INTERACTIONS BETWEEN COMMUTATIVE ALGEBRA AND CODING THEORY
A SECOND DRAFT

ŞTEFAN O. TOHĂNEANU

CONTENTS

1. Introduction 4
2. Preliminaries 10
2.1. Coding Theory. 10
2.2. Commutative Algebra. 12
2.2.1. Generalities. 12
2.2.2. Rings of fractions. 12
2.2.3. Primary decomposition. 13
2.2.4. Dimension theory. 13
2.2.5. Hilbert function and degree. 14
2.2.6. Graded free resolutions. 15
2.2.7. Monomial orders. 17
2.3. Combinatorics. 18
2.3.1. Simplicial Complexes. 18
2.3.2. Matroids. 19
2.3.3. Hyperplane arrangements. 20
3. Ideals generated by fold products of linear forms 23
3.1. The De Boer - Pellikaan method for computing minimum distance. 23
3.1.1. Generalized Hamming Weights. 25
3.2. Projective codewords of minimum weight. 26
3.2.1. Minimal codewords. 28
3.3. Primary decomposition of ideals generated by a-fold products of linear forms. 30
3.3.1. The general case. 33
3.3.2. Star Configurations. 36
3.4. An error-correction algorithm. 37
3.5. Linear codes interpolation. 40
3.5.1. Interpolating fat points in $\mathbb{P}^{k-1}$. 41
3.5.2. Interpolating reduced points with given regularity. 43
3.6. Minimum distance as the α-invariant. 47
3.6.1. The Fitting module of a linear code. 47
3.6.2. A binary associated graded algebra. 49
4. Fat points defining linear codes 51
4.1. The minimum distance and the α-invariant of points. 53
4.1.1. The reduced case. 53
4.1.2. The fat points case. 54
4.2. The minimum distance and the minimum socle degree. 56
4.2.1. The case of reduced complete intersections. 60
4.3. Other results for specific situations. 63
4.3.1. Minimum distance and the index of nilpotency. 63
4.3.2. Configurations of points associated to Steiner Systems. 64

4.3.3. Fat points having complete intersection support. 66
5. Linear codes obtained by evaluating polynomials 70
5.1. Reed-Muller codes. 70
5.1.1. Algebraic geometric and toric codes. 73
5.1.2. Weight distribution and weight enumerator. 75
5.2. Evaluation codes. 77
5.2.1. Generalized Hamming weights of evaluation codes. 80
5.2.2. Codes constructed from graphs. 83
5.3. Parameterized codes. 85
5.3.1. Codes parameterized by projective torus. 89
5.3.2. Codes parameterized by graphs. 90
5.3.3. Veronese type codes. 94
5.4. Affine Cartesian codes. 95
5.4.1. Projective nested Cartesian codes. 96
5.5. The dual of an evaluation code. 97
5.5.1. Self-dual codes and Gale transforms. 99
5.5.2. α-invariant of inverse systems. 99
6. Two additional topics 101
6.1. Stanley-Reisner ring of matroids of generating matrices of linear codes. 101
6.2. Minimum distance functions. 103
6.2.1. The $\mathbf{v}$-number of a graded ideal. 107
6.2.2. The Cayley-Bacharach conjectures and the minimum distance function. 109
References 112

To my wife, Mari, and my daughter, Emma.

1. INTRODUCTION

A *code* is a collection of rules meant to transform information, such as images, sounds, letters, etc., into another form, to facilitate communication through a channel from a starting point **A** to an endpoint **B**. The design of a code is similar to the design of a cryptosystem, the difference being in that if for a cryptosystem the conversion of information is meant to keep its privacy from an eavesdropper occurring in the communication channel, for a code the conversion is meant to allow fast communication of large amount of information, while enabling detecting and correcting as much error occurring during the transmission through the channel. For example, at point **A** (the factory), the sound of music is converted (i.e., *encoded*) into peaks and valleys and recorded as a very fine spiral on a CD. During the recording, or during packaging or transportation to point **B** (the customer's CD-player), errors can occur, such as scratches or fine particles of dust. If these errors are not too big, at point **B** these errors are being corrected and the spiral of peaks and valleys converted back (i.e., *decoded*) to the original sound.

Mathematically, a code is a finite subset of a finite-dimensional vector space V over a finite field. Its elements are called *codewords*. A *linear code* is a linear subspace of V; in the setup of the scheme of a code presented above, a linear code is a code that uses linear transformations for the encoding (and hence also decoding) of the information, i.e., the linear code is the image of this linear transformation. With today's computational technology, using Linear Algebra is still the most efficient way to design a code to satisfy the goals of large information conversion and error-correction, and fast communication. This sits at the complete opposite to designing a cryptosystem where any encryption that uses linear systems are easily broken by outside attackers. There are three main parameters that are associated to a linear code: *the dimension* (i.e., the rank of the encoding linear transformation), *the length* (i.e., the dimension of the codomain of the encoding linear transformation, or the dimension of V), and *the minimum (Hamming) distance* (i.e., the minimum number of nonzero entries in any nonzero element/vector of the linear code). All these parameters are important, but the one that is the most important, because it helps with the code's capabilities for error-correction, is the minimum distance. Unfortunately, for an arbitrary linear code, computing the minimum distance is an NP-hard problem.

Commutative Algebra started to play an important role in Coding Theory in the 90's. Until then, the main connection with this field was transparent with the creation of Reed-Solomon codes, and later their generalization to Reed-Muller codes; here the main objective has been to find good bounds on the number of zeroes of a multivariate polynomial (homogeneous or not) with coefficients in a finite field, because these produce bounds on the minimum distance. The ingenious techniques used to prove the results relied more on a solid knowledge of Algebraic Number Theory and Algebraic Geometry over a finite field, rather then classical concepts from the theory of rings of polynomials (e.g., ideals, modules, dimension theory). Dwelling even further into Algebraic Geometry, mathematicians constructed the *Goppa codes* (also known as *Algebraic Geometric (AG) codes*); these are similar codes obtained by evaluating sections of a line bundle on a curve over a finite field at some points of the curve. One of the main points of attraction concerning these codes is that for a AG codes, the computation of their dimension translates into solving the Riemann-Roch problem. Michael Tsfasman and Serge Vlăduţ, and their coauthors, pursued the study of these codes and convinced the Coding Theory community that the AG codes (and by similarity, the evaluation codes) are very good codes to consider: for an infinite class of finite fields, the AG codes are beating the (linear) Gilbert-Varshamov bound (see [126]), which concerns the ability to construct linear codes with given parameters.

It wasn't until Johan P. Hansen introduced a generalized version of Reed-Muller codes, called *evaluation codes* (also known as *generalized (projective) Reed-Muller codes*), when classical concepts from Commutative Algebra started to appear. For these linear codes the goal is the same: find what the (maximum) number of zeroes that a polynomial of certain degree can have, but in any given finite set of points (instead of the entire projective or affine space over finite field as we have seen before). This new approach entailed computations and handling of concepts new to the field of Coding Theory, such as defining ideals of sets of points, Hilbert functions values to determine the dimension of the linear code (in the end, it is still a computation of the dimension a finite-dimensional vector space, but placed in a larger setting), degrees of ideals, and so

forth. In late 90's, Mario De Boer and Ruud Pellikaan, in an exercise in their paper [25], basically relate the computation of the minimum distance to computation of heights of ideals. Also, in the same paper, to check if an ideal has maximum height or not, they use Gröbner bases calculations, which have been standard techniques in computational Algebraic Geometry and computational Commutative Algebra (and also the main attack method for public key cryptosystems in Cryptography). In [16], the first use of Gröbner bases to compute minimum distance is attributed to Daniel Augot in a paper that appeared a few years earlier [6].

As we will see in this manuscript, the focus will be on the connections and interactions of Coding Theory with the theoretical Commutative Algebra, overlooking almost entirely the details of Gröbner bases calculations mentioned above; these calculations are already implemented in the computer algebra system Macaulay 2 ([53]) that we will use almost exclusively for our supporting examples. Therefore one of the main goals is to organize the theoretical framework in which the very concrete parameter which is the minimum distance relates naturally (even becomes one) with homological invariants otherwise observed only in Commutative Algebra. Another important goal derived from this approach is to bring into discussions even more experts in Commutative Algebra than those already cited to advance the research and finding more Commutative Algebraic topics and concepts that overlap with Coding Theory concepts. Furthermore, as one can see in the first parts of this book, the combinatorial and linear algebraic properties of linear codes can disseminate homological information for various classes of homogeneous ideals. More specifically, there is a huge interest into connecting properties of defining ideals of finite sets of (projective) points with the combinatorics of the hyperplane arrangement defined by the linear forms dual to the points; it seems that taking an approach via Coding Theory may give insights into this problem.

Now we present what each chapter is about.

Chapter 2. In this chapter we provide a brief background on the Coding Theory, Commutative Algebra, and Combinatorics concepts and results used throughout this book. For all three areas we needed a starting point for the exposition. Before this point, basic definitions and results, such as finite fields, linear maps, rings, ideals, modules, graphs, etc., are not covered; these can be found in almost any introductory textbooks in Abstract and Linear Algebra, and Discrete Math. We also assume some basic knowledge on Algebraic Geometry concepts, such as the projective space, affine space, varieties and their defining ideals, etc.

As we mentioned, a linear code $\mathcal{C}$ is the image of a linear map $\mathbb{K}^k \longrightarrow \mathbb{K}^n$, where $\mathbb{K}$ is a field. The $k \times n$ matrix G of this linear map (in any bases, usually the standard bases) is called *a/the generating matrix of* $\mathcal{C}$. The rank of G equals the dimension of $\mathcal{C}$, and the number of rows n equals the block-length of $\mathcal{C}$.

Chapter 3. In Chapters 3 we will assume that $k = \dim(\mathcal{C})$ and that G doesn't have any zero columns, and we consider the linear forms dual to the columns of G. Classically, the combinatorics of the hyperplane arrangement defined by these linear forms (further assuming that no two such forms are proportional) has been known to provide crucial information about the parameters of $\mathcal{C}$. If, more generally, G has some columns that are proportional, then one considers the multi-arrangement defined by the dual linear forms. In both cases, one looks at the Tutte polynomial of the matroid of the arrangement (which is same as the matroid of the matrix G) to extract information about the weights (i.e., the number of nonzero entries) of codewords and the number of codewords of different weights (see for example [28], and for a great survey, [66]). Inspired by [25], we construct ideals generated by a-fold products of these dual linear forms (where $1 \leq a \leq n$ is an integer), and we study their commutative algebraic properties. As De Boer-Pellikaan observed, as we increase the value of a, the heights of the corresponding ideals generated by a-fold products of linear forms (denoted $I_a(\mathcal{C})$) decrease, and the last value of a when this height is maximum possible k, that will be the value of the minimum distance of $\mathcal{C}$ (see Section 3.1). Furthermore, using a similar approach, in Section 3.1.1 we can determine any generalized Hamming distance of $\mathcal{C}$. Also by [25], solving the ideal $I_{d+1}(\mathcal{C})$, where d is the minimum distance, will produce the projective codewords of weight equal to d; "projective" means the equivalence class of vectors multiplied by nonzero scalars. In the brief Section 3.4 we present a commutative algebraic interpretation of an error-correcting algorithm presented in [10] (a different view of the nearest-neighbor algorithm). The basic idea of this algorithm is to find the unique

projective codeword of minimum weight in a linear code with generating matrix obtained by augmenting the message received as an extra row to the generating matrix G of $\mathcal{C}$; this unique codeword is the error that occurred in the message. Our implementation uses ideals generated by fold products of linear forms and the operation of "colon of ideals".

As it turns out, if $1 \leq a \leq d$, one has even more than $\mathrm{ht}(I_a(\mathcal{C})) = k$: one has $I_a(\mathcal{C}) = \mathfrak{m}^a$, where $\mathfrak{m} = \langle x_1, \ldots, x_k \rangle$ is the (irrelevant) maximal ideal of $R := \mathbb{K}[x_1, \ldots, x_k]$. Then a natural question comes to mind about the structure (i.e., primary decomposition) of the ideals $I_a(\mathcal{C})$ for $d+1 \leq a \leq n$. This is especially important because for the special case when the linear code is Maximum Distance Separable (MDS) code (i.e., $d = n-k+1$), $I_a(\mathcal{C})$ is the defining ideal of the codimension $n-a+1$ star configuration with skeleton being the hyperplane arrangement defined by the dual linear forms (see Section 3.3.2). Star configurations have very good extremal and axiomatic properties that answer affirmatively a multitude of conjectures concerning homogeneous ideals, especially about symbolic powers of such ideals. In Section 3.3.1 we present the primary decomposition for $I_a(\mathcal{C})$, for any a and any $\mathcal{C}$. This decomposition becomes handy when one tries to obtain results and check conjectures for classes of ideals that are more general than the usual star configurations. One application of possessing some information about the primary decomposition of $I_a(\mathcal{C})$ is the construction of linear codes with prescribed projective codewords of minimum weight (see Section 3.5.2). The idea behind this "interpolation" is the following: given a finite set of points in $\mathbb{P}^{k-1}$, we would like to construct a linear code of dimension k with minimum distance d, such that the saturation of $I_{d+1}(\mathcal{C})$ is the defining ideal of the set of points. This question can be extended to replacing the reduced set of points with a fat-points zero-dimensional scheme; $d+1$ is replaced with a convenient a (see Section 3.5.1).

In Section 3.6 brings hope into actually identifying the minimum distance of a linear code with a homological invariant (the α-invariant). As it turns out, the generators of $I_a(\mathcal{C})$ are the $a \times a$ minors of the $n \times n$ diagonal matrix with the defining linear forms placed on the main diagonal. Ideals generated by all minors of certain size of a matrix are known as *Fitting ideals*; taking direct sum of successive quotients of such ideals produces *the Fitting module* of that matrix. In Section 3.6.1 we identify the minimum distance of a linear code plus one, with the α-invariant of its Fitting module (i.e., the Fitting module of the diagonal matrix we mentioned above). This result is an almost immediate consequence of the De Boer-Pellikaan method (and of Theorem 3.21); using the α-invariant of the Fitting module we basically hide the recursive computation of heights of ideals performed in this method to find the minimum distance. If the base field is $\mathbb{F}_2$, the ideals $I_a(\mathcal{C})$ form a filtration for a certain quotient ring, and one can link similarly the minimum distance to the α-invariant of the associated graded module corresponding to this filtration (see Section 3.6.2).

Chapter 4. Under the same assumption that $k = \dim(\mathcal{C})$, and that the generating matrix G doesn't have any zero columns, in Chapter 4 we look at the finite set of points in $\mathbb{P}^{k-1}$ with homogeneous coordinates given by the columns of G. If two or more columns are proportional, we associate the appropriate multiplicity to the corresponding point, and hence we will consider fat-points schemes instead. In both instances we will call this set of fat-points *the defining fat-points scheme of* $\mathcal{C}$.

This chapter starts with the geometric observation that the minimum distance of a linear code is the block-length of the code minus the maximum number of the points, counted with multiplicity, of the defining fat-points scheme that are contained in a hyperplane. With the help of this interpretation, in Section 4.1 we will see that, once again, the minimum distance connects to the α-invariant: the minimum degree of a nonzero element of the defining ideal of the defining fat-points scheme provides a lower bound for the minimum distance of the linear code.

Historically, going back to the earlier work of J.P. Hansen, it has been observed that when the defining fat-points scheme is a complete intersection reduced set of points, a stronger homological invariant provides a lower bound for the minimum distance: the Castelnuovo-Mumford regularity. In Section 4.2 we show that this bound comes as a particular result of the case when the defining fat-points scheme is homogeneous (all points have same multiplicity); in this result the regularity is replaced by the minimum socle degree, which for the case of complete intersections are equal integers. The downside of this generalization is that

we have to restrict to base field of characteristic zero due to the fact that the argument presented uses results concerning "degrees of separators of points". Some of the results and remarks in this section preamble the results in Section 5.2 that deals with evaluation codes. The case of complete intersections is a special case for which much better lower bounds for the minimum distance are conjectured to be true. In Section 4.2.1 we use Bézout's Theorem to support these conjectures for some special cases. Later, in Section 6.2.2, we will see that these conjectures are variations and coding theoretic interpretations of the famous Cayley-Bacharach conjectures.

The last part of Chapter 4 is dedicated to some special situations and points of view. In Section 4.3.1 we see how the minimum distance links to the index of nilpotency (this is an integer that measure how an ideal sits inside its radical). First, if $\mathcal{C}$ is defined by a finite reduced set of n points that is $(k-2)$-generic (i.e., any $k-1$ columns of G are linearly independent), then the maximum number of these points that are contained in a hyperplane can be read off from the maximum power of the components in the primary decomposition of $I_{n-k+2}(\mathcal{C})$. Second, with this genericity condition, this ideal is the defining ideal of a fat-points scheme with the maximum power of that component being equal to the maximum multiplicity of the corresponding point in this fat-points scheme. But this maximum multiplicity equals the index of nilpotency of $I_{n-k+2}(\mathcal{C})$. In the next Section 4.3.2, we look at points constructed from Steiner systems (these are very special subsets of star configurations) and with the knowledge of the minimum socle degree, we present some bounds on the minimum distance of the linear codes constructed from these sets of points. Lastly, in Section 4.3.3, we analyze a bit further the special case when the defining fat-points scheme has complete intersection support, but it is not necessarily homogeneous. In Remark 4.13(b) we conjecture a certain bound for the minimum distance, and in this section we check it for some various multiplicities and when the support is a complete intersection on a grid of lines in $\mathbb{P}^2$. The advantage here is twofold: the minimum distance is known and the minimum socle degree (in fact, the stronger invariant, the regularity) can be calculated using special techniques developed to find the Hilbert function of these special fat-points schemes.

Chapter 5. The next chapter builds around treating and surveying as many as possible results concerning evaluation codes, also known as generalized Reed-Muller codes. These linear codes are constructed in the following way: one start with a finite reduced set of affine/projective points X, and then evaluates every polynomial of degree at most a/equal a at all the points of X; the image of this evaluation (linear) map is *the (affine/projective) evaluation code of order/degree a on/associated to X*, denoted $C(X)_a$. By homogenization and embedding the affine space into the projective space, it is enough to study just the projective case.

In Section 5.1 we present a bit of the history of these codes and some brief flavours of the arguments used to study these codes. At the beginning the assumptions were that the base field is a finite field, and that X is the finite set of points which builds the entire ambient space. Next step in generalizing these codes was to take X to be the rational points on some projective curve, and evaluate rational functions from a certain Riemann-Roch space; these are the *algebraic geometric codes*. The toric codes have a similar flavor, but in general are different than the evaluation codes because the domain of the evaluation map often is not the entire vector space of polynomials of a certain degree, but a subspace spanned by monomials associated to lattice polytopes (see Section 5.1.1).

Section 5.2 picks up where some of the results in Section 4.2 left off. It is transparent that evaluation codes are natural generalizations of linear codes defined by reduced sets of points. First, observe that $C(X)_1$ is in fact the linear code defined by X: the image of the evaluation map is spanned by the vectors obtained by evaluating the basis of monomials of degree 1 (i.e., the variables), hence obtaining the coordinates of the points of X. Also, the minimum distance of $C(X)_a$ has the geometric interpretation that it is equal to the number of points of X minus the maximum number of points of X contained on a hypersurface of degree a. Although the generalized Hamming weights of classical Reed-Muller codes have been studied to some extent in the past, it is surprising that only very recently (see [45]) a nice commutative interpretation of these invariants has been discovered. This interpretation naturally generalizes the geometric interpretation of the minimum distance of $C(X)_a$ we have seen above (see Section 5.2.1). In Section 5.2.2 we present a first

class of examples where the generalized Hamming weights are known: the points of X are the columns of the incidence matrix of various type of graphs. As it is the case for a lot of the results in this Chapter, their proofs use ingenious arguments which belong to Computational Algebra or Graph Theory, and therefore we decided to skip them. A common denominator though which strongly involves Commutative Algebra is that whenever a is greater than or equal to the regularity of X, then the r-th generalized Hamming weight equals the value r. The affine Cartesian codes (in Section 5.4) is another class of examples where the generalized Hamming weights were able to be determined. This was mostly due to the fact that the defining ideal of the set X (which is a cartesian product of finite subsets of $\mathbb{K}$) is a complete intersection minimally generated by a Gröbner basis.

In Section 5.3 we look at *parameterized codes*, which are linear codes very similar to the toric codes. The idea is that we look at the evaluation codes of order a associated to an algebraic toric set X (i.e., the base field is taken to be a finite field, and X is the image of $\mathbb{P}^{k-1}$ through a map given by a finite set of monomials in k variables). In Section 5.3.2 this map is given by the monomials corresponding to the edges of a graph (e.g., for the case of a complete bipartite graph, we get the classical Segre map). One similar example would be to take X to be the image of any finite set through a classical Veronese map (see Sections 5.3.1 and 5.3.3). If for the case of codes parameterized by graphs the results about their parameters are sporadic and specific to different types of graphs, for the Veronese type codes the basic parameters and generalized Hamming weights coincide to those of an (usual) evaluation code associated to X of an appropriate order, and therefore more can be said about these. Overall, for any parameterized code, a good understanding of the defining ideal of X is necessary, and though this ideal has nice known properties (e.g., it is a radical lattice ideal) handling it to find some of the parameters requires a great deal of detailed computations.

The dual of a linear code, and the related self-dual codes, have been studied extensively for quite some time, yet only very recently, see [77], the dual of evaluation codes received a detail analysis. In Section 5.5 we approach the problem from the "Macaulay's Inverse Systems" perspective to obtain that when the evaluation code is associated to a Gorenstein set of points X, then $(C(X)_a)^{\perp}$ and $C(X)_{\mathrm{reg}(X)-a-1}$ have the same parameters and generalized Hamming weights. Section 5.5.1 is another sample of the nice interactions between Commutative Algebra and Coding Theory: using bounds on the minimum distance of evaluation codes and Gale transform, with the same Gorenstein assumption on the reduced finite set of points $X \subset \mathbb{P}^{k-1}$, we can conclude that if $|X| = 2k$, then $\mathrm{reg}(X) = 3$.

Chapter 6. The last chapter introduces the reader to two topics that support once more the main goal of this book which is to show the strong, and one would say, natural connections between commutative algebra and coding theory topics and concepts.

The result presented in Section 6 connects the generalized Hamming weights of the dual of a linear code $\mathcal{C}$ (and hence of the linear code $\mathcal{C}$ itself) to the nonzero graded Betti numbers of the Stanley-Reisner ring of the simplicial complex of the independent sets of the matroid of the generating matrix of $\mathcal{C}$. The proof is highly combinatorial (hence we skip it), but it has the same flavor as interpreting the coefficients of the Tutte polynomial of the same matroid, via Duursma's formula that computes the generalized Hamming weights for the dual of $\mathcal{C}$.

In Section 6.2, due to the results in Section 5.2.1, one is able extend the concept of generalized Hamming weights of an evaluation code associated to a reduced finite set X to functions that behave very similar but can be associated to more general classes of homogeneous ideals than $I(X)$. This way one is able to define *the minimum distance function*, *the Vasconcelos function*, or *the footprint function* of a homogeneous ideal I. The first two functions are identical in some particular cases: e.g., when I is unmixed and radical (such as the defining ideal of a reduced finite set of points), or when I is unmixed of dimension 1 (such as the defining ideal of a finite set of fat-points). But they lack the ability to be computed, since for the more general cases one doesn't possesses a "generating matrix" to be able to use, for example, Proposition 3.10. This is the moment when one appeals to *the footprint function* which is similar in definition, but requires monomial order and initial ideals, hence it is computable with a computer algebra system, such as Macaulay 2. The downside is that the footprint function provides a lower bound for the minimum distance function, but in a

lot of cases they are equal (e.g., when I is a monomial unmixed ideal, or when I defines a zero-dimensional scheme and has initial ideal a complete intersection).

For an arithmetically Cohen-Macaulay scheme, the Hilbert function of its coordinate ring starts stabilizing to the degree of the scheme when it is evaluated at the Castelnuovo-Mumford regularity of the scheme. Similarly, one can define *the regularity index* as the smallest integer where the minimum distance function stabilizes at value 1 (here the minimum distance function generalizes just the minimum distance, i.e., $r = 1$). In Section 6.2.1 we look at a relatively new homological invariant of a homogeneous ideal, called the **v-***number*. This integer is similar in flavor to the minimum socle degree, and when I is an unmixed ideal with only linear associated primes, it equals the regularity index.

In Section 6.2.2 we return to the results and conjectures treated in Section 4.2.1, and we establish the equivalence between a version of the Cayley-Bacharach conjecture and a conjecture regarding a lower bound on the minimum distance function of an ideal of dimension 1 and with only linear associated primes. The last result of the notes proves this conjecture for equigenerated complete intersection ideals.

There are two people who shaped the beginning of my journey into commutative algebra aspects of coding theory, and here I would like to express profound gratitude to the two of them: Hal Schenck and John Little. My first exposure to Coding Theory happened in 2006 when, at Texas A&M University, I presented two preparation lectures prefacing John Little's presentation in the Introductory Workshop for Algebraic Coding Theory. To prepare, I used [23, Chapter 9], and very quickly I became interested in evaluation codes. In previous discussions with Hal Schenck, my PhD adviser, I became hypnotized by the Cayley-Bacharach conjectures and theorems, and as soon as he showed me his paper with Leah Gold and John Little that made the connection between the two areas (see [42]), I was forever sold on the subject. Then, John Little had yet another impact into my journey into Coding Theory; if it weren't for our discussions back in 2008-09, probably I wouldn't have been aware of the work of De Boer and Pellikaan ([25]), and therefore a big part of my research agenda over the past 12-13 years wouldn't have surfaced. Also I would like to thank Rafael Villarreal, Hal Schenck, Adam Van Tuyl, Graham Denham,... for comments and corrections at the early stages of this manuscript.

2. PRELIMINARIES

2.1. **Coding Theory.** For the preliminaries in Coding Theory we will mostly use [96] and [23].

In general, a *code* is a subset of $\mathbb{K}^n$, where $\mathbb{K}$ is a finite field, but for the theoretical purposes of this book, we can assume that $\mathbb{K}$ is any field. A *linear code*, $\mathcal{C}$, is the image of a linear map $\phi : \mathbb{K}^k \to \mathbb{K}^n$; i.e., $\mathcal{C} = \phi(\mathbb{K}^k)$. The elements of $\mathcal{C}$ are called *codewords*. $\dim(\mathcal{C})$ is called *the dimension of* $\mathcal{C}$, and n is called *the block-length of* $\mathcal{C}$, and $\mathcal{C}$ is called $[n, \dim(\mathcal{C})]$-(linear) code.

The matrix of ϕ in any bases will be called *a generating matrix of* $\mathcal{C}$; note that we loosen the usual definition of a generating matrix of a linear code; i.e., any $\dim(\mathcal{C}) \times n$ matrix whose rows form a basis for $\mathcal{C}$. Most of the time ϕ is one-to-one and therefore the two definitions match. Furthermore, in this case when $\dim(\mathcal{C}) = k$, the row reduction algorithm produces a unique generating matrix of the form $(I_k|A)$, and we say that the generating matrix is in *standard form*. The convention throughout this book is that a codeword is obtained by multiplying its generating matrix to the left by a (horizontal) vector in $\mathbb{K}^k$.

Suppose $\mathcal{C}$ is an $[n, k]$-linear code. From linear algebra, the linear subspace $\mathcal{C} \subset \mathbb{K}^n$ can be thought of as the space of solutions of some homogeneous linear system. The matrix of coefficients of this linear system is an $(n - k) \times n$ matrix, called *the parity check matrix for* $\mathcal{C}$, and therefore $\mathcal{C}$ is the null space of this matrix. If the generating matrix of $\mathcal{C}$ is in standard form $(I_k|A)$, then the matrix $(-A^T|I_{n-k})$ is a parity check matrix for $\mathcal{C}$ (here A^T is the transpose of A).

The *dual* of $\mathcal{C}$ is the linear code

$$\mathcal{C}^\perp := \{\mathbf{w} \in \mathbb{K}^n | \mathbf{w} \bullet \mathbf{c} = 0 \text{ for all } \mathbf{c} \in \mathcal{C}\},$$

where $\bullet$ denotes the usual dot product. If $\mathcal{C}$ is an $[n, k]$-linear code, then $\mathcal{C}^\perp$ is an $[n, n - k]$-linear code, and any parity check matrix for $\mathcal{C}$ is a generating matrix for $\mathcal{C}^\perp$. A linear code is called *self-dual* if $\mathcal{C} = \mathcal{C}^\perp$.

Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be two $[n, k]$-linear codes with generating $k \times n$ matrices G_1 and G_2, respectively. If there exists an invertible $n \times n$ monomial matrix M such that $G_1 = G_2M$, then the two codes are called *(monomial) equivalent*; a monomial matrix is a matrix that is the product of a diagonal matrix and a permutation matrix. If the monomial matrix is just an invertible diagonal matrix (so no permutation matrix involved) with entries on the main diagonal $d_1, \ldots, d_n$, then we denote this as $\mathcal{C}_1 = (d_1, \ldots, d_n) \bullet \mathcal{C}_2$. In general, the definition of "equivalent codes" consists of monomial equivalence together with an automorphism of the field $\mathbb{K}$ applied to the entries of one of the generating matrices, but in this book we will not consider this more general aspect.

The *(Hamming) weight* of a vector $\mathbf{w} \in \mathbb{K}^n$ is the number of nonzero entries in $\mathbf{w}$, denoted $wt(\mathbf{w})$. The *(Hamming) distance* between two vectors $\mathbf{w}_1, \mathbf{w}_2 \in \mathbb{K}^n$ is $d(\mathbf{w}_1, \mathbf{w}_2) := wt(\mathbf{w}_1 - \mathbf{w}_2)$. The Hamming distance is a metric on $\mathbb{K}^n$. *The minimum distance* of $\mathcal{C}$ is the minimum weight of a nonzero codeword, i.e.,

$$d := \min\{wt(\mathbf{w}) | \mathbf{w} \in \mathcal{C} \setminus \{\mathbf{0}\}\}.$$

The block-length, the dimension (if $\mathcal{C}$ is linear), and the minimum distance of $\mathcal{C}$ are called *the parameters of* $\mathcal{C}$; and $\mathcal{C}$ is called an $[n, \dim(\mathcal{C}), d]$-(linear) code.

Suppose $\mathbb{K} = \mathbb{F}_q$, the finite field with q elements. For an $\mathbf{x} \in \mathbb{K}^n$, let $B_r(\mathbf{x}) := \{\mathbf{y} \in \mathbb{K}^n | d(\mathbf{y}, \mathbf{x}) \leq r\}$ be the closed ball centered at $\mathbf{x}$. If $\mathcal{C} \subset \mathbb{K}^n$ is a (general) code, and if its minimum distance satisfies $d \geq 2t+1$, for some integer $t \geq 1$, then, for any distinct codewords $\mathbf{c}, \mathbf{c}' \in \mathcal{C}$, one has $B_t(\mathbf{c}) \cap B_t(\mathbf{c}') = \emptyset$ (apply the triangle inequality and $d(\mathbf{c}, \mathbf{c}') \geq d$). This observation leads to two important comments:

- Any $d - 1$ errors can be detected in a received word $\mathbf{w} \in \mathbb{K}^n$, and any t errors can be corrected by the nearest neighbor $\mathbf{c} \in \mathcal{C}$ (i.e., $\mathbf{c} \in \mathcal{C}$ is the unique codeword such that $\mathbf{w} \in B_t(\mathbf{c})$).
- If $\mathbb{K}^n = \bigcup_{\mathbf{c} \in \mathcal{C}} B_t(\mathbf{c})$, then the code $\mathcal{C}$ is called *perfect code*. The existence of perfect codes resolves the "sphere packing problem". If $q = 2$, for every integer $u \geq 1$ there exists a perfect code of block-length $2^u - 1$, and minimum distance $d = 3$, called a *Hamming code*. There are two other known perfect codes, known as *Golay codes*: one is over $\mathbb{F}_2$, it has 2^{12} codewords, block-length 23, and minimum distance 7; the other one is over $\mathbb{F}_3$, it has 3^6 codewords, block-length 11, and minimum

distance 5. The existence of perfect codes is in strong connection with the construction of Steiner systems (for more details, see [122]): over $\mathbb{F}_2$, the Hamming codes correspond to Steiner systems of type $(2, 3, 2^t - 1)$, and the Golay code corresponds to the Steiner system of type $(4, 7, 23)$; over $\mathbb{F}_3$, the Golay code corresponds to the unique Steiner system of type $(4, 5, 11)$.

Suppose $\mathcal{C}$ is a (general) code over a finite field $\mathbb{K} = \mathbb{F}_q$, of block length n and minimum distance d. Denote with $A_q(n, d)$ the maximum size (i.e., maximum number of codewords) of $\mathcal{C}$. Then the *Gilbert-Varshamov bound* is the lower bound

$$A_q(n, d) \geq \frac{q^n}{\sum_{j=0}^{d-1} \binom{n}{j}(q-1)^j}.$$

Plotkin bound (for $q = 2$) and Johnson bound (for any q) provide upper bounds for $A_q(n, d)$. *The Gilbert-Varshamov bound for linear codes* is stated in the following way: if

$$q^{n-k} > \sum_{j=0}^{d-2} \binom{n-1}{j}(q-1)^j,$$

then there exists an $[n, k, d']$-linear code with $d' \geq d$. This can be obtained from the bound for a general code from the fact that if $\dim(\mathcal{C}) = k$, then $|\mathcal{C}| = q^k$.

Also, for an $[n, k, d]$-linear code, over any field, one has the *Singleton bound*: $d \leq n - k + 1$. Whenever the bound is attained, the linear code is called *Maximum distance separable (MDS) code*.

The above bounds concerning the parameters of linear codes are all addressing the question of ability to construct codes with certain parameters and properties. For any such construction, a feasible $[n, k, d]$-linear code has k/n not too small, yet d relatively large.

In the landmark paper [129], Wei introduces and analyzes the concepts of generalized Hamming weights. Let $\mathcal{C}$ be an $[n, k, d]$-linear code. Let $\mathcal{D} \subseteq \mathcal{C}$ be a subcode. The support of $\mathcal{D}$ is

$$Supp(\mathcal{D}) := \{i : \exists (x_1, \ldots, x_n) \in \mathcal{D} \text{ with } x_i \neq 0\}.$$

Let $m(\mathcal{D}) := |Supp(\mathcal{D})|$ be the cardinality of the support of $\mathcal{D}$.

For any $r = 1, \ldots, k$, the r^{th} *generalized Hamming weight of* $\mathcal{C}$ is the positive number

$$d_r(\mathcal{C}) := \min_{\mathcal{D} \subseteq \mathcal{C}, \dim \mathcal{D} = r} m(\mathcal{D}).$$

By convention, $d_0(\mathcal{C}) = 0$. It is not hard to see that $d_1(\mathcal{C})$ equals the minimum distance d of $\mathcal{C}$. The following are satisfied:

- $1 \leq d_1(\mathcal{C}) < d_2(\mathcal{C}) < \cdots < d_k(\mathcal{C}) \leq n$.
- $d_r(\mathcal{C}) \leq n - k + r$.
- From first two items, if $d_{r_0}(\mathcal{C}) = n - k + r_0$, for some $1 \leq r_0 \leq k$, then for any $r_0 \leq r \leq k$, $d_r(\mathcal{C}) = n - k + r$.
- $\{d_r(\mathcal{C}) | 1 \leq r \leq k\} = \{1, \ldots, n\} \setminus \{n + 1 - d_s(\mathcal{C}^\perp) | 1 \leq s \leq n - k\}$.
- Equivalent codes have the same parameters and the same generalized Hamming weights.

We end this very brief introduction by talking about the *nearest-neighbor error-correcting and decoding algorithm*. Suppose $\mathbf{w} \in \mathbb{K}^n$ is a word received that contains the error $\epsilon \in \mathbb{K}^n$, i.e. $\mathbf{w} = \mathbf{c} + \epsilon$, for a codeword $\mathbf{c} \in \mathcal{C}$. If $wt(\epsilon) \leq (d-1)/2$, then $\mathbf{c}$ is unique, and it is called *the nearest neighbor of* $\mathbf{w}$. The algorithm works in the following way: the nearest neighbor of $\mathbf{w}$ is the codeword $\mathbf{c} \in \mathcal{C}$ with minimal $wt(\mathbf{w} - \mathbf{c})$.

Here is an example: consider the linear code over $\mathbb{K} = \mathbb{F}_2$ with generating matrix $G = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$. This is a $[6, 3]$-linear code. Suppose $\mathbf{w} = (0, 1, 1, 1, 0, 0)$ is received. We have the table

$\mathbf{c} \in \mathcal{C}$	$wt(\mathbf{w}-\mathbf{c})$
$(0,0,0)G = (0,0,0,0,0,0)$	3
$(1,0,0)G = (1,0,0,1,1,0)$	4
$(0,1,0)G = (0,1,0,1,0,1)$	2
$(0,0,1)G = (0,0,1,0,1,1)$	4
$(1,0,1)G = (1,0,1,1,0,1)$	3
$(1,1,0)G = (1,1,0,0,1,1)$	5
$(0,1,1)G = (0,1,1,1,1,0)$	1
$(1,1,1)G = (1,1,1,0,0,0)$	2

$\mathbf{w}$ is corrected to its nearest neighbor $(0,1,1,1,1,0) \in \mathcal{C}$, and decoded to $(0,1,1)$.

2.2. **Commutative Algebra.** For the preliminaries addressing concepts in Commutative Algebra, we will use [30], [86], [105], and [106].

2.2.1. *Generalities.* Let R be a commutative ring. The ideal generated by $f_1, \ldots, f_n \in R$ will be denoted $\langle f_1, \ldots, f_n \rangle$. If $\mathcal{F}$ is a finite subset of elements of R, and if I is an ideal of R, then $\langle I, \mathcal{F} \rangle$ denotes the ideal $I + \langle \mathcal{F} \rangle$. If $f \in R$ and $I \subset R$ is an ideal, $\bar{f} \in R/I$ denotes the residue class $f + I$ in the quotient ring R/I. If I and J are ideals, then IJ denotes the ideal generated by the set $\{fg | f \in I \text{ and } g \in J\}$. We have that $IJ \subseteq I \cap J$.

Let I be a proper ideal of R. Denote $\mathrm{Var}(I) := \{\mathfrak{p} | \mathfrak{p} \text{ is a prime ideal of } R, I \subseteq \mathfrak{p}\}$. A prime ideal $\mathfrak{p}$ is called *minimal prime over* I if $\mathfrak{p} \in \mathrm{Var}(I)$ and it is minimal with respect to inclusion (i.e., $I \subseteq \mathfrak{p}$, and there is no prime ideal $\mathfrak{q}$ with $I \subsetneq \mathfrak{q} \subsetneq \mathfrak{p}$). Denote $\mathrm{Min}(I)$ to be the set of minimal primes over I.

If $I \subset R$ is an ideal, the *radical of* I is the ideal $\sqrt{I} := \{f \in R | \text{ there is integer } n(f) \geq 1, \text{ with } f^{n(f)} \in I\}$. Some of the properties are the following:

- $I \subseteq \sqrt{I}$. If equality, then I is called *radical*. $\sqrt{I}$ is a radical ideal; i.e., $\sqrt{\sqrt{I}} = \sqrt{I}$.
- If J is another ideal of R, then $\sqrt{I+J} = \sqrt{\sqrt{I} + \sqrt{I}}$, and $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J} = \sqrt{IJ}$.
- $\sqrt{I} = R$ iff $I = R$.
- $\sqrt{I} = \bigcap_{\mathfrak{p} \in \mathrm{Var}(I)} \mathfrak{p} = \bigcap_{\mathfrak{p} \in \mathrm{Min}(I)} \mathfrak{p}$.

If I and J are two ideals of R, *the colon ideal* is the ideal $\{f \in R | fJ \subseteq I\}$, denoted $I : J$. If $J = \langle f \rangle$ for some $f \in R$, then $I : \langle f \rangle$ is denoted $I : f$. Some properties are the following:

- If $J \subseteq I$, then $I : J = R$. Also, $I \subseteq I : J$.
- If K is another ideal of R, then $(I : J) : K = I : (JK) = (I : K) : J$.
- If $\{I_\lambda\}_\lambda$ is a family of ideals, then $\left(\bigcap_\lambda I_\lambda\right) : J = \bigcap_\lambda (I_\lambda : J)$, and $J : \sum_\lambda I_\lambda = \bigcap_\lambda (J : I_\lambda)$.
- Let I be an ideal of R. An element $f \in R$ is called *a zero-divisor of* R/I if there exists $\bar{0} \neq \bar{g} \in R/I$ such that $f\bar{g} = \bar{0}$; the set of zero-divisors of R/I is denoted with $Z(R/I)$. If $I = 0$, the zero ideal, one recovers the usual definition of zero-divisors in the ring R. If $f \notin Z(R/I)$, then f is called *regular* on R/I. We have: $f \in Z(R/I)$ iff $I : f \neq I$.

The ring R is called *Noetherian* if any ascending chain of ideals $I_1 \subseteq I_2 \subseteq \cdots$ is stationary; R is Noetherian iff every ideal of R is finitely generated. The ring R is called *Artinian* if any descending chain of ideals $I_1 \supseteq I_2 \supseteq \cdots$ is stationary.

2.2.2. *Rings of fractions.* Let R be a commutative ring. A subset S of R is called *multiplicatively closed* if $1 \in S$, and if $s_1, s_2 \in S$, then $s_1 s_2 \in S$. On pairs of elements $(a, s) \in R \times S$ we can define an equivalence relation $(a_1, s_1) \sim (a_2, s_2)$ iff there exists $u \in S$ such that $u(a_1 s_2 - a_2 s_1) = 0$. The equivalence class

of (a, s) is denoted $\frac{a}{s}$; the set of equivalence classes is denoted $S^{-1}R$, and it forms a ring with "standard" addition and multiplication of fractions.

If $\mathfrak{p}$ is a prime ideal of R, then $S := R \setminus \mathfrak{p}$ is a multiplicatively closed set; in this case $S^{-1}R$ is denoted $R_{\mathfrak{p}}$. If $f \in R$, then $S := \{1, f, f^2, \dots, \}$ is a multiplicatively closed set; in this case $S^{-1}R$ is denoted R_f. If R is an integral domain, then $S := R \setminus \{0\}$ is a multiplicatively closed set; in this case $S^{-1}R$ is denoted $Q(R)$, and it is called *the field of fractions of* R.

If S is a multiplicatively closed subset of R, the map $\phi : R \to S^{-1}R$, $\phi(a) = a/1$ is a homomorphism of rings. If I is an ideal of R, then the extension of I to $S^{-1}R$, which is the ideal generated by $\phi(I)$, equals $I^e := \{a/s \in S^{-1}R |$ for some $a \in I, s \in S\}$. We have the properties:

- $(I + J)^e = I^e + J^e$, $(IJ)^e = I^e J^e$, $(I \cap J)^e = I^e \cap J^e$, $(\sqrt{I})^e = \sqrt{I^e}$.
- $I^e = S^{-1}R$ iff $I \cap S \neq \emptyset$. In other words, the elements of S become invertible elements in $S^{-1}R$.
- There is a bijection between the prime ideals $\mathfrak{p} \subset R$ with $\mathfrak{p} \cap S = \emptyset$, and the prime ideals of $S^{-1}R$. This bijection is given by $\mathfrak{p} \mapsto \mathfrak{p}^e$.
- If $\mathfrak{p}$ is a prime ideal of R, then $R_{\mathfrak{p}}$ is a local ring with unique maximal ideal $\mathfrak{p}R_{\mathfrak{p}}$; in this ring of fractions, I^e is commonly denoted $IR_{\mathfrak{p}}$.

2.2.3. *Primary decomposition.* Let R be a commutative ring. A proper ideal $\mathfrak{q} \subset R$ is called *primary* if whenever $fg \in \mathfrak{q}$ with $f \notin \mathfrak{q}$, then $g \in \sqrt{\mathfrak{q}}$. If $\mathfrak{q}$ is a primary ideal, then $\sqrt{\mathfrak{q}} = \mathfrak{p}$ is a prime ideal and $\operatorname{Min}(\mathfrak{q}) = \{\mathfrak{p}\}$; to capture this property we say that $\mathfrak{q}$ is $\mathfrak{p}$-*primary*. Any ideal whose radical is a maximal ideal $\mathfrak{m}$ of R is $\mathfrak{m}$-primary. If $\mathfrak{q}_1, \dots, \mathfrak{q}_s$ are $\mathfrak{p}$-primary ideals, then $\mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_s$ is also a $\mathfrak{p}$-primary ideal.

Any proper ideal I of a Noetherian ring R can be expressed as

$$I = \mathfrak{q}_1 \cap \cdots \mathfrak{q}_s,$$

where each $\mathfrak{q}_i$ is $\mathfrak{p}_i$-primary ideal; this is called *a primary decomposition of* I. A primary decomposition is called *irredundant* or *minimal* if $\mathfrak{p}_1, \dots, \mathfrak{p}_s$ are distinct prime ideals of R, and for all $j = 1, \dots, s$, $\mathfrak{q}_j \not\supseteq \bigcap_{i \in \{1,\dots,s\} \setminus \{j\}} \mathfrak{q}_i$. Any irredundant primary decomposition is unique up to permuting the terms in the decomposition.

Suppose I has an irredundant primary decomposition as above. The set $\{\mathfrak{p}_1, \dots, \mathfrak{p}_s\}$ is called the set of *associated primes of* I, and it is denoted with $\operatorname{Ass}(I)$. We have the following properties:

- The minimal elements (under inclusion) of $\operatorname{Ass}(I)$ are the minimal primes of I; i.e., $\operatorname{Min}(I)$. If $\mathfrak{p} \in \operatorname{Ass}(I) \setminus \operatorname{Min}(I)$, then $\mathfrak{p}$ is called an *embedded prime of* I. The ideal I is called *unmixed* if $\operatorname{Ass}(I) = \operatorname{Min}(I)$.
- Let $\mathfrak{p}$ be a prime ideal. Then, $\mathfrak{p} \in \operatorname{Ass}(I)$ iff there exists $f \in R$ such that $I : f = \mathfrak{p}$.
- $Z(R/I) = \bigcup_{\mathfrak{p} \in \operatorname{Ass}(I)} \mathfrak{p}$.

Suppose I is a homogeneous ideal of $R = \mathbb{K}[x_1, \dots, x_k]$, the ring of homogeneous polynomials with coefficients in a field $\mathbb{K}$. Let $\mathfrak{m} := \langle x_1, \dots, x_k \rangle$ be the (irrelevant) maximal ideal. *The saturation of* I *w.r.t.* $\mathfrak{m}$ is the homogeneous ideal $I^{sat} := \{f \in R \,|\, \exists\, n(f) \geq 0$ such that $\mathfrak{m}^{n(f)} \cdot f \subset I\}$. From the definition, if I is $\mathfrak{m}$-primary, then $I^{sat} = R$. Also, $I \subseteq I^{sat}$, $(I \cap J)^{sat} = I^{sat} \cap J^{sat}$, and if I is a prime ideal different than $\mathfrak{m}$, then $I^{sat} = I$. Furthermore, the zero local cohomology of R/I is $\mathrm{H}^0_{\mathfrak{m}}(R/I) = I^{sat}/I$.

2.2.4. *Dimension theory.* Let R be a nontrivial commutative Noetherian ring. *The height* of a prime ideal $\mathfrak{p} \subset R$ is the supremum of lengths of chains of prime ideals $\mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_n = \mathfrak{p}$; this is denoted with $\operatorname{ht}(\mathfrak{p})$. *The Krull dimension* of R is the maximum of the heights of the prime ideals of R, and is denoted with $\dim(R)$. In our assumptions, $\dim(R) = \operatorname{ht}(\mathfrak{m})$, for any $\mathfrak{m}$, maximal ideal of R. If I is a proper ideal of R, *the height* of I is the height of any minimal prime $\mathfrak{p}$ over I.

Most of the time throughout this book, $R = \mathbb{K}[x_1, \dots, x_k]$, the ring of polynomial in k variables, with coefficients in a field $\mathbb{K}$. If $\mathfrak{p}$ is a prime ideal, then the Krull dimension of $R/\mathfrak{p}$ equals the transcendence

degree of the field of fractions of $R/\mathfrak{p}$ over $\mathbb{K}$; i.e., $\dim(R/\mathfrak{p}) = \mathrm{tr.deg}_{\mathbb{K}} Q(R/\mathfrak{p})$. Also, if I is an ideal of $R = \mathbb{K}[x_1, \ldots, x_k]$, then $\dim(R/I) = \dim(R) - \mathrm{ht}(I) = k - \mathrm{ht}(I)$; this is the reason why often "height" is replaced by "codimension".

If $\dim(R) = 0$, then R is also an Artinian ring; and conversely, any ring that is both Noetherian and Artinian has Krull dimension 0 (since every prime ideal is also a maximal ideal).

If a proper ideal I can be generated by n elements, then $\mathrm{ht}(I) \leq n$. Denote with $\mu(I)$ the minimum number of generators of an ideal I in a (Noetherian) ring R. I is called *(ideal-theoretic) complete intersection* if $\mu(I) = \mathrm{ht}(I)$. An ordered sequence of elements $f_1, \ldots, f_n \in R$ is called an *R-regular sequence*, if $f_1 \notin Z(R)$, and for $i = 2, \ldots, n$, $f_i \notin Z(R/\langle f_1, \ldots, f_{i-1}\rangle)$. In general, for an arbitrary ring R, not every permutation of an R-regular sequence is an R-regular sequence; but if $f_1, \ldots, f_n$ is an R-regular sequence, then $\mathrm{ht}(\langle f_1, \ldots, f_n\rangle) = n$.

If $R = \mathbb{K}[x_1, \ldots, x_k]$, the ring of homogeneous polynomials with coefficients in the field $\mathbb{K}$, and I is a homogeneous ideal of R, then we have the properties:

- Any permutation of an R-regular sequence (of homogeneous polynomials) remains an R-regular sequence.
- I is a complete intersection if and only if it is generated by an R-regular sequence.
- $\mathrm{ht}(I) = n$ iff I contains an R-regular sequence of n homogeneous polynomials.
- It often happens that the literature presents definitions and results addressing the case when $\mathrm{ht}(I) = k$ (i.e., R/I is Artinian), because otherwise (i.e., $\mathrm{ht}(I) = n < k$), then one usually does an *Artinian reduction*. This means that one looks at the Artinian ring $R/\langle I, \ell_1, \ldots, \ell_{k-n}\rangle$, where $\ell_1, \ldots, \ell_{k-n}$ are generic linear forms, therefore ensuring that $\mathrm{ht}(\langle I, \ell_1, \ldots, \ell_{k-n}\rangle) = k$.

Other properties concerning heights of ideals in a ring R are the following:

- If $I \subseteq J$ are two ideals, then $\mathrm{ht}(I) \leq \mathrm{ht}(J)$.
- $\mathrm{ht}(\sqrt{I}) = \mathrm{ht}(I)$.
- If I is unmixed, and $f \in Z(R/I)$, then $\mathrm{ht}(\langle I, f\rangle) = \mathrm{ht}(I)$. More generally, if $\mathcal{F}$ is a finite set of R, such that $I : \langle \mathcal{F}\rangle \neq I$, then $\mathrm{ht}(\langle I, \mathcal{F}\rangle) = \mathrm{ht}(I)$.

2.2.5. *Hilbert function and degree.* In this part we assume $R = \mathbb{K}[x_1, \ldots, x_k]$ is the ring of homogeneous polynomials with coefficients in a field $\mathbb{K}$. All ideals of R are homogeneous ideals; in this way R can be viewed as a local ring with $\mathfrak{m} := \langle x_1, \ldots, x_k\rangle$ being its (irrelevant) maximal ideal. R is a graded ring with the standard grading given by the degree of polynomials. The zero polynomial has any degree. Note that if I is a homogeneous ideal, then I and R/I naturally become graded R-modules.

Let i be an integer. Then R_i denotes the $\mathbb{K}$-vector space of homogeneous polynomials of degree i. If I is a homogeneous ideal, I_i is the linear subspace $R_i \cap I$. Also, $(R/I)_i \simeq R_i/I_i$. If $a \in \mathbb{Z}$, then $R(-a)$ is the same ring R but with shifted grading $R(-a)_i = R_{i-a}$.

If M is a finitely generated graded R-module, *the Hilbert function of* M is the function $HF(M, i) = \dim_{\mathbb{K}} M_i, i \in \mathbb{Z}$. We have the following properties:

- $HF(R, i) = \binom{k-1+i}{i}$, and $HF(R(-a), i) = HF(R, i-a)$.
- *The Hilbert series of* M is the formal power series $HS(M, t) = \sum_{i \in \mathbb{Z}} HF(M, i)t^i$. It turns out that $HS(M, t) = P(t)/(1-t)^k$, where $P(t) \in \mathbb{Z}[t, t^{-1}]$ is a Laurent polynomial. For example, $HS(R(-a), t) = t^a/(1-t)^k$. If I is an ideal of R, setting $m := k - \mathrm{ht}(I)$, then $HS(R/I, t) = (h_0 + \cdots + h_m t^m)/(1-t)^m$; in this case $(h_0, \ldots, h_m)$ is called *the h-vector of* R/I.
- There exists a polynomial $F(x) \in \mathbb{Q}[x]$, such that $HF(M, i) = F(i)$, for $i >> 0$. This polynomial is called *the Hilbert polynomial*, and it is denoted $HP(M, i)$.

- Let I be a homogeneous ideal of R. If R/I is Artinian (equivalently, I is $\mathfrak{m}$-primary, or $\mathrm{ht}(I) = k$), then $HP(R/I, i) = 0$. Otherwise, $HP(R/I, i) = \frac{a_m}{m} i^m + \frac{a_{m-1}}{(m-1)} i^{m-1} + \cdots$, where $a_j \in \mathbb{Z}$ with $a_m > 0$, and $m = k - 1 - \mathrm{ht}(I)$.
- If $0 \to M \to N \to P \to 0$ is a short exact sequence of finitely generated graded R-modules, then for any $i \in \mathbb{Z}$, $HF(N, i) = HF(M, i) + HF(P, i)$. The same additivity property is valid for the Hilbert polynomial and the Hilbert series.
- Suppose $\mathfrak{m} \notin \mathrm{Ass}(I)$ (i.e., $I = I^{sat}$). If $\mathrm{ht}(I) \leq k - 2$, then $HF(R/I, i) < HF(R/I, i + 1)$, for all $i \geq 0$. If $\mathrm{ht}(I) = k - 1$, then there exist positive integers r and e such that $1 = HF(R/I, 0) < HF(R/I, 1) < \cdots < HF(R/I, r - 1) < HF(R/I, i) = e$, for all $i \geq r$.

The degree of R/I is defined to be: (1) $\deg(R/I) := a_m$, if $\mathrm{ht}(I) < k$; (2) $\deg(R/I) := \dim_{\mathbb{K}}(R/I)$, if $\mathrm{ht}(I) = k$. In fact, in case (1), if $V(I) \subset \mathbb{P}^{k-1}$ is the projective variety/scheme defined by I, then a_m matches the geometrical description of the degree of $V(I)$, and $m > 0$ matches the geometrical description of the dimension of $V(I)$. These are some of the most important properties of the degree that we will see throughout the book:

- If I has irredundant primary decomposition $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_s$, then $\deg(R/I) = \sum_{\mathrm{ht}(\mathfrak{q}_i)=\mathrm{ht}(I)} \deg(R/\mathfrak{q}_i)$.
- If $\mathfrak{p} \subset R$ is a linear prime (i.e., it is generated by linear forms) of height $c \leq k - 1$, then, for any integer $u \geq 1$, $\deg(R/\mathfrak{p}^u) = \binom{c+u-1}{c}$. In particular, if $\mathbb{X} = \{P_1, \ldots, P_e\} \subset \mathbb{P}^{k-1}$ is a finite set of (reduced) points, then $\deg(R/I(\mathbb{X})) = e$. Here, for a projective variety $V \subseteq \mathbb{P}^{k-1}$, $I(V)$ denotes the (homogeneous) ideal in $R = \mathbb{K}[x_1, \ldots, x_k]$ defining V. For example, $I(\mathbb{X}) = I(P_1) \cap \cdots \cap I(P_e)$, and if $P = [a_1, \ldots, a_k] \in \mathbb{P}^{k-1}$ is projective point, then $I(P) = \langle \{a_i x_j - a_j x_i | i \neq j\} \rangle$. Furthermore, if $Z = u_1 P_1 + \cdots + u_e P_e \subset \mathbb{P}^{k-1}, u_j \geq 1$ is a *fat-points scheme*, then, by definition, $I(Z) = I(P_1)^{u_1} \cap \cdots \cap I(P_e)^{u_e}$.
- If $I \subsetneq J$ are ideals of the same height, then $\deg(R/I) > \deg(R/J)$. Furthermore, if I and J are unmixed, then $I = J$ iff $\deg(R/I) = \deg(R/J)$.
- If $I, J, K \subset R$ are homogeneous ideals with $I = J \cap K$, and $\mathrm{ht}(I) = \mathrm{ht}(J) \leq k - 1$. If $\mathrm{ht}(K) > \mathrm{ht}(I)$, then $\deg(R/I) = \deg(R/J)$. If $\mathrm{ht}(K) = \mathrm{ht}(I)$, but $\mathrm{ht}(J + K) > \mathrm{ht}(I)$, then $\deg(R/I) = \deg(R/J) + \deg(R/K)$. These properties come from the additivity of the Hilbert polynomial on the short exact sequence $0 \to \frac{R}{J \cap K} \to \frac{R}{J} \oplus \frac{R}{K} \to \frac{R}{J + K} \to 0$, and comparing leading terms of the corresponding Hilbert polynomials.

2.2.6. *Graded free resolutions.* For this part we restrict our preliminaries again to the case of $R = \mathbb{K}[x_1, \ldots, x_k]$, the ring of homogeneous polynomials with coefficients in a field $\mathbb{K}$; $\mathfrak{m}$ still denotes the irrelevant maximal ideal.

A *graded minimal free resolution* of a finitely generated graded R-module M is an exact chain complex

$$0 \to \mathbf{F}_p \to \mathbf{F}_{p-1} \to \cdots \to \mathbf{F}_1 \to \mathbf{F}_0 \to M \to 0,$$

where $\mathbf{F}_i$ are graded free R-modules, the homomorphisms $\phi_i : \mathbf{F}_i \to \mathbf{F}_{i-1}$ in the complex are graded maps, and $\phi_i(\mathbf{F}_i) \subseteq \mathfrak{m}\mathbf{F}_{i-1}$ (i.e., this gives "minimality").

• The length p is called *the projective dimension of* M, and is denoted $\mathrm{pdim}(M)$. By Hilbert Syzygy Theorem, $\mathrm{pdim}(M) \leq k$.

• For each $i = 0, \ldots, p$, $\mathbf{F}_i = \oplus_j R(-j)^{\beta_{i,j}}$. The numbers $\beta_{i,j}$ are called *the graded Betti numbers of* M. Except for finitely many, all graded Betti numbers of a finitely generated module are zero. *The (Castelnuovo-Mumford) regularity of* M is

$$\mathrm{reg}(M) := \max\{j - i | \beta_{i,j} \neq 0\}.$$

If $0 \to A \to B \to C \to 0$ is a short exact sequence of graded finitely generated R modules, then

(a) $\mathrm{reg}(A) \leq \max\{\mathrm{reg}(B), \mathrm{reg}(C)+1\}$.
(b) $\mathrm{reg}(B) \leq \max\{\mathrm{reg}(A), \mathrm{reg}(C)\}$.
(c) $\mathrm{reg}(C) \leq \max\{\mathrm{reg}(A)-1, \mathrm{reg}(B)\}$.
(d) If A has finite length (i.e., A is both Noetherian and Artinian module), then $\mathrm{reg}(B) = \max\{\mathrm{reg}(A), \mathrm{reg}(C)\}$.

• One of the main use of a graded minimal free resolution is that one can compute the Hilbert function of M using the additivity property; i.e.,

$$HF(M,a) = \sum_{i=0}^{p} (-1)^i HF(\mathbf{F}_i, a).$$

Our focus will be on $M = R/I$, where I is a homogeneous ideal of $R = \mathbb{K}[x_1, \ldots, x_k]$.

• R/I is called *(arithmetically) Cohen-Macaulay* if $\mathrm{pdim}(R/I) = \mathrm{ht}(I)$. In general, we have $\mathrm{pdim}(R/I) \geq \mathrm{ht}(I)$. If R/I is Cohen-Macaulay, then $\mathrm{reg}(R/I)$ equals the smallest integer r such that $HF(R/I, i) = HP(R/I, i)$, for all $i \geq r$; this r is called *the regularity index of* R/I.

R/I is called *(arithmetically) Gorenstein* if R/I is Cohen-Macaulay and the rank of the last free module in the graded minimal free resolution of R/I is 1.

• If I is the defining ideal of a fat-points scheme, then R/I is Cohen-Macaulay.

If I is a complete intersection ideal, then R/I is Gorenstein. Furthermore, if $I = \langle f_1, \ldots, f_n \rangle$, with $\mathrm{ht}(I) = n$, and $\deg(f_i) = d_i \geq 1$, then $\mathrm{reg}(R/I) = \sum_{i=1}^{n} (d_i - 1)$. Also, $\deg(R/I) = d_1 \cdots d_n$, and R/I has the graded minimal free resolution (given by the Koszul complex) $\mathbf{F}_\bullet \twoheadrightarrow R/I$, with

$$\mathbf{F}_0 = R \text{ and } \mathbf{F}_i = \bigoplus_{1 \leq j_1 < \cdots < j_i \leq n} R(-(d_{j_1} + \cdots + d_{j_i})), i = 1, \ldots, n.$$

• One of the most common way to obtain free resolutions is via *mapping cone*. Suppose $0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$ is a short exact sequence of $R-$modules. Suppose $\mathbf{F}_\bullet \twoheadrightarrow A$ and $\mathbf{G}_\bullet \twoheadrightarrow B$ are free resolutions. Then

$$\mathbf{F}_{\bullet -1} \oplus \mathbf{G}_\bullet \twoheadrightarrow C$$

is a free resolution (not minimal) of C, where $\mathbf{F}_{-1} := 0$.

A common short exact sequences is the following: if I is an ideal of R and if $f \in R_d$, then one has the short exact sequence of graded $R-$modules

$$0 \longrightarrow \frac{R(-d)}{I:f} \xrightarrow{\cdot f} \frac{R}{I} \longrightarrow \frac{R}{\langle I, f \rangle} \longrightarrow 0.$$

Mapping cone applied to this short exact sequence, together with induction, gives that if $\mathfrak{p}$ is a linear prime of height n, and if $a \geq 1$ is some integer, then $R/\mathfrak{p}^a$ has the graded minimal free resolution $\mathbf{F}_\bullet \twoheadrightarrow R/\mathfrak{p}^a$, where

$$\mathbf{F}_0 = R \text{ and } \mathbf{F}_i = R^{b_i}(-(a+i-1)), b_i = \binom{a+i-2}{a-1} \cdot \binom{n+a-1}{a+i-1}, i = 1, \ldots, n.$$

• A graded finitely generated $R-$module M is said to have *(α-)linear graded free resolution* if the graded minimal free resolution has the shape

$$0 \longrightarrow R^{b_p}(-(\alpha+p)) \longrightarrow \cdots \longrightarrow R^{b_1}(-(\alpha+1)) \longrightarrow R^{b_0}(-\alpha) \longrightarrow M \longrightarrow 0.$$

We say R/I *has linear graded free resolution*, if I has this property. We have the following:

(1) R/I has α-linear graded free resolution if and only if $\mathrm{reg}(R/I) = \alpha - 1$ and $I \subseteq \mathfrak{m}^\alpha$.
(2) If R/I has α-linear graded free resolution, then $I = I^{sat} \cap \mathfrak{m}^\alpha$.

• Next we do an example. Let $R = \mathbb{K}[x_1, x_2]$, and let $I = \langle x_1^2, x_1x_2, x_2^3\rangle$. We want to compute the graded minimal free resolution of R/I. The first couple of steps are natural:

$$\underbrace{R(-2) \oplus R(-2) \oplus R(-3)}_{\mathbf{F}_1} \stackrel{\phi_1}{\to} \underbrace{R}_{\mathbf{F}_0} \to R/I \to 0,$$

where $\phi_1(f_1, f_2, f_3) = f_1x_1^2 + f_2x_1x_2 + f_3x_2^3$. Observe that $Im(\phi_1) = I$, ensuring exactness at step 0. The shifts occurring in $\mathbf{F}_1$ ensure that ϕ_1 preserves the grading, i.e., it sends the degree 0 elements in each summand to a degree 0 in $\mathbf{F}_0$. For example, since $\deg(x_1^2) = 2$, what "degree" should f_1 have in order for $f_1x_1^2$ to have "degree" 0? The answer is that the "degree" of f_1 must be -2.

Let $(f_1, f_2, f_3) \in Ker(\phi_1)$; i.e., *a syzygy* on the generators of I. Then, $f_1x_1^2 + f_2x_1x_2 + f_3x_2^3 = 0$, which can be written as

$$x_1(f_1x_1 + f_2x_2) = x_2(-f_3x_2^2).$$

$\gcd(x_1, x_2) = 1$ gives

$$f_1x_1 + f_2x_2 = x_2g \text{ and } -f_3x_2^2 = x_1g \text{ for some } g \in R.$$

Using the same divisibility argument, we obtain $g = hx_2^2$ for some $h \in R$, and from this, there is another $h' \in R$ such that: $f_1 = x_2h', f_2 = x_2^2h - x_1h', f_3 = -x_1h$. So

$$(f_1, f_2, f_3) = h(0, x_2^2, -x_1) + h'(x_2, -x_1, 0),$$

leading to the next map in the free resolution to be

$$\phi_2 : \underbrace{R(-4) \oplus R(-3)}_{\mathbf{F}_2} \to \mathbf{F}_1,\ \phi_2(h, h') = (x_2h', x_2^2h - x_1h', -x_1h).$$

By the same token, since "the degree" of f_1 is -2, then "the degree" of h' must be -3, and since "the degree" of f_3 is -3, then "the degree" of h must be -4. To double-check, looking at "the degree" of f_2 we have indeed $-2 = 2 + (-4) = 1 + (-3)$.

It is not hard to see that $Ker(\phi_2) = \{(0, 0)\}$, hence we completed the graded minimal free resolution of R/I:

$$0 \to R(-4) \oplus R(-3) \to R(-2)^2 \oplus R(-3) \to R \to R/I \to 0.$$

From this we have $\mathrm{pdim}(R/I) = 2$ and $\mathrm{reg}(R/I) = \max\{0 - 0, 2 - 1, 2 - 1, 3 - 1, 4 - 2, 3 - 2\} = 2$.

Since $\sqrt{I} = \langle x_1, x_2\rangle =: \mathfrak{m}$, so I is $\mathfrak{m}$-primary, and $\mathrm{ht}(I) = \mathrm{ht}(\mathfrak{m}) = 2$. Therefore, R/I is Cohen-Macaulay and Artinian. Since $\mathrm{rank}(\mathbf{F}_2) \neq 1$, R/I is not Gorenstein.

i	0	1	2	3	$4 \cdots$
Basis for $(R/I)_i$	$\{\bar{1}\}$	$\{\bar{x}_1, \bar{x}_2\}$	$\{\bar{x}_2^2\}$	$\{\bar{0}\}$	$\{\bar{0}\} \cdots$
$HF(R/I, i)$	1	2	1	0	$0 \cdots$

The Hilbert polynomial is $HP(R/I, i) = 0$. From R/I being Artinian we have that R/I is a finite dimensional $\mathbb{K}$-vector space with basis $\{\bar{1}, \bar{x}_1, \bar{x}_2, \bar{x}_2^2\}$, and so $\deg(R/I) = 4$.

2.2.7. *Monomial orders.* Let $R = \mathbb{K}[x_1, \ldots, x_k]$ be the ring of polynomials (not necessarily homogeneous) with coefficients in a field $\mathbb{K}$. To a monomial $x_1^{u_1} \cdots x_k^{u_k}$ we associate its exponent vector $u = (u_1, \ldots, u_k)$, which is a k-tuple with nonnegative integer entries; also denote $|u| = u_1 + \cdots + u_k$, which is the degree of the monomial. *A monomial order* on R, denoted here $\prec$, is a total ordering on the exponent vectors with the properties: (1) for any exponent vector w, if $u \succ v$, then $u + w \succ v + w$, and (2) any nonempty subset of exponent vectors has a smallest element.

Classical examples of monomial orders are:

- *Lexicographic order*: $u \succ v$ if the leftmost nonzero entry of $u - v$ is positive.
- *Graded Lexicographic order*: $u \succ v$ if $|u| > |v|$, or $|u| = |v|$ and the leftmost nonzero entry of $u - v$ is positive.

- *Graded Reverse Lexicographic order*: $u \succ v$ if $|u| > |v|$, or $|u| = |v|$ and the rightmost nonzero entry of $u - v$ is negative.

A monomial $x_1^{u_1} \cdots x_k^{u_k}$ will be denoted simply x^u. If $f \in R$ is written as $f = \sum_{c_u \neq 0} c_u x^u, c_u \in \mathbb{K}$, we denote $\text{in}_\prec(f)$ to be the largest monomial (w.r.t. the monomial order $\prec$ chosen on R) x^u in this expression of f; this is called *the initial monomial of* f.

Division Algorithm: Let $f \in R$, and $\{f_1, \ldots, f_m\} \subset R$. Then $f = \sum_{i=1}^{m} a_i f_i + r$, where $a_i, r \in R$, and no monomial of r is divisible by any $\text{in}_\prec(f_i)$.

If $I \subset R$ is an ideal, *the initial ideal of* I is the ideal of R generated by the initial monomials of all the elements of I; this is denoted, $\text{in}_\prec(I)$. A subset $\{g_1, \ldots, g_m\}$ of the ideal I is called *a Gröbner basis for* I if $\text{in}_\prec(I) = \langle \text{in}_\prec(g_1), \ldots, \text{in}_\prec(g_m) \rangle$. A Gröbner basis is a generating set for I, but the converse is not true; the Buchberger Algorithm is able to produce a Gröbner basis from a generating set.

If I is a homogeneous ideal in R, and if $\prec$ is a monomial order on R, then R/I and $R/\text{in}_\prec(I)$ have the same Hilbert functions. Monomial ideals are very well understood (see [128]), and as is the case of the theorem that we just mentioned, a lot of study on homogeneous ideals is transferred to their much friendlier relatives, their initial ideals. Also, in terms of computational feasibility, almost everything we mentioned in the Commutative Algebra preliminaries has an implementation using Gröbner bases in a computer algebra system, such as Macaulay 2 ([53]); for more details see [105] and [23].

2.3. **Combinatorics.** In the preliminaries about the Combinatorics occurring in this book we will focus our attention mostly on simplicial complexes, matroids, and hyperplane arrangements, and we will use [88], [105], [95] and [94] as guidance.

2.3.1. *Simplicial Complexes. An* n*-simplex* on a finite (vertex) set V with $n+1$ elements is the set of all subsets of V. *A simplicial complex* Δ on a finite (vertex) set V is a set of subsets of V with the properties: (1) if $v \in V$, then $\{v\} \in \Delta$, and (2) if $\tau \in \Delta$ and $\sigma \subseteq \tau$, then $\sigma \in \Delta$. *The dimension of* Δ *is* d if d is the largest integer such that there is a d-simplex included in Δ. If $\tau \in \Delta$ and $|\tau| = i + 1$, then τ is called an i*-face* of Δ.

An *oriented simplex* is a simplex with an ordering of its vertices; two orientations are equivalent if they differ by an even permutation of its vertices. Given a ring A, define A-modules C_i with generators the oriented i-simplices (plural of "simplex") of Δ subject to the relations $\{v_{j_0}, \ldots, v_{j_i}\} = (-1)^{sgn(p)}\{v_{j_{p(0)}}, \ldots, v_{j_{p(i)}}\}$, where p is a permutation of the set $\{0, \ldots, i\}$. So C_i is a free A-module of rank f_i, the number of i-faces of Δ. For $i > \dim(\Delta)$ and $i < -1$, by convention, $C_i = 0$, and C_{-1} is a free module of rank 1 corresponding to the empty face.

Define a map $\partial_i : C_i \to C_{i-1}$ by extending via linearity the definition of ∂_i on oriented i-simplices:

$$\partial_i(\{v_{j_0}, \ldots, v_{j_i}\}) = \sum_{u=0}^{i} (-1)^u \{v_{j_0}, \ldots, \widehat{v_{j_u}}, \ldots, v_{j_i}\}.$$

Because $\partial_i \circ \partial_{i+1} = 0$, we have a chain complex whose homology (called *reduced homology with coefficients in* A) is $\widetilde{H}_i(\Delta) := Ker(\partial_i)/Im(\partial_{i+1})$. For $i \geq 1$, the rank of $\widetilde{H}_i(\Delta)$ is called *the* i*-th Betti number of* Δ; they are very important topological invariants of the geometric realization of Δ. Also, $\text{rank}(\widetilde{H}_0(\Delta)) + 1$ equals the number of connected components of Δ.

Given a simplicial complex Δ on a vertex set $V = \{x_1, \ldots, x_n\}$, one can associate *the Stanley-Reisner ring*, $\mathbb{K}[\Delta] := \mathbb{K}[x_1, \ldots, x_n]/I_\Delta$, where I_Δ is the ideal of $R := \mathbb{K}[x_1, \ldots, x_n]$ generated by the (squarefree) monomials corresponding to the nonfaces of Δ (for example, $x_1x_2x_4 \in I_\Delta$ iff $\{x_1, x_2, x_4\} \notin \Delta$). Since any subset of V that contains a nonface is itself a nonface, one can reduce the number of generators of I_Δ by looking only for "minimal" nonfaces of Δ.

The *f-vector* of a d-dimensional simplicial complex is the vector $(f_{-1} := 1, f_0, f_1, \ldots, f_d)$, where f_i is the number of i-faces of Δ. The Hilbert polynomial of the Stanley-Reisner ring of a d-dimensional simplicial complex Δ is

$$HP(R/I_\Delta, i) = \sum_{j=0}^{d} f_j \binom{i-1}{j}.$$

Let Δ be a simplicial complex on $V = \{x_1, \ldots, x_n\}$. *A maximal face* of Δ is a face $\tau \in \Delta$ such that $\tau \cup \{x\}$ is a nonface, for any $x \in V \setminus \tau$. *A minimal coface* of Δ is the complement (in V) of a maximal face of Δ. With these, a primary decomposition of the Stanley-Reisner ideal is

$$I_\Delta = \bigcap_{\{x_{j_1}, \ldots, x_{j_i}\} \text{ minimal coface of } \Delta} \langle x_{j_1}, \ldots, x_{j_i} \rangle.$$

If Δ is a simplicial complex on $V = \{x_1, \ldots, x_n\}$, and $\tau \in \Delta$ is a face, then one can define *the link of* τ to be the simplicial subcomplex of Δ, $\mathrm{link}(\tau) := \{\sigma \in \Delta | \sigma \cap \tau = \emptyset, \sigma \cup \tau \in \Delta\}$. Then, the Stanley-Reisner ring is Cohen-Macaulay iff for each $\tau \in \Delta$ and each $i < \dim(\mathrm{link}(\tau))$, one has $\widetilde{H}_i(\mathrm{link}(\tau)) = 0$, the relative homology with coefficients in $\mathbb{K}$. In this case we say that the simplicial complex Δ is *Cohen-Macaulay*.

If Δ is a simplicial complex on a vertex set V, its *Alexander dual*, Δ^*, is the simplicial complex on V consisting of the complements of the nonfaces of Δ. It turns out that Δ is Cohen-Macaulay iff I_{Δ^*} has linear graded free resolution (or, as we said previously "the Stanley-Reisner ring of Δ^* has linear graded free resolution").

A simplicial complex Δ is called *pure* if all its maximal faces have the same dimension. If a simplicial complex is pure and it has a "shelling" (which is a particular way on how the maximal faces glue), then it is called *shellable*. A shellable simplicial complex is Cohen-Macaulay.

2.3.2. *Matroids.* A *matroid* M is an ordered pair $(E, \mathcal{I})$ consisting of a finite set E (called *ground set*), and a collection $\mathcal{I}$ of subsets of E satisfying the properties: (1) $\emptyset \in \mathcal{I}$, (2) if $I \in \mathcal{I}$ and $I' \subseteq I$, then $I' \in \mathcal{I}$, and (3) if $I_1, I_2 \in \mathcal{I}$ and $|I_1| < |I_2|$, then there is an element $e \in I_2 \setminus I_1$, such that $I_1 \cup \{e\} \in \mathcal{I}$. The members of $\mathcal{I}$ are called *the independent sets* of M. A subset $J \notin \mathcal{I}$ is called *dependent*.

Let $M = (E, \mathcal{I})$ be a matroid. A minimal dependent set (i.e., a dependent set with all its strict subsets being independent) is called *a circuit* of M. Property (2) above allows us to construct a simplicial complex Δ, whose faces are the independent sets of M. Therefore, if $E = \{1, \ldots, n\}$, the Stanley-Reisner ideal of Δ, $I_\Delta \subset \mathbb{K}[x_1, \ldots, x_n]$ is generated by $x_{i_1} \cdots x_{i_j}$, where $\{i_1, \ldots, i_j\} \subset E$ is a circuit of M. It turns out that Δ is shellable, and therefore it is Cohen-Macaulay.

The following is the standard example of a matroid, that we will also use throughout the book (and where the above terminology comes from): Let A be an $k \times n$ matrix with entries in a field $\mathbb{K}$ (e.g., a generating matrix for an $[n, k]$-linear code). Let $E = \{1, \ldots, n\}$, and say that $I = \{i_1, \ldots, i_j\} \subseteq E$ is an element of $\mathcal{I}$ if the columns of the matrix A indexed by the elements of I are linearly independent vectors in $\mathbb{K}^k$. With these, $(E, \mathcal{I})$ is a matroid.

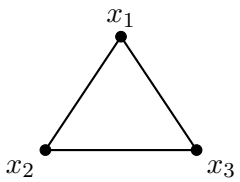
Suppose M is the matroid of a $k \times n$ matrix A of rank k. For any subset $I \subseteq E = \{1, \ldots, n\}$, let $r(I)$ be the dimension of the subspace of $\mathbb{K}^k$ spanned by the columns of A indexed by I (this is an example of a "rank function" on a matroid M). By definition, *the Tutte polynomial* of M is

$$T_M(x, y) = \sum_{I \subseteq E} (x-1)^{k-r(I)} (y-1)^{|I|-r(I)}.$$

Let's look at a simple example. Let

$$A = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}.$$

So $M = (E, \mathcal{I})$ with $E = \{1, 2, 3\}$ and $\mathcal{I} = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}\}$. Δ is the empty triangle



The only circuit is $\{1,2,3\}$, so $\{x_1,x_2,x_3\}$ is the only nonface of Δ, and so $I_\Delta = \langle x_1x_2x_3\rangle$. Or we can see that the maximal faces are the edges $\{x_1,x_2\},\{x_1,x_3\},\{x_2,x_3\}$, and hence the minimal cofaces are $\{x_3\},\{x_2\},\{x_1\}$, giving the primary decomposition $I_\Delta = \langle x_3\rangle \cap \langle x_2\rangle \cap \langle x_1\rangle = \langle x_1x_2x_3\rangle$. So, the Stanley-Reisner ring is $\mathbb{K}[\Delta] = \mathbb{K}[x_1,x_2,x_3]/\langle x_1x_2x_3\rangle$. Since I_Δ is a principal ideal, it is a complete intersection, and hence Δ is Cohen-Macaulay (confirming the results in this section).

The Tutte polynomial is equal to

$$\begin{aligned} T_M(x,y) &= \underbrace{(x-1)^{2-0}(y-1)^{0-0}}_{\emptyset} + 3\underbrace{(x-1)^{2-1}(y-1)^{1-1}}_{\{i\}} + 3\underbrace{(x-1)^{2-2}(y-1)^{2-2}}_{\{i,j\}} \\ &\quad + \underbrace{(x-1)^{2-2}(y-1)^{3-2}}_{\{1,2,3\}} \\ &= x^2+x+y, \end{aligned}$$

2.3.3. *Hyperplane arrangements.* Let $\mathcal{A} = \{H_1,\dots,H_n\}$ be a central essential hyperplane arrangement in V a vector space of dimension k over $\mathbb{K}$ a field of characteristic zero. "Central" means that each H_i is a linear subspace of dimension $k-1$ of V. The *rank* of $\mathcal{A}$, denoted $r(\mathcal{A})$, is defined to be the codimension of the vector subspace $H_1\cap\cdots\cap H_n$. "Essential" means that $r(\mathcal{A}) = k$. Throughout these notes, all hyperplane arrangements are assumed to central and essential.

A *flat* Y is any element of the intersection lattice, denoted $L(\mathcal{A})$, of $\mathcal{A}$; i.e., $Y = H_{i_1}\cap\cdots\cap H_{i_s}$, for some $H_{i_1},\dots,H_{i_s}\in\mathcal{A}$. The *closure* of a flat $Y\in L(\mathcal{A})$ is the subset of hyperplanes $cl(Y) := \{H\in\mathcal{A} | Y\subseteq H\} =: \mathcal{A}_Y$. The *rank* of Y is defined to be $r(Y) := r(\mathcal{A}_Y)$. The rank one flats are the hyperplanes of $\mathcal{A}$, and they are called *atoms*.

The *Möbius function* is the function $\mu : L(\mathcal{A}) \to \mathbb{Z}$ defined as

$$\mu(Y) = \begin{cases} 1, & \text{if } Y = V; \\ -\displaystyle\sum_{Z\in L(\mathcal{A}), Z\supsetneq Y} \mu(Z), & \text{if } Y\subsetneq V. \end{cases}$$

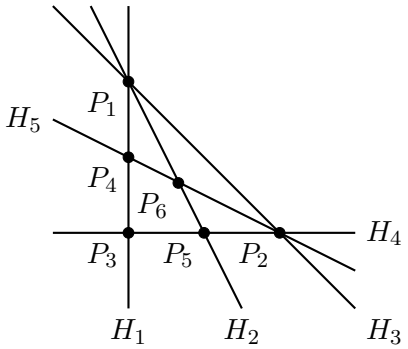
The characteristic polynomial of $\mathcal{A}$ is defined to be

$$\chi(\mathcal{A},t) = \sum_{Y\in L(\mathcal{A})} \mu(Y)t^{r(\mathcal{A})-r(Y)}.$$

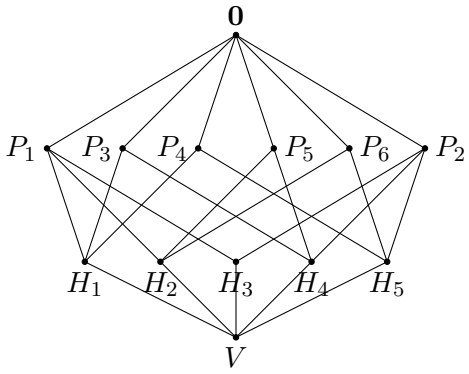
Let $R := Sym(V^*) = \mathbb{K}[x_1,\dots,x_k]$ and fix $\ell_i\in R, i=1,\dots,n$ the linear forms defining the hyperplanes of $\mathcal{A}$ (i.e., $H_i = V(\ell_i), i=1,\dots,n$); for our setup, the linear forms are mutually nonproportional (so we do not consider "multiarrangements"). The *matroid of* $\mathcal{A}$, denoted $M(\mathcal{A})$, is the matroid of the matrix of coefficients of the defining linear forms. The Tutte polynomial and the characteristic polynomial satisfy

$$\chi(\mathcal{A},t) = (-1)^{r(\mathcal{A})}T_{M(\mathcal{A})}(1-t,0).$$

Example 2.1. Consider $\mathcal{A} = \{H_1 = V(x), H_2 = V(x-z), H_3 = V(z), H_4 = V(y), H_5 = V(y-z)\} \subset \mathbb{P}^2$. We have $r(\mathcal{A}) = 3$ and the (affine) picture below (we also labeled the intersection points $P_1,\dots,P_6$, as they are rank two elements of $L(\mathcal{A})$).



The lattice of intersection has the following *Hasse diagram*:



The ranks and the Möbius function values of the elements of $L(\mathcal{A})$ are presented in the following table.

$Y \in L(\mathcal{A})$	V	H_1	H_2	H_3	H_4	H_5	P_1	P_2	P_3	P_4	P_5	P_6	$\mathbf{0}$
$r(Y)$	0	1	1	1	1	1	2	2	2	2	2	2	3
$\mu(Y)$	1	-1	-1	-1	-1	-1	2	2	1	1	1	1	-4

So the characteristic polynomial is $\chi(\mathcal{A}, t) = t^3 - 5t^2 + 8t - 4$.

The Tutte polynomial of the matroid of the coefficients matrix $\begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & -1 & 1 & 0 & -1 \end{pmatrix}$ is $T_{M(\mathcal{A})}(x, y) = x^3+2x^2+2xy+y^2+x+y$, and indeed $(-1)^3 T_{M(\mathcal{A})}(1-t, 0) = t^3-5t^2+8t-4 = \chi(\mathcal{A}, t)$.

• Suppose again that we fixed $\ell_i \in R = \mathbb{K}[x_1, \ldots, x_k], i = 1, \ldots, n$ the linear forms defining the hyperplanes of $\mathcal{A}$. After a change of coordinates, assume that $\ell_i = x_i, i = 1, \ldots, k$.

Let $\mathrm{Der}(R)$ be the set of $\mathbb{K}$-linear maps $\theta : R \longrightarrow R$ that satisfy the product rule; i.e., $\theta(f \cdot g) = f \cdot \theta(g) + g \cdot \theta(f)$, for all $f, g \in R$. A *logarithmic derivation* of $\mathcal{A}$ is an element $\theta \in \mathrm{Der}(R)$, such that $\theta(\ell_i) \in \langle \ell_i \rangle$, for all $i = 1, \ldots, n$. Picking the standard basis for $\mathrm{Der}(R)$, i.e., $\partial_1 := \partial/\partial x_1, \ldots, \partial_k := \partial/\partial x_k$, if θ is written as $\theta = \sum_{i=1}^{k} P_i \partial_i$, where $P_i \in R$ are homogeneous polynomials of the same degree, then we can define $\deg(\theta) := \deg(P_i)$.

The set of logarithmic derivations forms an R-module, often denoted $D(\mathcal{A})$, and whenever this module is free (of rank k) one says that the hyperplane arrangement is *free*. For a free arrangement, the degrees of the basis elements of $D(\mathcal{A})$ are called the *exponents* of $\mathcal{A}$, denoted $\exp(\mathcal{A}) := (1, d_2, \ldots, d_k)$. The exponent 1 is explained as follows: in general, every central hyperplane arrangement has *the Euler derivation* $\theta_E = x_1\partial_1 + \cdots + x_k\partial_k$, and for every central hyperplane arrangement, $\langle \theta_E \rangle := \theta_E \cdot R$ is a direct summand of $D(\mathcal{A})$:

$$D(\mathcal{A}) = \langle \theta_E \rangle \oplus D_0(\mathcal{A}),$$

where $D_0(\mathcal{A})$ is a submodule of $D(\mathcal{A})$ isomorphic to $D(\mathcal{A})/\langle\theta_E\rangle$.

(a) A flat $X \in L(\mathcal{A})$ is said to be *modular* if $X + Y \in L(\mathcal{A})$ for all flats $Y \in L(\mathcal{A})$. A central essential hyperplane arrangement $\mathcal{A}$ of rank k is called *supersolvable* if $L(\mathcal{A})$ has a maximal chain of modular elements: $V = X_0 < X_1 < \cdots < X_k = \mathbf{0}$, where $<$ is the reverse inclusion. Every supersolvable arrangement is free, and there is a "nice partition" of $\mathcal{A}$ (see [94, Proposition 2.67]) which determines the exponents of $\mathcal{A}$ (see [94, Theorem 4.58]).

(b) An important result in the theory of hyperplane arrangements is Terao's Factorization Theorem ([94, Theorem 4.61]), which says that if $\mathcal{A}$ is free with exponents $(1, d_2, \ldots, d_k)$, then $\chi(\mathcal{A}, t) = (t-1)(t-d_2)\cdots(t-d_k)$.

(c) Terao's Conjecture: "freeness is a combinatorial condition"; i.e., given two hyperplane arrangements with isomorphic intersection lattices, if one is free, so is the other.

Free arrangements make the connection between the combinatorics and the commutative algebra of a hyperplane arrangement. With our fixed $\ell_1, \ldots, \ell_n \in R$, we can define the *defining polynomial of* $\mathcal{A}$, $Q(\mathcal{A}) := \ell_1 \cdots \ell_n$, and the *Jacobian ideal of* $\mathcal{A}$, $J_{Q(\mathcal{A})} := \langle \partial_1 Q(\mathcal{A}), \ldots, \partial_k Q(\mathcal{A})\rangle \subset R$, the ideal generated by the first partial derivatives of the defining polynomial. $J_{Q(\mathcal{A})} \subset \langle \ell_i, \ell_j\rangle$, for any $i \neq j$, and since the $r(\mathcal{A}) = k \geq 2$, we have $\mathrm{ht}(J_{Q(\mathcal{A})}) = 2$.

(i) $D_0(\mathcal{A})$ is isomorphic to the first syzygy module of $J_{Q(\mathcal{A})}$.

(ii) $J_{Q(\mathcal{A})} \subset \langle \ell_i, \ell_j\rangle$, for any $i \neq j$, and since the $r(\mathcal{A}) = k \geq 2$, we have $\mathrm{ht}(J_{Q(\mathcal{A})}) = 2$. So $\mathcal{A}$ is free if and only if $\mathrm{pdim}(R/J_{Q(\mathcal{A})}) = 2$ (i.e., if and only if $R/J_{Q(\mathcal{A})}$ is Cohen-Macaulay).

(iii) The hyperplane arrangement in Example 2.1 is free, because it is supersolvable: $V < H_1 < P_1 < \mathbf{0}$ is a maximal chain of modular flats. We can also see this by observing that we have the minimal graded free resolution

$$0 \to R^2(-6) \to R^3(-4) \to R \to R/J_{Q(\mathcal{A})} \to 0.$$

Also, the degrees of the syzygies give the exponents $\exp(\mathcal{A}) = (1, \underbrace{2}_{6-4}, \underbrace{2}_{6-4})$, and we can see that $\chi(\mathcal{A}, t) = (t-1)(t-2)^2$.

3. IDEALS GENERATED BY FOLD PRODUCTS OF LINEAR FORMS

In this chapter the main idea to study a linear code with generating matrix G is to analyze properties of the linear forms dual to the columns of G. Let $\mathcal{C}$ be a linear code (i.e., the image of a linear map $\phi : \mathbb{K}^k \to \mathbb{K}^n$), and let

$$G = \begin{pmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & & \vdots \\ a_{k,1} & \cdots & a_{k,n} \end{pmatrix}$$

be a generating matrix. Suppose that none of the columns of G is the zero column vector in $\mathbb{K}^k$.

Then $\mathbf{w} = (w_1, \ldots, w_n) \in \mathcal{C}$ if and only if there exists $\mathbf{v} = (v_1, \ldots, v_k) \in \mathbb{K}^k$ such that $\phi(\mathbf{v}) = \mathbf{w}$, i.e. $(v_1, \ldots, v_k)G = (w_1, \ldots, w_n)$. This means that for all $j = 1, \ldots, n$, $a_{1,j}v_1 + \cdots + a_{k,j}v_k = w_j$. Furthermore, geometrically this translates into: for all $j = 1, \ldots, n$, the hyperplane of $\mathbb{K}^k$ of equation $a_{1,j}x_1 + \cdots + a_{k,j}x_k = w_j$, passes through the point of coordinates $(v_1, \ldots, v_k)$.

For $i = 1, \ldots, n$, we will denote $\ell_i := a_{1,i}x_1 + \cdots + a_{k,i}x_k$, the nonzero homogeneous linear form in $R := \mathbb{K}[x_1, \ldots, x_k]$, the ring of (homogeneous) polynomials with coefficients in $\mathbb{K}$. Observe that for each $i = 1, \ldots, n$, ℓ_i is the linear form dual to the i-th column of G. The linear forms $\ell_1, \ldots, \ell_n$ will be called *the defining linear forms for the linear code* $\mathcal{C}$. Sometimes we will denote this as $\mathcal{C} = (\ell_1, \ldots, \ell_n)$.

Note that if one multiplies a column of G by a nonzero scalar, the "structure" of $\mathcal{C}$ doesn't change. Same happens if one permutes the columns of G. In both instances, one obtains an equivalent code (see Section 2.1). So for the theoretical purposes this allows as to choose one equation for each dual linear form, and to list them regardless of the order of the columns in the matrix G; we will assume that the first linear form listed is dual to the first column of G, the second is dual to the second column of G, and so forth. In practice though, the order matters to great extent: for example, locating which entries of the received message contains an error it is crucial for the error-correction process.

Lemma 3.1. *Let $\mathcal{C}$ be a linear code, and let $\ell_1, \ldots, \ell_n$ be its defining linear forms. Then* $\dim(\mathcal{C}) = \dim_{\mathbb{F}} \operatorname{Span}\{\ell_1, \ldots, \ell_n\}$.

Proof. The dimension of $\mathcal{C}$ equals the rank of G, which in turn is the dimension of the column space of G. Via duality, we obtain the result. □

Remark 3.2. The linear code $\mathcal{C}$ is the subspace of $\mathbb{K}^n$ spanned by the rows of G. After a row reduction (i.e. multiplying G on the left by an invertible $k \times k$ matrix), we can assume that the first $\dim(\mathcal{C})$ rows contain pivot positions and the last $k - \dim(\mathcal{C})$ are rows of zeros. By this calculation we can assume that $\dim(\mathcal{C}) = k$, or that the rank of the $k \times n$ generating matrix is $k \leq n$. This assumption will be made for the entire chapter.

3.1. The De Boer - Pellikaan method for computing minimum distance.

Let $\mathbb{K}$ be a field and suppose $\mathbf{w} = (w_1, \ldots, w_n)$ is a vector in $\mathbb{K}^n$. We start with a lemma about the weight of $\mathbf{w}$.

Lemma 3.3. *Let $\mathbf{w} \in \mathbb{K}^n \setminus \{\mathbf{0}\}$, and let e be an integer with $1 \leq e \leq n$. Then $wt(\mathbf{w}) = e$ if and only if all $e+1$ fold products of the entries of $\mathbf{w}$ are 0, and there exists one product of e entries that is different than 0.*

Proof. $wt(\mathbf{w}) = e$ if and only if there exists $i_1, \ldots, i_e \in \{1, \ldots, n\}, i_a \neq i_b$ if $a \neq b$, such that $w_{i_c} \neq 0$, for $c = 1, \ldots, e$, and $w_j = 0$, for all $j \in \{1, \ldots, n\} \setminus \{i_1, \ldots, i_e\}$.

The result becomes clear since any $e+1$ of the entries of $\mathbf{w}$ will contain a 0, and since $w_{i_1} \cdots w_{i_e} \neq 0$. □

Suppose $\mathcal{C}$ is a linear code defined by the linear forms $\ell_1, \ldots, \ell_n$. Similarly, the weight of a nonzero codeword is described in the following lemma.

Lemma 3.4. *With the above notations, there exists $\mathbf{w} \in \mathcal{C} \setminus \{\mathbf{0}\}$ with $wt(\mathbf{w}) = e$ if and only if for all $1 \leq i_1 < \cdots < i_{e+1} \leq n$ the equations $\ell_{i_1} \cdots \ell_{i_{e+1}} = 0$ have a common nontrivial solution $(v_1, \ldots, v_k)$, and there exists $j_1, \ldots, j_e \in \{1, \ldots, n\}, j_a \neq j_b$ if $a \neq b$, such that $\ell_{j_1} \cdots \ell_{j_e}|_{(v_1, \ldots, v_k)} \neq 0$.*

Proof. The "$\Rightarrow$" implication is straightforward from Lemma 3.3.

For the "$\Leftarrow$" implication, define $\mathbf{w} := (\ell_1(v_1, \ldots, v_k), \ldots, \ell_n(v_1, \ldots, v_k))$, which, again by Lemma 3.3 has $wt(\mathbf{w}) = e$. □

The following is the key result of this chapter, and it is due to De Boer - Pellikaan ([25]):

Theorem 3.5. *Let $\mathcal{C}$ be a linear code with defining linear forms $\ell_1, \ldots, \ell_n \in R$. Then, the minimum distance of $\mathcal{C}$ is the smallest integer $d \geq 1$ such that the system of equations $\ell_{i_1} \cdots \ell_{i_{d+1}} = 0$, for all $1 \leq i_1 < \cdots < i_{d+1} \leq n$, has a common nontrivial solution.*

Proof. The proof is immediate from Lemma 3.4. □

As it is the main topic of this book, we will look at this result from a commutative algebraic point of view. Let $\mathcal{C}$ be a linear code with generating $k \times n$ matrix G, that has no zero columns. Let $\ell_1, \ldots, \ell_n \in R := \mathbb{K}[x_1, \ldots, x_k]$ be the linear forms dual to the columns of G (i.e., the defining linear forms). For each integer $a \in \{1, \ldots, n\}$ define the ideal of R

$$I_a(\mathcal{C}) := \langle \{\ell_{i_1} \cdots \ell_{i_a} | 1 \leq i_1 < \cdots < i_a \leq n\} \rangle,$$

the *ideal generated by a-fold products of linear forms defining $\mathcal{C}$*. The generators listed in the above set will be called *standard generators*. Sometimes, we denote $I_a(\mathcal{C})$ as $I_a(\ell_1 \ell_2 \cdots \ell_n)$. We have the natural inclusions of ideals

$$I_1(\mathcal{C}) = \langle \ell_1, \ldots, \ell_n \rangle \supset I_2(\mathcal{C}) \supset \cdots \supset I_{n-1}(\mathcal{C}) \supset I_n(\mathcal{C}) = \langle \ell_1 \cdots \ell_n \rangle.$$

By convention, $I_0(\mathcal{C}) = R$ and $I_{n+1}(\mathcal{C}) = 0$.

The first properties of these ideals are presented in the following two lemmas.

Lemma 3.6. *Let $\mathfrak{p} \subset R$ be a prime ideal. The $\mathfrak{p} \supset I_a(\mathcal{C})$ if and only if $\mathfrak{p}$ contains $n - a + 1$ of the linear forms defining $\mathcal{C}$.*

Proof. Let $\mathfrak{p}$ be a prime ideal that contains $I_a(\mathcal{C})$. Then $\ell_1 \ell_2 \cdots \ell_a \in \mathfrak{p}$. So at least one of its factors, say ℓ_1, belongs to $\mathfrak{p}$. Next we have $\ell_2 \cdots \ell_{a+1} \in \mathfrak{p}$. So we can assume $\ell_2 \in \mathfrak{p}$. So forth to the last generator $\ell_{n-a+1} \cdots \ell_n \in \mathfrak{p}$, which has a factor, say ℓ_{n-a+1}, in $\mathfrak{p}$. This way we obtained that the linear prime ideal $\langle \ell_1, \ldots, \ell_{n-a+1} \rangle$ is included in $\mathfrak{p}$.

For the converse, suppose $\{\ell_{j_1}, \ldots, \ell_{j_{n-a+1}}\} \subseteq \mathfrak{p}$, for some $1 \leq j_1 < \cdots < j_{n-a+1} \leq n$. Since every standard generator of $I_a(\mathcal{C})$ will have an ℓ_{j_a} as a factor, we obtain $I_a(\mathcal{C}) \subset \langle \ell_{j_1}, \ldots, \ell_{j_{n-a+1}} \rangle \subseteq \mathfrak{p}$. □

Corollary 3.7. *Let $\mathcal{C}$ be a linear code and let $1 \leq a \leq n$ be an integer. Then*

$$\mathrm{ht}(I_a(\mathcal{C})) = \min\{\dim \mathrm{Span}_{\mathbb{K}}\{\ell_{i_1}, \ldots, \ell_{i_{n-a+1}}\} | 1 \leq i_1 < \cdots < i_{n-a+1} \leq n\}.$$

Proof. The height of an ideal equals the minimum of the heights of its minimal primes. Let $\mathfrak{p}$ be a minimal prime of $I_a(\mathcal{C})$. From Lemma 3.6, there exists indices $1 \leq i_1 < \cdots < i_{n-a+1} \leq n$ such that

$$I_a(\mathcal{C}) \subset \langle \ell_{i_1}, \ldots, \ell_{i_{n-a+1}} \rangle \subseteq \mathfrak{p}.$$

Since $\langle \ell_{i_1}, \ldots, \ell_{i_{n-a+1}} \rangle$ is a prime ideal containing $I_a(\mathcal{C})$, and since $\mathfrak{p}$ is a minimal prime of $I_a(\mathcal{C})$, then they must be equal. Therefore

$$\mathrm{ht}(\mathfrak{p}) = \mathrm{ht}(\langle \ell_{i_1}, \ldots, \ell_{i_{n-a+1}} \rangle) = \dim \mathrm{Span}_{\mathbb{K}}\{\ell_{i_1}, \ldots, \ell_{i_{n-a+1}}\}.$$

By Lemma 3.6, any linear prime of the form $\langle \ell_{j_1}, \ldots, \ell_{j_{n-a+1}} \rangle$ contains $I_a(\mathcal{C})$. If this is not a minimal prime, then it will contain a minimal prime $\mathfrak{p}$ of $I_a(\mathcal{C})$, and as we have seen above, this is also a linear prime generated by $n - a + 1$ linear forms defining $\mathcal{C}$. The height of $\mathfrak{p}$ is the dimension of the space spanned by these $n - a + 1$ linear forms. This concludes the proof. □

With this in mind, the De Boer-Pellikaan theorem translates to the following

Let $\mathcal{C}$ be an $[n,k]$-linear code with generating matrix G a $k \times n$ of rank k. So $\mathcal{C} = Im(\phi_G)$, where $\phi_G : \mathbb{K}^k \to \mathbb{K}^n$ is the multiplication by G. Let $\mathcal{D} \subseteq \mathcal{C}$ be a subcode. Recall that the support of $\mathcal{D}$ is

$$Supp(\mathcal{D}) := \{i : \exists (y_1, \ldots, y_n) \in \mathcal{D} \text{ with } y_i \neq 0\}.$$

Let $m(\mathcal{D}) := |Supp(\mathcal{D})|$ be the cardinality of the support of $\mathcal{D}$.

Let $V_{\mathcal{D}} := \phi_G^{-1}(\mathcal{D})$ be the corresponding linear subspace of $\mathbb{K}^k$, the preimage of $\mathcal{D}$ under the injective linear map ϕ_G.

Suppose $\ell_1, \ldots, \ell_n \in R := \mathbb{K}[x_1, \ldots, x_k]$ are the defining linear forms of $\mathcal{C}$. If $m(\mathcal{D}) = s$, then all the elements of $\mathcal{D}$ have the same $n - s$ components $i_1, \ldots, i_{n-s} \in \{1, \ldots, n\}$ equal to zero. So, $V_{\mathcal{D}} \subseteq V(\ell_{i_1}, \ldots, \ell_{i_{n-s}})$, the common zero locus of these linear forms, and therefore, in terms of defining ideals in R,

$$\langle \ell_{i_1}, \ldots, \ell_{i_{n-s}} \rangle \subseteq I(V_{\mathcal{D}}).$$

Let $V_1, \ldots, V_m$ be the components of an essential subspace arrangement V as above, and let $\Lambda = \{\ell_1, \ldots, \ell_n\}$ be the set of linear forms from the proof of Theorem 3.33. Let $\mathcal{C}_\Lambda$ be the $[n,k]$-linear code with defining linear forms Λ, with generating matrix G_Λ, a rank k matrix of size $k \times n$.

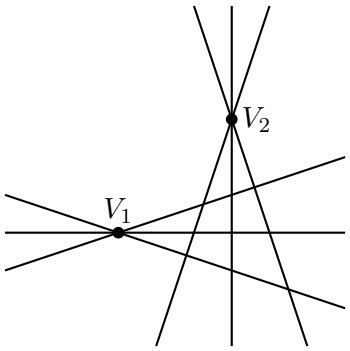
For each $i \in \{1, \ldots, m\}$, we have V_i defined by Λ_i, and let $\mathcal{D}_i := \phi_{G_\Lambda}(V_i)$. These are subcodes of $\mathcal{C}_\Lambda$ of support size $m(\mathcal{D}_i) \leq |\Lambda| - |\Lambda_i| = n - \aleph = a - 1$; we have inequality because it may be possible that we have chosen an $\ell \in \Lambda_j \setminus \Lambda_i, j \neq i$, yet $\ell(V_i) = 0$.

Let $\mathcal{D}$ be some nonzero subcode of support size $s \leq a - 1$. Then, as we have seen before, $\langle \ell_{i_1}, \ldots, \ell_{i_{n-s}} \rangle \subseteq I(V_{\mathcal{D}})$, for some $\ell_{i_1}, \ldots, \ell_{i_{n-s}} \in \Lambda$. Since $s \leq a - 1$, then $n - s \geq n - a + 1$, and therefore, from the proof of Theorem 3.33, we have $I(V_{\mathcal{D}}) \supseteq I(V_{i_0})$, for some $i_0 \in \{1, \ldots, m\}$. Consequently, $V_{\mathcal{D}} \subseteq V_{i_0}$, and hence $\mathcal{D} \subseteq \mathcal{D}_{i_0}$. We just proved the following result.

Proposition 3.35. *With the notations and conditions of this section, we have that for $i \in \{1, \ldots, m\}$, $\phi_{G_\Lambda}(V_i)$ are the maximal subcodes of $\mathcal{C}_\Lambda$ of support size $\leq a - 1$.*

Remark 3.36. Suppose V is a union of points in $\mathbb{P}^{k-1}$; in other words, V_i with $i \in \{1, \ldots, m\}$ are one-dimensional linear subspaces of $\mathbb{K}^k$. Then $V_{\mathcal{D}}$ from above must equal V_{i_0}. This leads to the conclusion that for $i \in \{1, \ldots, m\}$, $\mathcal{D}_i$ are the equivalence classes (under nonzero scalar multiplication) of minimal codewords of weight $\leq a - 1$; see for comparison [113, Proposition 4.1].

Also, still under the assumption that V is a set of points, if in the proof of Theorem 3.33 we pick the Λ_i's such that for all $i \neq j$, if $\ell \in \Lambda_j \setminus \Lambda_i$, then $\ell \notin I(V_i)$ (see figure below for $m = 2$ points in $\mathbb{P}^2$), then as observed before, $m(\mathcal{D}_i) = a - 1$, and therefore $\mathcal{D}_i = \phi_{G_\Lambda}(V_i), i \in \{1, \ldots, m\}$ are precisely <u>all</u> the projective codewords of minimum weight of $\mathcal{C}_\Lambda$; the minimum weight (or distance) is $a - 1$.



3.5.1. *Interpolating fat points in $\mathbb{P}^{k-1}$.* As we have seen above in Remark 3.36, any set of points can be thought of corresponding to the projective codewords of minimum weight of a certain linear code: if $\Omega = \{P_1, \ldots, P_u\} \subset \mathbb{P}^{k-1}$ is a (reduced) finite set of points, then, for each $i = 1, \ldots, u$, pick a collection of k sufficiently general hyperplanes intersecting at P_i, sufficiently general meaning that any other subsets of k of these $n = ku$ hyperplanes will span $\mathbb{P}^{k-1}$. The $[n,k,d]$-linear code $\mathcal{C}$ defined by the equations of

these hyperplanes satisfies the required conditions, since $\nu_{\mathcal{C}}(I(P_i)) = k$ for all $i = 1, \ldots, u$, maximum possible, and hence, by Proposition 3.10, $d = ku - k = k(u-1)$; recall that $\nu_{\mathcal{C}}(\mathfrak{p})$, for a prime ideal $\mathfrak{p}$, is the number of defining linear forms of $\mathcal{C}$ that belong to $\mathfrak{p}$. By Corollary 3.16 (b), we have

$$(I_{d+1}(\mathcal{C}))^{sat} = I(\Omega),$$

which is a stronger statement than Theorem 3.33. Such a linear code we will call *an interpolating code for the set* Ω.

The problem with constructing such $\mathcal{C}$ is that n becomes very big (yet, d becomes also very big and so there are better chances to detect and correct errors); see the figure above. As [115, Section 2.2] explains, allowing proportional defining linear forms as well as exploiting the geometry of the points, one can construct more viable $\mathcal{C}$.

Remark 3.37. As explained in [115], for points in $\mathbb{P}^2$ a procedure to interpolate them that will lead to a more viable interpolating code is the following: suppose $\Omega = \{P_1, \ldots, P_u\} \subset \mathbb{P}^2$ is not all contained on a line. Suppose $\ell_1, \ldots, \ell_u \in R := \mathbb{K}[x, y, z]$ are the corresponding linear forms dual to the points of Ω.

By Proposition 3.26, with $h = 2$, the (irredundant) primary decomposition of $I_{u-1}(\ell_1 \cdots \ell_u$ is

$$I_{u-1}(\ell_1 \cdots \ell_u) = I(Q_1)^{m_1} \cap \cdots \cap I(Q_s)^{m_s},$$

where, for $j = 1, \ldots, s$, $I(Q_j)$ is the defining (linear prime) ideal of a point $Q_j \in \mathbb{P}^2$, and $m_j \geq 1$ are some integers.

Next we consider $\ell'_1, \ldots, \ell'_s \in R$, the linear forms dual to the points $Q_1, \ldots, Q_s$. Then, an interpolating code for Ω is

$$\mathcal{C} = (\underbrace{\ell'_1, \ldots, \ell'_1}_{m_1}, \ldots, \underbrace{\ell'_s, \ldots, \ell'_s}_{m_s}).$$

If all the points of Ω are contained on a line $V(\ell)$, then choose the interpolating code to be

$$\mathcal{C} = (\ell, \ell, \ell''_1, \ldots, \ell''_u),$$

where, for $i = 1, \ldots, u$, $V(\ell''_i)$ is a generic line passing through the point P_i.

Next we look at interpolating fat-points, while preserving their multiplicities. Let $Z := m_1P_1 + \cdots + m_uP_u \subset \mathbb{P}^{k-1}, m_i \geq 1$ be a reduced fat-points scheme; the defining ideal is

$$I(Z) = I(P_1)^{m_1} \cap \cdots \cap I(P_u)^{m_u} \subset R := \mathbb{K}[x_1, \ldots, x_k].$$

The (usual) set of points $\Omega := \{P_1, \ldots, P_u\} \subset \mathbb{P}^{k-1}$ is call the *support of* Z, often denoted $supp(Z)$.

The question we would like to answer is if we can interpolate Z with a linear code, i.e., if there exists $\mathcal{C}$ an $[n, k]$-linear code and an $1 \leq a \leq n$, such that $(I_a(\mathcal{C}))^{sat} = I(Z)$. The answer is yes.

Let $\mathcal{C}'$ be an interpolating code for $\Omega = supp(Z)$. Suppose the parameters of $\mathcal{C}'$ are $[n', k, d']$. So we have $(I_{d'+1}(\mathcal{C}'))^{sat} = I(\Omega) = I(P_1) \cap \cdots \cap I(P_u)$. Since d' is the minimum distance of $\mathcal{C}'$ and $P_1, \ldots, P_u$ are the points corresponding to the projective codewords of minimum weight of $\mathcal{C}'$, we have $\nu_{\mathcal{C}'}(I(P_i)) = n' - d'$, for any $i \in \{1, \ldots, u\}$.

For each $i = 1, \ldots, u$, we choose $\Theta_i := \{\ell_{i,1}, \ldots, \ell_{i,m_i}\}$ distinct linear forms in $I(P_i)$, that are sufficiently general/generic.

Define the linear code

$$\mathcal{C} = \mathcal{C}' \cup \left(\bigcup_{i=1}^{u} \Theta_i \right).$$

The block-length of $\mathcal{C}$ is $n = n' + (m_1 + \cdots + m_u)$, and the dimension is still k. Also $\nu_{\mathcal{C}}(I(P_i)) = \nu_{\mathcal{C}'}(I(P_i)) + m_i = n' - d' + m_i$, for $i = 1, \ldots, u$. All the other intersection points Q among the hyperplanes defined by the linear forms defining $\mathcal{C}$ have $\nu_{\mathcal{C}}(I(Q)) = \nu_{\mathcal{C}'}(I(Q)) < n' - d'$, or $\nu_{\mathcal{C}}(I(Q)) = k - 1$. In both cases, since $d' \leq n' - k + 1$ from the Singleton bound, $\nu_{\mathcal{C}}(I(Q)) < \nu_{\mathcal{C}}(I(P_i))$, for any $i = 1, \ldots, u$.

Let $a := n + d' - n'$. Obviously, $1 \leq a \leq n$. If d is the minimum distance of $\mathcal{C}$, then, by Proposition 3.10, $n - d = \max\{\nu_{\mathcal{C}}(I(P_1)), \ldots, \nu_{\mathcal{C}}(I(P_u))\} = n' - d' + m$, where $m := \max\{m_1, \ldots, m_u\}$. So $a = d + m \geq d + 1 = d_1(\mathcal{C}) + 1$. By Proposition 3.10, $d_2(\mathcal{C}) = n - h$, where h is the maximum number of the defining linear forms of $\mathcal{C}$ that span a $k-2$ dimensional vector space. From generic condition, h equals the maximum number of the defining linear forms of $\mathcal{C}'$ that span a $k-2$ dimensional vector space (if we use the construction in Theorem 3.33, $h = k - 2$). So, from Proposition 3.10, $d_2(\mathcal{C}) = n - (n' - d_2(\mathcal{C}')) = a + d_2(\mathcal{C}') - d_1(\mathcal{C}')$. Since $d_2(\mathcal{C}') > d_1(\mathcal{C}')$, we have $a < d_2(\mathcal{C})$, and therefore, by Theorem 3.11, $\mathrm{ht}(I_a(\mathcal{C})) = k - 1$.

We have that $n - a + 1 = n' - d' \geq k - 1$, and therefore $I(P_1), \ldots, I(P_u)$ are the only minimal primes of $I_a(\mathcal{C})$. Since $a - n + \nu_{\mathcal{C}}(I(P_i)) = m_i$, from Corollary 3.22 with $r = 1$, we obtain $I_a(\mathcal{C}) = I(P_1)^{m_1} \cap \cdots \cap I(P_u)^{m_u} \cap K$, where $\mathrm{ht}(K) = k$, and therefore

$$(I_a(\mathcal{C}))^{sat} = I(P_1)^{m_1} \cap \cdots \cap I(P_u)^{m_u}.$$

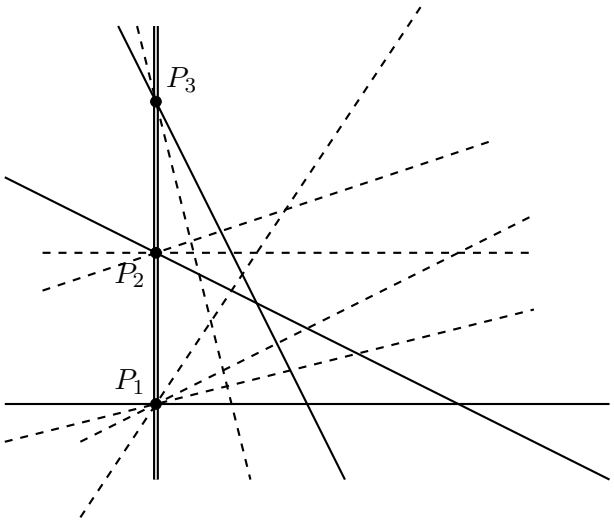
Example 3.38. Let $Z = 3P_1 + 2P_2 + P_3 \subset \mathbb{P}^2$, where $P_1 = [0,0,1], P_2 = [0,1,1], P_3 = [0,2,1]$. Using the method in Remark 3.37 we have that $\mathcal{C}' = (x, x, y, 7x - 2y + 2z, 3x + y - 2z)$ interpolates $\Omega = \{P_1, P_2, P_3\}$: we have $n' = 5$, $d' = 2$, and

$$(I_3(\mathcal{C}'))^{sat} = \langle x, y\rangle \cap \langle x, y - z\rangle \cap \langle x, y - 2z\rangle = I(\Omega).$$

Choose

$$\begin{aligned} \Theta_1 &= \{x + 13y, x - 8y, 2x - 9y\} \\ \Theta_2 &= \{5x + 22y - 22z, 3x + 10y - 10z\} \\ \Theta_3 &= \{17x - 3y + 6z\}. \end{aligned}$$

In the picture below the solid lines are defined by $\mathcal{C}'$, and the dashed lines are defined by $\Theta_1 \cup \Theta_2 \cup \Theta_3$.



So $\mathcal{C}$ has $n = 11$. Taking $a = n - n' + d' = 8$, we obtain

$$(I_8(\mathcal{C}))^{sat} = \langle x, y\rangle^3 \cap \langle x, y - z\rangle^2 \cap \langle x, y - 2z\rangle = I(Z).$$

3.5.2. *Interpolating reduced points with given regularity.* Let $\mathcal{C}$ be an interpolating code for the finite set $\Omega \subset \mathbb{P}^{k-1}$. In Corollary 3.23 (b) showed that

$$d \geq \mathrm{reg}(R/I(\Omega)).$$

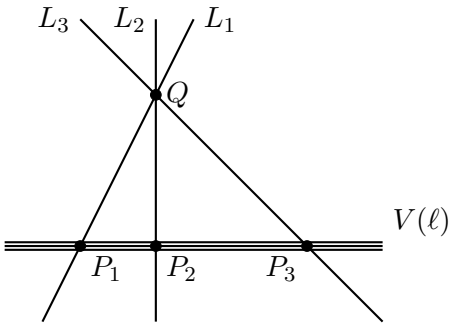
Conjecture 3.41. *Let Ω be a set of u points in $\mathbb{P}^2$ with defining ideal $I(\Omega) \subset R := \mathbb{K}[x,y,z]$. Let $p := \operatorname{reg}(R/I(\Omega)) \geq 1$. Then there exists a linear code $\mathcal{C}$ of minimum distance $d = p$ such that $I(\Omega) = I_{d+1}(\mathcal{C})^{sat}$ if and only if Ω is one of the following:*

(1) *Ω consists of $p+1$ collinear points (so $u = p+1$).*
(2) *Ω consists of $p+1$ points on a line, and a point not on that line (so $u = p+2$).*
(3) *Ω is a star configuration of $u = \binom{p+2}{2}$ points in $\mathbb{P}^2$.*

At this moment we can show that if Ω is of the types (1), (2), and (3), then Ω has an interpolation code with the desired properties.

• If Ω is contained on a line $V(\ell)$, then $I(\Omega) = \langle \ell, g \rangle$, where $\deg(g) = u = |\Omega|$. Because this is a complete intersection, $p = \operatorname{reg}(R/I(\Omega)) = u - 1$, so the minimum distance of our interpolating linear code $\mathcal{C}$ should be $d = u - 1$. This is how we can construct such an interpolating code (see figure below for $u = 3$):

(1.1) Pick a point Q not on $L := V(\ell)$.
(1.2) Let $\ell_1, \ldots, \ell_u$ be the linear forms defining the lines $L_1 := \overline{QP_1}, \ldots, L_u := \overline{QP_u}$.
(1.3) Consider $\mathcal{C} = (\ell_1, \ldots, \ell_u, \underbrace{\ell, \ldots, \ell}_{u})$. So $n = |\mathcal{C}| = 2u$.
(1.4) For each $i = 1, \ldots, u$, we have $\nu_{\mathcal{C}}(I(P_i)) = u + 1$, the maximum possible. Then $n - d = u + 1$, giving $d = u - 1$.



• Suppose $P_1, \ldots, P_{u-1} \in V(\ell)$, and $P_u \notin V(\ell) =: L$. Let ℓ' be the equation of the line $\overline{P_{u-1}P_u}$. Then Ω sits on the conic $V(\ell \cdot \ell')$, hence $a_{t+1} = 2$. By (iv) we have $t \leq 2$, and since $I(\Omega)$ is not a complete intersection, then $t = 2$.

Since $a_3 = 2$, then, by (ii), $2 = e_1 + e_2$, giving $e_1 = e_2 = 1$. By (i), we have $b_1 = a_1 + 1$, $b_2 = a_2 + 1$, $f_1 = b_1 - a_2$, and $f_2 = b_2 - 2$, which leads to $b_2 = f_2 + 2$, $a_2 = f_2 + 1$, $b_1 = f_1 + f_2 + 1$, and $a_1 = f_1 + f_2$. By (v), $p = b_1 - 2 = f_1 + f_2 - 1$, and by (iii), $u = f_1 + 2f_2$. Also, the minimal graded free resolution of $R/I(\Omega)$ is as it is depicted on page 40 in [31]

$$0 \to R(-f_1 - f_2 - 1) \oplus R(-f_2 - 2) \xrightarrow{M} R(-f_1 - f_2) \oplus R(-f_2 - 1) \oplus R(-2) \to R.$$

$I(\Omega)$ is minimally generated by the 2×2 minors of the 3×2 matrix M.

After a change of coordinates, we can assume $\ell = y$, $\ell' = x$, and so $P_{u-1} = [0,0,1]$. We also may assume $P_u = [0,1,0]$, and $P_1 = [1,0,0]$. Therefore, for $j = 2, \ldots, u-2$, $P_j = [\alpha_j, 0, 1]$, $\alpha_j \neq 0$. So

$$I(\Omega) = \langle y, z \rangle \cap \langle y, x - \alpha_1 z \rangle \cap \cdots \cap \langle y, x - \alpha_{u-2} z \rangle \cap \langle x, y \rangle \cap \langle x, z \rangle.$$

Then

$$I(\Omega) = \langle yz, xy, xz(x - \alpha_1 z) \cdots (x - \alpha_{u-2} z) \rangle.$$

This means that $a_2 = 2$ and $a_1 = u - 1$, leading to $f_2 = 1$, and $f_1 = u - 2$. Therefore, $p = u - 2$.

The geometric construction is the following (see figure below for $u = 4$):

(2.1) For $i = 1, \ldots, u-1$, consider the lines $L_i := V(\ell_i) = \overline{P_u P_i}$.

4. FAT POINTS DEFINING LINEAR CODES

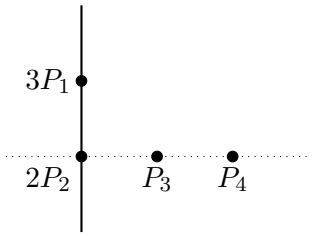
Let $\mathcal{C}$ be an $[n,k,d]$-linear code with generating matrix G of size $k \times n$, rank $k \geq 1$, and with no zero columns. In this chapter, we will look at each column of G as the homogeneous coordinates of a point in $\mathbb{P}^{k-1}$. If two columns are proportional, we will keep track of this multiplicity by considering fat points.

First we study the case when no two columns of G are proportional. So we consider the set of distinct n points $X_{\mathcal{C}} := \{P_1, \ldots, P_n\} \subset \mathbb{P}^{k-1}$, where the homogeneous coordinates of the point P_i are the entries of the i-th column of G. Since $\operatorname{rank}(G) = k$, then $X_{\mathcal{C}}$ is not all included in a hyperplane of $\mathbb{P}^{k-1}$. If there is no confusion, the subscript $\mathcal{C}$ will be omitted.

For a reduced finite set of points $X \subset \mathbb{P}^{k-1}$, not all on a hyperplane, define $hyp(X)$ to be the maximum number of the points of X that are contained in a hyperplane of $\mathbb{P}^{k-1}$. The defining ideal of $X = \{P_1, \ldots, P_n\}$ is $I(X) = I(P_1) \cap \cdots \cap I(P_n) \subset R := \mathbb{K}[x_1, \ldots, x_k]$.

Now, if G has proportional columns we will consider the fat points scheme $Z_{\mathcal{C}} = m_1P_1 + \cdots + m_sP_s \subset \mathbb{P}^{k-1}, m_1, \ldots, m_s \geq 1, m_1 + \cdots + m_s = n =: |Z_{\mathcal{C}}|$ with defining ideal $I(Z_{\mathcal{C}}) = I(P_1)^{m_1} \cap \cdots \cap I(P_s)^{m_s} \subset R$, where, for any $i \neq j$, the columns of G corresponding to the points P_i and P_j are not proportional, whereas for each $i = 1, \ldots, s$, there are m_i columns of G that are proportional to the column corresponding to the point P_i. Same as above, if there is no confusion, the subscript $\mathcal{C}$ will be omitted. The reduced set of points $\{P_1, \ldots, P_s\}$ is called *the support of* Z and it is denoted with $supp(Z)$. Since the rank of G is k, maximum, the support of Z is not contained entirely in a hyperplane of $\mathbb{P}^{k-1}$.

Same as above, for a fat points scheme $Z \subset \mathbb{P}^{k-1}$ as above, we will denote with $hyp(Z)$ the maximum number of points of Z, counted with multiplicity, that are contained in a hyperplane of $\mathbb{P}^{k-1}$. For example, if $Z = 3P_1 + 2P_2 + P_3 + P_4 \subset \mathbb{P}^2$, with P_1, P_2, P_3, P_4 not collinear (i.e., not all on a line), yet, P_2, P_3, P_4 are collinear, then $hyp(Z) = 3 + 2 = 5$, as P_1 and P_2 counted with multiplicity are the most number of points of Z that are collinear.



If G does not have proportional columns, then all $m_i = 1$ in $Z_{\mathcal{C}}$, $s = n$, and therefore $supp(Z_{\mathcal{C}}) = Z_{\mathcal{C}}$. In both cases (reduced or non-reduced), we will say that $\mathcal{C}$ *is defined by the fat points scheme* $Z_{\mathcal{C}}$.

Proposition 4.1. *Let $\mathcal{C}$ be an $[n,k,d]$-linear code with defining fat points scheme $Z_{\mathcal{C}} \subset \mathbb{P}^{k-1}$ as above. Then, the minimum distance of $\mathcal{C}$ satisfies $d = n - hyp(Z_{\mathcal{C}})$.*

Proof. From definition, the minimum distance of $\mathcal{C}$ is d if and only if there exists a nonzero codeword $\mathbf{w} = (w_1, \ldots, w_n) \in \mathcal{C}$ of weight $wt(\mathbf{w}) = d$, and any other codeword of weight $< d$ is the zero vector.

$\mathbf{w} = (w_1, \ldots, w_n) \in \mathcal{C}$ means there exists $\mathbf{v} = (v_1, \ldots, v_k) \in \mathbb{K}^k$, such that $\ell_1(\mathbf{v}) = w_1, \ldots, \ell_n(\mathbf{v}) = w_n$, where $\ell_1, \ldots, \ell_n \in R := \mathbb{K}[x_1, \ldots, x_k]$ are the defining linear forms of $\mathcal{C}$.

The other conditions say that there exists $i_1, \ldots, i_{n-d} \in \{1, \ldots, n\}$ such that $\ell_{i_a}(\mathbf{v}) = 0, a = 1, \ldots, n - d$, and if $j \in \{1, \ldots, n\} \setminus \{i_1, \ldots, i_{n-d}\}$, $\ell_j(\mathbf{v}) \neq 0$. But since $\ell_i = a_{1,i}x_1 + \cdots + a_{k,i}x_k$, where $a_{u,v}$ are the entries of the matrix G, then

$$\ell_i(\mathbf{v}) = a_{1,i}v_1 + \cdots + a_{k,i}v_k = L(P_i),$$

where $L := v_1x_1 + \cdots + v_kx_k \in R$ is a linear form and $P_i = [a_{1,i}, \ldots, a_{k,i}] \in \mathbb{P}^{k-1}$ is the point corresponding to the i-th column of G.

So $n - d$ is the maximum number of points of $Z_{\mathcal{C}}$, counted with multiplicities (namely, the points $P_{i_1}, \ldots, P_{i_{n-d}}$), that belong to a hyperplane of $\mathbb{P}^{k-1}$ (namely, $V(L)$). So $n - d = hyp(Z_{\mathcal{C}})$. □

and therefore

$$m_1 + \cdots + m_d \geq d(Z).$$

Alternatively, we can write

$$d(Z) = \min\left\{ m_{j_1} + \cdots + m_{j_{s-e}} \;\middle|\; \begin{array}{c} \{j_1, \ldots, j_{s-e}\} = \{1, \ldots, s\} \setminus \{i_1, \ldots, i_e\} \\ \text{with } \{c_{i_1}, \ldots, c_{i_e}\} \in \Lambda \end{array} \right\}.$$

Because any $W \in \Lambda$ has $|W| \leq s - d$, the smallest sum we can have contains $s - (s - d) = d$ terms. Moreover, since $m_1 \geq m_2 \geq \cdots \geq m_s$, we must have

$$d(Z) \geq \; m_{s-d+1} + \cdots + m_s.$$

When $m_1 = \cdots = m_s = m$, our two bounds give $md \geq d(Z) \geq md$. □

In the example before Proposition 4.1, using this proposition we have $d(Z) = 7-5 = 2$ and $d = d(X) = 4 - 3 = 1$. With $m_1 = 3, m_2 = 2, m_3 = 1, m_4 = 1$, we have $m_1 \geq d(Z) \geq m_4$, which is what Theorem 4.2 shows.

When $m_1 = \cdots = m_s = m$, then the corresponding linear code is sometimes called a *m-fold repetition code* (see [131]); also in this case, the fat points scheme Z is called *homogeneous*.

4.1. **The minimum distance and the α-invariant of points.** Let $\mathcal{C}$ be an $[n, k, d]$-linear code defined by the fat points scheme $Z_{\mathcal{C}}$. In this section we will look at the α-invariant of $I(Z_{\mathcal{C}})$ and we will see that it provides a good lower bound for the minimum distance d. Recall, the α-invariant of a homogeneous ideal is the smallest degree of a nonzero element of that ideal. So $\alpha(I(Z_{\mathcal{C}})) = \min\{t | (I(Z_{\mathcal{C}}))_t \neq 0\}$. For convenience, we will denote $\alpha(Z) := \alpha(I(Z_{\mathcal{C}}))$.

As we discussed already, we present the next results in terms of the invariants of the fat points schemes defining the linear code $\mathcal{C}$; this will allow a more clear exposition.

4.1.1. *The reduced case.* Let $X \subset \mathbb{P}^{k-1}, k \geq 3$ be a reduced set of n points, not all contained in a hyperplane (so $\alpha(X) \geq 2$). We have a first result, corollary to Proposition 4.1.

Proposition 4.3. *We have*

$$d(X) + u \geq (\alpha(X) - 1)(k - 1),$$

for some $u \in \{0, \ldots, k-2\}$.

Proof. From Proposition 4.1, $d(X) = n - hyp(X)$.

So $hyp(X)$ points of X belong to a hyperplane $V(L) \subset \mathbb{P}^{k-1}$, where L is a linear form in $R := \mathbb{K}[x_1, \ldots, x_k]$.

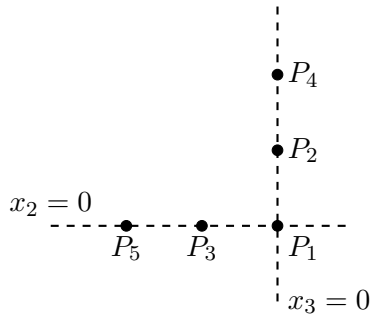
If $d(X) = n - hyp(X) \leq k - 1$, then these $d(X)$ points will belong to a hyperplane $V(L')$, and so $L \cdot L' \in I(X)$, giving that $\alpha(X) \leq 2$. Since X is not contained in a hyperplane, $\alpha(X) = 2$. This gives that $d(X) + u = (2 - 1)(k - 1)$ agreeing with $d(X) \leq k - 1$.

If $d(X) \geq k - 1$, any $k - 1$ points of the remaining $d(X) = n - hyp(X)$ will belong to a hyperplane, so there will be a union of $\delta := \lceil d(X)/(k-1) \rceil$ hyperplanes $V(L_1), \ldots, V(L_\delta) \subset \mathbb{P}^{k-1}$ that contains these remaining $d(X)$ points.

All together give that the product $L \cdot L_1 \cdots L_\delta$ belongs to $I(X)$, and so $\delta + 1 \geq \alpha(X)$. But $\delta \cdot (k-1) = d(X) + u$, for some $u \in \{0, \ldots, k-2\}$. □

Example 4.4. Let us go back to Example 3.9. The defining reduced set of points of $\mathcal{C}$ is

$$X := \{\underbrace{[1,0,0]}_{P_1}, \underbrace{[0,1,0]}_{P_2}, \underbrace{[0,0,1]}_{P_3}, \underbrace{[1,-1,0]}_{P_4}, \underbrace{[1,0,-1]}_{P_5}\} \subset \mathbb{P}^2,$$



with defining ideal

$$I(X) = \langle x_2, x_3\rangle \cap \langle x_1, x_3\rangle \cap \langle x_1, x_2\rangle \cap \langle x_1 + x_2, x_3\rangle \cap \langle x_1 + x_3, x_2\rangle \subset R = \mathbb{K}[x_1, x_2, x_3].$$

Observe that $P_1, P_2, P_4 \in V(x_3)$ and $P_1, P_3, P_5 \in V(x_2)$, which gives that $x_2x_3 \in I(X)$, and consequently $\alpha(X) \leq 2$, so it equals to 2. Also, these collinearities give that $hyp(X) = 3$, and therefore, by Proposition 4.1, $d(X) = 5 - 3 = 2$.

We satisfy the equality in Proposition 4.3, with $u = 0$: we have $2 + 0 = (2 - 1)(3 - 1)$.

Since $u \leq k - 2$ in Proposition 4.3, we have the following immediate result that generalizes the case $m = 1$ in the bound obtained in [120, Theorem 2.8].

Corollary 4.5. *Let $X \subset \mathbb{P}^{k-1}, k \geq 3$ be a reduced set of n points, not all contained in a hyperplane. Then,*

$$d(X) \geq (\alpha(X) - 2)(k - 1) + 1.$$

In particular, $d(X) \geq \alpha(X) - 1$.

As a corollary we obtain [120, Theorem 2.9].

Corollary 4.6. *Let $X \subset \mathbb{P}^{k-1}, k \geq 3$ be a reduced set of n points, not all contained in a hyperplane. Then,*

$$d = \alpha(X) - 1 \text{ iff } hyp(X) = n - 1 \text{ iff } d = 1.$$

Proof. From Corollary 4.5, $d(X) \geq (\alpha(X) - 2)(k - 1) + 1$.

Therefore, if $d(X) = \alpha(X) - 1$, then $0 \geq (\alpha(X) - 2)(k - 2)$, which implies that $\alpha(X) = 2$ (because $\alpha(X) \geq 2$ since X is not all contained in a hyperplane). But then, $d(X) = \alpha(X) - 1 = 1$, which is equivalent to $hyp(X) = n - 1$, by Proposition 4.1.

If $d(X) = 1$, then $1 \geq (\alpha(X) - 2)(k - 1) + 1$, which implies that $\alpha(X) = 2$, and hence $d(X) = 2 - 1 = \alpha(X) - 1$. □

4.1.2. *The fat points case.* Let $Z = m_1P_1 + \cdots + m_sP_s \subset \mathbb{P}^{k-1}, m_1, \ldots, m_s \geq 1$ be a fat points scheme, not all contained in a hyperplane, and with $n = m_1 + m_2 + \cdots + m_s$. Let $X = supp(Z)$ be the reduced support of Z. Let $m(Z) := m = \max\{m_1, \ldots, m_s\}$. We have [120, Theorem 2.8].

Theorem 4.7. *With the above notations and conditions one has*

$$d(Z) \geq \alpha(Z) - m.$$

Proof. First suppose $Z = X$, meaning that $m_1 = \cdots = m_s = 1$. Then, $m = 1$, and Corollary 4.5 proves the statement.

We now proceed by induction on the tuple $(s, (m_1, \ldots, m_s))$, that is, we assume that the statement holds for all tuples of the form $(s, (a_1, \ldots, a_s))$ with

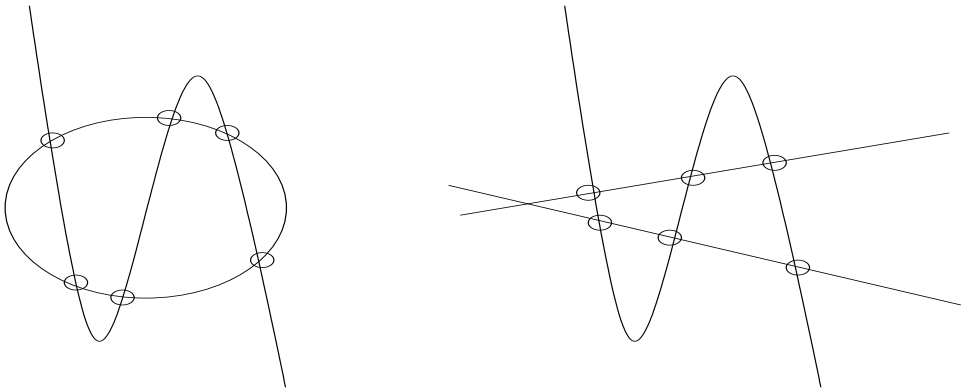
$$(\underbrace{1, \ldots, 1}_{s}) \preceq (a_1, \ldots, a_s) \prec (m_1, \ldots, m_s),$$

complete intersection property, in both situations we have the graded minimal free resolution:

$$0 \to R(-5) \to R(-2) \oplus R(-3) \to R \to R/I \to 0.$$

In particular, $s(X) = s(X') = 5 - 2 = 3$.

Suppose that for both X and X', the cubic is irreducible, but the conic is irreducible for X, weather it is reducible (i.e., union of two lines) for X'. See the attached picture.



As we can see, $hyp(X) = 2$, whereas $hyp(X') = 3$, and therefore $d(X) = 6 - 2 = 4$ and $d(X') = 6 - 3 = 3$.

As a side note, [37, Proposition 3.11] presents also a situation where two $[6, 3]$-linear codes have different minimum distances, yet the graded free resolutions of the Orlik-Terao algebras of the hyperplane arrangements defined by the linear forms dual to the generating matrices of these codes are the same. Since we are interested in interactions between Commutative Algebra and Coding Theory, in the back of our minds we will always be looking for graded algebras associated to linear codes. The Orlik-Terao algebra is such an object: it is the commutative algebraic version of the classical Orlik-Solomon algebra of a hyperplane arrangement. For more details we recommend [37, Section 3.3], where it is explained why one should think about this algebra in the coding theory context. This algebra is naturally constructed from the relation space of the hyperplane arrangement, which is the dual code of the initial code (see also the beginning of Section 3.6.2), but since the results are not yet very convincing, we will not present the details here, and refer the reader to the journal article.

In what follows we will use the classical Bézout's Theorem in $\mathbb{P}^{k-1}$ (as described in [38, Chapter 6.2]) to discuss better bounds for the minimum distance of reduced complete intersections sets of points. We assume that $\mathbb{K}$ is an algebraically closed field of any characteristic.

We first recall that the *degree* of a scheme $W \subseteq \mathbb{P}^{k-1}$, denoted $\deg(W)$, is defined to be $(\dim W)!$ times the leading coefficient of the Hilbert polynomial of W. If W is a reduced finite set of points, then $\deg(W) = |W|$. If $W = CI(e_1, \ldots, e_r)$, $2 \leq r \leq k-1$, then $\deg(W) = e_1 \cdots e_r$.

The Bézout's Theorem is the following.

Theorem 4.15. *Let X be a projective subscheme of $\mathbb{P}^{k-1}$ with $\dim X \geq 1$. If $f \in \mathbb{K}[x_1, \ldots, x_k]$ is a homogeneous form such that no component of X is contained in $V(f)$, the variety defined by f, then*

$$\deg(X \cap V(f)) = \deg(f) \cdot \deg(X).$$

We have the following result concerning the minimum distance of a more general class of reduced sets of points.

Theorem 4.16. *Let Y be a curve in $\mathbb{P}^{k-1}$ with no component contained in a hyperplane. Let $V(f)$ be a hypersurface of degree $a > 1$ such that $X = Y \cap V(f)$ is a reduced zero-dimensional scheme. Then X has minimum distance*

$$d(X) \geq (a-1)\deg(Y).$$

Proof. Suppose that Y has a component W contained in $V(f)$. Then $W \subseteq X$. Since $\dim(X) = 0$, then $\dim(W) = 0$, and so $W = W_1 \cup \cdots \cup W_u$, where each W_i is set-theoretically a point in $\mathbb{P}^{k-1}$. Since a point is always contained in a hyperplane, we have contradicted our assumption that Y has no component in a hyperplane. So we can apply Theorem 4.15 to obtain

$$|X| = \deg(X) = a \cdot \deg(Y).$$

We have that $d(X) = |X| - hyp(X)$, so it suffices to show that $hyp(X) \leq \deg(Y)$. Suppose to the contrary that $h := hyp(X) > \deg(Y)$ and that $V(L)$ is the hyperplane containing the h points of X. Since no component of Y is contained in $V(L)$, then $\dim(Y \cap V(L)) = 0$ and furthermore we can apply Theorem 4.15 once more to obtain that

$$\deg(Y \cap V(L)) = \deg(L) \cdot \deg(Y) = \deg(Y),$$

since $\deg(L) = 1$.

Since $X \subset Y$, then $X \cap V(L) \subseteq Y \cap V(L)$. Therefore the h points of X lying on $V(L)$ should be contained in $Y \cap V(L)$. But then $\deg(Y \cap V(L)) \geq h$, which contradicts the assumption that $h > \deg(Y)$. □

Remark 4.17. We can construct sets of points such that the bound in Theorem 4.16 is attained. Let $Y \subset \mathbb{P}^{k-1}$ be an irreducible curve, not contained in a hyperplane. Let g be a form of degree $a-1 \geq 1$ and let L be a linear form such that $X = V(L \cdot g) \cap Y$ is a reduced zero-dimensional scheme. Since $V(L \cdot g) = V(L) \cup V(g)$, then $V(L) \cap Y \subseteq X$, is a reduced zero-dimensional scheme of degree $\deg(V(L) \cap Y) = \deg(Y)$. So the hyperplane $V(L)$ contains $\deg(Y)$ points of X. This implies that $hyp(X) \geq \deg(Y)$. But from Theorem 4.16 we have $hyp(X) \leq \deg(Y)$, and therefore we get an equality.

As a corollary, we improve the bound on $d(X)$ when X is complete intersection with an additional condition.

Corollary 4.18. *Let $X = CI(e_1, \ldots, e_{k-1}) \subseteq \mathbb{P}^{k-1}$, with $2 \leq e_1 \leq \cdots \leq e_{k-1}$. If $I(X) = \langle F_1, \ldots, F_{k-1} \rangle$, then for each $i = 1, \ldots, k-1$, let $X_i := CI(e_1, \ldots, \hat{e_i}, \ldots, e_{k-1})$, with ideal $I(X_i) = \langle F_1, \ldots, \hat{F_i}, \ldots, F_{k-1} \rangle$. In addition, suppose that there exists an index $j \in \{1, \ldots, n\}$ such that X_j has no component contained in a hyperplane. Then*

$$d(X) \geq (e_1 - 1)e_2e_3 \cdots e_{k-1}.$$

Proof. Because X is a reduced complete intersection, $|X| = e_1 \cdots e_{k-1}$. Also, for each i, X_i is a complete intersection curve of degree $\deg(X_i) = e_1 \cdots \hat{e_i} \cdots e_{k-1}$.

Let j be the index such that X_j has no component contained in a hyperplane. From Theorem 4.16, with $Y = X_j$, and $f = F_j$, we obtain

$$d(X) \geq (e_j - 1)e_1 \cdots \hat{e_j} \cdots e_{k-1}.$$

Since $e_1 \leq e_2 \leq \cdots \leq e_{k-1}$, then $e_2 \cdots e_{k-1} \geq e_1 \cdots \hat{e_j} \cdots e_{k-1}$. Hence, the assertion. □

We expect that the hypothesis in Corollary 4.18 that there exists an X_j with no component contained in a hyperplane can be dropped. We make the following conjecture (see [120, Conjecture 4.9]):

Conjecture 4.19. *Let $X = CI(e_1, \ldots, e_{k-1}) \subseteq \mathbb{P}^{k-1}$, with $2 \leq e_1 \leq \cdots \leq e_{k-1}$. Then $d(X) \geq (e_1 - 1)e_2e_3 \cdots e_{k-1}$.*

We will return to this conjecture later when we will discuss about evaluation codes (see also [22, Section 6]).

When $k - 1 = 2$, we only need Bézout's Theorem for curves to prove Conjecture 4.19. This next result improves the bound in [42, Corollary 4.4], when $e_1 \geq 3$, and it is the same bound when $e_1 = 2$.

Proposition 4.20. *Let $X = CI(e_1, e_2) \subseteq \mathbb{P}^2$, with $2 \leq e_1 \leq e_2$. Then $d(X) \geq (e_1 - 1)e_2$.*

5. Linear codes obtained by evaluating polynomials

5.1. **Reed-Muller codes.** We begin this chapter by looking at Reed-Muller codes. For a computer science and computational approach we recommend the survey [1].

The Reed-Muller codes were first introduced in 1954 by Muller ([89]) and Reed ([97]); at their inception these linear codes were binary codes, using only polynomials in one variable. The generalization to any q-arry codes (i.e., the base field being $\mathbb{K} := \mathbb{F}_q$, the finite field with q elements, where q is a power of a prime) and to multi-variate polynomials is the following (see [67], [132], and for generalizations to polynomial codes, see [68]).

Let $r \geq 1$ be an integer, and let $R := \mathbb{K}[x_1, \ldots, x_m]$ be the ring of polynomials. Consider $\mathbb{A}^m = \mathbb{K}^m$ the affine space. Since $\mathbb{K}$ has q elements, $\mathbb{A}^m$ consists of $n := q^m$ points (i.e., elements or vectors), say ordered $P_1, \ldots, P_n$.

Let $R_{\leq r}$ be the $\mathbb{K}$-vector space of polynomials of R of degree $\leq r$. Then define the $\mathbb{K}$-linear map:

$$ev_r : R_{\leq r} \longrightarrow \mathbb{K}^n,\ ev_r(f) := (f(P_1), \ldots, f(P_n)).$$

The image of this linear map is the linear code called *the classical generalized Reed-Muller code*, and it is denoted with $RM_q(r, \mathbb{A}^m)$. For obvious reasons, these codes are also called *affine Reed-Muller codes*. The consistent study of the multi-variable polynomials case was done in [26]. In fact, in their work, among other results, they present the basic parameters of the affine Reed-Muller codes.

Theorem 5.1. *Suppose $r < q$. Then the parameters of $RM_q(r, \mathbb{A}^m)$ are:*

(a) *Length:* $n = q^m$.

(b) *Dimension:* $\binom{r+m}{m}$.

(c) *Minimum distance:* $(q-r)q^{m-1}$.

Proof. Part (a) is immediate since $\mathbb{K}^m$ consists of all m-tuples with entries in the finite set $\mathbb{K}$ that has q elements.

Part (b) is an immediate consequence from the fact that if $r < q$, the map ev_r is injective, and therefore the dimension of $RM_q(r, \mathbb{A}^m)$ equals the dimension of the vector space $R_{\leq r}$. If $q - 1 < r \leq m(q-1)$, the situation needs to be carefully handled, and we will look at this case in the next result.

Part (c) comes from the fact that the maximum number of zeroes of an element of $R_{\leq r}$ is rq^{m-1}, as [70] mentions. □

For the case $r \geq q$, the dimension and the minimum distance formulas are more complicated, see [67]:

- Dimension:
$$\sum_{t=0}^{r}\sum_{j=0}^{m}(-1)^j\binom{m}{j}\binom{t-jq+m-1}{t-jq}.$$
- Minimum distance:
$$d = (q-b)q^{m-a-1},$$
where $r = a(q-1)+b, 0 \leq b < q-1$.

The projective Reed-Muller codes are constructed in similar fashion (see the seminal papers [70] and [111]). Consider $\mathbb{P}^m$ the projective space over the base finite field $\mathbb{K} := \mathbb{F}_q$. $\mathbb{P}^m$ is a disjoint union of affine open patches $W_i, i = 0, \ldots, m$, where the point $[x_0, \ldots, x_m] \in W_i$ if and only if $x_0 = \cdots = x_{i-1} = 0$ and $x_i \neq 0$. Because $x_i \neq 0$, we can assume that the representative of an arbitrary point in W_i is $[0, \ldots, 0, 1, x_{i+1}, \ldots, x_m]$; this is called the *standard representative*.

Let $r \geq 1$ be an integer, let $R := \mathbb{K}[x_0, \ldots, x_m]$ be the ring of homogeneous polynomials, and consider R_r, the $\mathbb{K}$-vector space of homogeneous polynomials of degree r (the zero polynomial it is assumed that has any degree, so it is an element of R_r).

$\mathbb{P}^m$ itself has finitely many elements, say $P_1, \ldots, P_n$, so as for the affine case we define the following $\mathbb{K}$-linear map:

$$ev_r : R_r \longrightarrow \mathbb{K}^n,\ ev_r(f) := \left(\frac{f(P_1)}{x_{i_1}^r}, \ldots, \frac{f(P_n)}{x_{i_n}^r}\right),$$

where the set of indices (some repeated) $i_1, \ldots, i_n$ will form the set $\{0, \ldots, m\}$, and, for every $j = 1, \ldots, n$, $P_j \in W_{i_j}$. If we use standard representatives for each of the points P_j, then $ev_r(f) = (f(P_1), \ldots, f(P_n))$.

The image of this linear map is called *projective Reed-Muller code* and it is denoted with $RM_q(r, \mathbb{P}^m)$.

Example 5.2. Suppose $q = 3$ and $m = 2$. Then $\mathbb{P}^2$ is the disjoint union of the following affine patches:

$$\begin{aligned} W_0 &= \{[1,0,0],[1,0,1],[1,0,2],[1,1,0],[1,1,1],[1,1,2],[1,2,0],[1,2,1],[1,2,2]\} \\ W_1 &= \{[0,1,0],[0,1,1],[0,1,2]\} \\ W_2 &= \{[0,0,1]\}. \end{aligned}$$

If $r = 2$, and if we take $f = x_1^2 + 2x_0x_2$, then, in $\mathbb{F}_3$, we have

$$ev_2(x_1^2 + 2x_0x_2) = (\underbrace{0,2,1,1,0,2,1,0,2}_{W_0}, \underbrace{1,1,1}_{W_1}, \underbrace{0}_{W_2}).$$

By [70, Theorem 2], if $r < q$, the parameters of the projective Reed-Muller code are the following.

Theorem 5.3. *Let $r < q$. Then the parameters of $RM_q(r, \mathbb{P}^m)$ are:*

(a) *Length:* $n = (q^{m+1} - 1)/(q - 1)$.

(b) *Dimension:* $\binom{r+m}{m}$.

(c) *Minimum distance:* $(q - r + 1)q^{m-1}$.

Proof. Part (a) comes from the definition of $\mathbb{P}^m$: it is $(\mathbb{K}^{m+1} \setminus \{0\})/\sim$, where $(x_0, \ldots, x_m) \sim (y_0, \ldots, y_m)$ iff there exists $\lambda \neq 0$ in $\mathbb{K}$ such that $(x_0, \ldots, x_m) = \lambda(y_0, \ldots, y_m)$.

Part (b) is similar to proof of Theorem 5.1 (b): since $r < q$ then ev_r is injective.

Part (c) comes from an inequality conjectured by M. Tsfasman and showed by J.-P. Serre regarding the number of zeroes of a homogeneous polynomial of degree $r < q$. □

For general r, first, by [111, Remark 3], we can restrict to the case when $r \leq m(q-1)$. Here is why: if $r \geq m(q-1) + 1$, let $s := r - m(q-1)$, and for any point $P \in \mathbb{P}^m$ with standard representative $P = [0, \ldots, 0, 1, w_{i+1}, \ldots, w_m] \in W_i$ associate the following homogeneous polynomial of degree r:

$$F_P(x_0, \ldots, x_m) := x_i^s \prod_{j=0}^{i-1}(x_i^{q-1} - x_j^{q-1}) \prod_{k=i+1}^{m}(x_i^{q-1} - (x_k - w_k x_i)^{q-1}).$$

Note that $F_P(P) = 1$ and $F_P(Q) = 0$ for any $Q \neq P$ (this is because if $a \neq 0$ in $\mathbb{K}$, then $a^{q-1} = 1$). Now, let $(c_1, \ldots, c_n) \in \mathbb{K}^n$, and consider the homogeneous polynomial of degree r

$$F(x_0, \ldots, x_m) = \sum_{i=1}^{n} c_i F_{P_i}(x_0, \ldots, x_m).$$

Since $F(P_i) = c_i$ for all $i = 1, \ldots, n$, we obtain that $ev_r(F) = (c_1, \ldots, c_n)$, and hence, in this case, $RM_q(r, \mathbb{P}^m) = \mathbb{K}^n$, the trivial code.

In this general situation, when $1 \leq r \leq m(q-1)$, the main result [111, Theorem 1] presents the parameters of the projective Reed-Muller codes. The proof is very ingenious and requires interesting combinatorial arguments which go beyond the scope of this book, therefore we will not present it. We must note that,

We knew already that there is only one subcode of support size 0 (i.e., the zero codeword), which is once again confirmed by $A_0(t) = \chi_5(t) = 1$. Furthermore, $A_1(t) = \chi_4(t) = 0$, means that there are no subcodes of support size 1.

Let us look at $A_2(t) = \chi_3(t) = 2t - 2$. This says that $A_2^{(3)} = A_2^{(2)} = 0$, $A_2^{(1)} = 2$, and $A_2^{(0)} = 0$, confirming that there are two projective codewords of minimum weight $d = 2$. Next, if we look at $A_3(t) = \chi_4(t) = 4t - 4$, we get four projective codewords of weight 3, and since $A_3^{(3)} = A_3^{(2)} = 0$, they are also minimal projective codewords. Together with the two projective codewords of minimum weight, we obtain the total of six minimal projective codewords; we direct the reader's attention to Section 3.2.1, and especially at the discussion before Example 3.19, where we determined the same minimal projective codewords by means of the primary decomposition of ideals generated by fold products of linear forms.

The values $w > 0$ for which $A_w \neq 0$ will form what is called *the weight distribution of* $\mathcal{C}$. The first number in the weight distribution is the minimum distance of $\mathcal{C}$, and as being part of this list is denoted with $W^{(1)}$. There is a lot of interest also in the next weights in this list, namely $W^{(2)}, W^{(3)}, \ldots$. In the context of generalized Reed-Muller codes, there is substantial information known about $W^{(2)}$, and there is some progress towards the next weights; see [7] and [19].

5.2. **Evaluation codes.** Evaluation codes are almost identical to the generalized projective Reed-Muller codes we have seen above (sometimes the same terminology is used), but defined over any field $\mathbb{K}$, and the set X being a zero-dimensional reduced set of points of $\mathbb{P}^m$, the projective space over $\mathbb{K}$. If $X = \{P_1, \ldots, P_n\}$, then, the ideal of X is

$$I(X) = I(P_1) \cap \cdots \cap I(P_n),$$

which is a homogeneous ideal in $R := \mathbb{K}[x_0, \ldots, x_m]$ of height equal to m. Some authors call them *Reed-Muller-type codes*.

Remark 5.10. Let us look back at Example 5.6: the curve of equation $x_0^2 - x_1x_2 = 0$ in $\mathbb{P}^2_{\mathbb{F}_3}$ is a one-dimensional algebraic variety, yet "it consists of only the four points" $X = \{[1,1,1], [1,2,2], [0,1,0], [0,0,1]\}$. But the ideal of these points is

$$I(X) = \langle x_0(x_1 - x_2), x_0^2 - x_1x_2 \rangle \subset \mathbb{F}_3[x_0, x_1, x_2],$$

which is an ideal of height 2 (a complete intersection of two quadrics), hence it defines a zero-dimensional algebraic variety.

Where is the mistake? The mistake occurred when we said that the curve consists of only four points. The curve $V(x_0^2 - x_1x_2)$ is the set of zeroes of the polynomial $x_0^2 - x_1x_2$ in $\mathbb{P}^2_L$, where L is an algebraically closed extension of $\mathbb{F}_3$. Over L the curve consists of infinitely many points! The correct phrasing should have been "X is the set of $\mathbb{F}_3$-rational points of the curve $V(x_0^2 - x_1x_2)$".

Let $X = \{P_1, \ldots, P_n\} \subset \mathbb{P}^m$ be a finite set of points over a field $\mathbb{K}$, with defining ideal $I(X) \subset R := \mathbb{K}[x_0, \ldots, x_m]$. Suppose that we pick standard representatives for the projective points P_i, i.e., the first nonzero homogeneous coordinate of each P_i is 1. Let $a \geq 1$ be an integer and consider the $\mathbb{K}$-linear map

$$ev_a : R_a \longrightarrow \mathbb{K}^n,\ ev_a(f) = (f(P_1), \ldots, f(P_n)),$$

where R_a is the $\mathbb{K}$-vector space of homogeneous polynomials of R of degree a.

The image of ev_a is called *the evaluation code of degree* a *associated to* X, and it is denoted with $C(X)_a$. When $a = 1$, then $C(X)_1$ is the linear code defined by the set X (see the previous chapter).

The first occurrences of these codes was in [56]. As we will see below, commutative algebra plays a crucial role in studying the parameters of these linear codes. Because of this, a long list of articles, starting with [56] and [100], will tackle these linear codes for various sets X; we will try our best to include all of these contributions. In the first parts of this chapter we will study the general properties of evaluation codes,

and later on we will bring our attention towards results that occurred in the literature for more specific sets X.

Proposition 5.11. *Let $X \subset \mathbb{P}^m$ be a finite set of n reduced points, and let $a \geq 1$ be an integer. Let $I(X) \subset R := \mathbb{K}[x_0, \ldots, x_m]$ be the defining ideal of X. Then, the basic parameters of the evaluation code of degree a associated to X are the following:*

- *Length: $n = |X| = \deg(I(X))$.*
- *Dimension: $k(X, a) := HF(R/I(X), a)$, the Hilbert function value of $R/I(X)$ evaluated at a.*
- *Minimum distance: $d(X)_a := n - \max_{X' \subset X} \{|X'| \,|\, \dim_{\mathbb{K}}(I(X')_a) > \dim_{\mathbb{K}}(I(X)_a)\}$.*

Proof. The first item is obvious: the cardinality of a finite set of reduced points (i.e., no multiplicity) is the degree of the defining ideal of the set.

For the second statement, we have from the 1st Isomorphism Theorem that $R_a/\ker(ev_a) \simeq C(X)_a$. At the same time, $f \in \ker(ev_a)$ if and only if $f \in I(X)_a$. The claim follows from the definition of the Hilbert function.

The third statement was observed first in [56, Proposition 6]. Let $\mathbf{w} \in C(X)_a$ be a codeword of weight $s \geq 1$. Then $\mathbf{w} = (f(P_1), \ldots, f(P_n))$, where $f \in R_a$ with $f(P_{i_1}), \ldots, f(P_{i_s}) \neq 0$, and $f(P_j) = 0$ for all $j \in \{1, \ldots, n\} \setminus \{i_1, \ldots, i_s\}$. Let $X' := \{P_j | j \in \{1, \ldots, n\} \setminus \{i_1, \ldots, i_s\}\}$. We have $X' \subsetneq X$, $f \in I(X')_a \setminus I(X)_a$, and $s = n - |X'|$. Since $X' \subset X$, then $I(X)_a \subset I(X')_a$, and so $\dim(I(X')_a) > \dim(I(X)_a)$. If we want to minimize $s \geq 1$, we must maximize $|X'|$, where X' has the properties listed previously. □

Remark 5.12. We have the following remarks:

(a) An interesting way to describe the minimum distance of an evaluation code is to use Cayley-Bacharach (see [33]): any hypersurface of degree a passing through $|X| - d(X)_a + 1$ points of X, should pass through ALL points of X.

(b) As we saw above, if $X' \subset X$, then $I(X) \subset I(X')$, and therefore we have a short exact sequence of graded R-modules:

$$0 \longrightarrow I(X')/I(X) \longrightarrow R/I(X) \longrightarrow R/I(X') \longrightarrow 0.$$

The inequality $\dim(I(X')_a) > \dim(I(X)_a)$, means that $(I(X')/I(X))_a \neq 0$, which in turn, using Hilbert functions means that $HF(R/I(X), a) > HF(R/I(X'), a)$.

(c) Let $\mathcal{G}_a(X) := \{X' \subset X | (I(X')/I(X))_a \neq 0\}$. Suppose $a \geq 2$. Let $\tilde{X} \in \mathcal{G}_{a-1}(X)$ be such that $d(X)_{a-1} = |X| - |\tilde{X}|$. Then there exists $f \in I(\tilde{X})_{a-1} \setminus I(X)_{a-1}$. Let $\ell \in R$ be a linear form not vanishing at any point of X (there exists such a linear form because the Krull dimension of $R/I(X)$ is 1). Then $f \cdot \ell \in I(\tilde{X})_a \setminus I(X)_a$, and so $\tilde{X} \in \mathcal{G}_a(X)$. Hence $|\tilde{X}| \leq |X| - d(X)_a$, leading to

$$d(X)_{a-1} \geq d(X)_a, \text{ for all } a \geq 2.$$

(d) Using our chapter notations, Lemma 4.9 (which was initially expressed using evaluation codes; see [116, Proposition 2.1]) is the following: if there exists an $s \geq 2$ such that $d(X)_s \geq 2$, then for all $a \in \{2, \ldots, s\}$, we have $d(X)_{a-1} \geq d(X)_a + 1$, and therefore $d(X)_a \geq s - a + 2$, for $1 \leq a \leq s$.

(e) In the itemized list before Lemma 4.9, we presented results that present lower bounds of $d(X)_a$ most coming from item (d) above. Also there it is presented the geometric interpretation of $d(X)_a$ which can be rephrased as in item (a) above.

For the next result we refer the reader to the beginning of Section 4.2 for the recollection of the definitions of the minimum socle degree and the Castelnuovo-Mumford regularity; also Section 2.2 has all the details.

Proposition 5.13. *Let $X \subset \mathbb{P}^m$ be a finite set of points, and let $a \geq 1$ be an integer. Then:*

(i) *If $a \geq \mathrm{reg}(X)$, the Castelnuovo-Mumford regularity of X, then $d(X)_a = 1$.*

(ii) *If $char(\mathbb{K}) = 0$ and if $d(X)_a = 1$, then $a \geq s(X)$, the minimum socle degree of X.*

$(0,0,2,-1,0,0,0)$, a codeword of weight 2. Since rank of A is 6, we have that $C(X)_1$ is MDS (i.e., $2 = d(X)_1 = 7-6+1$, and therefore the generalized Hamming weights equal

$$\delta_X(1,r) = 7-6+r = r+1.$$

Now we consider the signed graph G_σ with the same picture above, where each edge gets a $+$ sign; therefore G_σ is balanced, and the incidence matrix is the coefficients matrix of the graphic arrangement $\mathcal{A}_G$

$$A_\sigma = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ -1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & -1 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 & -1 & -1 & 0 \end{pmatrix}.$$

Suppose $char(\mathbb{K}) = p \neq 2$. Adding all rows of A_σ produces the zero vector, so $\operatorname{rank}(A_\sigma) = 5$. If $\mathcal{C}$ is the linear code with generating matrix A_σ, then $\mathcal{C}$ is an $[7,5]$-linear code with generalized Hamming weights

$$d_r(\mathcal{C}) = \lambda_r(G_\sigma), r = 1,\ldots,5.$$

For $r=1$ we get $d_1(\mathcal{C}) = 1$ since removing edge 4 produces a graph with two connected components. For $r=2$, we need to remove a minimum of three edges (e.g., edges 4, 1, and 2) to produce a graph with three connected components; so $d_2(\mathcal{C}) = 3$. Removing next the edge 3, we get $d_3(\mathcal{C}) = 4$. To disconnect further, we need to remove two edges from the triangle on the right, so $d_4(\mathcal{C}) = 6 = 7-5+4$, the upper-bound for the generalized Hamming weights. Since $d_4(\mathcal{C}) < d_5(\mathcal{C}) \leq 7-5+5$, we are left with $d_5(\mathcal{C}) = 7$.

5.3. **Parameterized codes.** Let $\mathbb{K} = \mathbb{F}_q$ be a finite field with q elements. For $i = 0,\ldots,m$, let $v_i = (v_{i1},\ldots,v_{ik}) \in \mathbb{Z}^k$. Let $y^{v_i} := y_1^{v_{i1}}\cdots y_k^{v_{ik}}$ be the corresponding Laurent monomial. Let $X \subset \mathbb{P}^m$ be the *algebraic toric set parameterized by the monomials* $y^{v_0},\ldots,y^{v_m}$:

$$X = \{[y^{v_0},\ldots,y^{v_m}] \in \mathbb{P}^m | y_1,\ldots,y_k \in \mathbb{K}\setminus\{0\}\}.$$

The goal of this section is to study the evaluation code of degree a associated to X. Let $R := \mathbb{K}[x_0,\ldots,x_m]$ be the ring of homogeneous polynomials, and let $I(X)$ be the defining of X. Suppose $X = \{P_1,\ldots,P_n\}$, and let $a \geq 1$ be an integer. Consider the evaluation map:

$$ev_a : R_a \longrightarrow \mathbb{K}^{|X|},\ ev_a(f) = \left(\frac{f(P_1)}{f_0(P_1)},\ldots,\frac{f(P_n)}{f_0(P_n)}\right),$$

where $f_0(x_0,\ldots,x_m) = x_0^a$. As before, the image of this map is the evaluation code $C(X)_a$, called *a parameterized code of order* a.

Remark 5.22. Let $P \subset \mathbb{R}^k$ be a lattice polytope contained in the k-cube $[0,q-2]^k$, and take the vectors v_i to be all the elements of $P \cap \mathbb{Z}^k$. The monomials y^{v_i} that parameterize the algebraic toric set X are the spanning set of the vector space $\mathcal{L}$ that produces the toric code associated to P; Section 5.1.1. With the notations above and with those from that section, we have

$$C(X)_1 = C_P(\mathbb{F}_q).$$

Information about $I(X)$ is very important into finding the length and the dimension of $C(X)_a$; see Proposition 5.11. From this and the Singleton bound we can find an upper bound on the minimum distance, and furthermore, from Remark 5.12 (e), knowing $s(X)$, the minimum socle degree, we could discover lower bounds on the minimum distance of parameterized codes.

A first result about $I(X)$ is [99, Theorem 2.1]. For the experts, this is not a surprise, since $R/I(X)$ is the fiber cone algebra over $\mathbb{F}_q$ of the monomial ideal $\langle y^{v_0},\ldots,y^{v_m}\rangle \subset \mathbb{F}_q[y_1,\ldots,y_k]$. [128] is the best source of information about monomial ideals and their "elimination algebras", such as Rees algebra and fiber cones; it is classically known that defining fiber cones or Rees algebras of monomial ideals are binomial algebras.

Theorem 5.23. *With the above notations, let $B := \mathbb{K}[x_0, \ldots, x_m, y_1, \ldots, y_k, z]$. Then:*

a) $I(X) = \langle \{x_i - y^{v_i} z\}_{i=0}^m \cup \{y_j^{q-1} - 1\}_{j=1}^k \rangle \cap R$, *and $I(X)$ is a binomial ideal.*
b) *For all $i = 0, \ldots, m$, x_i is a nonzero divisor in $R/I(X)$, and $I(X)$ is a radical lattice ideal of R.*
c) *$R/I(X)$ is a Cohen-Macaulay ring of Krull dimension 1.*

Part c) together with $I(X)$ being a radical ideal from part b) gives that the length of $C(X)_a$ is $|X| = \deg(R/I(X))$. Also, in part b), $I(X)$ being a lattice ideal means that there is some lattice $\mathcal{L} \subset \mathbb{Z}^{m+1}$ such that $I(X) = \langle \{x^a - x^b | a, b \in \mathbb{N}^{m+1} \text{ with } a - b \in \mathcal{L}\} \rangle$; here, if $c = (c_0, \ldots, c_m) \in \mathbb{N}^{m+1}$, as above, $x^c = x_0^{c_0} \cdots x_m^{c_m}$ is the corresponding monomial of R.

Part a) comes intuitively from the fact that $y_i \neq 0$, and therefore satisfies the field equation $y_i^{q-1} = 1$, and from the fact that we would like to find all polynomials in variables $x_0, \ldots, x_m$ that vanish at points $[y^{v_0}, \ldots, y^{v_m}]$.

There is a more precise description of $I(X)$, coming from part a) in the above result. Let $\mathcal{A} = \{v_0, \ldots, v_m\} \subset \mathbb{Z}^k$. Let $I_{\mathcal{A}}$ be the prime ideal of R which is the kernel of the epimorphism of $\mathbb{K}$-algebras

$$R = \mathbb{K}[x_0, \ldots, x_m] \longrightarrow \mathbb{K}[y^{v_0}, \ldots, y^{v_m}],\ x_i \mapsto y^{v_i}.$$

Then,

$$I_{\mathcal{A}} = \langle \{x^a - x^b | a = (a_i), b = (b_i) \in \mathbb{N}^{m+1} \text{ and } \sum a_i v_i = \sum b_i v_i\} \rangle.$$

$I_{\mathcal{A}}$ is called *toric ideal associated to $\mathcal{A}$.*

$\mathcal{A}$ is called *homogeneous* if there exists a vector $c \in \mathbb{Q}^k$ such that $v_i \bullet c = 1$, for all $i = 0, \ldots, m$; here $\bullet$ denotes the usual dot product of vectors in $\mathbb{R}^k$. With this, [99, Theorem 2.5] shows the following:

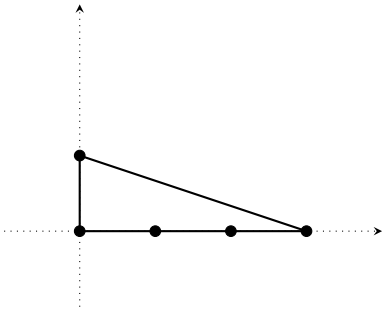
Theorem 5.24. *With the above notations, if $\mathcal{A}$ is homogeneous, then*

$$(I_{\mathcal{A}} + \langle x_1^{q-1} - x_0^{q-1}, \ldots, x_m^{q-1} - x_0^{q-1} \rangle) : (x_0 \cdots x_m)^\infty \subset I(X).$$

Furthermore, one has equality if and only if whenever there exists $w \in \mathbb{Z}^k$ such that $(q-1)w \in L := \mathbb{Z}\{v_i - v_0\}_{i=1}^m$, then $w \in L$ (i.e., $q-1$ is not a zero divisor in $\mathbb{Z}^k/L$).

If $\mathcal{A} = \{v_0, \ldots, v_m\} \subset \mathbb{Z}^k$ is not homogeneous, one can naturally create a homogeneous one $\mathcal{B} := \{(v_0, 1), \ldots, (v_m, 1)\} \subset \mathbb{Z}^{k+1}$ (we take $c = (0, \ldots, 0, 1) \in \mathbb{Z}^{k+1}$), and then use [99, Corollary 2.10] to obtain the similar information about $I(X)$, but now using $\mathcal{B}$ instead of $\mathcal{A}$.

Example 5.25. Let us consider $P = \text{conv}\{(0,0), (3,0), (0,1)\}$ in the picture below. We choose $\mathbb{K} = \mathbb{F}_5$.



Take $\mathcal{A} := P \cap \mathbb{Z}^2 = \{(0,0), (1,0), (2,0), (3,0), (0,1)\}$, and so the algebraic toric set is

$$X = \{[1, y_1, y_1^2, y_1^3, y_2] \in \mathbb{P}^4 | y_1, y_2 \in \mathbb{F}_5 \setminus \{0\}\}.$$

By [71, Proposition 3.2], the minimum distance of $C_P(\mathbb{F}_q)$ equals $4^2 - 3 \cdot 4 = 4$, and therefore, by Remark 5.22, $C(X)_1$ is an $[16, 5, 4]$-linear code.

Next we would like to determine $I(X)$. First we apply Theorem 5.23. With $R := \mathbb{F}_5[x_0, \ldots, x_4]$,

$$I(X) = \langle x_0 - z, x_1 - y_1 z, x_2 - y_1^2 z, x_3 - y_1^3 z, x_4 - y_2 z, y_1^4 - 1, y_2^4 - 1 \rangle \cap R.$$

With [53] we obtain

$$I(X) = \langle x_2^2 - x_1x_3, x_1x_2 - x_0x_3, x_0x_2 - x_3^2, x_1^2 - x_3^2, x_0x_1 - x_2x_3, x_0^2 - x_1x_3, x_3^4 - x_4^4\rangle.$$

This is a nice binomial ideal, but it is quite complicated.

Now let us apply Theorem 5.24. First we note that $\mathcal{A}$ is not homogeneous, so we homogenize it by considering $\mathcal{B} = \{(0,0,1),(1,0,1),(2,0,1),(3,0,1),(0,1,1)\}$. Next we want to determine the toric ideal $I_{\mathcal{B}}$, so we need to determine the vectors $c = (c_i) := (a_i) - (b_i) \in \mathbb{Z}^5$ such that $c_0v_0 + \cdots + c_4v_0 = (0,0,0)$. So we need to find the kernel the integral matrix

$$\begin{pmatrix} 0 & 1 & 2 & 3 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

The solution is $s(1,-2,1,0,0) + t(2,-3,0,1,0)$, for some $s,t \in \mathbb{Z}$. For $s = 2$ and $t = -1$ we obtain $(0,-1,2,-1,0)$ which equals $\underbrace{(0,0,2,0,0)}_{a} - \underbrace{(0,1,0,1,0)}_{b}$. This way we get the first generator in the list of generators for $I(X)$ we have seen above: $x^a - x^b = x_2^2 - x_1x_3$. More generally, again with [53], we obtain $I_{\mathcal{B}} = \langle x_2^2 - x_1x_3, x_1x_2 - x_0x_3, x_1^2 - x_0x_2\rangle$. Since any $w = (w_1,w_2,w_3) \in \mathbb{Z}^3$ is in $\mathbb{Z}\mathcal{B}$ (because $w = (w_3 - w_2 - w_1)(0,0,1) + w_1(1,0,1) + w_2(0,1,1)$), the condition (b) in [99, Corollary 2.10] is satisfied, and hence

$$\langle I_{\mathcal{B}}, x_1^4 - x_0^4, \ldots, x_4^4 - x_0^4\rangle : (x_0x_1x_2x_3x_4)^\infty = I(X).$$

We have $\operatorname{reg}(X) = 4$. With Proposition 5.13(i) and Theorem 5.20, with $r = 1$, and with $d(X)_1 = 4$ we get the following values for $d(X)_a$ and for the Hilbert function values which give the dimensions of $C(X)_a$.

a	1	2	3	4	$5\cdots$
$d(X)_a$	4	3	2	1	$1\cdots$
$HF(R/I,a)$	5	9	13	16	$16\cdots$

In the next topic we will investigate algebraic toric sets embedded into algebraic toric sets (see [50]). Let $\mathcal{A} := \{v_0,\ldots,v_p,\ldots,v_m\} \subset \mathbb{Z}^k$, and let $\mathcal{A}' := \{v_0,\ldots,v_p\}$. Let $X \subset \mathbb{P}^m$ be the algebraic toric set parameterized by the monomials $y^{v_0},\ldots,y^{v_m}$, and let $X' \subset \mathbb{P}^p$ be the algebraic toric set parameterized by the monomials $y^{v_0},\ldots,y^{v_p}$. We say that *X' is embedded into X*. The goal is to understand the connection between the parameters of $C(X)_a$ and the parameters of $C(X')_a$.

First, the component-wise multiplication gives a group epimorphism, which is the natural projection: $\pi : X \longrightarrow X'$, $\pi([y^{v_0},\ldots,y^{v_m}]) = [y^{v_0},\ldots,y^{v_p}]$, and therefore, $X' \simeq X/\ker\pi$. Denote $\nu := |\ker\pi|$; and one has

$$|X| = \nu|X'|.$$

In terms of defining ideals, it is not difficult to see that $I(X') = I(X) \cap R'$, where $R' := \mathbb{K}[x_0,\ldots,x_p]$ is the subring of $R := \mathbb{K}[x_0,\ldots,x_m]$. So, in terms of dimensions of the two parameterized codes of interest we have, for $a \geq 1$,

$$HF(R'/I(X'),a) \leq HF(R/I(X),a).$$

The minimum distances satisfy the following inequality (see [50, Theorem 1], which also generalizes [127, Lemma 3.5]):

Proposition 5.26. *With the above notations one has*

$$d(X)_a \leq \nu \cdot d(X')_a.$$

Proof. We will use Theorem 5.18 when $r = 1$; $d(X)_a = \delta_X(a,1)$ and $d(X')_a = \delta_{X'}(a,1)$.

Let $f \in R'_a$ be such that $d(X')_a = |X'| - |X' \cap V(f)|$. Let $P' \in X' \cap V(f) \subset \mathbb{P}^p$, and let $P \in \pi^{-1}(P')$. Then, $f(P) = 0$. But $R'_a \subset R_a$, and so $P \in X \cap V(f) \subset \mathbb{P}^m$. Furthermore, $|X \cap V(f)| = \nu|X' \cap V(f)|$, as $|\pi^{-1}(P')| = \nu$.

The set $X = [A_0 \times \cdots \times A_m] := \{[\gamma_0, \ldots, \gamma_m] \,|\, (\gamma_0, \ldots, \gamma_m) \in A_0 \times \cdots A_m \setminus \{(0, \ldots, 0)\}\} \subseteq \mathbb{P}^m$ is a *projective nested Cartesian set*. For example, $\mathbb{P}^m = [\mathbb{K} \times \cdots \times \mathbb{K}]$. Also a more specific example is $X = [A_0 \times A_1 \times A_2]$, where $A_2 = \mathbb{K} = \mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$, with $\alpha^2 + \alpha + 1 = 0$, and $A_0 = A_1 = \{0, 1\}$. X has 13 elements:

$$[0, 0, 1], [0, 1, 0], [0, 1, 1], [0, 1, \alpha], [0, 1, \alpha^2], \ldots, [1, 1, \alpha^2].$$

For an integer $a \geq 1$, consider $C(X)_a$, the evaluation code of degree a on X; this is called *a projective nested Cartesian code*. The creation of these linear codes and their initial study has been done in [20]. An important result that helps compute $|X|$, $\dim C(X)_a$, and $\operatorname{reg}(X)$ is [20, Lemma 2.4] which shows that

$$I(X) = \langle x_i \prod_{\gamma_j \in A_j} (x_j - \gamma_j x_i) | i < j,\ i, j = 0, \ldots, m \rangle \subset \mathbb{K}[x_0, \ldots, x_m].$$

If $|A_i| = d_i$, for $i = 0, \ldots, m$, [20, Theorem 2.8] presents the length of $C(X)_a$ to be $|X| = 1 + \sum_{i=1}^{m} d_i \cdots d_m$, and an explicit formula for the dimension of $C(X)_a$ which is $HF(R/I(X), a)$.

Regarding the minimum distance, when $X = [K_0 \times \cdots \times K_m]$, where $K_0 \subseteq \cdots \subseteq K_m$ are subfields of $\mathbb{K} = \mathbb{F}_q$ (in this case $d_{i+1} = d_i^{r_i}, r_i \geq 1$ and $q = d_n^{r_n}$), [20, Theorem 3.8] proves the following: if $a > \sum_{i=1}^{m} (d_i - 1)$, then $d(X)_a = 1$.

If $1 \leq a \leq \sum_{i=1}^{m} (d_i - 1)$, in the case where $d_1 = \cdots = d_m$ or $1 \leq a < d_{s+1}$, where $d_1 = \cdots = d_s < d_{s+1}$, one has

$$d(X)_a = (d_{h+1} - \ell + 1) d_{h+2} \cdots d_m,$$

where $0 \leq h \leq m - 1$ and $1 \leq \ell < d_{h+1}$ are the unique integers such that $a = \sum_{i=1}^{h} (d_i - 1) + \ell$.

5.5. **The dual of an evaluation code.** When $\mathcal{C}$ is an evaluation code, [77] goes to a great extent to analyze the dual code $\mathcal{C}^\perp$ (see Section 2.1), and discusses cases when $\mathcal{C}$ is self-dual (i.e., $\mathcal{C} = \mathcal{C}^\perp$). For this exposition, we will look at the dual of an evaluation code from the perspective of Macaulay Inverse Systems (see, for example, [119], more precisely the calculations presented in arXiv:1211.6355v1).

Let $X \subset \mathbb{P}^m$ be a finite set of points, let $a \geq 1$ be an integer, and consider $C(X)_a$ the evaluation code of order a on X. Suppose $X = \{P_1, \ldots, P_n\}$, with P_i written in standard form, and let $I(X) \subset R := \mathbb{K}[x_0, \ldots, x_m]$ be the defining ideal of X.

For each $i = 1, \ldots, n$, if $P_i = [a_{i,0}, \ldots, a_{i,m}]$, then we associate the dual linear form $L_i := a_{i,0} y_0 + \cdots + a_{i,m} y_m \in S := \mathbb{K}[y_0, \ldots, y_m]$.

Lemma 5.39. $\mathbf{w} = (w_1, \ldots, w_n) \in (C(X)_a)^\perp$ *if and only if* $w_1 L_1^a + \cdots + w_n L_n^a = 0$.

Proof. First of all, using Multinomial Theorem we have the expansion

$$L_i^a = \sum_{j_0 + \cdots + j_m = a} A_{j_0, \ldots, j_m} (a_{i,0}^{j_0} \cdots a_{i,m}^{j_m})(y_0^{j_0} \cdots y_m^{j_m}),$$

where $A_{j_0, \ldots, j_m}$ are the multinomial coefficients (which do not depend on i).

Grouping the terms of the sum $w_1 L_1^a + \cdots + w_n L_n^a$ by the monomials $y_0^{j_0} \cdots y_m^{j_m}$, we obtain that $w_1 L_1^a + \cdots + w_n L_n^a = 0$ if and only if for each $(j_0, \ldots, j_m)$ with $j_0 + \cdots + j_m = a$ we have $\sum_{i=1}^{n} w_i a_{i,0}^{j_0} \cdots a_{i,m}^{j_m} = 0$. This is equivalent to $\sum_{i=1}^{n} w_i M(P_i) = 0$, for every monomial $M \in S_a$, and hence, for every $F \in S_a$. By definition, this is equivalent to $\mathbf{w} \in (C(X)_a)^\perp$. $\square$

In general, for any ideal I, and for every $j \geq 0$, define

$$(I^{-1})_j := \{G \in S_j | f \circ G = 0 \text{ for any } f \in I_j\},$$

to be the *j-th degree inverse system of I*, and consequently,

$$I^{-1} := \oplus_j (I^{-1})_j,$$

is called *the inverse system of I*. The $\circ$ operation is basically the differentiation operation, where the polynomial f is considered as a polynomial differential operator acting on G: $x_i \leftrightarrow \partial/\partial y_i$. We recommend [39] for a detailed exposition.

By [35, Theorems IIA and IIB] one has

$$(I(X)^{-1})_j = \mathrm{Span}_{\mathbb{K}}\{L_1^j, \ldots, L_n^j\} \text{ and } HF(R/I(X), j) = \dim_{\mathbb{K}}(I(X)^{-1})_j,$$

which gives $\dim C(X)_j$.

For $F \in S_d$, define

$$Ann(F) := \{f \in R | f \circ F = 0\},$$

the *annihilator of F*, which by a famous result of Macaulay (see [78]) is an Artinian Gorenstein ideal of regularity d. If $I = Ann(F)$, then $(I^{-1})_j$ is the $\mathbb{K}$ vector space spanned by the partial derivatives of order $\deg(F) - j$ of F. Using inverse systems we can obtain the same result as [77, Corollary 6.15]:

Proposition 5.40. *If X is an arithmetically Gorenstein finite set of points with $\mathrm{reg}(X) =: \rho$, and $1 \leq a \leq \rho - 1$ is an integer, then the linear codes $(C(X)_a)^{\perp}$ and $C(X)_{\rho-a-1}$ are monomial equivalent, hence they have the same basic parameters and same generalized Hamming weights.*

Proof. Suppose X is a Gorenstein set of points of regularity $\rho := \mathrm{reg}(X)$. Then, for any $\ell \in R$, linear form with $\ell(P_i) \neq 0$, for all $i = 1, \ldots, n$, the Artinian reduction $\langle \ell, I(X) \rangle = Ann(F)$, where, by [119, Theorem 2.2],

$$F = c_1 L_1^{\rho} + \cdots + c_n L_n^{\rho},$$

with $c_1, \ldots, c_n \in \mathbb{K} \setminus \{0\}$, unique by multiplication by the same nonzero scalar, and such that

$$\underbrace{c_1 \ell(P_1)}_{d_1} L_1^{\rho-1} + \cdots + \underbrace{c_n \ell(P_n)}_{d_n} L_n^{\rho-1} = 0.$$

Let $f \in R_{\rho-a-1}$. Then,

$$f \circ (d_1 L_1^{\rho-1} + \cdots + d_n L_n^{\rho-1}) = \frac{(\rho-1)!}{a!}(d_1 f(P_1) L_1^a + \cdots + d_n f(P_n) L_n^a) = 0.$$

So, by Lemma 5.39, $(d_1 f(P_1), \ldots, d_n f(P_n)) \in (C(X)_a)^{\perp}$. So there exist $d_1, \ldots, d_n \in \mathbb{K} \setminus \{0\}$, such that for every $\mathbf{v} \in C(X)_{\rho-a-1}$, $(d_1, \ldots, d_n) \bullet \mathbf{v} \in (C(X)_a)^{\perp}$.

So $(d_1, \ldots, d_n) \bullet C(X)_{\rho-a-1}$ is a subcode of $(C(X)_a)^{\perp}$.

We have

$$\dim((d_1, \ldots, d_n) \bullet C(X)_{\rho-a-1}) = \dim(C(X)_{\rho-a-1}) = HF(R/I(X), \rho - a - 1),$$

and

$$\dim((C(X)_a)^{\perp}) = |X| - HF(R/I(X), a).$$

By [77, Corollary 2.9(a)], one has

$$HF(R/I(X), \rho - a - 1) + HF(R/I(X), a) = |X|,$$

and hence

$$(d_1, \ldots, d_n) \bullet C(X)_{\rho-a-1} = (C(X)_a)^{\perp}.$$

This proves the claim. □

5.5.1. *Self-dual codes and Gale transforms.* Let $\mathcal{C}$ be a $[2k, k]$-linear code with generating matrix in standard form $G := (I_k|A)$, where I_k is the $k \times k$ identity matrix, and A is some $k \times k$ matrix. Suppose G has no repeated columns. Also, let $X_{\mathcal{C}} \subset \mathbb{P}^{k-1}$ be the set of $2k$ points with homogeneous coordinates the columns of G.

Consider $\mathcal{C}^{\perp}$ the dual code of $\mathcal{C}$. $\mathcal{C}^{\perp}$ is a $[2k, k]$-linear code with generating matrix the parity check matrix of $\mathcal{C}$, i.e., $H := (-A^T|I_k)$. Same as above, let $X_{C^{\perp}} \subset \mathbb{P}^{k-1}$ be the $2k$ points with homogeneous coordinates the columns of H.

By definition, $X_{\mathcal{C}^{\perp}}$ is *the Gale transform of* $X_{\mathcal{C}}$. The set $X_{\mathcal{C}}$ is called *self-associated* if it is projectively equivalent to its Gale transform; i.e., after a projective change of coordinates $X_{\mathcal{C}} = X_{\mathcal{C}^{\perp}}$.

If $\mathcal{C}$ is self-dual, then there exists an invertible $k \times k$ matrix B, such that $G = B \cdot H$. This is equivalent to A being invertible and $-A \cdot A^T = I_k$. It is clear that if $\mathcal{C}$ is self-dual, then $X_{\mathcal{C}}$ is self-associated, but the converse is not true in general. Of course, if $X_{\mathcal{C}}$ is self-associated, then $\mathcal{C}$ and $\mathcal{C}^{\perp}$ are equivalent codes.

Putting together some results concerning Gale transform, Gorenstein finite sets of points and the coding theory of this section we can show the following result.

Proposition 5.41. *Let $X \subset \mathbb{P}^{k-1}$ be an arithmetically Gorenstein reduced finite set of $2k$ points, not all contained in a hyperplane. If $\mathbb{K}$ is algebraically closed, then* $\operatorname{reg}(X) = 3$.

Proof. Within our assumptions, [34, Theorem 7.3] concludes that X is self-associated, and fails to impose independent conditions on quadrics. Let $\mathcal{C}$ be the linear code with generating matrix having as columns the representatives of the homogeneous coordinates of the points of X. So $\mathcal{C}$ is a $[2k, k]$-linear code and it is equivalent to $\mathcal{C}^{\perp}$, and second conclusion means that $HF(R/I(X), 2) = 2k-1$, where $R := \mathbb{K}[x_1, \ldots, x_k]$.

From the Singleton bound, $d(X)_2 \leq 2k - (2k-1) + 2 = 3$, and, by [116, Proposition 3.1], if $\rho := \operatorname{reg}(X) \geq 2$, then $d(X)_2 \geq \rho - 2 + 1 = \rho - 1$. So $\rho \leq 4$.

In Proposition 5.40, with $a = 1$ we have that $\mathcal{C}^{\perp}$ has the same parameters as $C(X)_{\rho-2}$, and so $\mathcal{C} = C(X)_1$ has the same parameters as $C(X)_{\rho-2}$.

If $\rho = 4$, then $k = HF(R/I(X), 1) = HF(R/I(X), \rho - 2) = 2k - 1$; a contradiction. So we are left with $\rho = 3$, since if $\rho = 2$, then $HF(R/I(X), 2) = 2k \neq 2k - 1$. □

Example 5.42. Consider $\mathcal{C}$ the linear code over $\mathbb{F}_2$ with generating matrix

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}.$$

Once we check that $A \cdot A^T = I_4$, we can see that $\mathcal{C}$ is self-dual.

The ideal of the 8 points $X_{\mathcal{C}} \subset \mathbb{P}^3$ is

$$I(X) = \langle x_1x_4 + x_2x_4 + x_3x_4, x_1x_3 + x_2x_3 + x_3x_4, x_1x_2 + x_2x_3 + x_2x_4 \rangle \subset R = \mathbb{F}_2[x_1, x_2, x_3, x_4],$$

so $X_{\mathcal{C}} = CI(2, 2, 2)$.

So X_C is arithmetically Gorenstein, and $\operatorname{reg}(X_{\mathcal{C}}) = 2 + 2 + 2 - 3 = 3$.

We end this section with a question: if $\mathcal{C}$ is self-dual, does it imply that $X_{\mathcal{C}}$ is arithmetically Gorenstein?

5.5.2. α*-invariant of inverse systems.* Since we just have talked about inverse systems, here is yet another approach to minimum distance from commutative algebraic perspective. We go back to the setup of Chapter 3: let $\mathcal{C}$ be an $[n, k, d]$-linear code defined by linear forms $\ell_1, \ldots, \ell_n \in \mathbb{K}[x_1, \ldots, x_k]$. Suppose $\mathbb{K}$ is a field of characteristic 0, or characteristic strictly bigger than n. Let $\operatorname{ch}(\mathcal{C}) := \prod_{i=1}^{n} \ell_i$ be the *Chow form of* $\mathcal{C}$; if no two linear forms are proportional, this is the defining polynomial of the corresponding hyperplane arrangement.

6. TWO ADDITIONAL TOPICS

In this chapter we look at two more aspects that involve commutative algebra into studying linear codes: the Stanley-Reisner resolution of the matroid of the generating matrix of a linear code, and the generalized Hamming distance functions for ideals that are similar to defining ideals of finite sets of projective points.

6.1. **Stanley-Reisner ring of matroids of generating matrices of linear codes.** The combinatorics associated to the matroids of generating matrices of linear codes have been playing an important role in obtaining not only information about the linear code itself (see the great survey [66]), but also, as we have seen at the beginning of this book, they can give information about the commutative algebraic invariants of ideals generated by fold products of linear forms dual to the columns of the generating matrix (see [2]).

What we will see below is an alternative approach to the formula [28, Formula 11.7] for generalized Hamming weights of a linear code. Let $T_{\mathcal{C}}(x,y)$ be the Tutte polynomial of the matroid of the generating matrix of the linear code $\mathcal{C}$, and write $T_{\mathcal{C}}(x+1,y)=\sum_{i,j}c_{i,j}x^iy^j$. Let $p_r=\max\{j|c_{r,j}\neq 0\}$. Then, the r-th generalized Hamming weight is

$$d_r(\mathcal{C})=n-p_r-k+r.$$

This new approach uses the classical commutative algebraic invariants which are the graded betti numbers of Stanley-Reisner ring of the independent simplicial complex associated to M.

Let M be a matroid on $E=\{1,\ldots,n\}$ of rank k, and let Δ be the simplicial complex with faces the independent sets of M. By [14, Theorem 7.3.3], Δ is pure and shellable. This translates into the following very important property: in $R:=\mathbb{Q}[x_1,\ldots,x_n]$, the ideal I_Δ generated by $\prod_{i\in C}x_i$, for C a circuit in M (i.e., minimal dependent set), is Cohen-Macaulay, and the graded betti numbers of the Stanley-Reisner ring R/I_Δ are the same if $\mathbb{Q}$ is replaced with any other field (see also the nice presentations of this topic and next results in [84] or [36]). Note that $\mathrm{ht}(I_\Delta)=k$.

Suppose the graded R-module R/I_Δ has the minimal graded free resolution

$$0\to\oplus_j R(-j)^{\beta_{k,j}}\to\cdots\to\oplus_j R(-j)^{\beta_{1,j}}\to R\to R/I_\Delta\to 0.$$

The numbers $\beta_{i,j}$ are called *the graded betti numbers of* R/I_Δ.

The acclaimed result in [64] is Theorem 4.2, which translated into coding theory language is the following:

Theorem 6.1. *Let $\mathcal{C}$ be an $[n,k]$-linear code with matroid M of a $k\times n$ generating matrix of $\mathcal{C}$. Let Δ be the simplicial complex of the independent sets of M. Then, the s-th generalized Hamming weight of $\mathcal{C}^\perp$ are*

$$d_s(\mathcal{C}^\perp)=\min\{j|\beta_{s,j}(R/I_\Delta)\neq 0\},$$

for $1\leq s\leq n-k$.

One should remark that Theorem 6.1 also gives the r-th generalized Hamming weights of $\mathcal{C}$ itself. One just needs to use the fact that $1\leq d_1(\mathcal{C})<\cdots<d_k(\mathcal{C})\leq n$, and the Wei's Duality Theorem ([129, Theorem 3]):

$$\{d_r(\mathcal{C})|1\leq r\leq k\}=\{1,\ldots,n\}\setminus\{n+1-d_s(\mathcal{C}^\perp)|1\leq s\leq n-k\}.$$

Example 6.2. As an example we revisit [64, Example 2.1]. Let $\mathcal{C}$ be the $[6,3]$-linear code with generating matrix $G:=\begin{pmatrix}1&0&0&1&0&1\\0&1&0&1&1&0\\0&0&1&1&1&0\end{pmatrix}$.

The circuits of the matroid M of G on $E=\{1,2,3,4,5,6\}$ are

$$\{\{1,6\},\{1,4,5\},\{4,5,6\},\{2,3,5\},\{1,2,3,4\},\{2,3,4,6\}\},$$

leading to

$$R/I_\Delta=\mathbb{K}[x_1,\ldots,x_6]/\langle x_1x_6,x_1x_4x_5,x_4x_5x_6,x_2x_3x_5,x_1x_2x_3x_4,x_2x_3x_4x_6\rangle.$$

The graded minimal free resolution of R/I_Δ is (using [53])

$$0 \to R(-6)^4 \to R(-4)^2 \oplus R(-5)^7 \to R(-2) \oplus R(-3)^3 \oplus R(-4)^2 \to R,$$

giving that $d_1(\mathcal{C}^\perp) = 2$, $d_2(\mathcal{C}^\perp) = 4$, $d_3(\mathcal{C}^\perp) = 6$. Hence, the generalized Hamming weights of $\mathcal{C}$ are the numbers in increasing order of the set $\{1,2,3,4,5,6\} \setminus \{7-6=1, 7-4=3, 7-2=5\}$, i.e.,

$$d_1(\mathcal{C}) = 2, d_2(\mathcal{C}) = 4, d_3(\mathcal{C}) = 6.$$

Using the package "Matroids" in [53], we obtain

$$T_{\mathcal{C}}(x+1,y) = x^3 + x^2y + xy^2 + 5x^2 + 5xy + 8x + y^3 + 3y^2 + 5y + 4,$$

leading to $p_1 = 2$, $p_2 = 1$, $p_3 = 0$, and from this and Duursma's formula, to

$$d_1(\mathcal{C}) = 6-2-3+1 = 2,\ d_2(\mathcal{C}) = 6-1-3+2 = 4,\ d_3(\mathcal{C}) = 6-0-3+3 = 6.$$

Remark 6.3. The following are some comments that will link this new approach to facts about generalized Hamming weights, already known from other methods.

(a) Let $\mathcal{C}$ be an $[n,k]$-linear code. The Tutte polynomial of the dual matroid is

$$T_{\mathcal{C}^\perp}(x+1,y) = T_{\mathcal{C}}(y,x+1) = \sum_{I\subset[n]} (y-1)^{k-\rho(I)} x^{|I|-\rho(I)} = \sum_{i,j} c'_{i,j} x^i y^j,$$

where $[n] = \{1,\ldots,n\}$, and $\rho(I)$ is the dimension of the space spanned by columns of the generating matrix of $\mathcal{C}$ indexed by the elements of I.
From Duursma's Formula, if $p'_s := \max\{j | c'_{s,j} \neq 0\}$, then

$$d_s(\mathcal{C}^\perp) = n - p'_s - (n-k) + s = k + s - p'_s.$$

So p'_s is equal to a maximal j_0, where $j_0 = k - \rho(I)$ and $s = |I| - \rho(I)$; hence $j_0 = k + s - |I|$. This way we can look at $d_s(\mathcal{C}^\perp)$ as equal to $\min\{|I| \,||I| - \rho(I) = s\}$, which by [64, Theorems 4.1 and 4.2] equals $\min\{j | \beta_{s,j}(R/I_\Delta) \neq 0\}$.

(b) Another way to express the Tutte polynomial is by [12, Theorem 1.1], and it uses products of linear forms which are dual to the columns of the generating matrix of the $[n,k]$-linear code $\mathcal{C}$ (see also [37] for more discussions):

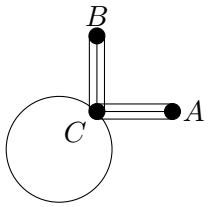
$$T_{\mathcal{C}}(x+1,y) = \sum_{0\le u\le v\le n} x^{k-u} y^{v-u} \dim P(\mathcal{C})_{u,v},$$

where

$$P(\mathcal{C})_{u,v} = \mathrm{Span}_{\mathbb{K}}\{\prod_{i\in I} \ell_i \,|\, \dim(\mathrm{Span}_{\mathbb{K}}\{\ell_j, j \in [n]\setminus I\}) = u \text{ and } v = n - |I|\}.$$

It is obvious that we can appeal to Duursma's Formula to express the generalized Hamming weights by using $\dim P(\mathcal{C})_{u,v}$, but, same as in item (a) above, everything in the end will reduce to the statement of Proposition 3.10.

(c) One other useful thing about this new approach is that one can find some combinatorial invariants of graphs as we have seen in Section 5.2.2, by using homological invariants of the Stanley-Reisner ring. Let us go back to Example 5.21, and find the generalized Hamming distances of the linear code with generating matrix A_σ by using Theorem 6.1. So we need to find the graded betti numbers of the Stanley-Reisner ring R/I_{Δ^*}, where Δ^* is the Alexander dual of Δ, the simplicial complex of independent sets of the matroid of A_σ. So Δ^* is the simplicial complex of independent sets of the dual matroid of A_σ, which is the matroid of the incidence matrix of the (signed) dual graph of G. In the picture of G, if we denote the left "triangle" (i.e., the corresponding K_3) with A, the right "triangle" with B, and the exterior region with C, the dual graph has vertices $\{A,B,C\}$, and edges between vertices whenever the corresponding regions share a common edge; the figure of the dual of G is the following.



The incidence matrix of this (signed) graph is $\begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ -1 & -1 & -1 & -1 & -1 & -1 & 0 \end{pmatrix}$. The circuits of this matrix are $\{\{1,2\},\{1,3\},\{2,3\},\{4,5\},\{4,6\},\{5,6\},\{7\}\}$, giving that $I_{\Delta^*} = \langle x_1x_2, x_1x_3, x_2x_3, x_4x_5, x_4x_6, x_5x_6, x_7\rangle \subset R := \mathbb{Q}[x_1,\ldots,x_7]$. We obtain the minimal graded free resolution of R/I_{Δ^*}

$$0 \to R^4(-7) \to R^{16}(-6) \to R^4(-4) \oplus R^{21}(-5) \to R^{10}(-3) \oplus R^9(-4) \to R(-1) \oplus R^6(-2) \to R.$$

The minimum nonzero graded betti numbers at each step in the free resolutions give

$$d_1(\mathcal{C}) = 1,\ d_2(\mathcal{C}) = 3,\ d_3(\mathcal{C}) = 4,\ d_4(\mathcal{C}) = 6,\ d_5(\mathcal{C}) = 7,$$

the same values we obtained back there in Example 5.21.

6.2. **Minimum distance functions.** In this section we study different functions associated to homogeneous ideals that mimic in spirit the generalized Hamming weight result for evaluation codes we presented in Theorem 5.18.

Let $R := \mathbb{K}[x_1,\ldots,x_k]$ be the ring of homogeneous polynomials with coefficients in a field $\mathbb{K}$, with the standard grading given by the degree of polynomials. Let $I \neq 0$ be a homogeneous ideal in R. Given d, r two positive integers define

$$\mathcal{F}_{d,r} := \{\{f_1,\ldots,f_r\} \subset R_d | \bar{f}_1,\ldots,\bar{f}_r \text{ are linearly independent over } \mathbb{K}, I : \langle f_1,\ldots,f_r\rangle \neq I\},$$

where $\bar{f} = f + I$ is the class of f modulo I. If needed, this set will be denoted with $\mathcal{F}_{d,r}(I)$.

The *generalized minimum distance function of* I is the integer value function

$$\delta_I(d,r) = \begin{cases} \deg(R/I) - \max\{\deg(R/\langle I,F\rangle) | F \in \mathcal{F}_{d,r}\}, & \text{if } \mathcal{F}_{d,r} \neq \emptyset, \\ \deg(R/I), & \text{if } \mathcal{F}_{d,r} = \emptyset. \end{cases}$$

When $r = 1$, $\mathcal{F}_{d,r}$ is denoted with $\mathcal{F}_d$, and $\delta_I(d,r)$ with $\delta_I(d)$, and is called *the minimum distance function of* I (see [81]). [45, Proposition 4.8] shows that if $\prec$ is a monomial order, in the above definition one can replace $\mathcal{F}_{d,r}$ with with the subset $\mathcal{F}_{\prec,d,r}$ of all $F = \{f_1,\ldots,f_r\} \in \mathcal{F}_{d,r}$ with the extra conditions that $f_1,\ldots,f_r$ are standard polynomials with mutually distinct initial terms.

The *hyp function of* I is the function

$$\mathrm{hyp}_I(d,r) = \begin{cases} \max\{\deg(R/\langle I,F\rangle) | F \in \mathcal{F}_{d,r}\}, & \text{if } \mathcal{F}_{d,r} \neq \emptyset, \\ 0, & \text{if } \mathcal{F}_{d,r} = \emptyset. \end{cases}$$

If $r = 1$ and I is the defining ideal of a fat point scheme Z, then $\mathrm{hyp}_I(d) := \mathrm{hyp}_I(d,1)$ equals $hyp(Z)$ in Proposition 4.1. If $r \geq 1$ and I is the defining ideal of a finite set of points X, then, by [45, Lemma 3.4], then $\deg(R/\langle I,F\rangle) = |X \cap V(F)|$. Similar to Proposition 4.1, we have the formula

$$\delta_I(d,r) = \deg(R/I) - \mathrm{hyp}_I(d,r).$$

Also, if I is the defining ideal of a finite set of points X, one obtains Theorem 5.18: $\delta_X(a,r) = \delta_I(a,r)$.

The *Vasconcelos function of* I is the function

$$\mathcal{V}_I(d,r) = \begin{cases} \min\{\deg(R/(I : \langle F\rangle)) | F \in \mathcal{F}_{d,r}\}, & \text{if } \mathcal{F}_{d,r} \neq \emptyset, \\ \deg(R/I), & \text{if } \mathcal{F}_{d,r} = \emptyset. \end{cases}$$

We have [22, Theorem 3.5] and [81, Theorem 4.4]:

All put together we have

$$\mathrm{hyp}_I(d,r) \geq \deg(R/\langle I, F'\rangle) \geq \deg(R/\langle I, F\rangle) = \mathrm{hyp}_I(d, r+1),$$

hence $\delta_I(d,r) = \deg(R/I) - \mathrm{hyp}_I(d,r) \leq \deg(R/I) - \mathrm{hyp}_I(d,r+1) = \delta_I(d,r+1)$.

For part (e), if $\mathcal{F}_{d,r} = \emptyset$, then $\delta_I(d,r) = \deg(R/I) \geq \delta_I(d+1,r)$.

Suppose $\mathcal{F}_{d,r} \neq \emptyset$, and let $F = \{f_1, \ldots, f_r\} \in \mathcal{F}_{d,r}$ be such that $\delta_I(d,r) = \deg(R/I) - \deg(R/\langle I, F\rangle)$. Let $L \in R_1$ be a nonzero divisor in R/I; i.e., $I : L = I$. Then it is not hard to see that $F' := \{f_1L, \ldots, f_rL\} \in \mathcal{F}_{d+1,r}$, and hence $\deg(R/\langle I, F'\rangle) \leq \deg(R/I) - \delta_I(d+1,r)$.

Since the ideals in the chain $I \subsetneq \langle I, F'\rangle \subset \langle I, F\rangle$ have the same height, same argument as in part (d) gives $\deg(R/\langle I, F'\rangle) \geq \deg(R/\langle I, F\rangle)$. Everything put together will give that $\delta_I(d,r) \geq \delta_I(d+1,r)$. □

If I is an unmixed ideal such that $\mathrm{fp}_I(d,1) = \delta_I(d,1)$, for all $d \geq 1$, then I is called *a Geil-Carvalho ideal*. If I is an unmixed ideal such that $\mathrm{fp}_I(d,r) = \delta_I(d,r)$, for all $d \geq 1$ and $r \geq 1$, then I is called *a strongly Geil-Carvalho ideal*.

Example 6.7. There are plenty of examples of unmixed ideals that are not Geil-Carvalho (e.g., [81, Example 7.2], [45, Example 6.4], [22, Example 3.11]).

Below we will take a brief look at [45, Examples 6.1, 6.2, 6.3], which provide an example of a strongly Geil-Carvalho ideal. Let $X \subset \mathbb{P}^2$ be the projective nested Cartesian set over $\mathbb{F}_4$ (see Section 5.4.1):

$$X = [\{0,1\} \times \{0,1\} \times \mathbb{F}_4].$$

By [20, Lemma 2.4], $I(X) = \langle x_0x_1(x_1 - x_0), x_0x_2(x_2^3 - x_0^3), x_1x_2(x_2^3 - x_1^3)\rangle \subset R := \mathbb{F}_4[x_0, x_1, x_2]$. This gives $\mathrm{reg}(X) = 5$, and $\deg(R/I(X)) = |X| = 13$.

In the table below we transcribe only the data for $1 \leq r \leq 6$ that confirms that $I(X)$ is a strongly Geil-Carvalho ideal. The footprint values have been provided by the computer, see [45, Procedure 7.3]. The discussions in [45, Examples 6.1 and 6.2] provide the values $\delta_X(d,1)$ and $\delta_X(d,2)$.

By Corollary 6.5(c)(f), if $r \geq HF(R/I(X), d)$, then $\delta_X(d,r) = |X| = 13$. This provides $\delta_X(1,3) = \delta_X(1,4) = \delta_X(1,5) = \delta_X(1,6) = \delta_X(2,6) = 13$.

If $\delta_X(d,r_0) = |X| - HF(R/I(X),d) + r_0$, the maximum possible (i.e. the Singleton bound is achieved), then for any $r \geq r_0$, one has $\delta_X(d,r) = |X| - HF(R/I(X),d) + r$ (see Section 2.1). Since $\delta_X(d,2) = |X| - HF(R/I(X),d) + 2$, for $d \geq 4$, we can fill the last three columns immediately.

By Theorem 6.6(a), we have $11 = \mathrm{fp}_{I(X)}(2,4) \leq \delta_X(2,4)$, and we also have the Singleton bound (Corollary 6.5(b)), $\delta_X(2,4) \leq |X| - HF(R/I(X),2) + 4 = 13 - 6 + 4 = 11$. So $\delta_X(2,4) = 11$, and by the same argument as before we obtain $\delta_X(2,5) = 12$, and, the already obtained, $\delta_X(2,6) = 13$. Similarly, since $10 = 13 - 9 + 6$, we obtain $\delta_X(3,6) = 10$.

The remaining four values that we marked with red are filled in the following trial-and-error kind of way. First the footprint gives the corresponding lower bounds; we specify also what are the possible values coming from the Singleton bound. Then, using a more general form of procedure [45, Procedure 7.2], one needs to find a system of r polynomials of degree d, not in $I(X)$, that have $|X| - \mathrm{fp}_{I(X)}(d,r)$ common zeroes in X. Then, by Corollary 6.5(a), $\delta_X(d,r) \leq \mathrm{fp}_{I(X)}(d,r)$, and hence, from Theorem 6.6(a) we have equality.

Actually, we need to find just that $\delta_X(2,3) = 8$, and $\delta_X(3,5) = 8$, to completely fill the table. This is because by Corollary 6.5(e), $\delta_X(3,5) > \delta_X(3,4) > \delta_X(3,3)$, and with Theorem 6.6(a), $\delta_X(3,4) = 7$ and $\delta_X(3,3) = 6$.

d	1	2	3	4	5	$6\cdots$
$\lvert X\rvert$	13	13	13	13	13	$13\cdots$
$HF(R/I(X),d)$	3	6	9	12	13	$13\cdots$
$\delta_X(d,1)$	8	4	3	1	1	$1\cdots$
$\mathrm{fp}_{I(X)}(d,1)$	8	4	3	1	1	$1\cdots$
$\delta_X(d,2)$	12	7	4	3	2	$2\cdots$
$\mathrm{fp}_{I(X)}(d,2)$	12	7	4	3	2	$2\cdots$
$\delta_X(d,3)$	13	8/9/10	6/7	4	3	$3\cdots$
$\mathrm{fp}_{I(X)}(d,3)$	13	8	6	4	3	$3\cdots$
$\delta_X(d,4)$	13	11	7/8	5	4	$4\cdots$
$\mathrm{fp}_{I(X)}(d,4)$	13	11	7	5	4	$4\cdots$
$\delta_X(d,5)$	13	12	8/9	6	5	$5\cdots$
$\mathrm{fp}_{I(X)}(d,5)$	13	12	8	6	5	$5\cdots$
$\delta_X(d,6)$	13	13	10	7	6	$6\cdots$
$\mathrm{fp}_{I(X)}(d,6)$	13	13	10	7	6	$6\cdots$

[82, Corollary 4.4] shows that the defining ideal of any projective Cartesian set (i.e., its evaluation code is an Affine Cartesian code, see Section 5.4) is a Geil-Carvalho ideal. This result is a corollary to the following theorem [82, Theorem 3.14]: Let $I \subset R = \mathbb{K}[x_1,\ldots,x_k]$ be a graded ideal and let $\prec$ be a monomial order. If $\mathrm{in}_\prec(I)$ is a complete intersection of height $k-1$, generated by monomials $x^{\alpha_2},\ldots,x^{\alpha_k}$, of degrees $1 \le d_2 \le \cdots \le d_k$, respectively, then

$$\mathrm{fp}_I(d,1) = \begin{cases} (d_{h+2}-\ell)d_{h+3}\cdots d_k, & \text{if } d \le \sum_{i=2}^{k}(d_i-1)-1, \\ 1, & \text{if } d \ge \sum_{i=2}^{k}(d_i-1), \end{cases}$$

where $0 \le h \le k-2$ and ℓ are integers such that $d = \sum_{i=2}^{h+1}(d_i-1)+\ell$, and $1 \le \ell \le d_{h+2}-1$.

If I is an unmixed monomial ideal, then, by [82, Proposition 3.11], I is a Geil-Carvalho ideal. The next result ([22, Proposition 3.13]) shows that if I is unmixed and monomial, then I is in fact strongly Geil-Carvalho.

Proposition 6.8. *If I is an unmixed monomial ideal, then I is a strongly Geil-Carvalho ideal.*

Proof. Let $\prec$ be any monomial order, and let $d, r \ge 1$ be integers. By Theorem 6.6 (a), we have $\mathrm{fp}_I(d,r) \le \delta_I(d,r)$. It remains to show the reverse inequality.

Since I is monomial, $I = \mathrm{in}_\prec(I)$, and hence $\mathcal{M}_{\prec,d,r} \subset \mathcal{F}_{\prec,d,r}$. Also, $\mathcal{M}_{\prec,d,r} = \emptyset$ if and only if $\mathcal{F}_{\prec,d,r} = \emptyset$. The result then follows from [45, Proposition 4.8]. □

6.2.1. *The* $\mathbf{v}$*-number of a graded ideal.* Let I be a homogeneous proper ideal in $R := \mathbb{K}[x_1,\ldots,x_k]$, and let $\mathrm{Ass}(I)$ denote the set of associated primes of I (i.e., $\mathfrak{p} \in \mathrm{Ass}(I)$ if $I : f = \mathfrak{p}$ for some $f \in R$).

For $\mathfrak{p} \in \mathrm{Ass}(I)$, define *the* $\mathbf{v}$*-number of* I *at* $\mathfrak{p}$ to be

$$\mathbf{v}_\mathfrak{p}(I) := \min\{d \ge 1 | \text{ there exists } f \in R_d \text{ with } I : f = \mathfrak{p}\}.$$

Since $\mathrm{Ass}(I)$ is a finite set, one defines *the* $\mathbf{v}$*-number of* I to be

$$\mathbf{v}(I) = \begin{cases} \min\{\mathbf{v}_\mathfrak{p}(I) | \mathfrak{p} \in \mathrm{Ass}(I)\}, & \text{if } I \subsetneq \mathfrak{m}, \\ 0, & \text{if } I = \mathfrak{m}, \end{cases}$$

where $\mathfrak{m} := \langle x_1,\ldots,x_k\rangle$ is the irrelevant maximal ideal. For any homogeneous ideal, $\mathbf{v}(I)$ is a finite integer. If $\mathfrak{p}$ is a prime ideal not equal to $\mathfrak{m}$, then $\mathbf{v}(\mathfrak{p}) = 1$.

If I is the defining ideal of a finite set of points $\mathbb{X} = \{P_1,\ldots,P_n\}$, then $\mathrm{Ass}(I) = \{I(P_1),\ldots,I(P_n)\}$, and therefore, for $i = 1,\ldots,n$, we have $\mathbf{v}_{I(P_i)}(I)$ is the minimal degree of a separator of P_i (see Proposition

REFERENCES

[1] E. Abbe, A. Shpilka and M. Ye, *Reed-Muller codes: theory and algorithms*, IEEE Trans. Inform. Theory **67** (2021), 3251–3277.

[2] B. Anzis, M. Garrousian and S. Tohaneanu, *Generalized star configurations and the Tutte polynomial*, J. Algebr. Comb. **46** (2017), 165–187.

[3] B. Anzis and S. Tohaneanu, *Error-correction of linear codes via colon ideals*, J. Algebra **443** (2015), 479–493.

[4] A. Ashikhmin and A. Barg, *Minimal Vectors in Linear Codes*, IEEE Trans. Inform. Theory **44** (1998), 2010–2017.

[5] Y. Aubry, *Reed-Muller codes associated to projective algebraic varieties*, in Algebraic Geometry and Coding Theory, Lecture Notes in Mathematics, 1518, Springer, 1992, pp. 4–17.

[6] D. Augot, *Description of minimum weight codewords of cyclic codes by algebraic system*, Finite Fields Appl. **2** (1996), 138-152.

[7] S. Ballet and R. Rolland, *On low weight codewords of generalized affine and projective Reed-Muller codes*, Des. Codes Cryptogr. **73** (2014), 271–297.

[8] E. Ballico, G. Favacchio, E. Guardo and L. Milazzo, *Steiner systems and configuration of points*, Des. Codes Cryptogr. **89** (2021), 199–219.

[9] E. Ballico and C. Fontanari, *The Horace method for error-correcting codes*, Appl. Algebra Eng. Commun. Comput. **17**(2006), 135–139.

[10] A. Barg, *Complexity issues in coding theory*, in Handbook of Coding Theory, vol. 1, Elsevier Science, 1998, pp. 649–754.

[11] P. Beelen and M. Datta, *Generalized Hamming weights of affine Cartesian codes*, Finite Fields Appl. **51** (2018), 130–145.

[12] A. Berget, *Products of linear forms and Tutte polynomials*, European J. Combin. **31** (2010), 1924–1935.

[13] D. Bernstein, T. Lange and C. Peters, *Attacking and defending the McEliece cryptosystem*, pp. 31–46 in: J. Buchmann, J. Ding (editors). Post-Quantum Cryptography, Second international workshop, PQCrypto 2008, Cincinnati, OH, USA, October 17-19, 2008, proceedings, Lecture Notes in Computer Science 5299, Springer, 2008.

[14] A. Bjorner, *Homology and Shellability of Matroids and Geometric Lattices*, in Matroid Applications, Cambridge University Press, 1992, pp. 226–283.

[15] S. Bulygin and R. Pellikaan, *Bounded distance decoding of linear error-correcting codes with Gröbner bases*, J. Symbolic Comput. **44** (2009), 1626–1643.

[16] S. Bulygin and R. Pellikaan, *Decoding and finding the minimum distance with Grbner bases : history and new insights*, pp. 585–622 in: I. Woungang, S. Misra, S.C. Misra (editors). Series on Coding Theory and Cryptology vol. 7, Selected Topics in Information and Coding Theory, World Scientific 2010.

[17] R. Burity, S. Tohaneanu and Y. Xie, *Ideals generated by a-fold products of linear forms have linear graded free resolution*, to appear in Michigan Math J., arXiv: 2004.07430.

[18] C. Carvalho, *On the second Hamming weight of some Reed-Muller type codes*, Finite Fields Appl. **24** (2013), 88–94.

[19] C. Carvalho and L. Neumann, *On the next-to-minimal weight of projective Reed-Muller codes*, Finite Fields Appl. **50** (2018), 382–390.

[20] C. Carvalho, L. Neumann and H. Lopez, *Projective nested Cartesian codes*, Bull. Braz. Math. Soc. (N.S.) **48** (2017), 283–302.

[21] S. Cooper and E. Guardo, *Fat points, partial intersections and Hamming distance*, J. Algebra Appl. **19** (2020), 2050071.

[22] S. Cooper, A. Seceleanu, S. Tohaneanu, M. Vaz Pinto and R. Villarreal, *Generalized minimum distance functions and algebraic invariants of Geramita ideals*, Adv. Appl. Math. **112** (2020), 101940.

[23] D. Cox, J. Little and D. O'shea, Using Algebraic Geometry, Graduate Texts in Mathematics 185, Springer-Verlag, New York 2005.

[24] P. Dankelmann, J. Key and B. Rodrigues, *Codes from incidence matrices of graphs*, Des. Codes Cryptogr. **68** (2013), 373–393.

[25] M. De Boer and R. Pellikaan, *Grobner Bases for Codes*, in Some Tapas of Computer Algebra, pp. 237–259, Springer, Berlin 1999.

[26] P. Delsarte, J. Goethals and F. Mac Williams, *On Generalized Reed-Muller codes and their relatives*, Information and Control **16** (1970), 403–442.

[27] H. Derksen and J. Sidman, *Castelnuovo-Mumford regularity by approximation*, Adv. Math. **188** (2004), 104–123.

[28] I. Duursma, *Combinatorics of the two-variables Zeta function*, in Finite Fields and Applications 2003 (editors: G. Mullen, A. Poli, H. Stichtenoth), Lecture Notes in Computer Science 2948, Springer, Berlin, 2004, pp. 109–136.

[29] I. Duursma, C. Renteria and H. Tapia-Recillas, *Reed-Muller codes on complete intersections*, Appl. Algebra Engrg. Comm. Comput. **11** (2001), 455–462.

[30] D. Eisenbud, Commutative Algebra with a View Toward Algebraic Geometry, Springer-Verlag, New York 1995.

[31] D. Eisenbud, The Geometry of Syzygies, Springer, New York 2005.

[32] D. Eisenbud and S. Goto, *Linear free resolutions and minimal multiplicity*, J. Algebra **88** (1984), 89–133.

[33] D. Eisenbud, M. Green and J. Harris, *Cayley-Bacharach theorems and conjectures*, Bull. American Math. Soc. **33** (1996), 295–324.

[34] D. Eisenbud and S. Popescu, *The projective geometry of the Gale transform*, J. Algebra **230** (2000), 127–173.

[35] J. Emsalem and A. Iarrobino, *Inverse system of a symbolic power I*, J. Algebra **174** (1995), 1080–1090.

[36] I. Garcia-Marco, I. Marquez-Corbella, E. Martinez-Moro and Y. Pitones, *Free resolutions and generalized Hamming weights of binary linear codes*, arXiv: 2203.17194.

[37] M. Garrousian and S. Tohaneanu, *Minimum distance of linear codes and the α-invariant*, Adv. Applied Math. **71** (2015), 190–207.

[38] A. Gathmann, Algebraic Geometry, University of Kaiserslautern 2002/2003, Available at http://www.mathematik.uni-kl.de/ gathmann/alggeom.php.

[39] A.V. Geramita, *Inverse Systems of Fat Points: Waring's Problem, Secant Varieties of Veronese Varieties, and Parameter Spaces for Gorenstein Ideals*, Queens Papers Pure Appl. Math. **102** (1996), 1–114.

[40] A.V. Geramita, B. Harbourne and J. Migliore, *Star configurations in $\mathbb{P}^n$*, J. Algebra **376** (2013), 279–299.

[41] A. V. Geramita, M. Kreuzer and L. Robbiano, *CayleyBacharach schemes and their canonical modules*, Trans. Amer. Math. Soc. **339** (1993), 163–189.

[42] L. Gold, J. Little and H. Schenck, *Cayley-Bacharach and evaluation codes on complete intersections*, J. Pure Appl. Algebra **196** (2005), 91–99.

[43] M. Gonzalez-Sarabia, E. Camps, E. Sarmiento and R. Villarreal, *The second generalized Hamming weight of some evaluation codes arising from a projective torus*, Finite Fields Appl. **52** (2018), 370–394.

[44] M. Gonzalez-Sarabia, D. Jaramillo and R. Villarreal, *On the generalized Hamming weights of certain Reed-Muller type codes*, An. St. Univ. Ovidius Constanta **28** (2020), 205–217.

[45] M. Gonzalez-Sarabia, J. Martinez-Bernal, R. Villarreal and C. Vivares, *Generalized minimum distance functions*, J. Algebr. Comb. **50** (2019), 317–346.

[46] M. Gonzalez-Sarabia and C. Renteria-Marquez, *Generalized Hamming weights and some parameterized codes*, Discrete Math. **339** (2016), 813–821.

[47] M. Gonzalez-Sarabia and C. Renteria-Marquez, *Evaluation codes associated to complete bipartite graphs*, Int. J. Algebra **2** (2008), 163–170.

[48] M. Gonzalez-Sarabia, C. Renteria and M. Hernandez de la Torre, *Minimum distance and second generalized Hamming weight of two particular linear codes*, Congr. Numer. **161** (2003), 105–116.

[49] M. Gonzalez-Sarabia, C. Renteria-Marquez and A. Sanchez-Hernandez, *Evaluation codes over a particular complete intersection*, Int. J. Contemp. Math. Sciences **6** (2011), 1497–1504.

[50] M. Gonzalez-Sarabia, C. Renteria-Marquez and E. Sarmiento, *Parameterized codes over some embedded sets and their applications to complete graphs*, Math Commun. **18** (2013), 377–391.

[51] M. Gonzalez-Sarabia, C. Renteria and H. Tapia-Recillas, *Reed-Muller-Type codes over the Segre variety*, Finite Fields Appl. **8** (2002), 511–518.

[52] V. Goppa, *A new class of linear error-correcting codes*, Problems of Information Transmission **6** (1970), 207–212.

[53] D. Grayson and M. Stillman, Macaulay2, a software system for research in algebraic geometry, Available at http://www.math.uiuc.edu/Macaulay2/.

[54] E. Guardo, A. Van Tuyl, *Powers of complete intersections: graded Betti numbers and applications*, Illinois J. Math **49** (2005), 265–279.

[55] E. Guardo, L. Marino, A. Van Tuyl, *Separators of fat points in $\mathbb{P}^n$*, J. Algebra **324** (2010), 1492–1512.

[56] J. Hansen, *Points in uniform position and maximum distance separable codes*, in Zero-Dimensional Schemes (Ravello, 1992), de Gruyter, Berlin, 1994, pp. 205–211.

[57] J. Hansen, *Linkage and codes on complete intersections*, Appl. Algebra Eng. Comm. Comput **14** (2003), 175–185.

[58] J. Hansen, *Toric surfaces and error-correcting codes*, in Coding theory, cryptography, and related areas, (ed., Bachmann et al), Springer-Verlag, 1999, pp. 132–142.

[59] J. Hansen, *Toric varieties Hirzebruch surfaces and error-correcting codes*, Appl. Algebra Eng. Comm. Comput. **13** (2002), 289–300.

[60] J. Harris, Algebraic Geometry - A First Course, Springer-Verlag, New York, 1993.

[61] P. Heijen and R. Pellikaan, *Generalized Hamming weights of q-arry Reed-Muller codes*, IEEE Trans. Inform. Theory **44** (1998), 181–196.

[62] T. Høholdt, J.H. van Lint and R. Pellikaan, *Algebraic geometry codes*, in Handbook of Coding Theory, vol. 1, Elsevier Science, 1998, pp. 871–962.

[63] W. Huffman and V. Pless, editors, Handbook of Coding Theory, Elsevier Science B.V., Netherlands 1998.

[64] T. Johnsen and H. Verdure, *Hamming weights and Betti numbers of StanleyReisner rings associated to matroids*, Appl. Algebra Engrg. Comm. Comput. **24** (2013), 73–93.

[65] D. Joyner, *Toric codes over finite fields*, Appl. Algebra Eng. Commun. Comput. **15** (2004), 63–79.

[66] R. Jurrius and R. Pellikaan, *Codes, arrangements and matroids*, in Series on Coding Theory and Cryptology vol. **8**, Algebraic Geometry Modeling in Information Theory (E. Martnez-Moro Ed.), World Scientific 2013, pp. 219–325.

[67] T. Kasami, S. Lin and W. Peterson, *New generalizations of the Reed-Muller codes-I: Primitive codes*, IEEE Trans. Inform. Theory **14** (1968), 189–199.

[68] T. Kasami, S. Lin and W. Peterson, *Polynomial codes*, IEEE Trans. Inform. Theory **14** (1968), 807–814.

[69] G. Katsman and M. Tsfasman, *Spectra of algebraic-geometric codes*, Problemy Peredachi Informatsii. **23** (1987), 19–34.

[70] G. Lachaud, *The parameters of projective Reed-Muller codes*, Discrete Math. **81** (1990), 217–221.
[71] J. Little and H. Schenck, *Toric surface codes and Minkowski sums*, SIAM J. Discrete Math. **20** (2006), 999–1014.
[72] J. Little and H. Schenck, *Codes from surfaces with small Picard number*, SIAM J. Appl. Algebra Geometry **2** (2018), 242–258
[73] J. Little and R. Schwarz, *On toric codes and multivariate Vandermonde matrices*, Appl. Algebra Eng. Comm. Comput. **18** (2007), 349–367.
[74] H. Lopez, G. Matthews and I. Soprunov, *Monomial-Cartesian codes and their duals, with applications to LCD codes, quantum codes, and locally recoverable codes*, Des. Codes Cryptogr. **88** (2020), 1673–1685.
[75] H. Lopez, C. Renteria-Marquez and R. Villarreal, *Affine Cartesian codes*, Des. Codes Cryptogr. **71** (2014), 5–19.
[76] H. Lopez, E. Sarmiento, M. Vaz Pinto and R. Villarreal, *Parameterized affine codes*, Stud. Sci. Math. Hung. **49** (2012), 406–418.
[77] H. Lopez, I. Soprunov and R. Villarreal, *The dual of an evaluation code*, Des. Codes Cryptogr. **89** (2021), 1367–1403.
[78] F. S. Macaulay, The Algebraic Theory of Modular Systems, Cambridge Tracts 19, Cambridge University Press, London 1916.
[79] R. Maggioni and A. Ragusa, *Construction of smooth curves of $\mathbb{P}^3$ with assigned Hilbert Function and generators' degrees*, Le Matematiche **42** (1987), 195–209.
[80] I. Manin and S. Vladut, *Linear codes and modular curves*, Itogi Nauki i Tekhniki **25** (1984), 209–257, and J. Soviet Math. **30** (1985), 2611–2643.
[81] J. Martinez-Bernal, Y. Pitones and R. Villarreal, *Minimum distance functions of graded ideals and Reed-Muller type codes*, J. Pure Appl. Algebra **221** (2017), 251–275.
[82] J. Martinez-Bernal, Y. Pitones and R. Villarreal, *Minimum distance functions of complete intersections*, J. Algebra Appl. **17** (2018), 18502054.
[83] J. Martinez-Bernal, M. Valencia-Bucio and R. Villarreal, *Generalized Hamming weights of projective Reed-Muller type codes over graphs*, Discrete Math **343** (2020), 111639.
[84] J. Martinez-Bernal, M. Valencia-Bucio and R. Villarreal, *Linear codes over signed graphs*, Des. Codes Cryptogr. **88** (2020), 273–296.
[85] J. Massey, *Minimal Codewords and Secret Sharing*, in Proceedings of the 6th Joint Swedish-Russian International Workshop on Information Theory, pp. 276–279, Molle, Sweden 1993.
[86] H. Matsumura, Commutative ring theory, Cambridge University Press, Cambridge, 1986.
[87] J. Migliore and C. Peterson, *A symbolic test for $(i, j)-$uniformity in reduced zero-dimensional schemes*, J. Symbolic Comput. **37** (2004), 403–413.
[88] E. Miller and B. Sturmfels, Combinatorial Commutative Algebra, Springer, New York, 2005.
[89] D. Muller, *Application of Boolean algebra to switching circuit design and to error detection*, Transactions of the I.R.E. Professional Group on Electronic Computers **EC-3** (1954), 6–12.
[90] J. Neves and M. Vaz Pinto, *Parameterized codes over graphs*, arXiv: 2112.07297.
[91] J. Neves, M. Vaz Pinto and R. Villarreal, *Vanishing ideals over graphs and even cycles*, Comm. Algebra **43** (2015), 10501075.
[92] J. Neves, M. Vaz Pinto and R. Villarreal, *Regularity and algebraic properties of certain lattice ideals*, Bull. Braz. Math. Soc., N.S. **45** (2014), 777–806.
[93] L. Nunez-Betancourt, Y. Pitones and R. Villarreal, *Footprint and minimum distance functions*, Commun. Korean Math. Soc. **33** (2018), 85–101.
[94] P. Orlik and H. Terao, Arrangements of Hyperplanes, Springer-Verlag, Berlin-Heidelberg-New York, 1992.
[95] J. Oxley, Matroid Theory, Oxford University Press, Oxford, 1992.
[96] V. Pless, W. Huffman and R. Brualdi, *An introduction to algebraic codes*, in Handbook of Coding Theory, vol. 1, Elsevier Science, 1998, pp. 3–140.
[97] I. Reed, *A class of multiple-error-correcting codes and the decoding scheme*, Transactions of the I.R.E. Professional Group on Information Theory **4** (1954), 38–49.
[98] I. Reed and G. Solomon, *Polynomial Codes over Certain Finite Fields*, Journal of SIAM **8** (1960), 300–304.
[99] C. Renteria-Marquez, A. Simis and R. Villarreal, *Algebraic methods for parameterized codes and invariants of vanishing ideals over finite fields*, Finite Fields Appl. **17** (2011), 81–104.
[100] C. Renteria and H. Tapia-Recillas, *ReedMuller codes: An ideal theory approach*, Comm. Algebra **25** (1997), 401–413.
[101] D. Ruano, *On the parameters of r-dimensional toric codes*, Finite Fields Appl. **13** (2007), 962–976.
[102] E. Sarmiento, M. Vaz Pinto and R. Villarreal, *The minimum distance of parameterized codes on projective tori*, Appl. Algebra Eng. Commun. Comput. **22** (2011), 249–264.
[103] E. Sarmiento, M. Vaz Pinto and R. Villarreal, *On the vanishing ideal of an algebraic toric set and its parameterized linear codes*, J. Algebra Appl. **11** (2012), 1250072.
[104] H. Schenck, *Resonance varieties via blowups of $\mathbb{P}^2$ and scrolls*, Inter. Math. Res. Notices **20** (2011), 4756–4778.
[105] H. Schenck, Computational Algebraic Geometry, Cambridge University Press, Cambridge, 2003.
[106] R. Sharp, Steps in Commutative Algebra, Cambridge University Press, Cambridge, 1990.
[107] I. Soprunov, *Toric complete intersection codes*, J. Symbolic Comput. **50** (2013), 374–385.
[108] I. Soprunov, *Lattice polytopes in coding theory*, J. Algebra Comb. Discrete Appl. **2** (2015), 85–94.

[109] I. Soprunov and J. Soprunova, *Toric surface codes and Minkowski length of polygons*, SIAM J. Discrete Math. **23** (2009), 384–400.
[110] I. Soprunov and J. Soprunova, *Bringing Toric Codes to the next dimension*, SIAM J. Discrete Math. **24** (2010), 655–665.
[111] A. Sørensen, *Projective Reed-Muller codes*, IEEE Trans. Inform. Theory **37** (1991), 1567–1576.
[112] A. Tochimani, M. Vaz Pinto and R. Villarreal, *Direct products in projective Segre codes*, Finite Fields Appl. **39** (2016), 96–110.
[113] S. Tohaneanu, *On the De Boer-Pellikaan method for computing minimum distance*, J. Symbolic Comput. **45** (2010), 965–974.
[114] S. Tohaneanu, *On ideals generated by a-fold products of linear forms*, J. Comm. Algebra **13** (2021), 549–570.
[115] S. Tohaneanu, *Subspace arrangements as generalized star configurations*, Math. Nachr. **290** (2017), 3029–3037.
[116] S. Tohaneanu, *Lower bounds on minimal distance of evaluation codes*, Appl. Algebra Eng. Commun. Comput. **20** (2009), 351–360.
[117] S. Tohaneanu, *The minimum distance of sets of points and the minimum socle degree*, J. Pure Appl. Algebra **215** (2011), 2645–2651.
[118] S. Tohaneanu, *A commutative algebraic approach to the fitting problem*, Proc. Amer. Math. Soc. **142** (2014), 659–665.
[119] S. Tohaneanu, *Finding inverse systems from coordinates*, J. Algebra **400** (2014), 72–77.
[120] S. Tohaneanu and A. Van Tuyl, *Bounding invariants of fat points using a Coding Theory construction*, J. Pure Appl. Algebra **217** (2013), 269–279.
[121] S. Tohaneanu and Y. Xie, *On Geramita-Harbourne-Migliore conjecture*, Trans. Amer. Math. Soc. **374** (2021), 4059–4073.
[122] V. Toncev, *Codes and designs*, in Handbook of Coding Theory, vol. 2, Elsevier Science, 1998, pp. 1229–1268.
[123] M. Tsfasman and S. Vladut, Algebraic-geometric codes, Kluwer Academic Publishers, Dordrecht, 1991.
[124] M. Tsfasman and S. Vladut, *Geometric approach to higher weights*, IEEE Trans. Inform. Theory. **41** (1995), 1564–1588.
[125] M. Tsfasman, S. Vladut and D. Nogin, Algebraic Geometric Codes: Basic Notions, American Mathematical Society, Providence, 2007.
[126] M. Tsfasman, S. Vladut and Th. Zink, *Modular curves, Shimura curves, and Goppa codes better than Varshamov-Gilbert bound*, Math. Nachr. **109** (1982), 21–28.
[127] M. Vaz Pinto and R. Villarreal, *The degree and regularity of vanishing ideals of algebraic toric sets over finite fields*, Comm. Algebra **41** (2013), 3376–3396.
[128] R. Villarreal, Monomial Algebras, 2nd Edition, Monographs and Research Notes in Mathematics, Chapman and Hall/CRC, 2015.
[129] V. Wei, *Generalized Hamming Weights for Linear Codes*, IEEE Trans. Inform. Theory **37** (1991), 1412–1413.
[130] V. Wei and K. Yang, *On the generalized Hamming weights of product codes*, IEEE Trans. Inform. Theory **39** (1993), 1709–1713.
[131] E. Weiss, *Linear codes of constant weight*, SIAM J. Appl. Math. **14** (1966), 106–111.
[132] E. Weldon, *New generalizations of the Reed-Muller codes-II: Nonprimitive codes*, IEEE Trans. Inform. Theory **14** (1968), 199–205.