mathbb{F}_q\},$$

for $i = 1, \ldots, r$.

$$D_{\{[\boldsymbol{h_{i_1}}], \ldots, [\boldsymbol{h_{i_s}}]\}} := \max \big\{ n - \mathrm{Supp}(\boldsymbol{h'_{i_1}}, \ldots, \boldsymbol{h'_{i_s}}) \mid \boldsymbol{h'_{i_t}} \in [\boldsymbol{h_{i_t}}], t = 1, \ldots, s \big\}$$

for $1 \leq i_1 < \cdots < i_s \leq r$. And

$$D_s := \max \left\{ D_{\{[\boldsymbol{h_{i_1}}], \ldots, [\boldsymbol{h_{i_s}}]\}} \mid 1 \leq i_1 < \cdots < i_s \leq r \right\}$$

for $s = 1, \ldots, r$. Denote by d_h the h.th generalized Hamming weight of $\mathcal{C}$. The by far most important part of the following theorem, namely the $\Leftarrow$ part of (i) was stated by Feng, Rao et. al. The rest is new.

Theorem
Let C be a code of length n with parity check matrix $H = [\boldsymbol{h_1}, \ldots, \boldsymbol{h_r}]^T$ (not necessarily of full rank). For any $d^* \leq r + h$, $h \leq k$, $d \leq n$ the following biimplications hold

(i) $d_h \geq d^* \Leftrightarrow D_{r-d^*+h+1} \leq d^* - 2$

(ii) $d_h \leq d^* \Leftrightarrow D_{r-d^*+h} \geq d^*$.

Of particular interest is the case where $\mathcal{C}$ is the dual of an evaluation code, that is where $\boldsymbol{h_i}$ is of the form $\boldsymbol{h_i} := (F_i(P_1), \ldots, F_i(P_n))$, $i = 1, \ldots, r$, where $P_j \in \mathbb{F}_q$, $j = 1, \ldots, n$. In this case the estimation/calculation of the number D_s corresponds to the estimation/calculation of the maximal number of common zeros from $\{P_1, \ldots, P_n\}$ between s polynomials of the form

$$F_{i_1} + \sum_{j=1}^{i_1-1} \alpha_j^{(1)} F_j, \ldots, F_{i_s} + \sum_{j=1}^{i_s-1} \alpha_j^{(s)} F_j,$$

with $1 \leq i_1 < i_2 < \cdots < i_s \leq r$. Note that all possible choices of $i_1, \ldots, i_s$ are to be considered, and that for each such choice we need to consider all possible combinations of the $\alpha_j^{(t)}$'s. To estimate the maximal number of common zeros whenever $i_1, \ldots, i_s$ is fixed but the $\alpha_j^{(t)}$'s takes on every possible values, Feng, Rao et. al. developed a generalization of Bezout's theorem. In the paper reproduced in part II, we demonstrate that it is more natural to use the footprint bound to make these estimations. We demonstrate this in two steps. In the first step we treat a number of theorems by Feng, Rao et. al. Theorems that give bounds on the number of common zeros between various polynomials. We give new and more simple proofs and show how the footprint technique suggests generalizations of the theorems. In the second step we are concerned with the estimation of the generalized Hamming weights of different codes, using the footprint bound in combination with the classical Bezout's theorem, instead of using the generalized Bezout's theorem. Feng, Rao et. al. defined an improved Klein code, and estimated its minimum distance. We not only estimate the minimum distance but find the actual value of all the generalized Hamming weights. Also Feng, Rao et. al. defined an improved Hermitian code for which they estimated the minimum distance. We estimate all the generalized Hamming weights and conclude that not only the minimum distance is improved. Feng, Rao et. al. gave two examples of codes over the affine space $\mathbb{F}_{2^m}$, that have large minimum distances.

We generalize their construction and estimate the minimum distances of the new codes. Finally we consider codes defined by use of Gröbner basis theory. Let $\prec$ be a monomial ordering on $\mathbb{F}_q[X_1, \ldots, X_m]$, $I \subseteq \mathbb{F}_q[X_1, \ldots, X_m]$ a prime ideal, and $\Delta(I)$ the footprint of I wrt. $\prec$. Choose $F_1, \ldots, F_r$ as the r smallest elements in $\Delta(I)$ wrt. $\prec$. And choose $\{P_1, \ldots, P_n\} := \mathcal{V}_{\mathbb{F}_q}(I)$, that is as the variety of I. The generalized Hamming weights of the evaluation codes constructed by choosing $G := [\boldsymbol{h_1}, \ldots, \boldsymbol{h_r}]^T$ as generator matrix were estimated by Shibuya et. al. We state a result dual to theirs, as we estimate the generalized Hamming weights of the codes with parity check matrix equal to $[\boldsymbol{h_1}, \ldots, \boldsymbol{h_r}]^T$.

Dansk resume (Summary in danish)

Denne afhandling har den danske titel *Koder konstrueret ved hjælp af en $\mathbb{F}_q$-algebra*. Afhandlingen har undertitlen *Ordensområder og deres anvendelser i kodningsteori. De generaliserede Hammingvægte af evalueringskodernes dualkoder.*
Afhandlingen består af to dele. Del I er en generel introduktion til det nye forskningsområde: Ordensområder og deres anvendelser i kodningsteori. Såvel velkendte som nye resultater behandles. Mange af de nye resultater er opnået i et samarbejde mellem doktor Ruud Pellikaan og forfatteren af denne afhandling. Del II er en gengivelse af en artikel skrevet af docent Tom Høholdt og forfatteren af denne afhandling. Den handler om metoder til at finde hhv. estimere de generaliserede Hammingvægte for evalueringskodernes dualkoder. I dette resume vil I[n] angive emne n i bibliografien på siderne 152-155 i del I, og II[n] vil angive emne n i bibliografien på siderne 183-184 i del II.

Resume af del I

Kapitel I.1 i afsnit I giver et overblik over den historiske udvikling af teorien om ordensområder og deres anvendelser i kodningsteorien. I kapitel I.2 behandles nogle velkendte definitioner og resultater vedrørende monoider, ordninger på sådanne samt specielt monomiale ordninger. Der indføres en ny og meget generel definition af en såkaldt vægtet graderet leksikografisk ordning på $k[X_1, \ldots, X_m]$. I senere kapitler viser det sig, at denne definition er et godt redskab, når der skal konstrueres ordensområder og ordensfunktioner vha. Gröbnerbasis-teori. I kapitel I.3 præsenteres de basale definitioner fra ordensområdeteorien. Som i I[13] defineres en ordensfunktion til at være en funktion ρ fra en k-algebra R ind i $\Lambda \cup \{-\infty\}$, hvor $(\Lambda, \prec_\Lambda)$ er en velorden. Ordensfunktionen skal opfylde fem specielle kriterier. En k-algebra, som besidder en ordensfunktion, kaldes et ordensområde. Ordensfunktionens struktur sikrer, at

der til ordensområdet er knyttet en såkaldt pæn basis. Elementerne i den pæne basis kaldes en ordensbasis. Ordensbasen udgør en basis for R som et vektorrum over k. Et kendskab til, hvorledes ρ virker på ordensbasen, tilsammen med en viden om $\prec_\Lambda$ fastlægger ordensfunktionen ρ fuldstændig. Definitionen fra I[13] er en mindre generalisering af de tidligere givne definitioner i I[21], I[30], og I[31]. F.eks. kræves det i I[21], at $(\Lambda, \prec_\Lambda) = (\mathbb{N}_0, <)$. Fordelen ved definitionen fra I[13] er ikke så meget de få nye ordensfunktioner, den giver anledning til, som det er den nye synsvinkel på ordensfunktioner, den giver anledning til. En specielt vigtig klasse af ordensfunktioner er de såkaldte vægtfunktioner, som ud over de fem kriterier opfylder et sjette kriterium. Den nye definition af ordensfunktioner fra I[13] inducerer en ny definition af vægtfunktioner. Mængden af vægtfunktioner mht. den nye definition er langt større end mængden af vægtfunktion mht. de gamle definitioner. Den store gevinst ved den nye definition er, at det vha. de nye vægtfunktioner bliver let at give ikke-trivielle eksempler på ordensfunktioner på k-algebraer af transcendensgrad større end 1. Dette har været vanskeligt indtil nu. I I[31] gives der ganske vist eksempler på ordensfunktioner på ordensområder af transcendensgrad højere end 1. Imidlertid benyttes der i disse eksempler relativt svært tilgængelig valuationsteori og algebraisk geometri. Sådanne teorier behøves ikke i denne afhandling. Videre introduceres i kapitel I.3 nye termer, vha. hvilke det bliver muligt at klassificere ordensfunktionerne hørende til et givet ordensområde. En ordning $\prec'_\Lambda$ på Λ siges at være legal mht. en given ordensbasis for R, hvis ordensbasen tilsammen med $\prec'_\Lambda$ beskriver en ordensfunktion. I kapitel I.4 vises det, at der for enhver semigruppe $\Lambda \subseteq \mathbb{N}_0^r$ (endelig såvel som ikke-endelig genereret) findes et ordensområde R med tilhørende vægtfunktion $\rho : R \to \Lambda \cup \{-\infty\}$. Kapitel I.5 indeholder nogle generelle resultater vedrørende ordensområder, som er kvotientringe af formen $R = k[\boldsymbol{X}]/I$, hvor $I \subseteq k[\boldsymbol{X}]$ er et ideal. Det vises, at et ordensområde, der er en kvotientring, altid kan beskrives på en særlig simpel form. Man kan nemlig antage, at hvis $f = F + I$, hvor $F \in k[\boldsymbol{X}]$ og $f \neq I$, da indeholder mængden af monomier $M_1, \ldots, M_s$ i F to forskellige monomier M_{i_1} og M_{i_2} således, at $\rho(M_{i_1} + I) = \rho(M_{i_2} + I) \succeq \rho(M_t + I)$ for $t = 1, \ldots, s$. I kapitel I.6 viser vi, hvorledes man givet en vilkårlig endeligt genereret semigruppe $\Lambda \subseteq \mathbb{N}_0^r$ kan konstruere et såkaldt torisk ideal $I \subseteq k[\boldsymbol{X}]$ med den egenskab, at der eksisterer en vægtfunktion $\rho : k[\boldsymbol{X}]/I \to \Lambda \cup \{-\infty\}$. Teorien om toriske idealer er velkendt, men anvendelsen af dem i ordensområdeteorien er ny. De tilhørende varieteter $\mathcal{V}_k(I)$ studeres i tilfældet $k = \mathbb{F}_q$. Det vises vha. simple teknikker, at $\#\mathcal{V}_{\mathbb{F}_q}(I) = q$ når I er et torisk ideal hørende til en semigruppe $\Lambda \subseteq \mathbb{N}_0$. Vha. eksempler vises det, at det imidlertid i det generelle tilfælde $\Lambda \subseteq \mathbb{N}_0^r$, $r > 1$, kan ske, at $\#\mathcal{V}_{\mathbb{F}_q}(I) > q^r$. En forklaring på dette fænomen gives vha. eliminationsteori. Kapitel I.7 omhandler, hvad vi vil kalde Pellikaan's kvotien-

tringssætning. I den originale version fra I[33] beskriver Pellikaan's kvotientringssætning, vha. Gröbnerbasis-teori, en meget stor klasse af ordensområder R, som besidder en vægtfunktion $\rho : R \to \Lambda \cup \{-\infty\}$, hvor $\Lambda \subseteq \mathbb{N}_0$. I I[13] og i denne afhandling er sætningen generaliseret til at behandle det generelle tilfælde $\Lambda \subseteq \mathbb{N}_0^r$, hvor r kan antage en vilkårlig værdi. Definitionen fra kapitel I.2 af en vægtet graderet leksikografisk ordning er central for denne generalisering. Der bliver givet flere eksempler på ordensområder konstrueret vha. den generaliserede version af Pellikaan's kvotientringssætning. Specielt studeres visse determinantringe. Kapitel I.8 beskriver forskellige tekniker vha. hvilke, man kan konstruere nye ordensområder fra gamle ordensområder. Tre tekniker fra I[13] betragtes. Først beskrives det, hvorledes man kan transformere et ordensområde $R = k[\boldsymbol{X}]/I$, hvor I er torisk, til et nyt ordensområde $R' = k[\boldsymbol{X}]/I'$, hvor I' ikke er torisk, ved at addere passende termer til generatorerne for I. Dernæst behandles den meget generelle tensorproduktskonstruktion. Til sidst præsenteres nogle resultater vedrørende, hvorledes man kan konstruere nye ordensområder fra gamle ordensområder vha. visse substitutioner. Kapitel I.9 beskriver Λ i det tilfælde, hvor ρ er en vægtfunktion. Vha. ren ordensområdeteori vises det, at Λ ikke kan være indeholdt i $\mathbb{N}_0$ når transcendensgraden af R overstiger 1. Et tilsvarende resultat er for nyligt blevet vist i I[31] og i I[26] vha. ganske andre tekniker (dvs. før denne afhandling er blevet publiceret). Kapitel I.9 indeholder videre et særdeles overraskende eksempel på en mængde af vægtfunktioner på $k[X_1, X_2]$. Kapitel I.10 beskriver diverse forfatteres kortlægning af forbindelsen mellem ordensområdeteorien og valuationsteorien. Specielt behandles den stærke forbindelse mellem ordensområder af transcendensgrad 1 og algebraiske funktionslegemer af transcendensgrad 1. Resten af del I omhandler ordensområdernes anvendelse i kodningsteorien. Kapitel I.11 starter med en behandling af de simpleste konstruktioner af koder hørende til de af ordensfunktionerne, som også er ordensfunktioner mht. definitionen i I[21]. Evalueringskoden E_l og dennes duale C_l behandles som i I[21]. Ordensgrænsen fra I[21] (og I[6]), som er en grænse på minimumsafstanden af C_l, opskrives og vises som i I[21]. Det vises dernæst, at ordensgrænsen stadig holder, når man anvender den mere generelle klasse af ordensfunktioner, der er defineret i I[13] og i denne afhandling. Generaliseringen af E_l betegnes E_λ og generaliseringen af C_l betegnes C_λ. I I[17] er det vist, hvorledes ordensgrænsen på minimumsafstanden af C_l-koden, kan udvides til en grænse for enhver generaliseret Hammingvægt af C_l-koden. Et tilsvarende resultat holder i det mere generelle tilfælde af en C_λ-kode. En skitse af et bevis for dette resultat gives. Også de såkaldt forbedrede koder $\tilde{C}(d)$ og $\tilde{C}_\varphi(d)$ fra I[21] (og I[6]) generaliseres til tilfældet, hvor ρ kun er en ordensfunktion mht. den mere generelle definition. Endelig har vi fra I[21] en grænse på minimumsafstanden af E_l-koden, i specialtilfældet, hvor ρ

er en vægtfunktion med værdisemigruppe $\Lambda \subseteq \mathbb{N}_0$. Denne grænse kan desværre ikke umiddelbart generaliseres til at gælde, når $\Lambda \not\subseteq \mathbb{N}_0$. I kapitel I.12 sammenlignes konstruktionen af koder fra ordensområder med tidligere kendte konstruktioner af koder. Vi beskriver det velkendte faktum, at man vha. ordensområdeteorien får en simpel og elegant beskrivelse af de såkaldte 1-punkts geometriske Goppakoder samt af deres dualkoder. Også de vægtede Reed-Muller koder kan beskrives og behandles vha. ordensområdeteori. Kapitel I.12 giver et overblik over forbindelsen mellem koderne, som er konstrueret fra ordensområder, og koderne, som er konstrueret vha. andre tekniker. Det fremgår, at ordensområdeteorien fra I[13] og fra denne afhandling giver anledning til en ny meget stor klasse af koder. I kapitel I.13 beskæftiger vi os med følgende spørgsmål. Antag, at der er givet et ordensområde R med to ordensfunktioner $\rho : R \to \Lambda \cup \{-\infty\}$ og $\rho' : R \to \Lambda \cup \{-\infty\}$, hvor ρ og ρ' er identiske på en given fælles ordensbasis, men hvor Λ er ordnet vha. $\prec_\Lambda$ i tilfældet af ρ og er ordnet vha. $\prec'_\Lambda$ i tilfældet af ρ'. Har de forskellige valg af ordninger på Λ nogen indflydelse på parametrene af de tilhørende $\tilde{C}_\varphi(d)$-koder? Vha. et eksempel viser vi, at dette faktisk kan være tilfældet. Kapitel I.14 beskriver forskellige tekniker, som er nyttige, når koderne skal konstrueres, og når deres parametre skal estimeres. Det såkaldt restringerede fodaftryk indføres på følgende måde. Givet et fodaftryk $\Delta(I)$ for $I \subseteq \mathbb{F}_q[X_1, \ldots, X_m]$, da er det restringerede fodaftryk givet ved

$$\Delta_q(I) := \{M \in \Delta(I) \mid \deg_{X_i}(M) < q, i = 1, \ldots, m\}.$$

Specielt har vi den restringerede fodaftryksgrænse $n := \#\mathcal{V}_{\mathbb{F}_q}(I) \leq \#\Delta_q(I)$, af hvilken man kan se, at de koder, der behandles i del I, højst kan være $\Delta_q(I)$ lange. I specialtilfældet af en type-I kurve sammenligner vi grænsen $n \leq \#\Delta_q(I)$ med den såkaldte Hasse-Weil grænse fra den algebraiske funktionslegemeteori. Det restringerede fodaftryk viser sig også at være et godt værktøj i den faktiske konstruktion af koder og i den praktiske anvendelse af ordensgrænsen. Kapitel I.14 indeholder flere eksempler på koder konstrueret fra ordensområder, der er beskrevet i tidligere kapitler. Disse koder er relativt gode, om end de ikke er bedre end i forvejen kendte koder. Kapitel I.15 beskæftiger sig med de asymptotiske egenskaber af visse klasser af koder konstrueret fra ordensområder. Koderne hørende til de gentagne tensorprodukter af ordensområder behandles i tre vigtige tilfælde. Mht. ordensgrænsen viser det sig, at koderne i alle tre tilfælde er asymptotisk dårlige. Endelig behandler vi Garcia og Stichtenoth's mest berømte tårn af funktionslegemer. Dette tårn vides at give anledning til gode følger af geometriske Goppakoder. Følger der er så gode, at de når Tsfasman-Vlăduţ-Zink-grænsen. Det er imidlertid endnu ikke lykkedes nogen at konstruere disse følger af koder hørende til tårnet i praksis. Vi foreslår

en metode til at angribe problemet vha. ordensområdeteori. Vi har dog ikke selv held med metoden.

Resume af del II

Del II indeholder et optryk af artiklen *Footprints or Generalized Bezout's Theorem* af Olav Geil og Tom Høholdt. Artiklen er antaget af *IEEE Transactions on Information Theory*, hvor den vil komme som en korrespondence. Artiklen er en naturlig fortsættelse af de tre nyere artikler II[2], II[3] og II[4] af Feng, Rao m.fl. I disse tre artikler beskriver forfatterne en metode til estimering af de generaliserede Hammingvægte af evalueringskodernes dualkoder. Som en vigtig del af metoden indgår en generalisering af Bezout's sætning. I artiklen, som er optrykt i del II, viser vi, hvorledes Feng, Rao m.fl.'s metode kan generaliseres, således at ikke blot estimater men derimod de faktiske værdier af de generaliserede Hammingvægte kan bestemmes. Som det vigtigste viser vi, at det er meget mere naturligt at benytte fodaftryksgrænsen fra Gröbnerbasis-teorien fremfor deres generalisering af Bezout's sætning, når de generaliserede Hammingvægte af evalueringskodernes dualkoder skal estimeres/bestemmes. Lad $\mathcal{C}$ være en vilkårlig k-dimensional kode med parititetstjekmatrix $H := [\boldsymbol{h_1}, \ldots, \boldsymbol{h_r}]^T$. Definer

$$[\boldsymbol{h_i}] := \{\boldsymbol{h_i} + \sum_{j=1}^{i-1} \alpha_j \boldsymbol{h_j} \,|\, \alpha_j \in \mathbb{F}_q\},$$

for $i = 1, \ldots, r$.

$$D_{\{[\boldsymbol{h_{i_1}}],\ldots,[\boldsymbol{h_{i_s}}]\}} := \max\big\{n - \mathrm{Supp}(\boldsymbol{h'_{i_1}}, \ldots, \boldsymbol{h'_{i_s}}) \,| \\ \boldsymbol{h'_{i_t}} \in [\boldsymbol{h_{i_t}}], t = 1, \ldots, s\big\}$$

for $1 \leq i_1 < \cdots < i_s \leq r$. Og

$$D_s := \max\Big\{D_{\{[\boldsymbol{h_{i_1}}],\ldots,[\boldsymbol{h_{i_s}}]\}} \,|\, 1 \leq i_1 < \cdots < i_s \leq r\Big\}$$

for $s = 1, \ldots, r$. Betegn med d_h den h'te generaliserede Hammingvægt af $\mathcal{C}$. Den vigtigste del af nedenstående sætning, nemlig $\Leftarrow$-delen af (i) er vist af Feng, Rao m.fl. Resten er nyt.

Sætning
Lad en kode C af længde n og med parititetstjekmatrix $H = [\boldsymbol{h_1}, \ldots, \boldsymbol{h_r}]^T$ (ikke nødvendigvis af fuld rang) være givet. For ethvert $d^* \leq r + h$, $h \leq k$, $d \leq n$ gælder følgende biimplikationer

(i) $d_h \geq d^* \Leftrightarrow D_{r-d^*+h+1} \leq d^* - 2$

(ii) $d_h \leq d^* \Leftrightarrow D_{r-d^*+h} \geq d^*$.

Specielt interessant er det tilfælde, hvor $\mathcal{C}$ er dualkoden til en evalueringskode, dvs, tilfældet hvor $\boldsymbol{h_i}$ er på formen $\boldsymbol{h_i} := (F_i(P_1), \ldots, F_i(P_n))$, $i = 1, \ldots, r$, hvor $P_j \in \mathbb{F}_q$, $j = 1, \ldots, n$. I dette tilfælde svarer estimeringen/beregningen af tallet D_s til en estimering/beregning af det maksimalt mulige antal punkter fra $\{P_1, \ldots, P_n\}$, som er fælles nulpunkter for s polynomier på formen

$$F_{i_1} + \sum_{j=1}^{i_1-1} \alpha_j^{(1)} F_j, \ldots, F_{i_s} + \sum_{j=1}^{i_s-1} \alpha_j^{(s)} F_j,$$

hvor $1 \leq i_1 < i_2 < \cdots < i_s \leq r$. Bemærk, at alle mulige valg af $i_1, \ldots, i_s$ skal betragtes, ligesom enhver mulig kombination af $\alpha_j^{(t)}$'erne skal betragtes for ethvert sådant valg. Med henblik på at kunne estimere det maksimale antal fælles nulpunkter når $i_1, \ldots, i_s$ fastholdes og $\alpha_j^{(t)}$'erne kan antage vilkårlige værdier, generaliserede Feng, Rao m.fl. Bezout's sætning. I artiklen, som er gengivet i del II, demonstrerer vi, at det er mere naturligt i stedet at benytte sig af fodaftryksgrænsen, når disse estimeringer skal foretages. Vi demonstrerer dette i to trin. I det første trin beskæftiger vi os med en række af Feng, Rao m.fl.'s sætninger. Sætninger som giver grænser for antallet af fælles nulpunkter mellem diverse polynomier. Vi giver nye og mere simple beviser og viser hvorledes fodaftryks-tekniken lægger op til generaliseringer af sætningerne. I det andet trin beskæftiger vi os med at estimerere de generaliserede Hammingvægte af forskellige koder, vha. fodaftryksgrænsen i kombination med den klassiske Bezout's sætning fremfor vha. den generaliserede Bezout's sætning. Feng, Rao m.fl. definerede en forbedret Klein-kode, og estimerede dennes minimumafstand. Vi ikke blot estimerer minimumsafstanden, men simpelthen finder de eksakte værdier af de generaliserede Hammingvægte. Feng, Rao m.fl. definerede også en forbedret Hermite-kode, for hvilken de estimerede minimumsafstanden. Vi estimerer alle de generaliserede Hammingvægte og konkluderer at ikke blot den første generaliserede Hammingvægt er forbedret. Feng, Rao m.fl. gav to eksempler på koder over det affine rum $\mathbb{F}_{2^m}$, som har store minimumsafstande.

Vi generaliserer deres konstruktion og estimerer minimumsafstanden af de nye koder. Endelig betragter vi koder defineret vha. Gröbnerbasis-teori. Lad $\prec$ være en monomial ordning på $\mathbb{F}_q[X_1, \ldots, X_m]$, $I \subseteq \mathbb{F}_q[X_1, \ldots, X_m]$ et primideal, og $\Delta(I)$ fodaftrykket af I mht. $\prec$. Vælg $F_1, \ldots, F_r$ som de r mindste elementer i $\Delta(I)$ mht. $\prec$. Og vælg $\{P_1, \ldots, P_n\} := \mathcal{V}_{\mathbb{F}_q}(I)$, dvs. som varieteten af I. De generaliserede Hammingvægte af evalueringskoderne, konstrueret ved at vælge $G := [\boldsymbol{h_1}, \ldots, \boldsymbol{h_r}]^T$ som generatormatrix, er estimeret af Shibuya m.fl. Vi præsenterer et resultat dualt til deres, idet vi estimerer de generaliserede Hammingvægte af koderne med paritetstjekmatrix lig $[\boldsymbol{h_1}, \ldots, \boldsymbol{h_r}]^T$.