Codes from order domains

Andersen, Henning Ejnar

Publication date:
2005

Document Version
Publisher's PDF, also known as Version of record

Link to publication from Aalborg University

Citation for published version (APA):
Andersen, H. E. (2005). *Codes from order domains*. Dept. of Matheamtical Science, Aalborg University.

Ph.D. Thesis

Codes from Order Domains

Koder baseret på ordensområder

Henning E. Andersen

July 2005

Department of Mathematical Sciences
Aalborg University, Denmark

Preface

This thesis is the result of my Ph.D. study at Department of Mathematical Sciences, Aalborg University, Denmark, conducted in the period from August 1st 2002 to July 31st 2005. The theme of this thesis is the construction of codes from order domains and development of bounds on their minimum distances.

The thesis is in two parts. In Part A the basic theory of order domains and Gröbner basis is introduced. Furthermore, Part A contains results from a study of Buchberger's algorithm and a case study of codes from the Suzuki curve constructed using order domains.

Part B contains reproductions of the submitted papers [2] and [1]. The paper [2] is the result of work done in cooperation with Associate Professor Olav Geil, Aalborg University, Denmark.

Each of the papers in Part B are self-contained and can be read independently of Part A. Thus the notation used in the included papers might differ slightly from the notation in Part A where the notation from [8] (modified to my personal likings) is used.

Part of the work was done during spring 2004 while visiting Associate Professor Marc P. C. Fossorier at Department of Electrical Engineering, University of Hawai'i at Manoa, Honolulu.

Acknowledgements

I wish to thank Associate Professor Marc P. C. Fossorier for making my visit at University of Hawai'i at Manoa, Honolulu, possible and for our helpful discussions. I thank Professor J. B. Nation, Department of Mathematics, University of Hawai'i at Manoa, Honolulu, for helpful discussions and for your time. My gratitude also goes to Nenad Miladinovic and the rest of the Ph.D students in POST 325. I learned so much from you. *Mahalo!*

I am deeply indebted to Associate Professor Olav Geil, Department of Mathematical Sciences, Aalborg University, Denmark. Thank you for helpful discussions, for doing cooperative work with me, for your patience and for believing in me. I am grateful to my advisor Associate Professor Christian Thommesen, Department of Mathematical Sciences, Aalborg University, Denmark, for helpful discussions, for sharing his knowledge with me and for his advise.

I would also like to express my gratitude to the following people:

Doris and Predrag Miocinovic and their friends in Hawai'i for all their help and for taking care of me while I was in Honolulu. You made my visit in Hawai'i a memorable experience and I wish we could see each other more often. A special thank you goes to Doris for all your help and support when my father passed away in April 2004 and for inviting me to your wedding in Sremski Karlovci, Serbia, in May 2005. I wish you and Predrag all the best!

Mogens Hinge for proof-reading this thesis and for being such a good friend.

My friends and family for putting up with me during my Ph.D. study.

And finally: Thank you Rose for your support, your love and understanding and for being there for me. *Akupendae!*

Aalborg, July 2005

Henning E. Andersen

Revised in December 2005. Minor errors, missing citations and some misspellings have been corrected.

Aalborg, December 2005

Henning E. Andersen

Summary

This thesis is in two parts. In Part A the basic theory of order domains and Gröbner bases is introduced. Furthermore, Part A contains results from a study of Buchberger's algorithm and a case study of codes from the Suzuki curve constructed using order domains.

Part B contains reproductions of the submitted papers [2] and [1]. The paper [2] is the result of work done in cooperation with Associate Professor Olav Geil, Aalborg University, Denmark.

Each of the papers in Part B are self-contained and can be read independently of Part A. Thus the notation used in the included papers differ slightly from the notation in Part A where the notation from [8] (modified to my personal likings) is used.

Summary of Part A

Chapter 2 gives a short introduction to the concept of an order function and an order domain as introduced by Høholdt, van Lint and Pellikaan in [21] and [20]. Furthermore, it contains a brief introduction to Gröbner basis theory and the construction of order domains using factor rings $\mathbb{F}_q[x_1, x_2, \ldots, x_m]/I$, where $I \subset \mathbb{F}_q[x_1, x_2, \ldots, x_m]$ is an ideal.

Given a well-order $(\Gamma, \prec)$ and a $\mathbb{F}_q$-algebra, denoted R, then an order function is a surjective map $\rho : R \to \Gamma$ that meet five criterions and a weight function is an order function that also meets a sixth criterion. An order domain is then a $\mathbb{F}_q$-algebra that has an order function and the triplet (R, ρ, Γ) is called an order structure. The important fact is that given an order structure (R, ρ, Γ) then the set $\{f_\gamma \mid \rho(f_\gamma) = \gamma\}_{\gamma \in \Gamma}$ constitutes a basis for R as a vector space over $\mathbb{F}_q$. Then using another surjective map (called a morphism), $\varphi : R \to \mathbb{F}_q^n$, it is possible to find a set $\Delta(R, \rho, \varphi) = \{\alpha(1), \alpha(2), \ldots, \alpha(n)\}$ such that the set $S = \{\varphi(f_{\alpha(1)}), \varphi(f_{\alpha(2)}), \ldots, \varphi(f_{\alpha(n)})\}$ spans $\mathbb{F}_q^n$. Codes described by means of their parity check matrix or generator matrix can then be defined by selecting a subset of S as the rows in the corresponding matrix. Furthermore, bounds on their minimum distance can be given as in [12, 20] and [2].

However, constructing order domains might not be simple but here Gröbner basis theory offers a solution. Given an ideal $I \subset \mathbb{F}_q[x_1, x_2, \ldots, x_m]$ then the factor ring $\mathbb{F}_q[x_1, x_2, \ldots, x_m]/I$ can be used as an order domain with a specific weight function if it meets the conditions given in Pellikaan's factor ring theorem from [33]. One of these conditions is that a Gröbner basis for I must consist of polynomials having two monomials of highest weight in their support.

Gröbner basis theory also offers the notion of a footprint, which, given an ideal $I \subset \mathbb{F}_q[x_1, x_2, \ldots, x_m]$, is defined to be the set of monomials in $\mathbb{F}_q[x_1, x_2, \ldots, x_m]$ that are not leading monomial of any polynomial $f \in I$. The footprint of an ideal I is very useful, since it offers an upper bound on the number of points in $\mathbb{F}_q^n$, where all polynomials in I are zero. This result is known as the footprint bound and allows us to give lower bounds on the minimum distance of a code, since a code word can be seen as a polynomial f that is a linear combination of monomials in the footprint of I.

One of the properties of a Gröbner basis for an ideal I is that it allows us to find the number of elements in the footprint of I, thus finding a Gröbner basis for an ideal is very useful. This can be done by using Buchberger's algorithm so Chapter 3 is concerned with the study of Buchberger's algorithm and the division algorithm involved. The study of these two algorithms is the foundation of many of the proofs given in this thesis.

Now, assume that we are given an ideal $I \in \mathbb{F}_q[x_1, x_2, \ldots, x_m]$ meeting the conditions in Pellikaan's factor ring theorem and having Gröbner basis $G = \{f_1, f_2, \ldots, f_s\}$ of the required form, i.e. $f_i = \boldsymbol{x}^{\boldsymbol{a}_i} + \eta_i \boldsymbol{x}^{\boldsymbol{b}_i} + f_i'(x_1, x_2, \ldots, x_m)$, for $i = 1, 2, \ldots, s$ and $\eta_i \in \mathbb{F}_q$, where the weight of $\boldsymbol{x}^{\boldsymbol{a}_i}$ is equal to the weight of $\boldsymbol{x}^{\boldsymbol{b}_i}$ which again is larger than the weighted degree of f_i'. Then we define the binomial part of G, denoted $\mathcal{B}(G)$, to be the set $\mathcal{B}(G) = \{b_1, b_2, \ldots, b_s\}$, where $b_i = \boldsymbol{x}^{\boldsymbol{a}_i} + \eta_i \boldsymbol{x}^{\boldsymbol{b}_i}$, for $i = 1, 2, \ldots, s$.

The key result in Chapter 3 is, given a code polynomial f with leading monomial $\boldsymbol{x}^{\boldsymbol{i}}$, then the footprint of the ideal $\langle f_1, f_2, \ldots, f_s, f\rangle$ is a subset of the footprint of the ideal $\langle b_1, b_2, \ldots, b_s, \boldsymbol{x}^{\boldsymbol{i}}\rangle$. This result is used in Chapter 4 to give a lower bound on the minimum distance of the evaluation codes defined in Chapter 4 and [4].

The bound given in Chapter 4 turns out to be equal to the bound given in [2], so in Chapter 5 we try a different approach to bounding the minimum distance of codes as defined in Chapter 4 but restricting ourselves to a special class of order domains of the form in Pellikaan's factor ring theorem.

The structure of the polynomials in the Gröbner basis for such an ideal allows us to find an upper bound on the size of the footprint of $\langle b_1, b_2, \ldots, b_s, \boldsymbol{x}^{\boldsymbol{i}}\rangle$ without doing any iterations in Buchberger's algorithm or any polynomial divisions but merely by defining a function on the leading monomial of a code polynomial f. This result is found by only considering some of the S-polynomials constructed when running Buchberger's algorithm and omit the rest. Unfortunately, as simple and promising as it may seem, we arrive at a well-known bound which is also easily calculated. Thus this approach yields nothing new.

In Chapter 6 we study the use of Buchberger's algorithm on a class of ideals called toric ideals. It is shown that if $\langle b_1, b_2, \ldots, b_s\rangle$ is a toric ideal, then the approach taken in Chapter 5 is actually not bad, because the S-polynomials omitted in the method developed in Chapter 5 adds nothing new when running Buchberger's algorithm. On the other hand: Since the bound given in Chapter 4 and [2] is better than the one found in Chapter 5, we will be do better by using that instead.

Finally, Chapter 7 contains a case study based on [6] where Chen and Duursma consider codes of length 64 based on the Suzuki curve over a finite field $\mathbb{F}_8$. In Chapter 7 we use the bounds from [2, 20, 12] and Chapter 4 to estimate the parameters of codes constructed from an order domain of the form in Pellikaan's factor ring theorem and where the ideal I is constructed to capture the relation between the four rational functions involved in [6]. The resulting parameters are in a few cases better than the ones found in [6]. Chapter 7

also contains an example of codes of length 1024 based on the Suzuki curve over a finite field $\mathbb{F}_{32}$ which was given as an example in [19].

Summary of Part B

Chapter 8 is a reproduction of the paper [2] which contains results found in cooperation with Associate Professor Olav Geil, Aalborg University, and Chapter 9 is a reproduction of the paper [1], which recently has been accepted for publishing in *Finite Fields and Their Applications*. Both papers can be read independently of Part A (and of each other), thus an extended abstract of each chapter is given separately.

Chapter 8

In [12] Feng and Rao showed how to estimate the minimum distance of a large class of algebraically defined codes by considering certain relations between the rows in the corresponding parity check matrices. This result is known today as the Feng-Rao bound. Using this bound Feng and Rao were able to improve a large class of well-known codes by leaving out certain rows in the corresponding parity check matrices.

In [30] and [31] Miura observed that the results by Feng and Rao can be obtained by using only linear algebra. In particular one can view the Feng-Rao bound as a bound on the minimum distance of any linear code (with known parity check matrix). Furthermore it was shown in [31] how to improve the Feng-Rao bound slightly in this general set-up.

What is obviously missing is a Feng-Rao type bound on the minimum distance of codes which are not defined on the basis of parity check matrices but are defined on the basis of generator matrices. This question was treated by Shibuya and Sakaniwa in [34] where they use the theory of generalized Hamming weights to translate the Feng-Rao bound for the codes defined by means of parity check matrices into a bound for the codes defined by means of generator matrices. The bound derived in this way is of a much more complicated form than the Feng-Rao bound and the problem of improving the codes by using the information from the bound is not so easy. Furthermore, the proof of the bound by Shibuya and Sakaniwa is rather complicated.

In this paper we derive a new and very simple bound on the minimum distance of codes defined by means of their generator matrices. Our bound is of a form very similar to the Feng-Rao bound and in particular from our bound it is obvious how to improve the codes. Furthermore our bound not only deals with the minimum distance but actually gives lower bounds on any generalized Hamming weights of the considered codes. We show how to deal with the new bounds and the new code construction from an order domain theoretical point of view. We give some very concrete results on how to deal with the code construction in the case of affine variety codes[1] defined from order domains and we derive some results concerning the connection between the Feng-Rao improved codes and the new improved codes. Also we show how to understand our new bound and code construction from a Gröbner basis theoretical point of view. For the case of one-point geometric Goppa codes our bound can easily be shown to be an improvement of the usual

[1] So named in [13].

bound from algebraic geometry and in many cases we are able to improve substantial on the one-point geometric Goppa code construction. In this way we improve the results in [34] where it was shown that their bound is at least as good as the usual bound from algebraic geometry for the case of one-point geometric Goppa codes from C_{ab} curves. Our new construction and our new bounds can be viewed as a generalization of the recent Gröbner basis theoretical descriptions in [17] and [16] concerning Reed-Muller codes, hyperbolic codes[2] and codes from norm-trace curves. For these codes our bounds are tight.

Chapter 9

Constructing codes from existing ones is not a new idea and over the years several ways of doing so has been developed. One such construction is by means of puncturing. Puncturing an (n, M, d) code $t, (t < d)$, times yields an $(n - t, M, \geqslant d - t)$ code where the parameter $d - t$ is a lower bound on the minimum distance [24, p. 28].

However, it is not clear how to select which t coordinates to erase in an existing code to get the best result or whether an optimal strategy for making such a selection exists for a given code and a given value t. The general bound given above is usually not tight which will be shown by an example.

Here we consider codes from Norm-Trace curves[3] which were studied in detail in [16]. Here we use nothing but order domains and Gröbner basis theory for code construction and the methods developed in [20, 2, 21, 11, 12] for estimating the minimum distances of the codes.

By [18] every finitely generated order domain can be represented as a factor ring $\mathbb{F}_q[x_1, x_2, \ldots, x_m]/I$, where $I \subset \mathbb{F}_q[x_1, x_2, \ldots, x_m]$ is an ideal of a special form. Using such an order domain and the usual evaluation map $\varphi : \mathbb{F}_q[x_1, x_2, \ldots, x_m]/I \to \mathbb{F}_q^n$ we define $\tilde{E}$ codes as a linear subspace of $\mathbb{F}_q^n$ spanned by the image of selected elements from $\mathbb{F}_q[x_1, x_2, \ldots, x_m]/I$ under φ and $\tilde{C}$ codes as the dual of such an image under φ (These are the improved $\tilde{E}$ codes from [2] and the improved $\tilde{C}$ codes from [20, 12]).

In this setting puncturing a code can be done by reducing the dimension of the corresponding factor ring $\mathbb{F}_q[x_1, x_2, \ldots, x_m]/I$ as a vector space over $\mathbb{F}_q$ by adding extra polynomials to the basis of the defining ideal I to define an new ideal J. This corresponds to redefining the evaluation map by leaving out a number of points from the variety $\mathbb{V}(I)$, since $I \subset J$ has the consequence that $\mathbb{V}(J) \subset \mathbb{V}(I)$ [8].

Leaving out t points from the variety $\mathbb{V}(I)$ can be done in several ways by adding different sets of polynomials to the basis of the ideal I to form the ideal J such that $\#\mathbb{V}(J) = \#\mathbb{V}(I) - t$. The evaluation map φ is still a morphism so the methods developed in [20, 2, 12] enables us to estimate the minimum distances of the codes constructed by using the variety $\mathbb{V}(J)$. This in turn allows us to choose the set of polynomials added to the basis of I (i.e. choose the ideal J) which has the smallest cost in terms of loss in minimum distance for a given integer t and a given code rate.

[2] Also called Massey-Costello-Justesen codes (see [22] and [25].

[3] Norm-Trace curves are a special case of the C_{ab} curves classified by Miura and Kamiya in [32].

The main result in this paper is that for any positive integer $t < d$ it is possible to construct a set of polynomials $\{g_1, g_2, \ldots, g_s\}$ such that a code of length $n - t$ is obtained by using the ideal $J = I + \langle g_1, g_2, \ldots, g_s \rangle$ and the affine variety $\mathbb{V}(J)$. Furthermore, the proof given here is constructive and examples of such constructions are included.

Danish summary (Dansk resumé)

Denne afhandling er i to dele. I Del A introduceres den grundlæggende teori om ordensområder og Gröbner baser. Ydermere indeholder Del A resultater fremkommet ved studiet af Buchbergers algoritme og et studie af koder baseret på Suzuki-kurven, men hvor ordensområder anvendes i stedet for den sædvanlige tilgang.

Del B indeholder reproduktioner af de to artikler [2] og [1], der begge er indsendt til videnskabelige tidsskrifter, og hvoraf artiklen [2] er resultatet af et samarbejde med Lektor Olav Geil, Aalborg Universitet.

Begge de to artikler i Del B er selvstændige artikler, der kan læses uafhængigt af Del A. Derfor kan notationen i de inkluderede artikler afvige en smule fra notationen anvendt i Del A, hvor notationen fra [8] (tilpasset min personlige smag) hovedsageligt bliver anvendt.

Resumé af Del A

Kapitel 2 giver en kort introduktion til ordensfunktioner og ordensområder som blev indført af Høholdt, van Lint og Pellikaan i [21] og [20]. Ydermere indeholder kapitlet en kort introduktion til Gröbnerbasisteori og konstruktionen af ordensområder ved hjælp af faktorringe $\mathbb{F}_q[x_1, x_2, \ldots, x_m]/I$, hvor $I \subset \mathbb{F}_q[x_1, x_2, \ldots, x_m]$ er et ideal.

Givet en såkaldt vel-ordning $(\Gamma, \prec)$ og en $\mathbb{F}_q$-algebra, betegnet med R, så er en ordensfunktion en surjektiv afbildning $\rho : R \rightarrow \Gamma$, der opfylder fem kriterier, og en vægtfunktion er en ordensfunktion, der opfylder et sjette kriterium. Et ordensområde er da en $\mathbb{F}_q$-algebra, der har en ordensfunktion og triplen (R, ρ, Γ) kaldes en ordensstruktur. Et vigtigt faktum er at givet en ordensstruktur, så er mængden $\{f_\gamma \mid \rho(f_\gamma) = \gamma\}_{\gamma \in \Gamma}$ en basis for R som vektorrum over $\mathbb{F}_q$. Ved at anvende endnu en surjektiv afbildning (kaldet en morfi), $\varphi : R \rightarrow \mathbb{F}_q^n$, så er det muligt at finde en mængde $\Delta(R, \rho, \varphi) = \{\alpha(1), \alpha(2), \ldots, \alpha(n)\}$ således at mængden $S = \{\varphi(f_{\alpha(1)}), \varphi(f_{\alpha(2)}), \ldots, \varphi(f_{\alpha(n)})\}$ udspænder hele $\mathbb{F}_q^n$. Fejlkorrigerende koder beskrevet ved hjælp af enten deres paritetscheckmatrice eller deres generatormatrice kan nu defineres ved at vælge en delmængde af S som rækkerne i den tilhørende matrice. Desuden kan grænser for deres minimumsafstand gives som vist i [12, 20] og [2].

At konstruere ordensområder er ikke nødvendigvis simpelt, men her er Gröbnerbasisteori en god hjælp. Givet et ideal $I \subset \mathbb{F}_q[x_1, x_2, \ldots, x_m]$, så kan faktorringen $\mathbb{F}_q[x_1, x_2, \ldots, x_m]/I$ anvendes som ordensområde med en specifik vægtfunktion, hvis $\mathbb{F}_q[x_1, x_2, \ldots, x_m]/I$ opfylder betingelserne i Pellikaans faktorringssætning fra [33]. En af disse betingelser er, at I skal have en Gröbnerbasis, der består af polynomier med præcist to monomier af højeste vægt i supporten.

Fra Gröbnerbasisteorien har vi også begrebet “fodaftryk”, der, givet et ideal $I \subset \mathbb{F}_q[x_1, x_2, \ldots, x_m]$, er defineret som mængden af monomier i $\mathbb{F}_q[x_1, x_2, \ldots, x_m]$, der ikke er ledende monomium i noget polynomium $f \in I$. Fodaftrykket af et ideal I er meget nyttigt, idet det antallet af elementer i fodaftrykket giver en øvre grænse for antallet af punkter i $\mathbb{F}_q^n$, hvor alle polynomier i I er nul. Dette resultat er kendt som “fodaftryksgrænsen” og tillader os at finde nedre grænser for minimumsafstanden i en fejlkorrigerende kode, idet et kodeord kan ses som et polynomium f skrevet som en linearkombination af monomier i fodaftrykket af I.

En af egenskaberne ved en Gröbnerbasis for et ideal I er, at den tillader os at finde antallet af elementer i fodaftrykket af I, så det er nyttigt at kunne finde en Gröbnerbasis for et ideal. Dette kan gøres ved hjælp af Buchbergers algoritme, så Kapitel 3 omhandler et studium af Buchbergers algoritme og divisionsalgoritmen, der er en del heraf. Studiet af disse to algoritmer er grundlaget for mange af beviserne i denne afhandling.

Antag nu, at vi har et givet ideal $I \in \mathbb{F}_q[x_1, x_2, \ldots, x_m]$, der opfylder betingelserne i Pellikaans faktorringssætning, med Gröbnerbasis $G = \{f_1, f_2, \ldots, f_s\}$ på den krævede form, dvs. $f_i = \boldsymbol{x}^{\boldsymbol{a}_i} + \eta_i \boldsymbol{x}^{\boldsymbol{b}_i} + f_i'(x_1, x_2, \ldots, x_m)$, for $i = 1, 2, \ldots, s$ og $\eta_i \in \mathbb{F}_q$, hvor vægten af $\boldsymbol{x}^{\boldsymbol{a}_i}$ er den samme som vægten af $\boldsymbol{x}^{\boldsymbol{b}_i}$, der igen er større end den vægtede grad af f_i'. Da definerer vi den binomielle del af G, skrevet $\mathcal{B}(G)$, til at være mængden $\mathcal{B}(G) = \{b_1, b_2, \ldots, b_s\}$, hvor $b_i = \boldsymbol{x}^{\boldsymbol{a}_i} + \eta_i \boldsymbol{x}^{\boldsymbol{b}_i}$, for $i = 1, 2, \ldots, s$.

Det vigtigste resultat i Kapitel 3 er, at givet et kodepolynomium f med ledende monomium $\boldsymbol{x}^{\boldsymbol{i}}$, så er fodaftrykket af idealet $\langle f_1, f_2, \ldots, f_s, f \rangle$ indeholdt i fodaftrykket af idealet $\langle b_1, b_2, \ldots, b_s, \boldsymbol{x}^{\boldsymbol{i}} \rangle$. Dette resultat bliver i Kapitel 4 anvendt til at give en nedre grænse for minimumsafstanden i evalueringskoderne defineret i Kapitel 4 og [4].

Grænsen fundet i Kapitel 4 viser sig at være den samme som grænsen fundet i [2], så i Kapitel 5 forsøges en anden tilgang til at give en grænse for minimumsafstanden af koderne defineret i Kapitel 4, men i Kapitel 5 begrænser vi os til en speciel klasse of ordensområder på formen givet i Pellikaans faktorringssætning.

Strukturen af polynomierne i Gröbnerbasen for et sådant ideal tillader os at finde en øvre grænse for antallet af elementer i fodaftrykket af idealet $\langle b_1, b_2, \ldots, b_s, \boldsymbol{x}^{\boldsymbol{i}} \rangle$, uden at skulle køre Buchbergers algoritme eller foretage nogen polynomiumsdivisioner, men ved blot at definere en funktion på det ledende monomium i et kodepolynomium f. Dette resultat findes ved kun at betragte en passende delmængde af de S-polynomier, der vil blive konstrueret ved anvendelsen af Buchbergers algoritme, og således udelade resten. Uanset hvor simpelt og lovende denne tilgang måtte lyde, så ender vi med at finde en velkendt grænse, der ligeledes er nem at beregne. Tilgangen anvendt i Kapitel 5 giver os således intet nyt.

I Kapitel 6 studeres anvendelsen af Buchbergers algoritme på en klasse af idealer kalder “toriske idealer”. Det vises, at hvis $\langle b_1, b_2, \ldots, b_s \rangle$ er et torisk ideal, så er tilgangen i Kapitel 5 ikke dårlig, idet de udeladte S-polynomier i metoden udviklet i Kapitel 5 ikke giver anledning til yderligere tilføjelser ved anvendelse af Buchbergers algoritme. På den anden hånd: Da grænsen givet i Kapitel 4 og [2] er bedre end den fundet i Kapitel 5, så er det bedre at anvende den i stedet for.

Endelig indeholder Kapitel 7 et studium baseret på [6] hvor Chen og Duursma konstruerer koder af længde 64 ved hjælp af Suzuki-kurven over et endeligt legeme $\mathbb{F}_8$. I Kapitel 7 anvendes grænserne fra [2, 20, 12] og Kapitel 4 til at estimere parametrene for koder baseret på et ordensområde på formen i Pellikaans faktorringssætning og hvor idealet I er konstrueret til at indfange relationerne mellem de fire implicerede rationelle funktioner fra [6]. De fundre parametre er i enkelte tilfælde bedre end dem, der blev fundet i [6]. Kapitel 7 indeholder også et eksempel på koder baseret på Suzuki-kurven over et endeligt legeme $\mathbb{F}_{32}$, der blev anvendt som eksempel i [19].

Resumé af Del B

Kapitel 8 er en reproduktion af artiklen [2], der indeholder resultater opnået i samarbejde med Lektor Olav Geil, Aalborg Universitet, og Kapitel 9 er en reproduktion af artiklen [1], der for nylig er blevet accepteret til publikation i tidsskriftet *Finite Fields and Their Applications.* Begge artikler kan læses uafhængigt af Del A (og uafhængigt af hinanden), hvorfor der gives separate resuméer af de to kapitler nedenfor.

Kapitel 8

I [12] viste Feng og Rao hvordan minimumsafstanden for en stor klasse af algebraisk definerede koder kan estimeres ved at betragte bestemte relationer mellem rækkerne i de tilhørende paritetscheckmatricer. Dette resultat kendes idag som Feng-Rao-grænsen. Ved hjælp af denne grænse lykkedes det Feng og Rao at forbedre en stor klasse af velkendte koder ved at udelade visse rækker i de tilhørende paritetscheckmatricer.

I [30] og [31] observerede Miura at resultaterne opnået af Feng og Rao kan vises udelukkende ved hjælp af lineær algebra. Specielt så kan Feng-Rao-grænsen ses som en grænse for minimumsafstanden af enhver lineær kode (med kendt paritetscheckmatrice). Ydermer blev det i [31] vist, hvordan Feng-Rao-grænsen kan forbedres lidt i denne generelle opsætning.

Det, der tydeligvis mangler i ovenstående beskrivelse, er en grænse for minimumsafstanden af samme type som Feng-Rao-grænsen for koder, der ikke er definerede ved hjælp af paritetscheckmatricer men ved hjælp af generatormatricer. Dette spørgsmål blev behandlet af Shibuya og Sakaniwa i [34], hvor de bruger teorien og generaliserede Hammingvægte til at oversætte Feng-Rao-grænsen for koder defineret ved hjælp af paritetscheckmatricer til en grænse for koder defineret ved hjælp af generatormatricer. Den grænse, de på den måde udleder, er meget mere kompliceret end Feng-Rao-grænsen og problemet med at anvende denne information til forbedring af koderne er ikke nemt. Ydermer er beviset for grænsen udledt af Shibuya og Sakaniwa forholdsvis kompliceret.

I denne artikel udleder vi en ny og meget simpel grænse for minimumsafstanden af koder defineret ved hjælp af deres generatormatricer. Vores grænse er på en form, der meget ligner Feng-Rao-grænsen, og specielt er det indlysende, hvordan koderne kan forbedres. Ydermere så giver vores grænse ikke bare en grænse for minimumsafstanden men faktisk også for en hvilken som helst genereliseret Hammingvægt af de betragtede koder. Vi viser, hvordan den nye grænse og konstruktionen af koder håndteres ud fra et ordensområde-teoretisk synspunkt. Vi viser nogle meget konkrete resultater vedrørende kodekonstruktionen i tilfældet med affine varietets koder[4] baseret på ordensområder og

[4] Navngivet således i [13].

vi udleder nogle resultater vedrørende forbindelsen mellem koder forbedret ved hjælp af Feng-Rao-grænsen og de nye forbedrede koder. Desuden viser vi, hvordan vores nye grænse og nye kodekonstruktion kan forstås fra et Gröbnerbasisteoretisk synspunkt. I tilfældet med et-punkts geometriske Goppa-koder kan det nemt vises, at vores grænse er en forbedring i forhold til den sædvanlige grænse fra algebraisk geometry og i flere tilfælde er vi i stand til at forbedre dramatisk på konstruktionen af et-punkts geometriske Goppa-koder. På denne måde forbedrer vi resultaterne i [34], hvor det blev vist at deres grænse er mindst lige så god som den sædvanlige grænse fra algebraisk geometri i tilfældet med et-punkts geometriske Goppa-koder fra C_{ab}-kurver. Vores nye konstruktion og nye grænse kan ses som en generelisering af den forholdsvis nye Gröbnerbasisteoretiske beskrivelse i [17] og [16] vedrørende Reed-Muller koder, hyperbolske koder[5] og koder fra Norm-Trace kurver. For disse koder angiver grænsen de virkelige minimumsafstande.

Kapitel 9

Konstuktion af nye koder ud fra eksisterende er ikke nogen ny idé og gennem årene er adskillige metoder hertil blevet udviklet. Én sådan metode kaldes "punktering". Ved at punktere en (n, M, d)-kode t gange, hvor $t < d$, så fåes en $(n - t, M, \geqslant d - t)$-kode, hvor parameteren $d - t$ er en nedre grænse for minimumsafstanden [24, p. 28].

Men det er ikke umiddelbart klart hvilket t koordinater, der skal slettes i en eksisterende kode for at opnå det bedste resultat, eller hvorvidt en optimal strategi for udvælgelsen af de t koordinater for en given kode og en given værdi t findes. Den sædvanlige grænse er som regel ikke god, hvilket vil blive vist ved hjælp af et eksempel.

Her betragtes koder baseret på Norm-Trace-kurver[6], der blev studeret i detalje i [16]. Her anvender vi udelukkende ordensområder og Gröbnerbasisteori til konstruktion af koder og metoderne udviklet i [20, 2, 21, 11, 12] til vurdering af minimumsafstanden.

Ifølge [18] kan ethvert endeligt genereret ordensområde repræsenteres som en faktorring $\mathbb{F}_q[x_1, x_2, \ldots, x_m]/I$, hvor $I \subset \mathbb{F}_q[x_1, x_2, \ldots, x_m]$ er et ideal på en speciel form. Ved hjælp af et sådant ordensområde og den sædvanlige evalueringsafbildning $\varphi : \mathbb{F}_q[x_1, x_2, \ldots, x_m]/I \to \mathbb{F}_q^n$ defineres $\tilde{E}$-koder som et lineært underrum af $\mathbb{F}_q^n$ udspændt af billedet under φ af udvalgte elementer i $\mathbb{F}_q[x_1, x_2, \ldots, x_m]/I$, og $\tilde{C}$-koder defineres som nul-rummet af et sådant billede under φ (Dette er de forbedrede $\tilde{E}$-koder fra [2] og de forbedrede $\tilde{C}$-koder fra [20, 12]).

I denne opsætning kan punkteringen af en kode udføres ved at reducere dimensionen af den tilsvarende faktorring $\mathbb{F}_q[x_1, x_2, \ldots, x_m]/I$ som vektorrum over $\mathbb{F}_q$, ved at tilføje ekstra polynomier til basen for idealet I og derved definere et nyt ideal J. Dette svarer til en redefinition af evalueringsafbildningen ved at udelade et antal punkter fra varieteten $\mathbb{V}(I)$, idet $I \subset J$ medfører at $\mathbb{V}(J) \subset \mathbb{V}(I)$ [8].

Udeladelse af t punkter fra varieteten $\mathbb{V}(I)$ kan gøres på mange forskellige måder ved at tilføje forskellige mængder af polynomier til basen for idealet I og derved konstruere idealet J således at $\#\mathbb{V}(J) = \#\mathbb{V}(I) - t$. Evalueringsafbildningen φ er stadigvæk en morfi, så metoderne udviklet i [20, 2, 12] finder stadigvæk anvendelse ved vurdering af

[5] Også kaldet Massey-Costello-Justesen koder (se [22] og [25]).

[6] Norm-Trace-kurverne er et specialtilfælde af C_{ab}-kurverne klassificeret af Miura og Kamiya i [32].

minimumsafstanden i de koder, der konstrueres ved hjælp af varieteten $\mathbb{V}(J)$. Dette tillader os at vælge den mængde polynomier, der tilføjes til basen for I (dvs. vælge idealet J), således at tabet i minimumsafstand er mindst muligt for en given værdi t og en given kodehastighed.

Hovedresultatet i denne artikel er, at for ethvert positivt heltal $t < d$ er det muligt at konstruere en mængde polynomier $\{g_1, g_2, \ldots, g_s\}$ således at en kode med længde $n - t$ opnåes ved at anvende idealet $J = I + \langle g_1, g_2, \ldots, g_s \rangle$ og varieteten $\mathbb{V}(J)$. Ydermere er beviset herfor konstruktivt og eksempler på konstruktioner er indkluderet.

Contents

Part A.

Codes from order domains

1. Introduction

1.1. A brief survey of order domains

The notion of an order domain was introduced in [20, 21] to make understanding of a large class of algebraic geometry codes easier and to give the code construction presented in [11, 12] a simpler foundation. Readers interested in the connection between the theory of order domains and the theory of algebraic geometry are recommended to read [20, 33].

Some of the results in [20, 21, 33] were found independently by Miura and published in Japanese in [29, 31, 30]. A proof in English of some of these results can be found in [26] and the connection to the work in [20, 21, 33] is studied in [27]. Since then order domains have been studied and used extensively in for instance [33, 18, 16, 15].

1.2. Codes from order domains

The order domains considered here are factor rings of the form $\mathbb{F}_q[x_1, x_2, \ldots, x_m]/I$, where $I \subset \mathbb{F}_q[x_1, x_2, \ldots, x_m]$ is an ideal, as described in Pellikaan's factor ring theorem [33, Thm. 5.11]. By [18] every finitely generated order domain (with weights embedded in $\mathbb{N}_0^r$) can be represented as a factor ring $\mathbb{F}_q[x_1, x_2, \ldots, x_m]/I$ of this form, where $I \subset \mathbb{F}_q[x_1, x_2, \ldots, x_m]$ is an ideal. In Part A of this thesis we only consider weights in $\mathbb{N}_0$ but an example using weights in $\mathbb{N}_0^2$ is given in Example 8.39.

Using such an order domain and an evaluation map $\varphi : \mathbb{F}_q[x_1, x_2, \ldots, x_m]/I \to \mathbb{F}_q^n$ then the $\tilde{E}$ codes are defined as a linear subspace of $\mathbb{F}_q^n$ spanned by the image of selected elements from $\mathbb{F}_q[x_1, x_2, \ldots, x_m]/I$ under φ and the $\tilde{C}$ codes as the dual of such an image under φ . These codes are the improved $\tilde{E}$ codes from [2] and the improved $\tilde{C}$ codes from [20, 12]. Only these improved codes will be considered throughout this thesis.

Also, using [13, Pro. 1] every $\mathbb{F}_q$-linear code may be represented as what the authors call affine variety codes, i.e. codes constructed from factor rings $\mathbb{F}_q[x_1, x_2, \ldots, x_m]/I$ using an evaluation map φ. This fact makes the study of factor rings interesting and in particular factor rings of the form in [33, Thm. 5.11] (finitely generated order domains) which can be used to describe a large class of $\mathbb{F}_q$-linear codes.

1.3. Outline of this thesis

This thesis is in two parts. In Part A of the thesis an introduction to order domains and Gröbner basis theory is given. Furthermore, some of the results from [4] leading to the more general result in [2] are stated and proven. This part also includes results on finding a Gröbner basis for toric ideals, results concerning a special case of a factor ring as in [33, Thm. 5.11] and a pure Gröbner basis theoretical approach to a case study of codes from Suzuki curves as seen in [6] and [19].

Part A is organized as follows: In Chapter 2 a short presentation of order domains and Gröbner basis theory is given, Chapter 3 contains details about using Buchberger's algorithm and the division algorithm, Chapter 4 contains the code definition and the lower bound on the minimum distance from [2] and [4] but as opposed to the proof in [2], only Gröbner basis theory is used in the proofs in Chapter 4. Chapter 5 holds an attempt to improve on the bound given in Chapter 4 and and Chapter 6 holds results on toric ideals. Finally, in Chapter 7 a case study of codes from Suzuki curves in the two cases considered in [6] and [19] is given.

Part B of this thesis contains the reproduction of the two submitted papers [1] and [2] which both are self-contained and can be read independently of Part A. The paper [1] has recently been accepted for publishing in *Finite Fields and Their Applications*.

2. Order domains and Gröbner basis theory

This chapter contains a short introduction to order domains in Section 2.1 and short introduction to Gröbner basis theory and the construction of order domains in Section 2.2.

2.1. Order domains and codes

The presentation of order domains given here is based on [2, 18]

Definition 2.1 *Let $\mathbb{F}$ be a field. Then an $\mathbb{F}$-algebra is a commutative ring with unity that contains $\mathbb{F}$ as a unitary subring.*

Definition 2.2 *Given a set Γ and a total ordering $\prec$ on Γ, then $(\Gamma, \prec)$ is called a well-order if every non-empty subset of Γ has a smallest element with respect to $\prec$.*

Given a well-order $(\Gamma, \prec)$, add an element $-\infty$ to Γ such that $\Gamma_{-\infty} = \Gamma \cup \{-\infty\}$ and extend the ordering $\prec$ with the rule $-\infty \prec \gamma$, for all $\gamma \in \Gamma$. Then $(\Gamma_{-\infty}, \prec)$ is a well-order.

Example 2.3 Let $\mathbb{N}_0$ denote the non-negative integers and let $\Gamma \subset \mathbb{N}_0$. If we add an element $-\infty$ to Γ such that $\Gamma_{-\infty} = \Gamma \cup \{-\infty\}$ and extend the ordinary ordering $<$ on elements in $\mathbb{N}_0$ with the rule $-\infty < n$, for all $n \in \mathbb{N}_0$, then $(\Gamma_{-\infty}, <)$ is a well-order. △

Definition 2.4 *Let $(\Gamma_{-\infty}, \prec)$ be a well-order, let $\mathbb{F}$ be a field and let R be a $\mathbb{F}$-algebra. A surjective map $\rho : R \rightarrow \Gamma_{-\infty}$ that satisfies the following five conditions for all $f, g, h \in R$ is called an order function on R.*

1. *$\rho(f) = -\infty$ if and only if $f = 0$.*
2. *$\rho(af) = \rho(f)$ for all non-zero $a \in \mathbb{F}$.*
3. *$\rho(f + g) \preceq max\{\rho(f), \rho(g)\}$ and equality holds when $\rho(f) \neq \rho(g)$.*
4. *If $\rho(f) \prec \rho(g)$ and $h \neq 0$, then $\rho(fh) \prec \rho(gh)$.*
5. *If f and g are non-zero and $\rho(f) = \rho(g)$, then there exists a non-zero $\alpha \in \mathbb{F}$ such that $\rho(f - \alpha g) \prec \rho(g)$.*

For the rest of Part A we will only consider well-orders of the form in Example 2.3[1], i.e. $\Gamma \subset \mathbb{N}_0$.

Given a well-order $(\Gamma_{-\infty}, <)$, where $\Gamma \subseteq \mathbb{N}_0$, consider the following definition.

Definition 2.5 *Let $(\Gamma_{-\infty}, <)$ be a well-order, let $\mathbb{F}$ be a field and let R be an $\mathbb{F}$-algebra. A weight function $\rho : R \to \Gamma_{-\infty}$ is an order function ρ on R that also satisfy the condition*

6. $\rho(fg) = \rho(f) + \rho(g)$

where $+$ is the ordinary addition on $\mathbb{N}_0$ extended with the rule that $-\infty + a = a + (-\infty) = -\infty + (-\infty) = -\infty$ for all $a \in \Gamma_{-\infty}$.

It is now possible to define an order structure and an order domain.

Definition 2.6 *Let $\mathbb{F}$ be a field, let R be an $\mathbb{F}$-algebra, ρ an order function and Γ a well-order. Then (R, ρ, Γ) is called an order structure and R is called an order domain (over $\mathbb{F}$).*

The order function being surjective ensures the existence of sets of the form $\{f_\gamma \mid \rho(f_\gamma) = \gamma\}_{\gamma \in \Gamma}$ with the following property from [18, Def. 3.1 & Pro. 3.2].

Theorem 2.7 *Let $\mathbb{F}$ be a field. Given an order structure (R, ρ, Γ) then any set $\mathcal{B} = \{f_\gamma \mid \rho(f_\gamma) = \gamma\}_{\gamma \in \Gamma}$ constitutes a basis for R as a vector space over $\mathbb{F}$. For any $f = c_{\gamma_1} f_{\gamma_1} + \cdots + c_{\gamma_d} f_{\gamma_d}$ with $c_{\gamma_1}, \ldots, c_{\gamma_d} \in \mathbb{F} \setminus \{0\}$, $\rho(f) = \max_{\prec}\{\gamma_1, \ldots, \gamma_d\}$ holds. In particular $\{f_\lambda \in \mathcal{B} \mid \lambda \preceq \gamma\}$ constitutes a basis for $R_\gamma = \{f \in R \mid \rho(f) \preceq \gamma\}$ as a vector space over $\mathbb{F}$.*

Let $\mathbb{F}_q$ denote a finite field with q elements and consider the following definition.

Definition 2.8 *Let R be an $\mathbb{F}_q$-algebra. A map $\varphi : R \to \mathbb{F}_q^n$ is called a morphism of $\mathbb{F}_q$-algebras if φ is $\mathbb{F}_q$-linear and $\varphi(fg) = \varphi(f) * \varphi(g)$ for all $f, g \in R$, where $*$ denotes component-wise multiplication.*

From now on we will only consider order domains R over finite fields $\mathbb{F}_q$ and surjective morphisms φ.

Definition 2.9 *Given an order structure (R, ρ, Γ) and a surjective morphism φ, let $\alpha(1)$ be equal to the smallest element of Γ. For $i = 2, 3, \ldots, n$ define recursively $\alpha(i)$ to be the smallest element in Γ greater than $\alpha(1), \alpha(2), \ldots, \alpha(i-1)$ and satisfying $\varphi(R_\gamma) \subsetneq \varphi(R_{\alpha(i)})$, for all $\gamma < \alpha(i)$. Write $\Delta(R, \rho, \varphi) = \{\alpha(1), \alpha(2), \ldots, \alpha(n)\}$.*

[1] More general well-orders can be found in [18]

Note, that if $\Gamma \subset \mathbb{N}_0$ and ρ in Definition 2.9 is a weight function (See Definition 2.5), then $\alpha(1)$ in Definition 2.9 is equal to $0 \in \mathbb{N}_0$. From Definition 2.9 we also see that the set $B = \{\varphi(f_{\alpha(1)}), \varphi(f_{\alpha(2)}), \ldots, \varphi(f_{\alpha(n)})\}$ constitutes a basis for $\mathbb{F}_q^n$ as a vector space over $\mathbb{F}_q$.

Definition 2.10 *For $\alpha(i) \in \Delta(R, \rho, \varphi)$ define*

$$N(\alpha(i)) = \{(\beta_1, \beta_2) \in (\Delta(R, \rho, \varphi))^2 \mid \rho(f_{\beta_1} f_{\beta_2}) = \alpha(i)\}$$

and define $\mu(\alpha(i)) = \#N(\alpha(i))$.
Furthermore, for $\alpha(j) \in \Delta(R, \rho, \varphi)$ define

$$M(\alpha(j)) = \{\gamma \in \Delta(R, \rho, \varphi) \mid \exists \beta \in \Delta(R, \rho, \varphi) \textit{ with } \rho(f_{\alpha(j)} f_\beta) = \gamma\}$$

and define $\sigma(\alpha(j)) = \#M(\alpha(j))$.

Note that if ρ in Definition 2.10 is a weight function then the two sets $N(\alpha(i))$ and $M(\alpha(j))$ can be defined as

$$N(\alpha(i)) = \{(\beta_1, \beta_2) \in (\Delta(R, \rho, \varphi))^2 \mid \beta_1 + \beta_2 = \alpha(i)\}$$

and

$$M(\alpha(j)) = \{\gamma \in \Delta(R, \rho, \varphi) \mid \exists \beta \in \Delta(R, \rho, \varphi) \text{ with } \alpha(j) + \beta = \gamma\},$$

where $+$ is the ordinary addition on elements in $\mathbb{N}_0$ extended as in Definition 2.5.

Both evaluation codes and dual codes from an order domain can now be defined. The codes considered here are the improved codes $\tilde{E}$ and $\tilde{C}$ from [16, 20, 2, 12].

Definition 2.11 *Consider a basis $\{f_\gamma \mid \rho(f_\gamma) = \lambda\}_{\lambda \in \Gamma}$ for an order structure (R, ρ, Γ) over $\mathbb{F}_q$. Let φ be a morphism as in Definition 2.8 and let $\Delta(R, \rho, \varphi)$ be as in Definition 2.9 so $B = \{\varphi(f_{\alpha(1)}), \varphi(f_{\alpha(2)}), \ldots, \varphi(f_{\alpha(n)})\}$ constitutes a basis for $\mathbb{F}_q^n$. Define*

$$\begin{aligned} \tilde{C}(\eta) &= \{\boldsymbol{c} \in \mathbb{F}_q^n \mid \boldsymbol{c} \cdot \varphi(f_{\alpha(i)}) = 0 \textit{ for all } \alpha(i) \in \Delta(R, \rho, \varphi) \textit{ with } \mu(\alpha(i)) < \eta\} \\ \tilde{E}(\delta) &= \mathit{Span}_{\mathbb{F}_q} \left\{\varphi(f_{\alpha(i)}) \mid \alpha(i) \in \Delta(R, \rho, \varphi) \textit{ and } \sigma(\alpha(i)) \geqslant \delta\right\} \end{aligned}$$

The following result concerning $\tilde{C}(\eta)$ is from [20, 12] and the result concerning $\tilde{E}(\delta)$ is from [2] (included in Part B).

Theorem 2.12 *The minimum distance of $\tilde{C}(\eta)$ and $\tilde{E}(\delta)$ satisfy $d(\tilde{C}(\eta)) \geqslant \eta$ and $d(\tilde{E}(\delta)) \geqslant \delta$.*

We now know (in principle) how to construct the $\tilde{E}$ and $\tilde{C}$ codes and estimate their minimum distance using Theorem 2.12 above but we need a practical way of constructing order domains. This is where Gröbner basis theory will be applied.

2.2. Gröbner basis theoretical approach to order domains

The Gröbner basis theory presented in this section is based on [8, 33] unless otherwise stated. First we need some fundamental definitions and some notation.

Definition 2.13 *A monomial in m variables $x_1, x_2, \ldots, x_m$ is a product of the form*

$$x_1^{a_1} x_2^{a_2} \cdots x_m^{a_m},$$

where all the exponents $a_1, a_2, \ldots, a_m \in \mathbb{N}_0$. Whenever m is clear from the context let $\boldsymbol{x}^{\boldsymbol{a}}$ denote the monomial $x_1^{a_1} x_2^{a_2} \cdots x_m^{a_m}$, where $\boldsymbol{a} = (a_1, a_2, \ldots, a_m) \in \mathbb{N}_0^m$.

Definition 2.14 *Let $\mathbb{F}$ be a field. A polynomial f in m variables $x_1, x_2, \ldots, x_m$ with coefficients in $\mathbb{F}$ is a finite linear combination (with coefficients in $\mathbb{F}$) of monomials. A polynomial f is written in the form*

$$f = \sum_i c_i \boldsymbol{x}^{\boldsymbol{a}_i}, \quad c_i \in \mathbb{F}$$

where the sum is over a finite set of m-tuples $\boldsymbol{a}_i = (a_{i,1}, a_{i,2}, \ldots, a_{i,m}) \in \mathbb{N}_0^m$. The set of all polynomials in $x_1, x_2, \ldots, x_m$ with coefficients in $\mathbb{F}$ is denoted $\mathbb{F}[x_1, x_2, \ldots, x_m]$. Moreover, we call $c_i \boldsymbol{x}^{\boldsymbol{a}_i}$ a term in f and the set $\{\boldsymbol{x}^{\boldsymbol{a}_i} \mid c_i \neq 0\}$ the support of f, denoted $\mathrm{Supp}(f)$.

Let $\mathbb{F}_q$ be a finite field and let $\mathcal{M}_m$ denote the set of monomials in $\mathbb{F}_q[x_1, x_2, \ldots, x_m]$ given by

$$\mathcal{M}_m = \left\{ \boldsymbol{x}^{\boldsymbol{a}} \;\middle|\; \boldsymbol{a} = (a_1, a_2, \ldots, a_m) \in \mathbb{N}_0^m \right\}.$$

In order to define a division algorithm (See [8, §2.3] or Chapter 3) on polynomials in several variables we need a way to order the set of monomials in $\mathcal{M}_m$. Thus we have the following definition.

Definition 2.15 *A monomial ordering $\prec$ on $\mathcal{M}_m$ is a relation on $\mathbb{N}_0^m$ satisfying the following conditions:*

1. *$\prec$ is a total ordering on $\mathbb{N}_0^m$.*
2. *If $\boldsymbol{a} \prec \boldsymbol{b}$ and $\boldsymbol{c} \in \mathbb{N}_0^m$, then $\boldsymbol{a} + \boldsymbol{c} \prec \boldsymbol{b} + \boldsymbol{c}$.*
3. *Every non-empty subset of $\mathbb{N}_0^m$ has a smallest element under $\prec$,i.e. the relation $\prec$ is a well-ordering on $\mathbb{N}_0^m$.*

An example of a monomial ordering is the lexicographic ordering defined below (See [8, §2.2, Pro. 4]).

Definition 2.16 *Let $\boldsymbol{a} = (a_1, a_2, \ldots, a_m)$ and $\boldsymbol{b} = (b_1, b_2, \ldots, b_m) \in \mathbb{N}_0^m$, $\boldsymbol{a} \neq \boldsymbol{b}$, and let i, where $1 \leqslant i \leqslant m$, be the largest index such that $a_i - b_i \neq 0$ in the vector difference $\boldsymbol{a} - \boldsymbol{b}$. Then $\boldsymbol{a}$ is said to be lexicographically smaller than $\boldsymbol{b}$, denoted $\boldsymbol{a} \prec_{lex} \boldsymbol{b}$, if $a_i - b_i < 0$. We write $\boldsymbol{x}^{\boldsymbol{a}} \prec_{lex} \boldsymbol{x}^{\boldsymbol{b}}$, if $\boldsymbol{a} \prec_{lex} \boldsymbol{b}$.*

Definition 2.17 *Given a monomial ordering $\prec$ on $\mathcal{M}_m$ and a polynomial $f \in \mathbb{F}_q[x_1, x_2, \ldots, x_m]$ of the form*

$$f = c_1 \boldsymbol{x}^{\boldsymbol{a}_1} + c_2 \boldsymbol{x}^{\boldsymbol{a}_2} + \cdots + c_n \boldsymbol{x}^{\boldsymbol{a}_n},$$

where $\boldsymbol{x}^{\boldsymbol{a}_1} \prec \boldsymbol{x}^{\boldsymbol{a}_2} \prec \cdots \prec \boldsymbol{x}^{\boldsymbol{a}_n}$, $c_i \in \mathbb{F}_q$ and $c_i \neq 0$, for $i = 1, 2, \ldots, n$, we call

1. *$c_n \boldsymbol{x}^{\boldsymbol{a}_n}$ the leading term in f, denoted* $\mathrm{lt}(f)$,
2. *c_n the leading coefficient in f, denoted* $\mathrm{lc}(f)$,
3. *$\boldsymbol{x}^{\boldsymbol{a}_n}$ the leading monomial in f, denoted* $\mathrm{lm}(f)$,
4. *$\boldsymbol{a}_n$ the multidegree of f, denoted* $\mathrm{multideg}(f)$,

all with respect to the monomial ordering $\prec$.

Definition 2.18 *Let $\mathbb{N}$ denote the positive integers. Given elements (called weights) $w(x_1), w(x_2), \ldots, w(x_m) \in \mathbb{N}$ define a monomial function $w : \mathcal{M}_m \to \mathbb{N}_0$ by*

$$w(x_1^{a_1} x_2^{a_2} \cdots x_m^{a_m}) = \sum_{i=1}^{m} a_i w(x_i).$$

For a monomial $\boldsymbol{x}^{\boldsymbol{a}} \in \mathcal{M}_m$ we call $w(\boldsymbol{x}^{\boldsymbol{a}})$ the weight of $\boldsymbol{x}^{\boldsymbol{a}}$.

Furthermore, for a polynomial $f \in \mathbb{F}_q[x_1, x_2, \ldots, x_m]$ we define the weighted degree of f, denoted $\mathrm{wdeg}(f)$, *to be the highest weight (with respect to the ordering $\leqslant$ on $\mathbb{N}_0$) that appears as the weight of a monomial in the support of f.*

Definition 2.19 *The weighted degree ordering $\prec_w$ induced by w from Definition 2.18 and a monomial ordering $\prec$ on $\mathcal{M}_m$ is the monomial ordering defined as follows. Given $\boldsymbol{x}^{\boldsymbol{a}}, \boldsymbol{x}^{\boldsymbol{b}} \in \mathcal{M}_m$ then $\boldsymbol{x}^{\boldsymbol{a}} \prec_w \boldsymbol{x}^{\boldsymbol{b}}$ if one of the following two conditions hold:*

1) $w(\boldsymbol{x}^{\boldsymbol{a}}) < w(\boldsymbol{x}^{\boldsymbol{b}})$ *2) $w(\boldsymbol{x}^{\boldsymbol{a}}) = w(\boldsymbol{x}^{\boldsymbol{b}})$ and $\boldsymbol{x}^{\boldsymbol{a}} \prec \boldsymbol{x}^{\boldsymbol{b}}$.*

Definition 2.20 *A subset $I \subseteq \mathbb{F}[x_1, x_2, \ldots, x_m]$ is called an ideal if it satisfies the following three conditions:*

1. $0 \in I$.

2. *If* $f, g \in I$, *then* $f + g \in I$.

3. *If* $f \in I$ *and* $h \in \mathbb{F}[x_1, x_2, \ldots, x_m]$, *then* $hf \in I$.

Definition 2.21 *Let* $f_1, f_2, \ldots, f_s \in \mathbb{F}[x_1, x_2, \ldots, x_m]$ *be polynomials. Define*

$$\langle f_1, f_2, \ldots, f_s \rangle = \left\{ \sum_{i=1}^{s} h_i f_i \;\middle|\; h_1, h_2, \ldots, h_s \in \mathbb{F}[x_1, x_2, \ldots, x_m] \right\}.$$

From [8, §1.4, Lemma 3] the set $\langle f_1, f_2, \ldots, f_s \rangle$ is an ideal in $\mathbb{F}[x_1, x_2, \ldots, x_m]$. We call $\langle f_1, f_2, \ldots, f_s \rangle$ the ideal generated by $f_1, f_2, \ldots, f_s$. Given a set $F = \{f_1, f_2, \ldots, f_s\}$ let $\langle F \rangle$ denote the ideal generated by the elements in F, i.e. $\langle F \rangle = \langle f_1, f_2, \ldots, f_s \rangle$.

Definition 2.22 *Let* $I \subset \mathbb{F}_q[x_1, x_2, \ldots, x_m]$ *be an ideal. Given a monomial ordering* $\prec$ *on* $\mathcal{M}_m$ *the set*

$$\Delta_{\prec}(I) = \left\{ \boldsymbol{x}^{\boldsymbol{a}} \in \mathcal{M}_m \;\middle|\; \boldsymbol{x}^{\boldsymbol{a}} \textit{ is not a leading monomial of any polynomial } f \in I \right\}$$

is called the footprint of I *with respect to* $\prec$.

Remark 2.23 Notice that if $I, J \subseteq \mathbb{F}[x_1, x_2, \ldots, x_m]$ are ideals such that $I \subseteq J$, then $\Delta_{\prec}(J) \subseteq \Delta_{\prec}(I)$. This is true since a leading monomial of a polynomial in I is also a leading monomial of a polynomial in J. $\triangledown$

Definition 2.24 *Let* $I = \langle f_1, f_2, \ldots, f_s \rangle$ *be an ideal in* $\mathbb{F}_q[x_1, x_2, \ldots, x_m]$, *let* $\mathbb{V}(I)$ *denote the corresponding variety given by*

$$\mathbb{V}(I) = \{p_1, p_2, \ldots, p_n\} = \{p \in \mathbb{F}_q^m \mid f(p) = 0 \textit{ for all } f \in I\}.$$

The following proposition from [8, §5.3, Pro. 8] and [9, Pro. 2.7] is known as the footprint bound.

Proposition 2.25 *Let* $\mathbb{F}$ *be a field and let* $I \subset \mathbb{F}[x_1, x_2, \ldots, x_m]$ *be an ideal. Then* $\#\mathbb{V}(I) \leqslant \#\Delta(I)$. *Furthermore, if* I *is a radical ideal and* $\mathbb{F}$ *is algebraically closed then equality holds.*

Recall, that an ideal $I \subseteq \mathbb{F}[x_1, x_2, \ldots, x_m]$ is called a radical ideal when $f \in I$ if and only if $f^m \in I$, for some positive integer m.

Definition 2.26 *Fix a monomial order. A finite subset $G = \{g_1, g_2, \ldots, g_s\}$ of an ideal I is said to be a Gröbner basis if $\langle \mathrm{lt}(g_1), \mathrm{lt}(g_2), \ldots, \mathrm{lt}(g_s)\rangle = \langle \mathrm{lt}(I)\rangle$, where $\langle \mathrm{lt}(I)\rangle$ denotes the ideal generated by the set of leading terms of polynomials in I.*

Remark 2.27 A consequence of Definition 2.26 is that every leading term of polynomials in I can be generated by the leading terms of the polynomials in a Gröbner basis G for the ideal I. Thus it follows from Definition 2.22 that the footprint $\Delta_{\prec}(I)$ of I is exactly the set of monomials in $\mathcal{M}_m$ which can not be divided by any leading monomial of polynomials in G, i.e. finding a Gröbner basis G for an ideal I gives us a way to find the set $\Delta_{\prec}(I)$. $\triangledown$

A special kind of Gröbner basis is defined below.

Definition 2.28 *A minimal Gröbner basis for a polynomial ideal I is a Gröbner basis G for I such that:*

1. $\mathrm{lc}(g) = 1$*, for all* $g \in G$.
2. *For all* $g \in G$, $\mathrm{lt}(g) \notin \langle \mathrm{lt}(G \setminus \{g\})\rangle$.

The existence of a minimal Gröbner basis as in Definition 2.28 follows by [8, §2.7, Lemma 3] given below.

Lemma 2.29 *Let G be a Gröbner basis for the polynomial ideal I. Let $f \in G$ be a polynomial such that $\mathrm{lt}(f) \in \langle \mathrm{lt}(G \setminus \{f\})\rangle$. Then $G \setminus \{f\}$ is also a Gröbner basis for I.*

The following proposition is from [8, 2§6, Pro. 1].

Proposition 2.30 *Let $G = \{g_1, g_2, \ldots, g_s\}$ be a Gröbner basis for an ideal $I \subset \mathbb{F}[x_1, x_2, \ldots, x_m]$ and let $f \in \mathbb{F}[x_1, x_2, \ldots, x_m]$ be a polynomial. There is a unique $r \in \mathbb{F}[x_1, x_2, \ldots, x_m]$ with the following properties:*

1. *No term of r is divisible by any of* $\mathrm{lt}(g_1), \mathrm{lt}(g_2), \ldots, \mathrm{lt}(g_s)$.
2. *There is $g \in I$ such that $f = g + r$.*

In particular, r is the remainder on division of f by G (see Theorem 3.1)no matter how the elements of G are listed when using the division algorithm. We will use the notation $\bar{f}$ for the unique remainder r on division of f by G.

The division algorithm mentioned in Proposition 2.30 will be stated in Chapter 3 (Or see [8, §2.3, Thm. 3]).

Proposition 2.30 has the following important corollary from [8, Cor. 2, §2.6] which we will be using in Chapter 6.

Corollary 2.31 *Let $G = \{g_1, g_2, \ldots, g_s\}$ be a Gröbner basis for an ideal $I \subseteq \mathbb{F}[x_1, x_2, \ldots, x_m]$ and let $f \in \mathbb{F}[x_1, x_2, \ldots, x_m]$ be a polynomial. Then $f \in I$ if and only if the remainder on division of f by G is zero, i.e. $\bar{f} = 0$.*

A Gröbner basis as in Definition 2.26 for an ideal I can always be found using Buchberger's algorithm (See [8, §2.7] or Chapter 3). S-polynomials defined below are an essential part of Buchberger's algorithm.

Definition 2.32 *Let $\mathbb{F}$ be a field, let $f, g \in \mathbb{F}[x_1, x_2, \ldots, x_m]$ be non-zero polynomials and let $\prec$ be a monomial ordering on the set $\mathcal{M}_m$.*

Let $lm(f) = x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_m^{\alpha_m}$ and let $lm(g) = x_1^{\beta_1} x_2^{\beta_2} \cdots x_m^{\beta_m}$ with respect to $\prec$ and define $x_1^{\gamma_1} x_2^{\gamma_2} \cdots x_m^{\gamma_m}$, where $\gamma_i = \max\{\alpha_i, \beta_i\}$, for $1 \leqslant i \leqslant m$.

The S-polynomial of f and g, written $S(f, g)$, is the combination

$$S(f,g) = \frac{x_1^{\gamma_1} x_2^{\gamma_2} \cdots x_m^{\gamma_m}}{\mathrm{lt}(f)} \cdot f - \frac{x_1^{\gamma_1} x_2^{\gamma_2} \cdots x_m^{\gamma_m}}{\mathrm{lt}(g)} \cdot g.$$

Notice that the monomial $x_1^{\gamma_1} x_2^{\gamma_2} \cdots x_m^{\gamma_m}$ in Definition 2.32 is the least common multiple of $\boldsymbol{x}^{\boldsymbol{\alpha}} = x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_m^{\alpha_m}$ and $\boldsymbol{x}^{\boldsymbol{\beta}} = x_1^{\beta_1} x_2^{\beta_2} \cdots x_m^{\beta_m}$, denoted $\mathrm{lcm}(\boldsymbol{x}^{\boldsymbol{\alpha}}, \boldsymbol{x}^{\boldsymbol{\beta}})$.

The following Definition is from [8, §2.9, Def. 1].

Definition 2.33 *Fix a monomial order and let $G = \{g_1, g_2, \ldots, g_s\} \subset \mathbb{F}[x_1, x_2, \ldots, x_m]$. Given a polynomial $f \in \mathbb{F}[x_1, x_2, \ldots, x_m]$, we say that f reduces to zero modulo G, written $f \rightarrow_G 0$, if f can be written in the form $f = a_1 g_1 + a_2 g_2 + \cdots + a_s g_s$, such that whenever $a_i g_i \neq 0$, we have $\mathrm{multideg}(f) \geqslant \mathrm{multideg}(a_i g_i)$.*

The S-polynomials in Definition 2.32 has the following property from [8, §2.9, Thm. 3] which is used in Buchberger's algorithm. We will study aspects of the algorithm itself later on.

Theorem 2.34 *A basis $G = \{g_1, g_2, \ldots, g_s\}$ for an ideal $I \in \mathbb{F}[x_1, x_2, \ldots, x_m]$ is a Gröbner basis for I if and only if $S(g_i, g_j) \rightarrow_G 0$, for all $i \neq j$.*

The S-polynomials in Definition 2.32 also has the following property from [8, §2.9, Pro. 4] which can be used to make Buchberger's algorithm faster by avoiding certain polynomial divisions.

Proposition 2.35 *Given a finite set $G \subset \mathbb{F}[x_1, x_2, \ldots, x_m]$, suppose that we have $f, g \in G$ such that $lcm(lm(f), lm(g)) = lm(f) \cdot lm(g)$. This means that the leading monomials of f and g are relatively prime. Then $S(f, g) \rightarrow_G 0$.*

Now, consider the following relation.

Definition 2.36 *Let $I \subset \mathbb{F}[x_1, x_2, \ldots, x_m]$ be an ideal and let $f, g \in \mathbb{F}[x_1, x_2, \ldots, x_m]$. We say that f and g are congruent modulo I, written $f \equiv g \mod I$, if $f - g \in I$.*

The most important property of the congruence relation from Definition 2.36 is that it is an equivalence relation on $\mathbb{F}[x_1, x_2, \ldots, x_m]$ [8, 5§2, Pro. 2].

Recall that an equivalence relation on a set L partitions L into a collection of disjoint subsets called equivalence classes. For any $f \in \mathbb{F}[x_1, x_2, \ldots, x_m]$ the equivalence class of f, written $[f]$, is the set

$$[f] = \{g \in \mathbb{F}[x_1, x_2, \ldots, x_m] \mid g \equiv f \mod I\}.$$

The set $[f]$ is also called the coset of f. Consider the following definition.

Definition 2.37 *The quotient of $\mathbb{F}[x_1, x_2, \ldots, x_m]$ modulo I, written $\mathbb{F}[x_1, x_2, \ldots, x_m]/I$, is the set of equivalence classes for congruence modulo I:*

$$\mathbb{F}[x_1, x_2, \ldots, x_m]/I = \{[f] \mid f \in \mathbb{F}[x_1, x_2, \ldots, x_m]\}.$$

Proposition 2.30 motivates the use of $\bar{f}$ as the standard representative for the equivalence class $[f] \in \mathbb{F}[x_1, x_2, \ldots, x_m]/I$. Addition and multiplication of elements in $\mathbb{F}[x_1, x_2, \ldots, x_m]/I$ are described in the following proposition from [8, §5.3, Pro. 8].

Proposition 2.38 *Let $I \subset \mathbb{F}[x_1, x_2, \ldots, x_m]$ be an ideal and let $G = \{g_1, g_2, \ldots, g_t\}$ be a Gröbner basis for I with respect to a given monomial order $\prec$. For each $[f] \in \mathbb{F}[x_1, x_2, \ldots, x_m]/I$ we get the standard representative $\bar{f}$ in the set $S = Span\{\boldsymbol{x}^{\boldsymbol{a}} \mid \boldsymbol{x}^{\boldsymbol{a}} \notin \langle lt(I) \rangle\}$. Then*

1. *$[f] + [g]$ is represented by $\bar{f} + \bar{g}$*
2. *$[f] \cdot [g]$ is represented by $\overline{\bar{f} \cdot \bar{g}}$*

The operations in Proposition 2.38 are well-defined by [8, §5.2, Pro. 5]. For a detailed description of computations in $\mathbb{F}[x_1, x_2, \ldots, x_m]/I$ see [8, Ch. 5].

A connection between the quotient $\mathbb{F}[x_1, x_2, \ldots, x_m]/I$ from Definition 2.37 and order domains from Definition 2.6 is given by Pellikaan's factor ring theorem from [33, Thm. 5.11].

Theorem 2.39 *Let I be an ideal in $\mathbb{F}[x_1, x_2, \ldots, x_m]$ with Gröbner basis G with respect to $\prec_w$ from Definition 2.19. Suppose that the elements of the footprint of I have mutually distinct weights and that every element of G has exactly two monomials of highest weight in its support. Then there exists a weight function ρ on $R = \mathbb{F}[x_1, x_2, \ldots, x_m]/I$ with the property that $\rho([f]) = \mathrm{wdeg}(\bar{f})$, for all polynomials f, where $[f]$ is the coset of f modulo*

I and $\bar{f}$ is the standard representative for $[f]$.

For the remaining part of Part A we will only consider order domains of the form described in Theorem 2.39.

Note that the Gröbner basis in Theorem 2.39 can (using Lemma 2.29) be assumed to be a minimal Gröbner basis as in Definition 2.28. Thus G can be assumed to be of the form $G = \{f_1, f_2, \ldots, f_s\}$, where $f_i = \boldsymbol{x}^{\boldsymbol{\beta}_i} + \eta_i \boldsymbol{x}^{\boldsymbol{\alpha}_i} + f_i'(x_1, x_2, \ldots, x_m)$, $w(\boldsymbol{x}^{\boldsymbol{\alpha}_i}) = w(\boldsymbol{x}^{\boldsymbol{\beta}_i}) > \mathrm{wdeg}(f_i'(x_1, x_2, \ldots, x_m))$, $\boldsymbol{x}^{\boldsymbol{\alpha}_i} \prec_w \boldsymbol{x}^{\boldsymbol{\beta}_i}$ and $\eta_i \in \mathbb{F} \setminus \{0\}$, for $i = 1, 2, \ldots, s$, where $\boldsymbol{x}^{\boldsymbol{\beta}_i}$ does not divide $\boldsymbol{x}^{\boldsymbol{\beta}_j}$ for any $i \neq j$.

From now on, whenever we refer to Theorem 2.39, we will assume that the Gröbner basis G is minimal and of the form described above.

Theorem 2.39 also motivates the following definition.

Definition 2.40 *Let $G = \{f_1, f_2, \ldots, f_s\} \subset \mathbb{F}_q[x_1, x_2, \ldots, x_m]$ be a set of polynomials where $f_i = \boldsymbol{x}^{\boldsymbol{\beta}_i} + \eta_i \boldsymbol{x}^{\boldsymbol{\alpha}_i} + f_i'(x_1, x_2, \ldots, x_m)$, $w(\boldsymbol{x}^{\boldsymbol{\alpha}_i}) = w(\boldsymbol{x}^{\boldsymbol{\beta}_i}) > \mathrm{wdeg}(f_i'(x_1, x_2, \ldots, x_m))$, $\boldsymbol{x}^{\boldsymbol{\alpha}_i} \prec_w \boldsymbol{x}^{\boldsymbol{\beta}_i}$ and $\eta_i \in \mathbb{F}$, for $i = 1, 2, \ldots, s$.*

Define $b_i = \boldsymbol{x}^{\boldsymbol{\beta}_i} + \eta_i \boldsymbol{x}^{\boldsymbol{\alpha}_i}$, for $i = 1, 2, \ldots, s$, and let $\mathcal{B}(G)$ denote the set $\mathcal{B}(G) = \{b_1, b_2, \ldots, b_s\}$ related to G. We call $\mathcal{B}(G)$ the binomial part of G (with respect to $\prec_w$).

Since we are going to construct evaluation codes using the factor ring $\mathbb{F}_q[x_1, x_2, \ldots, x_m]/I$ as an order domain, we need a morphism as in Definition 2.8 to be able to use both the code construction from Definition 2.11 and the bound on the minimum distance in Theorem 2.12. The morphism we will be using is the evaluation map φ defined below.

Definition 2.41 *Consider the ideal $I = \langle f_1, f_2, \ldots, f_s \rangle \subset \mathbb{F}_q[x_1, x_2, \ldots, x_m]$ and the variety $\mathbb{V}(I) = \{p_1, p_2, \ldots, p_n\}$. The evaluation map $\varphi : \mathbb{F}_q[x_1, x_2, \ldots, x_m]/I \rightarrow \mathbb{F}_q^n$ is given by $\varphi([f]) = (\bar{f}(p_1), \bar{f}(p_2), \ldots, \bar{f}(p_n))$.*

The surjective map $\varphi([f])$ is independent of the choice of representative of the equivalence class $[f]$, since every $f \in [f]$ can be written as $f = g + \bar{f}$, for $g \in I$, such that $f(p) = g(p) + \bar{f}(p) = \bar{f}(p)$, for all $p \in \mathbb{V}(I)$.

Surjectivity of φ can be shown by constructing polynomials $f_1, f_2, \ldots, f_n$ such that

$$f_i(p_j) = \begin{cases} 1 & \text{, if } i = j \\ 0 & \text{, otherwise,} \end{cases}$$

for $p_j \in \mathbb{V}(I)$, as it is done in the proof of [8, §5.3, Pro. 8]. This way

$$\mathbb{F}_q^n = \mathrm{Span}_{\mathbb{F}_q} \{\varphi([f_1]), \varphi([f_2]), \ldots, \varphi([f_n])\},$$

since $[f_1], [f_2], \ldots, [f_n] \in \mathbb{F}_q[x_1, x_2, \ldots, x_m]/I$ can be shown to be linearly independent (see the proof of [8, §5.3, Pro. 8]).

3. On Buchberger's algorithm

In this chapter we will be concerned with how Buchberger's algorithm finds a Gröbner basis for a polynomial ideal I. This chapter is based on [8, Ch. 2]. In this chapter the focus will be on using details from the algorithm as given in [8, §2.7, Thm. 2]. For reference the theorem is given in Section 3.2 with a small change in notation. Also, since polynomial division is an essential part of Buchberger's algorithm, the division algorithm from [8, §2.3, Thm. 3] is given in Section 3.1.

3.1. A division algorithm

Here we give the division algorithm as stated in the proof of [8, §2.3, Thm. 3] since we will be using the algorithm in the proofs in Section 3.3 and in Chapter 5.

Theorem 3.1 *Fix a monomial order $\prec$ on $\mathbb{N}_0^n$, and let $F = (f_1, f_2, \ldots, f_s)$ be an ordered s-tuple of polynomials in $\mathbb{F}[x_1, x_2, \ldots, x_m]$. Then every $f \in \mathbb{F}[x_1, x_2, \ldots, x_m]$ can be written as*

$$f = a_1 f_1 + a_2 f_2 + \cdots + a_s f_s + r,$$

where $a_i, r \in \mathbb{F}[x_1, x_2, \ldots, x_m]$, and either $r = 0$ or r is a linear combination, with coefficients in $\mathbb{F}$, of monomials, none of which is divisible by any of $\mathrm{lt}(f_1), \mathrm{lt}(f_2), \ldots, \mathrm{lt}(f_s)$. We will call r the remainder of f on division by F. Furthermore, if $a_i f_i \neq 0$, then we have $\mathrm{multideg}(a_i f_i) \preceq \mathrm{multideg}(f)$.

We will use the notation given in the following definition from [8, §2.6, Def. 3].

Definition 3.2 *We will write $\overline{f}^F$ for the remainder on division of f by the ordered s-tuple $F = (f_1, f_2, \ldots, f_s)$. If F is a Gröbner basis for the ideal $\langle f_1, f_2, \ldots, f_s \rangle$, then we can regard F as a set (without any particular order) by Proposition 2.30.*

The algorithm as stated in the proof of Theorem 3.1 given in [8, §2.3, Thm. 3] is given below.

```
Input: An ordered $s$-tuple $F = (f_1, f_2, \ldots, f_s)$ and a polynomial $f$

Output: $a_1, a_2, \ldots, a_s, r$

$a_1 := 0; a_2 := 0; \ldots; a_s := 0; r := 0$
$p := f$
WHILE $p \neq 0$ DO
BEGIN
    $i := 1$
    $divissionoccurred := false$
    WHILE $i \leqslant s$ AND $divisionoccurred = false$ DO
    BEGIN
        IF $\mathrm{lt}(f_i)$ divides $\mathrm{lt}(p)$ THEN
        BEGIN
            $a_i := a_i + \mathrm{lt}(p)/\mathrm{lt}(f_i)$
            $p := p - (\mathrm{lt}(p)/\mathrm{lt}(f_i))f_i$
            $divissionoccurred := true$
        END
        ELSE
        BEGIN
            $i := i + 1$
        END
    END
    IF $divissionoccurred = false$ THEN
    BEGIN
        $r := r + \mathrm{lt}(p)$
        $p := p - \mathrm{lt}(p)$
    END
END
```

Given an ordered s-tuple $F = (f_1, f_2, \ldots, f_s)$ of polynomials in $\mathbb{F}[x_1, x_2, \ldots, x_m]$ and a polynomial $f \in \mathbb{F}[x_1, x_2, \ldots, x_m]$ the algorithm does the following. Let the temporary variable p be initialized as being equal to f. The variable p will be holding an intermediate polynomial while the algorithm progresses.

First, we find the smallest index i such that $\mathrm{lt}(f_i)$ divides $\mathrm{lt}(p)$. If we can find such an index i then we add the term $\mathrm{lt}(p)/\mathrm{lt}(f_i)$ to a_i and construct a new p by subtracting $(\mathrm{lt}(p)/\mathrm{lt}(f_i))f_i$ from the old p. The algorithm then continues with this new p by again finding the smallest index i such that $\mathrm{lt}(f_i)$ divides $\mathrm{lt}(p)$

If no index $i \leqslant s$ exists such that $\mathrm{lt}(f_i)$ divides $\mathrm{lt}(p)$ then we add $\mathrm{lt}(p)$ to the variable r (which in the end will hold the remainder on division of f by F) and construct a new p by subtracting $\mathrm{lt}(p)$ from the old p. If the newly constructed p is non-zero then the algorithm makes another iteration.

The algorithm stops when $p = 0$. The variable r then contains the remainder on division of f by the ordered s-tuple F and the variables a_i contains polynomials such that

$$f = a_1 f_1 + a_2 f_2 + \cdots + a_s f_s + r$$

as given in Theorem 3.1.

3.2. Buchberger's algorithm

Here we give Buchberger's algorithm as stated in [8, §2.7, Thm. 2], with a slightly changed notation.

Theorem 3.3 *Let $I = \langle f_1, f_2, \ldots, f_s \rangle \neq \{0\}$ be a polynomial ideal. Then a Gröbner basis for I can be constructed in a finite number of steps by the following algorithm:*

Input: $F = (f_1, f_2, \ldots, f_s)$

Output: a Gröbner basis $L = (g_1, g_2, \ldots, g_t)$ *for* I*, with* $F \subseteq L$

```
$L := F$
REPEAT
BEGIN
        $L' := L$
        FOR each pair $\{p, q\}, p \neq q$ in $L'$ DO
        BEGIN
                $R := \overline{S(p,q)}^{L'}$
                IF $R \neq 0$ THEN $L := L \cup \{R\}$
        END
END
UNTIL $L = L'$
```

Buchberger's algorithm utilizes the property of a Gröbner basis given in Theorem 2.34 by expanding a given ordered list of polynomials until nothing new is added to the list and Theorem 2.34 is satisfied.

The algorithm does the following. Given an ordered list $F = (f_1, f_2, \ldots, f_s)$ of polynomials in $\mathbb{F}[x_1, x_2, \ldots, x_m]$ it starts by setting the two temporary lists L and L' equal to F. It then constructs the S-polynomials $S(p,q)$ for every pair $p \neq q$ in the list L'. If a non-zero remainder on division of $S(p,q)$ by L' is found, i.e. $R := \overline{S(p,q)}^{L'} \neq 0$, then this remainder R is added to the end of the list L. This continues until we have constructed $S(p,q)$, for every pair $p \neq q$ in L'.

If anything new was added to the list L during this iteration, then we let $L' := L$ and make another iteration with this new list L'. The algorithm continues until it encounters an iteration that adds nothing new to L, i.e. $L = L'$ after this iteration, and the algorithm stops.

That the elements in the list L is a basis for the ideal I follows from the fact that the elements in F are in L and the elements in F are a basis for I. Furthermore, the elements in L constitutes a Gröbner basis for I since they are constructed to satisfy Theorem 2.34.

3.3. On finding a Gröbner basis for ideals from Theorem 2.39

We will be using Buchberger's algorithm in Section 3.2, the division algorithm in Section 3.1 and the definition of S-polynomials in Definition 2.32 in the proofs of the following lemmas.

Consider an ideal I having Gröbner basis G of the form given in Theorem 2.39 and a polynomial $g \in \mathbb{F}[x_1, x_2, \dots, x_m]$, where $\operatorname{Supp}(g) \in \Delta_{\prec}(I)$. In the proof of Lemma 3.6 we will consider S-polynomials of the form $P_{(j_1)} = S(f_{j_1}, g)$, where $f_{j_1} \in G$, and polynomials $P_{(j_1,j_2,\dots,j_t)}$ defined recursively as

$$P_{(j_1,j_2,\dots,j_t)} = S(f_{j_r}, P_{(j_1,j_2,\dots,j_{t-1})}),$$

where $f_{j_1}, f_{j_2}, \dots, f_{j_t} \in G$ (with possible repetitions).

In the proofs of Lemma 3.5 and Lemma 3.6 we need to know something about the structure of these S-polynomials, thus we give the following Lemma 3.4. The proof of Lemma 3.4 may seem rather complicated at first glance but in reality the lemma follows just by writing the S-polynomials involved and observe what their leading monomials look like.

Lemma 3.4 *Let I be an ideal having Gröbner basis $G = \{f_1, f_2, \dots, f_s\}$ as in Theorem 2.39 with respect to $\prec_w$ as defined in Definition 2.19. For $i = 1, 2, \dots, s$, let $f_i = \boldsymbol{x}^{\boldsymbol{\beta}_i} + \eta_i \boldsymbol{x}^{\boldsymbol{\alpha}_i} + f_i'(x_1, x_2, \dots, x_m)$, $w(\boldsymbol{x}^{\boldsymbol{\alpha}_i}) = w(\boldsymbol{x}^{\boldsymbol{\beta}_i}) > \operatorname{wdeg}(f_i'(x_1, x_2, \dots, x_m))$ and $lm(f_i) = \boldsymbol{x}^{\boldsymbol{\beta}_i}$.*

Let $g = \boldsymbol{x}^{\boldsymbol{a}} + g'(x_1, x_2, \dots, x_m)$ be a polynomial in $\mathbb{F}[x_1, x_2, \dots, x_m]$ such that $w(g'(x_1, x_2, \dots, x_m)) < w(\boldsymbol{x}^{\boldsymbol{a}})$ and $\operatorname{Supp}(g) \subset \Delta_{\prec_w}(I)$.

Define the polynomial $P_{(j_1,j_2,\dots,j_t)}$ recursively as

$$P_{(j_1)} = S(f_{j_1}, g)$$

for some $1 \leqslant j_1 \leqslant s$, and

$$P_{(j_1,j_2,\dots,j_t)} = S(f_{j_t}, P_{(j_1,j_2,\dots,j_{t-1})}),$$

for some $1 \leqslant j_t \leqslant s$. Then $P_{(j_1,j_2,\dots,j_t)}$ is of the form

$$P_{(j_1,j_2,\dots,j_t)} = \eta_{j_t} \cdot \boldsymbol{x}^{\boldsymbol{p}_{j_t}} + P'_{(j_1,j_2,\dots,j_t)} \tag{3.1}$$

for specific $\boldsymbol{p}_{j_t} = (p_{j_t,1}, p_{j_t,2}, \dots, p_{j_t,m}) \in \mathbb{N}_0^m$ depending only on the two monomials of highest weight in $f_{j_1}, f_{j_2}, \dots, f_{j_t}$ and on $\operatorname{lm}(g)$. Furthermore, $\eta_{j_t} \in \mathbb{F}_q \setminus \{0\}$ and $w(P'_{(j_1,j_2,\dots,j_t)}) < w(\boldsymbol{x}^{\boldsymbol{p}_{j_t}})$ holds, i.e. $\operatorname{lm}(P_{(j_1,j_2,\dots,j_t)}) = \boldsymbol{x}^{\boldsymbol{p}_{j_t}}$.

Proof: The lemma is proven by induction in t.

Basis:

When $t = 1$ the polynomial $P_{(j_1)}$ is given by

$$\begin{aligned} P_{(j_1)} &= S(f_{j_1}, g) \\ &= \frac{\boldsymbol{x}^{\boldsymbol{\gamma}_{j_1}}}{\boldsymbol{x}^{\boldsymbol{\beta}_{j_1}}}\left(\boldsymbol{x}^{\boldsymbol{\beta}_{j_1}} + \eta_{j_1}\boldsymbol{x}^{\boldsymbol{\alpha}_{j_1}} + f'_{j_1}\right) - \frac{\boldsymbol{x}^{\boldsymbol{\gamma}_{j_1}}}{\boldsymbol{x}^{\boldsymbol{a}}}\left(\boldsymbol{x}^{\boldsymbol{a}} + g'\right) \\ &= \eta_{j_1}\boldsymbol{x}^{\boldsymbol{\gamma}_{j_1}-\boldsymbol{\beta}_{j_1}+\boldsymbol{\alpha}_{j_1}} + \boldsymbol{x}^{\boldsymbol{\gamma}_{j_1}-\boldsymbol{\beta}_{j_1}} \cdot f'_{j_1} - \boldsymbol{x}^{\boldsymbol{\gamma}_{j_1}-\boldsymbol{a}} \cdot g', \end{aligned}$$

where $\boldsymbol{\gamma}_{j_1} = (\gamma_{j_1,1}, \gamma_{j_1,2}, \ldots, \gamma_{j_1,m}) \in \mathbb{N}_0^m$ and $\gamma_{j_1,u} = \max\{\beta_{j_1,u}, i_u\}$, for $u = 1, 2, \ldots, m$. Furthermore, we have

$$w(\boldsymbol{x}^{\boldsymbol{\gamma}_{j_1}-\boldsymbol{a}} \cdot g') < w(\boldsymbol{x}^{\boldsymbol{\gamma}_{j_1}}) = w(\boldsymbol{x}^{\boldsymbol{\gamma}_{j_1}-\boldsymbol{\beta}_{j_1}+\boldsymbol{\alpha}_{j_1}})$$

and

$$w(\boldsymbol{x}^{\boldsymbol{\gamma}_{j_1}-\boldsymbol{\beta}_{j_1}} \cdot f'_{j_1}) < w(\boldsymbol{x}^{\boldsymbol{\gamma}_{j_1}}) = w(\boldsymbol{x}^{\boldsymbol{\gamma}_{j_1}-\boldsymbol{\beta}_{j_1}+\boldsymbol{\alpha}_{j_1}})$$

because $w(\boldsymbol{x}^{\boldsymbol{\beta}_{j_1}}) = w(\boldsymbol{x}^{\boldsymbol{\alpha}_{j_1}})$, $\operatorname{wdeg}(g') < w(\boldsymbol{x}^{\boldsymbol{a}})$ and $\operatorname{wdeg}(f'_{j_1}) < w(\boldsymbol{x}^{\boldsymbol{\beta}_{j_1}})$ by definition of f_{j_1} and g.

Step:

Assume that the lemma holds for $t \geqslant 1$ and

$$P_{(j_1,j_2,\ldots,j_t)} = \eta_{j_t} \cdot \boldsymbol{x}^{\boldsymbol{p}_{j_t}} + P'_{(j_1,j_2,\ldots,j_t)}.$$

Then for $j_{t+1} \in \{1, 2, \ldots, s\}$ we have

$$\begin{aligned} P_{(j_1,j_2,\ldots,j_{t+1})} &= S\left(f_{j_{t+1}}, P_{(j_1,j_2,\ldots,j_t)}\right) \\ &= \frac{\boldsymbol{x}^{\boldsymbol{\gamma}_{j_{t+1}}}}{\boldsymbol{x}^{\boldsymbol{\beta}_{j_{t+1}}}}\left(\boldsymbol{x}^{\boldsymbol{\beta}_{j_{t+1}}} + \eta_{j_{t+1}} \cdot \boldsymbol{x}^{\boldsymbol{\alpha}_{j_{t+1}}} + f'_{j_{t+1}}\right) \\ &\qquad - \frac{\boldsymbol{x}^{\boldsymbol{\gamma}_{j_{t+1}}}}{\eta_{j_t} \cdot \boldsymbol{x}^{\boldsymbol{p}_{j_t}}}\left(\eta_{j_t} \cdot \boldsymbol{x}^{\boldsymbol{p}_{j_t}} + P'_{(j_1,j_2,\ldots,j_t)}\right) \\ &= \eta_{j_{t+1}} \cdot \boldsymbol{x}^{\boldsymbol{\gamma}_{j_{t+1}}-\boldsymbol{\beta}_{j_{t+1}}+\boldsymbol{\alpha}_{j_{t+1}}} + \boldsymbol{x}^{\boldsymbol{\gamma}_{j_{t+1}}-\boldsymbol{\beta}_{j_{t+1}}} \cdot f'_{j_{t+1}} \\ &\qquad - \frac{1}{\eta_{j_t}} \cdot \boldsymbol{x}^{\boldsymbol{\gamma}_{j_{t+1}}-\boldsymbol{p}_{j_t}} \cdot P'_{(j_1,j_2,\ldots,j_t)}, \end{aligned}$$

where $\boldsymbol{\gamma}_{j_{t+1}} = (\gamma_{j_{t+1},1}, \gamma_{j_{t+1},2}, \ldots \gamma_{j_{t+1},m}) \in \mathbb{N}_0^m$ and $\gamma_{j_{t+1},u} = \max\{\beta_{j_{t+1},u}, p_{j_t,u}\}$, for $u = 1, 2, \ldots, m$. Furthermore, we have that

$$w\left(\boldsymbol{x}^{\boldsymbol{\gamma}_{j_{t+1}}-\boldsymbol{p}_{j_t}} \cdot P'_{(j_1,j_2,\ldots,j_t)}\right) < w\left(\boldsymbol{x}^{\boldsymbol{\gamma}_{j_{t+1}}}\right) = w\left(\boldsymbol{x}^{\boldsymbol{\gamma}_{j_{t+1}}-\boldsymbol{\beta}_{j_{t+1}}+\boldsymbol{\alpha}_{j_{t+1}}}\right)$$

and

$$w\left(\boldsymbol{x}^{\boldsymbol{\gamma}_{j_{t+1}}-\boldsymbol{\beta}_{j_{t+1}}} \cdot f'_{j_{t+1}}\right) < w\left(\boldsymbol{x}^{\boldsymbol{\gamma}_{j_{t+1}}}\right) = w\left(\boldsymbol{x}^{\boldsymbol{\gamma}_{j_{t+1}}-\boldsymbol{\beta}_{j_{t+1}}+\boldsymbol{\alpha}_{j_{t+1}}}\right)$$

because $w(\boldsymbol{x}^{\boldsymbol{\beta}_{j_{t+1}}}) = w(\boldsymbol{x}^{\boldsymbol{\alpha}_{j_{t+1}}})$ and $w(P'_{(j_1,j_2,\ldots,j_t)}) < w(\boldsymbol{x}^{\boldsymbol{p}_{j_t}})$ using the definition of $f_{j_{t+1}}$ and the induction hypothesis. □

At this point we make the following three important observations which will be used in the proofs of Lemma 3.5 and Lemma 3.6 (among others).

Observation 1:

The first observation follows from the proof of Lemma 3.4 given above. If we consider an ideal I having Gröbner basis $G = \{f_1, f_2, \dots f_s\}$ of the form given in Theorem 2.39 and a polynomial $g = \boldsymbol{x^a} + g'(x_1, x_2, \dots, x_m) \in \mathbb{F}[x_1, x_2, \dots, x_m]$, where $\mathrm{Supp}(g) \subset \Delta_{\prec}(I)$ and $\mathrm{lm}(g) = \boldsymbol{x^a}$. Furthermore, let $\mathcal{B}(G) = \{b_1, b_2, \dots, b_s\}$ be the binomial part of G as in Definition 2.40. Then from the proof of Lemma 3.4 it is clear that f_i' and g' have no influence on what the leading monomial of $P_{(j_1, j_2, \dots, j_t)}$ is, for any $i \in (j_1, j_2, \dots, j_t)$.

Now, let $(j_1, j_2, \dots, j_t)$ be fixed and replace the polynomials f_i with their corresponding binomial part b_i and g by it's leading monomial $\boldsymbol{x^a}$ in the lemma above. Then construct $Q_{(j_1)} = S(b_{j_1}, g)$ and $Q_{(j_1, j_2, \dots, j_t)} = S(b_{j_t}, q_{(j_1, j_2, \dots, j_{t-1})})$ recursively and we have the equality

$$\mathrm{lm}\left(Q_{(j_1, j_2, \dots, j_t)}\right) = \mathrm{lm}\left(P_{(j_1, j_2, \dots, j_t)}\right), \tag{3.2}$$

for a fixed monomial ordering $\prec$ and any $t \geqslant 1$.

Observation 2:

The second observation regards S-polynomials and their connection to the division algorithm given in Section 3.1. Consider two polynomials $p, q \in \mathbb{F}[x_1, x_2, \dots, x_m]$ such that $\mathrm{lm}(q)$ divides $\mathrm{lm}(p)$, i.e. $\mathrm{lcm}(\mathrm{lm}(q), \mathrm{lm}(p)) = \mathrm{lm}(p)$, with respect to a monomial ordering $\prec$. Then from Definition 2.32 we have

$$\begin{aligned} S(p, q) &= \frac{\mathrm{lcm}(\mathrm{lm}(p), \mathrm{lm}(q))}{\mathrm{lt}(p)} \cdot p - \frac{\mathrm{lcm}(\mathrm{lm}(p), \mathrm{lm}(q))}{\mathrm{lt}(q)} \cdot q \\ &= \frac{\mathrm{lm}(p)}{\mathrm{lt}(p)} \cdot p - \frac{\mathrm{lm}(p)}{\mathrm{lt}(q)} \cdot q \\ &= \frac{1}{\mathrm{lc}(p)} \cdot p - \frac{\mathrm{lm}(p)}{\mathrm{lt}(q)} \cdot q, \end{aligned} \tag{3.3}$$

which basically is the same as constructing the polynomial

$$p := p - (\mathrm{lt}(p)/\mathrm{lt}(q))q \tag{3.4}$$

during an iteration of the division algorithm (except that the new p in (3.4) not necessarily has the same leading coefficient as the S-polynomial in (3.3)).

When dividing $S(f_{j_1}, g) \neq 0$ with G (regarded as an ordered s-tuple), where f_{j_1}, g and G are as in Lemma 3.4, then the division algorithm updates the variable p, say t times, as in (3.4), before adding the first term $\gamma \neq 0$ to the variable r (r holds the reminder when the algorithm stops) and construct a new p from the old one by letting $p := p - \gamma$.

Assume that this new $p \neq 0$. Since $p \prec \gamma$ and the division algorithm has the property given in Theorem 3.1, then any non-zero term added to r in later iterations is smaller than γ (with respect to $\prec$). Thus the remainder $\overline{S(f_{j_1}, g)}^G \neq 0$ on division of $S(f_{j_1}, g)$ by G has the same leading monomial as some $P_{(j_1, j_2, \dots, j_t)}$ from Lemma 3.4, where $\mathrm{lt}(f_{j_i})$

divides $\mathrm{lt}(P_{(j_1,j_2,\ldots,j_{i-1})})$, for all $i = 2, 3, \ldots, t$, and no $f_i \in G$ divides $P_{(j_1,j_2,\ldots,j_t)}$, i.e we have that

$$\mathrm{lm}\left(\overline{S(f_{j_1}, g)}^{G}\right) = \mathrm{lm}\left(P_{(j_1,j_2,\ldots,j_t)}\right), \tag{3.5}$$

for some $t \geqslant 2$, if $S(f_{j_1}, g) \neq 0$. Note that $P_{(j_1,j_2,\ldots,j_t)}$ may not be equal to the remainder $\overline{S(f_{j_1}, g)}^{G}$ but all we need is the equality in (3.5). By using (3.3) and (3.4) in every iteration of the division algorithm it follows that if $\overline{S(f_{j_1}, g)}^{G} = 0$ then there exists a $t \geqslant 2$ such that $P_{(j_1,j_2,\ldots,j_t)} = 0$ and $\mathrm{lt}(f_{j_i})$ divides $\mathrm{lt}(P_{(j_1,j_2,\ldots,j_{i-1})})$, for all $i = 2, 3, \ldots, t$.

Observation 3:

The third observation concerns footprints. Consider two ideal $I, J \subseteq \mathbb{F}[x_1, x_2, \ldots, x_m]$ with Gröbner basis $F = \{f_1, f_2, \ldots, f_s\}$ and $G = \{g_1, g_2, \ldots, g_t\}$ respectively. Assume that for every $g \in G$ there exists a $f \in F$ such that $\mathrm{lt}(f)$ divides $\mathrm{lt}(g)$, then it follows from Remark 2.27 that

$$\Delta_{\prec}(I) \subseteq \Delta_{\prec}(J) \tag{3.6}$$

holds.

Lemma 3.5 will prove that given a Gröbner basis G for an ideal I as in Theorem 2.39, then the binomial part of G, i.e. $\mathcal{B}(G)$, constitutes a Gröbner basis for the ideal $\langle \mathcal{B}(G) \rangle$.

Lemma 3.5 *Let $\mathbb{F}_q[x_1, x_2, \ldots, x_m]/I$ be an order domain with Gröbner basis $G = \{f_1, f_2, \ldots, f_s\}$ as described in Theorem 2.39 and let $\mathcal{B}(G) = \{b_1, b_2, \ldots b_s\}$ be the binomial part of G as in Definition 2.40. Then $\mathcal{B}(G)$ is a Gröbner basis for the ideal $\langle b_1, b_2, \ldots, b_s \rangle$.*

Proof: Since G is a Gröbner basis for I then $\overline{S(f_i, f_j)}^{G} = 0$, for all $i \neq j$, using Theorem 2.34. Thus if we can show that $\overline{S(b_i, b_j)}^{\mathcal{B}(G)} = 0$ follows, for all $i \neq j$, then we have proven the lemma. The proof relies very much on observations 1 and 2 on page 20.

First we repeat the definition of the polynomials we need and take a look at the structure of the S-polynomials $S(f_i, f_j)$ and it's connection to $S(b_i, b_j)$, for fixed $i \neq j$.

Let $f_i = \boldsymbol{x}^{\boldsymbol{\beta}_i} + \eta_i \boldsymbol{x}^{\boldsymbol{\alpha}_i} + f_i'(x_1, x_2, \ldots, x_m) = b_i + f_i'(x_1, x_2, \ldots, x_m)$, where $w(\boldsymbol{x}^{\boldsymbol{\alpha}_i}) = w(\boldsymbol{x}^{\boldsymbol{\beta}_i}) > \mathrm{wdeg}(f_i'(x_1, x_2, \ldots, x_m))$, $\boldsymbol{x}^{\boldsymbol{\alpha}_i} \prec_w \boldsymbol{x}^{\boldsymbol{\beta}_i}$ and $\eta_i \in \mathbb{F}_q \setminus \{0\}$, for $i = 1, 2, \ldots, s$. Thus $\mathrm{lt}(f_i) = \mathrm{lt}(b_i) = \boldsymbol{x}^{\boldsymbol{\beta}_i}$, for all $i = 1, 2, \ldots, s$, and

$$\begin{aligned} S(f_i, f_j) &= \frac{\boldsymbol{x}^{\boldsymbol{\gamma}_{ij}}}{\boldsymbol{x}^{\boldsymbol{\beta}_i}} \eta_i \boldsymbol{x}^{\boldsymbol{\alpha}_i} + \frac{\boldsymbol{x}^{\boldsymbol{\gamma}_{ij}}}{\boldsymbol{x}^{\boldsymbol{\beta}_i}} f_i'(x_1, x_2, \ldots, x_m) - \frac{\boldsymbol{x}^{\boldsymbol{\gamma}_{ij}}}{\boldsymbol{x}^{\boldsymbol{\beta}_j}} \eta_j \boldsymbol{x}^{\boldsymbol{\alpha}_j} - \frac{\boldsymbol{x}^{\boldsymbol{\gamma}_{ij}}}{\boldsymbol{x}^{\boldsymbol{\beta}_j}} f_j'(x_1, x_2, \ldots, x_m), \\ &\hspace{30em} (3.7) \\ &= S(b_i, b_j) + \frac{\boldsymbol{x}^{\boldsymbol{\gamma}_{ij}}}{\boldsymbol{x}^{\boldsymbol{\beta}_i}} f_i'(x_1, x_2, \ldots, x_m) - \frac{\boldsymbol{x}^{\boldsymbol{\gamma}_{ij}}}{\boldsymbol{x}^{\boldsymbol{\beta}_j}} f_j'(x_1, x_2, \ldots, x_m), \end{aligned}$$

where $\boldsymbol{x}^{\boldsymbol{\gamma}_{ij}} = \mathrm{lcm}(\boldsymbol{x}^{\boldsymbol{\beta}_i}, \boldsymbol{x}^{\boldsymbol{\beta}_j})$ and $\mathrm{lt}(S(f_i, f_j)) = \mathrm{lt}(S(b_i, b_j))$, if $S(b_i, b_j) \neq 0$. The last statement follows by inspecting $S(b_i, b_j)$ and by noticing that

$$w(\boldsymbol{x}^{\boldsymbol{\gamma}_{ij} - \boldsymbol{\beta}_i + \boldsymbol{\alpha}_i}) = w(\boldsymbol{x}^{\boldsymbol{\gamma}_{ij} - \boldsymbol{\beta}_j + \boldsymbol{\alpha}_j}) > \mathrm{wdeg}(\boldsymbol{x}^{\boldsymbol{\gamma}_{ij} - \boldsymbol{\beta}_i} \cdot f_i'(x_1, x_2, \ldots, x_m))$$

and

$$w(\boldsymbol{x}^{\boldsymbol{\gamma}_{ij}-\boldsymbol{\beta}_j+\boldsymbol{\alpha}_j}) > \text{wdeg}(\boldsymbol{x}^{\boldsymbol{\gamma}_{ij}-\boldsymbol{\beta}_j} \cdot f'_j(x_1, x_2, \dots, x_m)),$$

since $w(\boldsymbol{x}^{\boldsymbol{\beta}_i}) = w(\boldsymbol{x}^{\boldsymbol{\alpha}_i}) > \text{wdeg}(f'_i(x_1, x_2, \dots, x_m))$ and $w(\boldsymbol{x}^{\boldsymbol{\beta}_j}) = w(\boldsymbol{x}^{\boldsymbol{\alpha}_j}) > \text{wdeg}(f'_j(x_1, x_2, \dots, x_m))$ by definition of f_i and f_j.

Then define $P_{(j_1)} = S(f_i, f_j)$ and define $P_{(j_1,j_2,\dots,j_t)}$ recursively as

$$P_{(j_1,j_2,\dots,j_t)} = S(f_{j_t}, P_{(j_1,j_2,\dots,j_{t-1})}),$$

for $t \geqslant 1$.

Now, using observation 2 on page 20 and the fact that G is a Gröbner basis for I, there exists a t such that $P_{(j_1,j_2,\dots,j_t)} = 0 = \overline{S(f_i, f_j)}^G$, where $\text{lt}(f_{j_u})$ divides $\text{lt}(P_{(j_1,j_2,\dots,j_{u-1})})$, for $u = 2, 3, \dots, t$ and t is as small as possible.

Claim: The support of $P_{(i,j_1,j_2,\dots,j_u)}$ contains two monomials of the highest weight, for all $u = 1, 2, \dots, t-1$.

Our claim is proven by contradiction. Assume that for some k, where $1 \leqslant k \leqslant t-1$, the support of $P_{(j_1,j_2,\dots,j_k)}$ contains only one monomial of highest weight. Then so would

$$P_{(j_1,j_2,\dots,j_{k+1})}, P_{(j_1,j_2,\dots,j_{k+2})}, \dots, P_{(j_1,j_2,\dots,j_{t-1})},$$

since $f_{j_{k+1}}, f_{j_{k+2}}, \dots, f_{j_{t-1}}$ all have two monomials of highest weight in their support. Thus we would never be able to cancel the monomial of highest weight in $P_{(j_1,j_2,\dots,j_{t-1})}$ by dividing it with f_{j_t} which contradicts the definition of $P_{(j_1,j_2,\dots,j_t)}$. This concludes the proof of our claim.

Let k be the smallest index such that $\text{wdeg}(P_{(j_1,j_2,\dots,j_k)}) < \text{wdeg}(P_{(j_1,j_2,\dots,j_{k-1})})$. This happens exactly when the two monomials of highest weight in f_{j_k} cancel the two monomials of highest weight in $P_{(j_1,j_2,\dots,j_{k-1})}$.

Let $i, j, (j_1, j_2, \dots, j_k)$ and $k \leqslant t$ be fixed. Define $Q_{(j_1)} = S(b_i, b_j)$ and define $Q_{(j_1,j_2,\dots,j_u)}$ recursively as

$$Q_{(j_1,j_2,\dots,j_u)} = S(b_{j_u}, Q_{(j_1,j_2,\dots,j_{u-1})}),$$

for $1 \leqslant u \leqslant k$. Then from the proof of Lemma 3.4 (with f_j playing the role of g) and observation 1 on page 20, we have that $\text{lm}(Q_{(j_1,j_2,\dots,j_u)}) = \text{lm}(P_{(j_1,j_2,\dots,j_u)})$, for all $u = 1, 2, \dots, k-1$, since $f'_{j_1}, f'_{j_2}, \dots, f'_{j_u}$ and f'_j has no influence on what is the leading monomial of $P_{(j_1,j_2,\dots,j_u)}$ and $f_v = b_v + f'_v$, for all $v = 1, 2, \dots, s$.

Furthermore, since the support of $P_{(j_1,j_2,\dots,j_u)}$ contains two monomials of highest weight, for all $u = 1, 2, \dots, k-1$ and $f_v = b_v + f'_v$, for all $v = 1, 2, \dots, s$, then the support of $Q_{(j_1,j_2,\dots,j_u)}$ contains two monomials of highest weight, for all $u = 1, 2, \dots, k-1$.

Since the two monomials of highest weight in f_{j_k} cancel the two monomials of highest weight in $P_{(j_1,j_2,\dots,j_{k-1})}$, we have that $Q_{(j_1,j_2,\dots,j_k)} = 0$. Which again (using observation 2 on page 20) means that $\overline{S(b_i, b_j)}^{\mathcal{B}(G)} = 0$, for all $i \neq j$, since $i \neq j$ were random. □

Lemma 3.6, which will be essential in Chapter 4, is proven by using the three observations above, i.e. by using (3.2), (3.5) and (3.6), and Lemma 3.5. The rather technical proof relies very much on Buchberger's algorithme given in Section 3.2, the division algorithm given in Section 3.1 and the three observations right after Lemma 3.4.

Lemma 3.6 only states the inclusion from Lemma 1 in the Appendix of [4], thus the proof given below is different than the one given in the Appendix of [4].

Lemma 3.6 *Let $\mathbb{F}_q[x_1, x_2, \ldots, x_m]/I$ be an order domain with Gröbner basis $G = \{f_1, f_2, \ldots, f_s\}$ as described in Theorem 2.39 and let $\mathcal{B}(G) = \{b_1, b_2, \ldots b_s\}$ be the binomial part of G as in Definition 2.40.*

Let g be a polynomial in $\mathbb{F}_q[x_1, x_2, \ldots, x_m]$, let $lm(g) = \boldsymbol{x}^{\boldsymbol{a}}$ with respect to $\prec_w$ and assume that $\mathrm{Supp}(g) \subset \Delta_{\prec_w}(\langle f_1, f_2, \ldots, f_s\rangle)$. *Then*

$$\Delta_{\prec_w}(\langle f_1, f_2, \ldots, f_s, g\rangle) \subseteq \Delta_{\prec_w}(\langle b_1, b_2, \ldots, b_s, \boldsymbol{x}^{\boldsymbol{a}}\rangle). \tag{3.8}$$

Proof: The lemma is proven by studying what happens when running Buchberger's algorithm on the ordered list $M = (b_1, b_2, \ldots, b_s, \boldsymbol{x}^{\boldsymbol{a}})$ compared to what happens when running the algorithm on the ordered list $L = (f_1, f_2, \ldots, f_s, g)$. In other words: we will show that every time a remainder q is added to the list M, when running Buchberger's algorithm on M, we can add a polynomial $p \in \langle L\rangle$ to the list L such that $\mathrm{lm}(p) = \mathrm{lm}(q)$. After expanding L this way we can use observation 3 on page 21 to prove the theorem.

In the following we will use the term *inner loop* for the **FOR**-loop in the algorithm and the term *outer loop* for the **REPEAT-UNTIL**-loop (See the listing of the algorithm in Section 3.2).

In the following, let M^* denote the ordered list $(b_1, b_2, \ldots, b_s)$ and let L^* denote the ordered list $(f_1, f_2, \ldots, f_s)$. First, notice that $\overline{S(b_i, b_j)}^{M^*} = 0$ and $\overline{S(f_i, f_j)}^{L^*} = 0$, for all $i \neq j$, since $\{f_1, f_2, \ldots, f_s\}$ is a Gröbner basis for $I = \langle f_1, f_2, \ldots, f_s\rangle$ and, using Lemma 3.5, $\{b_1, b_2, \ldots, b_s\}$ is a Gröbner basis for $J = \langle b_1, b_2, \ldots, b_s\rangle$.

Now, consider what happens during the first iteration in both the outer and the inner loop of Buchberger's algorithm running on the ordered list M given above. Then the only S-polynomials that might add something to M during the first iteration is an S-polynomial $S(b_{j_1}, \boldsymbol{x}^{\boldsymbol{a}})$ (which consists of one term), for some $1 \leqslant j_1 \leqslant s$.

Let $Q_{(j_1, j_2, \ldots, j_t)}$ be defined as in observation 1 on page 20, for some fixed t as small as possible, such that $\mathrm{lm}(Q_{(j_1, j_2, \ldots, j_t)}) = \mathrm{lm}(\overline{S(b_{j_1}, \boldsymbol{x}^{\boldsymbol{a}})}^{M^*}) \neq 0$, using observation 2 on page 20 and (3.5). Using observation 1 and 2 we also have that

$$\mathrm{lm}\left(\overline{S(b_{j_1}, \boldsymbol{x}^{\boldsymbol{a}})}^{M^*}\right) = \mathrm{lm}\left(Q_{(j_1, j_2, \ldots, j_t)}\right) = \mathrm{lm}\left(P_{(j_1, j_2, \ldots, j_t)}\right) = \mathrm{lm}\left(\overline{S(f_{j_1}, g)}^{L^*}\right), \tag{3.9}$$

for this t, where $P_{(j_1, j_2, \ldots, j_t)}$ is from observation 1 on page 20 and $(j_1, j_2, \ldots, j_t)$ is fixed.

We now have two cases to consider.

<u>Case 1: $\boldsymbol{x}^{\boldsymbol{a}}$ does not divide $\overline{S(b_{j_1}, \boldsymbol{x}^{\boldsymbol{a}})}^{M^*}$.</u>

In this case Buchberger's algorithm will add $\overline{S(b_{j_1}, \boldsymbol{x}^{\boldsymbol{a}})}^{M^*}$ to the ordered list M.

Since $\mathrm{lm}(g)$ does not divide $\overline{S(b_{j_1}, \boldsymbol{x^a})}^{M^*}$ and (3.9) holds, we add $\overline{S(f_{j_1}, g)}^{L^*}$ to the ordered list L, since we could add this remainder to L when running Buchberger's algorithm on L.

Thus, during this first iteration we add polynomials p and q to the lists L and M respectively, both having the same leading monomial, no matter which j_1 we choose.

Case 2: $\boldsymbol{x^a}$ divides $\overline{S(b_{j_1}, \boldsymbol{x^a})}^{M^*}$.

In this case Buchberger's algorithm will not add anything to the list M since $\overline{S(b_{j_1}, \boldsymbol{x^a})}^{M^*}$ consists of one term and the remainder on division of $\overline{S(b_{j_1}, \boldsymbol{x^a})}^{M^*}$ by $\boldsymbol{x^a}$ is zero.

In this case we add nothing to L either.

This ends the two cases. Now, since the algorithm only updates the list M once in the beginning of every iteration of the outer loop, all the iterations of the inner loop will only add polynomials q_i to the list M, as described in Case 1 above (and add polynomials p_i to the list L having $\mathrm{lm}(p_i) = \mathrm{lm}(q_i)$, when running on L).

This means that after the first iteration of the outer loop (and the lists are updated) the following holds: For every polynomial $q \in M$ there exists a polynomial $p \in L$ such that $\mathrm{lm}(p)$ is equal to $\mathrm{lm}(q)$.

Now, let consider a successive iteration in the outer loop in Buchberger's algorithm running on the list M such that

$$M = [b_1, b_2, \ldots, b_s, \boldsymbol{x^a}, q_1, q_2, \ldots, q_u], \tag{3.10}$$

where $q_1, q_2, \ldots, q_u$ have been added in the previous iterations. Furthermore, assume that $\#M = \#L$ and for every $q_i \in M$ there exists a $p_i \in L$ such that $\mathrm{lm}(p_i) = \mathrm{lm}(q_i)$.

First look at the list M in (3.10). Since the polynomials $q_1, q_2, \ldots, q_u$ all consists of one term, any S-polynomial $S(q_i, q_j) = 0$, for all i and j. The same holds for any S-polynomial $S(\boldsymbol{x^a}, q_i)$, for all i. Thus the only S-polynomials that might add something to the list M are S-polynomials of the form $S(b_i, q_j)$.

Let $Q_{(j_1,j_2,\ldots,j_k)}$ be defined as before such that $\mathrm{lm}(Q_{(j_1,j_2,\ldots,j_k)}) = \mathrm{lm}(\overline{S(b_{j_1}, q_j)}^{M^*}) \neq 0$, for some fixed k as small as possible. Since for every $q_i \in M$ there exists a $p_i \in L$ such that $\mathrm{lm}(p_i) = \mathrm{lm}(q_i)$, then, using observation 1 and 2 again, we also have that

$$\mathrm{lm}\left(\overline{S(b_{j_1}, \boldsymbol{x^a})}^{M^*}\right) = \mathrm{lm}\left(Q_{(j_1,j_2,\ldots,j_k)}\right) = \mathrm{lm}\left(P_{(j_1,j_2,\ldots,j_k)}\right) = \mathrm{lm}\left(\overline{S(f_{j_1}, g)}^{L^*}\right), \tag{3.11}$$

for this k, where $P_{(j_1,j_2,\ldots,j_k)}$ is from observation 1 on page 20 and $(j_1, j_2, \ldots, j_k)$ is fixed.

Again we have two cases to consider (which we will call Case 3 and Case 4 to distinguish them from the two first cases above).

Case 3: Neither $\boldsymbol{x^a}$ nor any q_i divides $\overline{S(b_{j_1}, q_j)}^{M^*}$, for $i = 1, 2, \ldots, u$,

In this case Buchberger's algorithm will add $\overline{S(b_{j_1}, q_j)}^{M^*}$ to the ordered list M.

Since neither $\mathrm{lm}(g)$ or $\mathrm{lm}(p_i) = \mathrm{lm}(q_i)$ divides $\overline{S(b_{j_1}, q_j)}^{M^*}$, for any $i = 1, 2, \ldots, u$, and (3.11) holds, we add $\overline{S(f_{j_1}, p_j)}^{L^*}$ to the ordered list L.

Thus during this iteration we again add polynomials p and q to the lists L and M respectively, both having the same leading monomial, no matter which j_1 or j we choose.

Case 4: $\boldsymbol{x}^{\boldsymbol{a}}$ or $\mathrm{lm}(q_i)$ divides $\overline{S(b_{j_1}, q_j)}^{M^*}$, for some i.

In this case Buchberger's algorithm will not add anything to the list M since $\overline{S(b_{j_1}, q_j)}^{M^*}$ consists of one term and the remainder on division of $\overline{S(b_{j_1}, q_j)}^{M^*}$ by $\boldsymbol{x}^{\boldsymbol{a}}$ or q_i is zero. Thus we add nothing to L.

This ends Cases 3 and 4. When running Buchberger's algorithm on the list M new polynomials will only be added when in Cases 1 and 3. When the algorithm stops we have added polynomials p_i to the ordered list L such that $\mathrm{lm}(p_i) = \mathrm{lm}(q_i)$ for every q_i added to M during the iterations.

Notice, that the elements in the expanded list L may not be a Gröbner basis for $\langle f_1, f_2, \ldots, f_s, f\rangle$ so we could run Buchberger's algorithm on L to find one. The important facts are that the polynomials p_i added to L are polynomials in $\langle L\rangle$ and for every polynomial q_i added to M when running Buchberger's algorithm on M, there exists a $p_i \in L$ such that $\mathrm{lm}(p_i) = \mathrm{lm}(q_i)$.

Thus observation 3 on page 21 holds, i.e. $\Delta_{\prec}(f_1, f_2, \ldots, f_s, g) \subseteq \Delta_{\prec}(b_1, b_2, \ldots, b_s, \boldsymbol{x}^{\boldsymbol{a}})$ holds. □

Lemma 3.6 has the following corollary which follows by letting $f_i'(x_1, x_2, \ldots, x_m) = 0$, for all $i = 1, 2, \ldots, s$.

Corollary 3.7 *Let $\mathbb{F}_q[x_1, x_2, \ldots, x_m]/I$ be an order domain with Gröbner basis $G = \{f_1, f_2, \ldots, f_s\}$ as described in Theorem 2.39 and let $\mathcal{B}(G) = \{b_1, b_2, \ldots b_s\}$ be the binomial part of G as in Definition 2.40.*

Let g be a polynomial in $\mathbb{F}_q[x_1, x_2, \ldots, x_m]$, let $lm(g) = \boldsymbol{x}^{\boldsymbol{a}}$ with respect to $\prec_w$ and assume that $\mathrm{Supp}(g) \subseteq \Delta_{\prec_w}(\langle f_1, f_2, \ldots, f_s\rangle)$. *Then*

$$\Delta_{\prec_w}(\langle b_1, b_2, \ldots, b_s, g\rangle) \subseteq \Delta_{\prec_w}(\langle b_1, b_2, \ldots, b_s, \boldsymbol{x}^{\boldsymbol{a}}\rangle). \tag{3.12}$$

We expect the inclusion

$$\Delta_{\prec_w}(\langle f_1, f_2, \ldots, f_s, g\rangle) \subseteq \Delta_{\prec_w}(\langle b_1, b_2, \ldots, b_s, g\rangle) \tag{3.13}$$

to hold as well but a proof similar to the one given for Lemma 3.6 requires us to keep track of additional S-polynomials of the form $S(g, q_j)$ as well (which is not an easy task). In Chapter 6 we will show that for a special kind of ideals the equality in (3.12) holds and the inclusion in (3.13) then follows from Lemma 3.6, i.e. for this special kind of ideals [4, Lemma 1] holds.

4. A Gröbner basis theoretical approach to codes from order domains

The main result given as Theorem 4.4 in Section 4.1 is presented in [2, Thm. 2] in a more general setting which includes generalized Hamming weights but the presentation and proof given here relies only on Gröbner basis theoretical methods while the more general result in [2] relies on the notion of a weakly well-behaving basis. The results given here were published in [4] which is a predecessor of [3] and [2].

4.1. Defining evaluation codes

First we need a few definitions. The first one is from [4, Def. 6].

Definition 4.1 *Let $\mathbb{F}_q[x_1, x_2, \ldots, x_m]/I$ be an order domain as in Theorem 2.39 with Gröbner basis $G = \{f_1, f_2, \ldots, f_s\}$ and let $\mathcal{B}(G) = \{b_1, b_2, \ldots, b_s\}$ be the binomial part of G. For any monomial $\boldsymbol{x}^{\boldsymbol{a}} \in \mathcal{M}_m$ define*

$$
\begin{aligned}
S(\boldsymbol{x}^{\boldsymbol{a}}) &= \Delta_{\prec_w}\left(\langle b_1, b_2, \ldots, b_s, \boldsymbol{x}^{\boldsymbol{a}}\rangle\right), \\
\hat{S}(\boldsymbol{x}^{\boldsymbol{a}}) &= S(\boldsymbol{x}^{\boldsymbol{a}}) \cap \Delta_{\prec_w}\left(\langle x_1^q - x_1, x_2^q - x_2, \ldots, x_m^q - x_m\rangle\right), \\
\tilde{S}(\boldsymbol{x}^{\boldsymbol{a}}) &= S(\boldsymbol{x}^{\boldsymbol{a}}) \cap \Delta_{\prec_w}\left(\langle f_1, f_2, \ldots, f_s, x_1^q - x_1, x_2^q - x_2, \ldots, x_m^q - x_m\rangle\right)
\end{aligned}
$$

and let $D(\boldsymbol{x}^{\boldsymbol{a}}) = \#S(\boldsymbol{x}^{\boldsymbol{a}})$, $\hat{D}(\boldsymbol{x}^{\boldsymbol{a}}) = \#\hat{S}(\boldsymbol{x}^{\boldsymbol{a}})$ and $\tilde{D}(\boldsymbol{x}^{\boldsymbol{a}}) = \#\tilde{S}(\boldsymbol{x}^{\boldsymbol{a}})$.

The following theorem, which is [4, Thm. 3], makes it possible to use Proposition 2.25 to give a lower bound on minimum distances in Theorem 4.4.

Theorem 4.2 *Let $\mathbb{F}_q[x_1, x_2, \ldots, x_m]/I$ be an order domain as in Theorem 2.39, let f be a polynomial in $\mathbb{F}_q[x_1, x_2, \ldots, x_m]$, let $lm(f) = \boldsymbol{x}^{\boldsymbol{a}}$ with respect to $\prec_w$, let $\mathrm{Supp}(f) \subseteq \Delta_{\prec_w}\left(\langle f_1, f_2, \ldots, f_s, x_1^q - x_1, x_2^q - x_2, \ldots, x_m^q - x_m\rangle\right)$ and let $S(\boldsymbol{x}^{\boldsymbol{a}}), \hat{S}(\boldsymbol{x}^{\boldsymbol{a}})$ and $\tilde{S}(\boldsymbol{x}^{\boldsymbol{a}})$ be defined as in Definition 4.1. Then the following holds*

$$
\Delta_{\prec_w}\left(\langle f_1, f_2, \ldots, f_s, x_1^q - x_1, x_2^q - x_2, \ldots, x_m^q - x_m, f\rangle\right) \subseteq \tilde{S}(\boldsymbol{x}^{\boldsymbol{a}}) \subseteq \hat{S}(\boldsymbol{x}^{\boldsymbol{a}}) \subseteq S(\boldsymbol{x}^{\boldsymbol{a}}).
$$

Proof: The first inclusion follows from Lemma 3.6, Definition 4.1 and observation 3 on page 21, since

$$
\begin{aligned}
&\Delta_{\prec_w}\left(\langle f_1, f_2, \ldots, f_s, x_1^q - x_1, x_2^q - x_2, \ldots, x_m^q - x_m, f\rangle\right) \\
&\qquad\qquad \subset \Delta_{\prec_w}\left(\langle f_1, f_2, \ldots, f_s, x_1^q - x_1, x_2^q - x_2, \ldots, x_m^q - x_m\rangle\right),
\end{aligned}
$$

using observation 3, and

$$\begin{aligned}&\Delta_{\prec_w}\left(\langle f_1, f_2, \ldots, f_s, x_1^q - x_1, x_2^q - x_2, \ldots, x_m^q - x_m, f\rangle\right)\\ &\qquad\subseteq \Delta_{\prec_w}\left(\langle f_1, f_2, \ldots, f_s, f\rangle\right) \subseteq \Delta_{\prec_w}\left(\langle b_1, b_2, \ldots, b_s, \boldsymbol{x}^{\boldsymbol{a}}\rangle\right),\end{aligned}$$

using observation 3 and Lemma 3.6. The remaining inclusions follows from Definition 4.1. □

Proposition 2.25 and Theorem 4.2 motivates the following definition from [4, Def. 7].

Definition 4.3 *Let $\mathbb{F}_q[x_1, x_2, \ldots, x_m]/I$ be an order domain as in Theorem 2.39 and let $I_q = I + \langle x_1^q - x_1, x_2^q - x_2, \ldots, x_m^q - x_m\rangle$. Define*

$$\begin{aligned}F(t) &= \mathit{Span}_{\mathbb{F}_q}\left\{\varphi(\boldsymbol{x}^{\boldsymbol{a}}) \mid \boldsymbol{x}^{\boldsymbol{a}} \in \Delta_{\prec_w}(I_q), D(\boldsymbol{x}^{\boldsymbol{a}}) \leqslant t\right\}\\ \hat{F}(t) &= \mathit{Span}_{\mathbb{F}_q}\left\{\varphi(\boldsymbol{x}^{\boldsymbol{a}}) \mid \boldsymbol{x}^{\boldsymbol{a}} \in \Delta_{\prec_w}(I_q), \hat{D}(\boldsymbol{x}^{\boldsymbol{a}}) \leqslant t\right\}\\ \tilde{F}(t) &= \mathit{Span}_{\mathbb{F}_q}\left\{\varphi(\boldsymbol{x}^{\boldsymbol{a}}) \mid \boldsymbol{x}^{\boldsymbol{a}} \in \Delta_{\prec_w}(I_q), \tilde{D}(\boldsymbol{x}^{\boldsymbol{a}}) \leqslant t\right\}\end{aligned}$$

where $\prec_w$ denotes the monomial order from Definition 2.19 and φ is the evaluation map from Definition 2.41.

A lower bound on the minimum distance of the codes in Definition 4.3 is given in Theorem 4.4, which is from [4, Thm. 4].

Theorem 4.4 *The minimum distances of the codes F, $\hat{F}$ and $\tilde{F}$ are bounded by:*

$$\begin{aligned}&d(F(t)) \geqslant n - \max\left\{\tilde{D}(\boldsymbol{x}^{\boldsymbol{a}}) \mid D(\boldsymbol{x}^{\boldsymbol{a}}) \leqslant t\right\} \geqslant n - \max\left\{\hat{D}(\boldsymbol{x}^{\boldsymbol{a}}) \mid D(\boldsymbol{x}^{\boldsymbol{a}}) \leqslant t\right\} \geqslant n - t\\ &d(\hat{F}(t)) \geqslant n - \max\left\{\tilde{D}(\boldsymbol{x}^{\boldsymbol{a}}) \mid \hat{D}(\boldsymbol{x}^{\boldsymbol{a}}) \leqslant t\right\} \geqslant n - t\\ &d(\tilde{F}(t)) \geqslant n - t.\end{aligned}$$

Proof: Consider the bound $d(\tilde{F}(t)) \geqslant n - t$. Let $I_q = \langle f_1, f_2, \ldots, f_s, x_1^q - x_1, x_2^q - x_2, \ldots, x_m^q - x_m\rangle$ as in Definition 4.3 and $\mathbb{V}_{\mathbb{F}_q}(I_q) = \{\boldsymbol{p} \in \mathbb{F}_q^m \mid g(\boldsymbol{p}) = 0, \text{ for all } g \in I_q\}$ and $\#\mathbb{V}(I_q) = n$.

Then a codeword $\boldsymbol{c} \in \tilde{F}(t)$ is constructed as $\varphi(f)$, for some polynomial f, where $\mathrm{Supp}(f) \in \Delta_{\prec_w}(I_q)$ and $\varphi : \mathbb{V}(I_q) \to \mathbb{F}_q^n$ is the evaluation map from Definition 2.41.

This means that the number of zeroes in $\boldsymbol{c}$ is upper bounded by the number of elements in the set $\{\boldsymbol{p} \in \mathbb{V}(I_q) \mid f(\boldsymbol{p}) = 0\}$, which again (using Proposition 2.25) is upper bounded by $\#\Delta_{\prec_w}(I_q + \langle f\rangle) \leqslant t$, where the last equality follows from Definition 4.3, Theorem 4.2 and Definition 4.1.

Also, from Theorem 4.2 and Definition 4.1 it follows that $\tilde{D}(\boldsymbol{x}^{\boldsymbol{a}}) \leqslant \hat{D}(\boldsymbol{x}^{\boldsymbol{a}}) \leqslant D(\boldsymbol{x}^{\boldsymbol{a}})$, thus the remaining two bounds holds. □

The result regarding $\tilde{F}(t)$ in Theorem 4.4 corresponds to the result in [2, Thm. 3] ,i.e. $\tilde{D}(\boldsymbol{x}^{\boldsymbol{a}}) = \sigma(w(\boldsymbol{x}^{\boldsymbol{a}}))$, for $\boldsymbol{x}^{\boldsymbol{a}} \in \Delta_{\prec_w}(I_q)$. This result is stated as Proposition 9 in the appendix of [2] (included as Proposition 8.41 in Part B), where the proof is given.

Notice, that the set $\{B_1, B_2, \ldots, B_s\}$ in the proof of Proposition 8.41 is different than the set we have called the binomial part in Part A and in [4], but a proof similar to the one given for Lemma 3.5 can be given to show that the set $\{B_1, B_2, \ldots, B_s\}$ in Proposition 8.41 is a Gröbner basis for the ideal $\langle B_1, B_2, \ldots, B_s \rangle$.

Regarding the $\hat{F}(t)$ codes examples have shown that they tend to have parameters very close to those of the $F(t)$ codes. See [4, Ex. 2] for an example.

5. Evaluation codes from a special class of order domains

In this chapter we will present a special class of order domains and a different approach than the one taken in Chapter 4 to bounding the minimum distance of codes from this class of order domains.

5.1. A special class of order domains

The following results regards a special class of order domains on the form in Theorem 2.39 where the two monomials of highest weight in the polynomials f_i generating I are monomials in one variable and where the weights of monomials are positive integers as in Example 2.3. Theorem 5.1 is from [4, Thm. 5].

Theorem 5.1 *Given positive integers $\alpha_1, \beta_1, \alpha_2, \beta_2, \ldots, \alpha_{m-1}, \beta_{m-1}$ such that $gcd(\alpha_i, \beta_j) = 1$ whenever $i \leqslant j$. Define weights $w(x_r) = \prod_{i=1}^{r-1} \alpha_i \cdot \prod_{j=r}^{m-1} \beta_j$ for $r = 1, 2, \ldots, m$, where the empty product is defined to be 1, and let $\prec_w$ be the monomial order from Definition 2.19 with $\prec_{\mathcal{M}_m} = \prec_{lex}$ and $x_1 \prec_{lex} x_2 \prec_{lex} \cdots \prec_{lex} x_m$.*

For $r = 1, 2, \ldots m-1$ let the polynomials $f_r = x_r^{\alpha_r} - x_{r+1}^{\beta_r} + f'_r(x_1, x_2, \ldots, x_m) \in \mathbb{F}_q[x_1, x_2, \ldots, x_m]$ be such that $w(x_r^{\alpha_r}) = w(x_{r+1}^{\beta_r}) > \mathrm{wdeg}(f'_r(x_1, x_2, \ldots, x_m))$.

Let $I = \langle f_1, f_2, \ldots, f_{m-1} \rangle$, then the following holds:

(1) The factor ring $\mathbb{F}_q[x_1, x_2, \ldots, x_m]/I$ is an order domain as described in Theorem 2.39.

(2) For any monomial $\boldsymbol{x}^{\boldsymbol{a}} \in \Delta_{\prec_w}(I)$ we have $D(\boldsymbol{x}^{\boldsymbol{a}}) \leqslant w(\boldsymbol{x}^{\boldsymbol{a}})$, where $D(\boldsymbol{x}^{\boldsymbol{a}})$ is from Definition 4.1.

The result in (1) in Theorem 5.1 is proven now and the proof of (2) is postponed until the end of this chapter.

Proof of Theorem 5.1 (1):

From the construction of $f_1, f_2, \ldots, f_{m-1}$ and the definition of $\prec_w$ it follows that $lm(f_r) = x_{r+1}^{\beta_r}$. Since $x_{i+1}^{\beta_i}$ and $x_{j+1}^{\beta_j}$ are relatively prime, for $i \neq j$, it follows from Proposition 2.35 that $\{f_1, f_2, \ldots, f_{m-1}\}$ is a Gröbner basis for I, which by construction meets the condition in Theorem 2.39. Then

$$\Delta_{\prec_w}(I) = \left\{ x_1^{a_1} x_2^{a_2} \cdots x_m^{a_m} \in \mathcal{M}_m \;\middle|\; 0 \leqslant a_i < \beta_{i-1} \text{ for } i = 2, 3, \ldots, m \right\}.$$

The factor ring $\mathbb{F}_q[x_1, x_2, \ldots, x_m]/I$ is an order domain, using Theorem 2.39, with weight function $\rho([f]) = w(\bar{f})$, for $[f] \in \mathbb{F}_q[x_1, x_2, \ldots, x_m]/I$ where $\bar{f}$ denotes the standard representative for $[f]$, if we can prove that the monomials in $\Delta_{\prec_w}(I)$ have mutually distinct weights.

We will prove this by induction in the number of variables m.

Basis: $m = 2$

Here $w(x_1) = \beta_1, w(x_2) = \alpha_1$ and $gcd(\alpha_1, \beta_1) = 1$. Let $x_1^{u_1}x_2^{u_2}, x_1^{v_1}x_2^{v_2} \in \Delta_{\prec_w}(I)$ be such that $w(x_1^{u_1}x_2^{u_2}) = w(x_1^{v_1}x_2^{v_2})$. This means that $(u_1 - v_1)\beta_1 = (v_2 - u_2)\alpha_1$. Since $v_2, u_2 < \beta_1$ and $\mathrm{lcm}(\alpha_1, \beta_1) = \alpha_1\beta_1$ then $v_2 = u_2$ is the only possibility. Thus $u_1 = v_1$ and $x_1^{u_1}x_2^{u_2} = x_1^{v_1}x_2^{v_2}$ holds.

Step: $m \geqslant 2$

Assume that in m variables the monomials in $\Delta_{\prec_w}(I)$ all have mutually distinct weights, i.e. whenever $w(x_1^{u_1}x_2^{u_2}\cdots x_m^{u_m}) = w(x_1^{v_1}x_2^{v_2}\cdots x_m^{v_m})$, for $\boldsymbol{x}^{\boldsymbol{u}}, \boldsymbol{x}^{\boldsymbol{v}} \in \Delta_{\prec_w}(I)$, then $u_r = v_r$, for all $r = 1, 2, \ldots, m$.

We will show that this also holds for $m + 1$ variables. Let $w_m(x_r)$ denote the weight of x_r in the case of m variables, for $r = 1, 2, \ldots, m$, and notice that from the definition of the weights we have $w_{m+1}(x_r) = \beta_m \cdot w_m(x_r)$, for all $r = 1, 2, \ldots, m$, and $w_{m+1}(x_{m+1}) = \prod_{r=1}^{m} \alpha_r$.

Let $x_1^{u_1}x_2^{u_2}\cdots x_m^{u_m}x_{m+1}^{u_{m+1}}$ and $x_1^{v_1}x_2^{v_2}\cdots x_m^{v_m}x_{m+1}^{v_{m+1}}$ be two monomials in $\Delta_{\prec_w}(I)$ (in the case of $m + 1$ variables) such that

$$w_{m+1}(x_1^{u_1}x_2^{u_2}\cdots x_m^{u_m}x_{m+1}^{u_{m+1}}) = w_{m+1}(x_1^{v_1}x_2^{v_2}\cdots x_m^{v_m}x_{m+1}^{v_{m+1}}),$$

which can be rewritten as

$$\left(w_m(x_1^{u_1}x_2^{u_2}\cdots x_m^{u_m}) - w_m(x_1^{v_1}x_2^{v_2}\cdots x_m^{v_m})\right)\beta_m = (v_{m+1} - u_{m+1})\prod_{r=1}^{m} \alpha_r.$$

Since $gcd(\alpha_r, \beta_m) = 1$, for $r \leqslant m$, and $v_{m+1}, u_{m+1} < \beta_m$, we have $v_{m+1} = u_{m+1}$ as the only possibility. Thus $w_m(x_1^{u_1}x_2^{u_2}\cdots x_m^{u_m}) = w_m(x_1^{v_1}x_2^{v_2}\cdots x_m^{v_m})$ must hold and, by the induction hypothesis, this means that $u_r = v_r$, for $r = 1, 2, \ldots, m$.

This proves part (1) of the theorem. □

The proof of (2) in Theorem 5.1 is postponed until the end of the chapter, because we need the results in the next section to prove it.

5.2. An attempt to improve the bound in Theorem 4.4

We could use the factor ring in Theorem 5.1 to construct codes as in Definition 4.3 and then use Theorem 4.4 to give a bound on their minimum distance but in this section we try another approach to bounding the minimum distance.

Notice, that one key element in the bounds in Theorem 4.4 is the sequence of inclusions in Theorem 4.2 but the definition of $\tilde{S}(\boldsymbol{x}^{\boldsymbol{a}})$ in Definition 4.1 may seem rather unnatural.

The question is: Can we do better by estimating the size of

$$\Delta_{\prec_w}\left(f_1, f_2, \ldots, f_s, x_1^q - x_1, x_2^q - x_2, \ldots, x_m^q - x_m, f\right)$$

directly by some (hopefully simple) function used on the polynomial f? Such an attempt on making a function Ω is made in this section.

First, by using observation 3 on page 21 we have that

$$\Delta_{\prec_w}\left(f_1, f_2, \ldots, f_s, x_1^q - x_1, x_2^q - x_2, \ldots, x_m^q - x_m, f\right) \subseteq \Delta_{\prec_w}\left(f_1, f_2, \ldots, f_s, f\right), \quad (5.1)$$

where equality might hold.

We would also like to find a way to estimate the size of the right hand side of (5.1) without having to run Buchberger's algorithm on the ordered list $L = (f_1, f_2, \ldots, f_s, f)$, since running Buchberger's algorithm might take a long time - even on a computer.[1]

The results shown below are based on the study of how Buchberger's algorithm in Section 3.2 constructs a Gröbner basis for an ideal $\langle f_1, f_2, \ldots, f_s, f\rangle$ and, in particular, how the division algorithm in Section 3.1 constructs $\overline{S(f_i, f)}^L$ but before going into details we will try to explain where our function Ω given in Definition 5.2 comes from and what we aim to do.

Let I be an ideal as in Theorem 5.1 with Gröbner basis $G = \{f_1, f_2, \ldots, f_{m-1}\}$, where

$$f_r = x_r^{\alpha_r} - x_{r+1}^{\beta_r} + f_r'(x_1, x_2, \ldots, x_m), \quad (5.2)$$

for $r = 1, 2, \ldots, m-1$. Furthermore, let $w(x_r)$, for all r, and $\prec_w$ be defined as in Theorem 5.1, i.e. $\mathrm{lm}(f_r) = x_{r+1}^{\beta_r}$, for all r. Let $f = \boldsymbol{x}^{\boldsymbol{a}} + f'(x_1, x_2, \ldots, x_m)$ be a polynomial in $\mathbb{F}_q[x_1, x_2, \ldots, x_m]$ such that $\mathrm{Supp}(f) \in \Delta_{\prec_w}(I)$ and $\mathrm{lm}(f) = \boldsymbol{x}^{\boldsymbol{a}} = x_1^{a_1} x_2^{a_2} \cdots x_m^{a_m}$.

If we construct $S(f_{k-1}, f)$, where $2 \leqslant k \leqslant m$, we then have

$$\begin{aligned} S(f_{k-1}, f) = {} & \frac{x_1^{a_1} x_2^{a_k} \cdots x_{k-1}^{a_{k-1}} x_k^{\beta_{k-1}} x_{k+1}^{a_{k+1}} \cdots x_m^{a_m}}{-x_k^{\beta_{k-1}}} \left(x_{k-1}^{\alpha_{k-1}} - x_k^{\beta_{k-1}} + f_{k-1}'\right) \\ & - \frac{x_1^{a_1} x_2^{a_k} \cdots x_{k-1}^{a_{k-1}} x_k^{\beta_{k-1}} x_{k+1}^{a_{k+1}} \cdots x_m^{a_m}}{x_1^{a_1} x_2^{a_2} \cdots x_m^{a_m}} \left(x_1^{a_1} x_2^{a_2} \cdots x_m^{a_m} + f'\right), \quad (5.3) \end{aligned}$$

which (using Lemma 3.4) has leading monomial

$$x_1^{a_1} x_2^{a_2} \cdots x_{k-2}^{a_{k-2}} x_{k-1}^{a_{k-1}+\alpha_{k-1}} x_{k+1}^{a_{k+1}} \cdots x_m^{a_m}. \quad (5.4)$$

When constructing the remainder of $S(f_{k-1}, f)$ on division by f_{k-2} we get

$$S(f_{k-1}, f) + x_1^{a_1} x_2^{a_k} \cdots x_{k-2}^{a_{k-2}} x_{k-1}^{a_{k-1}+\alpha_{k-1}-\beta_{k-2}} x_{k+1}^{a_{k+1}} \cdots x_m^{a_m} \left(x_{k-2}^{\alpha_{k-2}} - x_{k-1}^{\beta_{k-2}} + f_{k-2}'\right),$$

[1] Cryptosystems based on a set of polynomial equations have been proposed. Such a system might be cracked by running Buchberger's algorithm but the claim is that this is not feasible due to the complexity of the algorithm when working over a large finite field $\mathbb{F}_q, (q \geqslant 2^8)$. See for instance [7] for a reference.

which has leading monomial

$$x_1^{a_1} x_2^{a_2} \cdots x_{k-2}^{a_{k-2}+\alpha_{k-2}} x_{k-1}^{a_{k-1}+\alpha_{k-1}-\beta_{k-1}} x_{k+1}^{a_{k+1}} \cdots x_m^{a_m}$$

by Lemma 3.4.

Now, imagine running the division algorithm on the ordered list $L = (f_{m-1}, f_{m-2}, \ldots, f_1, f)$ (i.e. with the f_r's in reversed order), when constructing the remainder $\overline{S(f_{k-1}, f)}^{L}$. Then, due to the ordering of L, the division algorithm will do division with f_{k-2} exactly $s_{k-2} = \lfloor \frac{a_{k-1}+\alpha_{k-1}}{\beta_{k-2}} \rfloor$ times to construct a polynomial (again using Lemma 3.4 and observation 2 on page 20) with leading monomial

$$x_1^{a_1} x_2^{a_k} \cdots x_{k-2}^{a_{k-2}+s_{k-2}\cdot\alpha_{k-2}} x_{k-1}^{a_{k-1}+\alpha_{k-1}-s_{k-2}\cdot\beta_{k-2}} x_{k+1}^{a_{k+1}} \cdots x_m^{a_m}. \tag{5.5}$$

Then the division algorithm will do division with f_{k-3} exactly $s_{k-3} = \lfloor \frac{a_{k-2}+s_{k-2}\cdot\alpha_{k-2}}{\beta_{k-3}} \rfloor$ times to produce another polynomial, which might be divided with f_{k-4} and so on. We continue this way until we have done all the divisions we can with f_1 and no polynomials $f_r \in L$ divides the result. Call the remainder of these divisions p, i.e. $p = \overline{S(f_{k-1}, f)}^{L^*}$, where $L^* = (f_{m-1}, f_{m-2}, \ldots, f_1)$.

Now, notice the following:

- The constants $a_{k+1}, a_{k+2}, \ldots, a_m$ are not affected by the divisions with the f_r, for $r < k$, due to the structure of f_r in (5.2).
- The leading monomial in f might not divide the leading monomial of p since $lm(f) = \boldsymbol{x}^{\boldsymbol{a}}$ contains the variable $x_k^{a_k}$, where $0 \leqslant a_k < \beta_{k-1}$.
- If f does not divide p then we have found $\overline{S(f_{k-1}, f)}^{L}$. If f divides p then we at least have found a leading monomial in the ideal $\langle f_1, f_2, \ldots, f_{m-1}, f\rangle$, since p is a linear combination of $f_1, f_2, \ldots, f_{m-1}, f$.
- The procedure above is highly systematic, thus we can compute the leading monomial of $\overline{S(f_{k-1}, f)}^{L^*}$ without doing any polynomials divisions. This fact is again due to the structure of the f_r in (5.2), which allows us to eliminate one variable at the time (except x_1 since it is not in a leading monomial of any f_r).
- Since $\mathrm{Supp}(\overline{S(f_{k-1}, f)}^{L^*}) \in \Delta_{\prec_w}(I)$ and $\mathrm{lm}(p) = \mathrm{lm}(\overline{S(f_{k-1}, f)}^{L^*})$ by observation 2 on page 20, we can do this recursively by letting p have the role of f, i.e. by constructing $\overline{S(f_r, p)}^{L^*}$, for some r, as well. Note that $\mathrm{Supp}(p)$ may not be in $\Delta_{\prec_w}(I)$ but using p instead of $\overline{S(f_{k-1}, f)}^{L^*}$ does not affect the leading monomial of the resulting remainder by Lemma 3.4.

Furthermore, given a subset $S \subseteq \{2, 3, \ldots, m\}$ we can construct leading monomials in $\langle f_1, f_2, \ldots, f_{m-1}, f\rangle$ with x_r eliminated, for all $r \in S$. This is true because we can eliminate the variables x_r recursively in decreasing order, where $r \in S$, since the exponents larger than the one of x_r are not affected by the procedure this way, for any $r \in S$.

Now, let T be the set of leading monomials constructed this way, for all possible subsets $S \subseteq \{2, 3, \ldots, m\}$ (including the empty set, i.e. $\mathrm{lm}(f) \in T$). Then the number of elements in $\Delta_{\prec_w}(f_1, f_2, \ldots, f_{m-1}, f)$ is upper bounded by the number of elements in $\Delta_{\prec_w}(\langle T \rangle + \langle \mathrm{lm}(f_1), \mathrm{lm}(f_2), \ldots, \mathrm{lm}(f_{m-1}) \rangle)$ by Remark 2.27. Thus if f is a code polynomial then the number of elements in $\Delta_{\prec_w}(\langle T \rangle + \langle \mathrm{lm}(f_1), \mathrm{lm}(f_2), \ldots, \mathrm{lm}(f_{m-1}) \rangle)$ can be used to bound the minimum weight of the code word $\varphi(f)$ and thereby the minimum distance of the code as in Theorem 4.4, which is our goal.

Hopefully the reader by now has a good idea of what we are about to do, so let us get started and begin by defining a monomial function Ω, which will eliminate the k-th variable from the monomial as described above.

The following definition is from [4, Def. 8].

Definition 5.2 *Let I and $\prec_w$ be as in Theorem 5.1. Let $x_1^{i_1} x_2^{i_2} \cdots x_k^{i_k}$ be a monomial in $\mathcal{M}_m$, where $0 \leqslant i_r < \beta_{r-1}$ for all $r = 2, 3, \ldots, k \leqslant m$.*

Let $j_1, j_2, \ldots, j_{k-1} \in \mathbb{N}_0$ be defined as

$$\begin{aligned}
j_1 &= i_1 + s_1 \cdot \alpha_1 \\
j_2 &= i_2 + s_2 \cdot \alpha_2 - s_1 \cdot \beta_1 \\
&\vdots \\
j_r &= i_r + s_r \cdot \alpha_r - s_{r-1} \cdot \beta_{r-1} \\
j_{r+1} &= i_{r+1} + s_{r+1} \cdot \alpha_{r+1} - s_r \cdot \beta_r \\
&\vdots \\
j_{k-2} &= i_{k-2} + s_{k-2} \cdot \alpha_{k-2} - s_{k-3} \cdot \beta_{k-3} \\
j_{k-1} &= i_{k-1} + \alpha_{k-1} - s_{k-2} \cdot \beta_{k-2},
\end{aligned}$$

where $s_r = \lfloor \frac{i_{r+1} + s_{r+1} \cdot \alpha_{r+1}}{\beta_r} \rfloor$, for $r = k-2, k-3, \ldots, 1$ and $s_{k-1} = 1$. Define Ω to be the monomial function

$$\Omega\left(x_1^{i_1} x_2^{i_2} \cdots x_k^{i_k}\right) = x_1^{j_1} x_2^{j_2} \cdots x_{k-1}^{j_{k-1}}.$$

First we will show that using the function Ω from Definition 5.2 on a monomial in the footprint of I yields another monomial in the same footprint.

Lemma 5.3 *Let I and $\prec_w$ be as in Theorem 5.1 and let $j_1, j_2, \ldots, j_{k-1} \in \mathbb{N}_0$ be the integers from Definition 5.2. Then*

$$0 \leqslant j_r < \beta_{r-1} \quad \text{for} \quad r = 2, 3, \ldots, k-1 < m.$$

Proof: Let j_r and s_r be as in Definition 5.2, for $r = 1, 2, \ldots, k-1$. By definition of j_r we have

$$j_r = i_r + s_r \cdot \alpha_r - s_{r-1} \cdot \beta_{r-1} \tag{5.6}$$

where $s_{r-1} = \lfloor \frac{i_r + s_r \cdot \alpha_r}{\beta_{r-1}} \rfloor$ and $s_{k-1} = 1$.

If $\beta_{r-1} \mid (i_r + s_r \cdot \alpha_r)$ then

$$\frac{i_r + s_r \cdot \alpha_r}{\beta_{r-1}} = s_{r-1} > \frac{i_r + s_r \cdot \alpha_r}{\beta_{r-1}} - 1 \tag{5.7}$$

and if $\beta_{r-1} \nmid (i_r + s_r \cdot \alpha_r)$ then

$$\frac{i_r + s_r \cdot \alpha_r}{\beta_{r-1}} > s_{r-1} > \frac{i_r + s_r \cdot \alpha_r}{\beta_{r-1}} - 1, \tag{5.8}$$

by definition of s_{r-1}.

Using (5.6), (5.7) and (5.8) we have

$$\begin{aligned} j_r &= i_r + s_r \cdot \alpha_r - s_{r-1} \cdot \beta_{r-1} \\ &\geqslant i_r + s_r \cdot \alpha_r - \left(\frac{i_r + s_r \cdot \alpha_r}{\beta_{r-1}} \right) \beta_{r-1} \\ &= i_r + s_r \cdot \alpha_r - i_r - s_r \cdot \alpha_r = 0 \end{aligned}$$

and

$$\begin{aligned} j_r &= i_r + s_r \cdot \alpha_r - s_{r-1} \cdot \beta_{r-1} \\ &< i_r + s_r \cdot \alpha_r - \left(\frac{i_r + s_r \cdot \alpha_r}{\beta_{r-1}} - 1 \right) \beta_{r-1} \\ &= i_r + s_r \cdot \alpha_r - i_r - s_r \cdot \alpha_r + \beta_{r-1} = \beta_{r-1} \end{aligned}$$

which concludes the proof. □

Lemma 5.4 is a key result in this section since it's proof makes the connection between the monomial function Ω in Definition 5.2 and the use of Buchberger's algorithm.

Lemma 5.4 is essentilly a rewritten version of Lemma 2 from the Appendix of [4] and the proof promised in [4] is given below.

Lemma 5.4 *Let I and $\prec_w$ be as in Theorem 5.1 and let $f \in \mathbb{F}_q[x_1, x_2, \ldots, x_m]$ be a polynomial of the form $f = \boldsymbol{x}^{\boldsymbol{i}} - f'(x_1, x_2, \ldots, x_m)$, where Supp$(f) \in \Delta_{\prec_w}(I)$ and $w(\boldsymbol{x}^{\boldsymbol{i}}) > \mathrm{wdeg}(f'(x_1, x_2, \ldots, x_m))$. Let $J = I + \langle f \rangle$ and let Ω and j_r, for $r = 1, 2, \ldots, k-1$, be as in Definition 5.2.*

Then for every $k = 2, 3, \ldots, m$ there exists a polynomial $h_{(k)}(x_1, x_2, \ldots, x_m) \in J$ of the form

$$h_{(k)} = x_1^{j_1} x_2^{j_2} \cdots x_{k-1}^{j_{k-1}} \cdot x_{k+1}^{i_{k+1}} \cdots x_m^{i_m} + h'_{(k)}(x_1, x_2, \ldots, x_m),$$

where

$$w\left(x_1^{j_1} x_2^{j_2} \cdots x_{k-1}^{j_{k-1}} \cdot x_{k+1}^{i_{k+1}} \cdots x_m^{i_m} \right) > \mathrm{wdeg}\left(h'_{(k)}(x_1, x_2, \ldots, x_m) \right),$$

with $x_1^{j_1} x_2^{j_2} \cdots x_{k-1}^{j_{k-1}} \cdot x_{k+1}^{i_{k+1}} \cdots x_m^{i_m} \in \Delta_{\prec_w}(I)$ *and*

$$x_1^{j_1} x_2^{j_2} \cdots x_{k-1}^{j_{k-1}} \cdot x_{k+1}^{i_{k+1}} \cdots x_m^{i_m} = \Omega\left(x_1^{i_1} x_2^{i_2} \cdots x_{k-1}^{i_{k-1}} x_k^{i_k}\right) \cdot x_{k+1}^{i_{k+1}} \cdots x_m^{i_m}.$$

Proof: Let f_r be defined as in Theorem 5.1, for $r = 1, 2, \ldots, m-1$, let f be defined as in the lemma and let k be a fixed integer, where $2 \leqslant k \leqslant m$.

Now, construct the polynomial $p_1 = S(f_{k-1}, f)$ given by

$$\begin{aligned}
p_1 &= S(f_{k-1}, f) \\
&= \frac{x_1^{i_1} \cdots x_{k-1}^{i_{k-1}} x_k^{\beta_{k-1}} x_{k+1}^{i_{k+1}} \cdots x_m^{i_m}}{-x_k^{\beta_{k-1}}} \cdot f_{k-1} - \frac{x_1^{i_1} \cdots x_{k-1}^{i_{k-1}} x_k^{\beta_{k-1}} x_{k+1}^{i_{k+1}} \cdots x_m^{i_m}}{\boldsymbol{x}^{\boldsymbol{i}}} \cdot f \\
&= \frac{x_1^{i_1} \cdots x_{k-1}^{i_{k-1}} x_k^{\beta_{k-1}} x_{k+1}^{i_{k+1}} \cdots x_m^{i_m}}{-x_k^{\beta_{k-1}}} \cdot \left(x_{k-1}^{\alpha_{k-1}} - x_k^{\beta_{k-1}} - f'_{k-1}(\boldsymbol{x})\right) \\
&\quad - \frac{x_1^{i_1} \cdots x_{k-1}^{i_{k-1}} x_k^{\beta_{k-1}} x_{k+1}^{i_{k+1}} \cdots x_m^{i_m}}{\boldsymbol{x}^{\boldsymbol{i}}} \cdot \left(\boldsymbol{x}^{\boldsymbol{i}} - f'(\boldsymbol{x})\right) \\
&= -x_1^{i_1} \cdots x_{k-1}^{i_{k-1}+\alpha_{k-1}} x_{k+1}^{i_{k+1}} \cdots x_m^{i_m} \\
&\qquad + x_1^{i_1} \cdots x_{k-1}^{i_{k-1}} x_{k+1}^{i_{k+1}} \cdots x_m^{i_m} \cdot f'_{k-1}(\boldsymbol{x}) + x_k^{\beta_{k-1}-i_k} \cdot f'(\boldsymbol{x}),
\end{aligned}$$

which has $lm(p_1) = x_1^{i_1} \cdots x_{k-1}^{i_{k-1}+\alpha_{k-1}} x_{k+1}^{i_{k+1}} \cdots x_m^{i_m}$ by Lemma 3.4.

Notice that $lm(p_1)$ may not be in $\Delta_{\prec_w}(I)$ since $i_{k-1} + \alpha_{k-1}$ may not be smaller than β_{k-2}. This can be taken care of by finding the remainder of p_1 divided by $f_{k-2} = x_{k-2}^{\alpha_{k-2}} - x_{k-1}^{\beta_{k-2}} - f'_{k-2}(\boldsymbol{x})$ exactly $s_{k-2} = \lfloor \frac{i_{k-1}+\alpha_{k-1}}{\beta_{k-2}} \rfloor$ times, thereby constructing a polynomial p_2 given by

$$\begin{aligned}
p_2 = x_1^{i_1} &\cdots x_{k-2}^{i_{k-2}+s_{k-2}\cdot\alpha_{k-2}} x_{k-1}^{i_{k-1}+s_{k-1}\cdot\alpha_{k-1}-s_{k-2}\cdot\beta_{k-2}} x_{k+1}^{i_{k+1}} \cdots x_m^{i_m} \\
&+ x_1^{i_1} \cdots x_{k-2}^{i_{k-2}+(s_{k-2}-1)\cdot\alpha_{k-2}} x_{k-1}^{i_{k-1}+s_{k-1}\cdot\alpha_{k-1}-s_{k-2}\cdot\beta_{k-2}} x_{k+1}^{i_{k+1}} \cdots x_m^{i_m} \cdot f'_{k-2}(\boldsymbol{x}) \\
&+ x_1^{i_1} \cdots x_{k-2}^{i_{k-2}+(s_{k-2}-2)\alpha_{k-2}} x_{k-1}^{i_{k-1}+s_{k-1}\cdot\alpha_{k-1}-(s_{k-2}-1)\beta_{k-2}} x_{k+1}^{i_{k+1}} \cdots x_m^{i_m} \cdot f'_{k-2}(\boldsymbol{x}) \\
&\vdots \\
&+ x_1^{i_1} \cdots x_{k-2}^{i_{k-2}+\alpha_{k-2}} x_{k-1}^{i_{k-1}+s_{k-1}\cdot\alpha_{k-1}-2\cdot\beta_{k-2}} x_{k+1}^{i_{k+1}} \cdots x_m^{i_m} \cdot f'_{k-2}(\boldsymbol{x}) \\
&+ x_1^{i_1} \cdots x_{k-2}^{i_{k-2}} x_{k-1}^{i_{k-1}+s_{k-1}\cdot\alpha_{k-1}-\beta_{k-2}} x_{k+1}^{i_{k+1}} \cdots x_m^{i_m} \cdot f'_{k-2}(\boldsymbol{x}) \\
&+ x_1^{i_1} \cdots x_{k-1}^{i_{k-1}} x_{k+1}^{i_{k+1}} \cdots x_m^{i_m} \cdot f'_{k-1}(\boldsymbol{x}) + x_k^{\beta_{k-1}-i_k} \cdot f'(\boldsymbol{x})
\end{aligned}$$

where $s_{k-1} = 1$ and $s_{k-2} = \lfloor \frac{i_{k-1}+s_{k-1}\cdot\alpha_{k-1}}{\beta_{k-2}} \rfloor$.

The leading monomial of p_2 is

$$x_1^{i_1} \cdots x_{k-2}^{i_{k-2}+s_{k-2}\cdot\alpha_{k-2}} x_{k-1}^{i_{k-1}+s_{k-1}\cdot\alpha_{k-1}-s_{k-2}\cdot\beta_{k-2}} x_{k+1}^{i_{k+1}} \cdots x_m^{i_m}, \tag{5.9}$$

using Lemma 3.4 and observation 2 on page 20. Furthermore, notice that $w(lm(p_2)) = w(lm(p_1))$.

We continue to construct polynomials p_{r+1} as the remainder on division of p_r by the polynomial f_{k-r-1} exactly s_{k-r-1} times, for $r = 1, 2, \ldots, k-2$, until we get the polynomial p_{k-1} given by

$$\begin{aligned} p_{k-1} &= x_1^{i_1+s_1\cdot\alpha_1} x_2^{i_2+s_2\cdot\alpha_2-s_1\cdot\beta_3} \cdots x_{k-2}^{i_{k-2}+s_{k-2}\cdot\alpha_{k-2}-s_{k-3}\cdot\beta_{k-3}} \\ &\quad \cdot x_{k-1}^{i_{k-1}+s_{k-1}\cdot\alpha_{k-1}-s_{k-2}\cdot\beta_{k-2}} x_{k+1}^{i_{k+1}} \cdots x_m^{i_m} \ + \ p'_{k-1}(\boldsymbol{x}) \\ &= x_1^{j_1} x_2^{j_2} \cdots x_{k-1}^{j_{k-1}} x_{k+1}^{i_{k+1}} \cdots x_m^{i_m} \ + \ p'_{k-1}(\boldsymbol{x}) \\ &= \Omega\left(x_1^{i_1} \cdots x_k^{i_k}\right) \cdot x_{k+1}^{i_{k+1}} \cdots x_m^{i_m} \ + \ p'_{k-1}(\boldsymbol{x}), \end{aligned}$$

where $j_1, j_2, \ldots, j_{k-1}$ and the function Ω are from Definition 5.2. Furthermore, using Lemma 3.4 and observation 2 on page 20 we have that

$$lm(p_{k-1}) = x_1^{j_1} x_2^{j_2} \cdots x_{k-1}^{j_{k-1}} x_{k+1}^{i_{k+1}} \cdots x_m^{i_m} = \Omega\left(x_1^{i_1} \cdots x_k^{i_k}\right) \cdot x_{k+1}^{i_{k+1}} \cdots x_m^{i_m}$$

since $w(lm(p_1)) = w(lm(p_2)) = \cdots = w(x_1^{j_1} x_2^{j_2} \cdots x_{k-1}^{j_{k-1}} x_{k+1}^{i_{k+1}} \cdots x_m^{i_m}) > w(p'_{k-1}(\boldsymbol{x}))$, where the equalities are due to the structure of f_r, for $r = 1, 2, \ldots, k-1$, i.e. because f_r has two monomials of highest weight in it's support.

Let $h_{(k)} = p_{k-1}$, then the polynomial $h_{(k)}$ is in J since it is a linear combination of $f_1, f_2, \ldots, f_{m-1}, f$. Furthermore, using Lemma 5.3 $lm(h_{(k)}) \in \Delta_{\prec_w}(I)$ holds. □

As explained in the beginning of this section we would like to be able to do the following: Given a subset $S \subseteq \{2, 3, \ldots, m\}$ we want to construct leading monomials in $\langle f_1, f_2, \ldots, f_{m-1}, f\rangle$ with x_r eliminated, for all $r \in S$. The following corollary of Lemma 5.4 allows us to do exactly that.

Corollary 5.5 *Let I and $\prec_w$ be as in Theorem 5.1 and let $f \in \mathbb{F}_q[x_1, x_2, \ldots, x_m]$ be a polynomial of the form $f = \boldsymbol{x}^{\boldsymbol{i}} - f'(x_1, x_2, \ldots, x_m)$, where $Supp(f) \in \Delta_{\prec_w}(I)$ and $w(\boldsymbol{x}^{\boldsymbol{i}}) > \mathrm{wdeg}(f'(x_1, x_2, \ldots, x_m))$. Let $J = I + \langle f\rangle$.*

For every subset $S \subseteq \{2, 3, \ldots, m\}$ there exists a polynomial $h_{(S)}(x_1, x_2, \ldots, x_m) \in J$ on the form

$$h_{(S)} = x_1^{k_1} x_2^{k_2} \cdots x_m^{k_m} + h'_{(S)}(x_1, x_2, \ldots, x_m),$$

where

$$w\left(x_1^{k_1} x_2^{k_2} \cdots x_m^{k_m}\right) > \mathrm{wdeg}\left(h'_{(S)}(x_1, x_2, \ldots, x_m)\right),$$

where $x_1^{k_1} x_2^{k_2} \cdots x_m^{k_m} \in \Delta_{\prec_w}(I)$ and where $k_r = 0$, for every $r \in S$.

Proof: The result follows by using Lemma 5.4 recursively as explained in the beginning of this section. That is: Given a subset $S = \{l_1, l_2, \ldots, l_t\} \subseteq \{2, 3, \ldots, m\}$ such that $l_1 < l_2 < \cdots < l_t$, we can, by using Lemma 5.4, construct a polynomial $h_{(l_t)}$ such that x_{l_t} has exponent 0 in $\mathrm{lm}(h_{(l_t)})$ and $\mathrm{Supp}(h_{(l_t)}) \in \Delta_{\prec_w}(I)$. Then we can use $h_{(l_t)}$ to construct a polynomial $h_{(l_t, l_{t-1})}$ such that x_{l_t} and $x_{l_{t-1}}$ both have exponent 0 in $\mathrm{lm}(h_{(l_t,l_{t-1})})$ and $\mathrm{Supp}(h_{(l_t,l_{t-1})}) \in \Delta_{\prec_w}(I)$. We continue this way until we have a polynomial $h_{(S)}$ such that $x_{l_1}, x_{l_2}, \ldots, x_{l_t}$ all have exponent 0 in the leading monomial of $h_{(S)}$ and $\mathrm{lm}(h_{(S)}) \in \Delta_{\prec_w}(I)$. This proves the theorem. □

The result in Corollary 5.5 inspires the following definition.

Definition 5.6 *Let I and $\prec_w$ be as in Theorem 5.1 and let $f \in \mathbb{F}_q[x_1, x_2, \ldots, x_m]$ be a polynomial of the form $f = \boldsymbol{x}^{\boldsymbol{i}} - f'(x_1, x_2, \ldots, x_m)$, where Supp$(f) \in \Delta_{\prec_w}(I)$ and $w(\boldsymbol{x}^{\boldsymbol{i}}) > \mathrm{wdeg}(f'(x_1, x_2, \ldots, x_m))$.*

Define the set $H(\boldsymbol{x}^{\boldsymbol{i}})$ by

$$H(\boldsymbol{x}^{\boldsymbol{i}}) = \left\{ lm(h_{(S)}) \;\middle|\; S \subseteq \{2, 3, \ldots, m\} \right\},$$

where $lm(h_{(S)})$ denotes the leading monomial of $h_{(S)}$ from Corollary 5.5 with respect to the monomial ordering $\prec_w$.

Note, that the set $H(\boldsymbol{x}^{\boldsymbol{i}})$ from Definition 5.6 can be constructed by recursively using the function Ω from Definition 5.2 on the monomial $\boldsymbol{x}^{\boldsymbol{i}}$ since neither f' nor any f'_r has any influence on what is the leading monomial of $h_{(S)}$, for all r and all subsets $S \subseteq \{2, 3, \ldots, m\}$.

Our goal is to count the number of elements in $\Delta_w(\langle H(\boldsymbol{x}^{\boldsymbol{i}})\rangle + \langle x_2^{\beta_1}, x_3^{\beta_2}, \ldots, x_m^{\beta_{m-1}}\rangle)$ and use this as our bound as explained in the beginning of this section. It actually turns out that $\#\Delta_w(\langle H(\boldsymbol{x}^{\boldsymbol{i}})\rangle + \langle x_2^{\beta_1}, x_3^{\beta_2}, \ldots, x_m^{\beta_{m-1}}\rangle) = w(\boldsymbol{x}^{\boldsymbol{i}})$ as stated in Lemma 5.8. A key element in the proof of Lemma 5.8 is the following result.

Lemma 5.7 *Let I and $\prec_w$ be as in Theorem 5.1 and let $f \in \mathbb{F}_q[x_1, x_2, \ldots, x_m]$ be a polynomial of the form $f = \boldsymbol{x}^{\boldsymbol{i}} - f'(x_1, x_2, \ldots, x_m)$, where* $\mathrm{Supp}(f) \in \Delta_{\prec_w}(I)$ *and $w(\boldsymbol{x}^{\boldsymbol{i}}) > \mathrm{wdeg}(f'(x_1, x_2, \ldots, x_m))$. Then the following holds for all $m \geqslant 2$:*

$$w\left(\Omega\left(x_1^{i_1} x_2^{i_2} \cdots x_m^{i_m}\right)\right) - w\left(x_1^{i_1} x_2^{i_2} \cdots x_{m-1}^{i_{m-1}}\right) = \alpha_{m-1} \cdot w(x_{m-1}),$$

where Ω is the function from Definition 5.2.

Proof: Let $m \geqslant 2$ be fixed and let I, $w(x_r)$ and i_r be defined as in the lemma, for $r = 1, 2, \ldots, m$, and let j_r and s_r be defined as in Definition 5.2, for $r = 1, 2, \ldots, m-1$.

Consider the difference

$$\begin{aligned}
&w(\Omega(x_1^{i_1}x_2^{i_2}\cdots x_m^{i_m})) - w(x_1^{i_1}x_2^{i_2}\cdots x_{m-1}^{i_{m-1}})\\
&\quad= w(x_1^{j_1}x_2^{j_2}\cdots x_{m-1}^{j_{m-1}}) - w(x_1^{i_1}x_2^{i_2}\cdots x_{m-1}^{i_{m-1}})\\
&\quad= \sum_{r=1}^{m-1}(j_r - i_r)\cdot w(x_r)\\
&\quad= \big(i_1 + s_1\cdot\alpha_1 - i_1\big)\cdot w(x_1)\\
&\qquad\quad + \sum_{r=2}^{m-2}\Big(i_r + s_r\cdot\alpha_r - s_{r-1}\cdot\beta_{r-1} - i_r\Big)\cdot w(x_r)\\
&\qquad\qquad + \big(\alpha_{m-1} - s_{m-2}\cdot\beta_{m-2}\big)\cdot w(x_{m-1}).\\
&\quad= s_1\cdot\alpha_1\cdot w(x_1)\\
&\qquad\quad + \sum_{r=2}^{m-2}\Big(s_r\cdot\alpha_r\cdot w(x_r) - s_{r-1}\cdot\beta_{r-1}\cdot w(x_r)\Big)\\
&\qquad\qquad + \alpha_{m-1}\cdot w(x_{m-1}) - s_{m-2}\cdot\beta_{m-2}\cdot w(x_{m-1}). \qquad (5.10)
\end{aligned}$$

The sum in (5.10) is a telescoping sum including terms $s_r\cdot\alpha_r\cdot w(x_r)$ and $-s_r\cdot\beta_r\cdot w(x_{r+1})$ for all $r = 1,2,\ldots,m-2$. All these terms cancel because $\alpha_r\cdot w(x_r) = w(x_r^{\alpha_r}) = w(x_{r+1}^{\beta_r}) = \beta_r\cdot w(x_{r+1})$ by definition of the polynomials f_r and weights $w(x_r)$. The only term left in (5.10) is then the term $\alpha_{m-1}\cdot w(x_{m-1})$. □

Given an ideal I as in Theorem 5.1 and a polynomial $f\in\mathbb{F}_q[x_1,x_2,\ldots,x_m]$ on the form $f = \boldsymbol{x^i} - f'(x_1,x_2,\ldots,x_m)$, where $\mathrm{Supp}(f)\in\Delta_{\prec_w}(I)$ and $\mathrm{lm}(f) = \boldsymbol{x^i}$, it follows from Corollary 5.5 that the monomials in $H(\boldsymbol{x^i})$ are leading monomials in the ideal $I+\langle f\rangle$ so the footprint of $I+\langle f\rangle$ is contained in the footprint of $H(\boldsymbol{x^i})$ by observation 3 on page 21. The following lemma then gives an upper bound on the size of

$$\Delta_w(I+\langle f\rangle)\subseteq\Delta_w(H(\boldsymbol{x^i})+\langle x_2^{\beta_1},x_3^{\beta_2},\ldots,x_m^{\beta_{m-1}}\rangle).$$

Lemma 5.8 is essentially a rewritten version of Lemma 3 from the Appendix of [4] and the proof promised in [4] is given below.

Lemma 5.8 *Let I and $\prec_w$ be as in Theorem 5.1 and let $f\in\mathbb{F}_q[x_1,x_2,\ldots,x_m]$ be a polynomial of the form $f = \boldsymbol{x^i} - f'(x_1,x_2,\ldots,x_m)$, where* $\mathrm{Supp}(f)\in\Delta_{\prec_w}(I)$ *and $w(\boldsymbol{x^i}) > w(f'(x_1,x_2,\ldots,x_m))$.*

Let $T_m\subset\mathbb{F}_q[x_1,x_2,\ldots,x_m]$ be the ideal given by

$$T_m = \big\langle H(\boldsymbol{x^i})\big\rangle + \Big\langle x_2^{\beta_1},x_3^{\beta_2},\ldots,x_m^{\beta_{m-1}}\Big\rangle,$$

where $H(\boldsymbol{x^i})$ is the set from Definition 5.6. Then $\#\Delta_{\prec_w}(T_m) = w(x_1^{i_1}x_2^{i_2}\cdots x_m^{i_m})$.

Proof: The theorem is proven by induction in the number of variables m. Let I, $\prec_w$ and $w(x_r)$ be as in Theorem 5.1, let Ω be the function in Definition 5.2 and let $H(\boldsymbol{x}^{\boldsymbol{i}})$ be the set from Definition 5.6.

Basis:

Let $m = 2$. Then $H(x_1^{i_1}x_2^{i_2}) = \{x_1^{i_1}x_2^{i_2}, \Omega(x_1^{i_1}x_2^{i_2})\} = \{x_1^{i_1}x_2^{i_2}, x_1^{i_1+a_1}\}$ and $T_2 = \langle x_1^{i_1}x_2^{i_2}, x_1^{i_1+a_1}, x_2^{b_1}\rangle$. We now have

$$\begin{aligned}\#\Delta_{\prec_w}(T_2) &= \#\Delta_{\prec_w}\left(\langle x_1^{i_1}x_2^{i_2}, x_1^{i_1+\alpha_1}, x_2^{\beta_1}\rangle\right)\\ &= \beta_1(i_1+\alpha_1) - (i_1+\alpha_1-i_1)(\beta_1-i_2)\\ &= i_1\beta_1 + i_2\alpha_1 = w(x_1^{i_1}x_2^{i_2})\end{aligned}$$

by definition of $w(x_1)$ and $w(x_2)$ in Theorem 5.1.

Step:

Assume that the theorem holds for m variables where $i_r < \beta_{r-1}$ for $r = 2, 3, \ldots, m$. That is $\#\Delta_{\prec}(T_m) = w(x_1^{i_1}x_2^{i_2}\cdots x_m^{i_m})$ for m variables and let $w_m(x_r)$ denote the weight of x_r calculated in the case of m variables, i.e. $w_m(x_r) = \prod_{i=1}^{r-1}\alpha_i \cdot \prod_{j=r}^{m-1}\beta_j$, where the empty product is defined to be 1. Furthermore, let $w_{m+1}(x_r) = \prod_{i=1}^{r-1}\alpha_i \cdot \prod_{j=r}^{m}\beta_j$ denote the weight of x_r in the case of $m+1$ variables and let $i_1, i_2, \ldots, i_m, i_{m+1}$ be fixed.

Consider the set $H(x_1^{i_1}x_2^{i_2}\cdots x_{m+1}^{i_{m+1}})$. It can be divided into two disjoint subsets:

The first subset is the set where we keep $x_{m+1}^{i_{m+1}}$ and then eliminate all possible subsets $S \subseteq \{2, 3, \ldots, m\}$. This is the set given by

$$Q = \left\{\gamma \cdot x_{m+1}^{i_{m+1}} \;\middle|\; \gamma \in H\left(x_1^{i_1}x_2^{i_2}\cdots x_m^{i_m}\right)\right\} \subset H\left(x_1^{i_1}x_2^{i_2}\cdots x_{m+1}^{i_{m+1}}\right). \tag{5.11}$$

Since $x_1^{i_1}x_2^{i_2}\cdots x_m^{i_m}$ is a monomial in m variables in $\Delta_{\prec_w}(I)$, then by the induction hypothesis we have that

$$\#\Delta_{\prec_w}\left(\left\langle H\left(x_1^{i_1}x_2^{i_2}\cdots x_m^{i_m}\right)\right\rangle + \left\langle x_2^{\beta_1}, x_3^{\beta_2}, \ldots, x_m^{\beta_{m-1}}\right\rangle\right) = w_m\left(x_1^{i_1}x_2^{i_2}\cdots x_m^{i_m}\right). \tag{5.12}$$

The second subset is the set where we first eliminate x_{m+1} and then eliminate all possible subsets $S \subseteq \{2, 3, \ldots, m\}$. This is the set given by

$$H\left(\Omega\left(x_1^{i_1}x_2^{i_2}\cdots x_{m+1}^{i_{m+1}}\right)\right) \subset H\left(x_1^{i_1}x_2^{i_2}\cdots x_{m+1}^{i_{m+1}}\right). \tag{5.13}$$

Since $\Omega(x_1^{i_1}x_2^{i_2}\cdots x_{m+1}^{i_{m+1}})$ is a monomial in m variables and, by Lemma 5.3, is in $\Delta_{\prec_w}(I)$, then by the induction hypothesis we have that

$$\begin{aligned}\#\Delta_{\prec_w}&\left(\left\langle H\left(\Omega(x_1^{i_1}x_2^{i_2}\cdots x_{m+1}^{i_{m+1}})\right)\right\rangle + \left\langle x_2^{\beta_1}, x_3^{\beta_2}, \ldots, x_m^{\beta_{m-1}}\right\rangle\right)\\ &= w_m\left(\Omega(x_1^{i_1}x_2^{i_2}\cdots x_{m+1}^{i_{m+1}})\right).\end{aligned} \tag{5.14}$$

Let $T_{m+1} = \langle H(x_1^{i_1}x_2^{i_2}\cdots x_{m+1}^{i_{m+1}})\rangle + \langle x_2^{\beta_1}, x_3^{\beta_2}, \ldots, x_{m+1}^{\beta_m}\rangle$. Now we have to count the number of elements in $\Delta_{\prec_w}(T_{m+1})$. We will do so by counting the number of monomials in the intersection of the two footprints generated by the two subsets above.

First, consider the set Q in (5.11). Since $x_{m+1}^{i_{m+1}}$ is present in every monomial in Q we have that for every monomial

$$\nu \in \Delta_{\prec_w}\left(\langle H(x_1^{i-1}x_2^{i_2}\cdots x_m^{i_m})\rangle + \langle x_2^{\beta_1}, x_3^{\beta_2}, \ldots, x_m^{\beta_{m-1}}\rangle\right)$$

there exists β_m monomials of the form $\nu \cdot x_{m+1}^a$, where $0 \leqslant a < \beta_m$, in the footprint

$$\Delta_{\prec_w}\left(\langle Q\rangle + \langle x_2^{\beta_1}, x_3^{\beta_2}, \ldots, x_{m+1}^{\beta_m}\rangle\right). \tag{5.15}$$

This is true since multiplying $x_{m+1}^{i_{m+1}}$ on every monomial in $H(x_1^{i-1}x_2^{i_2}\cdots x_m^{i_m})$ does not put any restriction on the monomials in

$$\Delta_{\prec_w}\left(\langle H(x_1^{i-1}x_2^{i_2}\cdots x_m^{i_m})\rangle + \langle x_2^{\beta_1}, x_3^{\beta_2}, \ldots, x_m^{\beta_{m-1}}\rangle\right), \tag{5.16}$$

only the presence of $x_{m+1}^{\beta_m}$ in (5.15) does. Thus we have that the number of elements in (5.15) is at least the number of elements in (5.16) multiplied by β_m, i.e. using (5.12) we have that

$$\#\Delta_{\prec_w}\left(\langle Q\rangle + \langle x_2^{\beta_1}, x_3^{\beta_2}, \ldots, x_{m+1}^{\beta_m}\rangle\right) = w_m\left(x_1^{i_1}x_2^{i_2}\cdots x_m^{i_m}\right)\cdot\beta_m. \tag{5.17}$$

Note, that we have not yet counted the number of elements $x_1^{k_1}x_2^{k_2}\cdots x_m^{k_m}$ in the footprint in (5.15) such that $x_1^{k_1}x_2^{k_2}\cdots x_{m-1}^{k_{m-1}}$ is not in the footprint in (5.16) but where $x_1^{k_1}x_2^{k_2}\cdots x_{m-1}^{k_{m-1}}$ is in the footprint in (5.18). We will count those next.

Now, consider a monomial ν in the footprint

$$\Delta_{\prec_w}\left(\left\langle H\left(\Omega(x_1^{i_1}x_2^{i_2}\cdots x_{m+1}^{i_{m+1}})\right)\right\rangle + \left\langle x_2^{\beta_1}, x_3^{\beta_2}, \ldots, x_m^{\beta_{m-1}}\right\rangle\right) \tag{5.18}$$

but not in the footprint in (5.16). Since no monomial in $H(\Omega(x_1^{i_1}x_2^{i_2}\cdots x_{m+1}^{i_{m+1}}))$ contains the variable x_{m+1}, any monomial of the form $\nu \cdot x_{m+1}^a$, where $0 \leqslant a < \beta_m$, are present in the footprint

$$\Delta_{\prec_w}\left(\left\langle H\left(\Omega(x_1^{i_1}x_2^{i_2}\cdots x_{m+1}^{i_{m+1}})\right)\right\rangle + \left\langle x_2^{\beta_1}, x_3^{\beta_2}, \ldots, x_m^{\beta_{m-1}}, x_{m+1}^{\beta_m}\right\rangle\right). \tag{5.19}$$

But since every monomial in Q contains $x_{m+1}^{i_{m+1}}$ and $Q \subset T_{m+1}$, then the number of monomials in the footprint of (5.19) but not in the footprint (5.15) is

$$i_{m+1}\left(w_m\left(\Omega\left(x_1^{i_1}x_2^{i_2}\cdots x_m^{i_m}x_{m+1}^{i_{m+1}}\right)\right) - w_m\left(x_1^{i_1}x_2^{i_2}\cdots x_m^{i_m}\right)\right) \tag{5.20}$$

by using (5.12) and (5.14). This includes the monomials not counted in (5.17). We have counted every monomial in the intersection of the footprint in (5.15) and the footprint in (5.19) and no other monomials are in $\Delta_{\prec_w}(T_{m+1})$, thus we have that $\#\Delta_{\prec_w}(T_{m+1})$

is the number in (5.17) plus the number in (5.20), i.e.

$$\begin{aligned}
\#\Delta_{\prec}\left(T_{m+1}\right) &= \beta_m \cdot w_m\left(x_1^{i_1}x_2^{i_2}\cdots x_m^{i_m}\right) \\
&\quad + i_{m+1}\left(w_m\left(\Omega\left(x_1^{i_1}x_2^{i_2}\cdots x_m^{i_m}x_{m+1}^{i_{m+1}}\right)\right) - w_m\left(x_1^{i_1}x_2^{i_2}\cdots x_m^{i_m}\right)\right) \\
&= w_{m+1}\left(x_1^{i_1}x_2^{i_2}\cdots x_m^{i_m}\right) + i_{m+1}\cdot\alpha_m\cdot w_m(x_m) \\
&= w_{m+1}\left(x_1^{i_1}x_2^{i_2}\cdots x_m^{i_m}\right) + i_{m+1}\cdot w_{m+1}(x_{m+1}) \\
&= w_{m+1}\left(x_1^{i_1}x_2^{i_2}\cdots x_m^{i_m}x_{m+1}^{i_{m+1}}\right)
\end{aligned}$$

by using Lemma 5.7, using that $\beta_m \cdot w_m(x_r) = w_{m+1}(x_r)$, for $r = 1, 2, \ldots, m$, and using that $\alpha_m \cdot w_m(x_m) = w_{m+1}(x_{m+1})$ by definition of the weights in Theorem 5.1. □

We are now in a position where we can prove Theorem 5.1 (2).

Proof of Theorem 5.1 (2):

Let I and $\prec_w$ be as in Theorem 5.1 and let $f \in \mathbb{F}_q[x_1, x_2, \ldots, x_m]$ be a polynomial of the form $f = \boldsymbol{x}^{\boldsymbol{a}} - f'(x_1, x_2, \ldots, x_m)$, where $Supp(f) \in \Delta_{\prec_w}(I)$ and $w(\boldsymbol{x}^{\boldsymbol{a}}) >$ wdeg$(f'(x_1, x_2, \ldots, x_m))$. Furthermore, let $G = \{f_1, f-2, \ldots, f_s\}$ be the Gröbner basis for I, where $f_r = x_r^{\alpha_r} - x_{r+1}^{\beta_r} + f_r'(x_1, x_2, \ldots, x_m)$, for $r = 1, 2, \ldots, m-1$, and let $\mathcal{B}(G)$ be the binomial part of G.

By observation 1 on page 20 and the construction of polynomials $h_{(S)}$ in Corollary 5.5 it follows that lm$(H_{(S)})$ is also a leding monomial in the ideal $\langle\mathcal{B}(G)\rangle + \langle\boldsymbol{x}^{\boldsymbol{a}}\rangle$, for all subsets $S \subseteq \{2, 3, \ldots, m\}$. Thus the bound in Lemma 5.8 is also a bound on $\#\Delta_{\prec_w}\left(\langle\mathcal{B}(G)\rangle + \langle\boldsymbol{x}^{\boldsymbol{a}}\rangle\right)$ and from Definition 4.1 it then follows that $D(\boldsymbol{x}^{\boldsymbol{a}}) \leqslant w(\boldsymbol{x}^{\boldsymbol{a}})$. This proves (2) in Theorem 5.1. □

Finally, let us end this chapter by giving an example using the method developed here.

Example 5.9 Let $\mathbb{F}_{16} = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^{14}\}$ be a finite field with 16 elements and let $I \subset \mathbb{F}_{16}[x, y, z]$ be an ideal as in Theorem 5.1 with Gröbner basis $G = \{x^5 - y^8 - \alpha y, y^6 - z^7 - \alpha^2 xyz\}$. Let $w(x) = 56, w(y) = 35, w(z) = 30$ and let $x \prec_{lex} y \prec_{lex} z$. Then $\mathcal{B}(G) = \{x^5 - y^8, y^6 - z^7\}$.

Let $g = x^5y^7z^5 - \alpha^4x^5y^2z^5 - x^2yz + \alpha z \in \mathbb{F}_{16}[x, y, z]$. Then

$$\begin{aligned}
H\left(x^5y^7z^5\right) &= \left\{x^5y^7z^5, \Omega(x^5y^7z^5), \Omega(\Omega(x^5y^7z^5)), \Omega(x^5y^7)\cdot z^5\right\} \\
&= \left\{x^5y^7z^5, x^{10}y^5, \Omega(x^{10}y^5), x^{10}z^5\right\} \\
&= \left\{x^5y^7z^5, x^{10}y^5, x^{15}, x^{10}z^5\right\}
\end{aligned}$$

and

$$T_3 = \langle H(x^5y^7z^5)\rangle + \langle y^8, z^7\rangle,$$

where H is from Definition 5.6, T_3 is from Lemma 5.8 and Ω is from Definition 5.2.

Then we have

$$\Delta_{\prec_w}\left(\langle \mathcal{B}(G)\rangle + \langle g\rangle\right) \subseteq \Delta_{\prec_w}\left(T_3\right) = \Delta_{\prec_w}\left(\langle x^5y^7z^5, x^{10}y^5, x^{15}, x^{10}z^5, y^8, z^7\rangle\right)$$

and $\#\Delta_{\prec_w}\left(\langle \mathcal{B}(G)\rangle + \langle g\rangle\right) \leqslant w(x^5y^7z^5) = 5\cdot 56 + 7\cdot 35 + 5\cdot 30 = 675.$ $\triangle$

6. Regarding the use of Buchberger's algorithm on toric ideals

In Chapter 5 it was shown how to construct leading monomials in the ideal I given in Theorem 5.1 without actually constructing S-polynomials and doing polynomial divisions but using the method in Section 5.1 we can not be sure that we found the actual size of the footprint of the ideal generated by the binomial part of a Gröbner basis for I and a polynomial g, $\mathrm{Supp}(g) \in \Delta_{\prec}(I)$.

This chapter is concentrated on the use of Buchberger's algorithm on a class of ideals called toric ideals. Here we prove that the method developed in Chapter 5 actually finds the true size of the footprint, when the ideal generated by the binomial part of a Gröbner basis for I is a toric ideal, since the S-polynomials omitted in Chapter 5 adds nothing new when using Buchberger's algorithm.

6.1. Toric ideals

First we consider an example of what is known as a toric ideal which are usually defined from a set $A = \{\boldsymbol{a}_1, \boldsymbol{a}_2, \ldots, \boldsymbol{a}_m\} \in \mathbb{Z}^r$. See [35, Chap. 4] for details. Here we only consider toric ideals defined from a subset of $\mathbb{N}$.

Definition 6.1 *Let $\mathbb{F}$ be a field and let a set $A = \{a_1, a_2, \ldots, a_m\} \subset \mathbb{N}$ be given. Define a monomial function $w : \mathcal{M}_m \to \mathbb{N}$ by $w(x_1) = a_1, w(x_2) = a_2, \ldots, w(x_m) = a_m$ and $w(x_1^{i_1} x_2^{i_2} \cdots x_m^{i_m}) = \sum_{j=1}^{m} i_j w(x_j)$.*

Let $I \subset \mathbb{F}[x_1, x_2, \ldots, x_m]$ be the ideal generated by the set of binomials F given by

$$F = \{\boldsymbol{x}^{\boldsymbol{i}} - \boldsymbol{x}^{\boldsymbol{j}} \mid w(\boldsymbol{x}^{\boldsymbol{i}}) = w(\boldsymbol{x}^{\boldsymbol{j}}) \text{ for } \boldsymbol{i}, \boldsymbol{j} \in \mathbb{N}_0^m\}.$$

Then $I = \langle F \rangle$ is called the toric ideal related to A.

We need to have a Gröbner basis for the toric ideal in Definition 6.1 since we are going to use the property of a Gröbner basis given in Corollary 2.31 in the proof of Proposition 6.9. We can always find a basis for the toric ideal related to $A = \{w(x_1), w(x_2), \ldots, w(x_m)\}$ as in Definition 6.1 by using the algorithm given in [14, Chap. I.6] and [35, Chap. 4] and then expand it to a Gröbner basis but we need a Gröbner basis of a special form.

Lemma 6.2 *Let $\mathbb{F}$ be a field and let $I \in \mathbb{F}[x_1, x_2, \ldots, x_m]$ be a toric ideal spanned by the binomials in F in Definition 6.1. Let $\boldsymbol{i} = (i_1, i_2, \ldots, i_m), \boldsymbol{j} = (j_1, j_2, \ldots, j_m) \in \mathbb{N}_0^m$ and define the set B as*

$$B = \left\{\boldsymbol{x}^{\boldsymbol{i}} - \boldsymbol{x}^{\boldsymbol{j}} \in F \;\middle|\; \text{either } i_k = 0 \text{ or } j_k = 0 \text{ (or both), for } k = 1, 2, \ldots, m\right\}.$$

Then there exists a finite subset $G = \{b_1, b_2, \ldots, b_s\} \subset B$ which is a Gröbner basis for I.

Proof: That B is a basis for I follows from the observation that any $f = \boldsymbol{x}^{\boldsymbol{i}} - \boldsymbol{x}^{\boldsymbol{j}} \in F$ can be written as $f = \boldsymbol{x}^{\boldsymbol{\delta}}\left(\boldsymbol{x}^{\boldsymbol{i}-\boldsymbol{\delta}} - \boldsymbol{x}^{\boldsymbol{j}-\boldsymbol{\delta}}\right)$ where $\boldsymbol{\delta} = (\delta_1, \delta_2, \ldots, \delta_m) \in \mathbb{N}_0^m$ and $\delta_k = \min\{i_k, j_k\}$, for $1 \leqslant k \leqslant m$, then $\boldsymbol{x}^{\boldsymbol{i}-\boldsymbol{\delta}} - \boldsymbol{x}^{\boldsymbol{j}-\boldsymbol{\delta}} \in B$ holds and since F is a basis for I the set B is a basis for I.

Notice that B contains an infinite number of elements but using Hilbert Basis Theorem ([8, §2.5, Thm. 4]) a finite subset $B' = \{b_1, b_2, \ldots, b_r\} \subset B$ generates the ideal $\langle B \rangle$.

Since every $b_i \in B'$ is of the form $b_i = \boldsymbol{x}^{\boldsymbol{a}_i} - \boldsymbol{x}^{\boldsymbol{b}_i}$, every S-polynomial $S(b_i, b_j)$, for $i \neq j$, will either have two monomials of the same weight in it's support or be zero.

Furthermore, the remainder on division of $S(b_i, b_j)$ by some $b_k \in B'$ again has either two monomials of the same weight in it's support or is zero. Thus expanding B' to be a Gröbner basis for $\langle B \rangle$ will only add polynomials of the form $\boldsymbol{x}^{\boldsymbol{a}_i} - \boldsymbol{x}^{\boldsymbol{b}_i}$. Thus we have a Gröbner basis $G = \{b_1, b_2, \ldots, b_s\}$, where $b_i = \boldsymbol{x}^{\boldsymbol{a}_i} - \boldsymbol{x}^{\boldsymbol{b}_i}$ and $w(\boldsymbol{x}^{\boldsymbol{a}_i}) = w(\boldsymbol{x}^{\boldsymbol{b}_i})$, for all $i = 1, 2, \ldots, s$. □

6.2. On constructing a Gröbner basis

Lemma 6.3 below is a special case of Lemma 3.4 but here we repeat the proof since we need both more details in the result and some notation later on in the proof of Proposition 6.9 at the end of this chapter.

Lemma 6.3 *Let I be a toric ideal as defined in Definition 6.1 having Gröbner basis $G = \{b_1, b_2, \ldots, b_s\}$ as in Lemma 6.2. For $k = 1, 2, \ldots, s$, let $b_k = \boldsymbol{x}^{\boldsymbol{\alpha}_k} - \boldsymbol{x}^{\boldsymbol{\beta}_k}$ and let $lm(b_k) = \boldsymbol{x}^{\boldsymbol{\beta}_k}$ with respect to $\prec_w$ as defined in Definition 2.19.*

Let $g = \boldsymbol{x}^{\boldsymbol{i}} - g'(x_1, x_2, \ldots, x_m)$ be a polynomial in $\mathbb{F}[x_1, x_2, \ldots, x_m]$ such that $\operatorname{wdeg}(g'(x_1, x_2, \ldots, x_m)) < w(\boldsymbol{x}^{\boldsymbol{i}})$ and $\operatorname{Supp}(g) \subset \Delta_{\prec_w}(I)$.

Define the polynomial $P_{(j_1, j_2, \ldots, j_t)}$ recursively as

$$P_{(j_1)} = S(b_{j_1}, g)$$

for some $1 \leqslant j_1 \leqslant s$, and

$$P_{(j_1, j_2, \ldots, j_t)} = S(b_{j_t}, P_{(j_1, j_2, \ldots, j_{t-1})}),$$

for some $1 \leqslant j_t \leqslant s$. Then $P_{(j_1, j_2, \ldots, j_t)}$ is of the form

$$P_{(j_1, j_2, \ldots, j_t)} = \boldsymbol{x}^{\boldsymbol{p}_{j_t}} - \boldsymbol{x}^{\boldsymbol{q}_{j_t} - \boldsymbol{i}} \cdot g'(x_1, x_2, \ldots, x_m) \tag{6.1}$$

or on the form

$$P_{(j_1, j_2, \ldots, j_t)} = -\boldsymbol{x}^{\boldsymbol{p}_{j_t}} + \boldsymbol{x}^{\boldsymbol{q}_{j_t} - \boldsymbol{i}} \cdot g'(x_1, x_2, \ldots, x_m) \tag{6.2}$$

for specific $\boldsymbol{p}_{j_t} = (p_{j_t,1}, p_{j_t,2}, \ldots, p_{j_t,m}), \boldsymbol{q}_{j_t} = (q_{j_t,1}, q_{j_t,2}, \ldots, q_{j_t,m}) \in \mathbb{N}_0^m$ depending only on $b_{j_1}, b_{j_2}, \ldots, b_{j_t}$ and $lm(g)$.

Furthermore, $\mathrm{wdeg}(\boldsymbol{x}^{\boldsymbol{q}_{j_t}-\boldsymbol{i}} \cdot g'(x_1, x_2, \dots, x_m)) < w(\boldsymbol{x}^{\boldsymbol{p}_{j_t}})$ *holds.*

Proof: The lemma is proven by induction in t.
Basis:
When $t = 1$ the polynomial $P_{(j_1)}$ is given by

$$\begin{aligned} P_{(j_1)} &= S(b_{j_1}, g) \\ &= \frac{\boldsymbol{x}^{\boldsymbol{\gamma}_{j_1}}}{-\boldsymbol{x}^{\boldsymbol{\beta}_{j_1}}}\left(\boldsymbol{x}^{\boldsymbol{\alpha}_{j_1}} - \boldsymbol{x}^{\boldsymbol{\beta}_{j_1}}\right) - \frac{\boldsymbol{x}^{\boldsymbol{\gamma}_{j_1}}}{\boldsymbol{x}^{\boldsymbol{i}}}\left(\boldsymbol{x}^{\boldsymbol{i}} - g'(x_1, x_2, \dots, x_m)\right) \\ &= -\boldsymbol{x}^{\boldsymbol{\gamma}_{j_1}-\boldsymbol{\beta}_{j_1}+\boldsymbol{\alpha}_{j_1}} + \boldsymbol{x}^{\boldsymbol{\gamma}_{j_1}-\boldsymbol{i}} \cdot g'(x_1, x_2, \dots, x_m), \end{aligned}$$

where $\boldsymbol{\gamma}_{j_1} = (\gamma_{j_1,1}, \gamma_{j_1,2}, \dots, \gamma_{j_1,m}) \in \mathbb{N}_0^m$ and $\gamma_{j_1,u} = \max\{\beta_{j_1,u}, i_u\}$, for $u = 1, 2, \dots, m$.
Furthermore, we have

$$\mathrm{wdeg}(\boldsymbol{x}^{\boldsymbol{\gamma}_{j_1}-\boldsymbol{i}} \cdot g'(x_1, x_2, \dots, x_m)) < w(\boldsymbol{x}^{\boldsymbol{\gamma}_{j_1}}) = w(\boldsymbol{x}^{\boldsymbol{\gamma}_{j_1}-\boldsymbol{\beta}_{j_1}+\boldsymbol{\alpha}_{j_1}}),$$

because $w(\boldsymbol{x}^{\boldsymbol{\beta}_{j_1}}) = w(\boldsymbol{x}^{\boldsymbol{\alpha}_{j_1}})$ and $\mathrm{wdeg}(g'(x_1, x_2, \dots, x_m)) < w(\boldsymbol{x}^{\boldsymbol{i}})$ by definition of b_{j_1} and g.
Step:
Assume that the lemma holds for $t \geqslant 1$ and

$$P_{(j_1,j_2,\dots,j_t)} = \boldsymbol{x}^{\boldsymbol{p}_{j_t}} - \boldsymbol{x}^{\boldsymbol{q}_{j_t}-\boldsymbol{i}} \cdot g'(x_1, x_2, \dots, x_m).$$

Then for $j_{t+1} \in \{1, 2, \dots, s\}$ we have

$$\begin{aligned} P_{(j_1,j_2,\dots,j_{t+1})} &= S\left(b_{j_{t+1}}, P_{(j_1,j_2,\dots,j_t)}\right) \\ &= \frac{\boldsymbol{x}^{\boldsymbol{\gamma}_{j_{t+1}}}}{-\boldsymbol{x}^{\boldsymbol{\beta}_{j_{t+1}}}}\left(\boldsymbol{x}^{\boldsymbol{\alpha}_{j_{t+1}}} - \boldsymbol{x}^{\boldsymbol{\beta}_{j_{t+1}}}\right) - \frac{\boldsymbol{x}^{\boldsymbol{\gamma}_{j_{t+1}}}}{\boldsymbol{x}^{\boldsymbol{p}_{j_t}}}\left(\boldsymbol{x}^{\boldsymbol{p}_{j_t}} - \boldsymbol{x}^{\boldsymbol{q}_{j_t}-\boldsymbol{i}} \cdot g'(x_1, x_2, \dots, x_m)\right) \\ &= -\boldsymbol{x}^{\boldsymbol{\gamma}_{j_{t+1}}-\boldsymbol{\beta}_{j_{t+1}}+\boldsymbol{\alpha}_{j_{t+1}}} + \boldsymbol{x}^{\boldsymbol{\gamma}_{j_{t+1}}-\boldsymbol{p}_{j_t}+\boldsymbol{q}_{j_t}-\boldsymbol{i}} \cdot g'(x_1, x_2, \dots, x_m), \end{aligned}$$

where $\boldsymbol{\gamma}_{j_{t+1}} = (\gamma_{j_{t+1},1}, \gamma_{j_{t+1},2}, \dots \gamma_{j_{t+1},m}) \in \mathbb{N}_0^m$ and $\gamma_{j_{t+1},u} = \max\{\beta_{j_{t+1},u}, p_{j_t,u}\}$, for $u = 1, 2, \dots, m$. Furthermore, we have that

$$\mathrm{wdeg}\left(\boldsymbol{x}^{\boldsymbol{\gamma}_{j_{t+1}}-\boldsymbol{p}_{j_t}+\boldsymbol{q}_{j_t}-\boldsymbol{i}} \cdot g'(x_1, x_2, \dots, x_m)\right) < w\left(\boldsymbol{x}^{\boldsymbol{\gamma}_{j_{t+1}}}\right) = w\left(\boldsymbol{x}^{\boldsymbol{\gamma}_{j_{t+1}}-\boldsymbol{\beta}_{j_{t+1}}+\boldsymbol{\alpha}_{j_{t+1}}}\right),$$

because $w(\boldsymbol{x}^{\boldsymbol{\beta}_{j_{t+1}}}) = w(\boldsymbol{x}^{\boldsymbol{\alpha}_{j_{t+1}}})$ and $\mathrm{wdeg}(\boldsymbol{x}^{\boldsymbol{q}_{j_t}-\boldsymbol{i}} \cdot g'(x_1, x_2, \dots, x_m)) < w(\boldsymbol{x}^{\boldsymbol{p}_{j_t}})$ using the definition of $b_{j_{t+1}}$ and the induction hypothesis.
The calculations for $P_{(j_1,j_2,\dots,j_t)} = -\boldsymbol{x}^{\boldsymbol{p}_{j_t}} + \boldsymbol{x}^{\boldsymbol{q}_{j_t}-\boldsymbol{i}} \cdot g'(x_1, x_2, \dots, x_m)$ are similar. □

Consider a toric ideal I with Gröbner basis $G = \{b_1, b_2, \dots, b_s\}$ as in Lemma 6.2 where $b_k = \boldsymbol{x}^{\boldsymbol{\alpha}_k} - \boldsymbol{x}^{\boldsymbol{\beta}_k}$, for $k = 1, 2, \dots, s,$, and $lm(b_k) = \boldsymbol{x}^{\boldsymbol{\beta}_k}$ with respect to $\prec_w$.

Now, given a polynomial $g = \boldsymbol{x}^{\boldsymbol{i}} - g'(x_1, x_2, \dots, x_m)$, where $\mathrm{Supp}(g) \in \Delta_{\prec_w}(I)$ and $\mathrm{lm}(g) = \boldsymbol{x}^{\boldsymbol{i}}$, we will prove that the S-polynomials omitted in the method developed in Chapter 5 add nothing new, when running Buchberger's algorithm.

That is: Define polynomials $P_{(j_1,j_2,\dots,j_t)}$ recursively as

$$P_{(j_1)} = S(b_{j_1}, g)$$

for some $1 \leqslant j_1 \leqslant s$, and

$$P_{(j_1,j_2,\dots,j_t)} = S(b_{j_t}, P_{(j_1,j_2,\dots,j_{t-1})}),$$

for some $1 \leqslant j_t \leqslant s$. Then the polynomials in G divides $S(P_{(j_1,j_2,\dots,j_u)}, P_{(k_1,k_2,\dots,k_v)})$ and $S(P_{(l_1,l_2,\dots,l_w)}, g)$ for $1 \leqslant u, v, w \leqslant s$.

In other words: The only S-polynomials that will add something new when running Buchberger's algorithm are $P_{(j_1,j_2,\dots,j_t)}$. This is the statement in Proposition 6.9 which is proven by induction.

The following 5 lemmas ((6.4), (6.5), (6.6), (6.7) and (6.8)) are used to prove the basis in the proof of Proposition 6.9, since they prove that the S-polynomials

$$\begin{aligned}
&S(S(b_j, g), S(b_j, g)),\\
&S(S(b_j, g), g),\\
&S(S(b_{j_2}, S(b_{j_1}, g)), S(b_{k_2}, S(b_{k_1}, g))),\\
&S(S(b_{j_2}, S(b_{j_1}, g)), g)
\end{aligned}$$

and

$$S(S(b_{j_2}, S(b_{j_1}, g)), S(b_k, g))$$

all reduce to zero modulo G.

Lemma 6.4 *Let I be a toric ideal as defined in Definition 6.1 having Gröbner basis $G = \{b_1, b_2, \dots, b_s\}$ as in Lemma 6.2. For $k = 1, 2, \dots, s$, let $b_k = \boldsymbol{x}^{\boldsymbol{\alpha}_k} - \boldsymbol{x}^{\boldsymbol{\beta}_k}$ and let $lm(b_k) = \boldsymbol{x}^{\boldsymbol{\beta}_k}$ with respect to $\prec_w$ as defined in Definition 2.19.*

Let $g = \boldsymbol{x}^{\boldsymbol{i}} - g'(x_1, x_2, \dots, x_m)$ be a polynomial in $\mathbb{F}[x_1, x_2, \dots, x_m]$ such that $\mathrm{wdeg}(g'(x_1, x_2, \dots, x_m)) < w(\boldsymbol{x}^{\boldsymbol{i}})$ *and* $\mathrm{Supp}(g) \subset \Delta_{\prec_w}(I)$.

Let $P_{(j_1)} = S(b_{j_1}, g)$ and $P_{(k_1)} = S(b_{k_1}, g)$. Then the polynomials in G divides $S(P_{(j_1)}, P_{(k_1)})$, for all $1 \leqslant j_1, k_1 \leqslant s$.

Proof: Let $\boldsymbol{\gamma}_{t_1} = (\gamma_{t_1,1}, \gamma_{t_1,2}, \dots, \gamma_{t_1,m}) \in \mathbb{N}_0^m$, where $\gamma_{t_1,u} = \max\{\beta_{t_1,u}, i_u\}$, for $u = 1, 2, \dots, m$ and $t = j, k$. Using this $P_{(t_1)} = S(b_{t_1}, g)$ is given by

$$P_{(t_1)} = S(b_{t_1}, g) = -\omega_{t_1} \boldsymbol{x}^{\boldsymbol{\gamma}_{t_1} - \boldsymbol{\beta}_{t_1} + \boldsymbol{\alpha}_{t_1}} + \boldsymbol{x}^{\boldsymbol{\gamma}_{t_1} - \boldsymbol{i}} \cdot g'(x_1, x_2, \dots, x_m), \tag{6.3}$$

where $lt(P_{(t_1)}) = -\omega_{t_1} \boldsymbol{x}^{\boldsymbol{\gamma}_{t_1} - \boldsymbol{\beta}_{t_1} + \boldsymbol{\alpha}_{t_1}}$, for $t = j, k$, using Lemma 6.3.

Let $j_1 \neq k_1$ (if $j_1 = k_1$ then $S(P_{(j_1)}, P_{(k_1)}) = 0$). Define

$$\begin{aligned}
P &= S(P_{(j_1)}, P_{(k_1)}) \\
&= \frac{\boldsymbol{x}^{\boldsymbol{\delta}}}{-\boldsymbol{x}^{\boldsymbol{\gamma}_{j_1}-\boldsymbol{\beta}_{j_1}+\boldsymbol{\alpha}_{j_1}}}\left(-\boldsymbol{x}^{\boldsymbol{\gamma}_{j_1}-\boldsymbol{\beta}_{j_1}+\boldsymbol{\alpha}_{j_1}} + \boldsymbol{x}^{\boldsymbol{\gamma}_{j_1}-\boldsymbol{i}} \cdot g'(x_1, x_2, \ldots, x_m)\right) \\
&\quad - \frac{\boldsymbol{x}^{\boldsymbol{\delta}}}{-\boldsymbol{x}^{\boldsymbol{\gamma}_{k_1}-\boldsymbol{\beta}_{k_1}+\boldsymbol{\alpha}_{k_1}}}\left(-\boldsymbol{x}^{\boldsymbol{\gamma}_{k_1}-\boldsymbol{\beta}_{k_1}+\boldsymbol{\alpha}_{k_1}} + \boldsymbol{x}^{\boldsymbol{\gamma}_{k_1}-\boldsymbol{i}} \cdot g'(x_1, x_2, \ldots, x_m)\right) \\
&= \boldsymbol{x}^{\boldsymbol{\delta}+\boldsymbol{\beta}_{k_1}-\boldsymbol{\alpha}_{k_1}-\boldsymbol{i}} \cdot g'(x_1, x_2, \ldots, x_m) - \boldsymbol{x}^{\boldsymbol{\delta}+\boldsymbol{\beta}_{j_1}-\boldsymbol{\alpha}_{j_1}-\boldsymbol{i}} \cdot g'(x_1, x_2, \ldots, x_m) \\
&= \left(\boldsymbol{x}^{\boldsymbol{\delta}+\boldsymbol{\beta}_{k_1}-\boldsymbol{\alpha}_{k_1}-\boldsymbol{i}} - \boldsymbol{x}^{\boldsymbol{\delta}+\boldsymbol{\beta}_{j_1}-\boldsymbol{\alpha}_{j_1}-\boldsymbol{i}}\right) \cdot g'(x_1, x_2, \ldots, x_m) \qquad (6.4)
\end{aligned}$$

where $\boldsymbol{\delta} = (\delta_1, \delta_2, \ldots, \delta_m) \in \mathbb{N}_0^m$ and $\delta_u = \max\{\gamma_{j_1,u} - \beta_{j_1,u} + \alpha_{j_1,u}, \gamma_{k_1,u} - \beta_{k_1,u} + \alpha_{k_1,u}\}$, for $1 \leqslant u \leqslant m$.

Now we have

$$w\left(\boldsymbol{x}^{\boldsymbol{\delta}+\boldsymbol{\beta}_{k_1}-\boldsymbol{\alpha}_{k_1}-\boldsymbol{i}}\right) = w\left(\boldsymbol{x}^{\boldsymbol{\delta}-\boldsymbol{i}}\right) = w\left(\boldsymbol{x}^{\boldsymbol{\delta}+\boldsymbol{\beta}_{j_1}-\boldsymbol{\alpha}_{j_1}-\boldsymbol{i}}\right),$$

because $w(\boldsymbol{x}^{\boldsymbol{\beta}_{j_1}}) = w(\boldsymbol{x}^{\boldsymbol{\alpha}_{j_1}})$ and $w(\boldsymbol{x}^{\boldsymbol{\beta}_{k_1}}) = w(\boldsymbol{x}^{\boldsymbol{\alpha}_{k_1}})$ by definition of b_{j_1} and b_{k_1} so the binomial $\left(\boldsymbol{x}^{\boldsymbol{\delta}+\boldsymbol{\beta}_{k_1}-\boldsymbol{\alpha}_{k_1}-\boldsymbol{i}} - \boldsymbol{x}^{\boldsymbol{\delta}+\boldsymbol{\beta}_{j_1}-\boldsymbol{\alpha}_{j_1}-\boldsymbol{i}}\right)$ in (6.4) must be in I using Definition 6.1. Then the polynomials in B must divide $S(P_{(j_1)}, P_{(k_1)})$ since G is a Gröbner basis for I using Lemma 6.2 and Corollary 2.31. □

Lemma 6.5 *Let I be a toric ideal as defined in Definition 6.1 having Gröbner basis $G = \{b_1, b_2, \ldots, b_s\}$ as in Lemma 6.2. For $k = 1, 2, \ldots, s$, let $b_k = \boldsymbol{x}^{\boldsymbol{\alpha}_k} - \boldsymbol{x}^{\boldsymbol{\beta}_k}$ and let $lm(b_k) = \boldsymbol{x}^{\boldsymbol{\beta}_k}$ with respect to $\prec_w$ as defined in Definition 2.19.*

Let $g = \boldsymbol{x}^{\boldsymbol{i}} - g'(x_1, x_2, \ldots, x_m)$ be a polynomial in $\mathbb{F}[x_1, x_2, \ldots, x_m]$ such that $\operatorname{wdeg}(g'(x_1, x_2, \ldots, x_m)) < w(\boldsymbol{x}^{\boldsymbol{i}})$ *and* $\operatorname{Supp}(g) \subset \Delta_{\prec_w}(I)$.

Let $P_{(j_1)} = S(b_{j_1}, g)$. Then the polynomials in G divides $S(P_{(j_1)}, g)$ for all $1 \leqslant j_1 \leqslant s$.

Proof: Let $\boldsymbol{\gamma}_{j_1}$ be defined as in the proof of Lemma 6.4. Then $P_{(j_1)}$ is defined as in (6.3). Let P be defined as

$$\begin{aligned}
P &= S(P_{(j_1)}, g) \\
&= \frac{\boldsymbol{x}^{\boldsymbol{\nu}}}{-\boldsymbol{x}^{\boldsymbol{\gamma}_{j_1}-\boldsymbol{\beta}_{j_1}+\boldsymbol{\alpha}_{j_1}}}\left(-\boldsymbol{x}^{\boldsymbol{\gamma}_{j_1}-\boldsymbol{\beta}_{j_1}+\boldsymbol{\alpha}_{j_1}} + \boldsymbol{x}^{\boldsymbol{\gamma}_{j_1}-\boldsymbol{i}} \cdot g'(x_1, x_2, \ldots, x_m)\right) \\
&\quad - \frac{\boldsymbol{x}^{\boldsymbol{\nu}}}{\boldsymbol{x}^{\boldsymbol{i}}}\left(\boldsymbol{x}^{\boldsymbol{i}} - g'(x_1, x_2, \ldots, x_m)\right) \\
&= \left(\boldsymbol{x}^{\boldsymbol{\nu}-\boldsymbol{i}} - \boldsymbol{x}^{\boldsymbol{\nu}+\boldsymbol{\beta}_{j_1}-\boldsymbol{\alpha}_{j_1}-\boldsymbol{i}}\right) \cdot g'(x_1, x_2, \ldots, x_m),
\end{aligned}$$

where $\boldsymbol{\nu} = (\nu_1, \nu_2, \ldots, \nu_m) \in \mathbb{N}_0^m$ and $\nu_u = \max\{\gamma_{j_1,u} - \beta_{j_1,u} + \alpha_{j_1,u}, i_u\}$ for all $1 \leqslant u \leqslant m$.

Since $w(\boldsymbol{x}^{\boldsymbol{\alpha}_{j_1}}) = w(\boldsymbol{x}^{\boldsymbol{\beta}_{j_1}})$ the binomial $\boldsymbol{x}^{\boldsymbol{\nu}-\boldsymbol{i}} - \boldsymbol{x}^{\boldsymbol{\nu}+\boldsymbol{\beta}_{j_1}-\boldsymbol{\alpha}_{j_1}-\boldsymbol{i}} \in I$ using Definition 6.1 and the polynomials in G must divide P using Lemma 6.2 and Corollary 2.31. □

Lemma 6.6 *Let I be a toric ideal as defined in Definition 6.1 having Gröbner basis $G = \{b_1, b_2, \ldots, b_s\}$ as in Lemma 6.2. For $k = 1, 2, \ldots, s$, let $b_k = \boldsymbol{x}^{\boldsymbol{\alpha}_k} - \boldsymbol{x}^{\boldsymbol{\beta}_k}$ and let $lm(b_k) = \boldsymbol{x}^{\boldsymbol{\beta}_k}$ with respect to $\prec_w$ as defined in Definition 2.19.*

Let $g = \boldsymbol{x}^{\boldsymbol{i}} - g'(x_1, x_2, \ldots, x_m)$ be a polynomial in $\mathbb{F}[x_1, x_2, \ldots, x_m]$ such that $\operatorname{wdeg}(g'(x_1, x_2, \ldots, x_m)) < w(\boldsymbol{x}^{\boldsymbol{i}})$ *and* $\operatorname{Supp}(g) \subset \Delta_{\prec_w}(I)$ *.*

Let $P_{(t_1)} = S(b_{t_1}, g)$ and $P_{(t_1,t_2)} = S(b_{t_2}, P_{(t_1)})$, for $t = j, k$. Then the polynomials in G divides $S(P_{(j_1,j_2)}, P_{(k_1,k_2)})$ for all $1 \leqslant j_1, j_2, k_1, k_2 \leqslant s$ where $j_1 \neq j_2$ and $k_1 \neq k_2$.

Proof: Let $\boldsymbol{\gamma}_{t_1}$ be defined as in the proof of Lemma 6.4 and let $P_{(t_1)}$ be defined as in (6.3) for $t = j, k$. Define for $t_1 \neq t_2$

$$\begin{aligned} P_{(t_1,t_2)} &= S(b_{t_2}, P_{(t_1)}) \\ &= \frac{\boldsymbol{x}^{\boldsymbol{\delta}_{t_1,t_2}}}{-\boldsymbol{x}^{\boldsymbol{\beta}_{t_2}}} \left(\boldsymbol{x}^{\boldsymbol{\alpha}_{t_2}} - \boldsymbol{x}^{\boldsymbol{\beta}_{t_2}} \right) \\ &\quad - \frac{\boldsymbol{x}^{\boldsymbol{\delta}_{t_1,t_2}}}{-\boldsymbol{x}^{\boldsymbol{\gamma}_{t_1} - \boldsymbol{\beta}_{t_1} + \boldsymbol{\alpha}_{t_1}}} \left(-\boldsymbol{x}^{\boldsymbol{\gamma}_{t_1} - \boldsymbol{\beta}_{t_1} + \boldsymbol{\alpha}_{t_1}} + \boldsymbol{x}^{\boldsymbol{\gamma}_{t_1} - \boldsymbol{i}} \cdot g'(x_1, x_2, \ldots, x_m) \right) \\ &= \boldsymbol{x}^{\boldsymbol{\delta}_{t_1,t_2} - \boldsymbol{\beta}_{t_2} + \boldsymbol{\alpha}_{t_2}} - \boldsymbol{x}^{\boldsymbol{\delta}_{t_1,t_2} + \boldsymbol{\beta}_{t_1} - \boldsymbol{\alpha}_{t_1} - \boldsymbol{i}} \cdot g'(x_1, x_2, \ldots, x_m), \end{aligned} \tag{6.5}$$

where $\boldsymbol{\delta}_{t_1,t_2} = (\delta_{t_1,t_2,1}, \delta_{t_1,t_2,2}, \ldots, \delta_{t_1,t_2,m}) \in \mathbb{N}_0^m$ and $\delta_{t_1,t_2,u} = \max\{\gamma_{t_1,u} - \beta_{t_1,u} + \alpha_{t_1,u}, \beta_{t_2,u}\}$ for $1 \leqslant u \leqslant m$ and $t = j, k$. Using Lemma 6.3 the monomial $\boldsymbol{x}^{\boldsymbol{\delta}_{t_1,t_2} - \boldsymbol{\beta}_{t_2} + \boldsymbol{\alpha}_{t_2}}$ in (6.5) is the leading monomial of $P_{(t_1,t_2)}$.

Then for $1 \leqslant j_1, j_2, k_1, k_2 \leqslant s$, $j_1 \neq j_2$ and $k_1 \neq k_2$ we have

$$\begin{aligned} P &= S(P_{(j_1,j_2)}, P_{(k_1,k_2)}) \\ &= \frac{\boldsymbol{x}^{\boldsymbol{\nu}}}{\boldsymbol{x}^{\boldsymbol{\delta}_{j_1,j_2} - \boldsymbol{\beta}_{j_2} + \boldsymbol{\alpha}_{j_2}}} \left(\boldsymbol{x}^{\boldsymbol{\delta}_{j_1,j_2} - \boldsymbol{\beta}_{j_2} + \boldsymbol{\alpha}_{j_2}} - \boldsymbol{x}^{\boldsymbol{\delta}_{j_1,j_2} + \boldsymbol{\beta}_{j_1} - \boldsymbol{\alpha}_{j_1} - \boldsymbol{i}} \cdot g'(x_1, x_2, \ldots, x_m) \right) \\ &\quad - \frac{\boldsymbol{x}^{\boldsymbol{\nu}}}{\boldsymbol{x}^{\boldsymbol{\delta}_{k_1,k_2} - \boldsymbol{\beta}_{k_2} + \boldsymbol{\alpha}_{k_2}}} \left(\boldsymbol{x}^{\boldsymbol{\delta}_{k_1,k_2} - \boldsymbol{\beta}_{k_2} + \boldsymbol{\alpha}_{k_2}} - \boldsymbol{x}^{\boldsymbol{\delta}_{k_1,k_2} + \boldsymbol{\beta}_{k_1} - \boldsymbol{\alpha}_{k_1} - \boldsymbol{i}} \cdot g'(x_1, x_2, \ldots, x_m) \right) \\ &= \left(\boldsymbol{x}^{\boldsymbol{\nu} + \boldsymbol{\beta}_{k_2} - \boldsymbol{\alpha}_{k_2} + \boldsymbol{\beta}_{k_1} - \boldsymbol{\alpha}_{k_1} - \boldsymbol{i}} - \boldsymbol{x}^{\boldsymbol{\nu} + \boldsymbol{\beta}_{j_2} - \boldsymbol{\alpha}_{j_2} + \boldsymbol{\beta}_{j_1} - \boldsymbol{\alpha}_{j_1} - \boldsymbol{i}} \right) \cdot g'(x_1, x_2, \ldots, x_m), \end{aligned} \tag{6.6}$$

where $\boldsymbol{\nu} = (\nu_1, \nu_2, \ldots, \nu_m) \in \mathbb{N}_0^m$ and $\nu_u = \max\{\delta_{j_1,j_2,u} - \beta_{j_2,u} + \alpha_{j_2,u}, \delta_{k_1,k_2,u} - \beta_{k_2,u} + \alpha_{k_2,u}\}$ for $u = 1, 2, \ldots, m$. Since $w(\boldsymbol{x}^{\boldsymbol{\alpha}_{t_1}}) = w(\boldsymbol{x}^{\boldsymbol{\beta}_{t_1}})$ and $w(\boldsymbol{x}^{\boldsymbol{\alpha}_{t_2}}) = w(\boldsymbol{x}^{\boldsymbol{\beta}_{t_2}})$ for $t = j, k$ by definition the binomial in the parenthesis in (6.6) must be in I using Definition 6.1 and thereby P must be divisible by the polynomials in G using Lemma 6.2 and Corollary 2.31. □

Lemma 6.7 *Let I be a toric ideal as defined in Definition 6.1 having Gröbner basis $G = \{b_1, b_2, \ldots, b_s\}$ as in Lemma 6.2. For $k = 1, 2, \ldots, s$, let $b_k = \boldsymbol{x}^{\boldsymbol{\alpha}_k} - \boldsymbol{x}^{\boldsymbol{\beta}_k}$ and let $lm(b_k) = \boldsymbol{x}^{\boldsymbol{\beta}_k}$ with respect to $\prec_w$ as defined in Definition 2.19.*

Let $g = \boldsymbol{x}^{\boldsymbol{i}} - g'(x_1, x_2, \ldots, x_m)$ be a polynomial in $\mathbb{F}[x_1, x_2, \ldots, x_m]$ such that $\operatorname{wdeg}(g'(x_1, x_2, \ldots, x_m)) < w(\boldsymbol{x}^{\boldsymbol{i}})$ *and* $\operatorname{Supp}(g) \subset \Delta_{\prec_w}(I)$ *.*

Let $P_{(j_1)} = S(b_{j_1}, g)$ and $P_{(j_1,j_2)} = S(b_{j_2}, P_{(j_1)})$. Then the polynomials in G divides $S(P_{(j_1,j_2)}, g)$ for all $1 \leqslant j_1, j_2 \leqslant s$ and $j_1 \neq j_2$.

Proof: Let $\boldsymbol{\delta}_{j_1,j_2}$ be defined as in the proof of Lemma 6.6 and let $P_{(j_1,j_2)}$ be defined as in (6.5). Define

$$\begin{aligned} P &= S(P_{(j_1,j_2)}, g) \\ &= \frac{\boldsymbol{x}^{\boldsymbol{\nu}}}{\boldsymbol{x}^{\boldsymbol{\delta}_{j_1,j_2}-\boldsymbol{\beta}_{j_2}+\boldsymbol{\alpha}_{j_2}}} \left(\boldsymbol{x}^{\boldsymbol{\delta}_{j_1,j_2}-\boldsymbol{\beta}_{j_2}+\boldsymbol{\alpha}_{j_2}} - \boldsymbol{x}^{\boldsymbol{\delta}_{j_1,j_2}+\boldsymbol{\beta}_{j_1}-\boldsymbol{\alpha}_{j_1}-\boldsymbol{i}} \cdot g'(x_1, x_2, \dots, x_m)\right) \\ &\quad - \frac{\boldsymbol{x}^{\boldsymbol{\nu}}}{\boldsymbol{x}^{\boldsymbol{i}}} \left(\boldsymbol{x}^{\boldsymbol{i}} - g'(x_1, x_2, \dots, x_m)\right) \\ &= \left(\boldsymbol{x}^{\boldsymbol{\nu}-\boldsymbol{i}} - \boldsymbol{x}^{\boldsymbol{\nu}+\boldsymbol{\beta}_{j_2}-\boldsymbol{\alpha}_{j_2}+\boldsymbol{\beta}_{j_1}-\boldsymbol{\alpha}_{j_1}-\boldsymbol{i}}\right) \cdot g'(x_1, x_2, \dots, x_m), \end{aligned} \tag{6.7}$$

where $\boldsymbol{\nu} = (\nu_1, \nu_2, \dots, \nu_m) \in \mathbb{N}_0^m$ and $\nu_u = \max\{\delta_{j_1,j_2,u} - \beta_{j_2,u} + \alpha_{j_2,u}, i_u\}$ for $1 \leqslant u \leqslant m$. Since $w(\boldsymbol{x}^{\boldsymbol{\alpha}_{j_1}}) = w(\boldsymbol{x}^{\boldsymbol{\beta}_{j_1}})$ and $w(\boldsymbol{x}^{\boldsymbol{\alpha}_{j_2}}) = w(\boldsymbol{x}^{\boldsymbol{\beta}_{j_2}})$ by definition the binomial in the parenthesis in (6.7) must be in I using Definition 6.1 and thereby P must be divisible by the polynomials in G using Lemma 6.2 and Corollary 2.31. □

Lemma 6.8 *Let I be a toric ideal as defined in Definition 6.1 having Gröbner basis $G = \{b_1, b_2, \dots, b_s\}$ as in Lemma 6.2. For $k = 1, 2, \dots, s$, let $b_k = \boldsymbol{x}^{\boldsymbol{\alpha}_k} - \boldsymbol{x}^{\boldsymbol{\beta}_k}$ and let $lm(b_k) = \boldsymbol{x}^{\boldsymbol{\beta}_k}$ with respect to $\prec_w$ as defined in Definition 2.19.*

Let $g = \boldsymbol{x}^{\boldsymbol{i}} - g'(x_1, x_2, \dots, x_m)$ be a polynomial in $\mathbb{F}[x_1, x_2, \dots, x_m]$ such that $\mathrm{wdeg}(g'(x_1, x_2, \dots, x_m)) < w(\boldsymbol{x}^{\boldsymbol{i}})$ and $\mathrm{Supp}(g) \subset \Delta_{\prec_w}(I)$.

Let $P_{(t_1)} = S(b_{t_1}, g)$, for $t = j, k$, and let $P_{(j_1,j_2)} = S(b_{j_2}, P_{(j_1)})$. Then the polynomials in G divides $S(P_{(j_1,j_2)}, P_{(k_1)})$ for all $1 \leqslant j_1, j_2, k_1 \leqslant s$ and $j_1 \neq j_2$.

Proof: Let $\boldsymbol{\delta}_{j_1,j_2}$ be defined as in the proof of Lemma 6.6 and let $P_{(j_1,j_2)}$ be defined as in (6.5). Furthermore, let $\boldsymbol{\gamma}_{k_1}$ be defined as in the proof of Lemma 6.4 and let $P_{(k_1)}$ be defined as in (6.3). Then

$$\begin{aligned} P &= S(P_{(j_1,j_2)}, P_{(k_1)}) \\ &= \frac{\boldsymbol{x}^{\boldsymbol{\nu}}}{\boldsymbol{x}^{\boldsymbol{\delta}_{j_1,j_2}-\boldsymbol{\beta}_{j_2}+\boldsymbol{\alpha}_{j_2}}} \left(\boldsymbol{x}^{\boldsymbol{\delta}_{j_1,j_2}-\boldsymbol{\beta}_{j_2}+\boldsymbol{\alpha}_{j_2}} - \boldsymbol{x}^{\boldsymbol{\delta}_{j_1,j_2}+\boldsymbol{\beta}_{j_1}-\boldsymbol{\alpha}_{j_1}-\boldsymbol{i}} \cdot g'(x_1, x_2, \dots, x_m)\right) \\ &\quad - \frac{\boldsymbol{x}^{\boldsymbol{\nu}}}{-\boldsymbol{x}^{\boldsymbol{\gamma}_{k_1}-\boldsymbol{\beta}_{k_1}+\boldsymbol{\alpha}_{k_1}}} \left(-\boldsymbol{x}^{\boldsymbol{\gamma}_{k_1}-\boldsymbol{\beta}_{k_1}+\boldsymbol{\alpha}_{k_1}} + \boldsymbol{x}^{\boldsymbol{\gamma}_{k_1}-\boldsymbol{i}} \cdot g'(x_1, x_2, \dots, x_m)\right) \\ &= \left(\boldsymbol{x}^{\boldsymbol{\nu}+\boldsymbol{\beta}_{k_1}-\boldsymbol{\alpha}_{k_1}-\boldsymbol{i}} - \boldsymbol{x}^{\boldsymbol{\nu}+\boldsymbol{\beta}_{j_2}-\boldsymbol{\alpha}_{j_2}+\boldsymbol{\beta}_{j_1}-\boldsymbol{\alpha}_{j_1}-\boldsymbol{i}}\right) \cdot g'(x_1, x_2, \dots, x_m), \end{aligned} \tag{6.8}$$

where $\boldsymbol{\nu} = (\nu_1, \nu_2, \dots, \nu_m) \in \mathbb{N}_0^m$ and $\nu_u = \max\{\delta_{j_1,j_2,u} - \beta_{j_2,u} + \alpha_{j_2,u}, \gamma_{k_1,u} - \beta_{k_1,u} + \alpha_{k_1,u}\}$ for $u = 1, 2, \dots, m$. Since $w(\boldsymbol{x}^{\boldsymbol{\alpha}_{t_1}}) = w(\boldsymbol{x}^{\boldsymbol{\beta}_{t_1}})$, for $t = j, k$, and $w(\boldsymbol{x}^{\boldsymbol{\alpha}_{j_2}}) = w(\boldsymbol{x}^{\boldsymbol{\beta}_{j_2}})$ the binomial in the parenthesis in (6.8) must be in I using Definition 6.1 and thereby P must be divisible by the polynomials in G using Lemma 6.2 and Corollary 2.31. □

We are now ready to prove Proposition 6.9.

Proposition 6.9 *Let I be a toric ideal as defined in Definition 6.1 having Gröbner basis $G = \{b_1, b_2, \ldots, b_s\}$ as in Lemma 6.2. For $k = 1, 2, \ldots, s$, let $b_k = \boldsymbol{x}^{\boldsymbol{\alpha}_k} - \boldsymbol{x}^{\boldsymbol{\beta}_k}$ and let $lm(b_k) = \boldsymbol{x}^{\boldsymbol{\beta}_k}$ with respect to $\prec_w$ as defined in Definition 2.19.*

Let $g = \boldsymbol{x}^{\boldsymbol{i}} - g'(x_1, x_2, \ldots, x_m)$ be a polynomial in $\mathbb{F}[x_1, x_2, \ldots, x_m]$ such that $\mathrm{wdeg}(g'(x_1, x_2, \ldots, x_m)) < w(\boldsymbol{x}^{\boldsymbol{i}})$ and $\mathrm{Supp}(g) \subset \Delta_{\prec_w}(I)$.

Define the polynomial $P_{(j_1,j_2,\ldots,j_t)}$ recursively as

$$P_{(j_1)} = S(b_{j_1}, g)$$

for some $1 \leqslant j_1 \leqslant s$, and

$$P_{(j_1,j_2,\ldots,j_t)} = S(b_{j_t}, P_{(j_1,j_2,\ldots,j_{t-1})}),$$

for some $1 \leqslant j_t \leqslant s$. Then the polynomials in G divides $S(P_{(j_1,j_2,\ldots,j_u)}, P_{(k_1,k_2,\ldots,k_v)})$ and $S(P_{(l_1,l_2,\ldots,l_w)}, g)$ for $1 \leqslant u, v, w \leqslant s$.

Proof: Proof by induction in t where $1 \leqslant u, v, w \leqslant t \leqslant s$.

Basis:

The cases $t = 1$ and $t = 2$ follows from Lemmas 6.4, 6.5, 6.6, 6.7 and 6.8.

Step:

Let $2 < t \leqslant s$ and assume that the theorem holds for all u, v, w where $1 \leqslant u, v, w < t$. In order to prove the theorem for $1 \leqslant u, v, w \leqslant t$ we have four cases to consider.

Case 1: $u = t - 1$ and $1 \leqslant v < t - 1$.

Assume without loss of generality that the polynomials $P_{(j_1,j_2,\ldots,j_u)}$ and $P_{(k_1,k_2,\ldots,k_v)}$ are given by the expression in (6.1), i.e.

$$P_{(j_1,j_2,\ldots,j_u)} = \boldsymbol{x}^{\boldsymbol{p}_{j_u}} - \boldsymbol{x}^{\boldsymbol{q}_{j_u} - \boldsymbol{i}} \cdot g'(x_1, x_2, \ldots, x_m) \tag{6.9}$$

and

$$P_{(k_1,k_2,\ldots,k_v)} = \boldsymbol{x}^{\boldsymbol{p}_{k_v}} - \boldsymbol{x}^{\boldsymbol{q}_{k_v} - \boldsymbol{i}} \cdot g'(x_1, x_2, \ldots, x_m) \tag{6.10}$$

with $lm(P_{(j_1,j_2,\ldots,j_u)}) = \boldsymbol{x}^{\boldsymbol{p}_{j_u}}$ and $lm(P_{(k_1,k_2,\ldots,k_v)}) = \boldsymbol{x}^{\boldsymbol{p}_{k_v}}$ using Lemma 6.3.

Furthermore, since $u, v < t$ the induction hypothesis implies that

$$\begin{aligned} S&\left(P_{(j_1,j_2,\ldots,j_u)}, P_{(k_1,k_2,\ldots,k_v)}\right) \\ &= \frac{\boldsymbol{x}^{\boldsymbol{\gamma}_{j_u,k_v}}}{\boldsymbol{x}^{\boldsymbol{p}_{j_u}}} \left(\boldsymbol{x}^{\boldsymbol{p}_{j_u}} - \boldsymbol{x}^{\boldsymbol{q}_{j_u} - \boldsymbol{i}} \cdot g'(x_1, x_2, \ldots, x_m)\right) \\ &\quad - \frac{\boldsymbol{x}^{\boldsymbol{\gamma}_{j_u,k_v}}}{\boldsymbol{x}^{\boldsymbol{p}_{k_v}}} \left(\boldsymbol{x}^{\boldsymbol{p}_{k_v}} - \boldsymbol{x}^{\boldsymbol{q}_{k_v} - \boldsymbol{i}} \cdot g'(x_1, x_2, \ldots, x_m)\right) \\ &= \left(\boldsymbol{x}^{\boldsymbol{\gamma}_{j_u,k_v} - \boldsymbol{p}_{k_v} + \boldsymbol{q}_{k_v} - \boldsymbol{i}} - \boldsymbol{x}^{\boldsymbol{\gamma}_{j_u,k_v} - \boldsymbol{p}_{j_u} + \boldsymbol{q}_{j_u} - \boldsymbol{i}}\right) \cdot g'(x_1, x_2, \ldots, x_m) \end{aligned} \tag{6.11}$$

is divisible by the polynomials in G, where $\gamma_{j_u,k_v,n} = \max\{p_{j_u,n}, p_{k_v,n}\}$ for $n = 1, 2, \ldots, m$. Since the polynomial in (6.11) is in I and no monomials in the support of $g'(x_1, x_2, \ldots, x_m)$ have equal weights, Lemma 6.2 implies that

$$w\left(\boldsymbol{x}^{\boldsymbol{\gamma}_{j_u,k_v} - \boldsymbol{p}_{k_v} + \boldsymbol{q}_{k_v} - \boldsymbol{i}}\right) = w\left(\boldsymbol{x}^{\boldsymbol{\gamma}_{j_u,k_v} - \boldsymbol{p}_{j_u} + \boldsymbol{q}_{j_u} - \boldsymbol{i}}\right),$$

which again implies that

$$w\left(\boldsymbol{x}^{-\boldsymbol{p}_{k_v}+\boldsymbol{q}_{k_v}}\right) = w\left(\boldsymbol{x}^{-\boldsymbol{p}_{j_u}+\boldsymbol{q}_{j_u}}\right). \tag{6.12}$$

Now, calculating $P_{(j_1,j_2,\ldots,j_u,j_{u+1})} = P_{(j_1,j_2,\ldots,j_t)}$ we have

$$\begin{aligned} P_{(j_1,j_2,\ldots,j_t)} &= S\left(b_{j_t}, P_{(j_1,j_2,\ldots,j_u)}\right) \\ &= \frac{\boldsymbol{x}^{\boldsymbol{\delta}}}{-\boldsymbol{x}^{\boldsymbol{\beta}_{j_t}}}\left(\boldsymbol{x}^{\boldsymbol{\alpha}_{j_t}} - \boldsymbol{x}^{\boldsymbol{\beta}_{j_t}}\right) - \frac{\boldsymbol{x}^{\boldsymbol{\delta}}}{\boldsymbol{x}^{\boldsymbol{p}_{j_u}}}\left(\boldsymbol{x}^{\boldsymbol{p}_{j_u}} - \boldsymbol{x}^{\boldsymbol{q}_{j_u}-\boldsymbol{i}} \cdot g'(x_1, x_2, \ldots, x_m)\right) \\ &= -\boldsymbol{x}^{\boldsymbol{\delta}-\boldsymbol{\beta}_{j_t}+\boldsymbol{\alpha}_{j_t}} + \boldsymbol{x}^{\boldsymbol{\delta}-\boldsymbol{p}_{j_u}+\boldsymbol{q}_{j_u}-\boldsymbol{i}} \cdot g'(x_1, x_2, \ldots, x_m), \end{aligned} \tag{6.13}$$

where $\delta_n = \max\{\beta_{j_t,n}, p_{j_u,n}\}$ for $n = 1, 2, \ldots, m$.

Finally, calculating $S\left(P_{(j_1,j_2,\ldots,j_t)}, P_{(k_1,k_2,\ldots,k_v)}\right)$ we have

$$\begin{aligned} &S\left(P_{(j_1,j_2,\ldots,j_t)}, P_{(k_1,k_2,\ldots,k_v)}\right) \\ &\quad= \frac{\boldsymbol{x}^{\boldsymbol{\varepsilon}}}{-\boldsymbol{x}^{\boldsymbol{\delta}-\boldsymbol{\beta}_{j_t}+\boldsymbol{\alpha}_{j_t}}}\left(-\boldsymbol{x}^{\boldsymbol{\delta}-\boldsymbol{\beta}_{j_t}+\boldsymbol{\alpha}_{j_t}} + \boldsymbol{x}^{\boldsymbol{\delta}-\boldsymbol{p}_{j_u}+\boldsymbol{q}_{j_u}-\boldsymbol{i}} \cdot g'(x_1, x_2, \ldots, x_m)\right) \\ &\quad\quad - \frac{\boldsymbol{x}^{\boldsymbol{\varepsilon}}}{\boldsymbol{x}^{\boldsymbol{p}_{k_v}}}\left(\boldsymbol{x}^{\boldsymbol{p}_{k_v}} - \boldsymbol{x}^{\boldsymbol{q}_{k_v}-\boldsymbol{i}} \cdot g'(x_1, x_2, \ldots, x_m)\right) \\ &\quad= \left(\boldsymbol{x}^{\boldsymbol{\varepsilon}-\boldsymbol{p}_{k_v}+\boldsymbol{q}_{k_v}-\boldsymbol{i}} - \boldsymbol{x}^{\boldsymbol{\varepsilon}+\boldsymbol{\beta}_{j_t}-\boldsymbol{\alpha}_{j_t}-\boldsymbol{p}_{j_u}+\boldsymbol{q}_{j_u}-\boldsymbol{i}}\right) \cdot g'(x_1, x_2, \ldots, x_m), \end{aligned} \tag{6.14}$$

where $\varepsilon_n = \max\{\delta_n - \beta_{j_t,n} + \alpha_{j_t,n}, p_{k_v,n}\}$ for $n = 1, 2\ldots, m$. Using equation (6.12) and the definition of b_{j_t} we have that the two monomials in the parenthesis in (6.14) have equal weights, thus $S\left(P_{(j_1,j_2,\ldots,j_t)}, P_{(k_1,k_2,\ldots,k_v)}\right) \in I$ and the polynomials in G must divide $S\left(P_{(j_1,j_2,\ldots,j_t)}, P_{(k_1,k_2,\ldots,k_v)}\right)$ using Lemma 6.2 and Corollary 2.31.

The calculations above would have been similar if we had used polynomials $P_{(j_1,j_2,\ldots,j_u)}$ or $P_{(k_1,k_2,\ldots,k_v)}$ or both on the form in (6.2). This concludes the proof of Case 1.

Case 2: $1 \leqslant u < t-1$ and $v = t-1$.

Calculations and arguments in this case are the same as in Case 1 with the roles of u and v interchanged.

Case 3: $u = v = t-1$.

In this case we use the expression in (6.13) for both $P_{(j_1,j_2,\ldots,j_t)}$ and $P_{(k_1,k_2,\ldots,k_t)}$ and get

$$\begin{aligned} &S\left(P_{(j_1,j_2,\ldots,j_t)}, P_{(k_1,k_2,\ldots,k_t)}\right) \\ &\quad= \frac{\boldsymbol{x}^{\boldsymbol{\varepsilon}}}{-\boldsymbol{x}^{\boldsymbol{\delta}_{j_t,j_u}-\boldsymbol{\beta}_{j_t}+\boldsymbol{\alpha}_{j_t}}}\left(-\boldsymbol{x}^{\boldsymbol{\delta}_{j_t,j_u}-\boldsymbol{\beta}_{j_t}+\boldsymbol{\alpha}_{j_t}} + \boldsymbol{x}^{\boldsymbol{\delta}_{j_t,j_u}-\boldsymbol{p}_{j_u}+\boldsymbol{q}_{j_u}-\boldsymbol{i}} \cdot g'(x_1, x_2, \ldots, x_m)\right) \\ &\quad\quad - \frac{\boldsymbol{x}^{\boldsymbol{\varepsilon}}}{-\boldsymbol{x}^{\boldsymbol{\delta}_{k_t,k_v}-\boldsymbol{\beta}_{k_t}+\boldsymbol{\alpha}_{k_t}}}\left(-\boldsymbol{x}^{\boldsymbol{\delta}_{k_t,k_v}-\boldsymbol{\beta}_{k_t}+\boldsymbol{\alpha}_{k_t}} + \boldsymbol{x}^{\boldsymbol{\delta}_{k_t,k_v}-\boldsymbol{p}_{k_v}+\boldsymbol{q}_{k_v}-\boldsymbol{i}} \cdot g'(x_1, x_2, \ldots, x_m)\right) \\ &\quad= \left(\boldsymbol{x}^{\boldsymbol{\varepsilon}+\boldsymbol{\beta}_{k_t}-\boldsymbol{\alpha}_{k_t}-\boldsymbol{p}_{k_v}+\boldsymbol{q}_{k_v}-\boldsymbol{i}} - \boldsymbol{x}^{\boldsymbol{\varepsilon}+\boldsymbol{\beta}_{j_t}-\boldsymbol{\alpha}_{j_t}-\boldsymbol{p}_{j_u}+\boldsymbol{q}_{j_u}-\boldsymbol{i}}\right) \cdot g'(x_1, x_2, \ldots, x_m), \end{aligned} \tag{6.15}$$

where $\varepsilon_n = \max\{\delta_{j_t,j_u,n} - \beta_{j_t,n} + \alpha_{j_t,n}, \delta_{k_t,k_v,n} - \beta_{j_t,n} + \alpha_{j_t,n}\}$ for $n = 1, 2, \ldots, m$. Using (6.12) and the definition of b_{j_t} and b_{k_t} we have that the two monomials in the parenthesis in (6.15) have equal weights, thus $S\left(P_{(j_1,j_2,\ldots,j_t)}, p_{(k_1,k_2,\ldots,k_t)}\right) \in I$ and the polynomials in G must divide $S\left(P_{(j_1,j_2,\ldots,j_t)}, P_{(k_1,k_2,\ldots,k_t)}\right)$ using Lemma 6.2 and Corollary 2.31.

The calculations above would have been similar if we had used polynomials $P_{(j_1,j_2,\ldots,j_u)}$ or $P_{(k_1,k_2,\ldots,k_v)}$ or both on the form in (6.2). This concludes the proof of Case 3.

Case 4: $w = t-1$.

Assume that the theorem holds for $w = t-1$. Calculating $S\left(P_{(l_1,l_2,\ldots,l_w)}, g\right)$ using the expression for $P_{(l_1,l_2,\ldots,l_w)}$ given in (6.1) yields

$$\begin{aligned} &S\left(P_{(l_1,l_2,\ldots,l_w)}, g\right) \\ &\quad= \frac{\boldsymbol{x}^{\boldsymbol{\gamma}}}{\boldsymbol{x}^{\boldsymbol{p}_{l_w}}}\left(\boldsymbol{x}^{\boldsymbol{p}_{l_w}} - \boldsymbol{x}^{\boldsymbol{q}_{l_w}-\boldsymbol{i}} \cdot g'(x_1,x_2,\ldots,x_m)\right) - \frac{\boldsymbol{x}^{\boldsymbol{\gamma}}}{\boldsymbol{x}^{\boldsymbol{i}}}\left(\boldsymbol{x}^{\boldsymbol{i}} - g'(x_1,x_2,\ldots,x_m)\right) \\ &\quad= \left(\boldsymbol{x}^{\boldsymbol{\gamma}-\boldsymbol{i}} - \boldsymbol{x}^{\boldsymbol{\gamma}-\boldsymbol{p}_{l_w}+\boldsymbol{q}_{l_w}-\boldsymbol{i}}\right) \cdot g'(x_1,x_2,\ldots,x_m), \end{aligned} \tag{6.16}$$

where $\gamma_n = \max\{p_{l_w,n}, i_n\}$ for $n = 1,2,\ldots,m$. Since the polynomial in (6.16) is in I using the induction hypothesis and no monomial in the support of $g'(x_1,x_2,\ldots,x_m)$ have equal weights, Lemma 6.2 implies that

$$w\left(\boldsymbol{x}^{\boldsymbol{\gamma}-\boldsymbol{i}}\right) = w\left(\boldsymbol{x}^{\boldsymbol{\gamma}-\boldsymbol{p}_{l_w}+\boldsymbol{q}_{l_w}-\boldsymbol{i}}\right)$$

implies that

$$0 = w\left(\boldsymbol{x}^{-\boldsymbol{p}_{l_w}+\boldsymbol{q}_{l_w}}\right). \tag{6.17}$$

Using $P_{(l_1,l_2,\ldots,l_t)}$ equal to the expression in (6.13) and $g = \boldsymbol{x}^{\boldsymbol{i}} - g'(x_1,x_2,\ldots,x_m)$ we calculate

$$\begin{aligned} &S\left(P_{(l_1,l_2,\ldots,l_t)}, g\right) \\ &\quad= \frac{\boldsymbol{x}^{\boldsymbol{\varepsilon}}}{-\boldsymbol{x}^{\boldsymbol{\delta}-\boldsymbol{\beta}_{l_t}+\boldsymbol{\alpha}_{l_t}}}\left(-\boldsymbol{x}^{\boldsymbol{\delta}-\boldsymbol{\beta}_{l_t}+\boldsymbol{\alpha}_{l_t}} + \boldsymbol{x}^{\boldsymbol{\delta}-\boldsymbol{p}_{l_w}+\boldsymbol{q}_{l_w}-\boldsymbol{i}} \cdot g'(x_1,x_2,\ldots,x_m)\right) \\ &\qquad - \frac{\boldsymbol{x}^{\boldsymbol{\varepsilon}}}{\boldsymbol{x}^{\boldsymbol{i}}}\left(\boldsymbol{x}^{\boldsymbol{i}} - g'(x_1,x_2,\ldots,x_m)\right) \\ &\quad= \left(\boldsymbol{x}^{\boldsymbol{\varepsilon}-\boldsymbol{i}} - \boldsymbol{x}^{\boldsymbol{\varepsilon}+\boldsymbol{\beta}_{l_t}-\boldsymbol{\alpha}_{l_t}-\boldsymbol{p}_{l_w}+\boldsymbol{q}_{l_w}-\boldsymbol{i}}\right) \cdot g'(x_1,x_2,\ldots,x_m), \end{aligned} \tag{6.18}$$

where $\varepsilon_n = \max\{\delta_n - \beta_{l_t,n} + \alpha_{l_t,n}, i_n\}$ for $n = 1,2,\ldots,m$. Using (6.17) and the definition of b_{l_t} the two monomials in the parenthesis in (6.18) have equal weights, thus $S\left(P_{(l_1,l_2,\ldots,l_t)}, g\right) \in I$ and the polynomials in G must divide $S\left(P_{(l_1,l_2,\ldots,l_t)}, g\right)$ using Lemma 6.2 and Corollary 2.31.

The calculations above would have been similar if we had used polynomials $P_{(l_1,l_2,\ldots,l_w)}$ on the form in (6.2). This concludes the proof of Case 4 and the proposition. □

7. Codes from the Suzuki curve - a case study

This chapter is a case study on the construction of codes from a Suzuki curve using Gröbner basis theoretical based methods and the results from [2]. Specifically, we will construct both improved evaluation codes $\tilde{E}$ and improved dual codes $\tilde{C}$ in the case of the Suzuki curve over $\mathbb{F}_8$ and over $\mathbb{F}_{32}$.

In [6] the authors analyze the class of one-point codes defined in [19] by determining the actual dimension of the codes and using the Feng-Rao distance which was formulated in [23] based on the decoding algorithm proposed in [10]. Furthermore, the authors of [6] used Magma[1] to compute an upper bound and test the codes against this bound.

In this chapter we will reconsider the codes above in a Gröbner basis theoretical setting using an ideal as suggested in [19] and an order domain as described in Theorem 2.39.

7.1. The Suzuki curve

The short presentation of the Suzuki curve given in this section is based on the description given in [6, 19, 28].

Let $q_0 = 2^n$ and $q = 2^{2n+1}$ for some positive integer n. Let $\mathbb{F}_q$ be the finite field with q elements and let $\overline{\mathbb{F}_q}$ be the algebraic closure of $\mathbb{F}_q$. The curve $\mathcal{X} \subseteq \mathbb{P}^2(\overline{\mathbb{F}_q})$ defined over $\mathbb{F}_q$ by the homogeneous equation

$$u^{q_0}(y^q + yu^{q-1}) = x^{q_0}(x^q + xu^{q-1}).$$

The four rational functions on $\mathcal{X}$

$$\begin{aligned} f_q &= \frac{x}{u} \\ f_{q+q_0} &= \frac{y}{u} \\ f_{q+2q_0} &= f_q^{2q_0+1} + f_{q+q_0}^{2q_0} \\ f_{q+2q_0+1} &= f_q f_{q+q_0}^{2q_0} + f_{q+2q_0}^{2q_0} \end{aligned}$$

generate the algebra of all rational functions that are regular on $\mathcal{X} \setminus \{P_\infty\}$, where P_∞ is the point at infinity.

In the affine plane $\mathbb{A}^2(\overline{\mathbb{F}_q}) = \mathbb{P}^2(\overline{\mathbb{F}_q}) \setminus \{z = 0\}$ we have the corresponding inhomogeneous equation

$$y^q + y = x^{q_0}(x^q + x)$$

[1] Magma and documentation is available online at: http://magma.maths.usyd.edu.au/magma/

and the four functions

$$\begin{aligned}
f_q &= x \\
f_{q+q_0} &= y \\
f_{q+2q_0} &= f_q^{2q_0+1} + f_{q+q_0}^{2q_0} = x^{2q_0+1} + y^{2q_0} \\
f_{q+2q_0+1} &= f_q f_{q+q_0}^{2q_0} + f_{q+2q_0}^{2q_0} = xy^{2q_0} + (x^{2q_0+1} + y^{2q_0})^{2q_0}
\end{aligned}$$

which we will be using. Furthermore, we will use the Weierstrass semigroup for P_∞ given by $\langle q, q+q_0, q+2q_0, q+2q_0+1\rangle$ in the construction of an order domain in the next section.

7.2. The Gröbner basis theoretical approach to Suzuki curves

In this section we will be using the semigroup generated by $\langle q, q+q_0, q+2q_0, q+2q_0+1\rangle$ and the ordering $<$ of elements in $\mathbb{N}_0$ (properly extended with respect to an added element $-\infty$ as in Section 2.1) as our well-order when defining an order domain of the form in Theorem 2.39 and emulating the Suzuki curve in Section 7.1.

When it comes to defining an ideal I to construct our order domain we will have to capture the relation between the functions $f_q, f_{q+q_0}, f_{q+2q_0}$ and f_{q+2q_0+1} in Section 7.1. This is done by considering an ideal I in $\mathbb{F}_q[x,y,z,v]$, where the four variables x,y,z,v represent the four functions above, and add the two polynomials $z + x^{2q_0+1} + y^{2q_0}$ and $v + xy^{2q_0} + z^{2q_0}$ to the basis of I.

Thus we get the ideal I given by

$$I = \left\langle x^{q_0}(x^q + x) - y^q - y, z + x^{2q_0+1} + y^{2q_0}, v + xy^{2q_0} + z^{2q_0} \right\rangle \subseteq \mathbb{F}_q[x,y,z,v]. \quad (7.1)$$

Furthermore, we define the monomial ordering $\prec_w$ as in Definition 2.19 induced by $w(x) = q, w(y) = q+q_0, w(z) = q+2q_0, w(v) = q+2q_0+1$ and $x \prec_{lex} y \prec_{lex} z \prec_{lex} v$.

The set $G = \{x^q + x + y^{q_0}(y^q + y), z + x^{2q_0+1} + y^{2q_0}, v + xy^{2q_0} + z^{2q_0}\}$ may not be a Gröbner basis for I with respect to $\prec_w$ so for a given $\mathbb{F}_q$ we would have to find a Gröbner basis for I and check that the conditions in Theorem 2.39 hold in order to use $\mathbb{F}_q[x,y,z,v]/I$ as our order domain.

The next section will give two examples of such order domains for $q = 8$ and $q = 32$ (the cases $n = 1$ and $n = 2$ in Section 7.1) and the minimum distance of evaluation codes constructed by using the method described in Section 2.2.

7.3. Examples over $\mathbb{F}_8$ and $\mathbb{F}_{32}$

Here the two examples of codes considered in [6, 19] will be given using order domains as in Chapter 2.

Example 7.1 Here we consider the example studied in [6] over $\mathbb{F}_8$, i.e. the case $n = 1$ such that $q_0 = 2$ and $q = 8$. Thus from (7.1) we have the ideal

$$I = \left\langle y^8 + y + x^2(x^8 + x), z + x^5 + y^4, v + xy^4 + z^4 \right\rangle \in \mathbb{F}_8[x, y, z, v].$$

Furthermore, let $w(x) = 8, w(y) = 10, w(z) = 12$ and $w(v) = 13$. Using the monomial ordering $\prec_w$ from Definition 2.19 as described in Section 7.2 when running Buchberger's algorithm, we get the reduced Gröbner basis G for I given by

$$G = \{x^5 + y^4 + z, x^3 + z^2 + y, xz + y^2 + v, x^4 + y^2z + xy + zv, x^2y + v^2 + z\} \qquad (7.2)$$

which has leading monomials $\{y^4, z^2, xz, y^2z, v^2\}$. The Gröbner basis in (7.2) is on the form required in Theorem 2.39 (but not on the form in Theorem 5.1). Furthermore, it can be shown that the monomials in the footprint of I have different weights, thus $\mathbb{F}_8[x, y, z, v]/I$ is an order domain with weight function $\rho([f]) = w(\bar{f})$.

Moreover, by computer search we find that $\#\mathbb{V}\left(I + \langle x^8 - x, y^8 - y, z^8 - z, v^8 - v\rangle\right) = 64$, thus, using the method in Section 2.1 (from [2]), we can construct the improved evaluation codes $\tilde{E}(\delta)$ and get the parameters listed in Table 7.1

Table 7.1.: Parameters $[n, k, d]$ for the improved $\tilde{E}(\delta)$ from the Suzuki curve over $\mathbb{F}_8$.

$[64,1,64]$	$[64,13,39]$	$[64,26,25]$	$[64,42,12]$
$[64,2,56]$	$[64,14,38]$	$[64,27,24]$	$[64,44,10]$
$[64,3,54]$	$[64,15,36]$	$[64,28,23]$	$[64,45,9]$
$[64,4,52]$	$[64,16,35]$	$[64,29,22]$	$[64,49,8]$
$[64,5,51]$	$[64,17,34]$	$[64,31,21]$	$[64,50,7]$
$[64,6,48]$	$[64,18,33]$	$[64,32,20]$	$[64,51,6]$
$[64,7,46]$	$[64,19,32]$	$[64,33,19]$	$[64,53,5]$
$[64,8,44]$	$[64,20,31]$	$[64,34,18]$	$[64,58,4]$
$[64,9,43]$	$[64,21,30]$	$[64,35,17]$	$[64,59,3]$
$[64,10,42]$	$[64,22,29]$	$[64,37,16]$	$[64,63,2]$
$[64,11,41]$	$[64,24,28]$	$[64,38,14]$	$[64,64,1]$
$[64,12,40]$	$[64,25,26]$	$[64,40,13]$	

Note that the codes with parameters $[64, 31, 21]$, $[64, 33, 19]$, $[64, 35, 17]$, $[64, 38, 14]$, $[64, 40, 13]$, $[64, 44, 10]$ and $[64, 45, 9]$ in Table 7.1 have better parameters than those reported in [6] but none of these codes are better than the lower bound given in Brouwer's tables [5].

The code rates plotted against the relative minimum distances of the codes in Table 7.1 is shown in Figure 7.1.

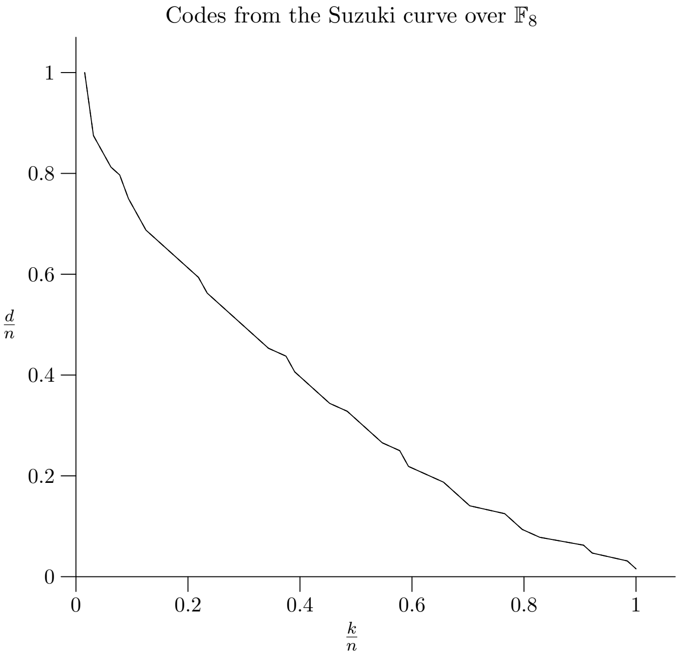

Figure 7.1.: Codes with length 64 from the Suzuki curve over $\mathbb{F}_8$.

By constructing the dual codes $\tilde{C}(\eta)$ and compare the parameters we find that for every code $\tilde{E}(\delta)$ there exists a $\tilde{C}(\eta)$ code with similar parameters. This result corresponds to the result in [19, Pro. 5.1]. In other words: The codes constructed here are an example of codes not on the form given in [2, Pro. 8] but where the result holds. △

Example 7.2 Here we consider the case $n = 2$ such that $q_0 = 4$ and $q = 32$. Thus from (7.1) we have the ideal

$$I = \left\langle y^{32} + y + x^4(x^{32} + x), z + x^9 + y^8, v + xy^8 + z^8 \right\rangle \in \mathbb{F}_{32}[x, y, z, v].$$

Furthermore, let $w(x) = 32, w(y) = 36, w(z) = 40$ and $w(v) = 41$. Using the monomial ordering $\prec_w$ from Definition 2.19 as described in Section 7.2 when running Buchberger's algorithm, we get the reduced Gröbner basis G for I given by

$$\begin{aligned} G =&\{x^9 + y^8 + z, x^5 + z^4 + y, xz + y^2 + v, x^6 + y^2z^3 + z^3v + xy, \\ &x^8 + y^6z + y^4zv + y^2zv^2 + x^3y + zv^3, x^7 + y^4z^2 + z^2v^2 + x^2y, x^4y + v^4 + z\} \end{aligned} \tag{7.3}$$

which has leading monomials $\{y^8, z^4, xz, y^2z^3, y^6z, y^4z^2, v^4\}$. The Gröbner basis in (7.3) is on the form required in Theorem 2.39 and $\mathbb{F}_{32}[x, y, z, v]/I$ is an order domain with weight function $\rho([f]) = w(\bar{f})$.

Again, using computer search we find that

$$\#\mathbb{V}\left(I + \langle x^{32} - x, y^{32} - y, z^{32} - z, v^{32} - v\rangle\right) = 1024.$$

Thus, using the method in Section 2.1 (from [2]), we construct the improved evaluation codes $\tilde{E}(\delta)$ and get the result plotted in Figure 7.2.

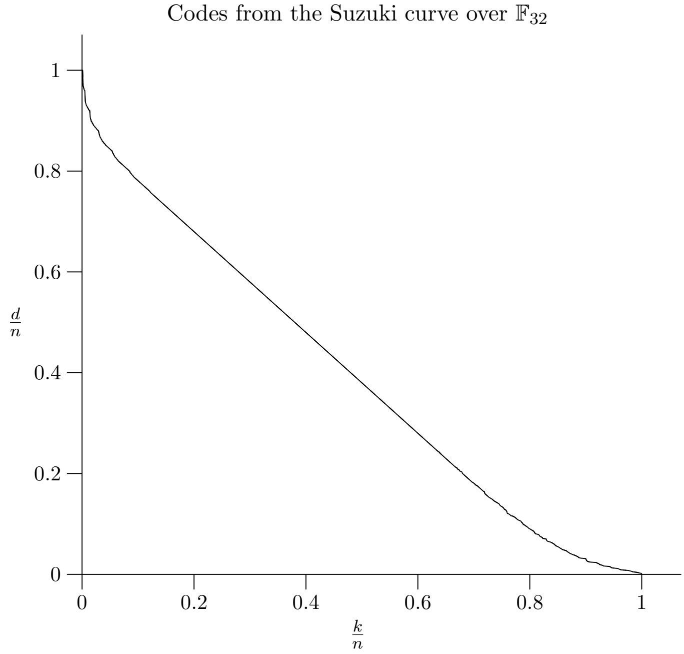

Figure 7.2.: Codes with length 1024 from the Suzuki curve over $\mathbb{F}_{32}$.

Again, by constructing the dual codes $\tilde{C}(\eta)$ and compare the parameters we find that for every code $\tilde{E}(\delta)$ there exists a $\tilde{C}(\eta)$ code with similar parameters. △

Bibliography for Part A

[1] H. Andersen. On Puncturing of Codes from Norm-Trace Curves. Submitted - preprint available at:
`http://www.math.aau.dk/research/reports/R-2005-10.pdf`.

[2] H. Andersen and O. Geil. The Missing Evaluation Codes from Order Domain Theory. Submitted - preprint available at:
`http://www.math.aau.dk/research/reports/R-2004-17.pdf`.

[3] H. Andersen and O. Geil. The Missing Evaluation Codes from Order Domain Theory. *Proc. of 2004 IEEE International Symposium on Information Theory, Chicago, USA, June 27 - July 2*, page 78, 2004.

[4] H. E. Andersen and O. Geil. *On the Missing Evaluation Codes from Order Domain Theory*, 6 pages, November, 2003, Unpublished. An abstract of this extended summary was published in: Mathematisches Forshungsinstitut Oberwolfach, Report No. 53, Kodierungstheorie, December 7th - December 13th, 2003, page 3.

[5] A. E. Brouwer. Linear code bounds.
Available at: `http://www.win.tue.nl/~aeb/voorlincod.html`.

[6] C.-Y. Chen and I. M. Duursma. Geometric Reed-Solomon codes of length 64 and 65 over $\mathbb{F}_8$. *IEEE Trans. Inform. Theory*, 49(5):1351–1353, 2003.

[7] J.-M. Chen and B.-Y. Yang. A More Secure and Efficacious TTS Signature Scheme. In J. I. Lim and D. H. Lee, editors, *Information Security and Cryptology - ICISC 2003: 6th International Conference, Seoul, Korea*, volume 2971 of *Lecture Notes in Computer Science*, pages 320–338. Springer-Verlag GmbH, 2004.

[8] D. Cox, J. Little, and D. O'Shea. *Ideals, Varieties and Algorithms - An Introduction to Computational Algebraic Geometry and Commutative Algebra.* Springer Verlag, New York, second edition, 1997.

[9] D. Cox, J. Little, and D. O'Shea. *Using Algebraic Geometry.* Springer Verlag, New York, 1998.

[10] G. L. Feng and T. R. N. Rao. Decoding algebraic-geometric codes up to the designed minimum distance. *IEEE Trans. Inform. Theory*, 39(1):37–45, 1993.

[11] G. L. Feng and T. R. N. Rao. A simple approach for construction of algebraic-geometric codes from affine plane curves. *IEEE Trans. Inform. Theory*, 40(4):1003–1012, 1994.

[12] G.-L. Feng and T. R. N. Rao. Improved geometric Goppa codes. I. Basic theory. *IEEE Trans. Inform. Theory*, 41(6, part 1):1678–1693, 1995. Special issue on algebraic geometry codes.

[13] J. Fitzgerald and R. F. Lax. Decoding affine variety codes using Gröbner bases. *Designs, Codes and Cryptography*, 13(2):147–158, 1998.

[14] O. Geil. *Codes Based on an $\mathbb{F}_q$-Algebra.* PhD thesis, Department of Mathematical Sciences, Aalborg University, Fredrik Bajers Vej 7G, DK 9220 Aalborg East, Denmark, June 2000.

[15] O. Geil. A Class of Gröbner Basis Theoretically Based Evaluation Codes. *Proc. of 2002 IEEE International Symposium on Information Theory, Lausanne, Schwitzerland, June 30 - July 5*, page 60, 2002.

[16] O. Geil. On Codes from Norm-Trace Curves. *Finite Fields and Their Applications*, 9(3):351–371, July 2003.

[17] O. Geil and T. Høholdt. On hyperbolic codes. In *Applied algebra, algebraic algorithms and error-correcting codes (Melbourne, 2001)*, volume 2227 of *Lecture Notes in Comput. Sci.*, pages 159–171. Springer, Berlin, 2001.

[18] O. Geil and R. Pellikaan. On the Structure of Order Domains. *Finite Fields and Their Applications*, 8:369–396, 2002.

[19] J. P. Hansen and H. Stichtenoth. Group codes on certain algebraic curves with many rational points. *Appl. Algebra Engrg. Comm. Comput.*, 1(1):67–77, 1990.

[20] T. Høholdt, J. van Lint, and R. Pellikaan. Chapter 10: "Algebraic geometry codes" in *Handbook of coding theory, V. S. Pless and W. C. Huffman (Eds.), vol. 1.* Elsevier, Amsterdam, 1998.

[21] T. Høholdt, J. H. van Lint, and R. Pellikaan. Order functions and evaluation codes. In *Applied algebra, algebraic algorithms and error-correcting codes (Toulouse, 1997)*, volume 1255 of *Lecture Notes in Comput. Sci.*, pages 138–150. Springer, Berlin, 1997.

[22] G. A. Kabatianskiĭ. Two generalizations of the product of codes. *Dokl. Akad. Nauk SSSR*, 232(6):1277–1280, 1977. (In Russian).

[23] C. Kirfel and R. Pellikaan. The minimum distance of codes in an array coming from telescopic semigroups. *IEEE Trans. Inform. Theory*, 41(6, part 1):1720–1732, 1995. Special issue on algebraic geometry codes.

[24] F. MacWilliams and N. Sloane. *The Theory of Error-Correcting Codes.* North-Holland Amsterdam, 1977.

[25] J. L. Massey, D. J. Costello, and J. Justesen. Polynomial weights and code constructions. *IEEE Trans. Information Theory*, IT-19:101–110, 1973.

[26] R. Matsumoto. The C_{ab} Curve.
Available at: `http://www.rmatsumoto.org/cab.html`.

[27] R. Matsumoto. Miura's Generalization of One-Point AG Codes is Equivalent to Høholdt, van Lint and Pellikaan's Generalization. *IEICE Trans. Fundamentals*, E82-A(10):2007–2010, October 1999.

[28] G. L. Matthews. Codes From the Suzuki Function Field. *IEEE Trans. Inform. Theory*, 50(12):3298–3302, December 2004.

[29] S. Miura. Algebraic geometric codes on certain plane curves. *IEICE Trans.*, J75-A(11):1735–1745, 1992. (In japanese).

[30] S. Miura. PhD thesis, University of Tokyo, May 1997. (In Japanese).

[31] S. Miura. Linear Codes on Affine Algebraic Varieties. *IEICE Trans.*, J81-A(10):1386–1397, 1998. (In Japanese).

[32] S. Miura and N. Kamiya. On the Minimum Distance of Codes from Some Maximal Curves. Technical Report IT92-147, IEICE, Marts 1993. (In Japanese).

[33] R. Pellikaan. On the existence of order functions. *Journal of Statistical Planning and Inference*, 94:287–301, 2001.

[34] T. Shibuya and K. Sakaniwa. A Dual of Well-Behaving Type Designed Minimum Distance. *IEICE Trans. Fundamentals*, E84-A(2):647–52, February 2001.

[35] B. Sturmfels. *Gröbner bases and convex polytopes*, volume 8 of *University Lecture Series*. American Mathematical Society, Providence, RI, 1996.

Index

Page numbers printed in **bold** are references to the definition of terms.

Part B.

Included papers

8. Paper I - H. E. Andersen and O. Geil: “The missing Evaluation Codes from Order Domain Theory”

H. E. Andersen and O. Geil

The missing Evaluation Codes from Order Domain Theory

Research report R-2004-17
Department of Mathematical Sciences
Aalborg University
Denmark

The results presented in this paper are the result of work done in cooperation with Olav Geil, Aalborg University. The main result was presented at 2004 IEEE International Symposium on Information Theory (ISIT 2004) in Chicago, USA, June 27 - July 2, and an extended summary was published in the proceedings. Furthermore, a predecessor of this paper and the extended summary was published as [1].

The Missing Evaluation Codes from Order Domain Theory

Henning E. Andersen and Olav Geil
Department of Mathematical Sciences
Aalborg University
Fredrik Bajers Vej 7 G
9220 Aalborg East, Denmark
henning@math.aau.dk, olav@math.auc.dk

Abstract

The Feng-Rao bound gives a lower bound on the minimum distance of codes defined by means of their parity check matrices. From the Feng-Rao bound it is clear how to improve a large family of codes by leaving out certain rows in their parity check matrices. In this paper we derive a simple lower bound on the minimum distance of codes defined by means of their generator matrices. From our bound it is clear how to improve a large family of codes by adding certain rows to their generator matrices. Actually our result not only deals with the minimum distance but gives lower bounds on any generalized Hamming weight. We interpret our methods into the setting of order domain theory. In this way we fill in an obvious gap in the theory of order domains. The improved codes from the present paper are not in general equal to the Feng-Rao improved codes but the constructions are very much related.

Key words: Affine variety code, evaluation code, Feng-Rao bound, footprint, generalized Hamming weight, geometric Goppa code, Gröbner basis, minimum distance, order bound, order domain, well-behaving pair.

8.1. Introduction

In [4] Feng and Rao showed how to estimate the minimum distance of a large class of algebraically defined codes by considering certain relations between the rows in the corresponding parity check matrices. This result is known today as the Feng-Rao bound.

Using the bound Feng and Rao were able to improve a large class of well-known codes by leaving out certain rows in the corresponding parity check matrices.

To deal with the above mentioned code constructions, Høholdt, van Lint and Pellikaan in [16] and [15] introduced the concept of an order function acting on what is known today as an order domain ([13]). Then they reformulated the most important results by Feng and Rao in this new setting. Their code constructions includes the set of duals of one-point geometric Goppa codes, the set of Feng-Rao improved such ones, the set of generalized Reed-Muller codes and the set of Feng-Rao improved such ones (the hyperbolic codes). It should be mentioned that independently of Høholdt et al. Miura in [21] and [23] derived many of the same results. Regarding codes defined by means of their generator matrices, Høholdt et al. in [15] only considered the one-point geometric Goppa codes. More precisely, they showed how to prove the Goppa bound without the use of the Riemann-Roch theorem. One of the nice things about order domains is that they can be understood without the use of algebraic geometry. More precisely, it was shown in [21], [22], [24] and [13] how Gröbner basis theory plays a fundamental role in the theory of order domains.

In [21] and [23] Miura observed that the results by Feng and Rao can be obtained by using only linear algebra. In particular one can view the Feng-Rao bound as a bound on the minimum distance of any linear code (with known parity check matrix). Furthermore it was shown in [23] how to improve the Feng-Rao bound slightly in this general set-up. In the present paper we will initially take the general point of view on the Feng-Rao bound from [23]. Later we will translate our findings into the frame work of order domain theory.

What is obviously missing in the above description is a Feng-Rao type bound on the minimum distance of codes which are not defined on the basis of parity check matrices but are defined on the basis of generator matrices. This question was treated by Shibuya and Sakaniwa in [29] where they use the theory of generalized Hamming weights to translate the Feng-Rao bound for the codes defined by means of parity check matrices into a bound for the codes defined by means of generator matrices. The bound derived in this way is of a much more complicated form than the Feng-Rao bound and the problem of improving the codes by using the information from the bound is not so easy. Furthermore, the proof of the bound by Shibuya and Sakaniwa is rather complicated.

In this paper we derive a new and very simple bound on the minimum distance of codes defined by means of their generator matrices. Our bound is of a form very similar to the Feng-Rao bound and in particular from our bound it is obvious how to improve the codes. The proof of the new bound is trivial and our result is at least as good as the result by Shibuya and Sakaniwa. Furthermore our bound not only deals with the minimum distance but actually gives lower bounds on any generalized Hamming weights of the considered codes. We show how to deal with the new bounds and the new code construction from an order domain theoretical point of view. We give some very concrete results on how to deal with the code construction in the case of affine variety codes[1] defined from order domains and we derive some results concerning the connection between the Feng-Rao improved codes and the new improved codes. Also we show how to understand our new bound and code construction from a Gröbner basis theoretical point

[1] So named in [5]

of view. For the case of one-point geometric Goppa codes our bound can easily be shown to be an improvement of the usual bound from algebraic geometry and in many cases we are able to improve substantial on the one-point geometric Goppa code construction. In this way we improve the results in [29] where it was shown that their bound is at least as good as the usual bound from algebraic geometry for the case of one-point geometric Goppa codes from C_{ab} curves. Our new construction and our new bounds can be viewed as a generalization of the recent Gröbner basis theoretical descriptions in [11] and [9] concerning Reed-Muller codes, hyperbolic codes[2] and codes from norm-trace curves. For these codes our bounds are tight.

The paper is organized as follows. In Section 8.2 we are concerned with the general set-up from [23]. Here we introduce our new bound on any linear code defined by means of a generator matrix and relate the new bound to the Feng-Rao bound and the bound by Shibuya and Sakaniwa. In Section 8.3 we describe the relevant concepts from order domain theory and show how to translate our findings from Section 8.2 into the language of order domain theory. In Section 8.4 we treat the connection to the theory of one-point geometric Goppa codes. In Section 8.5 we are concerned with affine variety codes from order domains. Section 8.5 includes a description of order domains from a Gröbner basis theoretical point of view. Section 8.6 contains some examples of codes and Section 8.7 is the conclusion. In Appendix A we deal with the connection between the construction of the present paper and the recent Gröbner basis theoretically defined constructions from [11] and [9].

8.2. The new Feng-Rao type bound

We start by introducing some terminology from [23] (the reader not experienced with Japanese can use [20] as a reference). To ease the comparison with the results in [29] we will mainly use the notation from there.

Definition 8.1 *Let $B = \boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n$ be a basis for $\mathbb{F}_q^n$ and consider $G \subseteq B$. We define the $k = \#G$ dimensional code $C(B,G)$ by $C(B,G) = \mathit{Span}_{\mathbb{F}_q}\{\boldsymbol{b} \mid \boldsymbol{b} \in G\}$. We denote the dual code by $C^{\perp}(B,G)$.*

The following definition plays a central role for the bounds on the minimum distances of the above codes.

Definition 8.2 *For $\boldsymbol{u} = (u_1, u_2, \ldots, u_n), \boldsymbol{v} = (v_1, v_2, \ldots, v_n) \in \mathbb{F}_q^n$ define the component-wise (or Schur or Hadamard) product $\boldsymbol{u} * \boldsymbol{v} = (u_1v_1, u_2v_2, \ldots, u_nv_n)$. Let $\boldsymbol{b}_0 = \boldsymbol{0} \in \mathbb{F}_q^n$ and define $L_l = \mathit{Span}_{\mathbb{F}_q}\{\boldsymbol{b}_0, \boldsymbol{b}_1, \ldots, \boldsymbol{b}_l\}$, for $l = 0, \ldots, n$, and $L_{-1} = \emptyset$.*

We obviously have a chain of spaces $\{\boldsymbol{0}\} = L_0 \subsetneq L1 \subsetneq \cdots \subsetneq L_{n-1} \subsetneq L_n = \mathbb{F}_q^n$ and $\dim(L_i) = i$ holds for $i = 0, 1, \ldots, n$. Next we recall the concept of a well-behaving ordered pair. The function $\bar{\mu}$ below is well-known whereas the function $\bar{\sigma}$ is new.

[2] Also called Massey-Costello-Justesen codes (see [17] and [18].

Definition 8.3 *Define* $\bar{\rho} : \mathbb{F}_q^n \rightarrow \{0, 1, \ldots, n\}$ *by* $\bar{\rho}(\boldsymbol{v}) = l$ *if* $\boldsymbol{v} \in L_l \setminus L_{l-1}$*. Let* $I = \{1, 2, \ldots, n\}$*. An ordered pair* $(i, j) \in I^2$ *is said to be well-behaving (WB) if* $\bar{\rho}(\boldsymbol{b}_u * \boldsymbol{b}_v) < \bar{\rho}(\boldsymbol{b}_i * \boldsymbol{b}_j)$ *for all* u *and* v *with* $1 \leqslant u \leqslant i, 1 \leqslant v \leqslant j$ *and* $(u, v) \neq (i, j)$*. An ordered pair* $(i, j) \in I^2$ *is said to be weakly well-behaving (WWB) if* $\bar{\rho}(\boldsymbol{b}_u * \boldsymbol{b}_j) < \bar{\rho}(\boldsymbol{b}_i * \boldsymbol{b}_j)$ *for* $u < i$ *and* $\bar{\rho}(\boldsymbol{b}_i * \boldsymbol{b}_v) < \bar{\rho}(\boldsymbol{b}_i * \boldsymbol{b}_j)$ *for* $v < j$*. For* $\{l_1, l_2, \ldots, l_t\} \subseteq I$ *and* $\{i_1, i_2, \ldots, i_t\} \subseteq I$ *define*[3]

$$\bar{\mu}(l_1, l_2, \ldots, l_t) = \# \bigcup_{s=1,2,\ldots,t} \{(i, j) \in I^2 \mid \bar{\rho}(\boldsymbol{b}_i * \boldsymbol{b}_j) = l_s \textit{ and } (i, j) \textit{ is WWB } \}$$

$$\bar{\sigma}(i_1, i_2, \ldots, i_t) = \# \bigcup_{s=1,2,\ldots,t} \Big(\{l \in I \mid \bar{\rho}(\boldsymbol{b}_{i_s} * \boldsymbol{b}_j) = l \textit{ for some } \boldsymbol{b}_j \in B$$
$$\textit{such that } (i_s, j) \textit{ is WWB } \} \cup \{i_s\}\Big).$$

We now state the celebrated Feng-Rao bound in the general version from [23, p. 1389].

Theorem 8.4 (Feng-Rao) *The minimum distance of* $C^{\perp}(B, G)$ *is at least equal to* $\min\{\bar{\mu}(i) \mid \boldsymbol{b}_i \in B \setminus G\}$*.*

A lower bound on the generalized Hamming weights of the codes $C^{\perp}(B, G)$ can be found in [25]. This bound, however, is not nearly as simple as the one we are going to present for the codes $C(B, G)$. In Definition 8.5 below we give the formal definition from [31] of the generalized Hamming weights. Recall, that for every $\boldsymbol{v} = (v_1, v_2, \ldots, v_n) \in \mathbb{F}_q^n$ the set $\mathrm{Supp}(\boldsymbol{v}) = \{i \mid v_i \neq 0\}$ is called the support of $\boldsymbol{v}$ and in general for any subset $A \in \mathbb{F}_q^n$ the set $\mathrm{Supp}(A) = \bigcup_{\boldsymbol{v} \in A} \mathrm{Supp}(\boldsymbol{v})$ is called the support of A.

Definition 8.5 *Consider a* k *dimensional code* C*. For* $t = 1, 2, \ldots, k$ *the* t*-th generalized Hamming weight is*

$$d_t(C) = \min\{\#\mathrm{Supp}(D) \mid D \textit{ is a } t \textit{ dimensional subcode of } C\}.$$

We next state the new Feng-Rao type bound on the generalized Hamming weights of the code $C(B, G)$.

Theorem 8.6 *Let* $G \subseteq B$ *with* $\#G = k$ *be fixed. For* $t = 1, 2, \ldots, k$ *the generalized Hamming weight* $d_t(C(B, G))$ *is at least equal to*

$$\min\{\bar{\sigma}(a_1, a_2, \ldots, a_t) \mid a_i \neq a_j \textit{ for } i \neq j \textit{ and } \{\boldsymbol{b}_{a_1}, \boldsymbol{b}_{a_2}, \ldots, \boldsymbol{b}_{a_t}\} \subseteq G\}.$$

[3] We note that writing WWB rather than only WB in the definition of $\bar{\mu}$ and $\bar{\sigma}$ strengthens the results to be presented in this paper. This is due to the fact that an ordered pair that is WB is of course also WWB.

In particular the minimum distance of $C(B,G)$ is at least equal to

$$\min\{\bar{\sigma}(i) \mid \boldsymbol{b}_i \in G\} = \min\{\#(\{l \in I \mid \bar{\rho}(\boldsymbol{b}_i * \boldsymbol{b}_j) = l \textit{ for some } \boldsymbol{b}_j \in B \\ \textit{such that } (i,j) \textit{ is WWB } \} \cup \{i\}) \mid \boldsymbol{b}_i \in G\}.$$

Proof: Denote $G = \{\boldsymbol{b}_{i_1}, \boldsymbol{b}_{i_2}, \ldots, \boldsymbol{b}_{i_k}\}$ where $i_1 < i_2 < \cdots < i_k$ holds. Let $D \subseteq C(B,G)$ be a subspace of dimension t, $t \leqslant k$. Consider basis vectors $\boldsymbol{d}_1, \boldsymbol{d}_2, \ldots, \boldsymbol{d}_t$ for D

$$\boldsymbol{d}_u = \sum_{s=1}^{k} \alpha_s^{(u)} \boldsymbol{b}_{i_s}, u = 1, 2, \ldots, t.$$

By a standard linear algebra result we may without loss of generality assume that

$$\max\{s \mid \alpha_s^{(v)} \neq 0\} \neq \max\{s \mid \alpha_s^{(w)} \neq 0\}$$

holds for any v, w with $v \neq w$. As by definition

$$\bar{\rho}(\boldsymbol{d}_u) = \max\{i_s \mid \alpha_s^{(u)} \neq 0\}$$

holds. The above assumption corresponds to assuming that $\bar{\rho}(\boldsymbol{d}_v) \neq \bar{\rho}(\boldsymbol{d}_w)$, for $v \neq w$. Let $a_u = \bar{\rho}(\boldsymbol{d}_u)$, for $u = 1, 2, \ldots, t$. We observe that if (a_u, j) is WWB for some $j \in \{1, 2, \ldots, n\}$ and $\bar{\rho}(\boldsymbol{b}_{a_u} * \boldsymbol{b}_j) = l$ (equivalent to saying $\boldsymbol{b}_{a_u} * \boldsymbol{b}_j \in L_l \setminus L_{l-1}$) then by the very definition of WWB we have

$$\begin{aligned} \bar{\rho}(\boldsymbol{d}_u * \boldsymbol{b}_j) &= \bar{\rho}\left(\sum_{s=1}^{k} \alpha_s^{(u)} (\boldsymbol{b}_{i_s} * \boldsymbol{b}_j)\right) \\ &= \bar{\rho}(\boldsymbol{b}_{a_u} * \boldsymbol{b}_j) \\ &= l. \end{aligned}$$

Hence, the set

$$S = \left(\bigcup_{u=1}^{t} \{\boldsymbol{d}_u * \boldsymbol{b}_j \mid (a_u, j) \text{ is WWB } \}\right) \cup \{\boldsymbol{d}_1, \boldsymbol{d}_2, \ldots, \boldsymbol{d}_t\} \tag{8.1}$$

contains at least

$$\begin{aligned} \#\Bigg(\bigg(\bigcup_{u=1,2,\ldots,t} &\{l \in I \mid \bar{\rho}(\boldsymbol{b}_{a_u} * \boldsymbol{b}_j) = l \text{ for some } \boldsymbol{b}_j \in B \\ &\text{such that } (a_u, j) \text{ is WWB } \}\bigg) \cup \{a_1, a_2, \ldots, a_t\}\Bigg) \\ = \bar{\sigma}(a_1, a_2, \ldots, a_t)& \end{aligned}$$

linearly independent vectors. But the support of S is equal to the support of $\{\boldsymbol{d}_1, \boldsymbol{d}_2, \ldots, \boldsymbol{d}_t\}$ which in turn is equal to the support of D. Hence, the size of the support of D is at least $\bar{\sigma}(a_1, a_2, \ldots, a_t)$. □

Remark 8.7 Notice that in [30, 28, 26, 27] Shibuya, Mizutani and Sakaniwa give bounds on the generalized Hamming weights of the $C(B,G)^{\perp}$ codes, thus the result in [31, Thm. 3] can be used to translate their findings into lower bounds on the generalized Hamming weights of the $C(B,G)$ codes. However, this method is rather complicated and requires that one is able to find all the generalized Hamming weights of the $C(B,G)^{\perp}$ codes, which can be computationally hard for large codes. $\triangledown$

It is now obvious how to optimize the choice of G to obtain the best codes with respect to the above bound. These are the $\tilde{E}(\delta)$ codes below. For use in Section 8.3 we also define the more naive codes $E(s)$.

Definition 8.8 *Let $B = \{\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n\}$ be a basis for $\mathbb{F}_q^n$. For $s = 1, 2, \ldots, n$ and $\delta = 0, 1, \ldots, n$ define*

$$\begin{aligned} E(s) &= \mathit{Span}_{\mathbb{F}_q}\{\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_s\} \\ \tilde{E}(\delta) &= \mathit{Span}_{\mathbb{F}_q}\{\boldsymbol{b}_i \mid \bar{\sigma}(i) \geqslant \delta\} \end{aligned}$$

Theorem 8.9 *The minimum distance of $E(s)$ is at least equal to* $\min\{\bar{\sigma}(i) \mid i = 1, 2, \ldots, s\}$. *The minimum distance of $\tilde{E}(\delta)$ is at least equal to δ.*

Proof: By Theorem 8.6. $\square$

In Appendix A it is shown that the hyperbolic codes (improved generalized Reed-Muller codes) and the improved one-point geometric Goppa codes from norm-trace curves described in [9] are special examples of the codes $\tilde{E}(\delta)$ of the present paper. Also it is shown that the bounds in Theorem 8.9 are tight for the Reed-Muller codes, the hyperbolic codes, the one-point geometric Goppa codes from norm-trace curves and for the improved one-point geometric Goppa codes from norm-trace curves. We conclude this section by relating the result in Theorem 8.6 to the result by Shibuya and Sakaniwa in [29]. Their result is as follows.

Theorem 8.10 (Shibuya, Sakaniwa) *For given B and G let for $i = 1, 2, \ldots, n$*

$$\mathcal{B}'_i = \{l \in I \mid \bar{\rho}(\boldsymbol{b}_i * \boldsymbol{b}_j) = l \text{ for some } \boldsymbol{b}_j \in B \text{ such that } (i,j) \text{ is WWB }\}$$

and $\mathcal{B}_i = \{\nu \mid \boldsymbol{b}_\nu \in B \setminus G\} \setminus \mathcal{B}'_i$. Define $t(B,G) = \max\{\#\mathcal{B}_i \mid \boldsymbol{b}_i \in G\}$. The minimum distance of $C(B,G)$ is at least $n - k + 1 - t(B,G)$.

Proposition 8.11 *The bound on the minimum distance of $C(B,G)$ in Theorem 8.6 is at least as good as the bound in Theorem 8.10.*

Proof: For $i = 1, 2, \ldots, n$ we have

$$\bar{\sigma}(i) = \#(\mathcal{B}'_i \cup \{i\}). \tag{8.2}$$

The set $\mathcal{B}_i$ consist of the basis elements outside G that does not contribute to the counting in (8.2). Hence, the number of basis elements outside G that contribute to the counting in (8.2) is $n-k-\#\mathcal{B}_i$. For i such that $\boldsymbol{b}_i \in G$ the number of elements in G that contribute to the counting in (8.2) is at least equal to $\#\{i\} = 1$. All together $n-k+1-\#\mathcal{B}_i \leqslant \bar{\sigma}(i)$ holds for all i such that $\boldsymbol{b}_i \in G$. □

8.3. Codes defined from order domains

In the previous section we saw how to estimate the parameters of any linear code. For the methods to be really practical we will need bases $B = \{\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n\}$ for $\mathbb{F}_q^n$ for which it is easy to decide if a given ordered pair (i, j) is WB (or WWB) and to calculate $\bar{\rho}(\boldsymbol{b}_i * \boldsymbol{b}_j)$. This is where order domain theory comes into action. The presentation of order domain theory to be given in this paper mostly relies on [13] where the concepts of an order function and a weight function from [15] are generalized.

Recall, that if Γ is a set and $\prec$ is a total ordering on Γ then $(\Gamma, \prec)$ is called a well-order if every non-empty subset of Γ has a smallest element with respect to $\prec$. Given a well-order $(\Gamma, \prec)$ we adjoin an element $-\infty$ to Γ to get $\Gamma_{-\infty} = \Gamma \cup \{-\infty\}$. The ordering $\prec$ extends to an ordering on $\Gamma_{-\infty}$ by the rule $-\infty \prec \gamma$ for all $\gamma \in \Gamma$. Clearly $(\Gamma_{-\infty}, \prec)$ is a well-order. The following definition corresponds to [13, Def. 2.1] (with the little change that in this paper we require an order function to be surjective).

Definition 8.12 *Let $(\Gamma, \prec)$ be a well-order. Let $\mathbb{F}$ be a field and let R be an $\mathbb{F}$-algebra (see [3, p. 36]). A surjective map $\rho : R \rightarrow \Gamma$ that satisfies the following five conditions is called an order function.*

$(O.0)$ $\rho(f) = -\infty$ *if and only if* $f = 0$

$(O.1)$ $\rho(af) = \rho(f)$ *for all non-zero* $a \in \mathbb{F}$

$(O.2)$ $\rho(f+g) \preceq \max\{\rho(f), \rho(g)\}$ *and equality holds when* $\rho(f) \prec \rho(g)$

$(O.3)$ *If* $\rho(f) \prec \rho(g)$ *and* $h \neq 0$, *then* $\rho(fh) \prec \rho(gh)$

$(O.4)$ *If* f *and* g *are non-zero and* $\rho(f) = \rho(g)$, *then there exists a non-zero* $a \in \mathbb{F}$ *such that* $\rho(f - ag) \prec \rho(g)$ *for all* $f, g \in R$.

We call (R, ρ, Γ) an order structure and R an order domain (over $\mathbb{F}$).

The order function being surjective ensures the existence of sets of the form $\{f_\gamma \mid \rho(f_\gamma) = \gamma\}_{\gamma \in \Gamma}$. From [13, Def. 3.1 and Pro. 3.2] we have

Theorem 8.13 *Given an order structure (R, ρ, Γ) then any set $\mathcal{B} = \{f_\gamma \mid \rho(f_\gamma) = \gamma\}_{\gamma \in \Gamma}$ constitutes a basis for R as a vector space over $\mathbb{F}$. For any $f = c_{\gamma_1} f_{\gamma_1} + c_{\gamma_2} f_{\gamma_2} + \cdots + c_{\gamma_d} f_{\gamma_d}$*

with $c_{\gamma_1}, c_{\gamma_2}, \ldots, c_{\gamma_d} \in \mathbb{F} \setminus \{0\}, \rho(f) = \max_{\prec}\{1, 2, \ldots, d\}$ holds. In particular $\{f_\lambda \in \mathcal{B} \mid \lambda \preceq \gamma\}$ constitutes a basis for $R_\gamma = \{f \in R \mid \rho(f) \preceq \gamma\}$ as a vector space over $\mathbb{F}$.

From [13, Def. 3.1 and Pro. 3.3] we have

Definition 8.14 *The set $\{f_\gamma \mid \rho(f_\gamma) = \gamma\}_{\gamma \in \Gamma}$ in Theorem 8.13 is called a well-behaving basis (for R).*

Besides the trivial case $R = \mathbb{F}$ order domains are always of transcendence degree at least 1. Hence, for non-trivial order domains the well-behaving basis $\{f_\gamma \mid \rho(f_\gamma) = \gamma\}_{\gamma \in \Gamma}$ consists of infinitely many elements. In this paper we will always assume that the order domain under consideration is non-trivial. The following well-known concept will help us construct the finite bases B needed in the code constructions from the previous section.

Definition 8.15 *Let R be an $\mathbb{F}_q$-algebra. A srjective map $\varphi : R \rightarrow \mathbb{F}_q^n$ is called a morphism of $\mathbb{F}_q$-algebras if φ is $\mathbb{F}_q$-linear and $\varphi(fg) = \varphi(f) * \varphi(g)$ for all $f, g \in R$.*

In the remaining part of this section an order domain R will always be assumed to be an order domain over $\mathbb{F}_q$. To derive the finite bases B we will just need the following definition.

Definition 8.16 *Let 0 be the smallest element of Γ and define $\alpha(1) = 0$. For $i = 2, 3, \ldots, n$ define recursively $\alpha(i)$ to be the smallest element in Γ that is greater than $\alpha(1), \alpha(2), \ldots, \alpha(i-1)$ and satisfies $\varphi(R_\gamma) \subsetneq \varphi(R_{\alpha(i)})$, for all $\gamma \prec \alpha(i)$. Write $\Delta(R, \rho, \varphi)$ $= \{\alpha(1), \alpha(2), \ldots, \alpha(n)\}$.*

The following theorem is easily proven.

Theorem 8.17 *Let $\Delta(R, \rho, \varphi) = \{\alpha(1), \alpha(2), \ldots, \alpha(n)\}$ be as in Definition 8.16. The set*

$$B = \{\boldsymbol{b}_1 = \varphi(f_{\alpha(1)}), \boldsymbol{b}_2 = \varphi(f_{\alpha(2)}), \ldots, \boldsymbol{b}_n = \varphi(f_{\alpha(n)})\} \tag{8.3}$$

constitutes a basis for $\mathbb{F}_q^n$ as a vector space over $\mathbb{F}_q$. For any $\boldsymbol{c} \in \mathbb{F}_q^n$ there exists a unique ordered set $\{\beta_1, \beta_2, \ldots, \beta_n\}, \beta_i \in \mathbb{F}_q$ such that $\boldsymbol{c} = \varphi(\sum_{i=1}^n \beta_i f_{\alpha(i)})$. The function $\bar{\rho} : \mathbb{F}_q^n \rightarrow \{0, 1, \ldots, n\}$ corresponding to B is given by

$$\bar{\rho}(c) = \begin{cases} 0 & \textit{if } c = 0 \\ \max\{i \mid \beta_i \neq 0\} & \textit{otherwise} \end{cases}$$

In the remaining part of this paper we will always assume that the basis $B = \{\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n\}$ is of the form in (8.3). According to our agenda we should now be concerned with studying which ordered pairs $(i, j) \in I^2$ that are well-behaving. The following two propositions will give us precisely the information that we need. The results described in these propositions can be found in [21], [23], [20] and [29] for the case of the order domain being of transcendence degree 1 or the order domain being equal to $\mathbb{F}_q[x_1, x_2, \ldots, x_m]$. Here we state the results explicit and for all non-trivial order domains.

Proposition 8.18 *Let $B = \{\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots, \boldsymbol{b}_n\}$ be the basis in (8.3). If $\alpha(i), \alpha(j), \alpha(l) \in \Delta(R, \rho, \varphi)$ are such that $\rho(f_{\alpha(i)} f_{\alpha(j)}) = \alpha(l)$ then $\bar{\rho}(\boldsymbol{b}_i * \boldsymbol{b}_j) = l$ and $(i, j) \in I^2$ is WB.*

Proof: We first show $\bar{\rho}(\boldsymbol{b}_i * \boldsymbol{b}_j) = l$. We have

$$\begin{aligned}
&\rho(f_{\alpha(i)} f_{\alpha(j)}) = \alpha(l) \\
&\Downarrow \\
&f_{\alpha(i)} f_{\alpha(j)} \in R_{\alpha(l)} \text{ and } f_{\alpha(i)} f_{\alpha(j)} \notin R_\gamma \text{ for any } \gamma \prec \alpha(l) \\
&\Downarrow \\
&\varphi(f_{\alpha(i)} f_{\alpha(j)}) \in \varphi(R_{\alpha(l)}) = L_l \text{ and } \varphi(f_{\alpha(i)} f_{\alpha(j)}) \notin L_w \text{ for any } w < l \\
&\Downarrow \\
&\varphi(f_{\alpha(i)} f_{\alpha(j)}) \in L_l \setminus L_{l-1} \\
&\Downarrow \\
&\boldsymbol{b}_i * \boldsymbol{b}_j \in L_l \setminus L_{l-1} \\
&\Downarrow \\
&\bar{\rho}(\boldsymbol{b}_i * \boldsymbol{b}_j) = l.
\end{aligned}$$

Next we show that (i, j) is WB. Let $1 \leqslant u \leqslant i, 1 \leqslant v \leqslant j$ with $(u, v) \neq (i, j)$. By condition (O.3) in Definition 8.12 we have $\rho(f_{\alpha(u)} f_{\alpha(v)}) \prec \alpha(l)$. But then by Definition 8.15 and Definition 8.16 we have $\boldsymbol{b}_u * \boldsymbol{b}_v = \varphi(f_{\alpha(u)} f_{\alpha(v)}) \in \varphi(R_\gamma) \subseteq L_{l-1}$ for some $\gamma \prec \alpha(l)$. This implies $\bar{\rho}(\boldsymbol{b}_u * \boldsymbol{b}_v) \leqslant l - 1$ and consequently $(\alpha(i), \alpha(j))$ is WB. □

Proposition 8.19 *Consider $\alpha(l) \in \Delta(R, \rho, \varphi)$ and assume $\beta_1, \beta_2 \in \Gamma$ satisfies $\rho(f_{\beta_1} f_{\beta_2}) = \alpha(l)$. Then $\beta_1, \beta_2 \in \Delta(R, \rho, \varphi)$ holds.*

Proof: By definition we have $f_{\beta_1} f_{\beta_2} \in R_{\alpha(l)}$ but $f_{\beta_1} f_{\beta_2} \notin R_\gamma$ for any $\gamma \prec \alpha(l)$. By symmetry it is enough to show that $\beta_1 \in \Delta(R, \rho, \varphi)$. We will assume that this is not the case and arrive at a contradiction. That is, we will assume that there exists $\omega \in \Gamma$ such that $\omega \prec \beta_1$ and $\varphi(f_{\beta_1}) \in \varphi(R_\omega)$. But then there exists $g \in R_\omega$ with $\varphi(g) = \varphi(f_{\beta_1})$ implying that $\varphi(g f_{\beta_2}) = \varphi(f_{\beta_1} f_{\beta_2})$. By (O.3) in Definition 8.12 and the fact that $\rho(g) \preceq \omega \prec \beta_1$ we have $\rho(g f_{\beta_2}) \prec \rho(f_{\beta_1} f_{\beta_2})$. Hence, there exists $\gamma \prec \alpha(l)$ such that $\varphi(f_{\beta_1} f_{\beta_2}) \in \varphi(R_\gamma)$. This is not possible according to the definition of $\alpha(l)$. □

We are now in the position that we can give a simple description of the codes $C^\perp(B, G)$ and $C(B, G)$ related to order domains. To this end consider Definition 8.20 and Definition 8.21 below. Here the N and μ notation is a slightly modification of the notation in [15, Def. 4.8], whereas the M and σ notation is new.

Definition 8.20 *For $\lambda \in \Gamma$ define*

$$N(\lambda) = \{(\alpha, \beta) \in \Gamma^2 \mid \rho(f_\alpha f_\beta) = \lambda\}.$$

Define $\mu(\lambda) = \#N(\lambda)$ if $N(\lambda)$ is finite and $\mu(\lambda) = \infty$ if not. For $\eta \in \Delta(R, \rho, \varphi) = \{\alpha(1), \alpha(2), \ldots, \alpha(n)\}$ define

$$M(\eta) = \{\gamma \in \Delta(R, \rho, \varphi) \mid \exists \beta \in \Delta(R, \rho, \varphi) \text{ with } \rho(f_\eta f_\beta) = \gamma\}$$

and $\sigma(\eta) = \#M(\eta)$.

Definition 8.21 *Let $t \leqslant n$ and $\{\eta_1, \eta_2, \ldots, \eta_t\} \subseteq \Delta(R, \rho, \varphi)$. Define $\sigma(\eta_1, \eta_2, \ldots, \eta_t) = \#(\bigcup_{i=1}^{t} M(\eta_i))$.*

The codes are now defined as follows.

Definition 8.22 *Consider a well-behaving basis $\{f_\lambda \mid \rho(f_\lambda) = \lambda\}_{\lambda \in \Gamma}$ for an order structure (R, ρ, Γ) over $\mathbb{F}_q$. Let φ be a morphism as in Definition 8.15 and let $B = \{\boldsymbol{b}_1 = \varphi(f_{\alpha(1)}), \boldsymbol{b}_2 = \varphi(f_{\alpha(2)}), \ldots, \boldsymbol{b}_n = \varphi(f_{\alpha(n)})\}$ as in (8.3). Define*

$$\begin{aligned}
C(\lambda) &= \{\boldsymbol{c} \in \mathbb{F}_q^n \mid \boldsymbol{c} \cdot \varphi(f_\gamma) = 0 \text{ for all } \gamma \preceq \lambda\} \\
&= (\varphi(R_\lambda))^\perp \\
\tilde{C}(\delta) &= \{\boldsymbol{c} \in \mathbb{F}_q^n \mid \boldsymbol{c} \cdot \varphi(f_{\alpha(i)}) = 0 \text{ for all } \alpha(i) \in \Delta(R, \rho, \varphi) \text{ with } \mu(\alpha(i)) < \delta\} \\
E(\lambda) &= \varphi(R_\lambda) \\
\tilde{E}(\delta) &= \mathit{Span}_{\mathbb{F}_q}\left\{\varphi(f_{\alpha(i)}) \mid \alpha(i) \in \Delta(R, \rho, \varphi) \text{ and } \sigma(\alpha(i)) \geqslant \delta\right\}.
\end{aligned}$$

The result concerning $C(\lambda)$ and $\tilde{C}(\delta)$ in the next theorem is from [15]. The result concerning $C(\lambda)$ is known as the order bound. The remaining results are new.

Theorem 8.23 *The minimum distance of $C(\lambda)$ and $\tilde{C}(\delta)$ satisfy*

$$\begin{aligned}
d(C(\lambda)) &\geqslant \min\{\mu(\eta) \mid \lambda \prec \eta, \eta \in \Delta(R, \rho, \varphi)\} && (8.4) \\
&\geqslant \min\{\mu(\eta) \mid \lambda \prec \eta\} && (8.5) \\
d(\tilde{C}(\delta)) &\geqslant \delta. && (8.6)
\end{aligned}$$

The t-th generalized Hamming weight of $E(\lambda)$ and $\tilde{E}(\delta)$ (t being at most equal to the dimension of the code) satisfies

$$\begin{aligned}
d_t(E(\lambda)) \geqslant \min\{&\sigma(\eta_1, \eta_2, \ldots, \eta_t) \mid \{\eta_1, \eta_2, \ldots, \eta_t\} \subseteq \Delta(R, \rho, \varphi) \\
&\eta_i \neq \eta_j \text{ for } i \neq j, \eta_s \preceq \lambda \text{ for } s = 1, 2, \ldots, t\} && (8.7) \\
d_t(\tilde{E}(\delta)) \geqslant \min\{&\sigma(\eta_1, \eta_2, \ldots, \eta_t) \mid \{\eta_1, \eta_2, \ldots, \eta_t\} \subseteq \Delta(R, \rho, \varphi) \\
&\eta_i \neq \eta_j \text{ for } i \neq j, \sigma(\eta_s) \geqslant \delta \text{ for } s = 1, 2, \ldots, t\}. && (8.8)
\end{aligned}$$

In particular

$$d(E(\lambda)) \geqslant \min\{\sigma(\eta) \mid \eta \in \Delta(R,\rho,\varphi), \eta \preceq \lambda\} \tag{8.9}$$

$$d(\tilde{E}(\delta)) \geqslant \delta. \tag{8.10}$$

Proof: Using the notation from Definition 8.3 and Definition 8.20 and the results from Proposition 8.18 and Proposition 8.19 we verify that $\bar{\mu}(i) \geqslant \mu(\alpha(i))$. To see that also $\bar{\sigma}(i) \geqslant \sigma(\alpha(i))$ we note that by [13, Pro. 2.5] the following holds. If the smallest element in Γ is denoted 0 then the elements in R that satisfy $\rho(f) = 0$ are precisely the elements in $\mathbb{F}_q \setminus \{0\}$. Hence, by condition $(O.1)$ in Definition 8.12 we have $\rho(f_0 f_\gamma) = \gamma$ for all $\gamma \in \Gamma$ and therefore by Proposition 8.18 and Proposition 8.19 $\bar{\sigma}(i) \geqslant \sigma(\alpha(i))$ holds. The theorem now follows by applying Theorem 8.4 and Theorem 8.6. □

It is obvious that with respect to the above bounds the $\tilde{C}(\delta)$ construction is an improvement to the $C(\lambda)$ construction and the $\tilde{E}(\delta)$ construction is an improvement to the $E(\lambda)$ construction. In Section 8.4 we will recall the well-known fact that every one-point geometric Goppa code can be described as an $E(\lambda)$ code related to an order domain of transcendence degree 1, and we will show by a very easy argument that the bound in (8.9) is an improvement to the usual bound from algebraic geometry.

We conclude this section by discussing the concept of a weight function. It is well-known that the order function ρ induces a binary operation on Γ by $\rho(f) + \rho(g) = \rho(fg)$. This turns Γ into a semigroup called the value semigroup of ρ. The order structure (R, ρ, Γ) is called finitely generated if the value semigroup is finitely generated. Whenever an order structure (R, ρ, Γ) is finitely generated then by [13, Cor. 5.7] we may without loss of generality assume that the order function is a weight function as in the following definition.

Definition 8.24 *Let $\prec$ be a monomial ordering on $\mathbb{N}_0^r$ and let $+$ be the ordinary $+$ extended with the rule $-\infty + a = a + (-\infty) = -\infty + (-\infty) = -\infty$. Let R be an $\mathbb{F}$-algebra. A weight function on R is an order function $\rho : R \to \Gamma \cup \{-\infty\} \subseteq \mathbb{N}_0^r \cup \{-\infty\}$ such that*

$$(O.5) \quad \rho(fg) = \rho(f) + \rho(g) \text{ for all } f, g \in R.$$

The calculation of the values of the functions μ and σ becomes much easier whenever ρ is not just an order function but merely a weight function. We have

$$\begin{aligned} N(\lambda) &= \{(\alpha,\beta) \in \Gamma^2 \mid \alpha + \beta = \lambda\} \\ M(\eta) &= \{\gamma \in \Delta(R,\rho,\varphi) \mid \exists \beta \in \Delta(R,\rho,\varphi) \text{ with } \eta + \beta = \gamma\} \\ &= (\eta + \Gamma) \cap \Delta(R,\rho,\varphi) \end{aligned} \tag{8.11}$$

where $\eta + \Gamma$ means $\{\eta + \lambda \mid \lambda \in \Gamma\}$.

8.4. Improved one-point geometric Goppa codes

In this section we will see how to construct improved one-point geometric Goppa codes and we will see how to improve on the Goppa bound. The following example is well-known (see [15, Ex. 3.8] and [19, Th. 1]).

Example 8.25 Consider a curve $\mathcal{X}$ with a single place $P_{-\infty}$ at infinity. Let $\nu_{P_{-\infty}}$ denote the discrete valuation corresponding to the place $P_{-\infty}$. Let R be any subring of the union of $\mathcal{L}$-spaces corresponding to $P_{-\infty}$. That is, let $R \subseteq \bigcup_{i=0}^{\infty} \mathcal{L}(iP_{-\infty})$. Then R is an order domain with a weight function given by $\rho(f) = -\nu_{P_{-\infty}}(f)$. It is well-known that all weight functions with a numerical value semigroup are of the form described in this example. △

From Example 8.25 it is clear that the one-point geometric Goppa codes are precisely the codes $E(\lambda)$ defined from order structures with a weight function with a numerical value semigroup. In the same way of course the duals of one-point geometric Goppa codes are precisely the codes $C(\lambda)$ defined from order structures with a weight function with a numerical value semigroup. By [15, Th. 5.24] the bound (8.5) and thereby also (8.4) are improvements to the Goppa bound for the duals of one-point geometric Goppa codes. Clearly, the corresponding codes $\tilde{C}(\delta)$ become improvements to the duals of one-point geometric Goppa codes.

By using the following lemma from [15, Lem. 5.15] we now give an easy proof that also the bound (8.9) is an improvement to the Goppa bound for the one-point geometric Goppa codes. It follows that the codes $\tilde{E}(\delta)$ can be viewed as improved one-point geometric Goppa codes.

Lemma 8.26 *Let Γ be a numerical semigroup with finitely many gaps. Let $i \in \Gamma$. Then the number of elements of $\Gamma \setminus (i + \Gamma)$ is equal to i.*

Now the Goppa bound for the one-point geometric Goppa code $E(\lambda)$ says $d(E(\lambda)) \geqslant n - \lambda$. For comparison, by (8.11) the bound (8.9) states

$$d(E(\lambda)) \geqslant \min\{\#((i + \Gamma) \cap \Delta(R, \rho, \varphi)) \mid i \in \Gamma, i \leqslant \lambda\}.$$

By Lemma 8.26 we have

$$\#((i + \Gamma) \cap \Delta(R, \rho, \varphi)) \geqslant n - i$$

with equality if and only if $\Gamma \setminus (i + \Gamma) \subseteq \Delta(R, \rho, \varphi)$. In particular for λ being of a high value compared to n the just mentioned condition for equality often turns out not be fulfilled and the new bound will be an improvement to the Goppa bound. We have proved the last part of the following proposition.

Proposition 8.27 *Any one-point geometric Goppa code is of the form $E(\lambda)$ in Definition 8.22 and the bound (8.9) is an improvement to the Goppa bound.*

For comparison, Shibuya et al. in [29] only show that their bound (Theorem 8.10) is an improvement to the Goppa bound in the case of codes defined from C_{ab} curves and in the case of some codes coming from Garcia and Stichtenoth's tower in [6]. In Section 8.6 we shall demonstrate that the new bound (8.9) can be much better than the Goppa bound and that the new construction $\tilde{E}(\delta)$ can be much better than traditional one-point geometric Goppa code.

8.5. The Gröbner basis approach

In this section we shall see how to easily construct order domains and related codes by the use of Gröbner basis theoretical methods. We start by introducing some concepts from Gröbner basis theory.

Definition 8.28 *Denote by $\mathcal{M}(x_1, x_2, \ldots, x_m)$ the set of monomials in $x_1, x_2, \ldots, x_m$. Given a monomial ordering $\prec$ on $\mathcal{M}(x_1, x_2, \ldots, x_m)$ and an ideal $L \subseteq \mathbb{F}[x_1, x_2, \ldots, x_m]$ the footprint*[4] *of L is the set*

$$\Delta_{\prec}(L) = \{M \in \mathcal{M}(x_1, x_2, \ldots, x_m) \mid M \textit{ is not a leading monomial of any polynomial in } L\}.$$

The following well-known proposition (for a reference, see [2, Pro. 4 in Paragraph 5.3]) explains why footprints are interesting.

Proposition 8.29 *Let $L \subseteq \mathbb{F}[x_1, x_2, \ldots, x_m]$ be any ideal, then $\{M + L \mid M \in \Delta_{\prec}(L)\}$ is a basis for $\mathbb{F}[x_1, x_2, \ldots, x_m]/L$ as a vectors pace over $\mathbb{F}$.*

The first part of the following proposition is a corollary to Proposition 8.29. It is known as the footprint bound. A proof of the proposition below can be found in [2, §5.3, Pro. 8] and [3, Pro. 2.7].

Proposition 8.30 *If $\Delta_{\prec}(L)$ is finite then the size of the variety $\mathbb{V}_{\mathbb{F}}(L)$ is bounded by*

$$\#\mathbb{V}_{\mathbb{F}}(L) \leqslant \#\Delta_{\prec}(L). \tag{8.12}$$

If L is a radical ideal and $\mathbb{F}$ is algebraically closed then equality holds in (8.12). In particular equality holds when $L \subseteq \mathbb{F}_q[x_1, x_2, \ldots, x_m]$ and $x_1^q - x_1, x_2^q - x_2, \ldots, x_m^q - x_m \in L$.

We will need the following generalization from [13, Def. 9.2] of the usual weighted degree lexicographic ordering.

[4] The name "footprint" was suggested by D. Blahut in 1991. The footprint was previously called the delta-set, the excluded point set and other things (see [14]).

Definition 8.31 *Given weights $w(x_1), w(x_2), \ldots, w(x_m) \in \mathbb{N}_0^r \setminus \{\mathbf{0}\}$ let $\mathbb{N}_0^r$ be ordered by some fixed monomial ordering $\prec_{\mathbb{N}_0^r}$ and let $\prec_{\mathcal{M}}$ be a fixed monomial ordering on $\mathcal{M}(x_1, x_2, \ldots, x_m)$. The weights extends to a monomial function $w : \mathcal{M}(x_1, x_2, \ldots, x_m) \to \mathbb{N}_0^r$ by $w(x_1^{a_1} x_2^{a_2} \cdots x_m^{a_m}) = \sum_{i=1}^m a_i w(x_i)$. For a monomial M we call $w(M)$ the weight of M. We define the weighted degree* wdeg(F) *of a polynomial F to be the highest weight (with respect to $\prec_{\mathbb{N}_0^r}$) that appears as a weight of a monomial in the support of F. Now the generalized weighted degree ordering $\prec_w$ induced by $w, \prec_{\mathbb{N}_0^r}$ and $\prec_{\mathcal{M}}$ is the monomial ordering defined as follows. Given $M_1, M_2 \in \mathcal{M}(x_1, x_2, \ldots, x_m)$ then $M_1 \prec_w M_2$ if and only if one of the following two conditions holds:*

$$\begin{aligned} &(1) \quad w(M_1) \prec_{\mathbb{N}_0^r} w(M_2) \\ &(2) \quad w(M_1) = w(M_2) \textit{ and } M_1 \prec_{\mathcal{M}} M_2. \end{aligned}$$

The next theorem characterizes all finitely generated order structures. Note that in particular (R, ρ, Γ) is finitely generated if ρ is a weight function with a numerical value semigroup. It corresponds to [13, Th. 9.1 and Th. 10.4].

Theorem 8.32 *Let $I \subset \mathbb{F}[x_1, x_2, \ldots, x_m]$ be an ideal with Gröbner basis $\mathcal{B}$ with respect to $\prec_w$ (see Definition 8.31). Suppose that the elements of the footprint $\Delta_{\prec_w}(I)$ have mutually distinct weights and that every element of $\mathcal{B}$ has exactly two monomials of highest weight (with respect to $\prec_{\mathbb{N}_0^r}$) in its support. Then $R = \mathbb{F}[x_1, x_2, \ldots, x_m]/I$ is an order domain with a weight function defined as follows. Given a nonzero $f \in \mathbb{F}[x_1, x_2, \ldots, x_m]/I$ write $f = F + I$ where $F \in Span_{\mathbb{F}}\{M \mid M \in \Delta_{\prec_w}(I)\}$. We have $\rho(f) =$* wdeg(F) *and $\rho(0) = -\infty$.*

On the other hand if (R, ρ, Γ) is a finitely generated order structure then after having embedded Γ into $\mathbb{N}_0^r$ one can up to isomorphism describe R as above. In this way the original order function on R becomes a weight function (described as above).

Not only have we by the above theorem a simple way of describing order domains but also by Proposition 8.34 below we have a simple way of actually constructing the corresponding codes. We will need the following definition.

Definition 8.33 *Given an ideal $I \subseteq \mathbb{F}_q[x_1, x_2, \ldots, x_m]$ write*

$$I_q = I + \langle x_1^q - x_1, x_2^q - x_2, \ldots, x_m^q - x_m \rangle.$$

The following result was treated in [21, Sec. 5.4] and [22, p. 147] (both in Japanese) for the case of $w(x_1), w(x_2), \ldots, w(x_m) \in \mathbb{N}_0$. Here we consider the general case (this result was included without a proof in the abstract [8]).

Proposition 8.34 *Let (R, ρ, Γ) be an order structure described as in Theorem 8.32. Consider the affine variety $\mathbb{V}_{\mathbb{F}_q}(I) = \mathbb{V}_{\mathbb{F}_q}(I_q) = \{p_1, p_2, \ldots, p_n\}$. The affine variety* *map $\varphi : R \rightarrow \mathbb{F}_q^n$ given by $\varphi(F+I) = (F(p_1), F(p_2), \ldots, F(p_n))$ is a morphism as in Definition 8.15. Let $\Delta(R, \rho, \varphi) = \{\alpha(1), \alpha(2), \ldots, \alpha(n)\}$ be given as in Definition 8.16. We have*

$$\Delta(R, \rho, \varphi) = \{w(M) \mid M \in \Delta_{\prec_w}(I_q)\}. \tag{8.13}$$

Proof: Clearly φ is well-defined and satisfies the conditions in Definition 8.15. This establish the first result.

By Proposition 8.30 the two sets in (8.13) are of the same size. Hence, we will be through if we can show that $\alpha(s) \in \{w(M) \mid M \in \Delta_{\prec_w}(I_q)\}$ for $s = 1, 2, \ldots, n$. Consider a fixed $\alpha(s) \in \Delta(R, \rho, \Gamma)$ and let $f \in R$ be such that $\rho(f) = \alpha(s)$. By the construction in Theorem 8.32 we can write $f = F + I$ where $F = \sum_{i=1}^{t} \eta_i M_i$ where $t \geqslant 1$, where $M_i \in \Delta_{\prec_w}(I), \eta_i \in \mathbb{F}_q \setminus \{0\}$ for $i = 1, 2, \ldots, t$, where $w(M_t) \prec_{\mathbb{N}_0^r} w(M_{t-1}) \prec_{\mathbb{N}_0^r} \cdots \prec_{\mathbb{N}_0^r} w(M_1)$ and where $\alpha(s) = \rho(f) = w(M_1)$. Let $\mathcal{B}'$ be a Gröbner basis for I_q with respect to $\prec_w$. We now reduce F modulo $\mathcal{B}'$ using the division algorithm ([2, Sec. 2, Par. 3]) and get a remainder $\sum_{i=1}^{l} \beta_i N_i$ where $N_i \in \Delta_{\prec_w}(I_q), \beta_i \in \mathbb{F}_q \setminus \{0\}$ for $i = 1, 2, \ldots, l$ and where $w(N_l) \prec_{\mathbb{N}_0^r} w(N_{l-1} \prec_{\mathbb{N}_0^r} \cdots \prec_{\mathbb{N}_0^r} w(N_1)$. We have $F - \sum_{i=1}^{l} \beta_i N_i \in I_q$ and therefore

$$\varphi(f) = \varphi(F+I) = \varphi\left(\sum_{i=1}^{l} \beta_i N_i + I\right). \tag{8.14}$$

Note that as $\varphi(f)$ by the very definition of $\alpha(s)$ is non-zero (8.14) implies that $\sum_{i=1}^{l} \beta_i N_i \neq 0$. This fact and the fact that $\Delta_{\prec_w}(I_q) \subseteq \Delta_{\prec_w}(I)$ implies

$$\rho\left(\sum_{i=1}^{l} \beta_i N_i + I\right) = w(N_1).$$

Next we observe that by the very nature of the division algorithm and by the definition of $\prec_w$ we have $\mathrm{wdeg}(F) \preceq_{\mathbb{N}_0^r} \mathrm{wdeg}(\sum_{i=1}^{l} \beta_i N_i)$. This is the same as saying

$$\alpha(s) \preceq_{\mathbb{N}_0^r} w(N_1). \tag{8.15}$$

Comparing (8.14) and (8.15) and using the definition of $\alpha(s)$ gives $\alpha(s) = w(N_1) \in \{w(M) \mid M \in \Delta_{\prec_w}(I_q)\}$. □

The following proposition gives some simple conditions under which the codes $\tilde{C}(\delta)$ and $\tilde{E}(\delta)$ defined by use of the affine variety map in Proposition 8.34 are of the same dimension.

Proposition 8.35 *Let R be an order domain over $\mathbb{F}_q$ described as in Theorem 8.32. Let $\mathbb{V}_{\mathbb{F}_q}(I_q) = \{p_1, p_2, \ldots, p_n\}$ and consider the evaluation map varphi $: R \rightarrow \mathbb{F}_q^n$ given by*

$\varphi(F+I) = (F(p_1), F(p_2), \ldots, F(p_n))$. Let $\Delta(R, \rho, \varphi) = \{\alpha(1), \alpha(2), \ldots, \alpha(n)\}$ be defined accordingly. If

$$\Delta_{\prec_w}(I_q) = \{x_1^{\beta_1} x_2^{\beta_2} \cdots x_m^{\beta_m} \mid \beta_1 \leqslant \gamma_1, \beta_2 \leqslant \gamma_2, \ldots, \beta_m \leqslant \gamma_m\} \tag{8.16}$$

for some $(\gamma_1, \gamma_2, \ldots, \gamma_m) \in \mathbb{N}_0^m$. Then for any $\delta \in \{1, 2, \ldots, n\}$ we have

$$\#\{i \in \{1, 2, \ldots, n\} \mid \sigma(\alpha(i)) = \delta\} = \#\{i \in \{1, 2, \ldots, n\} \mid \mu(\alpha(i)) = \delta\}. \tag{8.17}$$

Proof: Consider $\alpha(l) \in \Delta(R, \rho, \varphi) = \{w(M) \mid M \in \Delta_{\prec_w}(I_q)\}$. By assumption there exist $\omega_1, \omega_2, \ldots, \omega_m \in \mathbb{N}_0$ with $\omega_1 \leqslant \gamma_1, \omega_2 \leqslant \gamma_2, \ldots, \omega_m \leqslant \gamma_m$ such that $w(x_1^{\omega_1} x_2^{\omega_2} \cdots x_m^{\omega_m}) = \alpha(l)$. Also by assumption

$$w\left(x_1^{\gamma_1 - \omega_1} x_2^{\gamma_2 - \omega_2} \cdots x_m^{\gamma_m - \omega_m}\right) \in \Delta(R, \rho, \varphi).$$

Hence, if we write $\alpha_{max} = w(x_1^{\gamma_1} x_2^{\gamma_2} \cdots x_m^{\gamma_m})$ then we have $\alpha(l) \in \Delta(R, \rho, \varphi)$ if and only if $\alpha_{max} - \alpha(l) \in \Delta(R, \rho, \varphi)$. Moreover by the very definition of μ and σ (8.16) implies that for all $\alpha(l) \in \Delta(R, \rho, \varphi)$ we have $\mu(\alpha(l)) = \sigma(\alpha_{max} - \alpha(l))$. □

Clearly, if R and φ are given as in Proposition 8.35 and if (8.16) is satisfied then the dimensions of the related codes $\tilde{E}(\delta)$ and $\tilde{C}(\delta)$ will be the same. The next section includes examples where (8.16) is satisfied but also an example illustrating that if R and φ are given as in Proposition 8.35, but (8.16) is not satisfied then it may happen that the dimensions of the codes $\tilde{E}(\delta)$ and $\tilde{C}(\delta)$ are not the same for almost all choices of $\delta \in \{1, 2, \ldots, n\}$. In Appendix A two types of algebraic structures are described where not only (8.16) is satisfied but actually $\tilde{E}(\delta) = \tilde{C}(\delta)$ holds for all $\delta \in \{1, 2, \ldots, n\}$.

8.6. Examples

In this section we make extensive use of the notation from Definition 8.31, Theorem 8.32 and Proposition 8.34.

Example 8.36 Let $I = \langle x^5 + y^4 + y, y^5 + z^4 + z \rangle \subseteq \mathbb{F}_{16}[x, y, z]$. Define the weighted degree lexicographic ordering $\prec_w$ on $\mathcal{M}(x, y, z)$ as follows. Consider weights $w(x) = 16, w(y) = 20, w(z) = 25 \in \mathbb{N}_0$. Let $\prec_{\mathbb{N}_0}$ be the usual (and unique) monomial ordering on $\mathbb{N}_0$, and let $\prec_{\mathcal{M}}$ be the lexicographic ordering on $\mathcal{M}(x, y, z)$ given by $x \prec_{\mathcal{M}} y \prec_{\mathcal{M}} z$. Using Theorem 8.32 we get a weight function

$$\rho : R = \mathbb{F}_{16}[x, y, z]/I \rightarrow \langle 16, 20, 25 \rangle \cup \{-\infty\}.$$

By Proposition 8.30 the variety $\mathbb{V}_{\mathbb{F}_{16}}(I_{16})$ is of size equal to $\#\Delta_{\prec_w}(I_{16}) = 256$. Let φ be the affine variety map $\varphi : R \rightarrow \mathbb{F}_{16}^{256}$ given by

$$\varphi(f) = (f(p_1), f(p_2), \ldots, f(p_{256}))$$

where $\{p_1, p_2, \ldots, p_{256}\} = \mathbb{V}_{\mathbb{F}_{16}}(I_{16})$. As

$$\Delta_{\prec_w}(I_{16}) = \{x^a y^b z^c \mid 0 \leqslant a < 16,\ 0 \leqslant b < 4,\ 0 \leqslant c < 4\},$$

the condition in (8.16) of Proposition 8.35 is satisfied and therefore the dimension of $\tilde{C}(\delta)$ equals the dimension of $\tilde{E}(\delta)$, for all $\delta = 1, 2, \ldots, 256$.

In Figure 8.1 we plot the (estimated) parameters of the codes $\tilde{E}(\delta)$. For the $E(\lambda)$ codes we plot the usual Goppa bound (old bound) as well as the improved bound from the present paper (new bound). $\triangle$

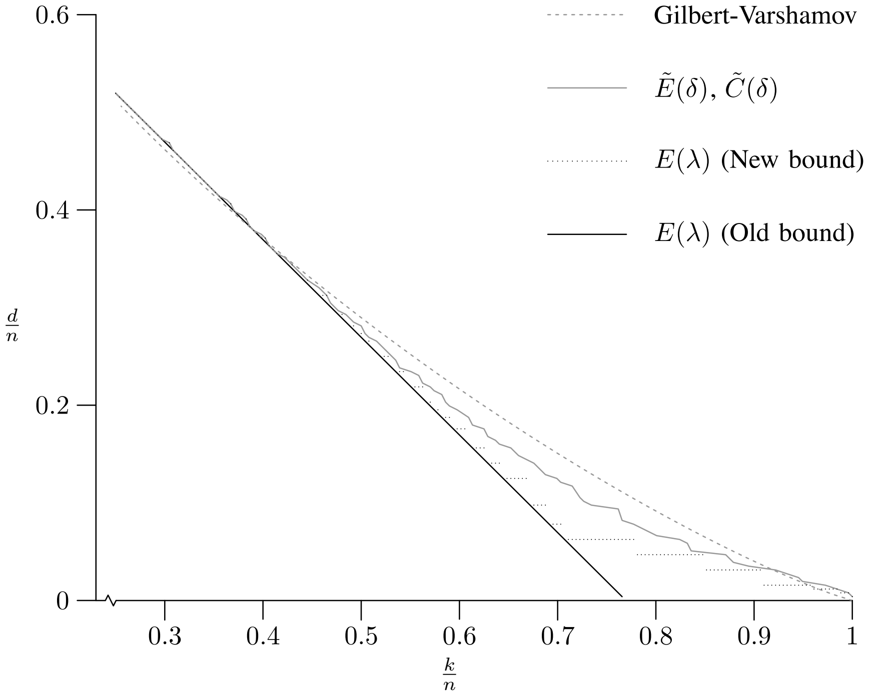

Figure 8.1.: Bounds for the $\tilde{E}(\delta)$ and $E(\lambda)$ codes from $I = \langle x^5 + y^4 + y, y^5 + z^4 + z\rangle \subseteq \mathbb{F}_{16}[x, y, z]$.

Example 8.37 In [12] and [10] the parameters of the codes $\tilde{C}(\delta)$ coming from repeated tensor products of the Hermitian order domain were considered. The footprint $\Delta_{\prec_w}(I_q)$ involved in the construction of the codes $\tilde{C}(\delta)$ and $\tilde{E}(\delta)$ from the (single) Hermitian order domain satisfies the condition in (8.16) of Proposition 8.35. It follows immediately that the footprints involved in the construction of the codes $\tilde{C}(\delta)$ and $\tilde{E}(\delta)$ from repeated tensor products of Hermitian order domains also satisfy the condition in (8.16) of proposition 8.35. Hence, the estimates in [12] of the parameters of the codes $\tilde{C}(\delta)$ from repeated tensor products also holds for the corresponding codes $\tilde{E}(\delta)$. △

Example 8.38 Consider the order domain $R = \mathbb{F}_{16}[x, y, z, u]/I$ where $I = \langle x^5 + y^4 + y, y^5 + z^4 + z, z^5 + u^4 + u^2 \rangle$ (note the term u^2). The construction of codes from this order domain does not satisfy the condition in (8.16) of Proposition 8.35. In Figure 8.2 we plot the estimated performance of the codes $\tilde{E}(\delta)$ and $\tilde{C}(\delta)$.

It is clear that for values of $\frac{k}{n}$ smaller than approximately 0.2 the codes $\tilde{E}(\delta)$ are the best whereas for larger values the codes $\tilde{C}(\delta)$ are the best. Finally in Figure 8.2 we plot the usual Goppa bound (old bound) for the $E(\lambda)$ codes versus the improved bound from the present paper (new bound). △

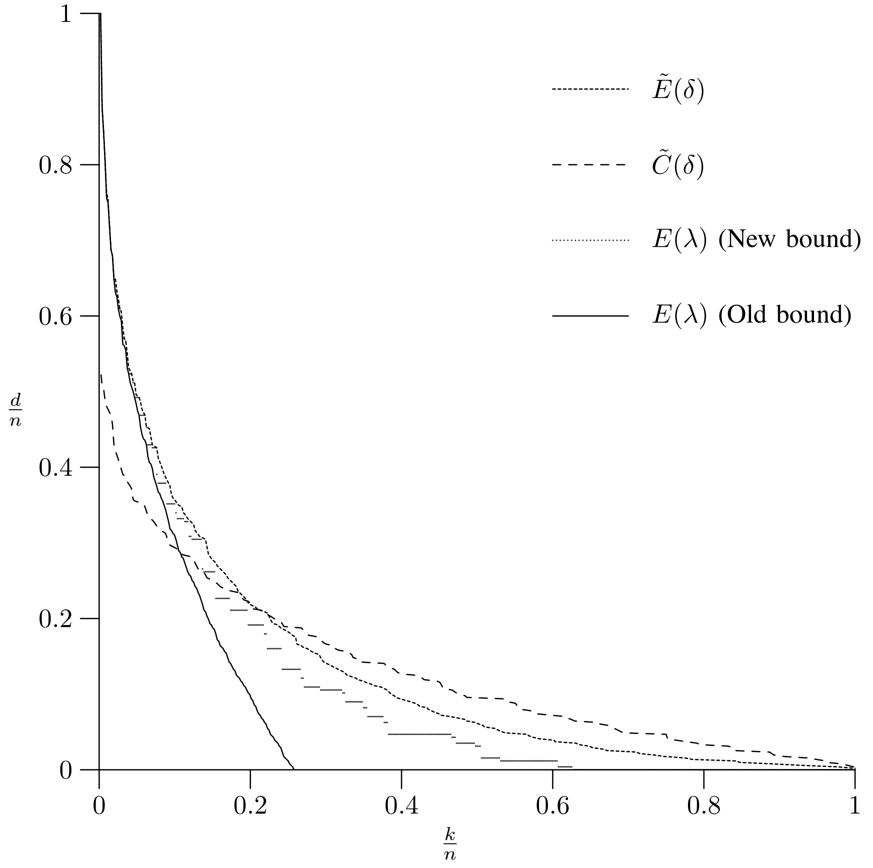

Figure 8.2.: Bounds for the $\tilde{E}(\delta), \tilde{C}(\delta)$ and $E(\lambda)$ codes from $I = \langle x^5 + y^4 + y, y^5 + z^4 + z, z^5 + u^4 + u^2 \rangle \subseteq \mathbb{F}_{16}[x, y, z, u]$.

Example 8.39 In the technical report [7, Ex. 12] it was shown that $\mathbb{F}_{q^2}[x,y,z,u]/I$ where

$$I = \langle x^q + yz^q - y^q z - x, u^q - z^{q+1} + \alpha x^q - \alpha y^q z + \beta y^{q+1} + u\rangle$$

and where $\alpha, \beta \in \mathbb{F}_q$, is an order domain with a weight function given as follows. Define weights

$$\begin{aligned} w(x) &= (q,1) \qquad & w(y) &= (0,q) \\ w(z) &= (q,0) \qquad & w(u) &= (q+1,0) \end{aligned}$$

Define $\prec_{\mathbb{N}_0^2}$ such that $(q,q^2) \prec_{\mathbb{N}_0^2} (q^2,q)$ and such that

$$(q^2,q),(q,q^2),(0,q^2+q) \prec_{\mathbb{N}_0^2} (q^2+q,0).$$

Finally define $\prec_{\mathcal{M}}$ such that $yz^q \prec_{\mathcal{M}} x^q, z^{q+1} \prec_{\mathcal{M}} u^q$ and apply Theorem 8.32. It was shown in [7, Ex. 12] that

$$\Delta_{\prec_w}\left(I_{q^2}\right) = \{x^a y^b z^c u^d \mid a,d < q \text{ and } b,c < q^2\}.$$

This footprint satisfies the condition in (8.16) of Proposition 8.35. Hence, the dimension of the code $\tilde{E}(\delta)$ equals the dimension of the code $\tilde{C}(\delta)$ for all choices of δ and the codes are of length $n = (q^2)^3 = q^6$.

In Figure 8.3 we plot the estimated performance of the codes $\tilde{E}(\delta)$ and $\tilde{C}(\delta)$ from the present example in the case $\mathbb{F}_{q^2} = \mathbb{F}_{64}$. These are of length $n = 262144$. The hyperbolic codes $\mathrm{Hyp}_{64}(s,3)$ and the generalized Reed-Muller codes $\mathrm{RM}_{64}(s,3)$ are of the same length, but according to Figure 8.3 they do not perform nearly as good as the codes from the present example. △

8.7. Conclusion

In this paper we have presented the missing evaluation codes from order domain theory and we have studied various features of these new codes. It remains to derive decoding algorithms for the new codes. It would be obvious to try to investigate if it is possible to modify the Guruswami-Sudan algorithm for one-point geometric Goppa codes to deal with the new improved one-point geometric Goppa codes. In the light of the relatively simple bound on the generalized Hamming weights for the codes $C(B,G)$ of this paper it would be obvious to try to derive a simpler bound on the generalized Hamming weights for the codes $C^{\perp}(B,G)$ than the ones that can be found in the literature.

8.8. Appendix - A pure Gröbner basis theoretical approach.

In [11] and [9] some concrete improved code constructions were given in the language of Gröbner basis theory. These code constructions heavily rely on the footprint bound

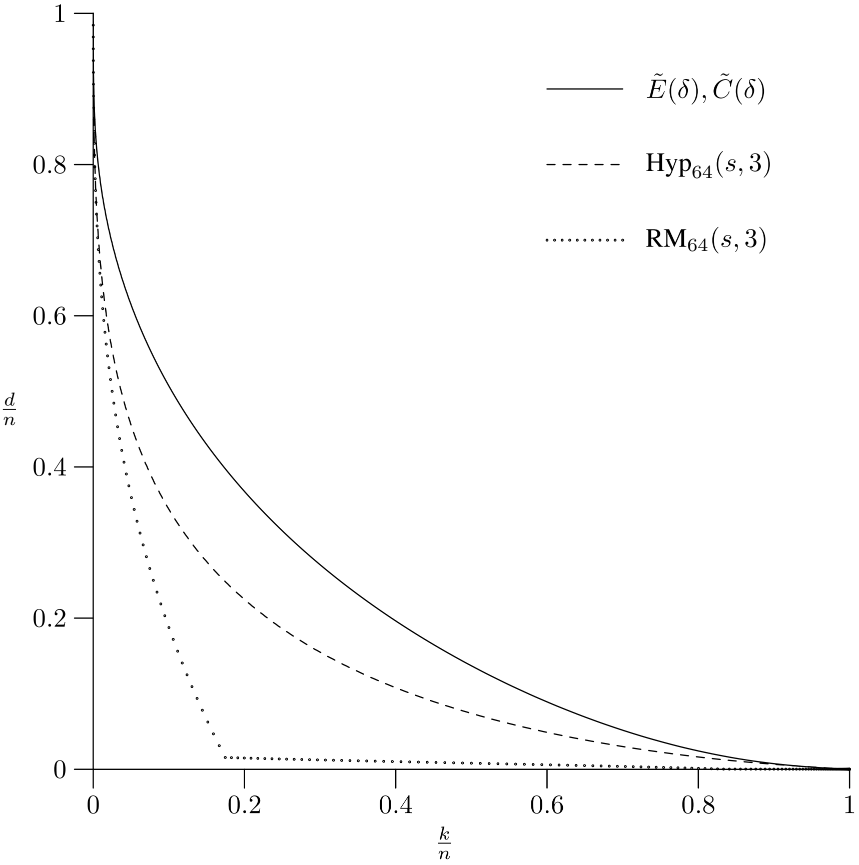

Figure 8.3.: Performance of the $\tilde{E}(\delta)$ and $\tilde{C}(\delta)$ codes in the case $\mathbb{F}_{q^2} = \mathbb{F}_{64}$ compared to the performance of the and hyperbolic codes $\mathrm{Hyp}_{64}(s, 3)$ and the generalized Reed-Muller codes $\mathrm{RM}_{64}(s, 3)$ of the same length.

(Proposition 8.30). To establish the connection between the results in [11] and [9] and the results in the present paper consider the following generalization of the function D from [11, p. 160] and [9, Def. 3].

Definition 8.40 *Assume a description of a finitely generated order domain is given as in Theorem 8.32. Write*

$$B = \{F_1(x_1, x_2, \ldots, x_m), F_2(x_1, x_2, \ldots, x_m), \ldots, F_s(x_1, x_2, \ldots, x_m)\}$$

and let for $i = 1, 2, \ldots, s$, B_i be a difference between the two monomials of highest weight in F_i. For all $M \in \Delta_{\prec_w}(I_q = I + \langle x_1^q - x_1, x_2^q - x_2, \ldots, x_m^q - x_m \rangle)$ define

$$D(M) = \#(\Delta_{\prec_w}(\langle B_1, B_2, \ldots, B_s, M \rangle) \cup \Delta_{\prec_w}(I_q)). \tag{8.18}$$

By use of Gröbner basis theoretical arguments we can show how to generalize the results from [11] and [9] to a construction of improved codes from any order domain. The function D from Definition 8.40 plays a fundamental role in this construction. However, our construction turns out to be just the code construction $\tilde{E}(\delta)$ from the present paper by Proposition 8.41 below. More general the following result together with Theorem 8.23 may serve as a guideline for the future work on constructing improved codes by the use of Gröbner basis theoretical methods.

Proposition 8.41 *Let $M \in \Delta_{\prec_w}(I_q)$ and $\rho(M+I)=\lambda$ (that is, $w(M)=\lambda$). We have $\sigma(\lambda)=n-D(M)$.*

Proof: We first note that $\{B_1, B_2, \ldots, B_s\}$ is a Gröbner basis for $\langle B_1, B_2, \ldots, B_s\rangle$ with respect to $\prec_w$ and that

$$\Delta_{\prec_w}(\langle B_1, B_2, \ldots, B_s\rangle) = \Delta_{\prec_w}(\langle F_1, F_2, \ldots, F_s\rangle)$$

holds. The first fact can be shown by considering what takes place in Buchberger's algorithm (see [2]) and the last fact is obvious. By the conditions in Theorem 8.32 the restriction of the map

$$w : \mathcal{M}(x_1, x_2, \ldots, x_m) \rightarrow \Gamma$$

to $\Delta_{\prec_w}(\langle B_1, B_2, \ldots, B_s\rangle)$ is a bijective map. The proposition will follow from (8.11) and Proposition 8.34 if we can show that

$$w(\Delta_{\prec_w}(\langle B_1, B_2, \ldots, B_s, M\rangle)) = \Gamma \setminus (\lambda + \Gamma). \tag{8.19}$$

We first show that the left hand side of (8.19) is contained in the right hand side. We have

$$\{w(MM') \mid M' \in \Delta_{\prec_w}(\langle B_1, B_2, \ldots, B_s\rangle)\} = \lambda + \Gamma$$

$$\Downarrow$$

$$\{w(MM' \text{ rem } \{B_1, B_2, \ldots, B_s\}) \mid M' \in \Delta_{\prec_w}(\langle B_1, B_2, \ldots, B_s\rangle)\} = \lambda + \Gamma \tag{8.20}$$

Here, MM' rem $\{B_1, B_2, \ldots, B_s\}$ means the remainder of MM' after division with $\{B_1, B_2, \ldots, B_s\}$ and the implication follows from the fact $w(MM') = w(MM' \text{ rem } \{B_1, B_2, \ldots, B_s\})$. Note that

$$MM' \text{ rem } \{B_1, B_2, \ldots, B_s\} \in \Delta_{\prec_w}(\langle B_1, B_2, \ldots, B_s\rangle)$$

and that

$$MM' \text{ rem } \{B_1, B_2, \ldots, B_s\} \in \langle B_1, B_2, \ldots, B_s, M\rangle.$$

In particular

$$MM' \text{ rem } \{B_1, B_2, \ldots, B_s\} \notin \Delta_{\prec_w}(\langle B_1, B_2, \ldots, B_s, M\rangle)$$

and we conclude

$$MM' \text{ rem } \{B_1, B_2, \ldots, B_s\} \in \Delta_{\prec_w}(\langle B_1, B_2, \ldots, B_s\rangle) \setminus \Delta_{\prec_w}(\langle B1, B2, \ldots, B_s, M\rangle). \tag{8.21}$$

Comparing (8.20) and (8.21) we have

$$\lambda + \Gamma \subseteq w(\Delta_{\prec_w}(\langle B_1, B_2, \ldots, B_s\rangle) \setminus \Delta_{\prec_w}(\langle B_1, B_2, \ldots, B_s, M\rangle))$$

and the fact that the restriction of w to $\Delta_{\prec_w}(\langle B_1, B_2, \ldots, B_s\rangle)$ is injective implies

$$w(\Delta_{\prec_w}(\langle B_1, B_2, \ldots, B_s, M\rangle) \subseteq \Gamma \setminus (\lambda + \Gamma).$$

Next we prove that the right hand side of (19) is contained in the left hand side. We start by considering what can happen when we use Buchberger's algorithm to extend $\{B_1, B_2, \ldots, B_s, M\}$ to a Gröbner basis with respect to $\prec_w$. Consider the S-polynomials (see [2]) $S(B_i, M)$. These polynomials (actually monomials) either reduces to 0 modulo $\{B_1, B_2, \ldots, B_s, M\}$ or reduces to a monomial of weight $\lambda + w'$, where $w' \in w(\mathcal{M}(x_1, x_2, \ldots, x_m)) = \Gamma$. The S-polynomial of two monomials in turn is 0. Hence, by induction every new polynomial adjoined to the basis in a given step of Buchberger's algorithm is a monomial with weight in $\lambda + \Gamma$. It follows that every monomial N, where $N \in \Delta_{\prec_w}(\langle B_1, B_2, \ldots, B_s\rangle) \setminus \Delta_{\prec_w}(\langle B_1, B_2, \ldots, B_s, M\rangle)$ has weight in $\lambda + \Gamma$. We conclude $w(\Delta_{\prec_w}(\langle B_1, B_2, \ldots, B_s, M\rangle)) \supseteq \Gamma \setminus (\lambda + \Gamma)$. □

As already mentioned the function $D(M)$ plays a fundamental role in [11] where the generalized Reed-Muller codes and the hyperbolic codes (improved generalized Reed-Muller codes) are studied. The function also plays a fundamental role in [9] where one-point geometric Goppa codes and improved one-point geometric Goppa codes from norm-trace curves $x^{(q^r-1)/(q-1)} - y^{q^{r-1}} - y^{q^{r-2}} - \cdots - y$ over $\mathbb{F}_{q^r}$ are studied (including improved Hermitian codes). Using Proposition 8.30 the authors of the above mentioned two papers derive improved code constructions for the considered algebraic structures that by the use of Proposition 8.41 can be shown to be identical to the improved code constructions from the present paper. Also bounds similar to (8.9) and (8.10) are described for the considered algebraic structures. Moreover these bounds are shown to be tight. Hence, our bounds (8.9) and (8.10) are known to be tight for some relatively large classes of codes. The code constructions in the two papers satisfy the conditions in Proposition 8.35. Moreover, it was shown it both papers that actually $\tilde{E}(\delta) = \tilde{C}(\delta)$ holds for all choices of $\delta \in \{1, 2, \ldots, n\}$ for the considered algebraic structures.

8.9. References

[1] H. E. Andersen and O. Geil. *On the Missing Evaluation Codes from Order Domain Theory*, 6 pages, November, 2003, Unpublished. An abstract of this extended summary was published in: Mathematisches Forshungsinstitut Oberwolfach, Report No. 53, Kodierungstheorie, December 7th - December 13th, 2003, page 3.

[2] D. Cox, J. Little, and D. O'Shea. *Ideals, Varieties and Algorithms - An Introduction to Computational Algebraic Geometry and Commutative Algebra.* Springer Verlag, New York, second edition, 1997.

[3] D. Cox, J. Little, and D. O'Shea. *Using Algebraic Geometry.* Springer Verlag, New York, 1998.

[4] G.-L. Feng and T. R. N. Rao. Improved geometric Goppa codes. I. Basic theory. *IEEE Trans. Inform. Theory*, 41(6, part 1):1678–1693, 1995. Special issue on algebraic geometry codes.

[5] J. Fitzgerald and R. F. Lax. Decoding affine variety codes using Gröbner bases. *Designs, Codes and Cryptography*, 13(2):147–158, 1998.

[6] A. García and H. Stichtenoth. A tower of Artin-Schreier extensions of function fields attaining the Drinfel′d-Vlăduţ bound. *Invent. Math.*, 121(1):211–222, 1995.

[7] O. Geil. On The Construction of Codes from Order Domains. Technical report, Department of Mathematical Sciences, Aalborg University; Denmark, 2000. Available at: `http://www.math.aau.dk/research/reports/R-00-2013.ps`.

[8] O. Geil. Codes from Order Domains. *Proc. of 2001 IEEE International Symposium on Information Theory, Washington, USA, June 24 - 29*, page 308, 2001.

[9] O. Geil. On Codes from Norm-Trace Curves. *Finite Fields and Their Applications*, 9(3):351–371, July 2003.

[10] O. Geil and T. Høholdt. On Hyperbolic Type Codes. Technical report. To appear.

[11] O. Geil and T. Høholdt. On hyperbolic codes. In *Applied algebra, algebraic algorithms and error-correcting codes (Melbourne, 2001)*, volume 2227 of *Lecture Notes in Comput. Sci.*, pages 159–171. Springer, Berlin, 2001.

[12] O. Geil and T. Høholdt. On Hyperbolic Type Codes. *Proc. of 2003 IEEE International Symposium on Information Theory, Yokohama, Japan, June 29 - July 4*, page 331, 2003.

[13] O. Geil and R. Pellikaan. On the Structure of Order Domains. *Finite Fields and Their Applications*, 8:369–396, 2002.

[14] T. Høholdt. On (or in) the Blahut footprint. In *Codes, curves, and signals (Urbana, IL, 1997)*, volume 485 of *Kluwer Internat. Ser. Engrg. Comput. Sci.*, pages 3–7. Kluwer Acad. Publ., Boston, MA, 1998.

[15] T. Høholdt, J. van Lint, and R. Pellikaan. Chapter 10: "Algebraic geometry codes" in *Handbook of coding theory, V. S. Pless and W. C. Huffman (Eds.), vol. 1.* Elsevier, Amsterdam, 1998.

[16] T. Høholdt, J. H. van Lint, and R. Pellikaan. Order functions and evaluation codes. In *Applied algebra, algebraic algorithms and error-correcting codes (Toulouse, 1997)*, volume 1255 of *Lecture Notes in Comput. Sci.*, pages 138–150. Springer, Berlin, 1997.

[17] G. A. Kabatianskiĭ. Two generalizations of the product of codes. *Dokl. Akad. Nauk SSSR*, 232(6):1277–1280, 1977. (In Russian).

[18] J. L. Massey, D. J. Costello, and J. Justesen. Polynomial weights and code constructions. *IEEE Trans. Information Theory*, IT-19:101–110, 1973.

[19] R. Matsumoto. Miura's Generalization of One-Point AG Codes is Equivalent to Høholdt, van Lint and Pellikaan's Generalization. *IEICE Trans. Fundamentals*, E82-A(10):2007–2010, October 1999.

[20] R. Matsumoto and S. Miura. On the Feng-Rao Bound for $\mathcal{L}$-Construction of Algebraic Geometry Codes. *IEICE Trans. Fundamentals*, E83-A(5):923–927, 2000.

[21] S. Miura. PhD thesis, University of Tokyo, May 1997. (In Japanese).

[22] S. Miura. Linear Codes on Affine Algebraic Curves. *IEICE Trans.*, J81-A(10):1398–1421, 1998. (In Japanese).

[23] S. Miura. Linear Codes on Affine Algebraic Varieties. *IEICE Trans.*, J81-A(10):1386–1397, 1998. (In Japanese).

[24] R. Pellikaan. On the existence of order functions. *Journal of Statistical Planning and Inference*, 94:287–301, 2001.

[25] T. Shibuya, R. Hasagawa, and K. Sakaniwa. A Lower Bound for Generalized Hamming Weights and a Condition for t-th MDS. *IEICE Trans. Fundamentals*, E82-A:1090–1101, 1999.

[26] T. Shibuya, J. Mizutani, and K. Sakaniwa. On generalized Hamming weights of codes constructed on affine algebraic sets. In *Applied algebra, algebraic algorithms and error-correcting codes (Toulouse, 1997)*, volume 1255 of *Lecture Notes in Comput. Sci.*, pages 311–320. Springer, Berlin, 1997.

[27] T. Shibuya, J. Mizutani, and K. Sakaniwa. On generalized Hamming weights of codes constructed on affine algebraic sets. *IEICE Trans. Fundamentals*, E81-A:1979–1989, 1998.

[28] T. Shibuya and K. Sakaniwa. A lower bound on generalized Hamming weights in terms of a notion of well-behaving. *Proc. of 1998 IEEE International Symposium on Information Theory, Cambridge, USA*, page 96, 1998.

[29] T. Shibuya and K. Sakaniwa. A Dual of Well-Behaving Type Designed Minimum Distance. *IEICE Trans. Fundamentals*, E84-A(2):647–52, February 2001.

[30] T. Shibuya and K. Sakaniwa. A note on a lower bound for generalized Hamming weights. *IEICE Trans. Fundamentals*, E84-A(12):3138–3145, December 2001.

[31] V. K. Wei. Generalized Hamming weights for linear codes. *IEEE Trans. Inform. Theory*, 37(5):1412–1418, 1991.

9. Paper II - “On Puncturing of Codes from Norm-Trace Curves”

H. E. Andersen

On Puncturing of Codes from Norm-Trace Curves

Research report R-2005-10
Department of Mathematical Sciences
Aalborg University
Denmark

Preliminary results from this paper were presented at the 8th Nordic Combinatorial Conference 2004 and a short abstract was printed in the proceedings. The version given here is a revised version of the research report R-2005-10. It has been accepted for publishing in *Finite Fields and Their Applecations.*

On Puncturing of Codes from Norm-Trace Curves

Henning E. Andersen
Department of Mathematical Sciences
Aalborg University
Fredrik Bajers Vej 7 G
9220 Aalborg East, Denmark
henning@math.aau.dk

Abstract

Constructing new codes from existing ones by puncturing is in this paper viewed in the context of order domains R where puncturing can be seen as redefinition of the evaluation map $\varphi : R \to \mathbb{F}_q^n$. The order domains considered here are of the form $R = \mathbb{F}[x_1, x_2, \ldots, x_m]/I$ where redefining φ can be done by adding one or more polynomials to the basis of the defining ideal I to form a new ideal J in such a way that the number of points in the variety $\mathbb{V}(I)$ is reduced by t to form $\mathbb{V}(J)$ and puncturing in t coordinates is achieved. An explicit construction of such polynomials is given in the case of codes defined by Norm-Trace curves and examples are given of both evaluation codes and dual codes. Finally, it is demonstrated that the improvement in minimum distance can be significant when compared to the lower bound obtained by ordinary puncturing.

Key words: Gröbner basis, Footprint, Evaluation codes, Dual codes, Puncturing, Minimum distance, Norm, Trace, Order domain.

9.1. Introduction

Constructing codes from existing ones is not a new idea and over the years several ways of doing so has been developed. One such construction is by means of puncturing. Puncturing an (n, M, d) code $t, (t < d)$, times yields an $(n - t, M, \geqslant d - t)$ code where the parameter $d - t$ is a lower bound on the minimum distance [12, p. 28].

However, it is not clear how to select which t coordinates to erase in an existing code to get the best result or whether an optimal strategy for making such a selection exists for a given code and a given value t. The general bound given above is usually not tight which will be shown by an example.

Here we consider codes from Norm-Trace curves[1] which were studied in detail in [7]. Here we use nothing but order domains and Gröbner basis theory for code construction and the methods developed in [9, 1, 10, 4, 5] for estimating the minimum distances of the codes.

The notion of an order domain was introduced in [9, 10] to make understanding of a large class of algebraic geometry codes easier and to give the code construction presented in [4, 5][2] a simpler foundation. Many of the results in [9, 10, 21] were found independently by Miura and published in Japanese in [16, 18, 17][3] (See [14] for details).

By [8] every finitely generated order domain can be represented as a factor ring $\mathbb{F}_q[x_1, x_2, \ldots, x_m]/I$, where $I \subset \mathbb{F}_q[x_1, x_2, \ldots, x_m]$ is an ideal of a special form. Using such an order domain and the usual evaluation map $\varphi : \mathbb{F}_q[x_1, x_2, \ldots, x_m]/I \to \mathbb{F}_q^n$ we define $\tilde{E}$ codes as a linear subspace of $\mathbb{F}_q^n$ spanned by the image of selected elements from $\mathbb{F}_q[x_1, x_2, \ldots, x_m]/I$ under φ and $\tilde{C}$ codes as the dual of such an image under φ (These are the improved $\tilde{E}$ codes from [1] and the improved $\tilde{C}$ codes from [9, 5]).

In this setting puncturing a code can be done by reducing the dimension of the corresponding factor ring $\mathbb{F}_q[x_1, x_2, \ldots, x_m]/I$ as a vector space over $\mathbb{F}_q$ by adding extra polynomials to the basis of the defining ideal I to define an new ideal J. This corresponds to redefining the evaluation map by leaving out a number of points from the variety $\mathbb{V}(I)$, since $I \subset J$ has the consequence that $\mathbb{V}(J) \subset \mathbb{V}(I)$ [2].

Leaving out t points from the variety $\mathbb{V}(I)$ can be done in several ways by adding different sets of polynomials to the basis of the ideal I to form the ideal J such that $\#\mathbb{V}(J) = \#\mathbb{V}(I) - t$. The evaluation map φ is still a morphism so the methods developed in [9, 1, 5] enables us to estimate the minimum distances of the codes constructed by using the variety $\mathbb{V}(J)$. This in turn allows us to choose the set of polynomials added to the basis of I (i.e. choose the ideal J) which has the smallest cost in terms of loss in minimum distance for a given integer t and a given code rate.

The main result in this paper is that for any positive integer $t < d$ it is possible to construct a set of polynomials $\{g_1, g_2, \ldots, g_s\}$ such that a code of length $n - t$ is obtained by using the ideal $J = I + \langle g_1, g_2, \ldots, g_s \rangle$ and the affine variety $\mathbb{V}(J)$. Furthermore, the proof given here is constructive and examples of such constructions are included.

The paper is organized as follows: In Section 9.2 a short presentation of order domains is given, Section 9.3 is an introduction to the necessary Gröbner basis theory used to construct order domains, Section 9.4 presents the construction of codes from Norm-Trace curves and Section 9.5 gives the new construction which can be seen as punctured codes from Norm-Trace curves. Section 9.6 contains some examples and Section 9.7 is the conclusion.

[1] Norm-Trace curves are a special case of the C_{ab} curves classified by Miura and Kamiya in [19]

[2] Readers interested in the connection between the theory of order domains and the theory of algebraic curves, or equivalently the theory of function fields, are recommended to read [9, 21]

[3] A proof in English of some of the results from [16, 18, 17] can be seen in [13].

9.2. Order domains and codes

The presentation of order domains given here is based on [1, 8]. For a more complete introduction to order domains the reader is referred to the literature.

Recall that an $\mathbb{F}$-algebra is a commutative ring with unity that contains $\mathbb{F}$ as a unitary subring (See [9, p. 901]).

Let $\mathbb{N}_0$ denote the non-negative integers and let $\Gamma \subset \mathbb{N}_0$. Since the relation $<$ on $\mathbb{N}_0$ is a total ordering then every non-empty subset of Γ has a smallest element with respect to $<$ and $(\Gamma, <)$ is called a well-order[4].

Now, add an element $-\infty$ to Γ such that $\Gamma_{-\infty} = \Gamma \cup \{-\infty\}$ and let $-\infty < n$ for all $n \in \mathbb{N}_0$, then $(\Gamma_{-\infty}, <)$ is a well-order. In the remaining part of this article we will only consider the well-order $(\Gamma_{-\infty}, <)$ defined here.

Definition 9.1 *Let $(\Gamma_{-\infty}, <)$ be a well-order, let $\mathbb{F}$ be a field and let R be an $\mathbb{F}$-algebra. A surjective map $\rho : R \to \Gamma_{-\infty}$ that satisfies the following five conditions for all $f, g, h \in R$ is called an order function on R.*

1. *$\rho(f) = -\infty$ if and only if $f = 0$.*
2. *$\rho(af) = \rho(f)$ for all non-zero $a \in \mathbb{F}$.*
3. *$\rho(f + g) \leqslant max\{\rho(f), \rho(g)\}$ and equality holds when $\rho(f) \neq \rho(g)$.*
4. *If $\rho(f) < \rho(g)$ and $h \neq 0$, then $\rho(fh) < \rho(gh)$.*
5. *If f and g are non-zero and $\rho(f) = \rho(g)$, then there exists a non-zero $a \in \mathbb{F}$ such that $\rho(f - ag) < \rho(g)$.*

Since $+$ is well-defined on $\Gamma \subset \mathbb{N}_0$ we can also give the following definition.

Definition 9.2 *Let $(\Gamma_{-\infty}, <)$ be a well-order, let $\mathbb{F}$ be a field and let R be an $\mathbb{F}$-algebra. A weight function on R is an order function ρ on R that also satisfy the condition*

6. *$\rho(fg) = \rho(f) + \rho(g)$*

where $+$ is the ordinary $+$ on $\mathbb{N}_0$ extended with the rule $-\infty + \gamma = -\infty$ for $\gamma \in \Gamma_{-\infty}$.

An order structure and an order domain can now be defined.

Definition 9.3 *Let $\mathbb{F}$ be a field, let R be an $\mathbb{F}$-algebra, ρ an order function and Γ a well-order. Then (R, ρ, Γ) is called an order structure and R is called an order domain (over $\mathbb{F}$).*

From [8, Def. 3.1 & Pro. 3.2] we have

[4] A more general discussion of well-orders can be seen in [8].

Theorem 9.4 *Given an order structure (R, ρ, Γ) then any set $\mathcal{B} = \{f_\gamma \mid \rho(f_\gamma) = \gamma\}_{\gamma\in\Gamma}$ constitutes a basis for R as a vector space over $\mathbb{F}$. For any $f = c_{\gamma_1} f_{\gamma_1} + \cdots + c_{\gamma_d} f_{\gamma_d}$ with $c_{\gamma_1}, \ldots, c_{\gamma_d} \in \mathbb{F}_q \setminus \{0\}$, $\rho(f) = \max_\prec\{\gamma_1, \ldots, \gamma_d\}$ holds. In particular $\{f_\lambda \in \mathcal{B} \mid \lambda \preceq \gamma\}$ constitutes a basis for $R_\gamma = \{f \in R \mid \rho(f) \preceq \gamma\}$ as a vector space over $\mathbb{F}$.*

Definition 9.5 *Let R be an $\mathbb{F}_q$-algebra. A map $\varphi : R \to \mathbb{F}_q^n$ is called a morphism of $\mathbb{F}_q$-algebras if φ is $\mathbb{F}_q$-linear and $\varphi(fg) = \varphi(f) * \varphi(g)$ for all $f, g \in R$, where $*$ denotes component-wise multiplication.*

Only surjective morphisms φ will be considered in the remaining part of this article.

Definition 9.6 *Given an order domain (R, ρ, Γ) and a surjective morphism φ, let 0 be the smallest element of Γ and define $\alpha(1) = 0$. For $i = 2, 3, \ldots, n$ define recursively $\alpha(i)$ to be the smallest element in Γ greater than $\alpha(1), \alpha(2), \ldots, \alpha(i-1)$ and satisfying $\varphi(R_\gamma) \subsetneq \varphi(R_{\alpha(i)})$, for all $\gamma \prec \alpha(i)$. Write $\Delta(R, \rho, \varphi) = \{\alpha(1), \alpha(2), \ldots, \alpha(n)\}$.*

From Definition 9.6 we see that the set $B = \{\varphi(f_{\alpha(1)}), \varphi(f_{\alpha(2)}), \ldots, \varphi(f_{\alpha(n)})\}$ constitutes a basis for $\mathbb{F}_q^n$ as a vector space over $\mathbb{F}_q$.

The set $\Delta(R, \rho, \varphi)$ has the following property from [1, Pro. 3].

Proposition 9.7 *Consider $\alpha(l) \in \Delta(R, \rho, \varphi)$ and assume $\beta_1, \beta_2 \in \Gamma$ satisfies $\rho(f_{\beta_1} f_{\beta_2}) = \alpha(l)$. Then $\beta_1, \beta_2 \in \Delta(R, \rho, \varphi)$ holds.*

As we shall see later one interesting consequence of Proposition 9.7 is that removing β_1 or β_2 from the set $\Delta(R, \rho, \varphi)$ (removing in a way that will be explained later) forces us to remove $\alpha(l)$ from the set as well if we want to make sure that φ continues to be a morphism. Later on we will also show the significance of this statement when dealing with certain ideals.

First, we need the following definition.

Definition 9.8 *For $\alpha(i) \in \Delta(R, \rho, \varphi)$ define*

$$N(\alpha(i)) = \{(\beta_1, \beta_2) \in (\Delta(R, \rho, \varphi))^2 \mid \rho(f_{\beta_1} f_{\beta_2}) = \alpha(i)\}$$

and define $\mu(\alpha(i)) = \#N(\alpha(i))$.

Furthermore, for $\alpha(j) \in \Delta(R, \rho, \varphi)$ define

$$M(\alpha(j)) = \{\gamma \in \Delta(R, \rho, \varphi) \mid \exists\beta \in \Delta(R, \rho, \varphi) \text{ with } \rho(f_{\alpha(j)} f_\beta) = \gamma\}$$

and define $\sigma(\alpha(j)) = \#M(\alpha(j))$.

Note that if ρ in Definition 9.8 is a weight function then the two sets $N(\alpha(i))$ and $M(\alpha(j))$ can be defined as

$$N(\alpha(i)) = \{(\beta_1, \beta_2) \in (\Delta(R, \rho, \varphi))^2 \mid \beta_1 + \beta_2 = \alpha(i)\}$$

and

$$M(\alpha(j)) = \{\gamma \in \Delta(R,\rho,\varphi) \mid \exists \beta \in \Delta(R,\rho,\varphi) \text{ with } \alpha(j)+\beta=\gamma\}.$$

In this case calculating $\mu(\alpha(i))$ and $\sigma(\alpha(j))$ involves nothing but the ordinary $+$ from $\mathbb{N}_0$.

Both the evaluation codes and dual codes from an order domain can now be defined. The codes considered here are the improved codes $\tilde{E}$ and $\tilde{C}$ from [7, 9, 1, 5].

Definition 9.9 *Consider a basis $\{f_\gamma \mid \rho(f_\gamma)=\lambda\}_{\lambda\in\Gamma}$ for an order structure (R,ρ,Γ) over $\mathbb{F}_q$. Let φ be a morphism as in Definition 9.5 and let $\Delta(R,\rho,\varphi)$ be as in Definition 9.6 so $B=\{\varphi(f_{\alpha(1)}),\varphi(f_{\alpha(2)}),\dots,\varphi(f_{\alpha(n)})\}$ constitutes a basis for $\mathbb{F}_q^n$. Define*

$$\tilde{C}(\eta) = \{\boldsymbol{c}\in\mathbb{F}_q^n \mid \boldsymbol{c}\cdot\varphi(f_{\alpha(i)})=0 \textit{ for all } \alpha(i)\in\Delta(R,\rho,\varphi) \textit{ with } \mu(\alpha(i))<\eta\}$$
$$\tilde{E}(\delta) = \mathit{Span}_{\mathbb{F}_q}\left\{\varphi(f_{\alpha(i)}) \mid \alpha(i)\in\Delta(R,\rho,\varphi) \textit{ and } \sigma(\alpha(i))\geqslant\delta\right\}$$

The following result concerning $\tilde{C}(\eta)$ is from [9, 5] and the result concerning $\tilde{E}(\delta)$ is from [1].

Theorem 9.10 *The minimum distance of $\tilde{C}(\eta)$ and $\tilde{E}(\delta)$ satisfy $d(\tilde{C}(\eta))\geqslant\eta$ and $d(\tilde{E}(\delta))\geqslant\delta$.*

Remark 9.11 In [1] a bound on the generalized Hamming weights of the $\tilde{E}(\delta)$ codes is given and this bound will also apply to the codes constructed in Section 9.5. However, generalized Hamming weights are beyond the scope of this article. ▽

We now know (in principle) how to construct the $\tilde{E}$ and $\tilde{C}$ codes and estimate their minimum distance using Theorem 9.10 above but we need a practical way of constructing order domains. This is where Gröbner basis theory will be used as shown in the next section.

9.3. The Gröbner basis approach to order domains

In this section we give a short introduction to order domains constructed using Gröbner basis theory (See [21, 8] for a detailed description). First we introduce the necessary concepts and a few results from Gröbner basis theory.

Let $\mathbb{F}_q$ denote a field with q elements and let $\mathcal{M}_m$ denote the set of monomials in $\mathbb{F}_q[x_1,x_2,\dots,x_m]$ given by $\mathcal{M}_m=\left\{x_1^{\alpha_1}x_2^{\alpha_2}\cdots x_m^{\alpha_m} \;\middle|\; (\alpha_1,\alpha_2,\dots,\alpha_m)\in\mathbb{N}_0^m\right\}$.

Recall that a monomial ordering $\prec$ on $\mathcal{M}_m$ is a relation on $\mathbb{N}_0^m$ satisfying the following conditions:

1. $\prec$ is a total ordering on $\mathbb{N}_0^m$.
2. If $\alpha\prec\beta$ and $\gamma\in\mathbb{N}_0^m$, then $\alpha+\gamma\prec\beta+\gamma$.

3. Every non-empty subset of $\mathbb{N}_0^m$ has a smallest element under $\prec$ (that is: $\prec$ is a well-ordering on $\mathbb{N}_0^m$).

Let $\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \ldots, \alpha_m)$ and $\boldsymbol{\beta} = (\beta_1, \beta_2, \ldots, \beta_m) \in \mathbb{N}_0^m$, $\boldsymbol{\alpha} \neq \boldsymbol{\beta}$, and let i, where $1 \leqslant i \leqslant m$, be the smallest index such that $\alpha_i - \beta_i \neq 0$ in the vector difference $\boldsymbol{\alpha} - \boldsymbol{\beta}$. Then $\boldsymbol{\alpha}$ is said to be lexicographically smaller than $\boldsymbol{\beta}$, denoted $\boldsymbol{\alpha} \prec_{lex} \boldsymbol{\beta}$, if $\alpha_i - \beta_i < 0$. We write $x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_m^{\alpha_m} \prec_{lex} x_1^{\beta_1} x_2^{\beta_2} \cdots x_m^{\beta_m}$ if $\boldsymbol{\alpha} \prec_{lex} \boldsymbol{\beta}$.

Given positive integers $w(x_1), w(x_2), \ldots, w(x_m) \in \mathbb{N}$ define a monomial function $w : \mathcal{M}_m \rightarrow \mathbb{N}$ by $w(x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_m^{\alpha_m}) = \sum_{i=1}^{m} \alpha_i w(x_i)$. For a monomial $m \in \mathcal{M}_m$ we call $w(m)$ the weight of m.

Remark 9.12 The weights $w(x_1), w(x_2), \ldots, w(x_m)$ can be defined as v-tuples from $\mathbb{N}_0^v \cup \{-\infty\}$. See [1] or [8, Sec. 4] for details. In this paper we only consider the case $v = 1$ which was studied in detail in [9, 15]. ▽

Definition 9.13 *The weighted degree ordering $\prec_w$ induced by w 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 one of the following two conditions hold:*

1) $w(m_1) < w(m_2)$ *2) $w(m_1) = w(m_2)$ and $m_1 \prec_{lex} m_2$.*

Given a monomial ordering $\prec$ on $\mathcal{M}_m$ and a polynomial $f \in \mathbb{F}_q[x_1, x_2, \ldots, x_m]$ let $lm(f)$ denote the leading monomial in the support of f with respect to $\prec$ and let $lt(f)$ denote the leading term in f with respect to $\prec$.

Definition 9.14 *Let $\mathbb{F}$ be a field and let $I \subset \mathbb{F}[x_1, x_2, \ldots, x_m]$ be an ideal. Given a monomial ordering $\prec$ on $\mathcal{M}_m$ the set*

$$\Delta_{\prec}(I) = \{m \in \mathcal{M}_m | m \textit{ is not a leading monomial of any } f \in I\}$$

is called the footprint of I with respect to $\prec$.

A Gröbner basis $G = \{g_1, g_2, \ldots, g_t\}$ for an ideal I is a basis for I with the property that $\langle lm(g_1), lm(g_2), \ldots, lm(g_t)\rangle = \langle lm(I)\rangle$, where $\langle lm(I)\rangle$ denotes the ideal generated by the leading monomials of $f \in I$ with respect to a given monomial ordering $\prec$. The footprint of I can always be found by constructing a Gröbner basis for I using Buchberger's algorithm [2, §2.7] since (using Definition 9.14 and the definition of a Gröbner basis) the monomials in $\Delta_{\prec}(I)$ are exactly the monomials in $\mathcal{M}_m$ which can't be divided by any of the leading monomials in G.

Let $I = \langle f_1, f_2, \ldots, f_s\rangle$ be an ideal in $\mathbb{F}[x_1, x_2, \ldots, x_m]$, let $\mathbb{V}(I)$ denote the corresponding variety given by $\mathbb{V}(I) = \{p_1, p_2, \ldots, p_n\} = \{p \in \mathbb{F}^m \mid f(p) = 0 \text{ for all } f \in I\}$. The following theorem from [2, Pro. 8] and [3, Pro. 2.7] is known as the footprint bound.

Theorem 9.15 *Let $\mathbb{F}$ be a field and let $I \subset \mathbb{F}[x_1, x_2, \ldots, x_m]$ be an ideal. Then $\#\mathbb{V}(I) \leqslant \#\Delta(I)$. Furthermore, if I is a radical ideal and $\mathbb{F}$ is algebraically closed then equality holds.*

Given an ideal $I \in \mathbb{F}[x_1, x_2, \ldots, x_m]$ consider the quotient of $\mathbb{F}[x_1, x_2, \ldots, x_m]$ modulo I, denoted $\mathbb{F}[x_1, x_2, \ldots, x_m]/I$ (see [2, §5.2]). Let $[f]$ denote the equivalence class of a polynomial $f \in \mathbb{F}[x_1, x_2, \ldots, x_m]$ given by

$$[f] = \{g \in \mathbb{F}[x_1, x_2, \ldots, x_m] \mid g \equiv f(mod\ I)\},$$

where $g \equiv f(mod\ I)$ (read: g and f are congruent modulo I), if $g - f \in I$. Let $\bar{f}$ denote the unique standard representative found as the remainder by dividing f with a Gröbner basis for I (See [2, Pro. 1, §5.3]).

From [2, Pro. 4, §5.3] we have the following result.

Proposition 9.16 *Let $I \subset \mathbb{F}_q[x_1, x_2, \ldots, x_m]$ be an ideal and let $\prec$ be a monomial ordering on $\mathcal{M}_m$. Then the set $B = \{[m] \mid m \in \Delta_\prec(I)\}$ is a basis for $\mathbb{F}_q[x_1, x_2, \ldots, x_m]/I$ as a vector space over $\mathbb{F}_q$.*

Consider the ideal $I_q = \langle f_1, f_2, \ldots, f_s, x_1^q - x_1, x_2^q - x_2, \ldots, x_m^q - x_m\rangle \subseteq \mathbb{F}_q[x_1, x_2, \ldots, x_m]$ and the variety $\mathbb{V}(I_q) = \{p_1, p_2, \ldots, p_n\}$, then the evaluation map $\varphi : \mathbb{F}_q[x_1, x_2, \ldots, x_m]/I_q \to \mathbb{F}_q^n$ given by

$$\varphi([f]) = (\bar{f}(p_1), \bar{f}(p_2), \ldots, \bar{f}(p_n)) = (f(p_1), f(p_2), \ldots, f(p_n))$$

is well-defined and is an isomorphism [6]. The following well-known corollary of Proposition 9.16 then follows.

Corollary 9.17 *Consider an ideal $I \subseteq \mathbb{F}_q[x_1, x_2, \ldots, x_m]$, let $I_q = I + \langle x_1^q - x_1, x_2^q - x_2, \ldots, x_m^q - x_m\rangle$ and let $\prec$ be any monomial ordering on $\mathcal{M}_m$. Then the footprint $\Delta_\prec(I_q)$ is finite and $\#\mathbb{V}(I_q) = \#\Delta_\prec(I_q)$ holds.*

Our goal in this section is to be able to use the factor ring $\mathbb{F}_q[x_1, x_2, \ldots, x_m]/I$ as our order domain in Definition 9.3 but to do so we are required to find an order function on $\mathbb{F}_q[x_1, x_2, \ldots, x_m]/I$. Pellikaan's factor ring theorem from [21, Thm. 5.11] given below gives us one way of doing this.

Theorem 9.18 *Let I be an ideal in $\mathbb{F}[x_1, x_2, \ldots, x_m]$ with Gröbner basis $\mathcal{B}$ with respect to $\prec_w$ (See Definition 9.13). Suppose that the elements of the footprint of I have mutually distinct weights and that every element of $\mathcal{B}$ has exactly two monomials of highest weight in its support. Then there exists a weight function ρ on $R = \mathbb{F}[x_1, x_2, \ldots, x_m]/I$ with the property that $\rho([f]) = w(\bar{f})$, for all polynomials f, where $[f]$ is the coset of f modulo I and $\bar{f}$ is the standard representative for $[f]$.*

Note that $w(\bar{f})$ in the theorem above is just the highest weight $w(m)$ of the monomials m in the support of $\bar{f}$, i.e. $w(\bar{f}) = \max\{w(m) \mid m \in Supp(\bar{f})\}$.

The consequence of Theorem 9.18 is that we can construct an order domain by defining an ideal $I \in \mathbb{F}[x_1, x_2, \ldots, x_m]$ with Gröbner basis $\mathcal{B}$, such that the elements in $\mathcal{B}$ and the monomials in $\Delta_{\prec}(I)$ satisfy the conditions in the theorem. This gives us the order structure (R, ρ, Γ) where $R = \mathbb{F}[x_1, x_2, \ldots, x_m]/I$, $\rho([f]) = w(\bar{f})$ and $\Gamma = \{w(m) \mid m \in \Delta_{\prec}(I)\} \subseteq \mathbb{N}_0$. This approach to constructing an order domain is shown in the next section.

9.4. Codes from Norm-Trace curves

The introduction to codes from Norm-Trace curves given here is based on the description in [7] where the evaluation codes $\tilde{E}$ from Definition 9.9 constructed using the order structure described in this section were studied in detail. Note that from here on the field $\mathbb{F}_{q^r}$ will be playing the role of $\mathbb{F}_q$ in Section 9.3. Furthermore, here we adopt the viewpoint from [11] where $\mathbb{F}_{q^r}$ is seen as a vector space over $\mathbb{F}_q$.

First we need the definition of Norm and Trace of an element in $\mathbb{F}_{q^r}$ over $\mathbb{F}_q$.

Definition 9.19 *For $\alpha \in \mathbb{F}_{q^r}$ the Norm $N_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\alpha)$ of α over $\mathbb{F}_q$ is defined as $N_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\alpha)$ $= \prod_{j=0}^{r-1} \alpha^{q^j} = \alpha^{(q^r-1)/(q-1)}$. The Trace $Tr_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\beta)$ of β over $\mathbb{F}_q$ is defined as $Tr_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\beta)$ $= \sum_{j=0}^{r-1} \beta^{q^j}$.*

Let $a = (q^r - 1)/(q - 1)$ and $b = q^{r-1}$. Let R be the factor ring given by $R = \mathbb{F}_{q^r}[x_1, x_2, \ldots, x_m]/I$, where $I = \langle x^a - y^b - y^{q^{r-2}} - \cdots - y\rangle$ and let $\prec$ be the monomial order induced by $w(x) = b, w(y) = a$ and $x \prec_{lex} y$. Since the polynomial $x^a - y^b - y^{q^{r-2}} - \cdots - y$ is a Gröbner basis for I satisfying the condition in Theorem 9.18 by definition, all we have to do is to check that the monomials in $\Delta_{\prec_w}(I) = \{x^i y^j \mid i, j \in \mathbb{N}_0 \text{ and } j < b\}$ have mutually distinct weights in order to use the theorem.

Let $x^{i_1}y^{j_1}, x^{i_2}y^{j_2} \in \Delta_{\prec_w}(I)$ and assume that $w(x^{i_1}y^{j_1}) = w(x^{i_2}y^{j_2})$. This is the same as $i_1 b + j_1 a = i_2 b + j_2 a \Leftrightarrow (i_1 - i_2)b = (j_2 - j_1)a$ but since $gcd(a, b) = 1$ then $(j_2 - j_1)$ must be equal to some integer c times b. Since $0 \leqslant j_1, j_2 < b$ then $c = 0$ is the only option. Hence $i_1 = i_2$ and $j_1 = j_2$.

Define $\Gamma = \{w(m) \mid m \in \Delta_{\prec_w}(I)\}$ and $\Gamma_{-\infty}$ as in Section 9.2, then the function $w(m) : R \to \Gamma_{-\infty}$ is a weight function (using Theorem 9.18) on R making $(R, w, \Gamma_{-\infty})$ an order structure and R an order domain. In the remaining part of this paper $(R, \rho, \Gamma_{-\infty})$ will denote an order structure as described here.

We still need a way of finding the set $\Delta(R, \rho, \varphi)$ in Definition 9.6 but the following proposition which is a more general version of [1, Pro. 7] gives us a way to do so. The proof given here is a modified version of the one given in [1].

Note that Proposition 9.20 contains [1, Pro. 7] as the special case where $J = I_{q^r} = I + \langle x_1^{q^r} - x_1, x_2^{q^r} - x_2, \ldots, x_m^{q^r} - x_m\rangle$.

Proposition 9.20 *Let $R = \mathbb{F}_{q^r}[x_1, x_2, \ldots, x_m]/I$ be an order domain as in Theorem 9.18, let $J = I + \langle x_1^{q^r} - x_1, x_2^{q^r} - x_2, \ldots, x_m^{q^r} - x_m, g_1, g_2, \ldots, g_s\rangle$, where $g_1, g_2, \ldots, g_s \in \mathbb{F}_{q^r}[x_1, x_2, \ldots, x_m]$, and consider the affine variety $\mathbb{V}(J) = \{p_1, p_2, \ldots, p_n\}$.*

The map $\varphi : R \to \mathbb{F}_{q^r}^n$ *given by* $\varphi([f]) = (\bar{f}(p_1), \bar{f}(p_2), \ldots, \bar{f}(p_n))$ *is a morphism as in Definition 9.5. Moreover,* φ *is surjective.*

Let $\Delta(R, \rho, \varphi) = \{\alpha(1), \alpha(2), \ldots, \alpha(n)\}$ *be given as in Definition 9.6. We have*

$$\Delta(R, \rho, \varphi) = \{w(m) \mid m \in \Delta_{\prec_w}(J)\}. \tag{9.1}$$

Proof: Clearly φ is well-defined and satisfies the conditions in Definition 9.5 which establish the first result. The surjectivity of φ follows from the comment after Proposition 9.16.

By Corollary 9.17 the equality $\#\mathbb{V}(J) = \#\Delta_{\prec_w}(J)$ holds and using Definition 9.6 the two sets in (9.1) must have the same number of elements. Thus if we can show that $\alpha(i) \in \{w(m) \mid m \in \Delta_{\prec_w}(J)\}$ for all $i = 1, 2, \ldots, n$ then we are done. Now, consider a fixed $\alpha(s) \in \Delta(R, \rho, \varphi)$ and a class $[f] \in R$ such that $\rho([f]) = \alpha(s)$ (Note that both f and $\bar{f}$ must be non-zero by Definition 9.6).

Furthermore, the standard representative $\bar{f}$ for $[f]$ can by definition be written as a linear combination of monomials in the footprint $\Delta_{\prec_w}(I)$ since $\bar{f}$ is the unique remainder of f divided by a Gröbner basis for I. Thus we have

$$\bar{f} = \sum_{i=1}^{t} a_i m_i$$

where $t \geqslant 1$, $a_i \in \mathbb{F}_{q^r} \setminus \{0\}$, $m_i \in \Delta_{\prec_w}(I)$, for $1 \leqslant i \leqslant t$, $w(m_1) < w(m_2) < \cdots < w(m_t)$ and $\alpha(s) = \rho([f]) = wdeg(\bar{f}) = w(m_t)$.

Let $\mathcal{B}'$ be a Gröbner basis for J. By reducing $\bar{f}$ modulo $\mathcal{B}'$ we get the (unique) remainder $\bar{r}$ given by

$$\bar{r} = \sum_{i=1}^{u} b_i n_i$$

where $u \geqslant 1$, $b_i \in \mathbb{F}_{q^r}$, $n_i \in \Delta_{\prec_w}(J)$, for $1 \leqslant i \leqslant u$, and $w(n_1) < w(n_2) < \cdots < w(n_u)$. Because $f - \bar{f} \in I$, $\bar{f} - \bar{r} \in J$ and $I \subseteq J$ (which means that $\mathbb{V}(J) \subseteq \mathbb{V}(I)$ (See [2, §4.2, Thm. 7])) we have

$$\varphi(\bar{r}) = \varphi(\bar{r}) + \varphi(\bar{f} - \bar{r}) = \varphi(\bar{r} + \bar{f} - \bar{r}) = \varphi(\bar{f}) = \varphi([f]), \tag{9.2}$$

since φ is a morphism (See Definition 9.5).

Note that $\varphi([f])$ in (9.2) by the definition of $\alpha(s)$ is non-zero which implies that $\bar{r}$ is non-zero. This fact and the fact that $\Delta_{\prec_w}(J) \subset \Delta_{\prec_w}(I)$ implies that $\rho([\bar{r}]) = w(n_u)$.

Using the division algorithm and the definition of $\prec_w$ we have $wdeg(\bar{f}) \geqslant wdeg(\bar{r})$ (See [2, §2.3, Thm. 3]) which is the same as saying that

$$\alpha(s) \geqslant w(n_u). \tag{9.3}$$

Comparing (9.2) and (9.3) and using the definition of $\alpha(s)$ in Definition 9.6 gives $\alpha(s) = w(n_u) \in \{w(m) \mid m \in \Delta_{\prec_w}(J)\}$. Since $\alpha(s)$ was arbitrary we have proved the theorem.

□

Proposition 9.20 allows us to construct codes using J and to use the technique described in Section 9.2 to estimate their minimum distance. The remaining part of this paper will focus on the $\tilde{E}(\delta)$ and $\tilde{C}(\eta)$ codes in Definition 9.9 constructed by evaluating points from $\mathbb{V}(J)$ using selected monomials in $\Delta_{\prec_w}(J)$.

9.5. Puncturing codes from Norm-Trace curves

In this section let $I = \langle x^a - y^b - y^{q^{r-2}} - \cdots - y\rangle$, let $(R, \varphi, \Gamma_{-\infty})$ be as in Proposition 9.20 and let $I_{q^r} = I + \langle x^{q^r} - x, y^{q^r} - y\rangle$. The variety $\mathbb{V}(I_{q^r})$ contains q^{2r-1} points (α, β) in $\mathbb{F}_{q^r}^2$ where $N_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\alpha) = Tr_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\beta)$ (See [7]) and the set $\{\varphi(m) \mid m \in \Delta_{\prec_w}(I_{q^r})\}$ is a basis for $\mathbb{F}_{q^r}^n$, where $n = q^{2r-1}$.

Puncturing a code from a Norm-Trace curve in t coordinates corresponds to redefining the evaluation map $\varphi : \mathbb{F}_{q^r}[x_1, x_2, \ldots, x_m]/I \to \mathbb{F}_{q^r}^n$ by leaving out t points from the variety $\mathbb{V}(I_{q^r})$ when evaluating, i.e. φ is redefined as:

$$\varphi([f]) = (\bar{f}(p_{i_1}), \bar{f}(p_{i_2}), \ldots, \bar{f}(p_{i_{n-t}})),$$

where $\{p_{i_1}, p_{i_2}, \ldots, p_{i_{n-t}}\} \subset \mathbb{V}(I_{q^r})$. Choosing the t randomly does not necessarily yield a case where Proposition 9.20 holds, so there may not be a good way to estimate the minimum distance of the punctured code.

This section shows how to construct a set of polynomials $S = \{g_1, g_2, \ldots, g_s\}$ such that $\#\mathbb{V}(I_{q^r} + \langle g_1, g_2, \ldots, g_s\rangle) = n - t$. For a given t a set S can be constructed in several different ways using the technique developed here but we can use the tools from Section 9.2 to estimate the minimum distance of the resulting codes and thereby select the best possible set S using this estimate.

Furthermore, the construction of $g_1, g_2, \ldots, g_s$ given here ensures that we remove nothing from the set $\{w(m) \mid m \in \Delta_{\prec_w}(I_{q^r})\}$ except the weights that we are forced to remove according to Proposition 9.7. In other words: the minimum distance of the resulting codes is the best possible using Theorem 9.10 when reducing the size of the footprint $\Delta_{\prec_w}(I_{q^r})$ by adding $g_1, g_2, \ldots, g_s$ to the basis of I_{q^r} (and thereby redefining the map φ).

It is well-known that Norm and Trace maps $\mathbb{F}_{q^r}$ onto $\mathbb{F}_q$ (See [11]). Furthermore, the Trace maps q^{r-1} elements from $\mathbb{F}_{q^r}$ onto every element in $\mathbb{F}_q$ and the Norm maps $\frac{q^r-1}{q-1}$ non-zero elements on every non-zero element in $\mathbb{F}_q$ (and only zero is mapped on zero using Norm). We now define the following two sets for every element in $\mathbb{F}_q$.

Definition 9.21 *Let $\mathbb{F}_q = \{\gamma_0, \gamma_1, \ldots, \gamma_{q-1}\} \subset \mathbb{F}_{q^r}$. Let $0 \leqslant i \leqslant q-1$ and define $\mathcal{N}(q, r, \gamma_i) \subset \mathbb{F}_{q^r}$ to be the set $\{\alpha \in \mathbb{F}_{q^r} \mid N_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\alpha) = \gamma_i\}$, where $N_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\alpha)$ is the Norm from Definition 9.19.*

Furthermore, define $\mathcal{T}(q, r, \gamma_i)$ to be the set $\{\beta \in \mathbb{F}_{q^r} \mid Tr_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\beta) = \gamma_i\}$, where and $Tr_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\beta)$ is the Trace from Definition 9.19.

Using the sets in Definition 9.21 we can define the following two orderings of the elements in $\mathbb{F}_{q^r}$.

Definition 9.22 *Let $\mathbb{F}_q = \{\gamma_0, \gamma_1, \ldots, \gamma_{q-1}\} \subset \mathbb{F}_{q^r}$, where $\gamma_0 = 0$, let $a = \frac{q^r-1}{q-1}$ and let $b = q^{r-1}$. Let $\mathbb{F}_{q^r}^{(\alpha)} = \{\alpha_0, \alpha_1, \ldots, \alpha_{q^r-1}\}$ be the elements in $\mathbb{F}_{q^r}$ ordered such that*

$$\begin{aligned}
\mathcal{N}(q,r,\gamma_0) &= \{\alpha_0\} \\
\mathcal{N}(q,r,\gamma_1) &= \{\alpha_1, \ldots, \alpha_a\} \\
\mathcal{N}(q,r,\gamma_2) &= \{\alpha_{a+1}, \ldots, \alpha_{2a}\} \\
&\vdots \\
\mathcal{N}(q,r,\gamma_{q-1}) &= \{\alpha_{(q-2)a+1}, \ldots, \alpha_{q^r-1}\}.
\end{aligned}$$

Furthermore, let $\mathbb{F}_{q^r}^{(\beta)} = \{\beta_0, \beta_1, \ldots, \beta_{q^r-1}\}$ be the elements in $\mathbb{F}_{q^r}$ ordered such that

$$\begin{aligned}
\mathcal{T}(q,r,\gamma_0) &= \{\beta_0, \ldots, \beta_{b-1}\} \\
\mathcal{T}(q,r,\gamma_1) &= \{\beta_b, \ldots, \beta_{2b-1}\} \\
\mathcal{T}(q,r,\gamma_2) &= \{\beta_{2b}, \ldots, \beta_{3b-1}\} \\
&\vdots \\
\mathcal{T}(q,r,\gamma_{q-1}) &= \{\beta_{(q-1)b}, \ldots, \beta_{q^r-1}\}.
\end{aligned}$$

Now we can construct the polynomials $g_1(x,y), g_2(x,y), \ldots, g_s(x,y)$ we need.

Definition 9.23 *Let $a = \frac{q^r-1}{q-1}$,$b = q^{r-1}$ and let $\{(i_1,j_1), (i_2,j_2), \ldots, (i_s,j_s)\}$ be given such that $0 \leqslant i_1 < i_2 < \cdots < i_{s-1} < i_s < \min\{i_1 + a, q^r\}$ and $0 \leqslant j_s < j_{s-1} < \cdots < j_2 < j_1 < b$. Define $g_1(x,y), g_2(x,y), \ldots, g_s(x,y)$ as follows.*

First define the polynomial $g(x) \in \mathbb{F}_{q^r}[x,y]$ as

$$g(x) = \prod_{u=0}^{i_1-1} (x - \alpha_u)$$

Then for every $1 \leqslant k \leqslant s$ define the polynomial $g_k(x,y) \in \mathbb{F}_{q^r}[x,y]$ as

$$g_k(x,y) = g(x) \prod_{u=q^r-(i_k-i_1)}^{q^r-1} (x - \alpha_u) \prod_{v=q^r-j_k}^{q^r-1} (y - \beta_v),$$

where the product over an empty set is defined to be 1.

Remark 9.24 The polynomials in Definition 9.23 have no multiple roots because the only way multiple roots could occur is if $i_1 > (q-2)a+1$ and $q^r - (i_k - i_1) < i_1$ for some $1 \leqslant k \leqslant s$. But this is not possible since $q^r - (i_k - i_1) < i_1 \Leftrightarrow q^r < i_k$, which contradicts the condition $0 \leqslant i_1 < i_2 < \cdots < i_s < \min\{i_1 + a, q^r\}$ from Definition 9.23. $\triangledown$

Furthermore, we need the following definition from [2, §2.6].

Definition 9.25 *Let $\mathbb{F}$ be a field, let $f, g \in \mathbb{F}[x_1, x_2, \ldots, x_m]$ be non-zero polynomials and let $\prec$ be a monomial ordering on the monomials in $\mathbb{F}[x_1, x_2, \ldots, x_m]$. Let $lm(f) = x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_m^{\alpha_m}$ and let $lm(g) = x_1^{\beta_1} x_2^{\beta_2} \cdots x_m^{\beta_m}$, where $lm(f)$ denotes the leading monomial of f with respect to $\prec$, and define $x_1^{\gamma_1} x_2^{\gamma_2} \cdots x_m^{\gamma_m}$ where $\gamma_i = \max\{\alpha_i, \beta_i\}$, for $1 \leqslant i \leqslant m$. The the S-polynomial of f and g, written $S(f,g)$, is the combination*

$$S(f,g) = \frac{x_1^{\gamma_1} x_2^{\gamma_2} \cdots x_m^{\gamma_m}}{lt(f)} \cdot f - \frac{x_1^{\gamma_1} x_2^{\gamma_2} \cdots x_m^{\gamma_m}}{lt(g)} \cdot g,$$

where $lt(f)$ is the leading term of f with respect to $\prec$.

The polynomials $g_1(x,y), g_2(x,y), \ldots, g_s(x,y)$ in Definition 9.23 have the following properties.

Proposition 9.26 *Let $g_1(x,y), g_2(x,y), \ldots, g_s(x,y) \in \mathbb{F}_{q^r}[x,y]$ be the polynomials from Definition 9.23 and let $\prec_w$ be the monomial ordering in Definition 9.13 where $w(x) = b = q^{r-1}, w(y) = a = \frac{q^r-1}{q-1}$ and $x \prec_{lex} y$. Furthermore, let $f(x,y) = x^a - y^b - y^{q^{r-2}} - \cdots - y^q - y$. Then the following holds:*

1. *$lm(g_k(x,y)) = x^{i_k} y^{j_k}$ with respect to the monomial ordering $\prec_w$, for all $1 \leqslant k \leqslant s$.*
2. *$\#\mathbb{V}\left(\langle f(x,y), x^{q^r} - x, y^{q^r} - y, g_1(x,y), g_2(x,y), \ldots, g_s(x,y)\rangle\right)$ $= \#\Delta_{\prec}\left(\langle y^b, x^{q^r}, x^{i_1} y^{j_1}, \ldots, x^{i_s} y^{j_s}, x^{i_1+a}\rangle\right)$*
3. *The set $\{f(x,y), x^{q^r} - x, y^{q^r} - y, g_1(x,y), g_2(x,y), \ldots, g_s(x,y), S(f,g_1)\}$ is a Gröbner basis for $\langle f(x,y), x^{q^r} - x, y^{q^r} - y, g_1(x,y), \ldots, g_s(x,y)\rangle$*

where $S(f,g_1)$ denotes the S-polynomial of $f(x,y)$ and $g_1(x,y)$.

Proof: That $lm(g_k(x,y)) = x^{i_k} y^{j_k}$, for $1 \leqslant k \leqslant s$, follows directly from Definition 9.23.

Let $J = \langle f(x,y), x^{q^r} - x, y^{q^r} - y, g_1(x,y), g_2(x,y), \ldots, g_s(x,y)\rangle$. Since the S-polynomial $S(f,g_1)$ is in J, we have that

$$\#\mathbb{V}(J) \leqslant \#\Delta_{\prec_w}(J) \leqslant \#\Delta_{\prec_w}\left(\langle y^b, x^{q^r}, x^{i_1} y^{j_1}, x^{i_2} y^{j_2}, \ldots, x^{i_s} y^{j_s}, x^{i_1+a}\rangle\right) \tag{9.4}$$

because the polynomial $S(f,g_1)$ has leading monomial x^{i_1+a}.

Let $\lambda = \min\{i_1 + a, q^r\}$. From Definition 9.23 we have that $0 \leqslant i_1 < i_2 < \cdots < i_{s-1} < i_s < \lambda$ and $0 \leqslant j_s < j_{s-1} < \cdots < j_2 < j_1 < b$.

The number at the right hand side of (9.4) is then equal to

$$\begin{aligned} &i_1 b + (i_2 - i_1)j_1 + (i_3 - i_2)j_2 + (i_4 - i_3)j_3 + \cdots + (i_s - i_{s-1})j_{s-1} + (\lambda - i_s)j_s \\ &\quad = i_1 b + \sum_{u=2}^{s} (i_u - i_{u-1}) j_{u-1} + (\lambda - i_s) j_s \end{aligned} \tag{9.5}$$

The remaining part of the theorem is proved by showing that the number of points in $\mathbb{V}(J)$ is equal to the sum in (9.5) and thereby showing that the set $\{f(x,y), x^{q^r} - x, y^{q^r} - y, g_1(x,y), g_2(x,y), \ldots, g_s(x,y), S(f,g_1)\}$ is a Gröbner basis for J.

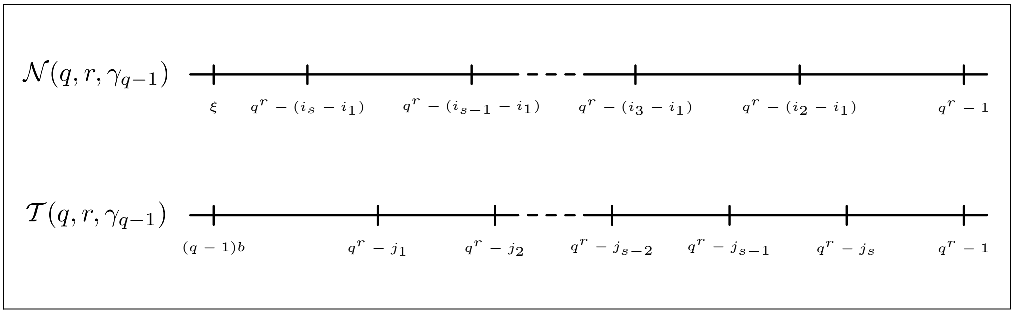

Figure 9.1.: A graphical representation of the two sets $\mathcal{N}(q,r,\gamma_{q-1})$ and $\mathcal{T}(q,r,\gamma_{q-1})$ in the situation from Definition 9.23 where $\xi=\max\{i_1+a,(q-2)a+1\}$.

Define $\xi=\max\{i_1,(q-2)a+1\}$. In Figure 9.1 a graphical representation of the set $\mathcal{N}(q,r,\gamma_{q-1})=\{\alpha_{(q-2)a+1},\dots,\alpha_{q^r-1}\}$ in $\mathbb{F}_{q^r}^{(\alpha)}$ and $\mathcal{T}(q,r,\gamma_{q-1})=\{\beta_{(q-1)b},\dots,\beta_{q^r-1}\}$ in $\mathbb{F}_{q^r}^{(\beta)}$ in the situation from Definition 9.23, for a given set $\{(i_1,j_1),(i_2,j_2),\dots,(i_s,j_s)\}$.

Note that when counting elements in $\mathbb{V}(J)$ we have no multiple roots (See Remark 9.24) and we have to make sure that we only count points (α,β) where $N_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\alpha)=Tr_{\mathbb{F}_{q^r}/fq}(\beta)$.

By construction of the polynomials $g_1(x,y),g_2(x,y),\dots,g_s(x,y)$ in Definition 9.23, the following number of points must be in the set $\mathbb{V}(J)$ (For reference see Figure 9.1):

- i_1b points (α_k,β) where $0\leqslant k<i_1$, since for every choice of $\alpha_k\in\mathbb{F}_{q^r}^{(\alpha)}$ there exists b different elements $\beta\in\mathbb{F}_{q^r}^{(\beta)}$ such that $N_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\alpha_k)=Tr_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\beta)$. These points are all the zeroes of $g(x)$ and thereby zeroes of every polynomial $g_1(x,y),g_2(x,y),\dots,$ $g_s(x,y)$.

- $(i_2-i_1)j_1$ points (α_k,β_l) where $\alpha_k\in\mathcal{N}(q,r,\gamma_{q-1})$, for $q^r-i_2+i_1\leqslant k<q^r$, and $\beta_l\in\mathcal{T}(q,r,\gamma_{q-1})$, for $q^r-j_1\leqslant l<q^r$. This is true because every counted α_k is a zero of $g_2(x,y),\dots,g_s(x,y)$ since $i_2<i_3<\cdots<i_s$ and every counted β_l is a zero of $g_1(x,y)$.

- $(i_3-i_2)j_2$ points (α_k,β_l) where $\alpha_k\in\mathcal{N}(q,r,\gamma_{q-1})$, for $q^r-(i_3-i_1-(i_2-i_1))=q^r-i_3+i_2\leqslant k<q^r$, and $\beta_l\in\mathcal{T}(q,r,\gamma_{q-1})$, for $q^r-j_2\leqslant l<q^r$. This holds because these α_k's are all zeroes of $g_3(x,y),\dots,g_s(x,y)$ because $i_3<i_4<\cdots<i_s$ and the β_l's are all zeroes of $g_1(x,y)$ and $g_2(x,y)$ since $j_1>j_2$. Furthermore, the choice of α_k's ensures that these points haven't been counted before.

- In general we have $(i_u-i_{u-1})j_{u-1}$ points (α_k,β_l) where α_k is a zero of $g_u(x,y)$, $g_{u+1}(x,y),\dots,g_s(x,y)$ and β_l is a zero of $g_1(x,y),\dots,g_{u-1}(x,y)$ for every choice of $2\leqslant u<s$. The construction in Definition 9.23 ensures that these points are zeroes of $g_1(x,y),\dots,g_s(x,y),f(x,y)$ and are all different.

- Finally, we have $(q^r-(i_s-i_1)-\xi)j_s$ points (α_k,β_l) where every β_l is a zero of $g_1(x,y),g_2(x,y),\dots,g_s(x,y)$ and the α_k's haven't been counted before. Since $\xi=$

$\max\{i_1, (q-2)a+1\} \Leftrightarrow \xi + a = \max\{i_1 + a, (q-1)a+1\} = \max\{i_1 + a, q^r\}$ and $\lambda = \min\{i_1 + a, q^r\}$, then $(q^r - (i_s - i_1) - \xi)j_s = (\lambda - i_s)j_s$ holds.

The number of points in $\mathbb{V}(J)$ is then at least $i_1 b + \sum_{u=2}^{s}(i_u - i_{u-1})j_{u-1} + (\lambda - i_s)j_s$ and equality must hold in (9.4) making the set $\{f(x,y), x^{q^r} - x, y^{q^r} - y, g_1(x,y), g_2(x,y), \ldots, g_s(x,y), S(f, g_1)\}$ a Gröbner basis for J. □

Before we move on to our main result an example of the construction of polynomials in Definition 9.23 is given to make the proof of Proposition 9.26 clear to the reader.

Example 9.27 The example given here is based on the Hermitian curve $f(x,y) = x^5 - y^4 - y$ over $\mathbb{F}_{16} = \{0, 1, \nu, \nu^2, \ldots, \nu^{14}\}$ where ν is a root of $1 + x^3 + x^4$ over $\mathbb{F}_2$, $q = 4$ and $q^2 = 16$. Let $a = 5$, $b = 4$, $w(x) = b$, $w(y) = a$ and $x \prec_{lex} y$.

We have that $\mathbb{F}_4 = \{0, 1, \nu^5, \nu^{10}\} \subset \mathbb{F}_{16}$.

$\mathbb{F}_{16}^{(\alpha)}$ from Definition 9.22 is then

$$\mathbb{F}_{16}^{(\alpha)} = \{\alpha_0, \ldots, \alpha_{15}\} = \{0, 1, \nu^3, \nu^6, \nu^9, \nu^{12}, \nu, \nu^4, \nu^7, \nu^{10}, \nu^{13}, \nu^2, \nu^5, \nu^8, \nu^{11}, \nu^{14}\}$$

where

$$\begin{aligned}
\mathcal{N}(4,2,0) &= \{0\} = \{\alpha_0\},\\
\mathcal{N}(4,2,1) &= \{1, \nu^3, \nu^6, \nu^9, \nu^{12}\} = \{\alpha_1, \ldots, \alpha_5\},\\
\mathcal{N}(4,2,\nu^5) &= \{\nu, \nu^4, \nu^7, \nu^{10}, \nu^{13}\} = \{\alpha_6, \ldots, \alpha_{10}\},\\
\mathcal{N}(4,2,\nu^{10}) &= \{\nu^2, \nu^5, \nu^8, \nu^{11}, \nu^{14}\} = \{\alpha_{11}, \ldots, \alpha_{15}\}.
\end{aligned}$$

Furthermore, we have

$$\mathbb{F}_{16}^{(\beta)} = \{\beta_0, \ldots, \beta_{15}\} = \{0, 1, \nu^5, \nu^{10}, \nu^7, \nu^{11}, \nu^{13}, \nu^{14}, \nu, \nu^3, \nu^4, \nu^{12}, \nu^2, \nu^6, \nu^8, \nu^9\}$$

where

$$\begin{aligned}
\mathcal{T}(4,2,0) &= \{0, 1, \nu^5, \nu^{10}\} = \{\beta_0, \ldots, \beta_3\},\\
\mathcal{T}(4,2,1) &= \{\nu^7, \nu^{11}, \nu^{13}, \nu^{14}\} = \{\beta_4, \ldots, \beta_7\},\\
\mathcal{T}(4,2,\nu^5) &= \{\nu, \nu^3, \nu^4, \nu^{12}\} = \{\beta_8, \ldots, \beta_{11}\},\\
\mathcal{T}(4,2,\nu^{10}) &= \{\nu^2, \nu^6, \nu^8, \nu^9\} = \{\beta_{12}, \ldots, \beta_{15}\}.
\end{aligned}$$

Let $(i_1, j_1) = (8, 3)$ and $(i_2, j_2) = (10, 2)$. We first define

$$g(x) = \prod_{u=0}^{7}(x - \alpha_u) = x(x-1)(x-\nu^3)(x-\nu^6)(x-\nu^9)(x-\nu^{12})(x-\nu)(x-\nu^4)$$

as in Definition 9.23 since $i_1 = 8$.

Then define $g_1(x,y) = g(x)\prod_{v=13}^{15}(y - \beta_v) = g(x)(y-\nu^6)(y-\nu^8)(y-\nu^9)$ since $j_1 = 3$.

Finally, define $g_2(x,y) = g(x)\prod_{u=14}^{15}(x-\alpha_u)\prod_{v=14}^{15}(y-\beta_v) = g(x)(x-\nu^{11})(x-\nu^{14})(y-\nu^8)(y-\nu^9)$ since $j_2 = 2$ and $i_2 - i_1 = 2$.

The following points are in $\mathbb{V}\left(\langle f(x,y), x^{16} - x, y^{16} - y, g_1(x,y), g_2(x,y)\rangle\right)$:

- All points of the form (α_u, β) where $0 \leqslant u < i_1 = 8$ and $N_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\alpha_u) = Tr_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\beta)$ because these points are both zeroes of $g(x)$ and $f(x,y)$ and thereby zeroes of $g_1(x,y), g_2(x,y)$ and $f(x,y)$. There are $i_1 \cdot b = 8 \cdot 4 = 32$ of these points since trace maps $b = 4$ elements from $\mathbb{F}_{q^2}$ on every element in $\mathbb{F}_q$.
- We then have $(i_2 - i_1)j_1 = 2 \cdot 3 = 6$ points (α_u, β_v) where $u = 14, 15$ and $v = 13, 14, 15$ since α_{14} and α_{15} are zeroes of $g_2(x,y)$ and β_{13}, β_{14} and β_{15} are zeroes of $g_1(x,y)$.
- Finally, we have the points (α_u, β_v) where $v = 14, 15$ and $\alpha_u \in \mathcal{N}(4, 2, \nu^{10})$ for $u \neq 14$ and $u \neq 15$. These points haven't been counted before and are zeroes of both $g_1(x,y), g_2(x,y)$ and $f(x,y)$ since every β_v that is a zero of $g_2(x,y)$ is also a zero of $g_1(x,y)$ by construction. We have $(a-(i_2-i_1))j_2 = (i_1+a-i_2)j_2 = (8+5-10)\cdot 2 = 6$ of these points.

We have found at least $32 + 6 + 6 = 44$ points in

$$\mathbb{V}\left(\langle f(x,y), x^{16} - x, y^{16} - y, g_1(x,y), g_2(x,y)\rangle\right)$$

which is equal to the size of the footprint of $\langle y^4, x^{16}, x^8y^3, x^{10}y^2, x^{13}\rangle$. △

Definition 9.28 *Let $I \subseteq \mathbb{F}_{q^r}[x,y]$ be an ideal, let $\prec$ be a monomial ordering and let $w(m)$ denote the weight of a monomial m. Define $W(I) = \{w(m) \mid m \in \Delta(I)\}$ and for $\alpha \in W(I)$ define*

$$M(\alpha) = \{\gamma \in W(I) \mid \exists\ \beta \in W(I) \text{ such that } \alpha + \beta = \gamma\}.$$

Now, we would like to prove that by adding polynomials constructed as in Definition 9.23 to the ideal I_{q^r} we remove exactly the smallest possible set of weights from $W(I_{q^r})$ (smallest in the sense that we remove exactly the weights that we are forced to remove from the set $W(I_{q^r})$ according to Proposition 9.7 and nothing more). This result is the consequence of Theorem 9.29 below.

Theorem 9.29 *Let $g_1(x,y), g_2(x,y), \ldots, g_s(x,y) \in \mathbb{F}_{q^r}[x,y]$ be the polynomials from Definition 9.23 and let $\prec$ be the monomial ordering in Definition 9.13 where $w(x) = b = q^{r-1}, w(y) = a = \frac{q^r-1}{q-1}$ and $x \prec_{lex} y$. Let $f(x,y) = x^a - y^b - y^{q^{r-2}} - \cdots - y^q - y$, let $I_{q^r} = \langle f(x,y), x^{q^r} - x, y^{q^r} - y\rangle \subset \mathbb{F}_{q^r}[x,y]$ and let*

$$J = I_{q^r} + \langle g_1(x,y), g_2(x,y), \ldots, g_s(x,y)\rangle.$$

Then the following equality holds:

$$W(J) = W(I_{q^r}) \Big\backslash \bigcup_{k=1}^{s} M\Big(w\big(lm(g_k(x,y))\big)\Big). \tag{9.6}$$

Proof: Since $\rho(m) = w(m)$ is a weight function (See Definition 9.2) we have that for every monomial $x^s y^t \in \Delta(I_{q^r})$, which can be divided by $x^{i_k} y^{j_k}$, the weight $w(x^s y^t) = sb + ta$ must be in the set $M(w(g_k(x, y)))$.

Because the set $\{f(x, y), x^{q^r} - x, y^{q^r} - y, g_1(x, y), \ldots, g_s(x, y), S(f, g_1)\}$ is a Gröbner basis for J (using Proposition 9.26) we only remove monomials from $\Delta(I_{q^r})$ which can be divided by at least one of the monomials $x^{i_1} y^{j_1}, \ldots, x^{i_s} y^{j_s}, x^{i_1+a}$ thereby having the equality

$$W(J) = W(I_{q^r}) \Bigg\backslash \left\{ \bigcup_{k=1}^{s} M(w(x^{i_k} y^{j_k})) \cup M(w(x^{i_1+a})) \right\}.$$

The only thing we need to prove is that $M(w(x^{i_1+a})) \subset M(w(x^{i_1} y^{j_1}))$ in order to have the equality in (9.6) and prove the theorem. This can be done by showing that $w(x^{i_1+a}) \in M(w(x^{i_1} y^{j_1}))$.

We consider the following two cases:

Case 1: $j_1 = 0$

In this case $x^{i_1} y^{j_1} = x^{i_1}$ which obviously divides x^{i_1+a} so $w(x^{i_1+a}) \in M(w(x^{i_1}))$.

Case 2: $j_1 > 0$

We have to find a monomial $x^s y^t \in \Delta(I_{q^r})$ such that

$$w(x^s y^t) + w(x^{i_1} y^{j_1}) = w(x^{i_1+a})$$

$$\Updownarrow$$

$$sb + ta + i_1 b + j_1 a = (i_1 + a)b \;\Leftrightarrow\; sb + (t + j_1)a = ab$$

which has the solution $s = 0, t = b - j_1$ and since $y^{b-j_1} \in \Delta(I_{q^r})$, we have proved the theorem. □

9.6. Examples

In this section we give a few examples of codes using the construction described in Section 9.5 and compare to known codes punctured in t coordinates.

Example 9.30 Here we continue Example 9.27 using the ideal $I_{16} = \langle x^5 - y^4 - y, x^{16} - x, y^{16} - y \rangle \in \mathbb{F}_{16}[x, y]$. Then

$$W(I_{16}) = \{0, 4, 5, 8, 9, 10, 12, 13, \ldots, 62, 63, 65, 66, 67, 70, 71, 75\}.$$

Let $t = 11$ so we want to puncture the Hermitian code at 11 coordinates to create codes of length 53. In Table 9.1 the first column is the parameters for the original improved Hermitian codes and the second column is the parameters for the punctured version we get by using ordinary puncturing 11 times.

The column labeled "Construction 1" in Table 9.1 is the parameters for the codes we get by using $J_{16}^{(1)} = I_{16} + \langle g_1^{(1)}(x,y), g_2^{(1)}(x,y)\rangle$ where $lm(g_1^{(1)}(x,y)) = x^{11}y^2$ and $lm(g_2^{(1)}(x,y)) = x^{15}y$. So

$$\begin{aligned} W(J_{16}^{(1)}) &= W(I_{16}) \setminus \{M(54) \cup M(65)\} \\ &= \{0,4,5,8,9,10,12,13,\ldots,52,53,55,56,57,60,61\}. \end{aligned}$$

The column labeled "Construction 2" is the parameters for the codes we get by using $J_{16}^{(2)} = I_{16} + \langle g_1^{(2)}(x,y), g_2^{(2)}(x,y)\rangle$ where $lm(g_1^{(2)}(x,y)) = x^{13}y$ and $lm(g_2^{(2)}(x,y)) = x^{14}$. We have

$$\begin{aligned} W(J_{16}^{(2)}) &= W(I_{16}) \setminus \{M(56) \cup M(57)\} \\ &= \{0,4,5,8,9,10,12,13,\ldots,52,53,54,55,58,59,63\}. \end{aligned}$$

For dimensions $38, 40, 41, 42, 43, 44, 45, 46, 49$ and 51 one or both of the two constructions are better than the bound obtained by ordinary puncturing. Also note that none of the two constructions are the best choice for every dimension since using construction 1 we get a $[53, 38, 11]$ code while using construction 2 we get a $[53, 38, 10]$ code. But using construction 2 gives a $[53, 40, 9]$ code and a $[53, 47, 4]$ code while construction 1 gives a $[53, 39, 9]$ code and a $[53, 46, 4]$.

Table 9.1.: Parameters for the improved Hermitian codes $\tilde{E}(\delta)$, improved Hermitian codes punctured at 11 coordinates and estimated parameters for construction 1 and 2 with length 53.

Improved Hermitian codes ($\tilde{E}(\delta)$)	Punctured improved Hermitian codes ($\tilde{E}(\delta)$)	Construction 1	Construction 2
$[64,1,64]$	$[53,1,53]$	$[53,1,53]$	$[53,1,53]$
$[64,2,60]$	$[53,2,49]$	$[53,2,49]$	$[53,2,49]$
$[64,3,59]$	$[53,3,48]$	$[53,3,48]$	$[53,3,48]$
$[64,4,56]$	$[53,4,45]$	$[53,4,45]$	$[53,4,45]$
$[64,5,55]$	$[53,5,44]$	$[53,5,44]$	$[53,5,44]$
$[64,6,54]$	$[53,6,43]$	$[53,6,43]$	$[53,6,43]$
$[64,7,52]$	$[53,7,41]$	$[53,7,41]$	$[53,7,41]$
$[64,8,51]$	$[53,8,40]$	$[53,8,40]$	$[53,8,40]$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
$[64,35,24]$	$[53,35,13]$	$[53,35,13]$	$[53,35,13]$
$[64,36,23]$	$[53,36,12]$	$[53,36,12]$	$[53,36,12]$
$[64,37,22]$	$[53,37,11]$	-	$[53,37,11]$
$[64,38,21]$	$[53,38,10]$	$[53,38,11]$	$[53,38,10]$
$[64,39,20]$	$[53,39,9]$	$[53,39,9]$	-
$[64,40,19]$	$[53,40,8]$	-	$[53,40,9]$

continued on the next page

Improved	Punctured improved		
Hermitian codes ($\tilde{E}$)	Hermitian codes ($\tilde{E}$)	Construction 1	Construction 2
$[64, 41, 18]$	$[53, 41, 7]$	$[53, 41, 8]$	$[53, 41, 8]$
$[64, 42, 17]$	$[53, 42, 6]$	-	-
$[64, 43, 16]$	$[53, 43, 5]$	$[53, 43, 7]$	-
$[64, 44, 15]$	$[53, 44, 4]$	-	$[53, 44, 6]$
$[64, 45, 14]$	$[53, 45, 3]$	$[53, 45, 5]$	$[53, 45, 5]$
$[64, 46, 13]$	$[53, 46, 2]$	$[53, 46, 4]$	-
-	-	-	$[53, 47, 4]$
$[64, 48, 12]$	$[53, 48, 1]$	-	-
$[64, 49, 10]$	$[53, 49, 1]$	$[53, 49, 3]$	$[53, 49, 3]$
$[64, 51, 9]$	$[53, 51, 1]$	$[53, 51, 2]$	$[53, 51, 2]$
$[64, 53, 8]$	$[53, 53, 1]$	$[53, 53, 1]$	$[53, 53, 1]$

Furthermore, notice that the parameters in Table 9.1 can be calculated without actually constructing any polynomials but by using Theorem 9.29, the code construction $\tilde{E}$ in Definition 9.9 and the bound on the minimum distance given in Theorem 9.10. We could construct the generator matrices by using Definition 9.23 to construct $g_1(x, y)$ and $g_2(x, y)$, find the 53 common zeros in $\mathbb{V}(J_{16})$ and use the evaluation map φ on the monomials selected in Definition 9.9 to construct the rows in the generator matrix for $\tilde{E}(\delta)$ for any given $\delta = 1, 2, \ldots, 53$.

We could have constructed codes with length 53 in several other ways than the two shown here but the two used here are the best choices. The remaining 10 possibilities are:

$$\begin{aligned}
W(J_{16}) &= W(I_{16}) \setminus \{M(55) \cup M(62)\} \\
W(J_{16}) &= W(I_{16}) \setminus \{M(56) \cup M(59)\} \\
W(J_{16}) &= W(I_{16}) \setminus \{M(57) \cup M(58)\} \\
W(J_{16}) &= W(I_{16}) \setminus \{M(57) \cup M(59)\} \\
W(J_{16}) &= W(I_{16}) \setminus \{M(56) \cup M(62) \cup M(63)\} \\
W(J_{16}) &= W(I_{16}) \setminus \{M(57) \cup M(60) \cup M(63)\} \\
W(J_{16}) &= W(I_{16}) \setminus \{M(58) \cup M(59) \cup M(60)\} \\
W(J_{16}) &= W(I_{16}) \setminus \{M(58) \cup M(59) \cup M(61)\} \\
W(J_{16}) &= W(I_{16}) \setminus \{M(58) \cup M(60) \cup M(61)\} \\
W(J_{16}) &= W(I_{16}) \setminus \{M(59) \cup M(60) \cup M(61) \cup M(62)\}
\end{aligned}$$

△

Example 9.31 In this example we use the same ideal, I_{16}, and the two constructions given in Example 9.30 but this time we construct the $\tilde{C}$ codes from Definition 9.9 using construction 1 and 2 from Example 9.30 instead. Note that the Hermitian codes $\tilde{C}(\eta)$

(and the ordinary puncturing of these) have the same parameters as the Hermitian $\tilde{E}(\delta)$ codes in Example 9.30 (see [1, Prop. 8]) but when using the new construction given here the resulting $\tilde{E}$ and $\tilde{C}$ no longer have the same parameters. The results are given in Table 9.2.

Notice that for dimensions $1, 2, \ldots, 6$ construction 1 and 2 are sometimes actually doing worse than ordinary puncturing but for dimensions $37, 40, 42, 44, 45, 48, 50$ and 52 constructions 1 and 2 are equally good and both better than ordinary puncturing.

Again, the parameters in Table 9.2 can be calculated without actually constructing any polynomials but we could construct the rows in the parity check matrix for $\tilde{C}(\eta)$ for any given $\eta = 1, 2, \ldots, 53$.

Table 9.2.: Parameters for the improved Hermitian codes $\tilde{C}(\eta)$, the improved Hermitian codes punctured at 11 coordinates and estimated parameters for construction 1 and 2 with length 53.

Improved Hermitian codes ($\tilde{C}(\eta)$)	Punctured improved Hermitian codes ($\tilde{C}(\eta)$)	Construction 1	Construction 2
$[64, 1, 64]$	$[53, 1, 53]$	$[53, 1, 50]$	$[53, 1, 52]$
$[64, 2, 60]$	$[53, 2, 49]$	$[53, 2, 49]$	$[53, 2, 48]$
$[64, 3, 59]$	$[53, 3, 48]$	$[53, 3, 46]$	$[53, 3, 47]$
$[64, 4, 56]$	$[53, 4, 45]$	$[53, 4, 45]$	$[53, 4, 44]$
$[64, 5, 55]$	$[53, 5, 44]$	$[53, 5, 44]$	$[53, 5, 43]$
$[64, 6, 54]$	$[53, 6, 43]$	$[53, 6, 42]$	$[53, 6, 42]$
$[64, 7, 52]$	$[53, 7, 41]$	$[53, 7, 41]$	$[53, 7, 41]$
$[64, 8, 51]$	$[53, 8, 40]$	$[53, 8, 40]$	$[53, 8, 40]$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
$[64, 35, 24]$	$[53, 35, 13]$	$[53, 35, 13]$	$[53, 35, 13]$
$[64, 36, 23]$	$[53, 36, 12]$	-	-
$[64, 37, 22]$	$[53, 37, 11]$	$[53, 37, 12]$	$[53, 37, 12]$
$[64, 38, 21]$	$[53, 38, 10]$	$[53, 38, 10]$	$[53, 38, 10]$
$[64, 39, 20]$	$[53, 39, 9]$	-	-
$[64, 40, 19]$	$[53, 40, 8]$	$[53, 40, 9]$	$[53, 40, 9]$
$[64, 41, 18]$	$[53, 41, 7]$	-	-
$[64, 42, 17]$	$[53, 42, 6]$	$[53, 42, 8]$	$[53, 42, 8]$
$[64, 43, 16]$	$[53, 43, 5]$	-	-
$[64, 44, 15]$	$[53, 44, 4]$	$[53, 44, 6]$	$[53, 44, 6]$
$[64, 45, 14]$	$[53, 45, 3]$	$[53, 45, 5]$	$[53, 45, 5]$
$[64, 46, 13]$	$[53, 46, 2]$	-	-
-	-	-	-
$[64, 48, 12]$	$[53, 48, 1]$	$[53, 48, 4]$	$[53, 48, 4]$
$[64, 49, 10]$	$[53, 49, 1]$	-	-
-	-	$[53, 50, 3]$	$[53, 50, 3]$

continued on the next page

Improved Hermitian codes ($\tilde{C}(\eta)$)	Punctured improved Hermitian codes ($\tilde{C}(\eta)$)	Construction 1	Construction 2
$[64, 51, 9]$	$[53, 51, 1]$	-	-
-	-	$[53, 52, 2]$	$[53, 52, 2]$
$[64, 53, 8]$	$[53, 53, 1]$	$[53, 53, 1]$	$[53, 53, 1]$

Furthermore, we could also have constructed codes with length 53 in several other ways than the two shown here. The remaining 10 possibilities are the same as in Example 9.30.

△

Remark 9.32 Notice that the function $\mu(\eta)$ from Definition 9.8 and the bound in Theorem 9.10 underestimates the minimum distance of the dimension 1 $\tilde{C}(\eta)$ codes in construction 1 and 2 in Example 9.31. This suggests that Theorem 9.10 doesn't give the true minimum distance of $\tilde{C}$ codes from an ideal not having a footprint meeting the condition in [1, Prop. 8]. Thus the conjecture in the conclusion of [20] doesn't hold for general codes such as those studied here. ▽

Example 9.33 In this final example let $q = 2$ and $r = 6$ over $\mathbb{F}_{64}$ such that

$$I_{64} = \langle x^{63} - y^{32} - y^{16} - y^8 - y^4 - y^2 - y, x^{64} - x, y^{64} - y \rangle.$$

The resulting codes have length $q^{2r-1} = 2^{11} = 2048$.

Let $t = 64$, $w(x) = 32$, $w(y) = 63$, $x \prec_{lex} y$ and $lm(g_1(x, y)) = x^{62}$ such that $J_{64} = I_{64} + \langle g_1(x, y) \rangle$ and $W(J_{64}) = W(I_{64}) \setminus M(1984)$. The codes constructed from $\mathbb{F}_q[x_1, x_2, \ldots, x_m]/J_{64}$ have length 1984 and a comparison with the ordinary puncturing of the codes from Norm-Trace curves of length 2048 can be seen in Figure 9.2.

Notice that for rates about 0.9 the difference between the two codes is the biggest. Parameters for a few codes with approximately this rate are given in Table 9.3.

Table 9.3.: Parameters for some $\tilde{E}$ codes from Norm-Trace curves, $\tilde{E}$ codes punctured at 64 coordinates and the new construction for rates about 0.9.

$\tilde{E}(\delta)$ codes from Norm-Trace curves	Punctured $\tilde{E}(\delta)$ codes from Norm-Trace curves	New construction
$[2048, 1791, 69]$	$[1984, 1791, 5]$	-
-	-	$[1984, 1792, 52]$
$[2048, 1794, 68]$	$[1984, 1794, 4]$	-
-	-	$[1984, 1795, 51]$
$[2048, 1799, 66]$	$[1984, 1799, 2]$	-
-	-	$[1984, 1800, 50]$
$[2048, 1801, 65]$	$[1984, 1801, 1]$	-
-	-	$[1984, 1802, 49]$

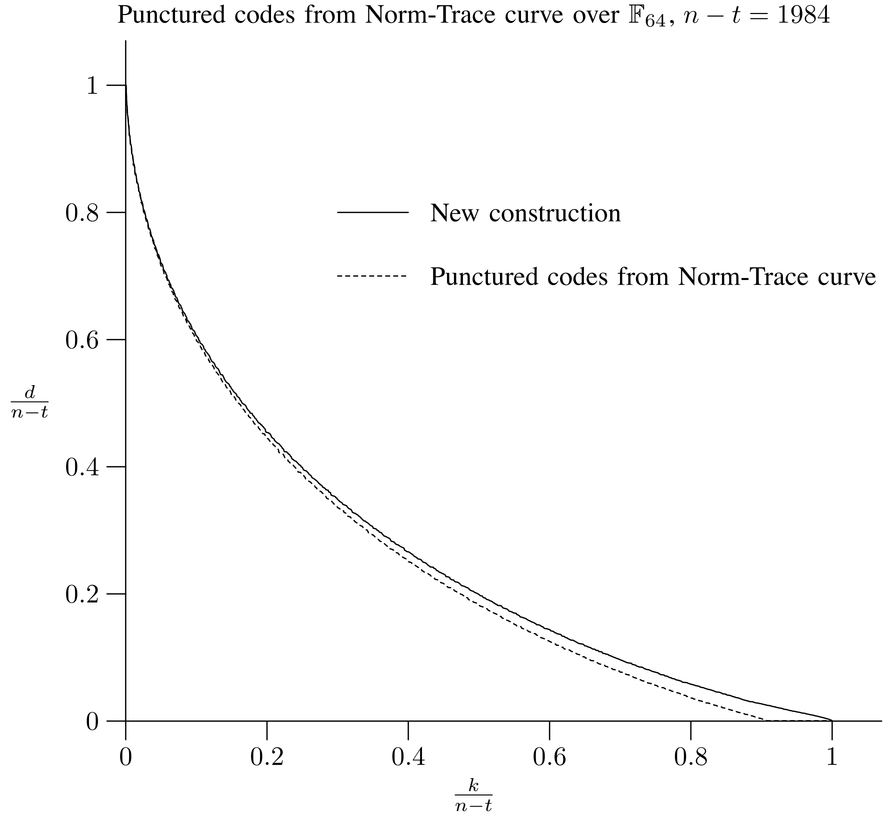

Figure 9.2.: Code rates $\frac{k}{n-t}$ plotted with relative minimum distance $\frac{d}{n-t}$ for ordinarily punctured codes from Norm-Trace curves and codes from the new construction, both of length $n-t=1984$.

△

9.7. Conclusion

In this paper it was demonstrated that the bound on the minimum distance of codes punctured in t coordinates can be substantially improved in the case of codes from Norm-Trace curves by adding polynomials to the ideal used to construct the order domain. Furthermore, a specific construction of such polynomials is given.

In cases where the puncturing in t coordinates can be constructed using several choices of polynomials, no single choice is the best possible for all code rates as demonstrated in Example 9.30. Furthermore, Example 9.31 shows a case where the order bound clearly doesn't give the true minimum distance when constructing the improved dual codes $\tilde{C}$ with extra polynomials added to the ideal.

The technique used here allows for explicit construction of generator or parity check matrices for evaluation codes and dual codes and the improvement compared to the ordinary bound on puncturing can be substantial as demonstrated in Example 9.33 where a puncturing in $t = 64$ coordinates results in a loss in minimum distance of at most 16 (for $k = 1802$ and $n - t = 1984$).

9.8. Acknowledgments

The author would like to thank Olav Geil and Christian Thommesen, Department of Mathematical Sciences, Aalborg University, Denmark, for helpful discussions.

9.9. References

[1] H. Andersen and O. Geil. The Missing Evaluation Codes from Order Domain Theory. Submitted - preprint available at: `http://www.math.aau.dk/research/reports/R-2004-17.pdf`.

[2] D. Cox, J. Little, and D. O'Shea. *Ideals, Varieties and Algorithms - An Introduction to Computational Algebraic Geometry and Commutative Algebra.* Springer Verlag, New York, second edition, 1997.

[3] D. Cox, J. Little, and D. O'Shea. *Using Algebraic Geometry.* Springer Verlag, New York, 1998.

[4] G. L. Feng and T. R. N. Rao. A simple approach for construction of algebraic-geometric codes from affine plane curves. *IEEE Trans. Inform. Theory*, 40(4):1003–1012, 1994.

[5] G.-L. Feng and T. R. N. Rao. Improved geometric Goppa codes. I. Basic theory. *IEEE Trans. Inform. Theory*, 41(6, part 1):1678–1693, 1995. Special issue on algebraic geometry codes.

[6] J. Fitzgerald and R. F. Lax. Decoding affine variety codes using Gröbner bases. *Designs, Codes and Cryptography*, 13(2):147–158, 1998.

[7] O. Geil. On Codes from Norm-Trace Curves. *Finite Fields and Their Applications*, 9(3):351–371, July 2003.

[8] O. Geil and R. Pellikaan. On the Structure of Order Domains. *Finite Fields and Their Applications*, 8:369–396, 2002.

[9] T. Høholdt, J. van Lint, and R. Pellikaan. Chapter 10: "Algebraic geometry codes" in *Handbook of coding theory, V. S. Pless and W. C. Huffman (Eds.), vol. 1.* Elsevier, Amsterdam, 1998.

[10] T. Høholdt, J. H. van Lint, and R. Pellikaan. Order functions and evaluation codes. In *Applied algebra, algebraic algorithms and error-correcting codes (Toulouse, 1997)*, volume 1255 of *Lecture Notes in Comput. Sci.*, pages 138–150. Springer, Berlin, 1997.

[11] R. Lidl and H. Niederreiter. *Introduction to finite fields and their applications.* Cambridge University Press, 1986.

[12] F. MacWilliams and N. Sloane. *The Theory of Error-Correcting Codes.* North-Holland Amsterdam, 1977.

[13] R. Matsumoto. The C_{ab} Curve.
Available at: `http://www.rmatsumoto.org/cab.html`.

[14] R. Matsumoto. Miura's Generalization of One-Point AG Codes is Equivalent to Høholdt, van Lint and Pellikaan's Generalization. *IEICE Trans. Fundamentals*, E82-A(10):2007–2010, October 1999.

[15] R. Matsumoto and S. Miura. On the Feng-Rao Bound for $\mathcal{L}$-Construction of Algebraic Geometry Codes. *IEICE Trans. Fundamentals*, E83-A(5):923–927, 2000.

[16] S. Miura. Algebraic geometric codes on certain plane curves. *IEICE Trans.*, J75-A(11):1735–1745, 1992. (In japanese).

[17] S. Miura. PhD thesis, University of Tokyo, May 1997. (In Japanese).

[18] S. Miura. Linear Codes on Affine Algebraic Varieties. *IEICE Trans.*, J81-A(10):1386–1397, 1998. (In Japanese).

[19] S. Miura and N. Kamiya. On the Minimum Distance of Codes from Some Maximal Curves. Technical Report IT92-147, IEICE, Marts 1993. (In Japanese).

[20] C. Munuera and D. Ramirez. The second and third generalized Hamming weights of Hermitian codes. *IEEE Trans. Inform. Theory*, 45(2):709–712, 1999.

[21] R. Pellikaan. On the existence of order functions. *Journal of Statistical Planning and Inference*, 94:287–301, 2001.