Albert Vico Oton

Collected results on semigroups, graphs and codes

TESI DOCTORAL

dirigida per la
Dra. Maria Bras-Amorós

Departament
d'Enginyeria Informàtica i
Matemàtiques



Universitat
Rovira i Virgili

Tarragona
Juliol 2012

Universitat Rovira i Virgili
Departament d'Enginyeria
Informàtica i Matemàtiques.

FAIG CONSTAR que aquest treball, titulat "Collected results on semigroups, graphs and codes", que presenta Albert Vico Oton per a l'obtenció del títol de Doctor URV, ha estat realitzat sota la meva direcció al Departament d'Enginyeria Informàtica i Matemàtiques d'aquesta universitat.

Tarragona, 14 de Juliol 2012.

El Director de la tesi doctoral

Dr. Maria Bras-Amorós.

Acknowledgements

Deserving of special mention is Dra. Maria Bras-Amorós, my advisor to whom I want to express my absolute gratitude for the outstanding work she did; supporting and helping me whenever I needed, giving always wise advices, patiently correcting my messed work and many more things that she didn't need to do but anyway did, without her that thesis wouldn't exist. Many, many thanks.

Also and special mention deserves my couple Isabel, for her blind support and trust, and for always being there besides the grumpy moments.

The author also wants to express his gratitude to Josep Domingo-Ferrer for many helpful comments and contributions. The author is also grateful to Pedro García-Sánchez, without whom the work on the non-homogeneous patterns of numerical semigroups wouldn't be the same. And at last, but not the least many thanks to Kwankyu Lee. His sharp comments and efficient contributions on the Feng-Rao numbers and Hamming weights made possible the development on one of the papers found in this thesis.

Contents

1 Introduction **7**
- 1.1 Abstract . . . 8
- 1.2 Context, hypotheses and objectives . . . 8
- 1.3 Contributions of this thesis . . . 11
- 1.4 Publications . . . 12

2 On the Geil-Matsumoto bound and the length of AG codes **17**
- 2.1 Introduction . . . 18
- 2.2 Membership for semigroups with two generators . . . 18
- 2.3 The Geil-Matsumoto bound . . . 20
- 2.4 Coincidences of Lewittes's and the Geil-Matsumoto bound . . . 21
- 2.5 Simplifying the computation . . . 22

3 New lower bounds on the generalized Hamming weights of AG codes **29**
- 3.1 Introduction . . . 30
- 3.2 The maximum integer not belonging to an ideal . . . 31
  - 3.2.1 An upper bound for the maximum integer not belonging to an ideal 31
  - 3.2.2 Ideals attaining the upper bound . . . 32
- 3.3 A lower bound on the Feng-Rao numbers . . . 34
  - 3.3.1 Feng-Rao numbers . . . 34
  - 3.3.2 Bound on the Feng-Rao numbers . . . 35
  - 3.3.3 Sharpness of the bound . . . 37
  - 3.3.4 An example . . . 38
- 3.4 Intervals of gaps in Hermitian codes and codes on a Garcia-Stichtenoth tower of codes . . . 40
  - 3.4.1 Hermitian codes . . . 40
  - 3.4.2 Codes on the Garcia-Stichtenoth tower of codes . . . 40

4 Non-homogeneous patterns on numerical semigroups **43**
- 4.1 Introduction . . . 44
- 4.2 Motivating examples . . . 44
  - 4.2.1 Semigroups with maximal embedding dimension . . . 44
  - 4.2.2 The Geil-Matsumoto bound . . . 45

4.2.3 Combinatorial configurations 46
4.3 Non-homogeneous patterns 46
4.4 Patterns involving the multiplicity 49
4.5 Non-homogeneous Frobenius varieties 50
4.6 Non-homogeneous strongly admissible patterns 53

5 On the minimum number of colluders of a pirate copy for fingerprinting with Reed-Solomon codes 57
5.1 Introduction 58
5.2 Reed-Solomon codes and interpolating polynomials 59
5.3 A lower bound 60
5.4 An upper bound, revisited 62
5.5 On shortened fingerprints 62
5.6 Drawback and overcoming it by a closer look to polynomial factorization . . 63
5.7 On the number of roots of a polynomial depending on the coefficients of highest degree 66

6 Co-citations and relevance of authors and author groups 69
6.1 Introduction 70
6.2 The co-citation graph 74
6.3 Relevance of individual authors 75
6.4 Relevance of a group of authors 78
6.5 Concluding remarks 82

7 Bibliography 85

Chapter 1

Introduction

1.1 Abstract

In this thesis we present a compendium of five works where discrete mathematics play a key role. The first three works describe different developments and applications of the semigroup theory while the other two have more independent topics. First we present a result on semigroups and code efficiency, where we introduce our results on the so-called Geil-Matsumoto bound and Lewittes' bound for algebraic geometry codes. Following that, we work on semigroup ideals and their relation with the Feng-Rao numbers; those numbers, in turn, are used to describe the Hamming weights which are used in a broad spectrum of applications, i.e. the wire-tap channel of type II or in the t-resilient functions used in cryptography. The third work presented describes the non-homogeneous patterns for semigroups, explains three different scenarios where these patterns arise and gives some results on their admissibility. The last two works are not as related as the first three but still use discrete mathematics. One of them is a work on the applications of coding theory to fingerprinting, where we give results on the traitor tracing problem and we bound the number of colluders in a colluder set trying to hack a fingerprinting mark made with a Reed-Solomon code. And finally in the last work we present our results on scientometrics and graphs, modeling the scientific community as a cocitation graph, where nodes represent authors and two nodes are connected if there is a paper citing both authors simultaneously. We use it to present three new indices to evaluate an author's impact in the community.

1.2 Context, hypotheses and objectives

This thesis deals with several different applied problems where discrete mathematics play an important role. The problems all have to do with secure and reliable communications and knowledge engineering. The mathematical tools used are objects such as graphs, numerical semigroups, error correcting codes, and polynomials over finite fields.

The thesis is a compendium of five different research papers that have already been published or that are submitted. Each chapter is devoted to a different work and constitutes a whole *corpus* by its own. Next we sketch the context, hypotheses, and objectives of each work.

Semigroups and code efficiency Error correcting codes are a mathematical tool used to add reliability to digital communications. Given n pairwise distinct elements $\alpha_1, \ldots, \alpha_n$ of a finite field $\mathbb{F}_q$, the Reed-Solomon code $RS_{\alpha_1,\ldots,\alpha_n}(k)$ is defined by $\{(f(\alpha_1), \ldots, f(\alpha_n)) : f \in \mathbb{F}_q[x], \deg(f) < k\}$. Reed-Solomon codes have very interesting properties but they have the problem that the length of $RS_{\alpha_1,\ldots,\alpha_n}(k)$ is n and so, it is bounded by the field size q. Algebraic geometry codes generalize this giving codes attaining very important asymptotic bounds. Given n pairwise distinct places $P_1, \ldots, P_n$ of degree one of an algebraic function field $F/\mathbb{F}_q$, and a divisor G with support disjoint from $\{P_1, \ldots, P_n\}$, the geometric Goppa code $C_{P_1,\ldots,P_n}(G)$ is defined by $\{(f(P_1), \ldots, f(P_n)) : f \in L(G)\}$.

Then, the length of $C_{P_1,\ldots,P_n}(G)$ is n and it is bounded by the number of places of degree one of $F/\mathbb{F}_q$. Thus, an important problem of algebraic coding theory is bounding the number of places of degree one of function fields. The Hasse-Weil bound for the number of places of degree one of a function field as well as Serre's improvement use only the genus of the function field and the field size. Geil and Matsumoto gave in 2009 a bound in terms of the Weierstrass semigroup of a rational place (i.e. the set of pole orders of rational functions having only poles in that place). It is a neat formula although it is not closed and it may be computationally hard to calculate. Our **hypothesis** is that the same bound can be stated with a simpler formula, at least for some particular classes of semigroups. Our **objective** is to give a closed formula of the Geil-Matsumoto bound for semigroups generated by two integers (as is the case of most of the semigroups used for algebraic-geometry codes), analyze in which cases the Geil-Matsumoto bound coincides with the much simpler Lewittes bound (1990), and try to find simplifications in the computation of the Geil-Matsumoto bound.

Semigroup ideals, Feng–Rao numbers and the generalized Hamming weights The generalized Hamming weights of a linear code are, for each given dimension, the minimum size of the support of the linear subspaces of that dimension. They were first used to analyze the performance of the wire-tap channel of type II and in connection to t-resilient functions. The generalized Hamming weights have also been used in the context of list decoding, for bounding the covering radius of linear codes, and recently for secure secret sharing based on linear codes. In particular, Guruswami shows that his (e, L)-list decodability concept for erasures is equivalent with the generalized Hamming weights for linear codes. In the case of algebraic geometry codes, the generalized Hamming weights can be studied through the so-called generalized order bounds, involving Weierstrass semigroups. A constant depending only on the semigroup and the dimension of the Hamming weights was introduced by Farrán and Munuera, from which the order bounds could be completely determined for codes of rate low enough. This constant was called Feng–Rao number. Besides, we can define an ideal of a numerical semigroup as a subset of the semigroup such that any element in the subset plus any element of the semigroup add up to an element of the subset. Our **hypothesis** is that the Feng–Rao numbers can be studied in terms of ideals of a numerical semigroup. Indeed, the definition of the Feng–Rao numbers, although not stated in these terms, is tightly related to the notion of gap of an ideal. Our **objective** is twofold. On one hand we want to find a bound on the maximum gap of an ideal paralleling the well known bound of the Frobenius number of a semigroup in terms of the genus. On the other hand we want to apply this results to improve the knowledge on the Feng–Rao numbers and to derive new improved bounds on the generalized Hamming weights of algebraic geometry codes.

Patterns on numerical semigroups A numerical semigroup Λ is a subset of the non-negative integers $\mathbb{N}_0$ that contains 0 and is closed under addition, and such that $\mathbb{N}_0 \setminus \Lambda$ is finite. Arf semigroups appear in many theoretical problems in algebraic geometry as well as in some applied areas such as coding theory. Arf semigroups are those semigroups such that for any elements x_1, x_2, x_3 in the semigroup with $x_1 \geq x_2 \geq x_3$, the integer $x_1 + x_2 - x_3$

also belongs to the semigroup. This definition inspired studying the so-called patterns on numerical semigroups. Patterns on numerical semigroups are multivariate polynomials such that evaluated at any decreasing sequence of elements of the semigroup give integers belonging to the semigroup. For their simplicity, and for their inspiration in Arf semigroups, patterns were first defined to be linear and homogeneous. Our **hypothesis** is that non-homogeneous patterns also must be studied and interesting results may be observed. Indeed, some families of numerical semigroups have appeared lately in very different areas of applied mathematics which satisfy linear non-homogeneous patterns. For instance, the semigroups for which the previously mentioned Geil-Matsumoto bound coincides with the Lewittes bound. Other examples can be found in finite geometries with applications to peer-to-peer user-private information retrieval (P2P UPIR) or in the study of maximal embedding dimension semigroups. Our **objective** is to extend the known results on homogeneous patterns to non-homogeneous patterns and find applications to the Geil-Matsumoto bound, to finite geometries and/or to P2P UPIR.

Error correcting codes and traceability of illegal redistribution In the digital era one main concern is the illegal redistribution of digital contents. One way to fight it is by marking every single copy of the material that one does not want to have redistributed. This can be done by embedding a different imperceptible string of bits or symbols to each copy. Once an illegal copy is caught, if it was not modified, the illegal re-distributor can be re-identified by the mark in his/her copy. This is called fingerprinting. An attack to fingerprinting can be performed by a group of colluders. They can compare their copies and create a new pirate copy by erasing all the bits or symbols in which their copies differ or by using at each position where they differ, the bit or symbol that one of the users has there. Reed-Solomon codes are a classical family of error control codes which have been extensively used also in the context of fingerprinting. The classical problem of fingerprinting is defining tracing algorithms for identifying at least one of the colluders that originated a given pirate copy. Our **hypothesis** is that once an illegal copy is caught, it is also important to have an estimate number of the size of the colluder set. Indeed, we want to know the minimum number of colluders capable of generating a given pirate copy when the code used for fingerprinting is a Reed-Solomon code. Our **objective** is to find a lower bound on this minimum number. Having this lower bound means that once an illegal copy is caught, we can assert that at least a certain number of colluders, given by this bound, were involved in it.

Graphs and scientometrics Scientometrics studies the importance and impact of the scientific production of either a sole author, a community of authors, a journal or a given event such as a conference. The h-index is a widely known measure but it has a lot of weaknesses. It counts the number of papers with a given number of citations. However it does not distinguish citations according to the distance between cited and citing authors. Sometimes the whole scientific community is modeled as a collaboration graph where each researcher is represented by a node and there is an edge between two different nodes if there exists a joint publication of both authors. Then one parameter to evaluate citations

is the node distance between citing and cited authors. Our **hypothesis** is that not only the collaboration distance of authors measures the *scientific distance* between them but also the cocitation distance. We propose to model the scientific community as a cocitation graph, instead of a collaboration graph, where the nodes still represent authors, but where two nodes are connected if there is a paper citing both authors simultaneously. Our **objective** is to propose and analyze new scientometric indices based on the cocitation graph.

1.3 Contributions of this thesis

Semigroups and code efficiency In the second chapter, we solve the membership problem for numerical semigroups generated by two co-prime integers. Then we use that result to deduce a closed formula for the Geil-Matsumoto bound when the Weierstrass semigroup is generated by two integers. After that, we return to semigroups generated by any number of integers and study in which cases Lewittes' bound and the Geil-Matsumoto bound coincide allowing us to efficiently compute the Geil-Matsumoto bound. Finally we give a result that may simplify the computation of the Geil-Matsumoto bound when we can not apply our previous results. We also distinguish what we call Geil-Matsumoto generators. The most tedious part on the computation of the Geil-Matsumoto bound can be restricted to computing on these generators.

Semigroup ideals, Feng–Rao numbers, and the generalized Hamming weights Our first result is an analogue of the upper bound on the Frobenius number of a numerical semigroup. For a numerical semigroup of genus g, the Frobenius number is at most $2g-1$. The Frobenius number is exactly $2g-1$ if and only if the semigroup is symmetric. We prove that if d is the number of elements in the complement of an ideal with respect to a semigroup of genus g then the maximum gap of the ideal is at most $d+2g-1$. Now, this maximum gap is exactly $d+2g-1$ if and only if the ideal is exactly the semigroup minus the set of divisors of a non-gap that can not be decomposed as a sum of non-gaps. The bound on the maximum gap of an ideal generalizes the bound on the Frobenius number since that bound can be derived from this bound by taking the ideal to be the whole semigroup. Using the new upper bound on the maximum element not belonging to an ideal, we derive a lower bound on the so-called Feng–Rao numbers and consequently a new bound on the generalized Hamming weights. The main tool is analyzing the length of the intervals of consecutive gaps of the Weierstrass semigroup. We finally study the intervals of consecutive gaps for Hermitian codes and for codes in one of the Garcia-Stichtenoth towers of codes attaining the Drinfeld-Vlăduţ bound.

Patterns on numerical semigroups Along the fourth chapter, we present our results on non-homogeneous patterns on numerical semigroups. First of all we explain three scenarios where non-homogeneous patterns arise. The first one is related to algebraic geometry, the second one is on pure theory of numerical semigroups, and the third one is related to finite geometry. After explaining those three examples we formally characterize the non-

homogeneous patterns that are admissible, and particularize this study to the case the independent term of the pattern is a multiple of the multiplicity of the semigroup. For the so called strongly admissible patterns, the set of numerical semigroups admitting these patterns with fixed multiplicity m form an m-variety, which allows us to represent this set in a tree and to describe minimal sets of generators of the semigroups in the variety with respect to the pattern. Furthermore, we characterize strongly admissible patterns having a finite associated tree.

Error correcting codes and traceability of illegal redistribution The main result presented in the fifth chapter (Theorem 5.3.2) is a lower bound on the minimum number of colluders capable of generating a given pirate copy when the code used for fingerprinting is a Reed-Solomon code. Having this lower bound means that once an illegal copy is caught, we can assert that at least a certain number of colluders, given by this bound, were involved in it. The bound in Theorem 5.3.2 is extended to shortened fingerprints obtaining an analogous bound for this case. This result can be used in turn for bounding the number of colluders that were not caught once a subset of colluders is caught. We finish the chapter with an open question whose solution would bring out a significant improvement of our bound allowing to further improve the bound on the number of colluders capable of generating a pirate copy.

Graphs and scientometrics In the sixth chapter we introduce the co-citation graph and use it to define three indices of relevance for individual authors. We then distinguish between the relevance of an author and the relevance of a group of authors, and give a group version of the previous three indices that measure the relevance of a group of authors, in the sense of evaluating how present the group is in the citations by papers in a certain subject. The indices are: *Maximum co-cited index:* counts the number of authors for which a given author is maximum co-cited; *Weighted maximum co-cited index:* counts the number of authors to which a given author is maximum co-cited weighted by the number of co-citations, so it is strongly related with the previous one; *Co-citation entropy:* which measures how transversal an author is perceived by the community. Furthermore we present the application of such indices on a well-known group of authors and their impact.

1.4 Publications

Next we list the publications that derived from this thesis.

Semigroups and code efficiency

1. M. Bras-Amorós, A. Vico-Oton: *On the Geil-Matsumoto Bound and the Length of AG Codes*, Designs, Codes and Cryptography, Accepted, 2012. Impact factor 0,771. DOI: 10.1007/s10623-012-9703-5.

2. M. Bras-Amorós, A. Vico-Oton: *On the Geil-Matsumoto Bound*, Third International Castle Meeting on Coding Theory and Applications, J. Borges and M. Villanueva (eds.), Servei de Publicacions Universitat Autònoma de Barcelona, pp. 75–80, September 2011, ISBN: 978–84–490–2688–1.

3. M. Bras-Amorós, A. Vico-Oton: *On the Geil-Matsumoto Bound*, Workshop on Computational Security, Centre de Recerca Matemàtica, pp. 51–54, November 2011.

Semigroup ideals, Feng–Rao numbers, and the generalized Hamming weights

1. M. Bras-Amorós, K. Lee, A. Vico-Oton: *On the Maximal Gap of an Ideal and the Feng-Rao Numbers*, Iberian Meeting on Numerical Semigroups (IMNS2012), Vila-Real, Portugal, July 2012. (abstract)

2. M. Bras-Amors, K. Lee, A. Vico-Oton: *Semigroup Ideals and New Lower Bounds on the Generalized Hamming Weights of AG Codes*, to be submitted.

Patterns on numerical semigroups

1. M. Bras-Amorós, A. Vico-Oton: *On Non-Homogeneous Patterns on Numerical Semigroups*, Encuentros de Álgebra Computacional y Aplicaciones (EACA), Alcalá de Henares, Spain, June 2012.

2. M. Bras-Amorós, A. Vico-Oton: *On Non-Homogeneous Patterns on Numerical Semigroups*, Iberian Meeting on Numerical Semigroups (IMNS2012), Vila-Real, Portugal, July 2012. (abstract).

3. M. Bras-Amorós, P. García-Sánchez, A. Vico-Oton: *NonHomogeneous Patterns on Numerical Semigroups*, Submitted to International Journal of Algebra and Computation.

Error correcting codes and traceability of illegal redistribution

1. M. Bras-Amorós, A. Vico-Oton: *On the Size of the Colluder Set in Fingerprinting Attacks*, Soria Summer School on Computational Mathematics (S3CM), July 2010. (abstract).

2. M. Bras-Amorós, A. Vico-Oton: *On the Size of the Colluder Set in Fingerprinting Attacks*, XI Reunión Española sobre Criptología y Seguridad de la Información (RECSI), September 2010. ISBN: 978–84–693–3304–4.

Graphs and scientometrics

1. M. Bras-Amorós, J. Domingo-Ferrer, A. Vico-Oton: *Co-citations and Relevance of Authors and Author Groups*, International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, World Scientific. vol. 19, pp. 127–139, September 2011, ISSN: 0218–4885. Impact factor 0,850. DOI: 10.1142/S0218488511007386.

2. M. Bras-Amorós, J. Domingo-Ferrer, A. Vico-Oton: *Co-citations and Relevance of Authors and Author Groups*, Encuentro de Jóvenes Investigadores en Matemáticas (PEJIM 2012), Tenerife, Spain, September 2012. (abstract)

Chapter 2

On the Geil-Matsumoto bound and the length of AG codes

2.1 Introduction

Given n pairwise distinct places $P_1, \ldots, P_n$ of degree one of an algebraic function field $F/\mathbb{F}_q$, and a divisor G with support disjoint from $\{P_1, \ldots, P_n\}$, the geometric Goppa code $C_{P_1,\ldots,P_n}(G)$ is defined by $\{(f(P_1), \ldots, f(P_n)) : f \in L(G)\}$. See [75] for a general reference. Then, the length of $C_{P_1,\ldots,P_n}(G)$ is n and it is bounded by the number of places of degree one of $F/\mathbb{F}_q$. Thus, an important problem of algebraic coding theory is bounding the number of places of degree one of function fields.

The Hasse-Weil bound for the number of places of degree one of a function field as well as Serre's improvement use only the genus of the function field and the field size. Geil and Matsumoto give in [30] a bound in terms of the Weierstrass semigroup of a rational place (i.e. the set of pole orders of rational functions having only poles in that place). It is a neat formula although it is not closed and it may be computationally hard to calculate. Lewittes' bound [46] preceded the Geil-Matsumoto bound and it only considers the smallest generator of the numerical semigroup. It can be derived from the Geil-Matsumoto bound and so it is weaker. The advantage of Lewittes' bound with respect to the Geil-Matsumoto bound is that Lewittes' bound is very simple to compute.

Important curves such as hyperelliptic curves, Hermitian curves or Geil's norm-trace curves [29] have Weierstrass semigroups generated by two integers. Also, for any numerical semigroup Λ generated by two coprime integers, one can get the equation of a curve having a place whose Weierstrass semigroup is Λ [39].

In Section 2.2, we give some notions on numerical semigroups and solve the membership problem for numerical semigroups generated by two coprime integers. Then in Section 2.3 we use the result in Section 2.2 to deduce a closed formula for the Geil-Matsumoto bound when the Weierstrass semigroup is generated by two integers. In Section 2.4 we return to semigroups generated by any number of integers and study in which cases Lewittes' bound and the Geil-Matsumoto bound coincide. In Section 2.5 we give a result that may simplify the computation of the Geil-Matsumoto bound.

2.2 Membership for semigroups with two generators

Let $\mathbb{N}_0$ be the set of non-negative integers. A *numerical semigroup* is a subset of $\mathbb{N}_0$ containing 0, closed under addition and with finite complement in $\mathbb{N}_0$. A general reference for numerical semigroups is [64]. For a numerical semigroup Λ define the *genus* of Λ as the number $g = \#(\mathbb{N}_0 \setminus \Lambda)$. The elements in Λ are called the *non-gaps* of Λ while the elements in $\mathbb{N}_0 \setminus \Lambda$ are called the *gaps* of Λ.

The *generators* of a numerical semigroup are those non-gaps which can not be obtained as a sum of two smaller non-gaps. If $a_1, \ldots, a_l$ are the generators of a semigroup Λ then $\Lambda = \{n_1a_1 + \cdots + n_la_l : n_1, \ldots, n_l \in \mathbb{N}_0\}$ and so $a_1, \ldots, a_l$ are necessarily coprime. If $a_1, \ldots, a_l$ are coprime, we call $\{n_1a_1 + \cdots + n_la_l : n_1, \ldots, n_l \in \mathbb{N}_0\}$ the *semigroup generated* by $a_1, \ldots, a_l$ and denote it by $\langle a_1, \ldots, a_l \rangle$.

Among numerical semigroups, those generated by two integers, that is, numerical semigroups of the form $\{ma + nb : m, n \in \mathbb{N}_0\}$ for some coprime integers a, b, have a particular interest. Important curves such as hyperelliptic curves, Hermitian curves or Geil's norm-trace curves [29] have Weierstrass semigroups generated by two integers. Properties of semigroups generated by two coprime integers can be found in [42]. For instance, the semigroup generated by a and b has genus $\frac{(a-1)(b-1)}{2}$, and any element $i \in \Lambda$ can be uniquely written as $i = ma + nb$ with m, n integers such that $0 \leqslant n \leqslant a-1$. From the results in [39, Section 3.2] one can get, for any numerical semigroup Λ generated by two coprime integers the equation of a curve having a point whose Weierstrass semigroup is Λ.

For a numerical semigroup, the membership problem is that of determining, for any integer i whether it belongs or not to the numerical semigroup. In the next lemma we first state a result already proved in [42] and then we give a solution to the membership problem for semigroups generated by two coprime integers. By $x \mod a$ with x, a integers we mean the smallest positive integer congruent with x modulo a.

Lemma 2.2.1. *Suppose Λ is generated by a, b with $a < b$. Let c be the inverse of b modulo a.*

1. *Any $i \in \Lambda$ can be uniquely written as $i = ma + nb$ for some $m, n \geqslant 0$ with $n \leqslant a - 1$.*

2. *$i \in \Lambda$ if and only if $b(i \cdot c \mod a) \leqslant i$.*

Proof. 1. Suppose $i \in \Lambda$. Then $i = \tilde{m}a + \tilde{n}b$ for some non-negative integers $\tilde{m}, \tilde{n}$. Let $n = \tilde{n} \mod a$ and $m = \tilde{m} + b\lfloor \frac{\tilde{n}}{a} \rfloor$. Then $i = \tilde{m}a + \tilde{n}b = \tilde{m}a + (a\lfloor \frac{\tilde{n}}{a} \rfloor + (\tilde{n} \mod a))b = ma + nb$ with obviously $m, n \geqslant 0$ and $n \leqslant a - 1$.

   For uniqueness, suppose $i = ma + nb$ for some $m, n \geqslant 0$ and $n \leqslant a-1$, and simultaneously, $i = m'a + n'b$ for some $m', n' \geqslant 0$ and $n' \leqslant a - 1$. Then $(m - m')a = (n' - n)b$. Since a and b are coprime, a must divide $n - n'$ which can only happen if $n = n'$ and so $m = m'$.

2. If $i \in \Lambda$ then by the previous statement there exist unique integers $m, n \geqslant 0$ with $n \leqslant a - 1$ such that $i = ma + nb$. In this case, $i \cdot c \mod a = (ma + nb) \cdot c \mod a = n$ and then it is obvious that $b(i \cdot c \mod a) \leqslant i$.

   On the other hand, suppose $i \in \mathbb{N}_0$ and define $n = i \cdot c \mod a$. Then $i - nb$ is a multiple of a since $(i - nb) \mod a = ((i \mod a) - (nb \mod a)) \mod a = 0$. If $nb \leqslant i$ then $i - nb$ is a positive multiple of a, say ma, and $i = ma + nb$, so $i \in \Lambda$.

□

Remark 2.2.2. *Notice that for the case $b = a + 1$ the condition $b(i \cdot c \mod a) \leqslant i$ is equivalent to $(a + 1)(i \mod a) \leqslant i$ and to $a(i \mod a) \leqslant i - (i \mod a)$ and so $i \mod a \leqslant \lfloor \frac{i}{a} \rfloor$. Therefore, $i \in \langle a, a+1 \rangle$ if and only if the remainder of the division of i by a is at most its quotient. This was already proved in [28].*

2.3 The Geil-Matsumoto bound

Let $N_q(g)$ be the maximum number of rational places of degree one of a function field over $\mathbb{F}_q$ with genus g. The Hasse-Weil bound [75, Theorem V.2.3] states $|N_q(g)-(q+1)| \leqslant 2g\sqrt{q}$. Serre's refinement [75, Theorem V.3.1] states $|N_q(g) - (q+1)| \leqslant g\lfloor 2\sqrt{q}\rfloor$ which leads to

$$N_q(g) \leqslant S_q(g) := q + 1 + g\lfloor 2\sqrt{q}\rfloor.$$

If we consider the Weierstrass semigroup Λ of any such places then we can define $N_q(\Lambda)$ as the maximum number of rational places of degree one of a function field over $\mathbb{F}_q$ such that the Weierstrass semigroup at one of the places is Λ. Lewittes' bound [46] states, if λ_1 is the first non-zero element in Λ,

$$N_q(\Lambda) \leqslant L_q(\Lambda) := q\lambda_1 + 1$$

and the Geil-Matsumoto bound [30] is

$$N_q(\Lambda) \leqslant GM_q(\Lambda) := \#(\Lambda \setminus \cup_{\lambda_i \text{ generator of } \Lambda}(q\lambda_i + \Lambda)) + 1. \tag{2.1}$$

In [30, 39] the next result is proved, from which Lewittes' bound can be deduced from the Geil-Matsumoto bound.

Lemma 2.3.1. $\#(\Lambda \setminus (q\lambda_1 + \Lambda)) = q\lambda_1$.

Here, for a numerical semigroup generated by two coprime integers a, b we describe the Geil-Matsumoto bound in terms of a, b giving a formula which is simpler to compute than (2.1).

Theorem 2.3.2. *The Geil-Matsumoto bound for the semigroup generated by a and b with $a < b$ is*

$$GM_q(\langle a, b\rangle) = 1 + \sum_{n=0}^{a-1} \min\left(q, \left\lceil \frac{q-n}{a} \right\rceil \cdot b\right) \tag{2.2}$$

$$= \begin{cases} 1 + qa & \text{if } q \leqslant \lfloor \frac{q}{a} \rfloor b \\ 1 + (q \bmod a)q + (a - (q \bmod a))\lfloor \frac{q}{a} \rfloor b & \text{if } \lfloor \frac{q}{a} \rfloor b < q \leqslant \lceil \frac{q}{a} \rceil b \\ 1 + ab\lceil \frac{q}{a} \rceil - (a - (q \bmod a))b & \text{if } q > \lceil \frac{q}{a} \rceil b \end{cases} \tag{2.3}$$

Proof. The Geil-Matsumoto bound for the semigroup generated by a and b with $a < b$ is $1 + \#\left\{ i \in \Lambda : \begin{array}{l} i - qa \notin \Lambda \\ i - qb \notin \Lambda \end{array} \right\}$. By Lemma 2.2.1 $i \in \Lambda$ if and only if $b(ic \mod a) \leqslant i$, where c is the inverse of b modulo a. Now, suppose that $i \in \Lambda$ can be expressed as $i = ma + nb$ for some integers $m, n \geqslant 0$, $n \leqslant a - 1$. Then

$$\begin{aligned} i - qa \notin \Lambda &\iff b((i-qa)c \mod a) > i - qa \\ &\iff b((ma + nb - qa)c \mod a) > i - qa \\ &\iff b(nbc \mod a) > i - qa \\ &\iff bn > i - qa \\ &\iff bn > (m-q)a + nb \\ &\iff (m-q)a < 0 \\ &\iff m < q \end{aligned}$$

$$\begin{aligned} i - qb \notin \Lambda &\iff b((i-qb)c \mod a) > i - qb \\ &\iff b((ma + nb - qb)c \mod a) > i - qb \\ &\iff b((n-q)bc \mod a) > i - qb \\ &\iff b((n-q) \mod a) > i - qb \\ &\iff b((n-q) \mod a) > ma + (n-q)b \\ &\iff b[((n-q) \mod a) - (n-q)] > ma \\ &\iff b\left\lceil \frac{q-n}{a} \right\rceil > m \end{aligned}$$

Consequently, the Geil-Matsumoto bound is

$$1 + \sum_{n=0}^{a-1} \min\left(q, \left\lceil \frac{q-n}{a} \right\rceil \cdot b\right)$$

Now some technical steps lead to the next formula.

$$GM_q(\langle a, b\rangle) = \begin{cases} 1 + qa & \text{if } q \leqslant \lceil \frac{q-a+1}{a} \rceil b \\ 1 + (q \mod a)q + (a - (q \mod a))\lceil \frac{q-a+1}{a} \rceil b & \text{if } \lceil \frac{q-a+1}{a} \rceil b < q \leqslant \lceil \frac{q}{a} \rceil b \\ 1 + ab\lceil \frac{q}{a} \rceil - (a - (q \mod a))b & \text{if } q > \lceil \frac{q}{a} \rceil b \end{cases} \tag{2.4}$$

Since $\lceil \frac{q-a+1}{a} \rceil$ is the unique integer between $\frac{q-a+1}{a}$ and $\frac{q}{a}$, one has $\lceil \frac{q-a+1}{a} \rceil = \lfloor \frac{q}{a} \rfloor$, and the formula in (2.4) coincides with that in (2.3). □

2.4 Coincidences of Lewittes's and the Geil-Matsumoto bound

We are interested now in the coincidences of Lewittes's and the Geil-Matsumoto bound. To get an idea, one can see in Table 2.1 the portion of semigroups for which they coincide for several values of the genus and the field size.

For the case of two generators, from equation (2.2) we deduce that $GM_q(\langle a, b\rangle) = L_q(\langle a, b\rangle)$ if and only if $q \leqslant \lfloor \frac{q}{a} \rfloor b$. Otherwise, the Geil-Matsumoto bound always gives an improvement with respect to Lewittes's bound. We want to generalize this to semigroups with any number of generators.

Lemma 2.4.1. *Let $\Lambda = \langle \lambda_1, \ldots, \lambda_n \rangle$ with $\lambda_1 < \lambda_i$ for all $i > 1$. The next statements are equivalent*

1. $GM_q(\Lambda) = L_q(\Lambda)$,
2. $\Lambda \setminus \cup_{i=1}^{n}(q\lambda_i + \Lambda) = \Lambda \setminus (q\lambda_1 + \Lambda)$,
3. $q(\lambda_i - \lambda_1) \in \Lambda$ *for all* $i > 1$.

Proof. By Lemma 2.3.1 it is obvious that 2 implies 1. The converse follows from the inclusion $\Lambda \setminus \cup_{i=1}^{n}(q\lambda_i+\Lambda) \subseteq \Lambda \setminus (q\lambda_1+\Lambda)$ and the equality $GM_q(\Lambda) = L_q(\Lambda)$ which, by Lemma 2.3.1, implies that $\#(\Lambda \setminus \cup_{i=1}^{n}(q\lambda_i+\Lambda)) = \#(\Lambda \setminus (q\lambda_1+\Lambda))$.

For the equivalence of the last two statements notice that $q(\lambda_i - \lambda_1) \in \Lambda$ for all $i > 1 \iff q\lambda_i \in q\lambda_1 + \Lambda$ for all $i > 1 \iff q\lambda_i + \Lambda \subseteq q\lambda_1 + \Lambda$ for all $i > 1 \iff \Lambda \setminus \cup_{i=1}^{n}(q\lambda_i + \Lambda) = \Lambda \setminus (q\lambda_1 + \Lambda)$. □

Lemma 2.4.1 suggests to analyze under what conditions $q(\lambda_i - \lambda_1) \in \Lambda$ for some $i > 1$. Let us first see in what cases $q(\lambda_i - \lambda_1) \in \{x\lambda_1 + y\lambda_i : x, y \in \mathbb{N}_0\}$. Notice that if $\gcd(\lambda_1, \lambda_i) = d$ then $\{x\lambda_1 + y\lambda_i : x, y \in \mathbb{N}_0\} = d\langle \frac{\lambda_1}{d}, \frac{\lambda_i}{d} \rangle$, where by $d\langle \frac{\lambda_1}{d}, \frac{\lambda_i}{d} \rangle$ we mean the set $\{d\lambda : \lambda \in \langle \frac{\lambda_1}{d}, \frac{\lambda_i}{d} \rangle\}$. Obviously, $d\langle \frac{\lambda_1}{d}, \frac{\lambda_i}{d} \rangle \subseteq \Lambda$.

Lemma 2.4.2. *Let* $\gcd(\lambda_1, \lambda_i) = d$. *Then* $q(\lambda_i - \lambda_1) \in d\langle \frac{\lambda_1}{d}, \frac{\lambda_i}{d} \rangle$ *if and only if* $qd \leqslant \lfloor \frac{qd}{\lambda_1} \rfloor \lambda_i$. *In particular, if* $q \leqslant \lfloor \frac{q}{\lambda_1} \rfloor \lambda_i$ *then* $q(\lambda_i - \lambda_1) \in d\langle \frac{\lambda_1}{d}, \frac{\lambda_i}{d} \rangle$.

Proof. We need to prove that $q(\frac{\lambda_i}{d} - \frac{\lambda_1}{d}) \in \langle \frac{\lambda_1}{d}, \frac{\lambda_i}{d} \rangle$ if and only if $qd \leqslant \lfloor \frac{qd}{\lambda_1} \rfloor \lambda_i$. Suppose that c is the inverse of $\frac{\lambda_i}{d}$ modulo $\frac{\lambda_1}{d}$. By Lemma 2.2.1, $q(\frac{\lambda_i}{d} - \frac{\lambda_1}{d}) \in \langle \frac{\lambda_1}{d}, \frac{\lambda_i}{d} \rangle$ if and only if $\frac{\lambda_i}{d}(q(\frac{\lambda_i}{d} - \frac{\lambda_1}{d})c \mod \frac{\lambda_1}{d}) \leqslant q(\frac{\lambda_i}{d} - \frac{\lambda_1}{d})$, that is, $\frac{\lambda_i}{d}(q \mod \frac{\lambda_1}{d}) \leqslant q(\frac{\lambda_i}{d} - \frac{\lambda_1}{d})$ which is equivalent to $qd \leqslant \lfloor \frac{qd}{\lambda_1} \rfloor \lambda_i$.

Now, if $q \leqslant \lfloor \frac{q}{\lambda_1} \rfloor \lambda_i$, then $qd \leqslant \lfloor \frac{q}{\lambda_1} \rfloor d\lambda_i \leqslant \lfloor \frac{qd}{\lambda_1} \rfloor \lambda_i$ and the last statement follows. □

Lemma 2.4.3. *Suppose* $\lambda_1 < \lambda_2 < \cdots < \lambda_n$ *and let* $\Lambda = \langle \lambda_1, \lambda_2, \ldots, \lambda_n \rangle$. *If* $q \leqslant \lfloor \frac{q}{\lambda_1} \rfloor \lambda_2$ *then* $GM_q(\Lambda) = L_q(\Lambda)$.

Proof. By hypothesis, $q \leqslant \lfloor \frac{q}{\lambda_1} \rfloor \lambda_i$ for all $i > 1$. By Lemma 2.4.2, $q(\lambda_i - \lambda_1) \in \Lambda$ for all $i > 1$ and by Lemma 2.4.1, $GM_q(\Lambda) = L_q(\Lambda)$. □

Remark 2.4.4. *As mentioned, the converse is true when restricted to semigroups with two generators. Otherwise the converse is not true in general. For instance, consider* $\Lambda = \langle 5, 7, 18 \rangle$ *with* $q = 9$. *We have* $\Lambda = \{0, 5, 7, 10, 12, 14, 15, 17, 18, \ldots\}$ *and* $\Lambda \setminus \cup_{\lambda_i}$ *generator of* $_\Lambda(q\lambda_i+\Lambda) = \{0, 5, 7, 10, 12, 14, 15, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 46, 47, 48, 49, 51, 53, 54, 56, 58, 61\} = \Lambda \setminus (q\lambda_1 + \Lambda)$. *So* $GM_q(\langle 5, 7, 18 \rangle) = L_q(\langle 5, 7, 18 \rangle) = 46$. *However,* $q(= 9) > \lfloor \frac{q}{\lambda_1} \rfloor \lambda_2 (= 7)$. *The reason is that although* $q(\lambda_2 - \lambda_1) \notin \langle \lambda_1, \lambda_2 \rangle$, *it holds that* $q(\lambda_2 - \lambda_1) \in \langle \lambda_1, \lambda_2, \lambda_3 \rangle = \Lambda$.

In Table 2.1, together with the portion of semigroups for which the Lewittes and the Geil-Matsumoto bounds coincide, we give the portion of semigroups satisfying the hypothesis in Lemma 2.4.3. From that table it is easy to check again that in general the converse of Lemma 2.4.3 is not true.

2.5 Simplifying the computation

Next we investigate in which cases the computation of $\Lambda \setminus \cup_{\lambda_i}$ generator of $_\Lambda(q\lambda_i + \Lambda)$ can be simplified to the computation of $\Lambda \setminus \cup_{i \in I}(q\lambda_i + \Lambda)$ for some index set I smaller than

	Lewittes = Geil-Matsumoto					$q \leqslant \lfloor \frac{q}{\lambda_1} \rfloor \lambda_2$				
Genus	q=2	q=3	q=9	q=16	q=256	q=2	q=3	q=9	q=16	q=256
2	50.00%	100%	100%	100%	100%	50.00%	100%	100%	100%	100%
3	25.00%	75.00%	100%	100%	100%	25.00%	75.00%	100%	100%	100%
4	42.86%	57.14%	100%	100%	100%	14.29%	42.86%	85.71%	100%	100%
5	33.33%	41.67%	91.67%	100%	100%	8.33%	25.00%	58.33%	91.67%	100%
6	21.74%	43.48%	86.96%	100%	100%	4.35%	17.39%	43.48%	82.61%	100%
7	17.95%	41.03%	87.18%	100%	100%	2.56%	10.26%	38.46%	84.62%	100%
8	14.93%	37.31%	85.07%	100%	100%	1.49%	5.97%	53.73%	91.04%	100%
9	11.02%	33.05%	88.14%	98.31%	100%	0.85%	4.24%	72.03%	87.29%	100%
10	8.82%	29.90%	88.24%	95.59%	100%	0.49%	2.45%	79.90%	78.92%	100%
11	7.58%	25.95%	84.55%	92.71%	100%	0.29%	1.46%	78.13%	65.89%	100%
12	6.59%	23.48%	78.89%	90.88%	100%	0.17%	1.01%	69.93%	54.05%	100%
13	5.69%	21.48%	73.73%	89.81%	100%	0.10%	0.60%	59.64%	42.76%	100%
14	5.02%	18.90%	69.76%	88.66%	100%	0.06%	0.35%	49.26%	33.73%	100%
15	4.10%	16.63%	66.26%	87.68%	100%	0.04%	0.25%	39.38%	28.35%	100%
16	3.45%	14.77%	63.23%	87.22%	100%	0.02%	0.15%	30.86%	28.67%	100%
17	2.92%	13.10%	60.66%	87.00%	100%	0.01%	0.09%	23.79%	35.23%	100%
18	2.38%	11.66%	58.74%	87.03%	100%	0.01%	0.06%	18.33%	45.70%	100%
19	1.93%	10.40%	57.06%	86.71%	100%	0.00%	0.04%	13.93%	55.89%	100%
20	1.60%	9.28%	55.71%	85.43%	100%	0.00%	0.02%	10.55%	62.47%	99.95%
21	1.31%	8.34%	54.67%	83.03%	100%	0.00%	0.01%	7.93%	64.51%	99.75%
22	1.09%	7.48%	53.95%	80.14%	100%	0.00%	0.01%	5.93%	62.93%	99.19%
23	0.90%	6.70%	53.29%	77.41%	100%	0.00%	0.01%	4.39%	59.00%	98.09%
24	0.75%	6.02%	52.46%	75.16%	100%	0.00%	0.00%	3.25%	53.67%	96.50%
25	0.63%	5.42%	51.33%	73.37%	100%	0.00%	0.00%	2.38%	47.63%	94.73%
26	0.53%	4.90%	49.94%	71.94%	100%	0.00%	0.00%	1.74%	41.35%	93.12%
27	0.45%	4.45%	48.39%	70.75%	100%	0.00%	0.00%	1.27%	35.24%	91.84%
28	0.38%	4.07%	46.81%	69.73%	100%	0.00%	0.00%	0.92%	29.58%	90.87%
29	0.32%	3.74%	45.25%	68.76%	100%	0.00%	0.00%	0.67%	24.52%	90.06%
30	0.27%	3.44%	43.76%	67.80%	100%	0.00%	0.00%	0.48%	20.12%	89.25%

Table 2.1: Portion of semigroups for which the Lewittes and the Geil-Matsumoto bounds coincide and portion of semigroups satisfying the hypothesis in Lemma 2.4.3, that is $q \leqslant \lfloor \frac{q}{\lambda_1} \rfloor \lambda_2$, where λ_1, λ_2 are the first and second smallest generators.

the number of generators of Λ. The next lemma can be proved very similarly as we proved Lemma 2.4.1.

Lemma 2.5.1. *Let $\Lambda = \langle \lambda_1, \ldots, \lambda_n \rangle$ and let I be an index set included in $\{1, \ldots, n\}$. The next statements are equivalent.*

1. $\Lambda \setminus \cup_{i=1}^{n}(q\lambda_i + \Lambda) = \Lambda \setminus \cup_{i \in I}(q\lambda_i + \Lambda)$.
2. *For all $i \notin I$ there exists $1 \leqslant j \leqslant n$, $j \in I$ such that $q(\lambda_i - \lambda_j) \in \Lambda$.*

One consequence of Lemma 2.5.1 is the next lemma.

Lemma 2.5.2. *Let $\Lambda = \langle \lambda_1, \ldots, \lambda_n \rangle$ with $\lambda_1 < \lambda_2 < \cdots < \lambda_n$ and $\lambda_1 < q$.*

1. *Let λ_j be the maximum generator strictly smaller than $\frac{q}{\lfloor \frac{q}{\lambda_1} \rfloor}$ then $\Lambda \setminus \cup_{i=1}^{n}(q\lambda_i + \Lambda) = \Lambda \setminus \cup_{i=1}^{j}(q\lambda_i + \Lambda)$.*
2. *Let λ_j be the maximum generator strictly smaller than $2\lambda_1 - 1$ then $\Lambda \setminus \cup_{i=1}^{n}(q\lambda_i + \Lambda) = \Lambda \setminus \cup_{i=1}^{j}(q\lambda_i + \Lambda)$.*

Proof. The first statement is a consequence of Lemma 2.4.2 together with Lemma 2.5.1. For the second statement suppose that $q = x\lambda_1 + y$ with x, y integers and $x \geqslant 1$. Then $\frac{q}{\lfloor \frac{q}{\lambda_1} \rfloor} = \lambda_1 + \frac{y}{x}$. The result follows from the inequalities $x \geqslant 1$ and $y \leqslant \lambda_1 - 1$. □

We will call Geil-Matsumoto generators those generators that are strictly smaller than $2\lambda_1 - 1$. What the last statement of the previous lemma says is that for computing the Geil-Matsumoto bound we only need to subtract from Λ the sets $q\mu + \Lambda$ for μ a Geil-Matsumoto generator. Since in general we need to subtract these sets for *all* generators, this constitutes an improvement in terms of computation. In Table 5.3.2, we give the mean of the number of Geil-Matsumoto generators and non-Geil-Matsumoto generators per semigroup for different genera. In Table 5.4.1, we give the portion of Geil-Matsumoto generators (and non-Geil-Matsumoto generators) with respect to the total number of generators for different genera. We observe that, although the portion of non-Geil-Matsumoto generators decreases with the genus, it remains still significant, with a portion of more than 30% for genus 25.

Lemma 2.5.2 is a first consequence of Lemma 2.5.1 and it can be used to simplify the computation of the Geil-Matsumoto bound. We leave it as a problem for future research to find other consequences of Lemma 2.5.1 to get further simplifications.

Genus	Mean of the number of GM generators per semigroup	Mean of the number of non-GM generators per semigroup
2	1.50	1.00
3	1.75	1.00
4	2.00	1.14
5	2.33	1.42
6	2.52	1.43
7	2.79	1.62
8	3.07	1.76
9	3.32	1.89
10	3.57	2.00
11	3.85	2.17
12	4.10	2.27
13	4.38	2.41
14	4.65	2.53
15	4.92	2.65
16	5.20	2.76
17	5.48	2.88
18	5.76	2.98
19	6.05	3.09
20	6.35	3.20
21	6.64	3.30
22	6.94	3.40
23	7.24	3.50
24	7.55	3.59
25	7.86	3.68
26	8.17	3.77
27	8.49	3.86
28	8.81	3.94
29	9.13	4.03
30	9.46	4.10

Table 2.2: Mean of the number of Geil-Matsumoto generators and non-Geil-Matsumoto generators per semigroup

Genus	Total number of GM generators divided by the total number of generators	Total number of non-GM generators divided by the total number of generators	Mean of the portion of non-GM generators per semigroup
2	60.00%	40.00%	41.67%
3	63.64%	36.36%	35.42%
4	63.64%	36.36%	38.57%
5	62.22%	37.78%	40.14%
6	63.74%	36.26%	37.43%
7	63.37%	36.63%	39.13%
8	63.58%	36.42%	39.03%
9	63.74%	36.26%	38.58%
10	64.03%	35.97%	38.39%
11	63.96%	36.04%	38.76%
12	64.34%	35.66%	38.26%
13	64.54%	35.46%	38.17%
14	64.75%	35.25%	37.99%
15	65.01%	34.99%	37.73%
16	65.30%	34.70%	37.45%
17	65.56%	34.44%	37.21%
18	65.88%	34.12%	36.87%
19	66.19%	33.81%	36.55%
20	66.49%	33.51%	36.25%
21	66.79%	33.21%	35.93%
22	67.11%	32.89%	35.59%
23	67.43%	32.57%	35.26%
24	67.76%	32.24%	34.91%
25	68.08%	31.92%	34.56%
26	68.41%	31.59%	34.21%
27	68.74%	31.26%	33.86%
28	69.07%	30.93%	33.50%
29	69.40%	30.60%	33.14%
30	69.74%	30.26%	32.77%

Table 2.3: Portion of Geil-Matsumoto generators

Chapter 3

New lower bounds on the generalized Hamming weights of AG codes

3.1 Introduction

The generalized Hamming weights of a linear code are, for each given dimension, the minimum size of the support of the linear subspaces of that dimension. They were first used by [79] to analyze the performance of the wire-tap channel of type II introduced in [59] and in connection to t-resilient functions. See also [49]. The connections with the wire-tap channel have been updated recently in [68], this time using network coding. The notion itself has also been generalized for network coding in [55]. The generalized Hamming weights have also been used in the context of list decoding [36, 31], for bounding the covering radius of linear codes [41], and recently for secure secret sharing based on linear codes [17, 43]. In particular, Guruswami shows that his (e, L)-list decodibility concept for erasures is equivalent with the generalized Hamming weights for linear codes.

In this contribution we deal with generalized Hamming weights of one-point AG codes from the perspective of the associated Weierstrass semigroup, that is, the set of pole orders of the rational functions having a unique pole at the defining one-point. We present one first result on the maximum integer not belonging to an ideal of a numerical semigroup (Theorem 3.2.3) and then we use it to give a lower bound on the generalized Hamming weights via the so-called Feng-Rao numbers (Theorem 3.3.1, Corollary 3.3.2).

A numerical semigroup is a subset of $\mathbb{N}_0$ that contains 0, is closed under addition, and has a finite complement in $\mathbb{N}_0$. The elements in this complement are called the gaps of the semigroup and the number of gaps is the genus. The maximum gap is usually referred to as the Frobenius number of the semigroup and the conductor is the Frobenius number plus one. By the pigeonhole principle it is easy to prove that the Frobenius number is at most twice the genus minus one, and there are semigroups, called symmetric semigroups, attaining this bound.

An ideal of a numerical semigroup is a subset of the semigroup such that any element in the subset plus any element of the semigroup add up to an element of the subset. Again the ideal will be a subset of $\mathbb{N}_0$ with finite complement in it. Our first result is an analogue of the upper bound on the Frobenius number, for the largest integer not belonging to an ideal. Indeed, we prove that it is at most the size of the complement of the ideal in the semigroup plus twice the genus minus one. This generalizes the bound on the Frobenius number since that bound can be derived from this bound by taking the ideal to be the whole semigroup. Then, we characterize the ideals of semigroups for which the maximum integer not belonging to the semigroup attains the bound.

A nice tool for tackling the generalized Hamming weights for AG codes are the generalized order bounds introduced in [37], involving Weierstrass semigroups. In [21], a constant depending only on the semigroup and the dimension of the Hamming weights was introduced, from which the order bounds could be completely determined for codes of rate low enough. This constant was called Feng-Rao number in the same reference. In the present contribution, using the upper bound on the maximum element not belonging to an ideal, we derive a lower bound on the so-called Feng-Rao numbers and consequently a new bound on

the generalized Hamming weights. The main tool is analyzing the intervals of consecutive gaps of the Weierstrass semigroup. Consecutive gaps were already used in [26] for bounding the minimum distance of codes and in [77] for bounding the generalized Hamming weights.

In the last section we study the intervals of consecutive gaps for Hermitian codes and for codes in one of the Garcia-Stichtenoth towers of codes attaining the Drinfeld-Vlăduţ bound.

3.2 The maximum integer not belonging to an ideal

From now on, Λ will denote a numerical semigroup and the elements of Λ are denoted $\{\lambda_0 = 0 < \lambda_1 < \dots\}$. The Frobenius number is F, the conductor is c, and the genus is g.

Given an ideal I of a numerical semigroup Λ, we call the size of $\Lambda \setminus I$ the *difference* of I with respect to Λ.

It was proved in [39, Lemma 5.15] and [44, Lemma 3.6] that the difference of the ideal $a+\Lambda$ with $a \in \Lambda$ is exactly a. So, for this particular class of ideals, the maximum element not belonging to the ideal is at most the difference plus twice the genus of the semigroup minus one. In Theorem 3.2.3 we will prove this result for *any* ideal of any numerical semigroup. Then we will characterize the semigroups for which the inequality is indeed an equality.

3.2.1 An upper bound for the maximum integer not belonging to an ideal

Define the set of divisors of λ_i by

$$D(i) = \{\lambda_j \leq \lambda_i : \lambda_i - \lambda_j \in \Lambda\}$$

and the sequence

$$\nu_i = \#D(i),$$

for $i \in \mathbb{N}_0$.

Some results related to this sequence and also to its applications to coding theory can be found for instance in [42, 8, 9, 50, 56, 57, 58].

Barucci proved in [3] the next result.

Theorem 3.2.1 ([3])**.** *Any ideal of a numerical semigroup is an intersection of irreducible ideals and irreducible ideals have the form $\Lambda \setminus D(i)$ for some i.*

Also, it was proved in [39, Theorem 5.24] the next result.

Lemma 3.2.2 ([39])**.** *Let $g(i)$ be the number of gaps smaller than λ_i and $G(i)$ the number of pairs of gaps adding up to λ_i. Then,*

$$\nu_i = i - g(i) + G(i) + 1$$

Now we can state the main result of this section.

Theorem 3.2.3. *The maximum integer not belonging to an ideal I of a semigroup Λ of genus g with difference d is at most $d + 2g - 1$. That is, $d + 2g + i \in I$ for all $i \geq 0$.*

Proof. If two ideals satisfy the result in the Theorem then their intersection also satisfies it and by Theorem 3.2.1 it is then enough to prove the result for irreducible ideals.

Now we want to prove the result for the ideal $I = \Lambda \setminus D(i)$. That is, $\nu_i + 2g \geq \max\{c, \lambda_i + 1\}$, where c is the conductor of Λ. If $c \geq \lambda_i + 1$ then we are done since $c \leq 2g$. Suppose then that $\lambda_i + 1 > c$. Then $g(i) = g$, $\lambda_i = i + g$, and hence by Lemma 3.2.2, $\nu_i + 2g = (i - g + G(i) + 1) + 2g = i + g + 1 + G(i) = \lambda_i + 1 + G(i) \geq \lambda_i + 1$. □

3.2.2 Ideals attaining the upper bound

We will now characterize the ideals of semigroups that attain the upper bound on the maximum integer not belonging to the ideal.

We first need some preliminary lemmas.

Lemma 3.2.4. *If $G(i) = 0$ then $\lambda_i \geq c$.*

Proof. If $G(i) = 0$ then, since $1, \ldots, \lambda_1 - 1$ are gaps, $\lambda_i - \lambda_1 + 1, \ldots, \lambda_i - 1$ are non-gaps. But also $\lambda_i \in \Lambda$ so the interval $[\lambda_i - \lambda_1 + 1, \ldots, \lambda_i]$ is included in Λ. Now, by adding multiples of λ_1 to the elements in this interval we get the whole set of integers $\lambda_i + k$ with $k \geq 0$. Then $\lambda_i \geq c$. □

Lemma 3.2.5. *$G(i) = 0$ if and only if $\{\lambda_i - F\} \cup \{\lambda_i - F + h : h \notin \Lambda, F - h \notin \Lambda\} \subseteq \Lambda$.*

Proof. Suppose $G(i) = 0$. Then obviously $\lambda_i - F \in \Lambda$. Now suppose that $h \notin \Lambda, F - h \notin \Lambda$. We need to see that $\lambda_i - F + h \in \Lambda$. But $\lambda_i - F + h = \lambda_i - (F - h) \in \Lambda$ since $G(i) = 0$ and $F - h \notin \Lambda$.

On the other hand, suppose that $\{\lambda_i - F\} \cup \{\lambda_i - F + h : h \notin \Lambda, F - h \notin \Lambda\} \subseteq \Lambda$ and we want to prove that $G(i) = 0$. If $G(i) \neq 0$ then there exists a gap h' such that $\lambda_i - h'$ is a gap. But $\lambda_i - h' = (\lambda_i - F) + (F - h')$. Since $\lambda_i - F \in \Lambda$ by hypothesis, $F - h'$ must be a gap. Let us call this gap $h = F - h'$. Then both h and $F - h = h'$ are gaps and, by the hypothesis, $\lambda_i - F + h \in \Lambda$. But $\lambda_i - F + h = \lambda_i - h'$ is a gap, a contradiction. Then $G(i) = 0$. □

Lemma 3.2.6. *If $G(i) = 0$ then $\Lambda \setminus D(i) = \{\lambda_i - h : h \in \mathbb{Z} \setminus \Lambda\}$.*

Proof. By Lemma 3.2.4, we know that $\lambda_i \geq c$.

To see the inclusion $\supseteq$ suppose that $h \in \mathbb{Z} \setminus \Lambda$. If $h < 0$ then $\lambda_i - h > \lambda_i$ and thus $\lambda_i \in \Lambda \setminus D(i)$. If $h > 0$ then $h < c$ and, since $\lambda_i \geq c$, $\lambda_i - h \geq 0$. Then $\lambda_i - h \in \Lambda$ because $G(i) = 0$. Finally $\lambda_i - h \notin D(i)$ by definition of $D(i)$.

For the reverse inclusion, suppose that $\lambda \in \Lambda \setminus D(i)$. If $\lambda > \lambda_i$ then $\lambda = \lambda_i - h$ with $h < 0$ and so $h \in \mathbb{Z} \setminus \Lambda$. If $\lambda < \lambda_i$ then $\lambda_i - \lambda$ is a gap h because otherwise $\lambda \in D(i)$. So, $\lambda \in \{\lambda_i - h : h \in \mathbb{Z} \setminus \Lambda\}$. □

Theorem 3.2.7. *Suppose that Λ is a numerical semigroup of genus g. Let I be an ideal of Λ with difference $d > 0$. Then the next statements are equivalent:*

1. *The maximum integer not belonging to I is exactly $d + 2g - 1$.*

2. $I = \Lambda \setminus D(i)$ *for some* i *with* $G(i) = 0$.

3. $I = \{\lambda_i - h : h \in \mathbb{Z} \setminus \Lambda\}$ *for some* i *with* $G(i) = 0$.

4. $\{a + h : h \notin \Lambda, F - h \notin \Lambda\} \subseteq \Lambda$ *and* $I = (a + \Lambda) \cup \{a + h : h \notin \Lambda, F - h \notin \Lambda\}$ *for some* $a \in \Lambda$, $a > 0$.

Proof. (1)$\Longleftrightarrow$(2): Suppose first that $I = \Lambda \setminus D(i)$ for some i with $G(i) = 0$. Then $d = \nu_i$. Also, by Lemma 3.2.4, $g(i) = 0$ and $\lambda_i = i + g$. Now, by Lemma 3.2.2, $d + 2g - 1 = \lambda_i \notin I$.

Conversely, suppose that the maximum integer not belonging to I is $d + 2g - 1$. If I is a proper intersection of two ideals I' and I'' with difference d' and d'' respectively, then I has difference d strictly larger than d' and strictly larger than d''. If $d + 2g - 1$ does not belong to I then it does not belong either to I' or to I'', but $d + 2g - 1$ is strictly larger than $d' + 2g - 1$ and strictly larger than $d'' + 2g - 1$, contradicting Theorem 3.2.3. So, I must be, by Theorem 3.2.1, $\Lambda \setminus D(i)$ for some i.

Since $I = \Lambda \setminus D(i)$, it holds $d = \nu_i$. If $\lambda_i < c$, then $\nu_i + 2g - 1 \geq 1 + 2g - 1 = 2g \geq c$ and so $d + 2g - 1 \in I$, which contradicts our assumption. Therefore $\lambda_i \geq c$. Then $\nu_i = i - g + G(i) + 1$ by Lemma 3.2.2. So $d + 2g - 1 = i + g + G(i) = \lambda_i + G(i)$. Since $d + 2g - 1 \notin I$, it follows that $G(i) = 0$.

(2)$\Longleftrightarrow$(3) follows immediatelly from Lemma 3.2.6.

(3)$\Longleftrightarrow$(4) follows from Lemma 3.2.5, by setting $a = \lambda_i - F$, and using the equality $\{\lambda_i - h : h \in \mathbb{Z} \setminus \Lambda\} = \{a + (F - h) : h \in \mathbb{Z} \setminus \Lambda\}$, and the fact that $\{F - h : h \in \mathbb{Z} \setminus \Lambda\} = \Lambda \cup \{h : h \notin \Lambda, F - h \notin \Lambda\}$. □

As an example, consider the semigroup

$$\Lambda = \{0, 4, 5, 8, 9, 10, 12, 13, \rightarrow\}.$$

We will list all the ideals I satisfying $d + 2g - 1 \notin I$ (d the difference of I). Since the largest i for which $G(i) > 0$ is $11 + 11 = 22 = \lambda_{16}$, all ideals $I = \Lambda \setminus D(i)$ with $i \geq 17$ attain the bound. It remains to see what indices i between 6 and 15 satisfy $G(i) = 0$.
For $i = 6$, $G(i) > 0$ since $\lambda_i = 12 = 11 + 1$.
For $i = 7$, $G(i) > 0$ since $\lambda_i = 13 = 11 + 2$.
For $i = 8$, $G(i) > 0$ since $\lambda_i = 14 = 11 + 3$.
For $i = 9$, $G(i) = 0$. Indeed, $\{15 - 1 = 14, 15 - 2 = 13, 15 - 3 = 12, 15 - 6 = 9, 15 - 7 = 8, 15 - 11 = 4\} \subseteq \Lambda$.
For $i = 10$ $G(i) = 0$. Indeed, $\{16 - 1 = 15, 16 - 2 = 14, 16 - 3 = 13, 16 - 6 = 10, 16 - 7 = 9, 16 - 11 = 5\} \subseteq \Lambda$.
For $i = 11$ $G(i) > 0$ since $\lambda_i = 17 = 11 + 6$.
For $i = 12$ $G(i) > 0$ since $\lambda_i = 18 = 11 + 7$.
For $i = 13$ $G(i) = 0$. Indeed, $\{19 - 1 = 18, 19 - 2 = 17, 19 - 3 = 16, 19 - 6 = 13, 19 - 7 = 12, 19 - 11 = 8\} \subseteq \Lambda$.
For $i = 14$ $G(i) = 0$. Indeed, $\{20 - 1 = 19, 20 - 2 = 18, 20 - 3 = 17, 20 - 6 = 14, 20 - 7 = 13, 20 - 11 = 9\} \subseteq \Lambda$.

For $i = 15$ $G(i) = 0$. Indeed, $\{21-1 = 20, 21-2 = 19, 21-3 = 18, 21-6 = 15, 21-7 = 14, 21-11 = 10\} \subseteq \Lambda$.

Hence, all ideals attaining the bound in Theorem 3.2.3 are $I_9 = \Lambda \setminus D(9) = \{4, \quad 8, 9, \quad 12$
with $D(9) = \{0, 5, 10, 15\}$, $d = 4$, $d + 2g - 1 = 15$;
$I_{10} = \Lambda \setminus D(10) = \{5, \quad 9, 10, \quad 13, 14, 15, \quad 17, 18, 19, 20, 21, 22, \dots\}$,
with $D(10) = \{0, 4, 8, 12, 16\}$, $d = 5$, $d + 2g - 1 = 16$;
$I_{13} = \Lambda \setminus D(13) = \{ \quad 8, \quad 12, 13, \quad 16, 17, 18, \quad 20, 21, 22, \dots\}$,
with $D(13) = \{0, 4, 5, 9, 10, 14, 15, 19\}$, $d = 8$, $d + 2g - 1 = 19$;
$I_{14} = \Lambda \setminus D(14) = \{ \quad 9, \quad 13, 14, \quad 17, 18, 19, \quad 21, 22, \dots\}$,
with $D(14) = \{0, 4, 5, 8, 10, 12, 15, 16, 20\}$, $d = 9$, $d + 2g - 1 = 20$;
$I_{15} = \Lambda \setminus D(15) = \{ \quad 10, \quad 14, 15, \quad 18, 19, 20, \quad 22, \dots\}$,
with $D(15) = \{0, 4, 5, 8, 9, 12, 13, 16, 17, 21\}$, $d = 10$, $d + 2g - 1 = 21$;
$I_{17} = \Lambda \setminus D(17) = \{ \quad 12, \quad 16, 17, \quad 20, 21, 22, \quad 24, \dots\}$,
with $D(17) = \{0, 4, 5, 8, 9, 10, 13, 14, 15, 18, 19, 23\}$, $d = 12$, $d + 2g - 1 = 23$;
and $\Lambda \setminus D(i)$ for all $i > 17$. In this last case, $D(i) = \{0, 4, 5, 8, 9, 10, 12, 13, \dots, i+6-12, i+6-10, i+6-9, i+6-8, i+6-5, i+6-4, i+6\}$, $d = i - 5$, $d + 2g - 1 = i + 6$.

We call the ideals of the form $a + \Lambda$ for some $a \in \Lambda$ *principal* ideals. In the next corollary we prove that for a symmetric semigroup, the ideals attaining the bound on the maximum integer not belonging to the ideal are exactly the principal ideals.

Corollary 3.2.8. *Let Λ be a symmetric numerical semigroup with Frobenius number F and genus g. Suppose that I is an ideal of Λ with difference d. Then the largest integer not belonging to I is $d + 2g - 1$ if and only if I is principal.*

Proof. It follows from Theorem 3.2.7 and the fact that for any gap h of a symmetric semigroup, $F - h \in \Lambda$. □

This can be checked again with the previous example since the semigroup Λ in there is symmetric. Notice though that the hypothesis of being symmetric is necessary. For instance, take $\Lambda = \{0, 4, 8, 9, \dots\}$ which has genus 6 and Frobenius number 7 and so it is not symmetric. Consider its ideal

$$I = \Lambda \setminus D(10) = \Lambda \setminus \{0, 4, 8, 12, 16\} = \{9, 10, 11, 13, 14, 15, 17, \dots\}$$

Its difference is $d = 5$ and the maximum element not belonging to it is $d + 2g - 1 = 16$. However, I is not

$$9 + \Lambda = \{9, 13, 17, 18, \dots\}.$$

The elements $10, 11, 14, 15$ have to be included in I in order to have $d + 2g - 1 \notin I$. Hence, I is not principal as $I = (9 + \Lambda) \cup \{10, 11, 14, 15\}$.

3.3 A lower bound on the Feng-Rao numbers

3.3.1 Feng-Rao numbers

Suppose $\Lambda = \{\lambda_0 = 0 < \lambda_1 < \dots\}$ is a numerical semigroup. In coding theory, the ν sequence of Λ defined above is very important. In particular, for an algebraic curve

with Weierstrass semigroup Λ at a rational point P, the order (or Feng-Rao) bound on the minimum distance of the one-point codes defined on P by the evaluation of rational functions having only poles at P of order at most λ_m is defined as $\delta(m) = \min\{\nu_i : i > m\}$ [22, 42, 39]. Some results on its computation can be found in [15, 39, 8, 50, 56, 57, 58].

A generalization of this bound, with applications not only in coding theory but also in some fields of cryptography, is the r-th order bound on the generalized r-th generalized Hamming weight. For this define $D(i)$ as before and

$$D(i_1, \ldots, i_r) = D(i_1) \cup \cdots \cup D(i_r).$$

Then the r-th order bound is defined as

$$\delta_r(m) = \min\{\#D(i_1, \ldots, i_r) : i_1, \ldots, i_r > m\}.$$

This definition was introduced in [37]. It is proved by Farrán and Munuera in [21] that for each numerical semigroup Λ and each integer $r \geq 2$ there exists a constant $E_r = E(\Lambda, r)$, called r-th Feng-Rao number, such that

1. $\delta_r(m) = m + 2 - g + E_r$ for all m such that $\lambda_m \geq 2c - 2$ [21, Theorem 3],
2. $\delta_r(m) \geq m + 2 - g + E_r$ for any m such that $\lambda_m \geq c$ [21, Theorem 8],

where c and g are respectively the conductor and the genus of Λ.

Furthermore, E_r satisfies

3. $r \leq E_r \leq \lambda_{r-1}$ if $g > 0$ [21, Proposition 5],
4. $E_r = \lambda_{r-1}$ if $r \geq c$ [21, Proposition 5],
5. $E_r = r - 1$ if $g = 0$.

Some further results related to the Feng-Rao number can be found in [21, 20, 18]. We will refer to the bound $E_r \geq r$ as the Farrán-Munuera bound. Here we use the main result in the previous section to obtain a bound on E_r, which is strictly better than the Farrán-Munuera bound for $r > 2$ and for semigroups with more than two intervals of gaps.

3.3.2 Bound on the Feng-Rao numbers

Theorem 3.3.1. *Suppose that n_ℓ is the number of intervals of at least ℓ gaps of Λ. Then*

$$E_r \geq \min\{r - 2 + \left\lceil \frac{r}{\ell - 1} \right\rceil, r - 1 + \left\lceil \frac{(\ell - 1)n_{\ell-1}}{\ell} \right\rceil\}. \tag{3.1}$$

In particular, if n is the number of intervals of Λ then

$$E_r \geq \min\{2(r - 1), r - 1 + \lceil n/2 \rceil\}. \tag{3.2}$$

Proof. Suppose that $2c-1-g \leq m < i_1 < \cdots < i_r$ are such that $D(i_1,\ldots,i_r) = m+2-g+E_r$. Denote $I = \{i_1,\ldots,i_r\}$. By the minimality of the set I, it necessarily holds that $i_1 = m+1$. By Theorem 3.2.3, $(m+2-g+E_r)+(2g-1) \geq \lambda_{i_r} = g+i_r$. Reorganizing the inequality gives

$$i_r \leq m+1+E_r. \tag{3.3}$$

Suppose now that there are no ℓ consecutive integers in I. Then

$$i_r \geq m+1+r-1+\left\lceil \frac{r-(\ell-1)}{\ell-1} \right\rceil. \tag{3.4}$$

Now, by (3.3), $E_r \geq r-2+\left\lceil \frac{r}{\ell-1} \right\rceil$.

Suppose on the other hand that there are at least ℓ consecutive integers in I. Let i_j be the maximum integer in I such that $i_j-\ell+1,\ldots,i_j \in I$ and so $i_{j-\ell+1} = i_j-\ell+1,\ldots,i_{j-1} = i_j-1$ and

$$\lambda_{i_{j-\ell+1}} = \lambda_{i_j}-\ell+1,\ldots,\lambda_{i_{j-1}} = \lambda_{i_j}-1.$$

Let

$$A = \{\lambda \in \Lambda : \lambda+1,\ldots,\lambda+\ell-1 \notin \Lambda\}.$$

In particular, if $\lambda \in A$ then $\lambda \leq c$, for c the conductor of Λ. Obviously $\#A = n_{\ell-1}$. If $\lambda \in A$ then

$$\begin{aligned}
(\lambda_{i_j}-1)-\lambda &\in D(i_{j-1}) \setminus D(i_j),\\
(\lambda_{i_j}-2)-\lambda &\in D(i_{j-2}) \setminus D(i_j),\\
&\vdots\\
(\lambda_{i_j}-\ell+1)-\lambda &\in D(i_{j-\ell+1}) \setminus D(i_j).
\end{aligned}$$

and so

$$\{\lambda_{i_j}-1-\lambda,\lambda_{i_j}-2-\lambda,\ldots,\lambda_{i_j}-\ell+1-\lambda\} \subseteq D(i_{j-\ell+1},\ldots,i_{j-1}) \setminus D(i_j).$$

In fact,

$$\cup_{\lambda\in A}\{\lambda_{i_j}-1-\lambda,\ldots,\lambda_{i_j}-\ell+1-\lambda\} \subseteq D(i_{j-\ell+1},\ldots,i_{j-1}) \setminus D(i_j)$$

and the sets in this union are disjoint. Indeed, for $\lambda,\lambda' \in A$, with $\lambda > \lambda'$, it holds $\lambda-\lambda' \geq \ell$. Then, $\min\{\lambda_{i_j}-1-\lambda',\ldots,\lambda_{i_j}-\ell+1-\lambda'\} = \lambda_{i_j}-\ell+1-\lambda' \geq \lambda_{i_j}+1-\lambda > \max\{\lambda_{i_j}-1-\lambda,\ldots,\lambda_{i_j}-\ell+1-\lambda\}$.

So, $\#D(i_1,\ldots,i_r) \geq \#D(i_{j-\ell+1},\ldots,i_j) \geq (\ell-1)n_{\ell-1}+\nu_{i_j} = (\ell-1)n_{\ell-1}+i_j+1-g$. Since $D(i_1,\ldots,i_r) = m+2-g+E_r$ we get that $m+2-g+E_r \geq (\ell-1)n_{\ell-1}+i_j+1-g$, so

$$E_r \geq (\ell-1)n_{\ell-1}+i_j-m-1. \tag{3.5}$$

Now, by the maximality of j,

$$i_j \geq i_1+(\ell-1)(i_1-i_r)+\ell(r-1). \tag{3.6}$$

Indeed, the subset of $\{i_1,\dots,i_r\}$ of r elements for which its maximum element k such that $k-1,\dots,k-\ell+1$ also belongs to the subset is minimum is $\{m+1,m+2,\dots,k=i_r-\ell t\}\cup\{i_r-\ell t+2,\dots,i_r-\ell(t-1)\}\cup\cdots\cup\{i_r-2\ell+2,\dots,i_r-\ell\}\cup\{i_r-\ell+2,\dots,i_r\}$ for t the number of integers in the interval $[i_1,\dots,i_r]$ not belonging to the subset, that is, $t=i_r-i_1+1-r$. So, $k=i_1+(\ell-1)(i_1-i_r)+\ell(r-1)$.

So, using (3.5) first and then (3.3),

$$\begin{aligned} E_r &\geq (\ell-1)n_{\ell-1}+i_1+(\ell-1)(i_1-i_r)+\ell(r-1)-m-1\\ &= (\ell-1)n_{\ell-1}+(\ell-1)(i_1-i_r)+\ell(r-1)\\ &\geq (\ell-1)n_{\ell-1}-(\ell-1)E_r+\ell(r-1)\end{aligned}$$

and we conclude that $E_r\geq r-1+\left\lceil\frac{(\ell-1)n_{\ell-1}}{\ell}\right\rceil$.

We have seen that depending on whether I contains consecutive integers or not either $E_r\geq r-2+\left\lceil\frac{r}{\ell-1}\right\rceil$ or $E_r\geq r-1+\left\lceil\frac{(\ell-1)n_{\ell-1}}{\ell}\right\rceil$. So, in either case, $E_r\geq\min\{r-2+\left\lceil\frac{r}{\ell-1}\right\rceil, r-1+\left\lceil\frac{(\ell-1)n_{\ell-1}}{\ell}\right\rceil\}$. □

Corollary 3.3.2. *Let m be such that $\lambda_m\geq c$ and let $\ell\geq 2$. Then*

$$\delta_r(m)\geq m+2-g+\min\{r-2+\left\lceil\frac{r}{\ell-1}\right\rceil, r-1+\left\lceil\frac{(\ell-1)n_{\ell-1}}{\ell}\right\rceil\}.$$

Remark 3.3.3. *If $r=2$ or $n\leq 2$ then bound* (3.2) *equals Farrán-Munuera's bound. But in any other case, bound* (3.2) *is better.*

Corollary 3.3.4. *If Λ is a semigroup with conductor c and n intervals of gaps then, for any m with $\lambda_m\geq c$,*

$$\delta_r(m)\geq\begin{cases} m-g+2r & \text{if } r\leq\lceil n/2\rceil+1,\\ m-g+r+\lceil n/2\rceil+1 & \text{otherwise.}\end{cases}$$

3.3.3 Sharpness of the bound

Analyzing the proof of Theorem 3.3.1 we see that the bound may be sharp only if

1. The inequality in (3.3) is indeed an equality, which means, by Theorem 3.2.7, that $D(i_1,\dots,i_r)=D(i_r)$, and so $i_1,\dots,i_{r-1}\subseteq i_r-\Lambda$. In particular, $i_r-i_{r-1}\geq\lambda_1$.
2. Either the inequality in (3.4) or the inequality in (3.6) are indeed equalities, which means that the difference between i_r and i_{r-1} is at most two. So, $i_r-i_{r-1}\leq 2$.

We conclude that the only semigroups for which the bound may be sharp are hyperelliptic semigroups, that is, semigroups that contain 2.

It is proved in [20, Theorem 1] that for hyperelliptic semigroups, $E_r=\lambda_{r-1}=2(r-1)$. The bound in Theorem 3.3.1 for the hyperelliptic semigroup of genus g is

$$E_r\geq\begin{cases} r-1 & \text{if } \ell>2\\ 2(r-1) & \text{if } \ell=2 \text{ and } r-1\leq\lceil g/2\rceil\\ r-1+\lceil g/2\rceil & \text{if } \ell=2 \text{ and } r-1>\lceil g/2\rceil\end{cases}$$

Hence the bound is sharp if and only if Λ is hyperelliptic, $\ell = 2$, and $r \leq 1 + \lceil g/2 \rceil$.

3.3.4 An example

As an example consider the semigroup

$$\{0, \ell, 2\ell, 3\ell, \dots, (\ell-1)\ell, \ell^2, \ell^2+1, \ell^2+2, \dots\},$$

with $\ell \geq 6$. Let us analyze the bounds in (3.1), (3.2) for different values of r. In this case $n_{\ell-1} = n_1 = \ell$ and so the bound in (3.1) is

$$\min\{r - 2 + \left\lceil \frac{r}{\ell-1} \right\rceil, r + \ell - 2\}$$

while the bound in (3.2) is

$$\min\{2(r-1), r - 1 + \lceil \ell/2 \rceil\}.$$

Case $r = (\ell-1)^2$

Bound (3.1) is

$$\begin{aligned} & \min\{r - 2 + \left\lceil \frac{r}{\ell-1} \right\rceil, r + \ell - 2\} \\ = \ & \min\{(\ell-1)^2 + \ell - 3, (\ell-1)^2 + \ell - 2\} \\ = \ & (\ell-1)^2 + \ell - 3 \end{aligned}$$

while bound (3.2) is

$$\begin{aligned} & \min\{2(r-1), r - 1 + \lceil \ell/2 \rceil\} \\ = \ & \min\{2(\ell-1)^2 - 2, (\ell-1)^2 - 1 + \lceil \ell/2 \rceil\} \\ = \ & (\ell-1)^2 + \lceil \ell/2 \rceil - 1 \end{aligned}$$

So, bound (3.1) (with the first element being the minimum) is better than bound (3.2).

Case $r = \ell^2 - \lceil \ell/2 \rceil$

Bound (3.1) is

$$\begin{aligned} & \min\{r - 2 + \left\lceil \frac{r}{\ell-1} \right\rceil, r + \ell - 2\} \\ = \ & \min\{\ell^2 - \lceil \ell/2 \rceil - 2 + \left\lceil \frac{(\ell-1)\ell + \lfloor \ell/2 \rfloor}{\ell-1} \right\rceil, \ell^2 - \lceil \ell/2 \rceil + \ell - 2\} \\ = \ & \min\{\ell^2 + \lfloor \ell/2 \rfloor - 1, \ell^2 + \lfloor \ell/2 \rfloor - 2\} \\ = \ & \ell^2 + \lfloor \ell/2 \rfloor - 2 \end{aligned}$$

while bound (3.2) is

$$\begin{aligned} & \min\{2(r-1), r-1+\lceil \ell/2 \rceil\} \\ = \; & \min\{2\ell^2 - 2\lceil \ell/2 \rceil - 2, \ell^2 - 1\} \\ = \; & \ell^2 - 1 \end{aligned}$$

So, bound (3.1) (with the second element being the minimum) is better than bound (3.2).

Case $r = \lfloor \ell/2 \rfloor$

Bound (3.1) is

$$\begin{aligned} & \min\{r - 2 + \left\lceil \frac{r}{\ell - 1} \right\rceil, r + \ell - 2\} \\ = \; & \min\{\lfloor \ell/2 \rfloor - 1, \lfloor \ell/2 \rfloor + \ell - 2\} \\ = \; & \lfloor \ell/2 \rfloor - 1 \end{aligned}$$

while bound (3.2) is

$$\begin{aligned} & \min\{2(r-1), r-1+\lceil \ell/2 \rceil\} \\ = \; & \min\{2\lfloor \ell/2 \rfloor - 2, \lfloor \ell/2 \rfloor + \lceil \ell/2 \rceil - 1\} \\ = \; & \min\{2\lfloor \ell/2 \rfloor - 2, \ell - 1\} \\ = \; & 2\lfloor \ell/2 \rfloor - 2 \end{aligned}$$

So, bound (3.2) (with the first element being the minimum) is better than bound (3.1).

Case $r = \lceil \ell/2 \rceil + 2$

Bound (3.1) is

$$\begin{aligned} & \min\{r - 2 + \left\lceil \frac{r}{\ell - 1} \right\rceil, r + \ell - 2\} \\ = \; & \min\{\lceil \ell/2 \rceil + 1, \lceil \ell/2 \rceil + \ell\} \\ = \; & \lceil \ell/2 \rceil + 1 \end{aligned}$$

while bound (3.2) is

$$\begin{aligned} & \min\{2(r-1), r-1+\lceil \ell/2 \rceil\} \\ = \; & \min\{2\lceil \ell/2 \rceil + 2, 2\lceil \ell/2 \rceil + 1\} \\ = \; & 2\lceil \ell/2 \rceil + 1 \end{aligned}$$

So, bound (3.2) (with the second element being the minimum) is better than bound (3.1).

3.4 Intervals of gaps in Hermitian codes and codes on a Garcia-Stichtenoth tower of codes

Now we analyze n_ℓ for two classical families of codes, that is, for Hermitian codes and for codes in one of the Garcia-Stichtenoth's towers of codes attaining the Drinfeld-Vlăduţ bound.

3.4.1 Hermitian codes

Let q be a prime power. The Hermitian curve over $\mathbb{F}_{q^2}$ is defined by the affine equation

$$x^{q+1} = y^q + y$$

and it has a single rational point at infinity and q^3 more rational points. Its weight hierarchy has already been studied in [80, 2]. However, for its simplicity, we wanted to give a description of n_ℓ. The Weierstrass semigroup at the rational point at infinity is generated by q and $q+1$ [74, 39]. Hence, it is $\{0\} \cup \{q, q+1\} \cup \{2q, 2q+1, 2q+2\} \cup \cdots \cup \{(q-2)q, (q-2)q+1, \ldots, (q-2)q+(q-2) = (q-1)q-2\} \cup \{j \in \mathbb{N}_0 : j \geq (q-1)q\}$. It is easy then to see that the lengths of the intervals of gaps, as they appear in the semigroup, are $q-1, q-2, \ldots, 1$. So,

$$n_\ell = \begin{cases} q-\ell & \text{if } 1 \leq \ell \leq q \\ 0 & \text{if } \ell \geq q \end{cases}$$

3.4.2 Codes on the Garcia-Stichtenoth tower of codes

Garcia and Stichtenoth gave in [27] a celebrated tower of function fields attaining the Drinfeld-Vlăduţ bound, which became of great importance in the area of algebraic coding theory. Since then other towers have also been found, although we will focus on the tower in [27]. It is defined over the finite field with q^2 elements $\mathbb{F}_{q^2}$ for q a prime power. It is given by $\mathcal{F}^{(1)} = \mathbb{F}_{q^2}(x_1)$; $\mathcal{F}^{(m)} = \mathcal{F}^{(m-1)}(x_m)$, with x_m satisfying

$$x_m^q + x_m = \frac{x_{m-1}^q}{x_{m-1}^{q-1}+1}.$$

It is shown in [27] that the number of its rational points is $N_q(\mathcal{F}^{(m)}) \geq (q^2-q)q^{m-1}$ and that the genus g_m of $\mathcal{F}^{(m)}$ is $g_m = (q^{\lfloor \frac{m+1}{2} \rfloor} - 1)(q^{\lceil \frac{m-1}{2} \rceil} - 1)$. Hence, the ratio between the genus $g(\mathcal{F}^{(m)})$ and $N_{q^2}(\mathcal{F}^{(m)})$ converges to $1/(q-1)$, the Drinfeld-Vlăduţ bound, as m increases. From these curves one can construct asymptotically good sequences of codes.

For every function field $\mathcal{F}^{(m)}$ in the tower we distinguish the rational point $Q^{(m)}$ that is the unique pole of x_1. The Weierstrass semigroup $\Lambda^{(m)}$ at $Q^{(m)}$ in $\mathcal{F}^{(m)}$ was recursively described in [61]. Indeed, the semigroups are given recursively by

$$\begin{aligned} \Lambda^{(1)} &= \mathbb{N}_0 \\ \Lambda^{(m)} &= q \cdot \Lambda_{m-1} \cup \{i \in \mathbb{N}_0 : i \geq q^m - q^{\lfloor \frac{m+1}{2} \rfloor}\}. \end{aligned} \tag{3.7}$$

In [12] a non-recursive description of these semigroups is given as follows.

$$\Lambda^{(m)} = \bigsqcup_{i=1}^{\lfloor \frac{m}{2} \rfloor} q^{m-2i+1} A_i \sqcup \{j \in \mathbb{N}_0 : j \geq c_m\}, \tag{3.8}$$

where c_m is the conductor of $\Lambda^{(m)}$, which is $q^m - q^{\lfloor \frac{m+1}{2} \rfloor}$, and $A_i = \{c_{2i-1} + j : j = 0, \ldots, q^{i-1}(q-1) - 1\}$.

From (3.8) we can deduce that there are exactly $\#A_i = q^{i-1}(q-1)$ intervals of length $q^{m-2i+1} - 1$. Now, if j is minimum such that $\ell \leq q^{m-2j+1} - 1$ then $n_\ell = \sum_{i=1}^{j} q^{i-1}(q-1) = q^j - 1$.

But $\ell \leq q^{m-2j+1} - 1$ is equivalent to $q^{2j} \leq \frac{q^{m+1}}{\ell+1}$ and to $q^j \leq \frac{q^{(m+1)/2}}{\sqrt{\ell+1}}$. Then $j \leq \log_q \left(\frac{q^{(m+1)/2}}{\sqrt{\ell+1}} \right)$ and we can take

$$j = \left\lfloor \log_q \left(\frac{q^{(m+1)/2}}{\sqrt{\ell+1}} \right) \right\rfloor = \left\lfloor \frac{m+1}{2} - \log_q(\sqrt{\ell+1}) \right\rfloor.$$

So, $n_\ell = q^{\left\lfloor \frac{m+1}{2} - \log_q(\sqrt{\ell+1}) \right\rfloor} - 1$.

Chapter 4

Non-homogeneous patterns on numerical semigroups

4.1 Introduction

A numerical semigroup Λ is a subset of the nonnegative integers $\mathbb{N}_0$ that contains 0 and is closed under addition, and such that $\mathbb{N}_0 \setminus \Lambda$ is finite. The number $\#(\mathbb{N}_0 \setminus \Lambda)$ is denoted the *genus* of the semigroup and the first nonzero nongap of Λ is called its *multiplicity*. The largest integer not in Λ is denoted $\mathrm{F}(\Lambda)$, and it is called the *Frobenius number* of Λ.

Arf semigroups appear in many theoretical problems in algebraic geometry as well as in some applied areas such as coding theory [4, 66, 16, 11, 7, 8]. Arf semigroups are those semigroups such that for any elements x_1, x_2, x_3 in the semigroup with $x_1 \geq x_2 \geq x_3$, the integer $x_1 + x_2 - x_3$ also belongs to the semigroup.

This definition inspired studying the so-called patterns on numerical semigroups [10]. Patterns on numerical semigroups are multivariate polynomials such that evaluated at any decreasing sequence of elements of the semigroup give integers belonging to the semigroup.

For their simplicity, and for their inspiration in Arf semigroups, patterns were first defined to be linear and homogeneous. However, Arf semigroups are of maximal embedding dimension, and this larger class of numerical semigroups fulfills a non-homogeneous pattern. Lately, other families of numerical semigroups that satisfy a non-homogeneous pattern have appeared in very different areas of applied mathematics. This suggests the need for studying non-homogeneous patterns on numerical semigroups.

In this contribution we give some results on non-homogeneous linear patterns. We start by presenting some motivating examples. Then we focus on the problem of characterizing patterns that are admissible, that is, there is at least a nontrivial numerical semigroup admitting them. Next, we particularize this study to the case the independent term of the pattern is a multiple of the multiplicity. Moreover, if we fix the multiplicity, the set of numerical semigroups admitting a strong admissible pattern is closed under intersections and the adjoin of the Frobenius number. This motivates the definition of m-varieties and the concept of minimal generating system associated to an m-variety, which allow us to represent the elements in an m-variety in a tree rooted in $\{0\} \cup (m + \mathbb{N}_0)$. Finally, for a given multiplicity we characterize those strongly admissible patterns yielding a finite tree.

4.2 Motivating examples

We will present three different scenarios where non-homogeneous patterns arise. The first one is related to commutative algebra, the second one is on algebraic geometry, and the third one is related to finite geometry.

4.2.1 Semigroups with maximal embedding dimension

Minimal generators of a numerical semigroup are those elements that can not be obtained as the sum of any other two nonzero elements of the semigroup. Equivalently, $x \in \Lambda$ is a minimal generator of the semigroup Λ if and only if $\Lambda \setminus \{x\}$ is still a numerical semigroup.

The number of minimal generators (usually referred to as the *embedding dimension*) is bounded by the multiplicity. Those numerical semigroups for which the number of minimal generators equals the multiplicity are said to be of *maximal embedding dimension* (MED). These semigroups also have other "maximal" properties as explained in [4] and [64, Chapter 2].

Maximal embedding dimension numerical semigroups are characterized by the fact that for any two nonzero elements x, y of the semigroup, one has that $x + y - m$ belongs to the semigroup where m is its multiplicity.

This example, for a fixed m (multiplicity) is related to the non-homogeneous pattern $x_1 + x_2 - m$. From this, it easily follows that every Arf numerical semigroup has maximal embedding dimension.

4.2.2 The Geil-Matsumoto bound

An important problem of algebraic coding theory is upper bounding the maximum number of places of degree one of function fields. The well known Hasse-Weil bound as well as Serre's improvement ($q+1+g\lfloor 2\sqrt{q}\rfloor$) use only the genus g of the function field and the field size q. Geil and Matsumoto give in [30] a bound in terms of the field size and the Weierstrass semigroup Λ of a rational place (that is, the set of pole orders of rational functions having only poles in that place). It is $\#(\Lambda \setminus \cup_{\lambda\in\Lambda\setminus\{0\}}(q\lambda_i+\Lambda))+1$. It is a neat formula although it is not closed and it may be computationally hard to calculate. Lewittes' bound [46] preceded the Geil-Matsumoto bound and it only considers, apart from the field size, the multiplicity m of the numerical semigroup. It is $1 + qm$. It can be derived from the Geil-Matsumoto bound and so it is weaker. The obvious advantadge of Lewittes' bound with respect to the Geil-Matsumoto bound is that Lewittes' bound is very simple to compute. Furthermore, the results by Beelen and Ruano in [6] allow bounding the number of rational places with nonzero coordinates by $\#(\Lambda \setminus \cup_{\lambda\in\Lambda\setminus\{0\}}((q-1)\lambda_i + \Lambda)) + 1$.

It is proved in [14] that the Geil-Matsumoto bound and the Lewittes' bound coincide if and only if $qx - qm \in \Lambda$ for all $x \in \Lambda \setminus \{0\}$, where m is the multiplicity of Λ. Similarly, it can be proved that Beelen-Ruano's bound on the number of rational places with nonzero coordinates equals $1 + (q-1)m$ if and only if $(q-1)x - (q-1)m \in \Lambda$ for all $x \in \Lambda \setminus \{0\}$.

These examples, for a fixed q (field size) and a fixed m (multiplicity), are related respectively to the non-homogeneous patterns $qx_1 - qm$ and $(q-1)x_1 - (q-1)m$.

Remark 4.2.1. *Let k be a positive integer, and let Λ be a numerical semigroup with multiplicity m. Let x and y be two integers such that $kx - km, ky - km \in \Lambda$. Then $k(x + y) - km = (kx - km) + (ky - km) + km \in \Lambda$. Consequently the following conditions are equivalent:*

(a) for every $x \in \Lambda \setminus \{0\}$, $kx - km \in \Lambda$,

(b) for every minimal generator x of Λ, $kx - km \in \Lambda$.

Set

$$\frac{\Lambda}{k} = \{x \in \mathbb{Z} \mid kx \in \Lambda\},$$

which is also a numerical semigroup (see [64, Chapter 5]). Then $kx-km \in \Lambda$ if and only if $x-m \in \Lambda/k$, or equivalently, $x \in m+\Lambda/k$. Hence the above conditions are also equivalent to

(c) $\Lambda \setminus \{0\} \subseteq m+\Lambda/k$.

In particular, if $k \in \Lambda \setminus \{0\}$, then $\Lambda/k = \mathbb{N}_0$. Trivially $\Lambda \setminus \{0\} \subseteq m+\mathbb{N}_0$.

4.2.3 Combinatorial configurations

A (v,b,r,k)-combinatorial configuration is an incidence structure with a set of v points and a set of b lines such that each line contains k points, each point is contained in r lines, and any two distinct lines are incident with at most one point or, equivalently, any two distinct points coincide in at most one line. It is easy to prove that if a (v,b,r,k)-configuration exists, then necessarily $vr = bk$ and so, there exists an integer d such that $(v,b,r,k) = (d\frac{k}{\gcd(r,k)}, d\frac{r}{\gcd(r,k)}, r, k)$. For a fixed pair r,k, the set $D_{r,k}$ of all integers d such that there exists a $(d\frac{k}{\gcd(r,k)}, d\frac{r}{\gcd(r,k)}, r, k)$-configuration is a numerical semigroup [13]. It is proved in [76] that $D_{r,k}$ satisfies the non-homogeneous pattern $x_1 + x_2 - n$ for any $n \in \{1, \ldots, \gcd(r,k)\}$. See other related results in [35].

4.3 Non-homogeneous patterns

Here by a *pattern* we will mean a linear polynomial with nonzero integer coefficients in $x_1, \ldots, x_n$ and eventually a nonzero integer constant term. We will say that n is the length of the pattern. Homogeneous patterns were first introduced and studied in [10]. In that paper a semigroup was said to *admit* a pattern $p(x_1, \ldots, x_n)$ if for every n elements $s_1, \ldots, s_n$ in Λ with $s_1 \geq s_2 \geq \cdots \geq s_n$ the integer $p(s_1, \ldots, s_n)$ belonged to Λ. For a non-homogeneous pattern with an integer nonzero constant term, it seems reasonable that the condition for a semigroup to admit it considers only nonzero elements of the semigroup. That is, we will say that a numerical semigroup admits a non-homogeneous pattern $p(x_1, \ldots, x_n)$ if for every n *nonzero* elements $s_1, \ldots, s_n$ in Λ with $s_1 \geq s_2 \geq \cdots \geq s_n$ the integer $p(s_1, \ldots, s_n)$ belongs to Λ.

We denote by $\mathcal{S}(p)$ the set of all numerical semigroups admitting p.

For the case of homogeneous patterns it was proved in [10] that the following conditions are equivalent for a pattern $p = \sum_{i=1}^{n} a_i x_i$:

(a) $\mathcal{S}(p) \neq \emptyset$,

(b) $\mathbb{N}_0 \in \mathcal{S}(p)$,

(c) $\sum_{i=1}^{j} a_i \geq 0$ for all $j \leq n$.

Here we will prove an equivalent result for non-homogeneous patterns. When dealing with non-homogeneous patterns, the role that $\mathbb{N}_0$ played for homogeneous patterns will be

played by an ordinary semigroup, that is, a semigroup of the form $\{0\} \cup (m + \mathbb{N}_0)$ for some integer m. This semigroup is represented by $\{0, m, \rightarrow\}$.

For a given pattern $p = \sum_{i=1}^{n} a_i x_i + a_0$ and for all $j \leq n$, considering the partial sums

$$\sigma_j = \sum_{i=1}^{j} a_i \tag{4.1}$$

will be useful for the formulation and proof of the following technical results.

Lemma 4.3.1. *Let $p = \sum_{i=1}^{n} a_i x_i + a_0$ be a non-homogeneous pattern such that $\sigma_j < 0$ for some $j \in \{1, \ldots, n\}$. Then $\mathcal{S}(p) = \emptyset$.*

Proof. For any numerical semigroup, let m be its multiplicity and take any positive integer l in the semigroup larger than $\frac{\sum_{k=j+1}^{n} a_k m + a_0}{-\sigma_j}$. Then $\sum_{i=1}^{j} a_i l + \sum_{i=j+1}^{n} a_i m + a_0 < \sum_{i=1}^{j} a_i \frac{\sum_{k=j+1}^{n} a_k m + a_0}{-\sum_{k=1}^{j} a_k} + \sum_{i=j+1}^{n} a_i m + a_0 = 0$, and so it does not belong to the semigroup. □

Lemma 4.3.2. *Let $p = \sum_{i=1}^{n} a_i x_i + a_0$ be a non-homogeneous pattern such that $\sigma_n \leq 0$ and $a_0 < 0$. Then $\mathcal{S}(p) = \emptyset$.*

Proof. Let Λ be a numerical semigroup and m be its multiplicity. Then $p(m, \ldots, m) = \sigma_n m + a_0 < 0$, so no numerical semigroup can admit p. □

Let Λ be a numerical semigroup and let x be a nonzero element of Λ. The Apéry set of x in Λ is

$$\mathrm{Ap}(\Lambda, x) = \{s \in \Lambda \mid x - s \notin \Lambda\}.$$

This set has exactly x elements, one for each congruent class modulo x ([64, Chapter 1]).

Lemma 4.3.3. *Let $p = \sum_{i=1}^{n} a_i x_i + a_0$ be a non-homogeneous pattern such that $\sigma_n = 1$ and $a_0 < 0$. Then $\mathcal{S}(p) \subseteq \{\mathbb{N}_0\}$.*

Proof. Let Λ be a numerical semigroup admitting p and m be its multiplicity. In this setting, $p(m, \ldots, m) = m + a_0$. Hence $p(m, \ldots, m) \in \Lambda$ forces $a_0 = -m$. If $\Lambda \neq \mathbb{N}_0$, then $m \neq 1$. Take an element $x \in \mathrm{Ap}(\Lambda, m) \setminus \{0\}$ (this set is not empty since $m > 1$). Then $p(x, \ldots, x) = x - m \notin \Lambda$, and so Λ does not admit p, a contradiction. □

Lemma 4.3.4. *If the non-homogeneous pattern $p = \sum_{i=1}^{n} a_i x_i + a_0$, $a_0 \neq 0$, is admitted at least by one semigroup other than $\mathbb{N}_0$, then $\sigma_j \geq 0$, for all $j \leq n$, and either $a_0 \geq 0$ or $\sigma_n > 1$.*

Proof. Suppose first that there exists $j \leq n$ such that $\sigma_j < 0$. Lemma 4.3.1 asserts that $\mathcal{S}(p) = \emptyset$, a contradiction.

Assume now that $a_0 < 0$ and $\sigma_n \leq 1$. Then Lemmas 4.3.2 and 4.3.3 state that there is no numerical semigroup other than $\mathbb{N}_0$ admitting p. □

Let $s_1, \ldots, s_n$ be a nonincreasing sequence of nonzero elements of a semigroup Λ. Define

$$\delta_j = \begin{cases} s_j - s_{j+1} & \text{if } 1 \leq j \leq n-1, \\ s_n - m & \text{if } j = n. \end{cases} \tag{4.2}$$

Then $\delta_i \geq 0$ for all $1 \leq i \leq n$. In particular, $s_i = \sum_{j=i}^{n-1}(s_j - s_{j+1}) + (s_n - m) + m = \sum_{j=i}^{n} \delta_j + m$. Then,

$$\begin{aligned} p(s_1, \ldots, s_n) &= \sum_{i=1}^{n} a_i s_i + a_0 = \sum_{i=1}^{n} a_i \left(\sum_{j=i}^{n} \delta_j + m \right) + a_0 \\ &= \sum_{i=1}^{n} a_i \sum_{j=i}^{n} \delta_j + \sigma_n m + a_0 = \sum_{j=1}^{n} \sum_{i=1}^{j} a_i \delta_j + \sigma_n m + a_0 \\ &= \sum_{j=1}^{n} \sigma_j \delta_j + \sigma_n m + a_0. \end{aligned} \tag{4.3}$$

Lemma 4.3.5. *Suppose that the non-homogeneous pattern $p = \sum_{i=1}^{n} a_i x_i + a_0$ satisfies $\sigma_j = \sum_{i=1}^{j} a_i \geq 0$ for all $j \leq n$ and either $a_0 \geq 0$ or $\sigma_n > 1$. Let m be any positive integer satisfying*

$$\begin{cases} m \geq -\frac{a_0}{\sigma_n - 1} & \text{if } \sigma_n > 1, \\ m \geq 0 & \text{if } \sigma_n = 1 (\text{and so } a_0 \geq 0), \\ m \leq a_0 & \text{if } \sigma_n = 0. \end{cases}$$

Then the ordinary semigroup $\{0, m, \rightarrow\}$ admits p.

Proof. Suppose that $s_1, \ldots, s_n$ is a nonincreasing sequence of nonzero elements of $\{0, m, \rightarrow\}$. By (4.3) and the hypothesis that $\sigma_j \geq 0$,

$$p(s_1, \ldots, s_n) = \sum_{j=1}^{n} \sigma_j \delta_j + \sigma_n m + a_0 \geq \sigma_n m + a_0.$$

Now, if $\sigma_n = 0$, then $p(s_1, \ldots, s_n) \geq a_0$. So, in this case, if m satisfies the hypothesis $m \leq a_0$, then $p(s_1, \ldots, s_n) \in \{0, m, \rightarrow\}$. If $\sigma_n = 1$ (and so $a_0 \geq 0$), then $p(s_1, \ldots, s_n) \geq m + a_0 \geq m$, so, again, $p(s_1, \ldots, s_n) \in \{0, m, \rightarrow\}$. Otherwise if $\sigma_n > 1$,

$$\begin{aligned} p(s_1, \ldots, s_n) &\geq \sigma_n m + a_0 = (\sigma_n - 1)\, m + a_0 + m \\ &\geq (\sigma_n - 1)\, (-\frac{a_0}{\sigma_n - 1}) + a_0 + m = m. \end{aligned}$$

So, $p(s_1, \ldots, s_n) \in \{0, m, \rightarrow\}$. □

Remark 4.3.6. *Let $p = \sum_{i=1}^{n} a_i x_i + a_0$ be a non-homogeneous pattern such that $\sigma_j = \sum_{i=1}^{j} a_i \geq 0$ for all $j \leq n$, $a_0 = -1$, and $\sigma_n = 1$. Then Lemma 4.3.3 asserts that $\mathcal{S}(p) \subseteq \{\mathbb{N}_0\}$. Also from (4.3), we obtain that for every nonincreasing sequence $s_1, \ldots, s_n$ of positive integers, $p(s_1, \ldots, s_n) = \sum_{j=1}^{n} \sigma_j \delta_j + m - 1$, which is a nonnegative integer. Hence $\mathcal{S}(p) = \{\mathbb{N}_0\}$.*

From the previous lemmas we obtain the following theorem.

Theorem 4.3.7. *The next conditions are equivalent for a pattern* $p = \sum_{i=1}^{n} a_i x_i + a_0$*, with* $a_0 \neq 0$*, where* $\sigma_j = \sum_{i=1}^{j} a_i$*:*

(a) $\mathcal{S}(p) \not\subseteq \{\mathbb{N}_0\}$*,*

(b) either $a_0 \geq 0$ *or* $\sigma_n > 1$*, and* $\sigma_j \geq 0$ *for all* $j \leq n$*.*

If any of these two conditions hold, then $\{0, m, \rightarrow\} \in \mathcal{S}(p)$ *for all* m *satisfying*

$$\begin{cases} m \geq -\frac{a_0}{\sigma_n - 1} & \text{if } \sigma_n > 1, \\ m \geq 0 & \text{if } \sigma_n = 1 \text{ and so } a_0 \geq 0, \\ m \leq a_0 & \text{if } \sigma_n = 0. \end{cases} \tag{4.4}$$

The patterns satisfying the conditions in Theorem 4.3.7 are called *admissible* patterns. Given one such pattern p, the multiplicities m satisfying (4.4) are called *p-admissible* multiplicities.

4.4 Patterns involving the multiplicity

Notice that both the pattern associated to the Geil-Matsumoto bound ($qx_1 - qm$) and the pattern associated to the maximal embedding dimension semigroups ($x_1 + x_2 - m$) involve in their constant parameter the multiplicity of the semigroup. The patterns whose constant term is an integer multiple of the multiplicity can be seen as an intermediate class between homogeneous and non-homogeneous patterns.

Here we are interested in the semigroups not only admitting the pattern but also having the desired multiplicity. Let $\mathcal{S}_m(p)$ be the set of numerical semigroups with multiplicity m admitting the pattern p. The first result we would like to analyze is whether, parallelizing the previous results, $\mathcal{S}_m(p) \neq \emptyset$ is equivalent to $\{0, m, \rightarrow\} \in \mathcal{S}_m(p)$. But we can see that this is not true in general. Indeed, the pattern related to the Geil-Matsumoto bound (that is, $qx_1 - qm$) gives a counterexample. Just take $q = 2$ and $m = 3$. In this case $\{0, 3, \rightarrow\} \notin \mathcal{S}_3(2x_1 - 6)$ because evaluating the pattern $2x_1 - 6$ at $s_1 = 4$ gives $2 \notin \{0, 3, \rightarrow\}$. However, $\mathcal{S}_3(2x_1 - 6) \neq \emptyset$ because for instance the semigroup $\{0, 3, 6, \rightarrow\}$ belongs to $\mathcal{S}_3(2x_1 - 6)$. Nevertheless, we show that for some particular cases, we can find results similar to the ones in the previous sections.

Theorem 4.4.1. *Let* $p = \sum_{i=1}^{n} a_i x_i + km$ *be a non-homogeneous pattern, with* $m > 1$ *and* k *a nonzero integer. Set* $\sigma_j = \sum_{i=1}^{j} a_i$*. Assume that either* $k = -1$ *or that there exists* $j \in \{1, \ldots, n\}$ *such that* $\sigma_j = 1$*. The following conditions are equivalent:*

(a) there exists a numerical semigroup of multiplicity m *that admits* p*,*

(b) $\{0, m, \rightarrow\}$ *admits* p*,*

(c) $\begin{cases} \sigma_j \geq 0 \text{ for all } j \leq n, \\ \sigma_n + k \geq 1. \end{cases}$

Proof. (a) implies (c). Let Λ be a numerical semigroup with multiplicity m admitting p (as $m > 1$, $\Lambda \neq \mathbb{N}_0$). In light of Theorem 4.3.7, $\sigma_j \geq 0$ for all $j \leq n$. So, it remains to prove that $\sigma_n + k \geq 1$. We distinguish two cases: $k > 0$ and $k < 0$. For the first case, the assertion follows trivially since $\sigma_n \geq 0$ and $k \geq 1$.

If $k < 0$, by Condition (b) in Theorem 4.3.7, we get $\sigma_n > 1$. For $k = -1$ we have $\sigma_n + k \geq 1$, and for $k < -1$, by hypothesis, there must be $j \in \{1, \ldots, n\}$ such that $\sigma_j = 1$. Let $\overline{\sigma}_j = \sum_{i=j+1}^{n} a_i$. Assume to the contrary that $\sigma_n + k \leq 0$. Then $\sigma_j + \overline{\sigma_j} + k = -t$ for some nonnegative integer t, and $\overline{\sigma}_j + k = -t - 1 = -(t+1) < 0$. Let x be a nonzero element of $\mathrm{Ap}(\Lambda, (t+1)m)$. Set $s_1 = x, \ldots, s_j = x, s_{j+1} = m, \ldots, s_n = m$. Then $p(s_1, \ldots, s_n) = \sigma_j x + \overline{\sigma}_j m + km = x - (t+1)m \notin \Lambda$, a contradiction.

(c) implies (b). By hypothesis $\sigma_n \geq 0$. We distinguish three cases.

- If $\sigma_n > 1$, then $\sigma_n - 1 > 0$, and consequently $m \geq \frac{-km}{\sigma_n - 1}$ if and only if $\sigma_n - 1 \geq -k$, that is, $\sigma_n + k \geq 1$. By Theorem 4.3.7, $\{0, m, \to\} \in \mathcal{S}(p)$.
- If $\sigma_n = 1$, then $\sigma_n + k \geq 1$ forces $km \geq 0$. As $m \geq 0$, Theorem 4.3.7 ensures that $\{0, m, \to\}$ admits p.
- For $\sigma_n = 0$, the condition $\sigma_n + k \geq 1$, implies that $k \geq 1$. Hence $km \geq 0$, and by Theorem 4.3.7 we obtain that $\{0, m, \to\} \in \mathcal{S}(p)$, because trivially $m \leq km$.

(b) implies (a). Trivial. □

4.5 Non-homogeneous Frobenius varieties

A *Frobenius variety* is a nonempty family $\mathcal{V}$ of numerical semigroups such that

1. if $\Lambda_1, \Lambda_2 \in \mathcal{V}$, then $\Lambda_1 \cap \Lambda_2 \in \mathcal{V}$,
2. if $\Lambda \in \mathcal{V}$, $\Lambda \neq \mathbb{N}_0$, then $\Lambda \cup \{\mathrm{F}(\Lambda)\} \in \mathcal{V}$.

The families of Arf, saturated, system proportionally modular numerical semigroups, and those admitting an homogeneous admissible pattern are Frobenius varieties (see [66], [67], [19] and [10], respectively). The class of system proportionally modular numerical semigroups coincides with the set of numerical semigroups having a Toms decomposition [63], and thus every numerical semigroup in this family can be realized as the positive cone of the K_0-group of a C^*-algebra [78].

Frobenius varieties were precisely introduced by Rosales in [62] because he observed that there was a common factor in [66, 67, 19, 10]: some of the proofs were based on the fact that these families were closed under intersections and the adjoin of the Frobenius number. Also due to this fact, it was possible to define minimal generating systems with respect to any of these families that are, in general, smaller than classical minimal generating systems (which are obtained by simply considering the Frobenius variety of all numerical semigroups). As in the classical sense, a minimal generator of a numerical semigroup Λ in a Frobenius variety is an element $x \in \Lambda$ such that $\Lambda \setminus \{x\}$ is also in the Frobenius variety. This allows to arrange

the semigroups in a Frobenius variety in a tree rooted in $\mathbb{N}_0$, and consequently theoretically construct all numerical semigroups in the variety up to a given genus.

We now modify slightly the definition of Frobenius variety mainly inspired in [65]. The proofs are similar to the classical case, indeed we will follow the sequence of arguments given in [64, Sections 6.4 and 6.5].

Let m be a positive integer, and let $\mathcal{V}$ be a set of numerical semigroups with multiplicity m. We say that $\mathcal{V}$ is a *non-homogeneous Frobenius variety of multiplicity* m or *m-variety* for short if

(V1) for every $\Lambda_1, \Lambda_2 \in \mathcal{V}$, $\Lambda_1 \cap \Lambda_2$ is also in $\mathcal{V}$,

(V2) for every $\Lambda \in \mathcal{V}$, $\Lambda \neq \{0, m, \rightarrow\}$, $\Lambda \cup \mathrm{F}(\Lambda) \in \mathcal{V}$.

Observe that according to this second condition, the semigroup $\{0, m, \rightarrow\}$ is in $\mathcal{V}$. Also, in light of [65, Proposition 3 and Lemma 10], the set of maximal embedding dimension numerical semigoups with multiplicity m is an m-variety.

A submonoid M of $\mathbb{N}_0$ is a *$\mathcal{V}$-monoid* if M can be expressed as an intersection of elements of $\mathcal{V}$. For a set of integers A larger than or equal to m, the *$\mathcal{V}$-monoid generated* by A, denoted by $\mathcal{V}(A)$, is the intersection of all elements in $\mathcal{V}$ containing A. The condition $A \subseteq \{0, m, \rightarrow\}$ implies that $\mathcal{V}(A)$ is not empty, and thus it is indeed a submonoid of $\mathbb{N}_0$. For a $\mathcal{V}$-monoid M, we say that $A \subseteq M$ is a *$\mathcal{V}$-generating system*, or that A *$\mathcal{V}$-generates* M, if $\mathcal{V}(A) = M$. In addition A is a *minimal* $\mathcal{V}$-generating system if no proper subset of A $\mathcal{V}$-generates M. Notice that m is never in a minimal $\mathcal{V}$-generating system of any $\mathcal{V}$-monoid.

From now on, given a subset A of $\mathbb{N}_0$, we will use the notation

$$\langle A \rangle = \left\{ \sum_{i=1}^{n} k_i a_i : n \in \mathbb{N}_0, k_i \in \mathbb{N}_0, a_i \in A \text{ for all } i \in \{1, \ldots, n\} \right\}.$$

Remark 4.5.1. *The following facts are easy consequences of the definitions.*

1) The intersection of $\mathcal{V}$-monoids is a $\mathcal{V}$-monoid.

2) Let A and B be subsets of $\{0, m, \rightarrow\}$. If $A \subseteq B$, then $\mathcal{V}(A) \subseteq \mathcal{V}(B)$.

3) For every set A of integers larger than or equal to m, $\mathcal{V}(\langle A \rangle) = \mathcal{V}(A)$.

4) If M is a $\mathcal{V}$-monoid, then $\mathcal{V}(M) = M$.

These two last assertions imply that every $\mathcal{V}$-monoid admits a $\mathcal{V}$-generating system with finitely many elements.

From this remark, the following characterization of minimal $\mathcal{V}$-generating systems can be proved easily (its proof is the same as [64, Lemma 7.24]).

Lemma 4.5.2. *Let $A \subseteq \{0, m, \rightarrow\}$ and $M = \mathcal{V}(A)$. The set A is a minimal $\mathcal{V}$-generating system of M if and only if $a \notin \mathcal{V}(A \setminus \{a\})$ for all $a \in A$.*

Next lemma is the key result to show that minimal $\mathcal{V}$-generating systems are unique. Its proof goes as that of [64, Lemma 7.25] with a slight modification.

Lemma 4.5.3. *Let $A \subseteq \{0, m, \to\}$. If $x \in \mathcal{V}(A)$, then $x \in \mathcal{V}(\{a \in A \mid a \leq x\})$.*

Proof. Assume to the contrary that $x \notin \mathcal{V}(\{a \in A \mid a \leq x\})$. Notice that this forces $x \notin \{0, m, \to\}$ and $x \notin A$. From the definition of $\mathcal{V}(\{a \in A \mid a \leq x\})$, it follows that there exists $\Lambda \in \mathcal{V}$ containing $\{a \in A \mid a \leq x\}$ such that $x \notin \Lambda$. As $m < x \leq \mathrm{F}(\Lambda)$, by applying as many times as needed Condition V2, the set $\Lambda \cup \{0, x+1, \to\}$ is in $\mathcal{V}$. Clearly $A \subseteq \Lambda \cup \{0, x+1, \to\}$ and $x \notin \Lambda \cup \{0, x+1, \to\}$, which implies $x \notin \mathcal{V}(A)$, a contradiction. □

Theorem 4.5.4. *Let m be a positive integer and let $\mathcal{V}$ be an m-variety. Every M monoid has a unique minimal $\mathcal{V}$-system of generators with finitely many elements.*

Proof. The proof that minimal $\mathcal{V}$-generating systems are unique is the same as that of [64, Theorem 7.26], where Remark 4.5.1 plays the role of [64, Lemma 7.22], and Lemmas 4.5.2 and 4.5.3 are the analogues to [64, Lemmas 7.24 and 7.25], respectively. The finiteness condition is a consequence of the last paragraph of Remark 4.5.1. □

An element in the unique minimal $\mathcal{V}$-generating system of a $\mathcal{V}$-monoid will be called a *minimal $\mathcal{V}$-generator*. As a consequence of Theorem 4.5.4, these elements can now be characterized as in a Frobenius variety. Actually, the proof of this description is exactly the same as [64, Proposition 7.28]. Notice that, as we already mentioned above, m is not a minimal $\mathcal{V}$-generator for any monoid in an m-variety.

Corollary 4.5.5. *Let M be a $\mathcal{V}$-monoid and let $x \in M$. The set $M \setminus \{x\}$ is a $\mathcal{V}$-monoid if and only if x is a minimal $\mathcal{V}$-generator.*

From this last result we easily obtain a slight modification of [64, Corollary 7.29]. The difference strives in the fact that for Λ in a m-variety $\mathcal{V}$, $\Lambda \cup \{\mathrm{F}(\Lambda)\}$ is not in $\mathcal{V}$ for $\Lambda = \{0, m, \to\}$. As we explain next, this result is used to arrange the elements of $\mathcal{V}$ in a tree.

Corollary 4.5.6. *Let Λ be a $\mathcal{V}$-monoid. The following are equivalent.*

1) $\Lambda = \Lambda' \cup \{\mathrm{F}(\Lambda')\}$ for some $\Lambda' \in \mathcal{V}$.

2) The minimal $\mathcal{V}$-generating system of Λ contains an element larger than $\mathrm{F}(\Lambda)$.

Proof. 1) implies 2). Clearly $\Lambda' = \Lambda \setminus \{\mathrm{F}(\Lambda')\} \in \mathcal{V}$, and by Corollary 4.5.5 we deduce that $\mathrm{F}(\Lambda')$ is a minimal $\mathcal{V}$-generator of Λ. Notice that $\mathrm{F}(\Lambda) < \mathrm{F}(\Lambda')$.

2) implies 1). If x is a minimal $\mathcal{V}$-generator, then Corollary 4.5.5 ensures that $\Lambda \setminus \{x\} \in \mathcal{V}$. If in addition x is larger than $\mathrm{F}(\Lambda)$, then $\mathrm{F}(\Lambda \setminus \{x\}) = x$, and thus we can choose $\Lambda' = \Lambda \setminus \{x\}$. □

With these ingredients, for an m-variety $\mathcal{V}$, we can arrange all the elements of $\mathcal{V}$ in a tree rooted in $\{0, m, \to\}$. For a vertex $\Lambda \in \mathcal{V}$ with minimal $\mathcal{V}$-generating system A, its descendants are $\Lambda \setminus \{a\}$ for all $a \in A$ with $a \geq \mathrm{F}(\Lambda)$ ([64, Theorem 7.30]). Observe also that

from any vertex in the tree we can construct the path to $\{0, m, \rightarrow\}$ by applying as many times as required Condition V2. In [65, Figure 1] the tree of maximal embedding dimension numerical semigroups with multiplicity 4 is shown up to genus 5. In view of [65, Corollary 17] this tree has infinitely many elements.

4.6 Non-homogeneous strongly admissible patterns

We can now define non-homogeneous strongly admissible patterns in a similar way as it was done in [10]. Given an admissible pattern $p = \sum_{i=1}^{n} a_i x_i + a_0$, set

$$p' = \begin{cases} p - x_1 & \text{if } a_1 > 1, \\ p(0, x_1, x_2, \ldots, x_{n-1}) & \text{if } a_1 = 1. \end{cases}$$

Observe that since p is a pattern $a_1 \neq 0$, and as we are choosing it to be admissible, by Lemmma 4.3.1, $a_1 = \sigma_1 \geq 0$.

Define for p' the partial sums σ'_j as in (4.1). A non-homogeneous admissible pattern p is said to be *strongly* admissible if $\sigma'_j \geq 0$ for all possible j.

Note that it can be the case that p is strongly admissible although p' is not admissible. As an example we can take the pattern $x_1 + x_2 - 1$. In this case $p' = x_1 - 1$ is not admissible, but still, p is considered to be strongly admissible.

We are going to prove that the set of numerical semigroups with given multiplicity m admitting a strongly admissible pattern form an m-variety. To this end, we need to prove the following technical lemma that will also be used later.

Lemma 4.6.1. *Let p be a strongly admissible pattern of length n and let m be a p-admissible multiplicity. Then for every sequence of integers $s_1 \geq \cdots \geq s_n \geq m$, it holds that $p(s_1, \ldots, s_n) \geq s_1 \geq \cdots \geq s_n$.*

Proof. Assume that $p = \sum_{i=1}^{n} a_i x_i + a_0$. If $a_1 > 1$, then $\sigma_n - 1 = \sigma'_n \geq 0$. Hence $\sigma_n \geq 1$. Define δ_j as in (4.2). By using that $\sigma'_j \geq 0$, in view of (4.3), we get $p'(s_1, \ldots, s_n) = \sum_{j=1}^{n} \sigma'_j \delta_j + \sigma'_n m + a_0 \geq \sigma'_n m + a_0 = (\sigma_n - 1)m + a_0$. For $\sigma_n = 1$, since p is admissible, Theorem 4.3.7 says that $a_0 \geq 0$, and consequently $p'(s_1, \ldots, s_n) \geq a_0 \geq 0$. If $\sigma_n > 1$, since m is a p-admissible multiplicity, $m \geq \frac{-a_0}{\sigma_n - 1}$, which leads to $p'(s_1, \ldots, s_n) \geq 0$. In both cases, $p(s_1, \ldots, s_n) = s_1 + p'(s_1, \ldots, s_n) \geq s_1$.

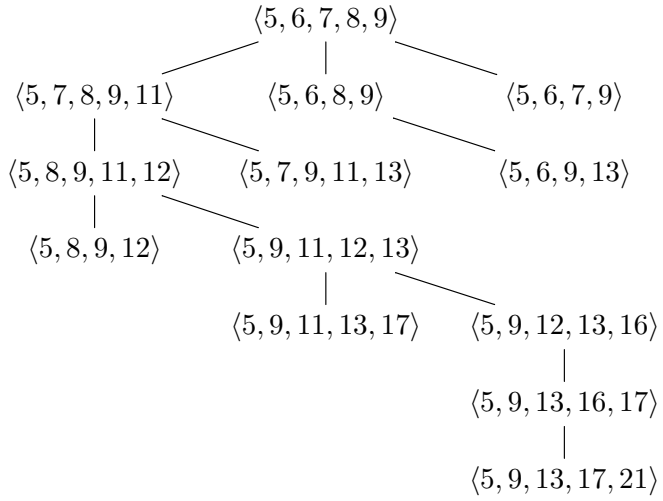
Now assume that $a_1 = 1$. In this setting, $\sigma_n - 1 = \sigma'_{n-1}$, and the proof follows as in the case $a_1 > 1$. □

Lemma 4.6.2. *Let $p = \sum_{i=1}^{n} a_i x_i + a_0$ be a strongly admissible pattern, and let m be a p-admissible multiplcicity.*

1. *If a nonordinary numerical semigroup Λ of multiplicity m admits p, then so does $\Lambda \cup \{\mathrm{F}(\Lambda)\}$.*

2. *The intersection of two numerical semigroups of multiplicity m admitting p also has multiplicity m and admits p.*

Figure 4.1: The tree of all numerical semigroups admitting the pattern $x_1 + x_2 - 1$ with multiplicity five.



Proof. The first statement follows from Lemma 4.6.1 while the second statement is immediate from the definitions. □

Theorem 4.6.3. *1. Given a strongly admissible pattern p and a p-admissible multiplicity m, the set of all semigroups with multiplicity m admitting p is an m-variety.*

2. Given a set of strongly admissible patterns $p_1, \ldots, p_r$ and a multiplicity m that is p_i-admissible for all $p_i \in \{p_1, \ldots, p_r\}$, the set of all semigroups with multiplicity m admitting simultaneously $p_1, \ldots, p_r$ is an m-variety.

Example 1. *We would like to highlight the beauty of the patterns x_1+x_2+1 and x_1+x_2-1 and their relationship with the intervals of nongaps of a numerical semigroup. Indeed, the semigroups admitting x_1+x_2+1 can be characterized by the fact that the maximum element in each interval of nongaps is a minimal generator. Similarly, the semigroups admitting $x_1 + x_2 - 1$ can be characterized by the fact that the minimum element in each interval of nongaps is a minimal generator. Figure 4.1 represents the (finite) tree of all numerical semigroups admitting the pattern $x_1 + x_2 - 1$ with multiplicity five.*

This example gives rise to a natural question. When is the tree of numerical semigroups with fixed multiplicity and admitting a strongly admissible pattern finite? The answer to this question is given in the following result.

Theorem 4.6.4. *Let $p = \sum_{i=1}^{n} a_i x_i + a_0$ be a strongly admissible pattern, and let m be a p-admissible multiplicity. Then $\mathcal{S}_m(p)$ contains infinitely many numerical semigroups if and only if $\gcd(m, a_0) \neq 1$.*

Proof. Necessity. Assume that $\gcd(m, a_0) = 1$. Then $\gcd(m, p(m, \dots, m)) = 1$, and consequently $\langle m, p(m, \dots, m)\rangle$ is a numerical semigroup. If $\Lambda \in \mathcal{S}_m(p)$, then $\langle m, p(m, \dots, m)\rangle \subseteq \Lambda$. Since there are finitely many numerical semigroups containing $\langle m, p(m, \dots, m)\rangle$, we deduce that the cardinality of $\mathcal{S}_m(p)$ is finite.

Sufficiency. Suppose now that $\gcd(m, a_0) = d \neq 1$, and let $m_0 = m/d$. Then for any $k \geq m$, the numerical semigroup $\Lambda_k = \{di : i \in \mathbb{N}_0, i \geq m_0\} \cup \{0, k, \to\}$ has multiplicity m and admits p. Indeed, let $s_1, \dots, s_n$ be a nondecreasing sequence of nonzero elements of Λ_k. By Lemma 4.6.1, $p(s_1, \dots, s_n)$ is at least s_n. If $s_n \geq k$, then obviously $p(s_1, \dots, s_n) \in \Lambda_k$. Otherwise, $s_1, \dots, s_n$ are multiples of d and so is $p(s_1, \dots, s_n)$. Now since $p(s_1, \dots, s_n)$ is a positive multiple of d larger than or equal to m, $p(s_1, \dots, s_n) \in \Lambda_k$. □

Chapter 5

On the minimum number of colluders of a pirate copy for fingerprinting with Reed-Solomon codes

5.1 Introduction

In the digital era one main concern is the illegal redistribution of digital contents. One way to fight it is by marking every single copy of the material that one does not want to have redistributed. This can be done by embedding a different imperceptible string of bits or symbols to each copy. Once an illegal copy is caught, if it was not modified, the illegal redistributor can be reidentified by the mark in his/her copy. This is called fingerprinting.

An attack to fingerprinting can be performed by a group of colluders. They can compare their copies and create a new pirate copy by erasing all the bits or symbols in which their copies differ or by using at each position where they differ, the bit or symbol that one of the users has there.

Formally, a subset of Σ^n for some alphabet Σ and positive integer n, called a code, is fixed. Then each depositary of a digital content is assigned a code word. A pirate copy is a vector $u = (u_0, \ldots, u_{n-1})$ in Σ^n, which is obtained from a set of colluders as follows. If the code words corresponding to the colluders are $c^{(1)}, \ldots, c^{(s)}$, then for all i in $\{0, \ldots, n-1\}$ one has $u_i = c_i^{(j)}$ for some j in $\{1, \ldots, s\}$, where $c_i^{(j)}$ is the ith coordinate of $c^{(j)}$. If erasures are also considered, then the pirate copy belongs to $(\Sigma \cup \{?\})^n$, and it must satisfy that for all i, either $u_i = c_i^{(j)}$ for some j or $u_i =?$. If a pirate copy contains erasures we say that it is a shortened copy.

Reed-Solomon codes are a classical family of error control codes which have been extensively used also in the context of fingerprinting.

The identifiable parent property (IPP), for which all sets of colluders capable of generating a given pirate copy share at least one colluder, is defined in [40]. It is a desirable property when we are interested in the applications to fingerprinting. It is proved in the same reference that there exist Reed-Solomon codes with this property.

Another important property for fingerprinting codes is that given a pirate copy one of the colluders can allways be identified by performing minimum distance error correction whenever the pirate copy has been created by at most a given number w of colluders. This property is denoted w-traceability or w-TA. Reed-Solomon codes are also used to find w-TA codes [73].

Further results on Reed-Solomon codes and the IPP and w-TA properties can be found in [70, 23]. Also generalized Reed-Solomon codes are used in [69] for dealing with shortened and corrupted fingerprints.

While the classical problem of fingerprinting is defining tracing algorithms for identifying at least one of the colluders that originated a given pirate copy, our aim is to elaborate on the minimum number of colluders capable of generating a given pirate copy when the code used for fingerprinting is a Reed-Solomon code.

Our main result (Theorem 5.3.2) is a lower bound on this minimum number. In the application side, having this lower bound means that once an illegal copy is caught, we can assert that at least a certain number of colluders, given by this bound, were involved in it.

This result is illustrated with several examples showing that in many cases the bound is sharp.

The tools used for proving the main result are then used to prove an upper bound on the minimum number M of colluders that can obtain any given pirate copy. This same bound can be also derived from the fact that Reed-Solomon codes are MDS. Using the main result we then see that this upper bound is sharp which means that there are certain pirate copies which can not be obtained with less than M colluders.

The bound in Theorem 5.3.2 is extenxed to shortened fingerprints obtaining an analogous bound for this case. This result can be used in turn for bounding the number of colluders that were not caught once a subset of the colluders is caught.

Finally we point out the main drawback of this bound and sketch the way to overcoming it by a closer look to the interpolated polynomial. We finish with an open question whose solution would bring out a significant improvement of our bound.

5.2 Reed-Solomon codes and interpolating polynomials

Let $\mathbb{F}_q$ be the field with q elements (q a prime power) and let α be a primitive element of $\mathbb{F}_q$. Then $\mathbb{F}_q = \{0, 1, \alpha, \alpha^2, \ldots, \alpha^{q-2}\}$. The Reed-Solomon code of length $n = q - 1$ and dimension k, denoted $RS_q(k)$, is the set

$$\{(f(1), f(\alpha), f(\alpha^2), \ldots, f(\alpha^{n-1})) : f \in \mathbb{F}_q[x], \deg(f) < k\}.$$

First we notice that for each vector $u = (u_0, \ldots, u_{n-1})$ in $\mathbb{F}_q^n$, there exists a unique polynomial f_u of degree at most $n-1$ such that $f_u(\alpha^i) = u_i$ for all i in $\{0, \ldots, n-1\}$. It can be computed, for instance, using the formula

$$f_u = \sum_{i=0}^{n-1} \left(u_i \prod_{\substack{j=0 \\ j \neq i}}^{n-1} \frac{x - \alpha^j}{\alpha^i - \alpha^j} \right).$$

The uniqueness is a consequence of the fact that if $f_u = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}$, then the coefficents $a_0, \ldots, a_{n-1}$ are a solution of the linear system of equations

$$\begin{pmatrix} 1 & 1 & 1 & 1 & \ldots & 1 \\ 1 & \alpha & \alpha^2 & \alpha^3 & \ldots & \alpha^{(n-1)} \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \ldots & \alpha^{2(n-1)} \\ 1 & \alpha^3 & \alpha^6 & \alpha^9 & \ldots & \alpha^{3(n-1)} \\ \vdots & & & & & \vdots \\ 1 & \alpha^{n-1} & \alpha^{2(n-1)} & \alpha^{3(n-1)} & \ldots & \alpha^{(n-1)(n-1)} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{pmatrix} = \begin{pmatrix} u_0 \\ u_1 \\ \vdots \\ u_{n-1} \end{pmatrix}. \qquad (5.1)$$

The matrix of this system is a Vandermonde matrix which is known to be invertible. So, any u in $\mathbb{F}_q^n$ is of the form $(f(1), f(\alpha), f(\alpha^2), \ldots, f(\alpha^{n-1}))$ for some unique $f \in \mathbb{F}_q[x]$ of degree less than n.

Given a vector $u = (u_0, \dots, u_{n-1})$ in $\mathbb{F}_q^n$, u is a code word if and only if $\deg(f_u) < k$. Now if $\deg(f_u) < k$ then u is a code word and so it can be obtained by just one single colluder. Our focus is on the case when $u \notin RS_q(k)$ and so when $\deg(f_u) \geq k$.

5.3 A lower bound

Lemma 5.3.1. *With the same notations as above, a vector $u = (u_0, \dots, u_{n-1})$ in $\mathbb{F}_q^n$, $u \notin RS_q(k)$, agrees with any code word $c \in RS_q(k)$ in at most $\deg(f_u)$ positions.*

Proof. If the vector u agrees with a code word c in the position corresponding to the ith power of α this means that $f_u(\alpha^i) = f_c(\alpha^i)$ and so $(f_u - f_c)(\alpha^i) = 0$. Now since the number of roots of a polynomial over a finite field is upper bounded by its degree, the equality $(f_u - f_c)(\alpha^i) = 0$ will be satisfied by at most $\deg(f_u - f_c)$ different powers of α. But since $u \notin RS_q(k)$, $\deg(f_u) \geq k$ and since $c \in RS_q(k)$, $\deg(f_c) < k$. So, $\deg(f_u - f_c) = \deg(f_u)$ and $u = (u_0, \dots, u_{n-1})$ agrees with c in at most $\deg(f_u)$ positions. □

Theorem 5.3.2. *With the same notations as above, the minimum number of colluders required to obtain a vector $u = (u_0, \dots, u_{n-1})$ in $\mathbb{F}_q^n$, with $u \notin RS_q(k)$ is at least $\left\lceil \frac{n}{\deg(f_u)} \right\rceil$.*

Proof. It is a consequence of Lemma 5.3.1. □

Next we will illustrate this theorem with basic examples for $\deg(f_u)$ equal to $1, 2$ and $n-1$, and then with two further examples dealing with the norm and trace polynomials. See [48] for more details on these polynomials related to finite fields. We will see that for the examples with $\deg(f_u) = 1$ and most of the examples with $\deg(f_u) = 2$, and the examples with the norm and trace polynomials the lower bound is sharp. However, the example with $\deg(f_u) = n - 1$ shows that the bound may be not sharp.

The case $\deg(f_u) = 1$ Suppose first that $\deg(f_u) = 1$. This case only makes sense when $k = 1$ and so $RS_q(k)$ is the repetition code. In this case $\lceil \frac{n}{\deg(f_u)} \rceil$ equals n. Since $\deg(f_u) = 1$ it holds that $f_u = a_0 + a_1 x$ for some $a_0, a_1 \in \mathbb{F}_q$, $a_1 \neq 0$ and so f_u represents a permutation of $\mathbb{F}_q$. The n different components of u can be covered by $n = q - 1$ out of the q constant vectors of the repetition code.

The case $\deg(f_u) = 2$ The case $\deg(f_u) = 2$ makes sense when $k = 1$ or $k = 2$. In this case $\lceil \frac{n}{\deg(f_u)} \rceil$ equals $\frac{q-1}{2}$ if q is odd and $\frac{q}{2}$ if q is even. Since $\deg(f_u) = 2$ it holds that $f_u = a_0 + a_1 x + a_2 x^2$ for some $a_0, a_1, a_2 \in \mathbb{F}_q$, $a_2 \neq 0$. Consider the set $U = \{a_0 + a_1\beta + a_2\beta^2, \beta \in \mathbb{F}_q\}$. One can check that the equation on γ given by $a_0 + a_1\beta + a_2\beta^2 = a_0 + a_1\gamma + a_2\gamma^2$ has only two possible solutions, $\gamma = \beta$ and $\gamma = -\frac{a_1}{a_2} - \beta$. The two solutions are equal only for those β's such that $\beta = -\frac{a_1}{a_2} - \beta$. If q is odd this is only possible for $\beta = -\frac{a_1}{2a_2}$ so U has exactly $\frac{q-1}{2} + 1$ elements. Conversely, if q is even then $\beta = -\frac{a_1}{a_2} - \beta$ is true for all β if $a_1 = 0$ and it is false for all β if $a_1 \neq 0$. So, in the case q even the set U has either q elements if a_1 equals 0 and $\frac{q}{2}$ if $a_1 \neq 0$. Now, the set of components of u is exactly the

set of elements in $U_0 = \{a_0 + a_1\beta + a_2\beta^2, \beta \in \mathbb{F}_q \setminus \{0\}\}$. Now, for q odd, $\#U_0 = \frac{q-1}{2}$ if $a_1 = 0$ and $\#U_0 = \frac{q-1}{2} + 1$ if $a_1 \neq 0$, while for q even, $\#U_0 = q - 1$ if $a_1 = 0$ and $\#U_0 = \frac{q}{2}$ if $a_1 \neq 0$. So, if we take the repetition code, that is, $k = 1$ then the upper bound is tight only for q odd and $a_1 = 0$ or for q even and $a_1 \neq 0$. We will see in the next section that for $k = 2$ the bound is always tight.

The case $\deg(f_u) = n - 1$ If $\deg(f_u) = n - 1$ then the upper bound on the number of colluders is $\lceil \frac{n}{n-1} \rceil = 2$. But the only information given by this bound is that one single colluder could not obtain u. And this is already known from the fact that $u \notin RS_q(k)$.

Example with the trace polynomial Suppose $q = \tilde{q}^m$ for some prime power $\tilde{q}$ and positive integer m. Then $\mathbb{F}_{\tilde{q}}$ is a subfield of $\mathbb{F}_q$. The trace polynomial of the field extension $\mathbb{F}_q/\mathbb{F}_{\tilde{q}}$, is defined as the polynomial

$$T(x) = x^{\tilde{q}^{m-1}} + x^{\tilde{q}^{m-2}} + \cdots + x^{\tilde{q}} + x.$$

The trace polynomial when evaluated at $\mathbb{F}_q$ gives elements of $\mathbb{F}_{\tilde{q}}$. The antiimage of each element in $\mathbb{F}_{\tilde{q}}$ consists of exactly $\tilde{q}^{m-1}$ elements in $\mathbb{F}_q$. All this means that if we take the pirate word $u = (u_0, \ldots, u_{n-1}) = (T(1), T(\alpha), T(\alpha^2), \ldots, T(\alpha^{n-1}))$ then u has for each β in $\mathbb{F}_{\tilde{q}} \setminus \{0\}$ exactly $\tilde{q}^{m-1}$ components equal to β plus $\tilde{q}^{m-1} - 1$ components equal to 0. In particular u can be obtained from the $\tilde{q}$ colluders consisting of the constant vectors $(\beta, \ldots, \beta)$ with $\beta \in \mathbb{F}_{\tilde{q}}$. These constant vectors are obtained by evaluating constant polynomials (with degree at most 0) in $1, \alpha, \ldots, \alpha^{n-1}$ and so they are code words of $RS_q(k)$ for any $k > 0$. So, u can be obtained by only $\tilde{q}$ colluders.

On the other hand, since $\deg(T) = \tilde{q}^{m-1} < q - 1 = n$, by the uniqueness of f_u we have that $f_u = T$ and so $\lceil \frac{n}{\deg(f_u)} \rceil = \lceil \frac{q-1}{\tilde{q}^{m-1}} \rceil = \lceil \frac{\tilde{q}^m - 1}{\tilde{q}^{m-1}} \rceil = \lceil \tilde{q} - \frac{1}{\tilde{q}^{m-1}} \rceil = \tilde{q}$. So, we can see that in this case the bound in Theorem 5.3.2 is sharp.

Example with the norm polynomial We use now the same notations as before, just with the assumption that $\tilde{q} \neq 2$. The norm polynomial of the field extension $\mathbb{F}_q/\mathbb{F}_{\tilde{q}}$, is defined as the polynomial

$$N(x) = x^{\frac{\tilde{q}^m - 1}{\tilde{q} - 1}}.$$

The norm polynomial when evaluated at $\mathbb{F}_q$ gives also elements of $\mathbb{F}_{\tilde{q}}$. The antiimage of each element β in $\mathbb{F}_{\tilde{q}}$ consists of exactly $\frac{\tilde{q}^m - 1}{\tilde{q} - 1}$ elements in $\mathbb{F}_q$ if $\beta \neq 0$ and exactly one if $\beta = 0$. All this means that if we take the pirate word $u = (u_0, \ldots, u_{n-1}) = (N(1), N(\alpha), N(\alpha^2), \ldots, N(\alpha^{n-1}))$ then u has for each β in $\mathbb{F}_{\tilde{q}} \setminus \{0\}$ exactly $\frac{\tilde{q}^m - 1}{\tilde{q} - 1}$ components equal to β. In particular u can be obtained from the $\tilde{q} - 1$ colluders consisting of the constant vectors $(\beta, \ldots, \beta)$ with $\beta \in \mathbb{F}_{\tilde{q}} \setminus \{0\}$ which, as explained before, are code words of $RS_q(k)$ for any $k > 0$. So, u can be obtained by only $\tilde{q} - 1$ colluders.

On the other hand, since $\deg(N) = \frac{\tilde{q}^m - 1}{\tilde{q} - 1} < q - 1 = n$, by the uniqueness of f_u we have that $f_u = N$ and so $\lceil \frac{n}{\deg(f_u)} \rceil = \lceil \frac{q-1}{\frac{\tilde{q}^m - 1}{\tilde{q} - 1}} \rceil = \lceil \tilde{q} - 1 \rceil = \tilde{q} - 1$. So, we can see that again in this case the bound in Theorem 5.3.2 is sharp.

5.4 An upper bound, revisited

Now we can state the upper bound $\lceil \frac{n}{k} \rceil$. It is already known and it can be proved by using the fact that Reed-Solomon codes are MDS. However, we chose to use a new proof here because it only uses the same tools used for the previous theorem, without any need for the MDS property.

Theorem 5.4.1. *A number of $\lceil \frac{n}{k} \rceil$ colluders is enough for obtaining any pirate copy $u \in \mathbb{F}_q^n$.*

Proof. Consider a set of k positions $i_1, \ldots, i_k$ in u. The polynomial

$$f = \sum_{l=1}^{k} \left(u_{i_l} \prod_{\substack{j=1 \\ j \neq i_l}}^{k} \frac{x - \alpha^{i_j}}{\alpha^{i_l} - \alpha^{i_j}} \right)$$

has degree less than k and so $(f(1), f(\alpha), f(\alpha^2), \ldots, f(\alpha^{n-1}))$ is a code word c in $RS_q(k)$. Also $c_{i_l} = f(\alpha^{i_l}) = u_{i_l}$ for all l in $\{1, \ldots, k\}$. Then c and u agree in the positions $i_1, \ldots, i_k$. The same argument holds for any selection of less then k positions.

Divide u into $\lfloor \frac{n}{k} \rfloor$ disjoint sets of k positions plus the set of the $n - \lfloor \frac{n}{k} \rfloor$ remaining positions which are less than k and which may be empty. For each of these sets we can find a code word as before, which agrees with u in the selected positions. This gives a set of $\lceil \frac{n}{k} \rceil$ code words capable of generating the pirate copy u. □

Remark 5.4.2. *From Theorem 5.3.2 we deduce that the bound on the number of colluders in Theorem 5.4.1 is attained when f_u has degree exactly equal to k. So, there are words in $\mathbb{F}_q^n$ which can not be obtained by less than $\lceil \frac{n}{k} \rceil$ colluders.*

5.5 On shortened fingerprints

In this section we make some remarks on the case when part of the fingerprint has been simply erased. Tracing of traitors based on shortened fingerprints is treated in [69]. We show that the results in the previous sections can be naturally extended to this case.

Formally, instead of considering pirate copies in $\mathbb{F}_q^n$ we consider pirate copies $u = (u_0, \ldots, u_{n-1})$ in $(\mathbb{F}_q \cup \{?\})^n$ which are obtained from a set of colluders as follows. If the code words corresponding to the colluders are $c^{(1)}, \ldots, c^{(s)}$, then for all i in $\{0, \ldots, n-1\}$ one has $u_i = c_i^{(j)}$ for some j in $\{1, \ldots, s\}$, or $u_i =?$. We call n^* the number of erased positions in u, that is, the number of components u_i which are equal to ?. Now $n - n^*$ will play the role played by n in the previous sections.

The polynomial f_u can be redefined as follows.

$$f_u = \sum_{\substack{i=0 \\ u_i \neq ?}}^{n-1} \left(u_i \prod_{\substack{j=0 \\ u_j \neq ? \\ j \neq i}}^{n-1} \frac{x-\alpha^j}{\alpha^i - \alpha^j} \right).$$

The vector $(f_u(1), f_u(\alpha), \ldots, f_u(\alpha^{n-1}))$ has the particularity that it agrees with u in all the non-erased positions and that it is the one with smallest degree with this property. Notice that now the degree of f_u is at most $n - n^* - 1$ and that f_u is, as before, the unique polynomial agreeing with u in all the non-erased positions and with degree at most $n - n^* - 1$. Uniqueness follows as before using a Vandermonde matrix. If $n^* = 0$ then the polynomial f_u is the same polynomial that we already had.

If $\deg(f_u) < k$ and in particular, if $n - n^* - 1 < k$ then $(f_u(1), f_u(\alpha), \ldots, f_u(\alpha^{n-1}))$ is a code word and so u agrees with a code word in all its non-erased positions. So, it can be obtained with just one colluder. Next we consider the case $\deg(f_u) \geq k$.

Lemma 5.3.1 and Theorem 5.3.2 can be now reformulated. The proof of the new lemma is parallel to that of Lemma 5.3.1 and hence it has been ommitted. Also, the proof of the new theorem follows from the lemma.

Lemma 5.5.1. *A vector u in $(\mathbb{F}_q \cup \{?\})^n$, $u \notin RS_q(k)$, agrees with any code word $c \in RS_q(k)$ in at most $\deg(f_u)$ positions.*

Theorem 5.5.2. *Suppose that a vector u is in $(\mathbb{F}_q \cup \{?\})^n$, and $u \notin RS_q(k)$. Then the minimum number of colluders required to obtain u is at least $\left\lceil \frac{n-n^*}{\deg(f_u)} \right\rceil$.*

We would like to end with the remark that this result can be used in turn for bounding the number of colluders that were not caught once a subset of the colluders is caught. Indeed, suppose that a set of colluders is caught that collaborated in the pirate copy u. Then erase all the positions of the pirate copy which agree with the copy of at least one of the caught colluders and obtain a new pirate copy u^*. Let n^{**} be the total number of erased positions in u^*. Then, Theorem 5.5.2 applied to u^* tells us that at least $\left\lceil \frac{n-n^{**}}{\deg(f_{u^*})} \right\rceil$ colluders are still not caught.

5.6 Drawback and overcoming it by a closer look to polynomial factorization

In Table 5.1 there is an analysis of the performance of the bound in Theorem 5.3.2. It turns out that $\lceil \frac{n}{\deg(f_u)} \rceil$ is most of the times 2 and this does not introduce any information. Indeed, having at least two colluders is equivalent to having u not a code word, which is something that is very easy to check without any need of interpolating polynomials. The

reason for having $\lceil \frac{n}{\deg(f_u)} \rceil = 2$ most of the times is that the coefficients of f_u are a solution of the linear system (5.1). Then, having $\lceil \frac{n}{\deg(f_u)} \rceil > 2$ would mean $\deg(f_u) < \frac{n}{2}$ and, if $f_u = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}$, this would mean having $a_{\lceil \frac{n}{2} \rceil} = \cdots = a_{n-1} = 0$, which happens only with a probability $\frac{q^{\lceil \frac{n}{2} \rceil - 1}}{q^n} = q^{-\lceil \frac{n}{2} \rceil - 1}$.

The limitation of this bound already comes from Lemma 5.3.1 and the fact that, in its proof, we only bound the number of roots of the polynomial $f_u - f_c$ (and so the number of agreements between the caught word u and a general code word c) by the degree of $f_u - f_c$ which is exactly the degree of f_u. But conversely, it is well known that a random polynomial from $\mathbb{F}_q[x]$ has "on the average", as q increases, exactly one root in the field $\mathbb{F}_q$ [24, 60, 45]. So, on average, our bound in Lemma 5.3.1 is very far from the real number of agreements between the caught word and a general code word.

But we have more information on the polynomial $f_u - f_c$ rather than its degree. Indeed we know all its terms of degree at least k. In some cases this knowledge may slightly modify the result in Lemma 5.3.1 and this may improve drastically the bound in Theorem 5.3.2.

In the next lemma we illustrate it with a particular example.

Lemma 5.6.1. *Suppose that $q = \tilde{q}^m$ for some prime power $\tilde{q}$ and positive integer m. Suppose that $u \in \mathbb{F}_q^n$, $u \notin RS_q(k)$ with $1 \leq k \leq \tilde{q}^{m-1}$ is such that $f_u = x^{\tilde{q}^{m-1}} + x^{\tilde{q}^{m-2}} + \cdots + x^{\tilde{q}^i} + g_k(x)$, with $\tilde{q}^{i-1} < k < \tilde{q}^i$ and $g_k(x)$ a polynomial of degree less than k. Then the word u agrees with any code word $c \in RS_q(k)$ in at most $(k-1)\tilde{q}$ positions.*

Proof. Suppose that u and c agree in the position corresponding to α^i and suppose that $T(\alpha^i) = \beta \in \mathbb{F}_{\tilde{q}}$. Then α^i is a root of the polynomial

$$h_\beta(x) = f_u(x) - f_c(x) - T(x) + \beta.$$

In general, all the powers α^i corresponding to positions where u and c agree are roots of $h_\beta(x)$ for some $\beta \in \mathbb{F}_{\tilde{q}}$, and so they are roots of

$$H(x) = \prod_{\beta \in \mathbb{F}_{\tilde{q}}} h_\beta(x).$$

By the hypothesis on f_u, $\deg(f_u - T(x)) < k$ and also $\deg(f_c) < k$ and $\deg(\beta) \leq 0 < k$. So, $\deg(h_\beta) < k$ for all $\beta \in \mathbb{F}_{\tilde{q}}$ and $\deg(H) \leq (k-1)\tilde{q}$. This proves the Lemma. □

Lemma 5.6.1 leads to a refinement of the bound in Theorem 5.3.2 for this particular case, whenever $(k-1)\tilde{q} < \deg(f_u)$. Indeed the new bound is $\lceil \frac{n}{(k-1)\tilde{q}} \rceil$.

An analogous lemma associated to the norm polynomial is next. The proof is left to the reader since it is very similar to the previous one. The only difference is on the fact that the norm polynomial evaluated at powers of α runs $\mathbb{F}_{\tilde{q}} \setminus \{0\}$ while the trace polynomial runs all $\mathbb{F}_{\tilde{q}}$.

Lemma 5.6.2. *Suppose that $q = \tilde{q}^m$ for some prime power $\tilde{q}$ and positive integer m. Suppose that $u \in \mathbb{F}_q^n$, $u \notin RS_q(k)$ with $1 \leq k \leq \frac{\tilde{q}^m - 1}{\tilde{q} - 1}$ is such that $f_u = x^{\frac{\tilde{q}^m - 1}{\tilde{q} - 1}} + g_k(x)$, with $g_k(x)$ a polynomial of degree less than k. Then the word u agrees with any code word $c \in RS_q(k)$ in at most $(k-1)(\tilde{q}-1)$ positions.*

$k = 3$	coalition size	trials	mean value m of $\deg(f_u)$	$\lceil \frac{n}{m} \rceil$
	2	100	24.95	2
	3	100	24.99	2
	4	100	24.95	2
	5	100	24.95	2
	6	100	24.95	2
	7	100	25.00	2
	8	100	24.98	2
	9	100	24.94	2
$k = 4$	coalition size	trials	mean value m of $\deg(f_u)$	$\lceil \frac{n}{m} \rceil$
	2	100	24.96	2
	3	100	24.96	2
	4	100	24.98	2
	5	100	24.97	2
	6	100	24.96	2
	7	100	24.96	2
$k = 5$	coalition size	trials	mean value m of $\deg(f_u)$	$\lceil \frac{n}{m} \rceil$
	2	100	24.97	2
	3	100	24.98	2
	4	100	24.97	2
	5	100	24.97	2
	6	100	24.96	2

Table 5.1: We consider $RS_{27}(3)$, $RS_{27}(4)$, and $RS_{27}(5)$. For each of these codes and for each coalition size s from $s = 2$ to $s = \lceil \frac{n}{k} \rceil$, we generated 100 pirate copies u, each one randomly obtained from s random colluders. We computed the mean m of $\deg(f_u)$ among these 100 pirate copies. Then we computed $\lceil \frac{n}{m} \rceil$, which shoul give an idea of what we can expect from the bound in Theorem 5.3.2.

In this particular case the bound in Theorem 5.3.2 would be improved to $\lceil \frac{n}{(k-1)(\tilde{q}-1)} \rceil$.

5.7 On the number of roots of a polynomial depending on the coefficients of highest degree

The discussion in the last section suggests the question to have an equivalent of the last lemmas for general polynomials.

More specifically, given a polynomial in $\mathbb{F}_q[x]$

$$f(x) = h(x) + g(x)$$

with

$$h(x) = a_r x^r + a_{r-1}x^{r-1} + \cdots + a_k x^k,$$
$$g(x) = a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + \cdots + a_1 x + a_0,$$

we wish to have an upper bound on the number of roots of f depending only on $h(x)$. We always have the bound r and for the case $r = k$ this bound is sharp. For the case $r > k$ we would like the bound to be potentially smaller than r.

It is important to notice that the low degree terms may play a very important role. For instance, if $h(x) = x^{q-1}$ then $f(x)$ can have no roots if $g(x) = \beta \in \mathbb{F}_q \setminus \{0, 1\}$, only one root if $g(x) = 0$, and up to $q - 1$ roots if $g(x) = -1$.

The next lemma shows that we can do better than the bound r provided that there exists a polynomial $\tilde{f}(x) = h(x) + \tilde{g}(x) \in \mathbb{F}_q[x]$, with $\deg \tilde{g}(x) < k$, whose value set (i.e. the set $\{\tilde{f}(\alpha) : \alpha \in \mathbb{F}_q\}$) is bounded by a relatively small parameter s. Observe that this is what is essentially used in Lemma 5.6.1 (with $\tilde{f}(x) = T(x)$, $s = q$) and in Lemma 5.6.2 (with $\tilde{f}(x) = N(x)$, $s = q$).

Lemma 5.7.1. *Suppose that there exists a polynomial $\tilde{f}(x) = h(x) + \tilde{g}(x) \in \mathbb{F}_q[x]$ with $h(x) = a_r x^r + \cdots + a_k x^k$ and $\tilde{g}(x) = \tilde{a}_{k-1}x^{k-1} + \cdots + \tilde{a}_0$, which evaluates at s different values at most (i.e. $\#\{\tilde{f}(\alpha) : \alpha \in \mathbb{F}_q\} \leq s$). Then the polynomial $f(x) = h(x) + g(x)$ with $g(x) = a_{k-1}x^{k-1} + \cdots + a_0$, has at most $(k-1)s$ different roots in $\mathbb{F}_q[x]$.*

Proof. Suppose $B = \{\tilde{f}(\alpha) : \alpha \in \mathbb{F}_q\}$. By hypothesis, $\#B \leq s$. Suppose that α is a root of f and suppose that $\tilde{f}(\alpha) = \beta \in B$. Then α is a root of the polynomial

$$\begin{aligned} p_\beta(x) &= f(x) - \tilde{f}(x) + \beta \\ &= g(x) - \tilde{g}(x) + \beta \end{aligned}$$

In general, all roots α of f are roots of $p_\beta(x)$ for some $\beta \in B$, and so they are roots of

$$P(x) = \prod_{\beta \in B} p_\beta(x).$$

By hypothesis $\deg(p_\beta) \leq k - 1$ for all $\beta \in B$ and $\deg(P) \leq (k-1)s$. This proves the Lemma. □

Chapter 6

Co-citations and relevance of authors and author groups

6.1 Introduction

Usually the proximity or mutual influence between authors is investigated in terms of the collaboration graph, in which each author is represented by a node and two authors are connected if they have co-authored at least one paper. The collaboration graph has attracted some attention from the mathematical community. For instance we can find collaboration graphs in the web pages of several mathematics departments, like the ones at the University of Georgia (Figure 6.1), Oakland University (Figure 6.2), or the Naval Postgraduate School in Monterey, California (Figure 6.3).

The Erdös number, reflecting the collaboration distance between a certain author and the mathematician Paul Erdös (who directly collaborated with 511 authors in his lifetime), is a popular index computed on the collaboration graph. Professor Jerrold W. Grossman leads a project devoted to the Erdös number [32]. More generally, the collaboration graph is used to find the collaboration distance between two mathematical authors. The Erdös number of mathematicians and collaboration distances between any two mathematical authors can be automatically computed using the MathSciNet database run by the American Mathematical Society [72].

Scientific studies about the collaboration network can be found, for instance in Grossman's contributions [33, 34], in Mark E. J. Newman's contributions [51, 52, 53, 54], or in [5] by Batagelj and Mrvar. It is quite standard to use a more accurate version of the collaboration graph, the weighted collaboration graph, where the edges are weighted according to the number of collaborations.

Rather than the collaboration graph, we will use in this paper the co-citation graph, in which the nodes corresponding to two authors are connected by an edge if there exists a paper simultaneously citing both authors. The co-citation concept was first defined by Henry Small in [71]. This author defined the co-citation between two papers as the frequency with which two items of earlier literature are cited together by later literature. We resume that co-citation idea but we apply it to the authorship of papers, that is, we focus on the relationships between authors rather than papers.

There are some contributions in the literature using co-citations to measure author features. In [1], Ahlgren, Jarneving and Rousseau classify authors by indices that try to establish their similarity in view of clustering them. In [47], concepts of information theory (like mutual information) are applied with a similar aim of creating clusters of authors.

While Small focuses on the concept of a "core" paper, the one with most co-citations among the papers in a certain subject, we use co-citations to derive indices to measure the relevance of authors and groups of authors.

Contribution and plan of this paper

It is widely accepted that citations tell at least as much about an author as authorship itself does. This is the origin, for instance, of the h-index [38]. We propose to use co-citations to derive indices measuring the relevance of authors and groups of authors.

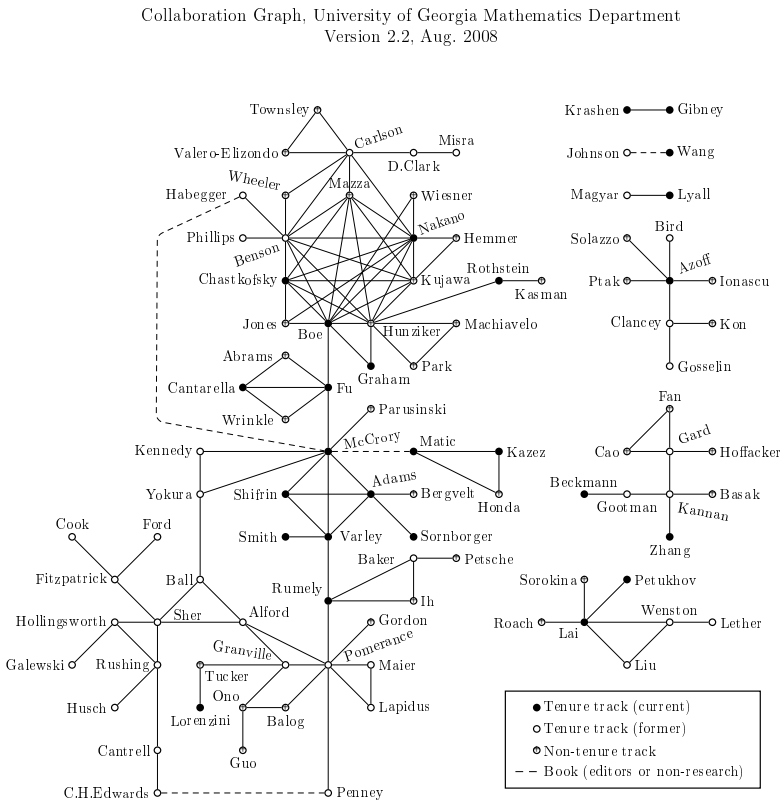


Figure 6.1: Collaboration graph of the Mathematics Department at the University of Georgia

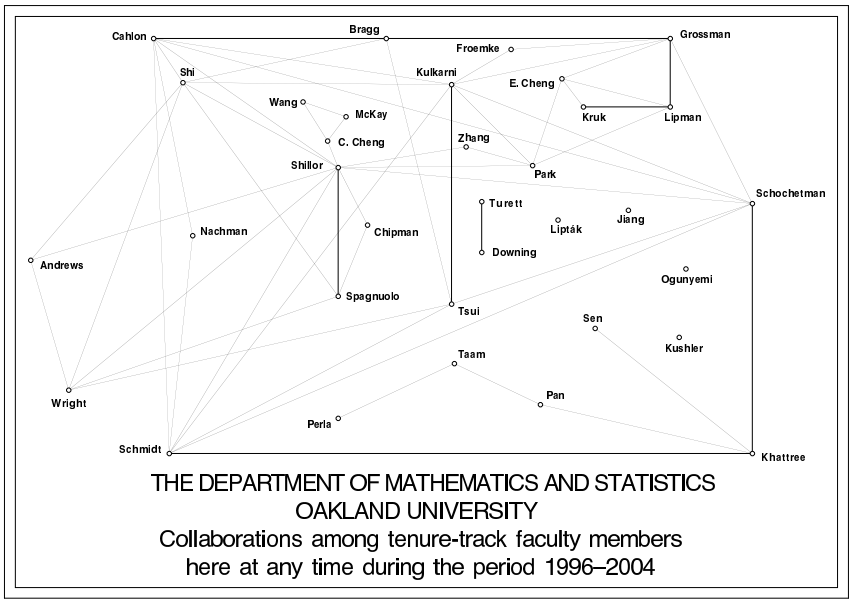


Figure 6.2: Collaboration graph of the Mathematics Department at Oakland University

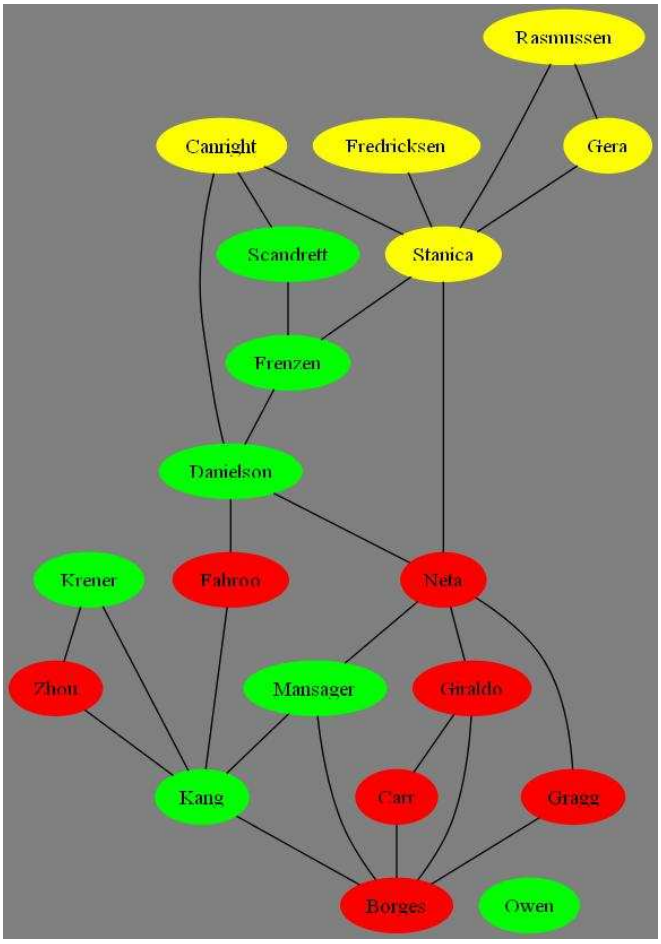


Figure 6.3: Collaboration graphs of the Mathematics Department at the Naval Postgraduate School in Monterey

In Section 6.2 we formally define co-citations and the co-citation graph. In Section 6.3 we use the co-citation graph to define three indices of relevance for individual authors. In Section 6.4 we distinguish between the relevance of an author and the relevance of a group of authors, and we give several indices based on co-citations that measure the relevance of a group of authors, in the sense of evaluating how present the group is in the citations by papers in a certain subject. Section 6.5 contains some conclusions.

For the sake of realism, in the examples throughout this paper we mention real names of authors and departments whose bibliometric data are publicly available. We wish to emphasize that it is not our purpose to judge such authors or departments in any way. In fact, our examples are unlikely to give an accurate portrait of the mentioned authors or departments, for at least two reasons: i) no single bibliometric database is guaranteed to index 100% of the scientific production or the citations of anybody; ii) our examples may not be current because they are based on the database contents at the time of writing the first version of this paper.

6.2 The co-citation graph

Co-citations and the co-citation graph can be defined as follows.

Definition 1 (Co-citation)**.** *Let $G(p)$ be the set of authors cited in the list of references of a paper p. Paper p is a co-citation to an unordered pair of authors (i, j), with $i \neq j$ if $i, j \in G(p)$. In plain words, a paper simultaneously citing an unordered pair of distinct authors is a co-citation to that pair of authors.*

Definition 2 (Co-citation graph)**.** *The* co-citation graph *is a graph having authors as nodes such that an undirected edge between two authors i and j exists if at least one co-citation to the pair (i, j) exists. The* weighted co-citation graph *is a co-citation graph where each edge is assigned a weight equal to the number of co-citations to the pair of authors (i, j) connected by the edge.*

Our hypothesis is that, while the connections in the collaboration graph show the mathematical social network, the connections in the co-citation graph show better the connections in terms of visibility or impact of the published work. For instance, two names mentioned in Section 6.1, Jerrold W. Grossman and Mark E. J. Newman, corresponded to non-adjacent nodes in the collaboration graph at the time of collecting data for this paper (according to the MathSciNet database), but they are connected in the co-citation graph, because they are often cited together.

In Table 6.1 we show the collaborations between authors in the Mathematics Department of Oakland University. A white cell means no collaboration (no edge in the collaboration graph) and a black cell means maximum number of collaborations, which in this case is 132 and is the number of publications of Professor Meir Shillor. It is important to notice that the highest number of collaborations of any author is with herself/himself, and equals the number of her/his publications. In the off-diagonal cells of Table 6.2 we show the co-citations between authors in the same department. Cells along the diagonal represent the number

of papers which contain citations to each author (citing papers); note that the number of citing papers to an author X may be less than the number of citations to X, because a citing paper can cite several papers by X. A white cell means no co-citation/citing paper and a black cell means maximum number of co-citations/citing papers. In this case, the black cell is 233 and corresponds to the number of papers citing Professor Meir Shillor. Again, the highest values for each author are in the diagonal: by definition, the number of co-citations of an author X with any other author can be no more than the number of papers citing X. Note that:

- Two authors i and j can have collaborations and no co-citations: this happens when no single paper cites their collaborations and, in addition, no single paper cites independent publications by i and by j. For example, Table 6.1 shows that, when the data were collected, Eddie Cheng and Serge Kruk had collaborated (they actually had 5 publications in common) but Table 6.2 shows that they had no co-citations.
- Two authors i and j can have co-citations and no collaborations: this happens when at least one paper cites at least one paper by i and at least one paper by j. The above mentioned example of Jerrold W. Grossman and Mark E. J. Newman illustrates a case of co-citations without collaborations.

6.3 Relevance of individual authors

We suggest three indices for the relevance of an individual author.

Maximum co-cited count

This index counts the number of authors for which a given author is maximum co-cited. A formal definition of the indicator follows.

Definition 3. *The* maximum co-cited count *of author i is m if and only if there exists a set of authors $\{i_1, \cdots, i_m\}$, where $i_k \neq i$ for all $1 \leq k \leq m$, such that the following conditions hold:*

- *Author i is co-cited with each author in the set $\{i_1, \cdots, i_m\}$;*
- *For all $1 \leq k \leq m$, in the weighted co-citation graph the edge (i, i_k) has maximum weight among those edges incident to i_k;*
- *The previous condition does not hold for any other authors not belonging to $\{i_1, \cdots, i_m\}$*

Example 2. Assume that author i is co-cited 4 times with author i_1, 5 times with author i_2 and 6 times with author i_3. At the same time, i_1 is not co-cited more than 4 times with any other author different from i, i_2 is not co-cited more than 5 times with any other author different from i and i_3 is not co-cited more than 6 times with any other author different from i. That is, i is the maximum co-cited author for authors in the set $\{i_1, i_2, i_3\}$. If there is no other author for whom i is the maximum co-cited author (last condition of Definition 3), then the maximum co-cited count of author i is 3.

Table 6.1: Number of collaborations between authors of the Oakland Mathematics Department

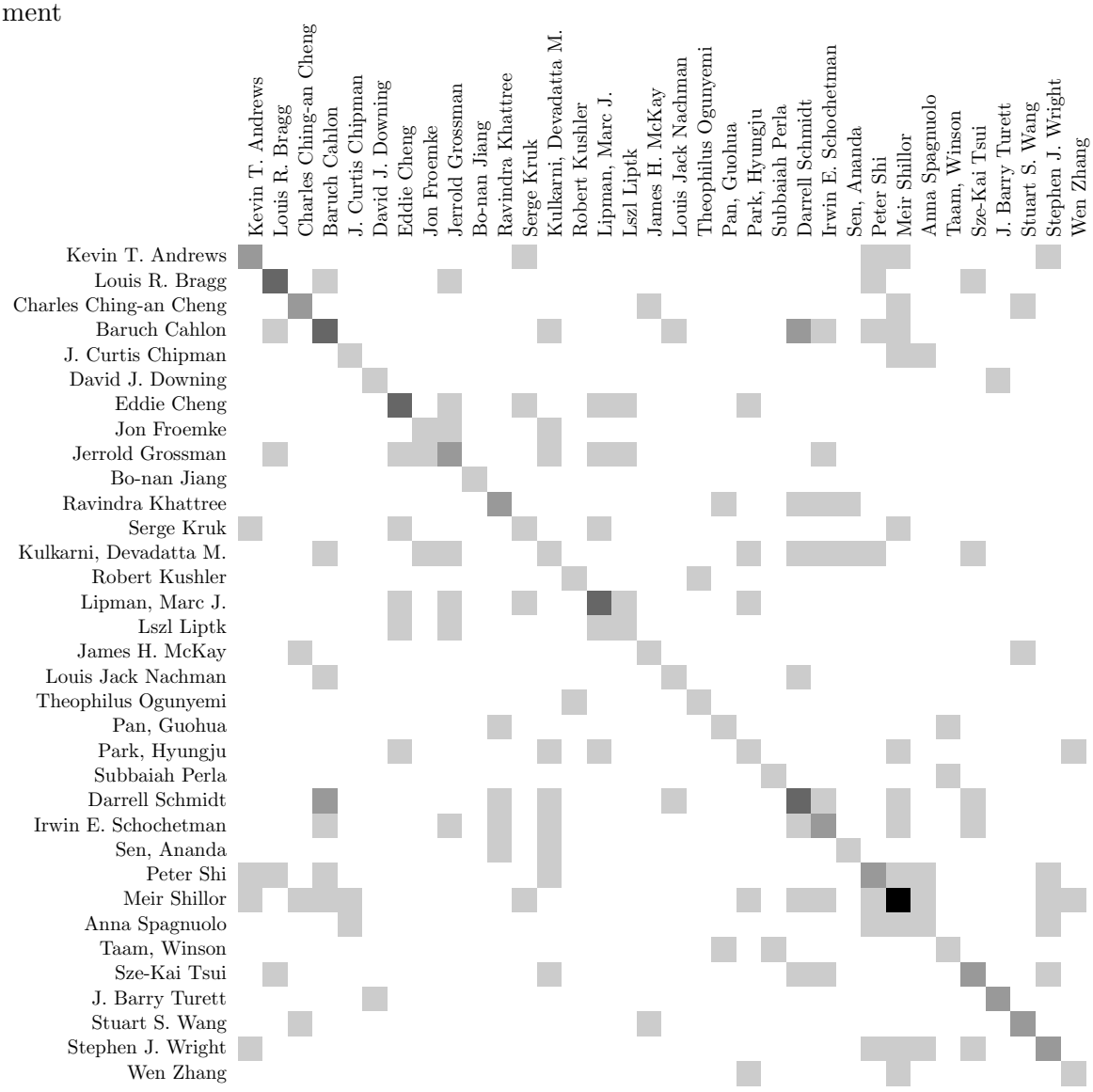
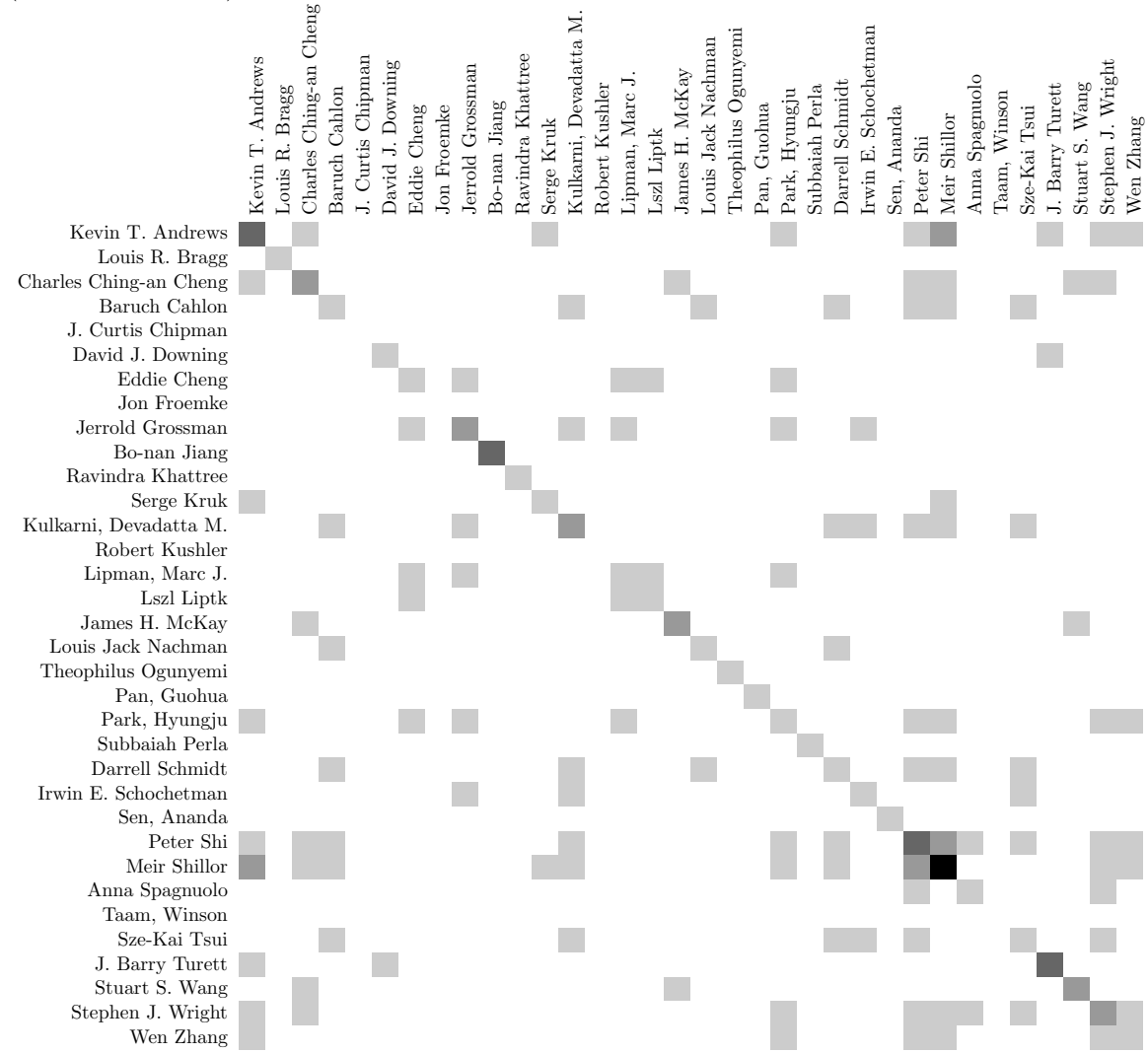


Table 6.2: Number of co-citations between authors of the Oakland Mathematics Department (off-diagonal cells). Diagonal cells represent the number of papers citing each author.



Weighted maximum co-cited count

This index counts the number of authors to which a given author is maximum co-cited weighted by the number of co-citations. A formal definition follows.

Definition 4. *The* weighted maximum co-cited count *of author i is $\sum_{k=1}^{m} c(i, i_k)$ if and only if there exists a set of authors $\{i_1, \cdots, i_m\}$, where $i_k \neq i$ for all $1 \leq k \leq m$, such that the following conditions hold:*

- *Author i is co-cited with each author in the set $\{i_1, \cdots, i_m\}$;*
- *For all $1 \leq k \leq m$, in the weighted co-citation graph the edge (i, i_k) has maximum weight among those edges incident to i_k;*
- *The previous condition does not hold for any other authors not belonging to $\{i_1, \cdots, i_m\}$;*
- *The weight of (i, i_k) is $c(i, i_k)$.*

Co-citation entropy

The co-citation entropy measures how transversal an author is perceived by the community. For example, let there be two authors i_1 and i_2 who have the same number of co-citations (sum of weights of edges incident to each author in the weighted co-citation graph), but author i_1 has been co-cited with a very small set of other authors, whereas author i_2 has been co-cited with a larger set of authors. In this case, the work of i_1 is perceived as "clique work", whereas the work of i_2 is seen as more transversal, because i_2 is cited together with a higher diversity of other authors. A formal definition of the co-citation entropy follows.

Definition 5. *Given an author i, let $w_1(i), \cdots, w_{n_i}(i)$ be the weights of the edges incident to the node of that author in the weighted co-citation graph. Define $W(i)$ as the sum of the previous weights and the relative weights as $rw_k(i) = w_k(i)/W(i)$, for $k = 1$ to n_i. Consider the set of relative weights as a probability distribution over the authors $i_1, \cdots, i_{n_i}$ co-cited with i. The Shannon entropy $H(\{rw_1(i), \cdots, rw_{n_i}(i)\})$ of that distribution is the co-citation entropy of i.*

The greater the co-citation entropy of an author, the more scattered and evenly distributed are her/his co-citations, and the greater is her/his transversality.

In Table 6.3 we show the above relevance indices computed for all authors in the Oakland Mathematics Department, with the authors sorted by increasing order of the weighted maximum co-cited count. One can appreciate some correlation between the three indices.

6.4 Relevance of a group of authors

Just like the relevance of an author can be measured by how present is she/he in the citations of a certain subject matter, the relevance of a group of authors can be measured by how present is the group of authors in those citations. A group of authors is understood here

Table 6.3: Relevance indices of authors of the Oakland Mathematics Department sorted by increasing order of the weighted maximum co-cited count

Author	Maximum co-cited count	Weighted maximum co-cited count	Co-citation entropy
Subbaiah Perla	0	0	0
Jon Froemke	0	0	0
Winson Taam	0	0	0
J. Curtis Chipman	0	0	0
Robert Kushler	0	0	0
Wen Zhang	6	7	5.8287
Theophilus Ogunyemi	14	14	4.3219
Ananda Sen	16	16	4.6438
Guohua Pan	42	47	5.4495
László Lipták	84	103	7.1421
Louis R. Bragg	117	159	7.2116
Anna Spagnuolo	150	207	7.9383
Ravindra Khattree	171	207	7.5203
David J. Downing	155	224	7.9347
Sze-Kai Tsui	187	245	7.9876
Louis Jack Nachman	196	265	8.0325
Marc J. Lipman	237	333	7.9221
Eddie Cheng	263	384	8.1200
Hyungju Park	266	395	8.4561
Irwin E. Schochetman	296	422	8.5321
James H. McKay	301	425	8.1576
Charles Ching-an Cheng	319	483	8.3218
Darrell Schmidt	381	507	8.8641
Stephen J. Wright	413	530	8.8550
Stuart S. Wang	386	597	8.2806
Baruch Cahlon	399	644	8.5870
Kevin T. Andrews	431	648	8.8418
Peter Shi	500	802	9.1075
Devadatta M. Kulkarni	499	834	8.8448
Serge Kruk	716	1032	9.3886
J. Barry Turett	434	1056	8.6478
Jerrold Grossman	1026	1566	9.6836
Bo-nan Jiang	1120	2501	9.1857
Meir Shillor	872	2981	8.9189

in a broad sense, and includes research groups, research institutes, university departments, entire universities and even all scientists in a country.

There are several conceivable group relevance metrics. We will focus on metrics that are monotonic with set inclusion, that is, such that, if A, B are groups of authors with $A \subseteq B$, then the relevance of A is less than or equal to the relevance of B. In other words, we consider metrics such that adding new authors to a group does not decrease the relevance of the group. Subadditivity is another reasonable property of a group relevance metric: if A and B are two groups of authors, the relevance of $A \cup B$ is no more than the sum of the relevance of A plus the relevance of B. Even if $A \cap B = \emptyset$, the relevance of $A \cup B$ can be less than the sum of the relevances of A and B; in particular, the relevance of a group of authors can be less than the sum of the relevances of individual authors in the group. Consider the following two extreme examples.

Example 3. In a group in which all members of the group sign all papers written by anyone in the group (such groups exist in real life!), the citations received by the group are exactly the citations received by any individual member of the group. Hence, if we use a relevance metric proportional to received citations, the relevance of the group is the same as the relevance of any individual member.

Example 4. In a group where all members publish independently and no paper is ever coauthored between two group members, the citations received by the group are the result of adding the citations received by its members. Hence, if we use a relevance metric proportional to received citations, the relevance of the group is the sum of the relevances of its individual members.

Appropriate metrics must be devised to assess the joint impact of a group. These metrics can also be useful when hiring new group members: *e.g.* one might be interested in hiring those candidates who most boost the relevance of the group, which differs from the usual criterion that one should hire those candidates with whom group members have already been collaborating.

Definition 6. *The* group citation count *in a certain subject matter is the number of papers published in that subject matter which cite at least one member of the group. This count can be normalized by dividing it by the number of papers published in the subject matter, in order to obtain the* group citation fraction*, which takes values in* $[0, 1]$.

We can also adapt the indices given in Definitions 3, 4 and 5 for groups of authors.

Definition 7. *The* maximum co-cited count of a group of authors $\{i^1, \cdots, i^g\}$ *is* m *if and only if there exists a set of authors* $\{i_1, \cdots, i_m\}$*, where* $\{i_1, \cdots, i_m\} \cap \{i^1, \cdots, i^g\} = \emptyset$ *such that the following conditions hold:*

- *Each author in* $\{i_1, \cdots, i_m\}$ *is co-cited with at least one author in* $\{i^1, \cdots, i^g\}$*;*
- *For every* $1 \leq k \leq m$*, there exists an author* $i(i_k) \in \{i^1, \cdots, i^g\}$ *such that in the weighted co-citation graph the edge* $(i(i_k), i_k)$ *has maximum weight among those edges incident to* i_k*;*

- *No strict superset of* $\{i_1, \cdots, i_m\}$ *verifies the above conditions.*

Definition 8. *The* weighted maximum co-cited count of a group of authors $\{i^1, \cdots, i^g\}$ *is* $\sum_{k=1}^{m} c(i(i_k), i_k)$ *if and only if there exists a set of authors* $\{i_1, \cdots, i_m\}$*, where* $\{i_1, \cdots, i_m\} \cap \{i^1, \cdots, i^g\} = \emptyset$ *such that the following conditions hold:*

- *Each author in* $\{i_1, \cdots, i_m\}$ *is co-cited with at least one author in* $\{i^1, \cdots, i^g\}$*;*
- *For every* $1 \leq k \leq m$*, there exists an author* $i(i_k) \in \{i^1, \cdots, i^g\}$ *such that in the weighted co-citation graph the edge* $(i(i_k), i_k)$ *has maximum weight among those edges incident to* i_k *and this weight is* $c(i(i_k), i_k)$*;*
- *No strict superset of* $\{i_1, \cdots, i_m\}$ *verifies the above conditions.*

Definition 9. *Given a group of authors* $G = \{i^1, \cdots, i^g\}$*, let* $w_1(G), \cdots, w_{n_G}(G)$ *be the weights of the edges connecting members of* G *with non-members of* G *in the weighted co-citation graph. Define* $W(G)$ *as the sum of the previous weights and the relative weights as* $rw_k(G) = w_k(G)/W(G)$*, for* $k = 1$ *to* n_G*. Consider the set of relative weights as a probability distribution over the non-members of* G *co-cited with members of* G*. The Shannon entropy* $H(\{rw_1(G), \cdots, rw_{n_G}(G)\})$ *of that distribution is the co-citation entropy of* G*.*

Indices in Definitions 7, 8 and 9 have the same interpretation as the respective indices in Definitions 3, 4 and 5: the higher their values, the better. Hence, we do not discuss them further.

We will, however, provide some discussion on the group citation count (Definition 6). The following lemma is straighforward but enlightening.

Lemma 6.4.1. *Given a group of authors* $G = \{i^1, \cdots, i^g\}$*, where each author* $i^k \in G$ *has received* $c(i^k)$ *citations and* $A(i^k)$ *is the set of articles citing* i^k*, the group citation is maximized if and only if* $A(i^k) \cap A(i^l) = \emptyset$ *for all* $i^k, i^l \in G$ *with* $i^k \neq i^l$*. In this case the group citation count is* $\sum_{k=1}^{g} c(i^k)$*.*

Hence, a group is optimal in the group citation count sense if there is no overlap in the papers citing different group members. When hiring new group members within a certain subject matter, this contradicts the usual idea that one should hire new researchers who are already related via collaboration to the group members: a joint paper by several group members implies subsequent citation overlap, because a paper citing that joint paper will cite several group members. In fact, pushed to the limit, maximization of the group citation count could be seen as discouraging collaboration between group members. Collaboration between group members would only be "rational" if their interaction resulted in a qualitative leap in their joint paper, in such a way that this joint paper would attract more citations than the sum of citations that the contributions of each author to the joint paper would separately attract as independent papers.

Some famous institutions *de facto* follow a pattern of activity which is not very far from the one sketched above. Their model is to hire a limited number of permanent faculty in

Table 6.4: Relevance indices of the Oakland Mathematics Department and the Princeton Mathematics Departments as groups

	Maximum co-cited count	Weighted maximum co-cited count	Co-citation entropy
Oakland group	560	1227	12.2070
Princeton group	10207	31764	11.9721

several areas, who tend to do research in collaboration with a large community of external or visiting co-authors. For example, in the Princeton Institute for Advanced Study, a permanent faculty of no more than twenty-eight academics each year awards fellowships to some 190 visiting members from about one hundred universities and research institutions throughout the world [25].

In Table 6.4 we show the above group relevance indices computed for the Oakland Mathematics Department and the Princeton Mathematics Department.

6.5 Concluding remarks

Human evaluation criteria can always be more refined and rich than automated indices. However, when comparing authors or groups, for instance in competitions for work positions or for funding, it is not always possible to analyze one by one the different papers and the production of each candidate (especially if there are many of them). In such cases automated indices may be helpful.

Along this line of thought, we have introduced co-citations and the co-citation graph as new tools to measure the impact of the work by scientific authors. We have argued that the co-citation graph may in fact be more informative than the collaboration graph in gauging the scientific impact: indeed, the co-citation graph gives an idea about how the community perceives and classifies the work by an author, beyond the collaborations that the author has pursued during her/his career.

Co-citations, co-citation graphs and the proposed indices are useful to assess the relevance of individual authors and also the relevance of groups of authors. It has been argued that the relevance of a group of authors is not the sum of the relevances of individuals in the group. Indeed, new indices such as the proposed ones are required in order to measure not only the output of individual authors, but also the output of any research organization, from research groups to entire national or corporate research communities. Open research issues include devising or enhancing the proposed relevance indicators.

Chapter 7

Bibliography

Bibliography

[1] P. Ahlgren, B. Jarneving, and R. Rousseau. Requirements for a cocitation similarity measure, with special reference to pearson's correlation coefficient. *Journal of the American Society for Information Science and Technology*, 54(6):550–560, 2003.

[2] A. I. Barbero and C. Munuera. The weight hierarchy of Hermitian codes. *SIAM J. Discrete Math.*, 13(1):79–104 (electronic), 2000.

[3] V. Barucci. Decompositions of ideals into irreducible ideals in numerical semigroups. *J. Commut. Algebra*, 2(3):281–294, 2010.

[4] V. Barucci, D. E. Dobbs, and M. Fontana. Maximality properties in numerical semigroups and applications to one-dimensional analytically irreducible local domains. *Mem. Amer. Math. Soc.*, 125(598):x+78, 1997.

[5] V. Batagelj and A. Mrvar. Some analyses of Erdős collaboration graph. *Social Networks*, 22(2):173–186, 2000.

[6] P. Beelen and D. Ruano. *Bounding the number of points on a curve using a generalization of Weierstrass semigroups*. Springer Netherlands, 2012.

[7] M. Bras-Amorós. Improvements to evaluation codes and new characterizations of Arf semigroups. *Applied algebra, algebraic algorithms and error-correcting codes (Toulouse, 2003)*.

[8] M. Bras-Amorós. Acute semigroups, the order bound on the minimum distance, and the Feng-Rao improvements. *IEEE Trans. Inform. Theory*, 50(6):1282–1289, 2004.

[9] M. Bras-Amorós. A note on numerical semigroups. *IEEE Trans. Inform. Theory*, 53(2):821–823, 2007.

[10] M. Bras-Amorós and P. A. García-Sánchez. Patterns on numerical semigroups. *Linear Algebra Appl*, 414(2-3):652–669, 2006.

[11] M. Bras-Amorós and M. E. O'Sullivan. The correction capability of the Berlekamp-Massey-Sakata algorithm with majority voting. *Appl. Algebra Engrg. Comm. Comput*, 17(5):315–335, 2006.

[12] M. Bras-Amorós and M. E. O'Sullivan. The order bound on the minimum distance of the one-point codes associated to the Garcia-Stichtenoth tower. *IEEE Trans. Inform. Theory*, 53(11):4241–4245, 2007.

[13] M. Bras-Amorós and K. Stokes. The semigroup of combinatorial configurations. *Semigroup Forum*, 84(1):91–96, 2012.

[14] M. Bras-Amorós and A. Vico-Oton. On the Geil-Matsumoto bound and the length of AG codes. *Designs, Codes and Cryptography*, pages 1–9, 2012.

[15] A. Campillo and J. I. Farrán. Computing Weierstrass semigroups and the Feng-Rao distance from singular plane models. *Finite Fields Appl.*, 6(1):71–92, 2000.

[16] A. Campillo, J. I. Farrán, and C. Munuera. On the parameters of algebraic-geometry codes related to Arf semigroups. *IEEE Trans. Inform. Theory*, 46(7):2634–2638, 2000.

[17] R. dela Cruz, A. Meyer, and P. Sole. An extension of Massey scheme for secret sharing. In *Information Theory Workshop, IEEE*, 2010.

[18] M. Delgado, J. I. Farrán, P. A. García Sánchez, and D. Llena. On the generalized Feng-Rao numbers of numerical semigroups generated by intervals. arXiv:1105.4833v1, 2011.

[19] M. Delgado, P. A. García-Sánchez, J. C. Rosales, and J. M. Urbano-Blanco. Systems of proportionally modular diophantine inequalities. *Semigroup Forum*, (76):469–488, 2008.

[20] J. I. Farrán, P. A. García Sánchez, and D. Llena. On the Feng-Rao numbers. In *VII Jornadas de Matemática Discreta y Algorítmica*, 2010.

[21] J. I. Farrán and C. Munuera. Goppa-like bounds for the generalized Feng-Rao distances. *Discrete Appl. Math.*, 128(1):145–156, 2003. International Workshop on Coding and Cryptography (WCC 2001) (Paris).

[22] 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.

[23] M. Fernandez, J. Cotrina, M. Soriano, and N. Domingo. A note about the identifier parent property in Reed-Solomon codes. *Computers & Security, In Press, Corrected Proof*, 2010.

[24] P. Flajolet, X. Gourdon, and D. Panario. The complete analysis of a polynomial factorization algorithm over finite fields. *Journal of Algorithms*, 40(1):37 – 81, 2001.

[25] Institute for Advanced Study. Mission and history. http://www.ias.edu/about/mission-and-history.html.

[26] A. García, S. J. Kim, and R. F. Lax. Consecutive Weierstrass gaps and minimum distance of Goppa codes. *J. Pure Appl. Algebra*, 84(2):199–207, 1993.

[27] A. García and H. Stichtenoth. On the asymptotic behaviour of some towers of function fields over finite fields. *J. Number Theory*, 61(2):248–273, 1996.

[28] P. A. García-Sánchez and J. C. Rosales. Numerical semigroups generated by intervals. *Pacific J. Math.*, pages 75–83, 1999.

[29] O. Geil. On codes from norm-trace curves. *Finite Fields Appl.*, pages 75–83, 2003.

[30] Olav Geil and Ryutaroh Matsumoto. Bounding the number of $\mathbb{F}_q$-rational places in algebraic function fields using Weierstrass semigroups. *J. Pure Appl. Algebra*, 213(6):1152–1156, 2009.

[31] P. Gopalan, V. Guruswami, and P. Raghavendra. List decoding tensor products and interleaved codes. In *STOC'09—Proceedings of the 2009 ACM International Symposium on Theory of Computing*, pages 13–22. ACM, New York, 2009.

[32] J. W. Grossman. The Erdös number project. http://www.oakland.edu/enp.

[33] J. W. Grossman. Patterns of collaboration in mathematical research. *SIAM News*, 35(9), 2002.

[34] J. W. Grossman. Patterns of research in mathematics. *Notices Amer. Math. Soc.*, 52(1):35–41, 2005.

[35] B. Grünbaum. Configurations of points and lines. *Graduate Studies in Mathematics*, 103:xiv+399, 2009.

[36] V. Guruswami. List decoding from erasures: bounds and code constructions. *IEEE Trans. Inform. Theory*, 49(11):2826–2833, 2003.

[37] P. Heijnen and R. Pellikaan. Generalized Hamming weights of q-ary Reed-Muller codes. *IEEE Trans. Inform. Theory*, 44(1):181–196, 1998.

[38] J. E. Hirsch. An index to quantify an individual's scientific research output. *Proceedings of the National Academy of Sciences of the United States of America*, 102(46):16569–16572, 2005.

[39] T. Høholdt, J. H. van Lint, and R. Pellikaan. Algebraic Geometry Codes. In *Handbook of coding theory, Vol. I, II*, pages 871–961. North-Holland, Amsterdam, 1998.

[40] H. D. L. Hollmann, J. H. van Lint, JP. Linnartz, and L. M. G. M. Tolhuizen. On codes with the identifiable parent property. *Journal of Combinatorial Theory, Series A*, 82(2):121 – 133, 1998.

[41] H. Janwa and A. K. Lal. On generalized Hamming weights and the covering radius of linear codes. In *Applied algebra, algebraic algorithms and error-correcting codes*, volume 4851 of *Lecture Notes in Comput. Sci.*, pages 347–356. Springer, Berlin, 2007.

[42] 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.

[43] J. Kurihara and T. Uyematsu. Strongly-secure secret sharing based on linear codes can be characterized by generalized Hamming weight. In *49th Annual Allerton Conference Communication, Control, and Computing*, 2011.

[44] L. Kwankyu. Fast unique decoding of plane AG codes. 2012.

[45] V. K. Leont'ev. On the roots of random polynomials over a finite field. *Mat. Zametki*, 80(2):313–316, 2006.

[46] J. Lewittes. Places of degree one in function fields over finite fields. *J. Pure Appl. Algebra*, 69(2):177–183, 1990.

[47] L. Leydesdorff. Similarity measures, author cocitation analysis, and information theory. *Journal of the American Society for Information Science and Technology*, 56(7):769–772, 2005.

[48] R. Lidl and H. Niederreiter. *Finite elds, 2nd ed., ser. Encyclopedia of Mathematics and its Applications*, volume 20. 1997.

[49] C. Munuera. Generalized Hamming weights and trellis complexity. *Advances in Algebraic Geometry Codes, E. Martinez-Moro, C. Munuera, D. Ruano (eds.), World Scientific*, pages 363–390, 2008.

[50] C. Munuera and F. Torres. A note on the order bound on the minimum distance of AG codes and acute semigroups. *Adv. Math. Commun.*, 2(2):175–181, 2008.

[51] M. E. J. Newman. The structure of scientific collaboration networks. *Proc. Natl. Acad. Sci. USA*, 98(2):404–409 (electronic), 2001.

[52] M. E. J. Newman. A study of scientific collaboration networks I. Network construction and fundamental results. *Phys. Rev. E*, 64(016131), 2001.

[53] M. E. J. Newman. A study of scientific collaboration networks II. Shortest paths, weighted networks, and centrality. *Phys. Rev. E*, 64(016132), 2001.

[54] M. E. J. Newman. Who is the best connected scientist? A study of scientific coauthorship networks. In *Complex networks*, volume 650 of *Lecture Notes in Phys.*, pages 337–370. Springer, Berlin, 2004.

[55] CK. Ngai, R. W. Yeung, and Z. Zhang. Network generalized Hamming weight. *IEEE Trans. Inform. Theory*, 57(2):1136–1143, 2011.

[56] A. Oneto and G. Tamone. On numerical semigroups and the order bound. *J. Pure Appl. Algebra*, 212(10):2271–2283, 2008.

[57] A. Oneto and G. Tamone. On the order bound of one-point algebraic geometry codes. *J. Pure Appl. Algebra*, 213(6):1179–1191, 2009.

[58] A. Oneto and G. Tamone. On some invariants in numerical semigroups and estimations of the order bound. *Semigroup Forum*, 81(3):483–509, 2010.

[59] L. H. Ozarow and A. D.Wyner. Wire-tap channel II. In *Advances in cryptology (Paris, 1984)*, volume 209 of *Lecture Notes in Comput. Sci.*, pages 33–50. Springer, Berlin, 1985.

[60] D. Panario. What do random polynomials over finite fields look like? *Finite elds and applications, ser. Lecture Notes in Comput. Sci.*, 2948:89108, 2004.

[61] R. Pellikaan, H. Stichtenoth, and F. Torres. Weierstrass semigroups in an asymptotically good tower of function fields. *Finite Fields Appl.*, 4(4):381–392, 1998.

[62] J. C. Rosales. Families of numerical semigroups closed under finite intersections and for the Frobenius number. *Houston J. Math.*, (34):469–488, 2003.

[63] J. C. Rosales and P. A. García-Sánchez. Numerical semigroups having a toms decompositoin. *Canadian Math. Bull.*, (51):134–139, 2008.

[64] J. C. Rosales and P. A. García-Sánchez. Numerical semigroups. *Developments in Mathematics*, 20:x+181, 2009.

[65] J. C. Rosales, P. A. García-Sánchez, J. I. García-García, and M. B. Branco. Numerical semigroups with maximal embedding dimension. *Int. J. Commut. Rings*, 2(1):47–53, 2003.

[66] J. C. Rosales, P. A. García-Sánchez, J. I. García-García, and M. B. Branco. Arf numerical semigroups. *J. Algebra*, 276(1):3–12, 2004.

[67] J. C. Rosales, P. A. García-Sánchez, J. I. García-García, and M. B. Branco. Saturated numerical semigroups. *Houston J. Math.*, (30):321–330, 2004.

[68] S. El Rouayheb, E. Soljanin, and A. Sprintson. Secure network coding for wiretap networks of type II. *IEEE Trans. Inform. Theory*, 58(3):1361–1371, 2012.

[69] R. Safavi-Naini and Y. Wang. Traitor tracing for shortened and corrupted ngerprints. *Digital Rights Management Workshop. Lecture Notes in Computer Science*, 2696:81100, 2003.

[70] A. Silverberg, J. Staddon, and J. L. Walker. Applications of list decoding to tracing traitors. *IEEE Trans. Inform. Theory*, 49(5):1312–1318, 2003.

[71] H. Small. Co-citation in the scientific literature: A new measure of the relationship between two documents. *Journal of the American Society for Information Science*, 24(4):265–269, 1973.

[72] American Mathematical Society. Mathscinet: Collaboration distance. http://www.ams.org/mathscinet/collaborationDistance.html.

[73] J. Staddon, D. R. Stinson, and R. Wei. Combinatorial properties of frameproof and traceability codes. *IEEE Transactions on Information Theory*, 47.

[74] H. Stichtenoth. A note on Hermitian codes over GF(q^2). *IEEE Trans. Inform. Theory*, 34(5, part 2):1345–1348, 1988. Coding techniques and coding theory.

[75] H. Stichtenoth. *Algebraic function fields and codes.* Universitext. Springer-Verlag, Berlin, 1993.

[76] K. Stokes and M. Bras-Amorós. Linear non-homogenous patterns in numerical semigroups associated to combinatorial configurations. *Preprint*, 2012.

[77] L. Tang. Consecutive Weierstrass gaps and weight hierarchy of geometric Goppa codes. *Algebra Colloq.*, 3(1):1–10, 1996.

[78] A. Toms. Strongly perforated k_0-groups of simple c^*-algebras. *Canad. Math. Bull.*, (46):457–472, 2003.

[79] V. K. Wei. Generalized Hamming weights for linear codes. *IEEE Trans. Inform. Theory*, 37(5):1412–1418, 1991.

[80] K. Yang, P. V. Kumar, and H. Stichtenoth. On the weight hierarchy of geometric Goppa codes. *IEEE Trans. Inform. Theory*, 40(3):913–920, 1994.