2015

Free Resolutions Associated to Representable Matroids

Nicholas D. Armenoff
University of Kentucky, nicholas.armenoff@gmail.com

STUDENT AGREEMENT:

I represent that my thesis or dissertation and abstract are my original work. Proper attribution has been given to all outside sources. I understand that I am solely responsible for obtaining any needed copyright permissions. I have obtained needed written permission statement(s) from the owner(s) of each third-party copyrighted matter to be included in my work, allowing electronic distribution (if such use is not permitted by the fair use doctrine) which will be submitted to UKnowledge as Additional File.

I hereby grant to The University of Kentucky and its agents the irrevocable, non-exclusive, and royalty-free license to archive and make accessible my work in whole or in part in all forms of media, now or hereafter known. I agree that the document mentioned above may be made available immediately for worldwide access unless an embargo applies.

I retain all other ownership rights to the copyright of my work. I also retain the right to use in future works (such as articles or books) all or part of my work. I understand that I am free to register the copyright to my work.

REVIEW, APPROVAL AND ACCEPTANCE

The document mentioned above has been reviewed and accepted by the student's advisor, on behalf of the advisory committee, and by the Director of Graduate Studies (DGS), on behalf of the program; we verify that this is the final, approved version of the student's thesis including all changes required by the advisory committee. The undersigned agree to abide by the statements above.

Nicholas D. Armenoff, Student

Dr. Uwe Nagel, Major Professor

Dr. Peter Perry, Director of Graduate Studies

Free Resolutions Associated to Representable Matroids

ABSTRACT OF DISSERTATION

A dissertation submitted in partial
fulfillment of the requirements for
the degree of Doctor of Philosophy
in the College of Arts and Sciences
at the University of Kentucky

By
Nicholas Armenoff
Lexington, Kentucky

Director: Dr. Uwe Nagel, Professor of Mathematics
Lexington, Kentucky 2015

ABSTRACT OF DISSERTATION

Free Resolutions Associated to Representable Matroids

As a matroid is naturally a simplicial complex, one can study its combinatorial properties via the associated Stanley-Reisner ideal and its corresponding free resolution. Using results by Johnsen and Verdure, we prove that a matroid is the dual to a perfect matroid design if and only if its corresponding Stanley-Reisner ideal has a pure free resolution, and, motivated by applications to their generalized Hamming weights, characterize free resolutions corresponding to the vector matroids of the parity check matrices of Reed-Solomon codes and certain BCH codes. Furthermore, using an inductive mapping cone argument, we construct a cellular resolution for the matroid duals to finite projective geometries and discuss consequences for finite affine geometries. Finally, we provide algorithms for computing such cellular resolutions explicitly.

KEYWORDS: Cellular resolution, representable matroid, error-correcting code, combinatorial geometry, finite projective geometry

Author's signature: Nicholas Armenoff

Date: May 4, 2015

Free Resolutions Associated to Representable Matroids

By
Nicholas Armenoff

Director of Dissertation: Uwe Nagel

Director of Graduate Studies: Peter Perry

Date: May 4, 2015

ACKNOWLEDGMENTS

I would first like to thank my advisor, Dr. Uwe Nagel. His guidance has particularly been beneficial to my work, and this thesis would not have been possible without his knowledge and patience, for which I am grateful. I would also like to thank the rest of my committee members – Dr. Alberto Corso, Dr. Edgar Enochs, Dr. Connie Wood, and Dr. Katherine Thompson. Additionally, I would not have pursued graduate school had it not been for the encouragement of my parents, David and Marsha, for which I wish to thank them. Finally, I would like to thank my wife (and best friend) Claire for her love and support.

TABLE OF CONTENTS

LIST OF FIGURES

Chapter 1: Introduction

When studying properties of combinatorial and algebraic structures whose subsets are equipped with a notion of independence, one frequently wishes to focus on the properties of those subsets which are independent. Matroids, structures which abstract the combinatorial properties of linear independence, arise naturally when studying such combinatorial and algebraic structures. In particular, given a matrix, one may form the corresponding vector matroid taking the collection of independent sets of the matroid to be the collection consisting of the sets of linearly independent columns of the matrix.

Coding theory aims at efficiently correcting transmission errors when data is sent via a noisy channel. This is achieved by introducing redundancy into the messages to be sent prior to their transmission. Although other encoding schemes exist, the most common encoding scheme for this type of error-correction uses linear algebra, leading to the linear block codes. Each linear block code can be described (up to monomial equivalence) by a generator matrix, or equivalently, by a parity check matrix. Thus, one may associate a matroid to a given linear block code by taking the vector matroid of a parity check matrix for the code.

In the case of matroids arising from linear block error-correcting codes, one can translate the generalized Hamming distances of a code, related to its error-correction performance, into distances of the corresponding matroid. As a simplicial complex, a matroid can be associated to a Stanley-Reisner ideal, and hence to a minimal free resolution whose Betti numbers are related to the distances of the matroid [9]. Additionally, certain free resolutions can be realized as cellular resolutions. In this thesis, we study the properties of free resolutions arising from linear codes, as well as cellular resolutions of certain linear codes.

Chapter 2 consists mostly of preliminaries. We define the basic objects we will investigate, including linear block codes, matroids, free resolutions, and cellular resolutions. Additionally, we present basic properties of and operations on these objects and discuss how these properties translate to properties of related objects.

In Chapter 3, we further discuss the homological properties of the Stanley-Reisner ideals of matroids. In particular, we provide simplified proofs of some results of [9] and characterize the Stanley-Reisner ideal of the matroid associated to a linear code. We also prove that the Stanley-Reisner ideal of a matroid admits a pure minimal free resolution if and only if the given matroid is the dual to a perfect matroid design (Theorem 3.1.7).

Our focus in Chapter 4 is on properties of free resolutions of the Stanley-Reisner ideal of the matroid associated to a cyclic code. We derive the existence of a group action on the syzygy modules of such a free resolution (Proposition 4.1.1). After defining the class of BCH codes, we determine the Betti numbers of free resolutions associated to Reed-Solomon codes and furthermore, derive a free resolution for the Stanley-Reisner ideal of a certain family of BCH codes.

We discuss simplex codes, and more generally, codes related to finite projective and affine geometries, in Chapter 5. Specifically, we derive an explicit nonlinear pure minimal cellular resolution of the Stanley-Reisner ideal of the matroid dual to a finite projective geometry using an inductive mapping cone process, yielding an algorithm for computing such resolutions (Theorem 5.1.16). Mapping cones have been used in the literature to produce linear cellular resolutions (see e.g. [2], [3], [6]). However, we use it to produce a nonlinear cellular resolution whose supporting cell complex is simplicial.

Finally, we use our characterization for the Stanley-Reisner ideal of the dual to a finite projective geometry to derive a characterization for the Stanley-Reisner ideal of the dual to a finite affine geometry. We demonstrate a recursion among the Stanley-Reisner ideals of duals to finite affine geometries (see Corollary 5.3.6), analogous to that among the Stanley-Reisner ideals of duals to finite projective geometries; this suggests the existence of another pure cellular resolution, computed through an inductive mapping cone process, associated to duals to finite affine geometries.

Chapter 2: Preliminaries

2.1 Linear Block Codes

We begin with the objects which motivate our study, linear block codes. Given a finite field $\mathbb{F}_q$ of size q and a positive integer n, a *linear block code* $\mathcal{C}$ is a linear subspace of $\mathbb{F}_q^n$. The integer n is called the *block length*, and elements of $\mathcal{C}$ are called *codewords*. Although there are other families of codes, we will be concerned only with the linear block codes. Thus, all uses of the term 'code' or 'linear code' should be understood to mean 'linear block code'.

Linear subspaces of $\mathcal{C}$ are called *subcodes*. As $\mathcal{C}$ is a linear subspace of $\mathbb{F}_q^n$, it can be represented as the image of a matrix; such a matrix is called the *generator matrix* of $\mathcal{C}$. By convention, a code $\mathcal{C}$ with generator matrix G is taken to be the row space of G; if $\mathcal{C}$ has block length n and dimension k as a subspace of $\mathbb{F}_q^n$, then it is said to be an $[n, k]$ code. Given a generator matrix $G \in \mathbb{F}_q^{m\times n}$, there exists a matrix $H \in \mathbb{F}_q^{p\times n}$ such that $GH^T = 0$; such a matrix is called a *parity check matrix* for $\mathcal{C}$. A parity check matrix for a code $\mathcal{C}$ can be itself regarded as a generator matrix for a code, called the *dual code* to $\mathcal{C}$, and usually denoted $\mathcal{C}^\perp$.

2.1.1 Example. Let k be a positive integer and let $\mathbb{F}_q$ be a finite field. Let G denote a $k \times \frac{q^k-1}{q-1}$ matrix whose columns are vectors in $\mathbb{F}_q^k$ which are pairwise linearly independent. Then G is a generator matrix for the *simplex code* with rank k over $\mathbb{F}_q$, denoted $S(k, \mathbb{F}_q)$.

An important class of linear codes are cyclic codes: assume $\mathcal{C}$ is a linear code and that $c = (c_1, \ldots, c_n)$ is a codeword in $\mathcal{C}$. The cyclic shift $\sigma(c)$ of c is the row vector $(c_n, c_1, \ldots, c_{n-1})$; note that the cyclic shift σ is a linear map on $\mathbb{F}_q^n$, and can be implemented as the (left) image of the matrix $A = (A_{i,j}) \in \mathbb{F}_q^{n\times n}$ for which $A_{i,i+1} = A_{n,1} = 1$ and all other entries are zero. Generally speaking, $\sigma(c)$ need not be a codeword for every $c \in \mathcal{C}$ – but if $\sigma(c)$ is in fact a codeword in $\mathcal{C}$ for every $c \in \mathcal{C}$, $\mathcal{C}$ is said to be *cyclic*.

Assume $\mathcal{C} \subseteq \mathbb{F}_q^n$ is cyclic and let $R := \mathbb{F}_q[x]$ be a polynomial ring in the variable x. One may establish a bijective correspondence between polynomials in $R/(x^n - 1)$ and vectors in $\mathbb{F}_q^n$ by associating the vector $c = (c_1, \ldots, c_n)$ with the image of the polynomial $c_1 + c_2 x + \cdots + c_n x^{n-1}$ in $R/(x^n - 1)$; under this correspondence, multiplication by x in the residue class ring corresponds to the cyclic shift in $\mathbb{F}_q^n$. Thus, we may identify a linear subspace of $\mathbb{F}_q^n$ with a corresponding ideal in $R/(x^n - 1)$. However, as $R/(x^n - 1)$ is a principal ideal domain, the ideal in $R/(x^n - 1)$ corresponding to a linear code $\mathcal{C}$ is generated by a polynomial in R with degree less than n – this polynomial is called the *generator polynomial* of $\mathcal{C}$. Furthermore, if $g(x) = c_0 + c_1 x + \cdots + c_{k-1} x^{k-1}$ is a generator polynomial for a cyclic code $\mathcal{C}$, then a generator matrix for $\mathcal{C}$ is:

$$\begin{bmatrix} c_0 & c_1 & \cdots & c_{k-1} & 0 & 0 & \cdots & 0 \\ 0 & c_0 & \cdots & c_{k-2} & c_{k-1} & 0 & \cdots & 0 \\ & & & \vdots & & & & \\ 0 & 0 & \cdots & 0 & c_0 & c_1 & \cdots & c_{k-1} \end{bmatrix}.$$

Note that the generator matrix of a cyclic code is simply a truncated circulant matrix over a finite field.

Since a generator polynomial for an $[n, k]$ cyclic code $\mathcal{C}$ is a divisor of $x^n - 1$, one may define $h(x) := \frac{x^n - 1}{g(x)}$. Then $x^{\deg(h)} h(x^{-1})$ is a generator polynomial for an $[n, n-k]$ cyclic code; in fact, this code is the dual code to $\mathcal{C}$. For further discussion of this, see [11].

2.1.2 Example. Let $g(x) = 1 + x + x^3$ be the generator polynomial for a block length 7 binary cyclic code. The corresponding generator matrix is therefore

$$\begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix} \in \mathbb{F}_2^{4 \times 7}$$

This code is the 4-dimensional binary *Hamming code*. Computing the generator

polynomial for the dual code, one obtains $f(x) = 1 + x^2 + x^3 + x^4$, and thus a generator matrix

$$\begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix} \in \mathbb{F}_2^{3\times 7}$$

for the dual code. However, the columns of this matrix are the pairwise linearly independent vectors in $\mathbb{F}_2^3$ (in fact, all of them), and consequently it is also a generator matrix for the 3-dimensional binary simplex code.

An important invariant of a linear block code correlated to its error correction performance is its Hamming distance, defined as follows.

2.1.3 Definition. Let $\mathcal{C} \subseteq \mathbb{F}_q^n$ be a linear block code, and define $[n] := \{1, \ldots, n\}$. Given a codeword $c \in \mathcal{C}$, the *Hamming weight* of c, denoted $d_H(c)$, is the number of nonzero positions of c:

$$d_H(c) := |\{i \in [n] \,|\, c_i \neq 0\}| \,.$$

The *Hamming distance* of $\mathcal{C}$, denoted $d_H(\mathcal{C})$, is the minimum Hamming weight among all nonzero codewords in $\mathcal{C}$:

$$d_H(\mathcal{C}) := \min\{d_H(c) \,|\, c \in \mathcal{C} - 0\}.$$

2.1.4 Example. One can check that the minimum Hamming weight among the nonzero codewords of $S(3, \mathbb{F}_2)$ is 4, and consequently $S(3, \mathbb{F}_2)$ has Hamming distance 4. In fact, every nonzero codeword of $S(k, \mathbb{F}_q)$ has Hamming weight q^{k-1}. A code in which every nonzero codeword has the same Hamming weight is called a *constant weight* code, and every constant weight linear block code is equivalent to a replication of a simplex code (see Theorem 7.9.5 of [7]).

One natural generalization of the notion of the Hamming distance is to subcodes of $\mathcal{C}$. Let $G_i(\mathcal{C})$ denote the collection of i-dimensional subcodes of $\mathcal{C}$. Suppose $\mathcal{D}$ is

a subcode of $\mathcal{C}$. The *support* of $\mathcal{D}$, denoted $\mathrm{Supp}(\mathcal{D})$, is the set of indices which are not always zero in $\mathcal{D}$, or more precisely:

$$Supp(\mathcal{D}) := \{i \in [n] \,|\, \exists\, c \in \mathcal{D} \text{ such that } c_i \neq 0\}.$$

If $\mathcal{D}$ is i-dimensional, we will refer to its support $\operatorname{supp} D$ as an i-support; a *minimal* i-support is thus an i-support of $\mathcal{C}$ whose proper subsets are not i-supports. Consequently, each minimal 1-support of $\mathcal{C}$ is the support of a 1-dimensional subspace of $\mathcal{C}$, whose codewords we will also call *minimal*.

The *support weight* of a subcode $\mathcal{D}$ of $\mathcal{C}$ is defined to be the cardinality of its support. Thus,

2.1.5 Definition. The *i-th generalized Hamming weight* of $\mathcal{C}$, denoted $d_i(\mathcal{C})$, is the minimum support weight over all i-dimensional subcodes of $\mathcal{C}$.

As the support weight of a one-dimensional subcode is equal to the Hamming weight of any of its constituent codewords, the minimum support weight over all one-dimensional subcodes of a code is equal to the minimum Hamming weight a codeword in the code may attain - hence $d_1(\mathcal{C}) = d_H(\mathcal{C})$. The set of generalized Hamming weights of $\mathcal{C}$ is called the *higher weight hierarchy*; as shown in [22], if $\mathcal{C}$ is k-dimensional, there are k such higher weights, $d_1(\mathcal{C}), \ldots, d_k(\mathcal{C})$. In fact, the generalized Hamming weights of a code characterize its performance under the type 2 wiretap model; for further discussion of this, see [22].

2.2 Matroids

To isolate the combinatorial properties determining the generalized Hamming weights of a code, we will recast the generalized Hamming weights into the language of matroids. To do so, we begin by defining abstract simplicial complexes. Properly speaking, a simplicial complex is a topological space consisting of glued together simplices; an abstract simplicial complex is a collection of sets obeying properties which model the combinatorial relations among the constituent simplices of a simplicial

complex. As we will be concerned with only abstract simplicial complexes, we will simply refer to them as simplicial complexes.

2.2.1 Definition. An *(abstract) simplicial complex* Δ is a pair $(E, \mathcal{F})$ where $\mathcal{F}$ consists of subsets of a finite set E satisfying:

i. $\emptyset \in \mathcal{F}$, and

ii. if $F_1 \in \mathcal{F}$ and $F_2 \subseteq F_1$ then $F_2 \in \mathcal{F}$.

Elements of E are called the *vertices* of Δ and elements of $\mathcal{F}$ are called the *faces* of Δ. If F is a face of Δ, we will frequently write $F \in \Delta$, rather than stating $F \in \mathcal{F}$ where $\mathcal{F}$ is the set of faces of Δ. Given a simplicial complex Δ with vertices E and faces $\mathcal{F}$, if $S \subseteq E$, then the *induced subcomplex* on S, denoted Δ_S, is the simplicial complex with vertex set S whose faces are the faces in F which are also subsets of S. The *dimension* of a face F in a simplicial complex, $\dim F$, is defined to be $|F| - 1$. Generally speaking, a simplicial complex need not consist of finite-dimensional faces. For this reason, we define the *dimension* of Δ, $\dim \Delta$, to be the supremum of the set of dimensions of faces of Δ. Furthermore, a face F of Δ is said to be a *facet* if F is maximal with respect to inclusion. In the event that the facets of Δ are equidimensional, we say that Δ is *pure*.

2.2.2 Definition. A *matroid* is a pair $(E, \mathcal{I})$, where E is a finite set and $\mathcal{I}$ consists of subsets of E satisfying:

i. $\emptyset \in \mathcal{F}$,

ii. if $I_1 \in \mathcal{I}$ and $I_2 \subseteq I_1$ then $I_2 \in \mathcal{I}$, and

iii. if $I_1, I_2 \in \mathcal{I}$ and $|I_1| < |I_2|$, then there exists $x \in I_2 - I_1$ such that $I_1 \cup \{x\} \in \mathcal{I}$.

The set E is called the *ground set* of $(E, \mathcal{I})$ and its elements are called *points* or *vertices*. Members of $\mathcal{I}$ are said to be *independent*, while nonmembers are said to be *dependent*. Two matroids are *isomorphic* if there is an independence preserving bijection between their ground sets. An inclusion-maximal independent set is called a *basis*, while an inclusion-minimal dependent set is called a *circuit*. In fact, one may

equivalently define matroids either in terms of their bases or in terms of their circuits; moreover, equivalent (cryptomorphic) characterizations of matroids abound.

Notice that a matroid is a finite simplicial complex whose faces are the independent sets. They satisfy a third axiom, sometimes called the exchange axiom. In this context, one instead sometimes refers to the matroid as a *matroid complex*. The facets of a matroid complex are the bases, while the minimal nonfaces of the complex are the matroid's circuits. As suggested by the terminology, the bases of a matroid are equicardinal. Thus, matroid complexes are pure; conversely, if every induced subcomplex of a simplicial complex is pure, the simplicial complex is in fact a matroid complex.

As combinatorial structures modeling the combinatorial properties of linear independence, matroids inherit several terms usually applied to vector spaces. Given a matroid $M = (E, \mathcal{I})$ and a subset $A \subseteq E$, the *rank* of A, denoted by $r_M(A)$, is the cardinality of the largest independent set contained in A; furthermore, the rank of a matroid is defined to be the rank of its ground set. The *closure* of a set $A \subseteq E$ consists of the points x in E for which $r_M(A \cup \{x\}) = r_M(A)$, and A is said to be *closed* if it is equal to its closure; consequently, the addition to a closed set A of any point x not in A produces a set with rank $r_M(A)+1$. If A is a closed set with rank k, then it is termed a *k-flat* or *k-subspace*. If a matroid has rank k, then its $(k-1)$-flats are its *hyperplanes*. Finally, if A is a subset of E for which the closure of A is equal to the ground set E, then A is said to be a *spanning set* for M.

Dual to the rank function of a matroid $M = (E, \mathcal{I})$ is its *nullity* function, defined as $n_M(A) := |A| - r_M(A)$; this is the minimum number of elements one must delete from A in order to obtain an M-independent set. The nullity of M itself is the nullity of its ground set. One may thus show that the circuits of M are the sets $A \subseteq E$ for which $n_M(A) = 1$.

2.2.3 Example. Let E be the n-set, $[n] = \{0, 1, \ldots, n-1\}$, and fix an integer k. Define the *uniform matroid*, denoted $U_{n,k}$, to be the matroid with ground set E with bases the k-subsets of E. Thus, the independent sets of $U_{n,k}$ are the subsets of the k-subsets of E, while the circuits are the $(k+1)$-subsets; the hyperplanes of $U_{n,k}$ are the $(k-1)$-subsets of E.

2.2.4 Example. Consider the matrix

$$A := \begin{bmatrix} 1 & 2 & 0 & 1 \\ 0 & 1 & 2 & 2 \end{bmatrix}$$

with entries in $\mathbb{F}_3$. Every pair of columns of A is linearly independent, except for the pair consisting of the second and fourth columns - call the set of pairs of linearly independent columns $\mathcal{B}$. Set $E := [4]$, the column labels of A, and denote by $\mathcal{I}$ the set whose members are the sets of columns in A which are linearly independent. Then $(E, \mathcal{I})$ is a matroid whose bases are the members of $\mathcal{B}$.

Given a matrix A with n columns labeled 1 through n and a subset $X \subseteq [n]$, let A_X denote the columns of A with labels in X. As shown in [18], the above procedure can be generalized in the following manner:

2.2.5 Proposition. *Let $A \in \mathbb{F}^{m \times n}$ be a matrix and let E denote the column labels 1 through n of A. Let $\mathcal{I}$ denote the subsets X of E for which A_X is linearly independent in $\mathbb{F}^m$. Then $(E, \mathcal{I})$ is a matroid.*

Denote this matroid by $\mathcal{M}(A)$; a matroid defined in this manner is called a *vector* matroid (or alternatively, a *linear* matroid). Note that as row operations preserve the linear relations among the columns of a matrix, the corresponding vector matroid is invariant under row operations – thus, given a code $\mathcal{C}$, there is exactly one vector matroid (up to isomorphism) corresponding to the code's parity check matrix. We will denote this matroid by $\mathcal{M}(\mathcal{C})$.

A matroid M which is also the vector matroid of a matrix A with entries in a field $\mathbb{F}$ is said to be *linearly representable* or $\mathbb{F}$-*representable*, while A is said to be a *representation* of M; a matroid which is representable over any field is *regular*. Note that there are matroids which are not representable over any field; for example, the *Vámos matroid*, defined by taking as its ground set

$$E := \{a, b, c, d, e, f, g, h\}$$

and circuits

$$\mathcal{C} := \{abef, cdgh, adeh, bcfg, bdfh\},$$

is a matroid which is not representable over any field – see Proposition 2.2.26 of [18]. As one expects, matroids which are not representable over any field are called *nonrepresentable*.

There are several standard operations on matroids: given a matroid M, with bases $\mathcal{B}$, the *dual* to M (which we will denote by $M^{\perp}$) is the matroid whose bases are the complements of the bases in $\mathcal{B}$; consequently, the dual to the dual of M is M itself. More generally, the independent sets of the dual to M are the complements (relative to the ground set) of the spanning sets of M. This can be extended further in the case of linear matroids: if M is the vector matroid of a matrix A, then through appropriate choices of a row basis for the row space of A and of the orthogonal complement to the row space of A, one obtains that the dual matroid to M is the vector matroid of the orthogonal complement of the row space of A (for details, see Theorem 2.2.8 and Proposition 2.2.23 of [18]). Consequently, the matroid dual to the vector matroid corresponding to a linear block code is the vector matroid corresponding to the dual code.

In addition to the matroid corresponding to a parity check matrix H for a code $\mathcal{C}$, one may also consider the vector matroid of a code's generator matrix G. However, since G is also a parity check matrix for $\mathcal{C}^{\perp}$,

$$\mathcal{M}(G) = \mathcal{M}(\mathcal{C}^{\perp}) = \mathcal{M}(\mathcal{C})^{\perp} = \mathcal{M}(H)^{\perp}.$$

The *direct sum* of two matroids is the matroid whose ground set is the disjoint union of the ground sets and whose independent sets are the disjoint unions of pairs of independent sets from the two summand matroids; thus, this is nothing more than their join as simplicial complexes. Given codes $\mathcal{C}_1$ and $\mathcal{C}_2$, one may take as a parity

check matrix for $\mathcal{C}_1 \oplus \mathcal{C}_2$ the matrix

$$\begin{bmatrix} H_1 & 0 \\ 0 & H_2 \end{bmatrix},$$

where H_1 and H_2 are parity check matrices for $\mathcal{C}_1$ and $\mathcal{C}_2$, respectively, and since the maximal independent column sets of this matrix are the pairs of maximal independent sets from H_1 and H_2, the matroid corresponding to $\mathcal{C}_1 \oplus \mathcal{C}_2$ is the direct sum of the vector matroids of $\mathcal{C}_1$ and $\mathcal{C}_2$.

One may also consider the truncation of a matroid M with independent sets $\mathcal{I}$. Assume k is a positive integer at most $r(M)$ and consider the collection of independent sets in $\mathcal{I}$ with cardinality at most k; as these sets inherit the properties which they possess as independent sets of M, they form the independent sets for another matroid on the same ground set as M, called the *truncation* of M to rank k; the bases of the truncation of M to rank k are the independent sets of M with size k.

On the other hand, denoting the truncation of M to rank k by $T_k(M)$ and assuming the ground set of M has cardinality n, the dual to $T_k(M)$ has as its bases the spanning sets of the dual to M with cardinality equal to $n-k$. The dual to $T_k(M)$, denoted $E_{n-k}(M)$, is a matroid called the *elongation* of M to rank $n-k$, and consequently, one has the relation [23]:

2.2.6 Proposition. *Denote by $T_k(M)$ the truncation of a matroid to rank k and $E_k(M)$ the elongation of a matroid to rank k. Then $T_k(M^\perp) = E_{n-k}(M)^\perp$.*

Alternatively, given an integer k between $r(M)$ and n, the elongation of M to rank k is the matroid whose independent sets are the subsets A of the ground set of M for which $n - r(A) \leq k$. Although the terms are suggestive, in general, truncation does not commute with elongation. Additionally, one may consider the truncation and elongation by i ranks, which we will denote by $T^i(M)$ and $E^i(M)$, respectively.

Note that although we will be primarily concerned with vector matroids, other families of matroids exist. For example, given a field extension $\mathbb{G} \,/\, \mathbb{F}$, one may form a matroid on a finite collection E of elements of $\mathbb{G}$ by taking as independent sets the subsets of E whose elements are algebraically independent over $\mathbb{F}$. Such a matroid is

called an *algebraic* matroid, and as one might expect, its bases are the transcendence bases of the field extension [4]. Given an $\mathbb{F}$-linear matroid M, one may show that the inner product of the $\mathbb{F}$-coordinate vector of a vector v relative to a fixed basis of the k-dimensional vector space over $\mathbb{F}$ with a fixed collection of k transcendentals over $\mathbb{F}$ is an algebraic representation of M (see [18]). Consequently, every linear matroid is also an algebraic matroid; on the other hand, not every algebraic matroid is linear, and furthermore, not every matroid is algebraic.

Another class of matroids are the so-called *graphic* matroids: matroids whose independent sets are the forests of an undirected graph with finitely many vertices. Moreover, the bases of a graphic matroid are the spanning forests of the underlying graph. Since the incidence matrix of an (oriented) graph G defines a vector matroid isomorphic to the matroid corresponding to G, every graphic matroid is also linear (see [18]). However, not every linear matroid is graphic: the vector matroid of

$$A := \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix} \in \mathbb{F}_2^{3\times 7},$$

called the *Fano plane* and computed in 2.1.2 as a generator matrix for the 3-dimensional binary simplex code, is not graphic. To see this, note that A has rank 3, hence each spanning tree of the associated graph G would have 3 edges. Thus, G should possess 4 vertices, supporting at most 6 edges, insufficient for the 7 edges implied by A.

As a final remark to illustrate the ubiquity (and utility) of matroids, notice that one may generalize Kruskal's algorithm for computing a minimum weight spanning forest of a weighted undirected graph to matroids. Kruskal's algorithm can in fact be generalized to the naive greedy algorithm, which correctly computes a minimum weight basis of a *weighted* matroid: a matroid $(E, \mathcal{I})$ for which there exists a mapping $w\colon E \longrightarrow \mathbb{R}$, called its *weight function*. Finally, the naive greedy algorithm fails to produce an optimal solution on simplicial complexes which are not matroids [18].

2.3 Free Resolutions and Hochster's Formula

Since we wish to illuminate the structure of vector matroids via algebraic means, we turn to Stanley-Reisner theory. Stanley-Reisner theory connects the homological properties of a simplicial complex to those of an associated squarefree monomial ideal, the Stanley-Reisner ideal. As we will primarily be working with squarefree ideals, we define

$$x_\sigma := \prod_{i \in \sigma} x_i,$$

provided that $\sigma \subseteq [n]$.

2.3.1 Definition. Let Δ be a simplicial complex with vertex set $[n]$ and let $S := \mathbb{F}[x_1, \ldots, x_n]$ be a polynomial ring in n variables over a field $\mathbb{F}$. Then the *Stanley-Reisner ideal* of Δ is

$$I(\Delta) := (x_\sigma \,|\, \sigma \notin \Delta)\,.$$

In fact, $I(\Delta)$ is minimally generated by the monomials x_σ for which σ is a minimal nonface (with respect to inclusion).

The *Stanley-Reisner ring* or *face ring* of Δ is the quotient ring $\mathbb{F}[\Delta] := S/I(\Delta)$. To understand the structure of the Stanley-Reisner ring of a simplicial complex, we regard it as a graded ring, defined as follows:

2.3.2 Definition. Let R be a ring, A a commutative monoid, and assume there are abelian groups R_i such that

$$R = \bigoplus_{i \in A} R_i,$$

where $R_i R_j \subseteq R_{i+j}$. Then R is said to be *A-graded* (or simply *graded*) and the i-th summand R_i is called the *i-th graded component* of R. Elements of R_i are said to be *homogeneous* with *degree* i, while A is called the *monoid of degrees* of R.

Two commonly chosen monoids of degrees are $\mathbb{Z}$, giving the *$\mathbb{Z}$-grading* of R, and

$\mathbb{Z}^n$ with componentwise addition, giving the $\mathbb{Z}^n$-*grading* of R. If R is a graded ring with i-th graded component R_i, the *d-th twist* or *shift* of R, denoted $R(-d)$, is defined to be R with i-th graded component R_{i-d}. Given a graded ring, one can define graded modules with respect to the grading of the given ring:

2.3.3 Definition. Let M be an R-module, where $R = \oplus_{i \in A} R_i$ is a graded ring with monoid of degrees A. Assume there are abelian groups M_i such that

$$M = \bigoplus_{i \in A} M_i,$$

where $R_i M_j \subseteq M_{i+j}$. Then M is said to be *graded*.

Graded components, homogeneous elements, and twists of modules are defined analogously. In particular, we will denote the degree i component of a graded module M by M_i. If M and N are graded R-modules and $\varphi\colon M \to N$ is R-linear, then φ is said to be *graded* or *homogeneous* with *degree d* provided that $\varphi(M_i) \subseteq N_{i+d}$ for each degree i.

2.3.4 Definition. Let M be a module. Suppose R is a ring and $\{F_i\}$ a family of free R-modules. Then a complex

$$\mathfrak{F}\colon \cdots \to F_i \to F_{i-1} \to \cdots \to F_1 \to F_0$$

is called a *free resolution* of M if $\mathfrak{F}$ is exact and the cokernel of the map $F_1 \to F_0$ is isomorphic to M. In the event that R is a graded ring, each F_i is a graded free module, and each map $F_i \to F_{i-1}$ is homogeneous of degree zero, $\mathfrak{F}$ is called a *graded free resolution* of M.

This notation is frequently abused by writing $\mathfrak{F}$ as

$$\mathfrak{F}\colon \cdots \to F_i \to F_{i-1} \to \cdots \to F_1 \to F_0 \to M \to 0$$

with the stipulation that all modules in $\mathfrak{F}$ are free except possibly M. If $\mathfrak{F}$ is a free resolution with free modules F_i and there exists an integer n such that $F_i = 0$ for all

$i > n$, then the smallest such n is called the *length* of $\mathfrak{F}$ or *projective dimension* of M.

One can compute a free resolution through repeated kernel calculations. In particular, let R be a ring and let M an R-module with s generators. Consider the map induced by sending the k-th generator of R^s to the k-th generator of M. The kernel of this map, a free R-module consisting of the linear relations among the generators of M, is called the *first syzygy module* of M and is denoted $\mathrm{Syz}_1(M)$. Elements of $\mathrm{Syz}_1(M)$ are called *first syzygies* (or simply *syzygies*). Then, after finding a generating set for $\mathrm{Syz}_1(M)$ with s_1 generators, consider the map induced by sending the k-th generator of R^{s_1} to the k-th generator of $\mathrm{Syz}_1(M)$, and proceed as before. Repeating this process, with the role of $\mathrm{Syz}_i(M)$ replacing that of $\mathrm{Syz}_{i-1}(M)$ at the start of each step, one obtains a diagram of the form:

$$\cdots \dashrightarrow F_i \dashrightarrow F_{i-1} \dashrightarrow \cdots \dashrightarrow F_0 \longrightarrow M \longrightarrow 0$$

$$\mathrm{Syz}_i(M)$$

Together with the compositions $F_i \dashrightarrow F_{i-1}$ as differentials, the free modules $F_i \cong \oplus_{k \in I_i} R$ form a free resolution of M. If M is graded, then by choosing a twist d_k for each copy of R in $\oplus_{k \in I_i} R$ so that the map $F_i \to \mathrm{Syz}_i(M)$ is homogeneous of degree zero, one obtains a graded free resolution. If a minimal generating set is chosen for M and each $\mathrm{Syz}_i(M)$, one obtains a *minimal graded free resolution* which is unique up to isomorphism. This process is not generally guaranteed to terminate; however, if M is finitely generated and R is a polynomial ring in n variables over a field, it will [4]:

2.3.5 Theorem (Hilbert's Syzygy Theorem)**.** *Let $R = \mathbb{F}[x_1, \ldots, x_n]$ be a polynomial ring in n variables over a field $\mathbb{F}$, and let M be a finitely generated graded R-module. Then there exists a graded free resolution of M, with length at most n, by finitely generated free modules.*

Let $R := \mathbb{F}[x_1, \ldots, x_n]$, with $\mathbb{F}$ a field. If $\mathfrak{F}$ is a minimal graded free resolution of

a finitely generated graded R-module M, then $\mathfrak{F}$ can be written as

$$\mathfrak{F}\colon F_n \to F_{n-1} \to \cdots \to F_2 \to F_1 \to F_0,$$

where the differential maps are homogeneous maps in degree 0 and

$$F_i \cong \bigoplus_{j \in A} R(-j)^{\beta_{i,j}}.$$

The exponent $\beta_{i,j}$, where j is taken to be an element of the monoid of degrees, is called the *i-th Betti number in degree j*. The *Betti table* of a free resolution of a $\mathbb{Z}$-graded module is an array for which the entry in the i-th column and j-th row is $\beta_{i,i+j}$. The smallest integer r such that all generators of F_i have degree at most $r+i$ is called the *Castelnuovo-Mumford regularity* (or simply the *regularity*) of M, and is denoted $\operatorname{reg} M$. If the regularity of M is also the largest integer r such that all generators of F_i have degree at least $r+i$, then $\mathfrak{F}$ is said to be a *linear* free resolution of M. Note that the differentials of a free resolution, being maps between free modules over R, are R-linear, hence can be implemented with matrices; the column spaces of these matrices are the syzygy modules of M.

Of particular interest are the free resolutions which are *pure*, in which each F_i is twisted in exactly one degree; by the Boij-Söderberg theory, every Betti table can be decomposed into a positive $\mathbb{Q}$-linear combination of pure Betti tables. Although the theory provides that a given Betti table can be algorithmically decomposed into pure Betti tables, it does not provide a means by which to compute modules whose Betti diagrams are the diagrams in the Boij-Söderberg decomposition of a given module's Betti table.

2.3.6 Example. Let $R := \mathbb{Q}[x_0, x_1, x_2]$ and set $I := (x_0x_1, x_0x_2, x_1x_2)$. Then a minimal $\mathbb{Z}$-graded resolution of R/I is

$$\mathfrak{F}\colon R(-3)^2 \xrightarrow{\begin{bmatrix} -x_2 & 0 \\ x_1 & -x_1 \\ 0 & x_0 \end{bmatrix}} R(-2)^3 \xrightarrow{\begin{bmatrix} x_0x_1 & x_0x_2 & x_1x_2 \end{bmatrix}} R$$

with Betti numbers $\beta_{1,2} = 3$, $\beta_{2,3} = 2$, and $\beta_{i,j} = 0$ otherwise. Moreover, $\mathfrak{F}$ is linear, hence also pure. Its Betti table is

$\beta_{i,j}$	0	1	2
0	1	0	0
1	0	3	2

,

where the i-th entry in the j-th column is $\beta_{i,i+j}$.

One can obtain free resolutions (and sometimes minimal free resolutions) from other free resolutions via the mapping cone construction.

2.3.7 Proposition. *Assume R is a graded ring and*

$$0 \to A \to B \to C \to 0$$

is a short exact sequence of graded R-modules. Furthermore, assume there are graded free resolutions

$$\mathfrak{A}\colon 0 \to F_a^A \xrightarrow{d_a^A} F_{a-1}^A \xrightarrow{d_{a-1}^A} \cdots \xrightarrow{d_2^A} F_1^A \xrightarrow{d_1^A} A \to 0$$

and

$$\mathfrak{B}\colon 0 \to F_b^B \xrightarrow{d_b^B} F_{b-1}^B \xrightarrow{d_{b-1}^B} \cdots \xrightarrow{d_2^B} F_1^B \xrightarrow{d_1^B} B \to 0$$

for A and B, respectively. Then the map $A \to B$ induces R-linear maps $f_i\colon F_i^A \longrightarrow F_i^B$, called comparison maps *between $\mathfrak{A}$ and $\mathfrak{B}$, for which the squares*

$$\begin{array}{ccc} F_{i-1}^A & \xrightarrow{f_{i-1}} & F_{i-1}^B \\ {\scriptstyle d_i^A}\uparrow & & \uparrow{\scriptstyle d_i^B} \\ F_i^A & \xrightarrow{f_i} & F_i^B \end{array}$$

commute.

If necessary, extend $\mathfrak{A}$ or $\mathfrak{B}$ by adding copies of the zero module so that they

are the same length, say n, and let f_i be comparison maps between $\mathfrak{A}$ and $\mathfrak{B}$. The *mapping cone* of $\mathfrak{A}$ and $\mathfrak{B}$ with comparison maps f_i is the resolution

$$0 \to F_n^A \xrightarrow{\partial_{n+1}} F_{n-1}^A \oplus F_n^B \xrightarrow{\partial_n} \cdots \xrightarrow{\partial_3} F_1^A \oplus F_2^B \xrightarrow{\partial_2} A \oplus F_1^B \xrightarrow{\partial_1} C \to 0$$

of C, where the differential maps

$$\partial_i \colon F_{i-1}^A \oplus F_i^B \longrightarrow F_{i-2}^A \oplus F_{i-1}^B$$

of the mapping cone are defined by the rule

$$\partial_i = \begin{bmatrix} d_i^B & (-1)^{i-1} f_{i-1} \\ 0 & d_{i-1}^A \end{bmatrix}.$$

Even if $\mathfrak{A}$ and $\mathfrak{B}$ are minimal, the mapping cone of $\mathfrak{A}$ and $\mathfrak{B}$ may not necessarily be minimal; however, if $\mathfrak{A}$ and $\mathfrak{B}$ are minimal and the comparison maps f_i between $\mathfrak{A}$ and $\mathfrak{B}$ satisfy $f_i(F_i^A) \subseteq \mathfrak{m} F_i^B$, where $\mathfrak{m}$ is the irrelevant maximal ideal, the mapping cone will be minimal.

As the differential maps in a free resolution of a free module are frequently rather complicated, we wish to express them in a more illuminative manner whenever possible. One means of doing so is via a cellular resolution, provided that the given module supports one. In the following, we largely adopt the notation and terminology in [1], albeit with a focus on resolutions of finitely generated monomial ideals. For further reference, one may wish to consult [13] or [19].

Let $R := \mathbb{F}[x_1, \ldots, x_n]$. Assume I is a finitely generated monomial R-ideal, hence generated by its minimal monomials under divisibility. Let $\min I := \{m_i \,|\, i \in I\}$ be the minimal generating set for I, and let X be a regular cell complex with each vertex labeled by one member of $\min I$. If F is a face in X, set $m_F := \operatorname{lcm}\{m_i \,|\, i \text{ is a vertex of } F\}$ and let a_F denote the exponent vector of m_F. If $F = \emptyset$, we define $m_F := 1$. As X is a regular cell complex, it admits an *incidence* function – a function $\varepsilon(F, G)$ on every pair of faces (F, G), such that $\varepsilon(F, G) = \pm 1$ if F is a facet of G, $\varepsilon(F, G) = 0$ otherwise, $\varepsilon(\emptyset, G) = 1$ if $\dim G = 0$, and for faces F of G with

codimension 2,

$$\varepsilon(F, F_1)\varepsilon(F_1, G) + \varepsilon(F, F_2)\varepsilon(F_2, G) = 0,$$

where F_1 and F_2 are facets of G each containing F. For a proof of the existence of an incidence function on regular cell complexes, one may wish to consult [12].

2.3.8 Definition. The *cellular complex* of I supported by X is the $\mathbb{Z}^n$-graded complex

$$\mathfrak{F}_X \colon F_{n-1} \xrightarrow{\partial_{n-1}} F_{n-2} \xrightarrow{\partial_{n-2}} \cdots \xrightarrow{\partial_1} F_0 \xrightarrow{\partial_0} F_{-1}$$

where

$$F_i := \bigoplus_{F \in X,\ \dim F = i} R(-a_F)$$

with differential maps $\partial_i \colon F_i \longrightarrow F_{i-1}$ induced by extending

$$\partial_i(e_G) := \sum_{\substack{\text{facets } F \\ \text{of } G \in X}} \varepsilon(F, G)\frac{m_G}{m_F} e_F$$

linearly, where e_G is a free generator for F_i in degree a_G and e_F is a free generator for F_{i-1} in degree a_F.

2.3.9 Example. Let X be the complex consisting of three vertices $\{G_1, G_2, G_3\}$, with G_1, G_2 connected by the edge H_1 and G_2, G_3 connected by the edge H_2; label the vertices $m_{G_1} := x_0x_2$, $m_{G_2} := x_0x_1$, and $m_{G_3} := x_1x_2$ to obtain the complex in Figure 2.1 as the associated labeled cell complex. Set $\varepsilon(G_1, H_1) := \varepsilon(G_1, H_2) := -1$ and $\varepsilon(G_2, H_1) := \varepsilon(G_3, H_2) := 1$. Thus, there are differentials $\partial_1 \colon F_1 \longrightarrow F_0$ and $\partial_0 \colon F_0 \longrightarrow F_{-1}$, and hence a $\mathbb{Z}^n$-graded cellular complex of $(m_{G_1}, m_{G_2}, m_{G_3})$. As $\beta_{i,j} = \sum_{i,|\sigma|=j} \beta_{i,\sigma}$, one can obtain a $\mathbb{Z}$-graded complex from the aforementioned $\mathbb{Z}^n$-graded cellular complex. The differentials of this $\mathbb{Z}$-graded complex can be implemented via the matrices in Example 2.3.6 through appropriate choices of bases; consequently, the $\mathbb{Z}$-graded complex is also a free resolution.

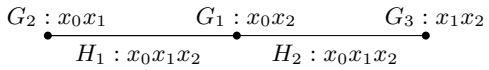


Figure 2.1: The labeled cell complex associated to the ideal (x_0x_2, x_0x_1, x_1x_2).

Not every cellular complex is a free resolution; those which are free resolutions are called *cellular resolutions*. In general, whether a given complex is a free resolution depends on the field of coefficients of the underlying polynomial ring; a complex which is a free resolution with respect to one field may fail to be a free resolution with respect to another field. However, due to the independence of the incidence function from the field, if a complex is a cellular resolution, it is also (remarkably) a free resolution over any field.

There is a characterization of exactness of complexes discussed in [13], and for this we again largely adopt its notation and terminology. Let X be a labeled cell complex and let X_i denote the collection of i-faces of X. The *reduced chain complex* of X over the field $\mathbb{F}$ is the complex of $\mathbb{F}$-vector spaces

$$0 \to \mathbb{F}^{X_n} \to \cdots \to \mathbb{F}^{X_0} \to \mathbb{F}^{X_{-1}} \to 0$$

where $\mathbb{F}^{X_i}$ denotes the $\mathbb{F}$-vector space generated by the free generators e_σ, with σ an i-face. The differential maps $\partial_i \colon \mathbb{F}^{X_i} \longrightarrow \mathbb{F}^{X_{i-1}}$ of the reduced chain complex of X are defined by the rule

$$e_G \longmapsto \sum_{\substack{\text{facets } F \\ \text{of } G \in X}} \varepsilon(F, G) e_F,$$

where G is an i-face, and extending linearly. The *reduced homology* of X is the homology of the reduced chain complex of X.

Let d be a vector in $\mathbb{Z}^n$ and denote by $X_{\leq d}$ the subcomplex obtained from X by selecting the faces of X whose labels have $\mathbb{Z}^n$-graded degree componentwise at most d. Then from [13],

2.3.10 Proposition. *The cellular complex supported on X is a cellular resolution if*

and only if $X_{\leq d}$ either is empty or has zero reduced homology for every $d \in \mathbb{Z}^n$.

If $X_{\leq d}$ has zero reduced homology for every $d \in \mathbb{Z}^n$, we will say that X is *acyclic*.

2.3.11 Example. Let R be the polynomial ring over a field $\mathbb{F}$ in the n variables $x_1, \ldots, x_n$. Label each vertex v_i of the n-simplex $X^{(n)}$ with the variable x_i; then each restriction $X^{(n)}_{\leq d}$ of $X^{(n)}$ is a k-simplex on k variables. It follows that the cellular complex supported on $X^{(n)}_{\leq d}$ is a cellular resolution by induction and 2.3.10. As each summand in the maps involves at least (in fact, exactly) one variable, the cellular resolution is minimal and is called the *Koszul complex* of $(x_1, \ldots, x_n)$, the irrelevant maximal ideal. This renders the Betti numbers of the Koszul complex transparent – in particular, $\beta_{i,i} = \binom{n}{i}$. Thus, as a resolution of $\mathbb{F} \cong R/(x_1, \ldots, x_n)$, the Koszul complex is

$$0 \to \mathbb{F} \to \mathbb{F}^n \to \cdots \to \mathbb{F}^{\binom{n}{2}} \to \mathbb{F}^n \to \mathbb{F} \to 0.$$

Finally, the existence of the Koszul complex (as a resolution of $\mathbb{F}$) provides a particularly simple proof of Hilbert's Syzygy Theorem: the i-th Betti number in degree d of M is

$$\beta_{i,d}(M) = \dim_{\mathbb{F}} \operatorname{Tor}_i^R(M, \mathbb{F})_d,$$

but by the symmetry of $\operatorname{Tor}(-,-)$,

$$\operatorname{Tor}_i^R(M, \mathbb{F})_d \cong \operatorname{Tor}_i^R(\mathbb{F}, M)_d.$$

However, the latter vanishes for all $i > n$.

Cellular complexes of ideals can be generalized to cellular complexes of monomial modules which are generated by their minimal monomials. Furthermore, cellular complexes supported by a regular cell complex may be generalized to CW cellular complexes: chain complexes supported by a CW complex. As shown in [21] though, not every monomial module has a minimal free resolution supported by a CW complex.

Hochster's formula provides a means of connecting the combinatorial properties of a simplicial complex with free resolutions of its associated Stanley-Reisner ideal. First, some notation: given a simplicial complex Δ, we will denote by $\widetilde{H}^i(\Delta, \mathbb{F})$ the i-th simplicial cohomology group of Δ with coefficients from $\mathbb{F}$. Furthermore, we will regard a subset $\sigma \subseteq [n]$ as either a subset of $[n]$ or as a vector in $\{0,1\}^n$, depending on context.

2.3.12 Theorem (Hochster's Tor Formula)**.** *Let R be a polynomial ring in n variables with the $\mathbb{Z}^n$-grading. Suppose Δ is a simplicial complex on $[n]$ with Stanley-Reisner ideal $I(\Delta)$. Let $\sigma \subseteq [n]$. Then*

$$\operatorname{Tor}_{i-1}^R(I(\Delta), \mathbb{F})_\sigma \cong \widetilde{H}^{|\sigma|-i-1}(\Delta_\sigma, \mathbb{F}).$$

Assume M is an R-module, with $\mathfrak{F}$ a minimal free resolution. As before, note that by tensoring $\mathfrak{F}$ with $\mathbb{F}$ over R,

$$\beta_{i,d}(M) = \dim_{\mathbb{F}} \operatorname{Tor}_i^R(M, \mathbb{F})_d.$$

Thus, by applying Hochster's formula and taking dimension, one obtains Betti numbers for the face ring $k[\Delta]$ of

$$\beta_{i,\sigma}(k[\Delta]) = \dim_{\mathbb{F}} \widetilde{H}^{|\sigma|-i-1}(\Delta_\sigma, \mathbb{F})$$

provided that $i \geq 1$.

Chapter 3: Observations on Resolutions of the Stanley-Reisner Ideal of a Matroid

3.1 Free Resolutions Associated to Matroids

As the vector matroid M of a linear code $\mathcal{C}$ is also a simplicial complex, one avenue into studying the combinatorial properties of $\mathcal{C}$ (or equivalently, of a representable matroid) is via free resolutions of the Stanley-Reisner ideal of M – in fact, this is the approach we shall take. More generally, one may study free resolutions of the Stanley-Reisner ideal of a matroid. Such ideals satisfy several homological properties, two of which are that they are *Cohen-Macaulay* and *level*. We explore further homological consequences below.

3.1.1 Definition. If $R = (R, \mathfrak{m})$ is a noetherian local ring and M is a finitely generated R-module, then M is said to be *Cohen-Macaulay* if $\operatorname{depth} M = \dim M$. If R is a noetherian ring (not necessarily local) and M is a finitely generated R-module, then M is said to be *Cohen-Macaulay* if for every maximal ideal $\mathfrak{m}$ of R, the localization $M_{\mathfrak{m}}$ satisfies $\operatorname{depth} M_{\mathfrak{m}} = \dim M_{\mathfrak{m}}$.

In particular, the face ring of a matroid complex is Cohen-Macaulay, while the Krull dimension of the face ring of a matroid complex is equal to the matroid's rank. Thus, the Auslander-Buchsbaum formula implies that the projective dimension is equal to the rank of the dual matroid. In fact, the face ring of a matroid complex is level [20]:

3.1.2 Definition. Let A be a graded Cohen-Macaulay algebra over a field $\mathbb{F}$, and assume A has Krull dimension d. Then A is said to be *level* if every minimal free resolution of A as a module over a polynomial ring over $\mathbb{F}$ with n variables has the form

$$0 \to F_{n-d} \to \cdots \to F_0 \to A \to 0,$$

where the last module F_{n-d} is generated in one degree.

In the case of matroid complexes, one may go further: from the proof of Theorem 3.4 of [20], the last module F_{n-d} in a minimal free resolution of the face ring of a matroid complex with n elements in its ground set is minimally generated in degree n. In turn, this implies the regularity of the face ring is $d+1$.

Notice that as each facet of a matroid complex M is a basis of M, the minimal nonfaces of M are the circuits of M, and consequently, the Stanley-Reisner ideal of M is minimally generated by the monomials in the polynomial ring $R := \mathbb{F}[x_1, \ldots, x_n]$ (with n the cardinality of the ground set of M) whose support is an M-circuit. Conversely, the minimal generators of the Stanley-Reisner ideal of M each correspond to a minimal nonface of M, i.e., an M-circuit. Thus,

3.1.3 Proposition. *Let M be a matroid on a ground set with n elements, and let $I(M)$ be the Stanley-Reisner ideal of M. Then*

$$I(M) = (x_\sigma \,|\, \sigma \text{ is an } M\text{-circuit}).$$

A matroid may alternatively be characterized in terms of its circuits – if M is a matroid with C_1 and C_2 as two distinct circuits, and $x \in C_1 \cap C_2$, then there is an M-circuit C_3 such that

$$C_3 \subseteq (C_1 \cup C_2) - \{x\}.$$

As each minimal generator of the Stanley-Reisner ideal I of M has an M-circuit as its support, one may translate this into the following condition on the minimal generators of I: if x_{σ_1} and x_{σ_2} are distinct minimal generators of I and x_i is a variable which divides $\gcd(x_{\sigma_1}, x_{\sigma_2})$, then there is a third minimal generator x_{σ_3} of I for which

$$x_{\sigma_3} \;\Big|\; \frac{\operatorname{lcm}(x_{\sigma_1}, x_{\sigma_2})}{x_i}.$$

Such ideals are discussed further in [16] and [17].

Due to the importance of pure free resolutions, we focus on the Stanley-Reisner ideals of matroids whose free resolution is pure. In [16], an (essentially abstract) cellular resolution of the Stanley-Reisner ideal of a matroid is derived, and from this,

the authors of [17] obtain a characterization of the matroids whose Stanley-Reisner ideals support a pure minimal free resolution. We obtain the same characterization, albeit in a different manner, as follows.

A matroid M is said to be a *perfect matroid design* if each k-flat of M has the same cardinality, f_k. Let $E_k(M)$ be the elongation of M to rank k, and let $I(E_k(M))$ be the Stanley-Reisner ideal of $E_k(M)$. Then from [8],

$$\beta_{i,d}(I(E_k(M))) \neq 0 \iff \beta_{i-1,d}(I(E_{k+1}(M))) \neq 0.$$

Slightly rephrasing this in terms of the truncation to rank k and re-indexing,

3.1.4 Lemma. *Let M be a matroid on a ground set with cardinality n, and let $E_{n-k}(M^\perp) = T_k(M)^\perp$ be the dual to the truncation of M to rank k. Then*

$$\beta_{i,d}(I(T_k(M)^\perp)) \neq 0 \iff \beta_{i-1,d}(I(T_{k+1}(M)^\perp)) \neq 0.$$

Notice that if σ is a circuit of $T_k(M)^\perp$, where M is a matroid on a ground set E, then $E - \sigma$ is a hyperplane of $T_k(M)$. However, one may check that $r_k(A) := \min(k, r(A))$ is a rank function for $T_k(M)$, and so consequently, rank $k-1$ sets of $T_k(M)$ also have rank $k-1$ when considered as sets of M. Furthermore, a subset which is closed in $T_k(M)$ is also closed in M. As a result, $E - \sigma$ is a $(k-1)$-flat of M. The converse of these properties also applies, provided that the subset considered has rank at most $k-1$, thus,

3.1.5 Proposition. *The circuits of $T_k(M)^\perp$ are the complements (relative to the ground set of M) of the $(k-1)$-flats of M.*

Combining these, one obtains:

3.1.6 Proposition. *Let M be a matroid and let I be the Stanley-Reisner ideal of $M^\perp$. If M is a perfect matroid design, then I has a pure minimal free resolution.*

Proof. We will assume M is a perfect matroid design, with f_k as the cardinality of any k-flat, and prove that $I(M^\perp)$, the Stanley-Reisner ideal of the dual to M, has a

pure minimal free resolution. Let E denote the ground set of M and set $n := |E|$. Given the sequence of duals to truncations

$$\{T_k(M)^\perp \mid k = 0, \ldots, r(M)\},$$

one may induct on the members of this sequence. Consider $(T_0(M))^\perp$; $T_0(M)$ contains exactly one hyperplane, namely, the empty set. Consequently, using 3.1.5, $T_0(M)^\perp$ has exactly one circuit, $E - \emptyset = E$, so

$$\begin{aligned} I(T_0(M)^\perp) &= I(E_n(M^\perp)) \\ &= (x_E). \end{aligned}$$

This has the trivial resolution

$$0 \leftarrow R(-n) \leftarrow 0$$

as a minimal free resolution, where $R := \mathbb{F}[x_1, \ldots, x_n]$.

Let $\beta_{i,d}^{(k)}$ be the i-th Betti number in degree d of $I(E_{n-k}(M^\perp))$ and assume inductively that $I(E_{n-k}(M^\perp))$ has

$$0 \leftarrow R(-d_1)^{\beta_{1,d_1}^{(k)}} \leftarrow R(-d_2)^{\beta_{2,d_2}^{(k)}} \leftarrow \cdots \leftarrow R(-d_p)^{\beta_{p,d_p}^{(k)}} \leftarrow 0$$

as a minimal free resolution. Then, using 3.1.4, $I(E_{n-(k+1)}(M^\perp))$ has a minimal free resolution of the form

$$0 \leftarrow \bigoplus_{j \geq 0} R(-d_{0,j})^{\beta_{0,d_{0,j}}^{(k+1)}} \leftarrow R(-d_1)^{\beta_{1,d_1}^{(k+1)}} \leftarrow \cdots \leftarrow R(-d_p)^{\beta_{p,d_p}^{(k+1)}} \leftarrow 0.$$

It remains to show that $I(E_{n-(k+1)}(M^\perp))$ is generated in one degree. For this, note that

$$\begin{aligned} &x_\sigma \text{ is a minimal generator of } I(E_{n-(k+1)}(M^\perp)) \\ &\quad \iff \sigma \text{ is a circuit in } E_{n-(k+1)}(M^\perp) \end{aligned}$$

$$\iff \sigma \text{ is a circuit in } T_{k+1}(M)^{\perp}$$
$$\iff E - \sigma \text{ is a hyperplane in } T_{k+1}(M)$$
$$\iff E - \sigma \text{ is a } k\text{-flat in M},$$

where the last two equivalences follow from 3.1.5. However, k-flats in M are equicardinal by hypothesis – hence each x_σ has the same degree. $\square$

This logic reverses itself in the following manner. Again, we will denote the i-th Betti number in degree d of $I(E_{n-k}(M^{\perp}))$ by $\beta_{i,d}^{(k)}$. Additionally, assume $I(E_{n-k}(M^{\perp}))$ has the pure minimal free resolution

$$0 \leftarrow I(E_{n-k}(M^{\perp})) \leftarrow R(-d_1)^{\beta_{1,d_1}^{(k)}} \leftarrow R(-d_2)^{\beta_{2,d_2}^{(k)}} \leftarrow \cdots \leftarrow R(-d_p)^{\beta_{p,d_p}^{(k)}}.$$

Thus, the circuits of $T_k(M)^{\perp}$, hence hyperplanes of $T_k(M)$, each have cardinality d_1. But as the hyperplanes of $T_k(M)$ are $(k-1)$-flats of M, each of the $(k-1)$-flats of M are equicardinal. Applying 3.1.4 to the above resolution, one obtains the resolution

$$0 \leftarrow I(E_{n-(k-1)}(M^{\perp})) \leftarrow R(-d_2)^{\beta_{2,d_2}^{(k-1)}} \leftarrow \cdots \leftarrow R(-d_p)^{\beta_{p,d_p}^{(k-1)}}$$

for $I(T_{k-1}(M)^{\perp})$; the same logic implies that the $(k-2)$-flats of M are equicardinal. By induction, each flat of M of a given rank is equicardinal. Thus, we obtain the converse, hence

3.1.7 Theorem. *Let M be a matroid and let I be the Stanley-Reisner ideal of $M^{\perp}$. Assume $\mathfrak{F}$ is a minimal free resolution of I. Then $\mathfrak{F}$ is pure if and only if M is a perfect matroid design.*

This argument suggests a more general relation between the dependent sets of a matroid and the flats of its dual. Recall that the elongation of a matroid $M = (E, \mathcal{I})$ by i ranks is defined to be the matroid whose independent sets are the subsets $A \subseteq E$ for which $n_M(A) := |A| - r_M(A) \leq i$. Denote the elongation of M by i ranks by $E^i(M)$ and the truncation by i ranks $T^i(M)$; rewriting 2.2.6 in terms of $E^i(M)$ and $T^i(M)$, one obtains $E^i(M) = T^i(M^{\perp})^{\perp}$. Furthermore, note from Proposition 1 of [8]

that

$$n_{E^i(M)}(A) = \begin{cases} n_M(A) - i & \text{if } n_M(A) > i \\ 0 & \text{otherwise.} \end{cases}$$

If $\sigma \subseteq E$ is an inclusion-minimal set for which $n_M(\sigma) = i$, then $n_{E^{i-1}(M)}(\sigma) = n_M(\sigma) - (i-1) = 1$, hence σ is an $E_{i-1}(M)$-circuit. But $E^{i-1}(M) = T^{i-1}(M^\perp)^\perp$, so $E - \sigma$ is a $T^{i-1}(M^\perp)$-hyperplane, and thus a $(r(M^\perp) - i)$-flat of $M^\perp$. Again, this logic is reversible, therefore providing the following duality:

3.1.8 Proposition. *Assume M is a matroid with ground set E. Then $n_M(\sigma) = i$ if and only if $E - \sigma$ is a $(r(M^\perp) - i)$-flat of $M^\perp$.*

In particular, this provides another combinatorial characterization for the $\mathbb{Z}^n$-graded Betti numbers of the Stanley-Reisner ideal of a matroid; in conjunction with Theorem 1 of [9], $\beta_{i,\sigma} \neq 0$ if and only if σ is the complement of a $(r(M^\perp) - i)$-flat of $M^\perp$. Thus, as we expect, if the flats of $M^\perp$ are equicardinal in each dimension, the minimal free resolution of the Stanley-Reisner ideal of M will be pure.

3.2 Generalized Hamming Weights of Matroids

Following [9], one may extend the notion of generalized Hamming weights of a code to matroids:

3.2.1 Definition. Let M be a matroid with vertices E. The *i-th generalized Hamming weight* of M, denoted $d_i(M)$, is

$$d_i(M) := \min\{|\sigma| \mid \sigma \subseteq E \text{ and } |\sigma| - \dim M_\sigma - 1 = i\},$$

where $\sigma \subseteq E$, and $1 \leq i \leq |E| - \dim M - 1$.

In analogy with linear block codes, the set of generalized Hamming weights of a matroid M is called the *higher weight hierarchy*. As shown in [9], if M is the vector matroid of a parity check matrix for a linear code $\mathcal{C}$, the generalized Hamming weights of M and $\mathcal{C}$ are equal. The authors of [9] established the following lemma

and theorem; here, we provide simplified proofs. First, some notation: assume M is a matroid. By taking the independent sets of M to be faces, M is also naturally a simplicial complex. If σ is a subset of the ground set of M, we define M_σ to be the subcomplex of M induced by σ – thus, the faces of M_σ consist of the faces of M which are subsets of σ. We also identify σ as either a vector in $\{0,1\}^n \subseteq \mathbb{N}^n$ with support equal to σ, or, depending on context, a subset of $[n]$.

3.2.2 Lemma. *Let M be a matroid on $[n]$, with σ a face. Let $\beta_{i,d}$ be the i-th Betti number in degree $d \in \mathbb{N}^n$ of the free resolution for the Stanley-Reisner ideal corresponding to M. Then $\beta_{i-1,\sigma}$ is nonzero if and only if $i = |\sigma| - \dim M_\sigma - 1$.*

Proof. Since each subcomplex M_σ is a matroid and thus Cohen-Macaulay, we get that $\widetilde{H}^{|\sigma|-i-1}(M_\sigma, \mathbb{F}) \neq 0$ if and only if $|\sigma| - i - 1 = \dim M_\sigma$. The result then follows by applying Hochster's Tor formula and taking dimension. □

As one may then expect, the minimal degree shifts in a minimal free resolution of the Stanley-Reisner ideal of a matroid are thus matroid's generalized Hamming weights:

3.2.3 Theorem. *The generalized Hamming weights of a matroid M with vertices E are given by*

$$d_i = \min\{d \,|\, \beta_{i-1,d} \neq 0\}$$

for $1 \leq i \leq |E| - \dim M + 1$ where $\beta_{i,d}$ is the i-th Betti number of M in degree d.

Proof. Applying Hochster's Tor formula, along with 3.2.2:

$$\begin{aligned}
&\min\{d \,|\, |\sigma| = d \text{ and } \beta_{i-1,\sigma} \neq 0\} \\
&\quad = \min\{d \,|\, |\sigma| = d \text{ and } \widetilde{H}^{|\sigma|-i-1}(M_\sigma, \mathbb{F}) \neq 0\} \\
&\quad = \min\{d \,|\, |\sigma| = d \text{ and } |\sigma| - i - 1 = \dim M_\sigma\} \\
&\quad = \min\{|\sigma| \mid |\sigma| - \dim M_\sigma - 1 = i\} \\
&\quad = d_i.
\end{aligned}$$

□

Recall that the Stanley-Reisner ideal of a matroid M is generated by the minimal nonfaces of M, considered as a simplicial complex, i.e., the M-circuits. If M is the vector matroid of a linear code's parity check matrix, this relationship extends to the underlying code. If A is a matrix with columns labeled 1 through n, and $\sigma \subseteq [n]$, we will denote by A_σ the matrix whose columns are the columns of A whose labels are in σ.

Assume M is the vector matroid of a parity check matrix H of a linear code $\mathcal{C}$ with block length n. Thus, the bases of M are the subsets $\sigma \subseteq [n]$ for which the columns of H_σ are linearly independent, and if $\tau \subseteq [n]$ contains σ as a proper subset, then the columns of H_τ are linearly dependent. If σ is an M-basis, the addition of any one element from $[n] - \sigma$ produces a dependent set. Although not necessarily an M-circuit itself, this dependent set does contain at least one M-circuit, τ. Furthermore, the columns of H_τ are linearly dependent, and thus, correspond to a codeword of $\mathcal{C}$ with support equal to τ. As proper subsets of τ are independent and are thus not the support of a codeword, τ is a minimal 1-support of $\mathcal{C}$. Conversely, a minimal 1-support of $\mathcal{C}$ is also an M-circuit, thus, one obtains the following (equivalent to Proposition 9.2.4 of [18]):

3.2.4 Proposition. *Let $\mathcal{C}$ be a linear block code with parity check matrix H, and let $I(\mathcal{M}(\mathcal{C}))$ denote the Stanley-Reisner ideal of the vector matroid of H. Then*

$$I(\mathcal{M}(\mathcal{C})) = (x_\sigma \,|\, \sigma \text{ is a minimal 1-support of } \mathcal{C}) .$$

Chapter 4: Resolutions of Cyclic Codes

4.1 Cyclic Codes and their Stanley-Reisner Ideals

Recall that a cyclic code $\mathcal{C}$ with block length n is a code for which whenever $c = (c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}$ is a codeword, $\sigma(c) := (c_{n-1}, c_0, c_1, \ldots, c_{n-2})$, called the *cyclic shift* of c is also a codeword in $\mathcal{C}$. One may then check that $\{\sigma, \sigma^2, \ldots\}$ is the cyclic group of order n and thus σ induces a group action on $\mathcal{C}$. We will show that this group action also induces a group action on the corresponding Stanley-Reisner ideal.

Let $R := \mathbb{F}[x_1, \ldots, x_n]$ and let $s := \{s_1, \ldots, s_p\} \subseteq [n]$. Define

$$\sigma(s) := \{(s_1 + 1) \mod n, \ldots, (s_p + 1) \mod n\}$$

and, if m is a squarefree monomial in R, set $\sigma_0(m)$ to be the squarefree monomial in R with support equal to $\sigma(\text{supp}(m))$. Given squarefree monomials $m_1, \ldots, m_k \in R$ and scalars $a_1, \ldots, a_k \in \mathbb{F}$, we define

$$\sigma_0(a_1 m_1 + \cdots + a_k m_k) := a_1 \sigma_0(m_1) + \cdots + a_k \sigma_0(m_k).$$

Assume $\mathcal{C}$ has $s := \{s_1, \ldots, s_p\}$ as a minimal 1-support. As each 1-support is the support of at least one codeword in $\mathcal{C}$, let $c \in \mathcal{C}$ be a codeword with support s. Since $\sigma(c)$ is also a codeword, one has that $\sigma(s)$ is also a 1-support and is in fact minimal. To see this, note that $\sigma^{-1}(c) := \sigma^{n-1}(c)$ is a codeword in $\mathcal{C}$, with support

$$\sigma^{-1}(s) := \{(s_1 - 1) \mod n, \ldots, (s_p - 1) \mod n\}.$$

Assume s is minimal, but that $\sigma(s)$ is not minimal; thus there is a 1-support $t \subseteq \sigma(s)$ with size strictly less than $\sigma(s)$, and consequently $\sigma^{-1}(t)$ is a 1-support properly contained in s, a contradiction to the minimality of s.

Let $\mathcal{M}(\mathcal{C})$ denote the vector matroid corresponding to a parity check matrix of

$\mathcal{C}$, with $I \subseteq R := \mathbb{F}[x_1, \ldots, x_n]$ the Stanley-Reisner ideal of $\mathcal{M}(\mathcal{C})$. Each minimal 1-support of $\mathcal{C}$ bijectively corresponds to a minimal generator of I. Thus, given a squarefree monomial $m \in R$, one may specialize σ to I; by the previous discussion, if m is a minimal generator of I, then so is $\sigma_0(m)$.

Fix an ordering $\{m_1, \ldots, m_{k_0}\}$ of the minimal generators of I and for each such generator m_i, find coefficients $a_{1,i}, \ldots, a_{k_0,i}$ such that

$$\sigma_0(m_i) = a_{i,1}m_1 + \ldots + a_{i,k_0}m_{k_0}.$$

Thus, one computes a $k_0 \times k_0$ permutation matrix

$$A_1 := \begin{bmatrix} a_{1,1}^{(1)} & \cdots & a_{k_0,1}^{(1)} \\ \vdots & \ddots & \vdots \\ a_{k_0,1}^{(1)} & \cdots & a_{k_0,k_0}^{(1)} \end{bmatrix}$$

Since exactly one of the coefficients $a_{1,i}, \ldots, a_{k_0,i}$ is nonzero, we have $\sigma_0(m_i) = m_j$ for some j, and thus inductively, $\sigma_0^{p-1}(m_i) = m_j$ for some j; hence we may define

$$\sigma_0^p(m_i) := \sigma_0(\sigma_0^{p-1}(m_i)).$$

Furthermore, given a minimal generator m_i of I, there is a codeword $c \in \mathcal{C}$ with support equal to the support of m_i, and $\sigma^n(c) = c$; consequently, $\sigma_0^n(m_i) = m_i$ for each minimal generator m_i.

Let s denote a $k_0 \times 1$ column vector with monomial entries and extend σ_0 by defining $\sigma_0(s)$ to be the $k_0 \times 1$ vector obtained from s by replacing each entry m of s with $\sigma_0(m)$. As before, $\sigma_0^n(s) = s$. With this notation, define

$$\sigma_1(s) := A_1\sigma_0(s).$$

Since the order of the isotropy subgroup of each m_i divides n, $A_1^n = I_{k_0}$, the $k_0 \times k_0$ identity. Noting that $\sigma_0(A_1 s) = A_1\sigma_0(s)$ and defining

$$\sigma_1^p(s) := \sigma_1(\sigma_1^{p-1}(s))$$

we get

$$\begin{aligned}\sigma_1^p(s) &= \sigma_1(\sigma_1^{p-1}(s)) \\ &= \sigma_1(A_1^{p-1}\sigma_0^{p-1}(s)) \\ &= A_1\sigma_0(A_1^{p-1}\sigma_0^{p-1}(s)) \\ &= A_1^p\sigma_0^p(s)\end{aligned}$$

by induction on p. Consequently, $\sigma_1^n(s) = s$, and furthermore, σ_1 induces a group action on R^{k_0}.

More generally, we proceed recursively as follows. Choose a free resolution $\mathfrak{F}$ of $I = (m_1, \ldots, m_{k_0})$ and assume σ_{m-1} has been computed. Let $r_1, \ldots, r_{k_{m-1}}$ be minimal generators for $\mathrm{Syz}_{m-1}(I)$ and for each i, find coefficients $a_{i,1}^{(m)}, \ldots, a_{i,k_{m-1}}^{(m)}$ such that

$$\sigma_{m-1}(r_i) = \sum_{j=1}^{k_{m-1}} a_{i,j}^{(m)} r_{i,j}$$

for each entry $r_{i,j}$ of r_i. Define

$$A_m := \begin{bmatrix} a_{1,1}^{(m)} & \cdots & a_{1,k_{m-1}}^{(m)} \\ \vdots & \ddots & \vdots \\ a_{k_{m-1},1}^{(m)} & \cdots & a_{k_{m-1},k_{m-1}}^{(m)} \end{bmatrix}$$

and if $s \in R^{k_{m-1}}$, set

$$\sigma_m(s) := A_m\sigma_0(s)$$

and

$$\sigma_m^p(s) := \sigma_m(\sigma_m^{p-1}(s)).$$

As before, one may compute that $A_m\sigma_0(s) = \sigma_0(A_m s)$, so inducting on p,

$$\sigma_m^p(s) = \sigma_m(\sigma_m^{p-1}(s))$$

$$
\begin{aligned}
&= \sigma_m(A_m^{p-1}\sigma_0^{p-1}(s)) \\
&= A_m\sigma_m(A_m^{p-1}\sigma_0^{p-1}(s)) \\
&= A_m^p\sigma_0^p(s).
\end{aligned}
$$

One may alternatively compute σ_m^{n+1} by finding coefficients $b_{i,1}^{(m)}, \ldots, b_{i,k_{m-1}}^{(m)}$ such that

$$
\sigma_{m-1}^{n+1}(r_i) = \sum_{j=1}^{k_{m-1}} b_{i,j}^{(m)} r_{i,j}
$$

But by induction, $\sigma_{m-1}^{n+1} = \sigma_{m-1}$, so $b_{i,j}^{(m)} = a_{i,j}^{(m)}$, and thus $\sigma_m^{n+1} = \sigma_m$.

Furthermore, note that each σ_m maps $\mathrm{Syz}_m(I)$ into itself. Assume $s = [s_1, \ldots, s_{k_m}]^T \in \mathrm{Syz}_m(I)$ and let $r_1, \ldots, r_{k_m}$ denote the minimal generators of $\mathrm{Syz}_{m-1}(I)$ used to compute σ_m. Note that by construction,

$$
[\sigma_{m-1}(r_1) \cdots \sigma_{m-1}(r_{k_m})] = [r_1 \cdots r_{k_m}]\, A_m
$$

Thus,

$$
\begin{aligned}
\begin{bmatrix} r_1 & \cdots & r_{k_m} \end{bmatrix} \sigma_m(s) &= \begin{bmatrix} r_1 & \cdots & r_{k_m} \end{bmatrix} A_m\sigma_0(s) \\
&= \begin{bmatrix} r_1 & \cdots & r_{k_m} \end{bmatrix} A_m \begin{bmatrix} \sigma_0(s_1) \\ \vdots \\ \sigma_0(s_{k_m}) \end{bmatrix} \\
&= \begin{bmatrix} \sigma_{m-1}(r_1) & \cdots & \sigma_{m-1}(r_{k_m}) \end{bmatrix} \begin{bmatrix} \sigma_0(s_1) \\ \vdots \\ \sigma_0(s_{k_0}) \end{bmatrix} \\
&= \sigma_0(s_1)\sigma_{m-1}(r_1) + \cdots + \sigma_0(s_{k_m})\sigma_{m-1}(r_{k_m}) \\
&= A_{m-1}(\sigma_0(s_1)\sigma_0(r_1) + \cdots + \sigma_0(s_{k_m})\sigma_0(r_{k_m})) \\
&= A_{m-1}\sigma_0(s_1r_1 + \cdots + s_{k_m}r_{k_m}) \\
&= 0,
\end{aligned}
$$

so by induction, each element in the orbit of s is also a syzygy. Consequently,

4.1.1 Proposition. *Let $\mathcal{C}$ denote a cyclic code and let I be the Stanley-Reisner ideal of $\mathcal{M}(\mathcal{C})$, the vector matroid of a parity check matrix for $\mathcal{C}$. Let $\mathfrak{F}$ be a free resolution of I, with $\mathrm{Syz}_m(I)$ the m-th syzygy module. Then σ_m induces a group action on $\mathrm{Syz}_m(I)$.*

4.2 BCH and Reed-Solomon Codes

We begin by expounding further on some of the basic properties of cyclic codes. In the following discussion, we largely follow [11] and [7].

4.2.1 Definition. Choose a positive integer n and let q be a prime power. The *q-cyclotomic coset* of i modulo n is the set $C_i := \{iq^k \mod n \mid k \in \mathbb{Z}\}$

A standard result in the theory of cyclic codes states that given a cyclic code over $\mathbb{F}_q$ with block length n and generator polynomial $g(x)$, if there exists a primitive n-th root of unity α in some field extension of $\mathbb{F}_q$, then $g(x) = \prod_{i \in C} \mu_{\alpha_i}(x)$, where μ_{α_i} is the minimal polynomial of α^i over $\mathbb{F}_q$ and C is a set of representatives drawn from each member of a subcollection $\{C_{i_1}, \ldots, C_{i_r}\}$ of the q-cyclotomic cosets modulo n. Furthermore, μ_{α_i} may be factored into the product $\prod_{s \in C_i}(x - \alpha^s)$; thus, the roots of g are precisely the powers α^s for which $s \in \bigcup_{j=1}^{r} C_{i_j}$ [7]. This motivates the following:

4.2.2 Definition. Let $\mathcal{C}$ be a cyclic code with block length n over $\mathbb{F}_q$ with generator polynomial g. Assume that α is a primitive n-th root of unity in a field extension of $\mathbb{F}_q$ and that the roots of g are the powers α^s whose exponents s lie in a collection $\{C_{i_1}, \ldots, C_{i_r}\}$ of q-cyclotomic cosets modulo n. Then $\bigcup_{j=1}^{r} C_{i_j}$ is said to be the *defining set* of $\mathcal{C}$.

4.2.3 Definition. Fix a block length n and let δ be an integer such that $2 \leq \delta \leq n$. Let b denote an integer and choose a field $\mathbb{F}$. Let C_i denote the q-cyclotomic coset of i modulo n. The cyclic code with defining set $\bigcup_{i=0}^{\delta-2} C_{b+i}$ and block length n is called a *BCH code* and is said to have *designed distance* δ.

As the name suggests, a BCH code with designed distance δ has Hamming distance at least δ [7]. Unfortunately, there is no guarantee that the actual distance of a BCH

code is equal to its designed distance; indeed, finding bounds on the actual distance is a current topic of interest. Consequently, we focus on BCH codes for which the actual distance can be readily derived. First, however, we will derive a parity check matrix for BCH codes.

Assume $\mathcal{C}$ is a BCH code and let α be an n-th root of unity in an extension field of $\mathbb{F}_q$. Let $g(x)$ denote the generator polynomial for $\mathcal{C}$. Identifying $\mathcal{C}$ with its ideal in $\frac{\mathbb{F}_q[x]}{(x^n-1)}$, and consequently codewords in $\mathcal{C}$ with their polynomial representations in $\frac{\mathbb{F}_q[x]}{(x^n-1)}$, if $c(x)$ is a codeword in $\mathcal{C}$, then $g(x)$ divides $c(x)$. By the choice of the defining set, each of $\alpha^b, \alpha^{b+1}, \ldots, \alpha^{b+\delta-2}$ are roots of g, and consequently of c. Thus, one has the equations

$$0 = c(\alpha^{b+r}) = c_0 + c_1\alpha^{b+r} + c_2\alpha^{2(b+r)} + \cdots + c_{n-1}\alpha^{(n-1)(b+r)},$$

where $c_0, \ldots, c_{n-1}$ are the coefficients of c. Reinterpreting c as a column vector, this implies that $H'c = 0$, where

$$H' := \begin{bmatrix} 1 & \alpha^b & \alpha^{2b} & \cdots & \alpha^{(n-1)b} \\ 1 & \alpha^{b+1} & \alpha^{2(b+1)} & \cdots & \alpha^{(n-1)(b+1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{b+\delta-2} & \alpha^{2(b+\delta-2)} & \cdots & \alpha^{(n-1)(b+\delta-2)} \end{bmatrix}$$

has entries in the chosen extension field $\mathbb{F}$ of $\mathbb{F}_q$. The associated BCH code is thus the collection of codewords in the kernel of H' whose entries all lie in $\mathbb{F}_q$. To find a parity check matrix, one may use the procedure in Ch. 7, §7 of [11], which is as follows. Let $\beta := \{\beta_1, \ldots, \beta_k\}$ be a basis for $\mathbb{F}$ as an $\mathbb{F}_q$-vector space, and let H be the matrix obtained from H' by replacing each entry α^r of H' with its coordinate (column) vector relative to β; thus

$$H'_{ij} = H_{ij1}\beta_1 + \cdots + H_{ijk}\beta_k.$$

For any row vector c whose entries all lie in $\mathbb{F}_q$,

$$0 = H'_i c^T \text{ for each row } H'_i \text{ of } H'$$

$$
\begin{aligned}
&\iff 0 = H'_{i1}c_1 + \cdots + H'_{in}c_n \text{ for each } i \\
&\iff 0 = (H_{i11}\beta_1 + \cdots + H_{i1k}\beta_k)\, c_1 + \cdots \\
&\qquad\qquad + (H_{in1}\beta_1 + \cdots + H_{ink}\beta_k)\, c_n \text{ for each } i \\
&\iff 0 = (H_{i11}c_1 + \cdots + H_{in1}c_n)\, \beta_1 + \cdots \\
&\qquad\qquad + (H_{i1k}c_1 + \cdots + H_{ink}c_n)\, \beta_k \text{ for each } i \\
&\iff 0 = H_{ij}c^T \text{ for each row } H_{ij} \text{ of } H,
\end{aligned}
$$

hence H is a parity check matrix for the chosen BCH code.

4.2.4 Example. Let $b = 1$ and α be a 7-th primitive root of unity in $\mathbb{F}_8$. Let $\mathcal{B} := \{1, \alpha, \alpha^2\}$; $\mathcal{B}$ is thus an ordered basis for $\mathbb{F}_8$ as an $\mathbb{F}_2$-vector space. Replacing the entries of

$$
H' = \begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha^8 & \alpha^{10} & \alpha^{12} \end{bmatrix}
$$

with their coordinate vectors relative to $\mathcal{B}$ and then performing row operations, one obtains

$$
H = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}
$$

as a parity check matrix for a code $\mathcal{C}$. Since H is a permutation of the parity check matrix computed in 2.1.2, $\mathcal{C}$ is the 4-dimensional binary Hamming code.

Note that one may choose a field $\mathbb{F}_q$ which itself contains an n-th root of unity, for example, by choosing $n := q - 1$. Thus,

4.2.5 Definition. If $\mathcal{C}$ is a BCH code over $\mathbb{F}_q$ with block length equal to $q - 1$, then $\mathcal{C}$ is said to be a *Reed-Solomon* code.

In such a case, one may take H' as a parity check matrix for the chosen Reed-Solomon code. However, H' is a Vandermonde matrix, and thus, since H' contains $\delta - 1$ rows, every collection of $\delta - 1$ columns of H' is linearly independent [11]. Thus,

every collection of δ columns is linearly dependent – as a codeword corresponds to a linear dependence among a set of columns, every codeword of the corresponding code has Hamming weight at least δ. However, taking d to be the actual Hamming distance, one obtains

$$\delta \leq d \leq n - k + 1 = n - (n - (\delta - 1)) + 1 = \delta,$$

thus Reed-Solomon codes are maximum distance separable.

4.3 Observations on Resolutions of Reed-Solomon Codes

Assume $\mathcal{C}$ is a Reed-Solomon code with parity check matrix H. By the discussion in 4.2, H is a Vandermonde matrix; thus, if H contains m columns, then any collection of m columns of H is linearly independent [11]. As the designed distance of $\mathcal{C}$ is equal to m,

4.3.1 Proposition. *Assume $\mathcal{C}$ is a Reed-Solomon code with block length n and designed distance m. Then $\mathcal{M}(\mathcal{C})$, the vector matroid of a parity check matrix of $\mathcal{C}$, is the uniform matroid $U_{n,m-1}$, the matroid whose bases are the $(m-1)$-subsets of $[n]$.*

The circuits of the uniform matroid $U_{n,m}$ are the m-subsets of $[n]$, thus

4.3.2 Proposition. *Assume $\mathcal{C}$ is a Reed-Solomon code with block length n and designed distance m. Then the Stanley-Reisner ideal of $\mathcal{M}(\mathcal{C})$ is generated by the square-free monomials $x_\sigma \in \mathbb{F}[x_1, \ldots, x_n]$ for which $|\sigma| = m$.*

Let I denote such an ideal; then I is a specialized Ferrers ideal in m variables and with partition $\lambda = (m-1, m-2, \ldots, 0)$. Thus, I is minimally resolved via the complex of boxes cellular resolution of [14]; by counting i-faces in the complex of boxes, one arrives at the $\mathbb{Z}$-graded Betti numbers

$$\beta_{i,d_i} = \binom{r+c}{r+i}\binom{r+i-1}{r}$$

for $i > 0$, where r denotes the regularity and c the codimension of I. Consequently,

4.3.3 Proposition. *Assume $\mathcal{C}$ is a Reed-Solomon code with block length n and designed distance m. Then the Stanley-Reisner ideal of $\mathcal{M}(\mathcal{C})$ has a linear minimal cellular free resolution with $\beta_{i,d_i} = \binom{n}{m+i}\binom{m+i-1}{m}$.*

4.4 Cyclic Codes Corresponding to Complete Intersections

Let $\mathcal{C}$ be a cyclic code with block length p^k, p a prime, and generator polynomial $g(x) := \frac{x^{p^k}-1}{x^{p^a}-1}$, where $0 \leq a \leq k$. Thus,

$$g(x) = 1 + x^{p^a} + x^{2p^a} + \cdots + x^{(p^{k-a}-1)p^a}.$$

Therefore, $\mathcal{C}$ has as a generator matrix

$$G := \begin{bmatrix} I_{p^a} & I_{p^a} & \cdots & I_{p^a} \end{bmatrix}$$

where the $p^a \times p^a$ identity I_{p^a} occurs p^{k-a} times. By permuting the columns of G, one may produce

$$G' := \begin{bmatrix} U_{p^{k-a}} & 0 & \cdots & 0 \\ 0 & U_{p^{k-a}} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & U_{p^{k-a}} \end{bmatrix},$$

where each of the p^a occurrences of $U_{p^{k-a}}$ denotes a row consisting of p^{k-a} ones. Thus, $\mathcal{C}$ permutation equivalent to a direct sum of codes with generator matrix $U_{p^{k-a}}$. Then, trivially, the rows of G' are the minimal support codewords of $\mathcal{C}$, and consequently the circuits of $\mathcal{M}(\mathcal{C})$ are the subsets of $[p^k] := \{0, 1, \ldots, p^k - 1\}$ of form

$$ip^{k-a} + [p^{k-a}] := \{ip^{k-a}, ip^{k-a} + 1, \ldots, ip^{k-a} + p^{k-a} - 1\}.$$

This proves:

4.4.1 Proposition. *Let $\mathcal{C}$ be a cyclic code with generator polynomial $g(x) = \frac{x^{p^k}-1}{x^{p^a}-1}$. Then the Stanley-Reisner ideal of $\mathcal{M}(\mathcal{C})$ is minimally generated by the squarefree*

monomials $x_{ip^{k-a}+[p^{k-a}]}$ *for* $i = 0, \ldots, p^{a-1}$.

Denote by I the Stanley-Reisner ideal of $\mathcal{M}(\mathcal{C})$. Since each of the supports $ip^{k-a} + [p^{k-a}]$ of the minimal generators of I are pairwise disjoint, each generator x_{σ_i} of I is trivially a nonzero divisor on $\frac{\mathbb{F}[x_0,\ldots,x_{p^k-1}]}{(x_{\sigma_0},\ldots,x_{\sigma_{i-1}})}$ – and thus, the variety of I is a complete intersection. As such, I is minimally resolved by the Taylor complex.

On the other hand, one may consider G' as a parity check matrix for $\mathcal{C}^{\perp}$. As such, each $U_{p^{k-a}}$ contains as its minimal dependent subsets the 2-subsets of $[p^{k-a}]$ – thus, the Stanley-Reisner ideal of $\mathcal{M}(U_{p^{k-a}})$ is minimally generated by the monomials x_σ with σ a 2-subset of $[p^{k-a}]$. As this is a Ferrers ideal, it supports a linear minimal free cellular resolution [2], with Betti numbers

$$\begin{aligned}\beta_j &= -\binom{m}{j+2} + \sum_{k=1}^{m} \binom{\lambda_k + k - 1}{j+1} \\ &= -\binom{m}{j+2} + m\binom{m-1}{j+1} \\ &= (j+1)\binom{m}{j+2}.\end{aligned}$$

With no nontrivial linear dependencies between copies of $U_{p^{k-a}}$ in G', one therefore obtains that the Stanley-Reisner ideal of $\mathcal{M}(\mathcal{C})$ is equal to $I_0 + I_1 + \cdots + I_{p^a-1}$, where

$$I_i = (x_{i+\sigma} \,|\, \sigma \subseteq [p^{k-a}] \text{ and } |\sigma| = 2).$$

In fact, as each 1-subset is independent, the corresponding matroid is the uniform matroid $U_{1,p^{k-a}}$. Moreover, the matroid $\mathcal{M}(\mathcal{C})$ is the direct sum of p^a copies of $U_{1,p^{k-a}}$, a partition matroid. Each I_i is in distinct variables, so $I_0 + I_1 + \cdots + I_{p^a-1}$ is minimally resolved by the tensor product of minimal free resolutions $\mathfrak{F}_i$ of I_i. Thus, one obtains the resolution

$$\mathfrak{F}\colon 0 \to \cdots \to \bigoplus_{d=i_1+\cdots+i_j} \left(F_{i_1} \otimes \cdots \otimes F_{i_j}\right) \to \cdots \to I_0 + \cdots + I_{p^a-1} \to 0$$

of $I_0 + I_1 + \cdots + I_{p^a-1}$, and therefore Betti numbers

$$\beta_d = \sum_{d=i_1+\cdots+i_j} \beta_{i_1} \cdots \beta_{i_j}.$$

Finally, note that each of the above codes may be realized as a narrow-sense BCH code. The zeros of $g(x) = \frac{x^{p^k}-1}{x^{p^a}-1}$ are the p^k-th roots of unity which are not also p^a-th roots of unity. Thus there are (at least) $p^a - 1$ consecutive zeros of g: $\alpha, \alpha^2, \ldots, \alpha^{p^a-1}$. Taking the defining set to be $C_1 \cup C_2 \cup \cdots \cup C_{p^a-1}$ defines the cyclic code with generator polynomial g as a BCH code with block length p^k and designed distance p^a.

Chapter 5: Resolutions of Duals to Finite Projective and Affine Geometries

5.1 Resolutions of Duals to Finite Projective Geometries

In general, given a vector space V, one may define its projectivization as follows:

5.1.1 Definition. Let V be a k-dimensional vector space. The *projectivization* of V, denoted $\mathbb{P}(V)$, is defined to be the set of one-dimensional subspaces of V. The *dimension* of $\mathbb{P}(V)$, denoted $\dim \mathbb{P}(V)$, is defined to be $k-1$.

5.1.2 Notation. We will denote by $PG(k, \mathbb{F}_q)$ the projectivization of $\mathbb{F}_q^k$; this is called the $(k-1)$-*dimensional finite projective geometry over* $\mathbb{F}_q$.

Note that in the literature, the notation $PG(k, \mathbb{F}_q)$ generally denotes the k-dimensional projective geometry over $\mathbb{F}_q$; here, however, $PG(k, \mathbb{F}_q)$ has dimension $k-1$. Recall that in 2.1.1, we defined the k-dimensional simplex code over $\mathbb{F}_q$ by taking its generator matrix to be any matrix whose columns are the pairwise linearly independent vectors in $\mathbb{F}_q^k$. As linearly independent pairs of vectors in $\mathbb{F}_q^k$ reside in distinct one-dimensional subspaces of $\mathbb{F}_q^k$, and thus correspond to distinct points of $PG(k, \mathbb{F}_q)$, we obtain an (equivalent) definition for the simplex codes.

5.1.3 Definition. The k-dimensional simplex code over $\mathbb{F}_q$, denoted $S(k, \mathbb{F}_q)$, is defined (up to permutation equivalence) to be the code whose generator matrix columns are the points in $PG(k, \mathbb{F}_q)$.

Consequently, we may (and will) consider $PG(k, \mathbb{F}_q)$ as the vector matroid of any generator matrix for $S(k, \mathbb{F}_q)$. In addition, $PG(k, \mathbb{F}_q)$ has rank k, and the r-flats of $PG(k, \mathbb{F}_q)$ correspond to the r-dimensional linear subspaces of $\mathbb{F}_q^k$. Thus, its hyperplanes are the $(k-1)$-dimensional subspaces of $\mathbb{F}_q^k$. Each such subspace is orthogonal to a one-dimensional subspace of $\mathbb{F}_q^k$, thus, the points on every $PG(k, \mathbb{F}_q)$-hyperplane H satisfy a homogeneous linear form $l_H(x_1, \ldots, x_k) = 0$. Furthermore, this relation also implies that the relation between the dimensions of subspaces U

and V of $\mathbb{F}_q^k$,

$$\dim(U+V)+\dim(U\cap V)=\dim(U)+\dim(V),$$

carries over into $PG(k,\mathbb{F}_q)$ in essentially identical form: given flats U and V of $PG(k,\mathbb{F}_q)$ with ranks $r(U)$ and $r(V)$,

$$r(U\cup V)+r(U\cap V)=r(U)+r(V).$$

As we identify the one-dimensional subspaces of $\mathbb{F}_q^k$ with the points in $PG(k,\mathbb{F}_q)$, we may label (and identify) each point with the vector in its corresponding subspace whose leading nonzero entry is $1_{\mathbb{F}_q}$. Taking α to be a $(q-1)st$ root of unity in $\mathbb{F}_q$, and assuming a generator matrix S_q^{k-1} for $S(k-1,\mathbb{F}_q)$ has been computed, one may take all multiples of S_q^{k-1} of the form $\alpha^i S_q^{k-1}$, for $i=0,\ldots,q-2$; this produces all vectors in $\mathbb{F}_q^{k-1}$. Prepending each of these points with $1_{\mathbb{F}_q}$ and including the point at infinity, represented as $(1\colon 0\colon \cdots\colon 0)$, one obtains all points of form $(1\colon a_1\colon \cdots\colon a_{k-1})$. Assuming via induction that all points of form $(0\colon \cdots\colon 0\colon 1\colon a_p\colon \cdots\colon a_{k-1})$ are contained as columns of S_q^{k-1}, one arrives at the following recursive description of a generator matrix for $S(k,\mathbb{F}_q)$.

5.1.4 Proposition. *Let α be a $(q-1)st$ root of unity in $\mathbb{F}_q$ and define $S_q^1:=[1]$. For $k\geq 2$, define the $k\times\frac{q^k-1}{q-1}$ matrix S_q^k recursively by setting*

$$S_q^k=\begin{bmatrix} \overline{0} & 1 & \overline{1} & \overline{1} & \cdots & \overline{1} \\ S_q^{k-1} & \overline{0} & S_q^{k-1} & \alpha S_q^{k-1} & \cdots & \alpha^{q-2}S_q^{k-1}\end{bmatrix}\in\mathbb{F}_q^{k\times\frac{q^k-1}{q-1}},$$

where $\overline{0}$ and $\overline{1}$ denote rows or columns of 0s and 1s in $\mathbb{F}_q$. Then S_q^k is a generator matrix for the k-dimensional simplex code over $\mathbb{F}_q$.

Let $\mathcal{M}(S_q^k)$ denote the vector matroid of S_q^k and denote by $\mathcal{M}(S_q^k)^\perp$ the matroid dual to $\mathcal{M}(S_q^k)$. The block length of $S(k,\mathbb{F}_q)$ is $n:=\frac{q^k-1}{q-1}$, and there exists an $(n-k)\times n$ parity check matrix over $\mathbb{F}_q$ to S_q^k – call it H_q^k. For the sake of simplifying notation, we will let I_k denote the Stanley-Reisner ideal of $\mathcal{M}(S(k,\mathbb{F}_q))=\mathcal{M}(H_q^k)=\mathcal{M}(S_q^k)^\perp=PG(k,\mathbb{F}_q)^\perp$. By [10], there are $\begin{bmatrix}k\\1\end{bmatrix}_q=\frac{q^k-1}{q-1}$ monomial generators of

I_k, each with degree equal to the Hamming weight of $S(k, \mathbb{F}_q)$. Since there are $\begin{bmatrix} k \\ 1 \end{bmatrix}_q$ codewords in $S(k, \mathbb{F}_q)$, each corresponding to a minimal 1-support due to the constant-weight property of $S(k, \mathbb{F}_q)$, each generator of I_k corresponds to exactly one codeword in $S(k, \mathbb{F}_q)$. Since $[\overline{0}\,1\,\overline{1}\,\cdots\,\overline{1}]$ is a codeword in $S(k, \mathbb{F}_q)$ and all other codewords in $S(k, \mathbb{F}_q)$ have equicardinal support, the supports of all other codewords in $S(k, \mathbb{F}_q)$ are permutations of the support of $[\overline{0}\,1\,\overline{1}\,\cdots\,\overline{1}]$. Fix a generator r of I_k; then the support of r, $\operatorname{supp}(r)$, is a circuit in $\mathcal{M}(S_q^k)^\perp$, and hence corresponds to a choice of columns in S_q^k. Thus, $[n] - \operatorname{supp}(r)$ is a hyperplane in $\mathcal{M}(S_q^k)$, so the corresponding (possibly permuted) columns of the generator matrix S_q^k are the points of a $PG(k, \mathbb{F}_q)$-hyperplane. Since this logic is reversible,

5.1.5 Proposition. *Assume I_k is the Stanley-Reisner ideal of the matroid*

$$\mathcal{M}(S(k, \mathbb{F}_q)) = \mathcal{M}(S_q^k)^\perp = PG(k, \mathbb{F}_q)^\perp.$$

Then r is a minimal monomial generator of I_k if and only if $\operatorname{supp}(r)$ *is the complement of a $PG(k, \mathbb{F}_q)$-hyperplane.*

Suppose s is a monomial generator of I_k distinct from r and set $U := [n] - \operatorname{supp}(r)$ and $V := [n] - \operatorname{supp}(s)$. Identifying U and V with their corresponding $PG(k, \mathbb{F}_q)$-hyperplanes, one obtains $\dim(U) = \dim(V) = k - 1$ and $\dim(U + V) = k$. Thus, $\dim(U \cap V) = k - 2$, and it follows that

$$\begin{aligned} \operatorname{supp}(r : s) &= U - V \\ &= V - (U \cap V) \end{aligned}$$

is a $PG(k-1, \mathbb{F}_q)$-hyperplane. Additionally, assume r is a monomial generator of I_{k-1} and let $m := \frac{q^{k-1}-1}{q-1}$. Since the complement of $\operatorname{supp}(r)$ is a $PG(k-1, \mathbb{F}_q)$-hyperplane, there exists a linear form l_r such that

$$\operatorname{supp}(r) = [m] - \{P \in PG(k-1, \mathbb{F}_q) \mid l_r(P) = 0\}.$$

Moreover, since l_r uniquely defines a hyperplane in any projective space, there exists

a unique monomial $r' \in I_k$ such that

$$\operatorname{supp}(r') = [n] - \{P \in PG(k, \mathbb{F}_q) \,|\, l_r(P) = 0\}.$$

Consequently, for each monomial generator of I_{k-1}, there exists a unique corresponding monomial generator of I_k. This motivates the following:

5.1.6 Definition. Assume r is a monomial generator of I_{k-1} corresponding to a hyperplane in $PG(k-1, \mathbb{F}_q)$ whose points satisfy the hyperplane's corresponding linear form l_r. Let r' denote the monomial generator of I_k corresponding to the hyperplane of $PG(k, \mathbb{F}_q)$ whose points satisfy l_r, and define I'_{k-1} to be the ideal generated by the monomials r', where r is a minimal generator of I_{k-1}.

5.1.7 Example. We will use

$$S_2^2 = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix} \in \mathbb{F}_2^{2\times 3}$$

and

$$S_2^3 = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix} \in \mathbb{F}_2^{3\times 7},$$

as defined via 5.1.4. The Stanley-Reisner ideal of $\mathcal{M}(S_2^2)^\perp$ is

$$I_2 = (x_0x_1, x_0x_2, x_1x_2)\,.$$

The generators are complements of $PG(2, \mathbb{F}_2)$-hyperplanes, which we compute as the varieties of $l_1 = y_0 + y_1$, $l_2 = y_1$, and $l_3 = y_0$, for x_0x_1, x_0x_2, and x_1x_2, respectively. To compute I'_2, we introduce an additional variable, y_{-1}, associated to the top row of S_2^3. Regarding l_1, l_2, and l_3 as linear forms in y_0, y_1, and the additional variable, y_{-1}, one obtains the $PG(3, \mathbb{F}_2)$-hyperplanes $\{2, 3, 6\}$, $\{1, 3, 5\}$, and $\{0, 3, 4\}$. This implies

$$I'_2 = (x_0x_1x_4x_5, x_0x_2x_4x_6, x_1x_2x_5x_6)\,.$$

There are four minimal generators of I_3 which are not minimal generators of I_2', namely, $x_0x_1x_3x_6$, $x_0x_2x_3x_5$, $x_1x_2x_3x_4$, and $x_3x_4x_5x_6$. Adding these to I_2', one obtains

$$I_3 = (x_0x_1x_4x_5, x_0x_2x_4x_6, x_1x_2x_5x_6, x_0x_1x_3x_6, x_0x_2x_3x_5, x_1x_2x_3x_4, x_3x_4x_5x_6)\,.$$

Note that I_{k-1}' can also be characterized as the ideal generated by the monomials in I_k corresponding to the natural inclusion of $PG(k-1,\mathbb{F}_q)$ into $PG(k,\mathbb{F}_q)$. Employing this construction, one obtains:

5.1.8 Lemma. *Assume I_{k-1} and $I_k \subseteq R$ are the Stanley-Reisner ideals of the matroids $\mathcal{M}(S(k-1,\mathbb{F}_q)) = PG(k-1,\mathbb{F}_q)^\perp$ and $\mathcal{M}(S(k,\mathbb{F}_q)) = PG(k,\mathbb{F}_q)^\perp$, respectively. Let x_{V^C} be a monomial generator of I_k corresponding to a $PG(k,\mathbb{F}_q)$-hyperplane V. Assume x_{V^C} is not a generator of I_{k-1}' and denote by $I_k - x_{V^C}$ the ideal generated by the minimal generators of I_k, except for x_{V^C}. Then*

$$(I_k - x_{V^C})\colon x_{V^C} \cong I_{k-1}.$$

Proof. Denote by N the $PG(k,\mathbb{F}_q)$-hyperplane corresponding to the natural inclusion of $PG(k-1,\mathbb{F}_q)$ into $PG(k,\mathbb{F}_q)$. Let U be any $PG(k,\mathbb{F}_q)$-hyperplane, with x_{U^C} the corresponding generator of I_k. Then

$$\begin{aligned} supp(x_{U^C}\colon x_{V^C}) &= U^C - V^C \\ &= V - U \cap V. \end{aligned}$$

Since $\dim(U \cap V) = k-2$, $U \cap V \cong PG(k-2,\mathbb{F}_q)$. Thus,

$$\begin{aligned} I_k\colon x_{V^C} &= (x_{V-U\cap V} \,|\, U \cong PG(k-1,\mathbb{F}_q)) \\ &= (x_{V-L} \,|\, L \cong PG(k-2,\mathbb{F}_q))\,. \end{aligned}$$

Let φ be any permutation on $[n]$ such that $\varphi(N) = V$ and $\varphi(U \cap N) = U \cap V$. Then φ induces an automorphism on R under which

$$(x_{V-L} \mid L \cong PG(k-2,\mathbb{F}_q)) \cong (x_{N-L} \mid L \cong PG(k-2,\mathbb{F}_q))$$
$$= I_{k-1}.$$

□

As an immediate consequence, we obtain the following:

5.1.9 Corollary. *Assume I_{k-1} and $I_k \subseteq R$ are the Stanley-Reisner ideals of the matroids $\mathcal{M}(S(k-1,\mathbb{F}_q))$ and $\mathcal{M}(S(k,\mathbb{F}_q))$ of the simplex codes $S(k-1,\mathbb{F}_q)$ and $S(k,\mathbb{F}_q)$, respectively. Let I'_{k-1} be as defined above, and assume $x_{V_1^C},\ldots,x_{V_{p+1}^C}$ are distinct monomial generators of I_k which are not also generators of I'_{k-1}. Then*

$$(I'_{k-1}, x_{V_1^C},\ldots,x_{V_p^C})\colon x_{V_{p+1}^C} \cong I_{k-1}.$$

Proof. Let $I_k = (I'_{k-1}, x_{V_1^C},\ldots x_{V_n^C})$, where $x_{V_1^C},\ldots,x_{V_n^C}$ are the distinct minimal generators of I_k which are not generators of I'_{k-1}, and note that the proof of 5.1.8 also implies $I'_{k-1}\colon x_{V_{p+1}^C} \cong I_{k-1}$ for any $p < n$. Let N be the natural inclusion of $PG(k-1,\mathbb{F}_q)$ into $PG(k,\mathbb{F}_q)$. Denote by $I_k - x_{V_{p+1}^C}$ the ideal generated by the minimal generators of I_k except for $x_{V_{p+1}^C}$. Then

$$\begin{aligned} I_{k-1} &\cong I'_{k-1}\colon x_{V_{p+1}^C} \\ &\subseteq (I'_{k-1}, x_{V_1^C},\ldots,x_{V_p^C})\colon x_{V_{p+1}^C} \\ &\subseteq (I_k - x_{V_{p+1}^C})\colon x_{V_{p+1}^C} \\ &\cong I_{k-1}, \end{aligned}$$

where the two isomorphisms are given by the same automorphism φ on R for which $\varphi(N) = V$ and $\varphi(U \cap N) = U \cap V$. □

We will compute a cellular resolution for I_k by first recursively describing the (unlabeled) cell complex C_k on which our resolution of I_k is supported, defined as follows.

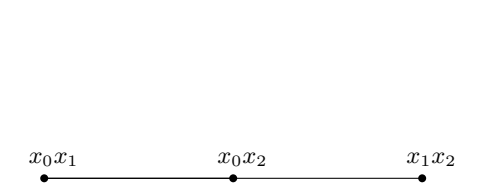
5.1.10 Definition. Let I_k be the Stanley-Reisner ideal of $\mathcal{M}(S_q^k)^\perp$. If $k = 1$, define the cell complex C_1 to be a point. Otherwise, assume C_{k-1} is the cell complex associated to I_{k-1} and form q^{k-1} new vertices. For each new vertex v, form the cone of v over C_{k-1}; call the resulting cell complex C_k.

Thus, C_{k-1} is a subcomplex of C_k. We will also define the labeled cell complex recursively.

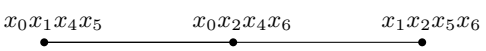
5.1.11 Definition. Let I_{k-1} and I_k be the Stanley-Reisner ideals of $\mathcal{M}(S(k-1, \mathbb{F}_q))$ and $\mathcal{M}(S(k, \mathbb{F}_q))$, respectively. If $k = 1$, define the labeled cell complex $L(C_1)$ to be C_1 with its sole vertex labeled by the generator of I_1, x_1. Otherwise, assume $x_{V_1^C}, \ldots, x_{V_n^C}$ are the distinct monomial generators of I_k which are not also generators of I'_{k-1}. Let C_k be the associated unlabeled complex and assume that $L(C_{k-1})$ is the labeled version of the unlabeled complex C_{k-1} contained as a subcomplex within C_k. Replace each label r of $L(C_{k-1})$ with r' to obtain $L(C_{k-1})'$ and label each vertex of C_k not in C_{k-1} with a generator of I_k which is not also a generator of I'_{k-1}. Call the resulting labeled cell complex $L(C_k)$.

5.1.12 Example. Notice that the ideal $I_2 = I(\mathcal{M}(S_2^2)^\perp)$, computed in 5.1.7, is the same as the ideal considered in 2.3.9; indeed, one may show that the labeled cell complex of 2.3.9 is precisely $L(C_2)$ for $I(\mathcal{M}(S_2^2)^\perp)$ and is replicated in 5.1a, sans the labels of the faces with dimension greater than one. Apply the map $r \longmapsto r'$ to the vertex labels of $L(C_2)$ to obtain $L(C_2)'$, shown in 5.1b. This also alters the labels of the 1-faces; rather than display these (and higher dimensional) labels, we take them to be understood. One may then form C_3 from C_2 by coning 4 points over C_2. To form $L(C_3)$, we label the vertices of the copy of C_2 one coned over with the corresponding vertex labels of $L(C_2)'$. There are 4 minimal generators of $I_3 = I(\mathcal{M}(S_2^3)^\perp)$ which are not also minimal generators of I'_2 which become the labels of the 4 new points added to C_2 to form C_3 – one thus obtains $L(C_3)$, shown in 5.1c.

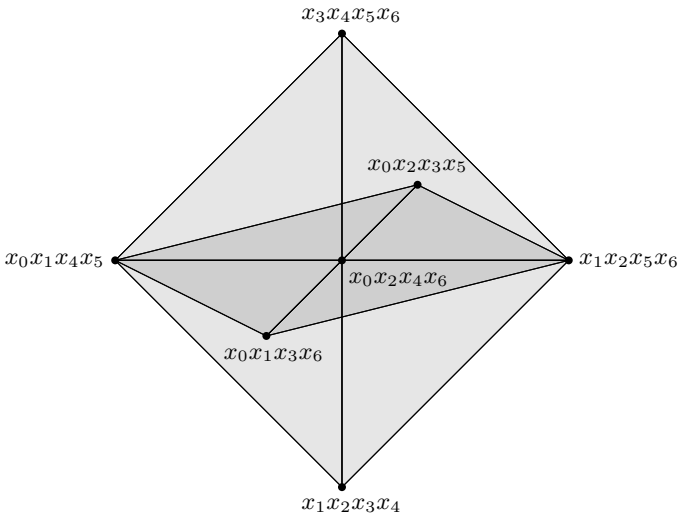
For the sake of brevity, we will denote by $x_1, \ldots, \widehat{x_i}, \ldots, x_p$ the set $\{x_1, \ldots, x_p\} - \{x_i\}$; when the context is clear, we will denote $\{x_1, \ldots, x_p\}$ by F and $\{x_1, \ldots, x_p\} - \{x_i\}$ by $F - \{x_i\}$. Assume I_{k-1} has a minimal cellular resolution supported on C_{k-1}, with the vertices on C_{k-1} labeled $x_{r_1}, \ldots, x_{r_m}$. As C_{k-1} is simplicial, we may identify



(a) $L(C_2)$



(b) $L(C_2)'$



(c) $L(C_3)$

Figure 5.1: The labeled cell complexes $L(C_2)$, $L(C_2)'$, and $L(C_3)$ associated to the ideals $I(\mathcal{M}(S_2^2)^\perp)$, $I(\mathcal{M}(S_2^2)^\perp)'$, and $I(\mathcal{M}(S_2^3)^\perp)$, respectively.

a face in C_{k-1} with its vertex set, and hence with the set consisting of its vertex labels. Furthermore, given faces $F := \{x_{r_{a_1}}, \ldots, x_{r_{a_i}}\}$, the i-th differential map $d_i^{I_{k-1}}$ is defined by extending

$$e_F \longmapsto \sum_{1\leq j\leq i} \varepsilon(F - \{x_{r_{a_j}}\}, F)\frac{\operatorname{lcm}(F)}{\operatorname{lcm}(F - \{x_{r_{a_j}}\})}e_{F-\{x_{r_{a_j}}\}}$$

linearly, where e_F is a free generator associated to the face with vertices labeled $x_{r_{a_1}}, \ldots, x_{r_{a_i}}$ and each $e_{F-\{x_{r_{a_j}}\}}$ is a free generator associated to the face with vertices labeled $x_{r_{a_1}}, \ldots, \widehat{x_{r_{a_j}}}, \ldots, x_{r_{a_i}}$. For each vertex v in C_{k-1}, replace the generator r of I_{k-1} assigned as the label for v with the corresponding generator r' of I'_{k-1} to obtain labels $x'_{r_{a_1}}, \ldots, x'_{r_{a_i}}$; we will denote such a face by F'. One can obtain a resolution for I'_{k-1} from the preceding resolution for I_{k-1} by adjusting the label of each vertex from x_v to x'_v. Thus, the i-th differential map $d_i^{I'_{k-1}}$ is

$$e_{F'} \longmapsto \sum_{1\leq j\leq i} \varepsilon(F' - \{x'_{r_{a_j}}\}, F')\frac{\operatorname{lcm}(F')}{\operatorname{lcm}(F' - \{x'_{r_{a_j}}\})}e_{F'-\{x'_{r_{a_j}}\}}$$

extended linearly:

5.1.13 Proposition. *Let I_{k-1} be the Stanley-Reisner ideal of $\mathcal{M}(S(k-1,\mathbb{F}_q))$. Assume there exists a minimal cellular resolution $\mathfrak{A}$ of $A := I_{k-1}$,*

$$\mathfrak{A}\colon 0 \to F_n^A \xrightarrow{d_n^A} \cdots \xrightarrow{d_2^A} F_1^A \xrightarrow{d_1^A} I_{k-1} \to 0.$$

Let $B := I'_{k-1}$ be as defined above and define d_i^B to be the map d_i^A with coefficients m replaced by m'. Then

$$\mathfrak{B}\colon 0 \to F_n^B \xrightarrow{d_n^B} \cdots \xrightarrow{d_2^B} F_1^B \xrightarrow{d_1^B} I'_{k-1} \to 0.$$

is a minimal cellular resolution of I'_{k-1}.

Proof. Let $b' \in \mathbb{Z}^{\frac{q^k-1}{q-1}}$ be given and let the vertices of $L(C_{k-1})'_{\leq b'}$ be labeled by a set of monomials $r'_{a_1},\ldots,r'_{a_p}$ in I'_{k-1}. Let $b := \operatorname{lcm}(r_{a_1},\ldots,r_{a_p})$; as b is squarefree, we will identify b with its exponent vector. We will prove that the complex underlying $L(C_{k-1})'_{\leq b'}$ is equal to the complex underlying $L(C_{k-1})_{\leq b}$.

Let F' be a face in $L(C_{k-1})'_{\leq b'}$ labeled by

$$\{r'_{a_{i_1}},\ldots,r'_{a_{i_k}}\} \subseteq \{r'_{a_1},\ldots,r'_{a_p}\},$$

and thus

$$\{r_{a_{i_1}},\ldots,r_{a_{i_k}}\} \subseteq \{r_{a_1},\ldots,r_{a_p}\}. \qquad (*)$$

Since the labellings of $L(C_{k-1})$ and $L(C_{k-1})'$ are by construction consistent with each other, $\{r_{a_{i_1}},\ldots,r_{a_{i_k}}\}$ may be identified with a face in $L(C_{k-1})$ - in particular, with the face defined by the vertex labels $r'_{a_{i_1}},\ldots,r'_{a_{i_k}}$. By *, one has $r_{a_{i_j}}|b$ for any j, so $\{r_{a_{i_1}},\ldots,r_{a_{i_k}}\}$ defines a face in $L(C_{k-1})_{\leq b}$.

On the other hand, if F is a face of $L(C_{k-1})_{\leq b}$ which is defined by vertices labeled $r_{a_{i_1}},\ldots,r_{a_{i_k}}$, where $r_{a_{i_j}}|b$ for each $j=1,\ldots,q$. Then as

$$F' = \{r'_{a_{i_1}},\ldots,r'_{a_{i_k}}\} \subseteq \{r'_{a_1},\ldots,r'_{a_p}\},$$

one has that $r'_{a_{i_j}} | b'$ for each j; therefore, F' is a face of $L(C_{k-1})'_{\leq b'}$.

However, the complex underlying $L(C_{k-1})_{\leq b}$ is acyclic for every b, and, therefore, $L(C_{k-1})'_{\leq b'}$ is also acyclic. Minimality of $\mathfrak{B}$ follows by noting that the map $m \longmapsto m'$ has positive degree. $\square$

Let v be the vertex of the cone over C_{k-1} and label v with a monomial generator x_v of I_k which is not also a generator of I'_{k-1}. Notice that there is a bijective correspondence $F \leftrightarrow F' \cup \{x_v\}$, where $F := \{x_{r_{a_1}}, \ldots, x_{r_{a_i}}\}$ and $F' := \{x'_{r_{a_1}}, \ldots, x'_{r_{a_i}}\}$. Define $f_i^{x_v}$ by extending

$$e_{F' \cup \{x_v\}} \longmapsto (-1)^i \varepsilon(F', F' \cup \{x_v\}) \frac{\operatorname{lcm}(F' \cup \{x_v\})}{\operatorname{lcm}(F')} e_{F'}$$

linearly.

For convenience, given an R-linear map $d_i \colon F_i \longrightarrow F_{i-1}$ and an R-automorphism φ, we will denote by $\varphi(d_i)$ the map $\varphi(F_i) \longrightarrow \varphi(F_{i-1})$ in which each term m in d_i is replaced by $\varphi(m)$. Furthermore, if $\mathfrak{F}$ is a free resolution, denote by $\varphi(\mathfrak{F})$ the permutation φ applied to each module and differential map in $\mathfrak{F}$. Note that if $\mathfrak{F}$ is a free resolution of an R-ideal I, and φ is any permutation on the variables of R which fixes each element of the field of R, then $\varphi(\mathfrak{F})$ is a free resolution of $\varphi(I)$. Using this notation, one obtains the following:

5.1.14 Proposition. *Assume I_{k-1} and I_k are the Stanley-Reisner ideals of $\mathcal{M}(S(k-1, \mathbb{F}_q))$ and $\mathcal{M}(S(k, \mathbb{F}_q))$, respectively, and let I'_{k-1} be as defined above. Let $x_{V_1^C}, \ldots, x_{V_{p+1}^C}$ be distinct generators of $I_k \subseteq R$ which are not generators of I'_{k-1}. As before, let N denote the hyperplane corresponding to the natural inclusion of $PG(k-1, \mathbb{F}_q)$ into $PG(k, \mathbb{F}_q)$ and take V to be the $PG(k, \mathbb{F}_q)$-hyperplane corresponding to $\operatorname{supp}(x_{V_{p+1}^C})$. Let $\varphi := \varphi_{x_{V_{p+1}^C}}$ be a permutation on the variables of R for which $\varphi(N) = V$ and $\varphi(U \cap N) = U \cap V$ for any hyperplane U of $PG(k, \mathbb{F}_q)$. Assume*

$$\begin{aligned} \mathfrak{A} \colon 0 \to \varphi(F_n^A) &\xrightarrow{\varphi(d_n^A)} \cdots \xrightarrow{\varphi(d_2^A)} \varphi(F_1^A) \\ &\xrightarrow{\varphi(d_1^A)} (I'_{k-1}, x_{V_1^C}, \ldots, x_{V_p^C}) \colon x_{V_{p+1}^C} = \varphi(I_{k-1}) \to 0 \end{aligned}$$

and

$$\mathfrak{B}_p\colon 0 \to F_n^{B_p} \xrightarrow{d_n^{B_p}} \cdots \xrightarrow{d_2^{B_p}} F_1^{B_p} \xrightarrow{d_1^{B_p}} (I'_{k-1}, x_{V_1^C}, \ldots, x_{V_p^C}) \to 0$$

are minimal simplicial cellular resolutions of $(I'_{k-1}, \{x_{V_1^C}, \ldots, x_{V_p^C}\colon x_{V_{p+1}^C}\}$ *and* $B_p := (I'_{k-1}, x_{V_1^C}, \ldots, x_{V_p^C})$ *respectively supported on* $\varphi(L(C_{k-1}))$ *and* $L(C_{k-1})' \cup \{x_{V_1^C}, \ldots, x_{V_p^C}\}$. *Then the squares*

$$\begin{array}{ccc} \varphi(F_{i-1}^A) & \xrightarrow{f_{i-1}^{x_{V_{p+1}^C}}} & F_{i-1}^{B_p} \\ {\scriptstyle \varphi(d_i^A)}\uparrow & & \uparrow{\scriptstyle d_i^{B_p}} \\ \varphi(F_i^A) & \xrightarrow{f_i^{x_{V_{p+1}^C}}} & F_i^{B_p} \end{array}$$

commute.

Proof. Since each codeword in $S(k, \mathbb{F}_q)$ has equal weight, and since $[0 \cdots 01 \cdots 1]$ is a codeword in $S(k, \mathbb{F}_q)$, we may assume that the codeword in $S(k, \mathbb{F}_q)$ whose support is equal to the support of $x_{V_{p+1}^C}$ may be permuted so that its support is equal to the support of $[0 \cdots 01 \cdots 1]$. However, $[0 \cdots 01 \cdots 1]$ is supported on N^C; thus, without loss of generality, we may take $x_{V_{p+1}^C}$ to be x_{N^C}, the monomial whose support is the support of $[0 \cdots 01 \cdots 1]$. Consequently, we may take φ to be the identity automorphism on R, and we define $f_i^{x_{N^C}} := f_i^{x_{V_{p+1}^C}}$.

Let $F := \{x_{r_{a_1}}, \ldots, x_{r_{a_i}}\}$ and assume e_F is a free generator of F_i^A. Again, one has the bijective correspondence $F \leftrightarrow F' := \{x'_{r_{a_1}}, \ldots, x'_{r_{a_i}}\}$ and so one may relabel the free generators of F_i^A with $e_{F'}$ as necessary. Since $\mathfrak{A}$ is cellular, one may write

$$d_i^A\colon e_F \longmapsto \sum_{1 \le j \le i} \varepsilon(F - \{x_{r_{a_j}}\}, F) \frac{\operatorname{lcm}(F)}{\operatorname{lcm}(F - \{x_{r_{a_j}}\})} e_{F - \{x_{r_{a_j}}\}}.$$

For convenience, we will define $G' := F' \cup \{x_{N^C}\}$. For each k, $x'_{r_{a_k}}$ is a generator of I'_{k-1}, $x_{r_{a_k}}$ is a generator of I_{k-1}, and $I'_{k-1}\colon x_{N^C} = I_{k-1}$, thus

$$\frac{\operatorname{lcm}(F)}{\operatorname{lcm}(F - \{x_{r_{a_j}}\})} = \frac{\operatorname{lcm}(G')}{\operatorname{lcm}(G' - \{x'_{r_{a_j}}\})}.$$

As these quotients are equal, we may rewrite the image of e_F under d_i^A as

$$d_i^A \colon e_{G'} \longmapsto \sum_{1\leq j\leq i} \varepsilon(G' - \{x'_{r_{a_j}}\}, G') \frac{\operatorname{lcm}(G')}{\operatorname{lcm}(G' - \{x'_{r_{a_j}}\})} e_{G'-\{x'_{r_{a_j}}\}}$$

after adjusting the labels of the free generators, thus obtaining the same resolution, but supported on the cone.

Consequently, $f_{i-1}^{x_{N^C}} \circ d_i^A$ maps $e_{G'}$ to

$$\sum_{1\leq j\leq i} (-1)^{i-1} \varepsilon(G' - \{x'_{r_{a_j}}, x_{N^C}\}, G' - \{x'_{r_{a_j}}\}) \varepsilon(G' - \{x'_{r_{a_j}}\}, G') \cdot \frac{\operatorname{lcm}(G')}{\operatorname{lcm}(G' - \{x'_{r_{a_j}}, x_{N^C}\})} e_{G'-\{x'_{r_{a_j}}, x_{N^C}\}}.$$

On the other hand, under $d_i^{B_p} \circ f_i^{x_{N^C}}$, $e_{G'}$ maps to

$$\sum_{1\leq j\leq i} (-1)^{i} \varepsilon(G' - \{x'_{r_{a_j}}, x_{N^C}\}, G' - \{x_{N^C}\}) \varepsilon(G' - \{x_{N^C}\}, G') \cdot \frac{\operatorname{lcm}(G')}{\operatorname{lcm}(G' - \{x'_{r_{a_j}}, x_{N^C}\})} e_{G'-\{x'_{r_{a_j}}, x_{N^C}\}}.$$

Since ε satisfies

$$\varepsilon(G' - \{x'_{r_{a_j}}, x_{N^C}\}, G' - \{x'_{r_{a_j}}\}) \varepsilon(G' - \{x'_{r_{a_j}}\}, G') + \varepsilon(G' - \{x'_{r_{a_j}}, x_{N^C}\}, G' - \{x_{N^C}\}) \varepsilon(G' - \{x_{N^C}\}, G') = 0,$$

it follows that the squares commute. □

Thus, commutativity of the squares guarantees, via the mapping cone, the existence of a free resolution for $(I'_{k-1}, x_{V_1^C}, \ldots, x_{V_{p+1}^C})$, given free minimal cellular resolutions for $(I'_{k-1}, x_{V_1^C}, \ldots, x_{V_p^C})$: $x_{V_{p+1}^C} \cong I_{k-1}$ and $(I'_{k-1}, x_{V_1^C}, \ldots, x_{V_p^C})$. Furthermore, as the comparison maps $f_i^{x_{V_{p+1}^C}}$ do not involve any constants, the subsequent free resolution of $(I'_{k-1}, x_{V_1^C}, \ldots, x_{V_{p+1}^C})$ is also minimal. Moreover, the mapping cone resolution is in fact cellular:

5.1.15 Lemma. *Assume $A := I_{k-1}$ and B_p have minimal cellular resolutions, supported on $L(C_{k-1})$ and $L(C_{k-1})' \cup \{x_{V_1^C}, \ldots, x_{V_p^C}\}$, respectively. Let V be the hyperplane corresponding to the support of $x_{V_{p+1}^C}$ and let N be the hyperplane corresponding to the natural inclusion of $PG(k-1, \mathbb{F}_q)$ into $PG(k, \mathbb{F}_q)$. Let φ be an R-automorphism for which $\varphi(U \cap N) = U \cap V$ for any hyperplane U of $PG(k, \mathbb{F}_q)$ – hence B_p: $x_{V_{p+1}^C} = \varphi(A)$. Let B_{p+1} be the mapping cone of $\varphi(A)$ and B_p under the comparison maps $f_i^{x_{V_{p+1}^C}}$. Then B_{p+1} is a minimal cellular resolution supported on $L(C_{k-1})' \cup \{x_{V_1^C}, \ldots, x_{V_{p+1}^C}\}$.*

Proof. As before, we may assume that $x_{V_{p+1}^C}$ is x_{N^C}, and thus we may take φ to be the identity on R. Since B_{p+1} is a minimal free resolution, one need only check that it is also a cellular resolution with the desired support. Let $F := \{x_{r_{a_1}}, \ldots, x_{r_{a_i}}\}$ be an $(i-1)$-face in $L(C_{k-1})$ and let $G' := \{x'_{r_{a_1}}, \ldots, x'_{r_{a_i}}, x_{V_{p+1}^C}\}$ denote an i-face in $L(C_{k-1})' \cup \{x_{V_1^C}, \ldots, x_{V_{p+1}^C}\}$; thus, there is a bijective correspondence

$$G' - \{x'_{r_{a_j}}\} \longleftrightarrow F - \{x_{r_{a_j}}\}.$$

Notice that the i-th differential d_i of the cellular complex of $L(C_{k-1})' \cup \{x_{V_1^C}, \ldots, x_{V_{p+1}^C}\}$ can be written as:

$$\begin{aligned} d_i(e_{G'}) &= \sum_{\text{facets } F' \subseteq G'} \varepsilon(F', G') \frac{\operatorname{lcm}(G')}{\operatorname{lcm}(F')} e_{F'} \\ &= \varepsilon(G' - \{x_{N^C}\}, G') \frac{\operatorname{lcm}(G')}{\operatorname{lcm}(G' - \{x_{N^C}\})} e_{G' - \{x_{N^C}\}} \\ &\qquad + \sum_{1 \le j \le i} \varepsilon(G' - \{x'_{r_{a_j}}\}, G') \frac{\operatorname{lcm}(G')}{\operatorname{lcm}(G' - \{x'_{r_{a_j}}\})} e_{G' - \{x'_{r_{a_j}}\}}. \end{aligned}$$

However, as before,

$$\frac{\operatorname{lcm}(G')}{\operatorname{lcm}(G' - \{x'_{r_{a_j}}\})} = \frac{\operatorname{lcm}(F)}{\operatorname{lcm}(F - \{x_{r_{a_j}}\})}$$

thus (after relabeling the free generators $e_{G' - \{x'_{r_{a_j}}\}}$ with $F - \{x_{r_{a_j}}\}$), one obtains

$$d_i(e_{G'}) = \varepsilon(G' - \{x_{N^C}\}, G') \frac{\operatorname{lcm}(G')}{\operatorname{lcm}(G' - \{x_{N^C}\})} e_{G' - \{x_{N^C}\}}$$

$$+ \sum_{1 \leq j \leq i} \varepsilon(G' - \{x'_{r_{a_j}}\}, G') \frac{\operatorname{lcm}(F)}{\operatorname{lcm}(F - \{x_{r_{a_j}}\})} e_{F - \{x_{r_{a_j}}\}}.$$

However, the summation is by induction cellular and equal to $d_{i-1}^{A_{p+1}}(e_F)$, and so consequently,

$$d_i(e_{G'}) = d_{i-1}^{A_{p+1}}(e_F) + (-1)^i f_i^{x_{N^C}}(e_{G'}),$$

a syzygy in the mapping cone. □

5.1.16 Theorem. *There exists a minimal cellular resolution of I_k, supported on C_k.*

Proof. Assume I_{k-1} has a minimal cellular resolution supported on C_{k-1}. As I_k is finitely generated, repeated application of 5.1.15 to I_{k-1} eventually exhausts the minimal generators of I_k which are not minimal generators of I'_{k-1}. Thus, at this point, one has a minimal cellular resolution of I_k supported on the labeled cell complex $L(C_k)$. □

Note that this process in a sense generalizes the methods of [3]; instead of applying the mapping cone to ideals with linear quotients, we apply it to certain ideals with pure (nonlinear) quotients. Another cellular resolution of this family of ideals, using different (less explicit) techniques, is given in [15], while the Betti numbers of the Stanley-Reisner ideals of duals to finite projective geometries are computed in [10].

5.2 Finite Projective Geometries: The Binary Case

We are able to express resolutions of duals to binary finite projective geometries in a more explicit manner. Each codeword c of $S(k, \mathbb{F}_2)$, the k-dimensional binary simplex code, is the only nonzero codeword in the subspace generated by c; consequently, the nonzero codewords of $S(k, \mathbb{F}_2)$ and the 1-supports of $S(k, \mathbb{F}_2)$ are in bijective correspondence. Since $S(k, \mathbb{F}_2)$ contains $2^k - 1$ distinct nonzero codewords, each of the same Hamming weight (see 2.1.4), there are $2^k - 1$ distinct 1-supports of $S(k, \mathbb{F}_2)$, each of the same cardinality. As the 1-supports are equicardinal, they are also minimal, thus:

5.2.1 Proposition. *Let $\mathcal{M}(S(k,\mathbb{F}_2))$ denote the vector matroid of a parity check matrix for $S(k,\mathbb{F}_2)$. Then the collection of circuits of $\mathcal{M}$ is equal to the collection of supports of nonzero codewords of $S(k,\mathbb{F}_2)$.*

Specializing the generator matrix for S_q^k (see 5.1.4) to $\mathbb{F}_2$, one obtains

$$S_2^k = \begin{bmatrix} \overline{0} & 1 & \overline{1} \\ S_2^{k-1} & \overline{0} & S_2^{k-1} \end{bmatrix} \in \mathbb{F}_2^{k\times 2^k-1}$$

as a generator matrix for $S(k,\mathbb{F}_2)$. By permuting the columns of this matrix, one may also obtain

$$S_2^k = \begin{bmatrix} \overline{1} & 1 & \overline{0} \\ S_2^{k-1} & \overline{0} & S_2^{k-1} \end{bmatrix} \in \mathbb{F}_2^{k\times 2^k-1}$$

as a recursive description of S_2^k; for the purposes of this section, we take this description as our definition for S_2^k. Assume the nonzero codewords of S_2^{k-1} are $c_1,\ldots,c_{2^{k-1}-1}$, with supports $s_1,\ldots,s_{2^{k-1}-1}$. Let s be a subset of $\mathbb{Z}$ with $k\in\mathbb{Z}$ and denote by $s+k$ the set whose elements are s_i+k, where $s_i\in s$. From inspecting the above generator matrix for $S(k,\mathbb{F}_2)$,

$$(c_1,0,c_1),\ldots,(c_{2^{k-1}-1},0,c_{2^{k-1}-1})$$

are codewords in $S(k,\mathbb{F}_2)$ and hence have corresponding supports

$$s_1\cup(s_1+2^{k-1}),\ldots,s_{2^{k-1}-1}\cup(s_{2^{k-1}-1}+2^{k-1}).$$

Assuming via induction that each of the $2^{k-1}-1$ supports s is distinct, there are an additional $2^{k-1}-1$ distinct supports of $S(k,\mathbb{F}_2)$ obtained by subtracting the first row of S_2^k from each of the codewords $(c_i,0,c_i)$. Including the support of the first row, this yields the 2^k-1 supports

$$s_1 \cup (s_1 + 2^{k-1}), \ldots, s_{2^{k-1}-1} \cup (s_{2^{k-1}-1} + 2^{k-1}),$$
$$\overline{s_1} \cup s_1 + 2^{k-1}, \ldots, \overline{s_{2^{k-1}-1}} \cup (s_{2^{k-1}-1} + 2^{k-1}),$$
$$s_{N^C}$$

of $S(k, \mathbb{F}_2)$, and hence circuits for the vector matroid of any parity check matrix corresponding to S_2^k – for convenience, call this matroid $\mathcal{M}(S_2^k)^\perp$. Note that $\overline{s_i}$ denotes the complement of s_i relative to the indices of the columns in S_2^k whose topmost entry is 1. Consequently, we obtain the following recursive description for the Stanley-Reisner ideal:

5.2.2 Proposition. *Let $I_{k-1} = (x_{s_1}, \ldots, x_{s_{2^{k-1}-1}})$ be the Stanley-Reisner ideal of $\mathcal{M}(S_2^{k-1})^\perp$. Then I_k is minimally generated by the monomials*

$$x_{s_1} x_{s_1+2^{k-1}}, \ldots, x_{s_{2^{k-1}-1}} x_{s_{2^{k-1}-1}+2^{k-1}},$$
$$x_{\overline{s_1}} x_{s_1+2^{k-1}}, \ldots, x_{\overline{s_{2^{k-1}-1}}} x_{s_{2^{k-1}-1}+2^{k-1}},$$
$$x_{s_{N^C}}.$$

Remark. Note that for a fixed ordering of the points of $PG(k, \mathbb{F}_q)$, this may be generalized to an essentially similar procedure which produces the generators of I_k, given generators for I_{k-1}; code implementing this procedure is given in Appendix 5.3. Essentially, one chooses the ordering of the columns of S_q^k as given in 5.1.4. Let r denote the top row of S_q^k and $\gamma \in \mathbb{F}_q$. Then for each of the q^{k-2} codewords of $S(k, \mathbb{F}_q)$ of form

$$c' = (c, 0, c, \alpha c, \alpha^2 c, \ldots, \alpha^{q-2} c),$$

where c is one of the q^{k-2} codewords of $S(k-1, \mathbb{F}_q)$ with 1 as the leading nonzero entry, one may produce q codewords of form $c' - \gamma r$, each with distinct support. By induction, each c has distinct support and has 1 as its leading nonzero entry, so the same is true of $c' - \gamma r$. There are q^{k-1} codewords of this form – thus, one obtains

the q^{k-1} distinct minimal 1-supports of $S(k, \mathbb{F}_q)$, each corresponding to a generator of the Stanley-Reisner ideal of $PG(k, \mathbb{F}_q)^{\perp}$.

Each of the generators $x_{s_i}x_{s_i+2^{k-1}}$ is in fact the image of x_{s_i} under the map $r \mapsto r'$ defined in 5.1.6. Consequently,

$$\left(x_{s_1}x_{s_1+2^{k-1}}, \ldots, x_{s_{2^{k-1}-1}}x_{s_{2^{k-1}-1}+2^{k-1}}\right) : (x_{\overline{s_i}}x_{s_i+2^{k-1}}) \cong \left(x_{s_1}, \ldots, x_{s_{2^{k-1}-1}}\right).$$

In particular, the proof of 5.1.8 implies the ideal on the left is equal to $\varphi((x_{s_1}, \ldots, x_{s_{2^{k-1}-1}}))$, where φ is a permutation on the variables of the ambient ring. In this case, we are able to describe such a permutation explicitly.

5.2.3 Proposition. *Assume I_{k-1} is minimally generated by $x_{s_1}, \ldots, x_{s_{2^{k-1}-1}}$ and let $m := x_{\overline{V}}x_{V+2^{k-1}}$ be a minimal generator of $I_k \subseteq R := \mathbb{F}[x_0, \ldots, x_{2^k-1}]$ which is not also a minimal generator of I'_{k-1}. Define $\varphi_m \colon \left[2^k - 1\right] \longrightarrow \left[2^k - 1\right]$ by setting*

$$\varphi_m(i) = \begin{cases} i + 2^{k-1} & \text{if } i \in \overline{V} \text{ and } i \neq \max(\overline{V}) \\ i - 2^{k-1} & \text{if } i \in \overline{V} + 2^{k-1} \text{ and } i \neq \max(\overline{V} + 2^{k-1}) \\ i & \text{otherwise.} \end{cases}$$

Then φ_m induces an R-automorphism under which

$$\left(x_{s_1}x_{s_1+2^{k-1}}, \ldots, x_{s_{2^{k-1}-1}}x_{s_{2^{k-1}-1}+2^{k-1}}\right) : (x_{\overline{V}}x_{V+2^{k-1}}) = \varphi_m\left(I_{k-1}\right),$$

where I_{k-1} is considered as an R-ideal.

Proof. One may check that φ_m is a permutation on the variables of R – hence, we must prove that $\varphi_m(I_{k-1})$ is the quotient ideal. Let $U \in \{s_1, \ldots, s_{2^{k-1}-1}\}$. Notice that

$$\left(U \cup (U + 2^{k-1})\right) - \left(\overline{V} \cup (V + 2^{k-1})\right) = (U \cap V) \uplus \left((U - (U \cap V)) + 2^{k-1}\right);$$

thus we will prove that

$$(U \cap V) \uplus \left((U - (U \cap V)) + 2^{k-1}\right) = \varphi_m(U \cup (U + 2^{k-1})).$$

Let $x \in \varphi_m(U \cup (U + 2^{k-1}))$. Then there is a $y \in U \cup (U + 2^{k-1})$ such that $\varphi_m(y) = x$. If $x = y + 2^{k-1}$, then $y \in \overline{V}$ and $y \neq \max(\overline{V})$ – thus $x \notin V + 2^{k-1}$ and $y \notin U + 2^{k-1}$. But by assumption, $y \in U \cup (U + 2^{k-1})$, so $y \in U$, hence

$$x \in (U + 2^{k-1}) - (V + 2^{k-1}) \subseteq (U \cap V) \uplus \left((U - (U \cap V)) + 2^{k-1}\right).$$

The argument is similar if $x = y - 2^{k-1}$, so we will assume $x = y$. Since $\overline{V} \cap (\overline{V} + 2^{k-1}) = \emptyset$, the case when $y = \max(\overline{V})$ and $y = \max(\overline{V} + 2^{k-1})$ cannot occur. In addition, the case when $y = \max(\overline{V})$ and $y \notin \overline{V} + 2^{k-1}$ cannot occur – if so, then since $\max(\overline{V}) \leq 2^{k-1} - 1$, one also has $\max(\overline{V}) \notin U + 2^{k-1}$. Furthermore, $\max(\overline{V}) \notin U$ – so $y \notin U \cup (U + 2^{k-1})$. Similarly, $y = \max(\overline{V} + 2^{k-1})$ and $y \notin \overline{V}$ cannot occur. Thus, the only case remaining is when $y \notin \overline{V}$ and $y \notin \overline{V} + 2^{k-1}$, in which case

$$y \in (U \cup (U + 2^{k-1})) - (\overline{V} \cup (\overline{V} + 2^{k-1})).$$

On the other hand, assume $x \in (U \cap V) \uplus \left((U - U \cap V) + 2^{k-1}\right)$. If $x \in (U - U \cap V) + 2^{k-1}$, then $x - 2^{k-1} \in U - U \cap V$, so $x - 2^{k-1} \notin V$. Nonetheless, $x - 2^{k-1}$ is the index of a column in S_2^k whose topmost entry is 1, so $x - 2^{k-1} \in \overline{V}$. But by construction, $\max(\overline{V}) \notin U$ – hence $x - 2^{k-1} \neq \max(\overline{V})$. Thus,

$$x = \sigma_m(x - 2^{k-1}) \in \sigma_m(I \cup (I + 2^{k-1})).$$

Assume $x \in U \cap V$. Then $x \notin \overline{V}$, and since $x \in U$, $x \leq 2^{k-1}$, so $x \notin \overline{V} + 2^{k-1}$. Thus, $x = \sigma_m(x) \in \sigma_m(U \cup (U + 2^{k-1}))$. □

5.3 Resolutions of Duals to Finite Affine Geometries

5.3.1 Definition. Let $P = PG(k, \mathbb{F}_q)$ be a finite projective geometry and let H be a hyperplane in P. The space $P - H$ is called a *k-dimensional finite affine geometry* over $\mathbb{F}_q$.

To specify a matrix whose corresponding vector matroid is, up to permutation, an affine geometry, let S_q^k be a generator matrix for the k-dimensional simplex code over

$\mathbb{F}_q$ – its corresponding vector matroid is $PG(k, \mathbb{F}_q)$. Deleting the columns of S_q^k which correspond to the natural inclusion N of $PG(k-1, \mathbb{F}_q)$ into $PG(k, \mathbb{F}_q)$ (discussed in 5.1), one obtains

$$A_q^k := \begin{bmatrix} 1 & \overline{1} & \overline{1} & \cdots & \overline{1} \\ \overline{0} & S_q^{k-1} & \alpha S_q^{k-1} & \cdots & \alpha^{q-2} S_q^{k-1} \end{bmatrix},$$

where S_q^{k-1} is a generator matrix for the $(k-1)$-dimensional simplex code over $\mathbb{F}_q$. Denote the vector matroid to A_q^k by $AG(k, \mathbb{F}_q)$. Abusing notation slightly, we refer to $AG(k, \mathbb{F}_q)$ as the k-dimensional affine geometry over $\mathbb{F}_q$. Note that the matrix whose columns are the coordinate vectors of points in $\mathbb{F}_q^k$ has column dependencies which differ from those of A_q^k; indeed, as this matrix may be permuted into

$$\begin{bmatrix} \overline{0} & S_q^{k-1} & \alpha S_q^{k-1} & \cdots & \alpha^{q-2} S_q^{k-1} \end{bmatrix},$$

one sees that the circuits of the corresponding matroid are merely repetitions of the circuits of $PG(k, \mathbb{F}_q)^\perp$. The Stanley-Reisner ideal of this matroid is seen to be isomorphic to the ideal of $PG(k, \mathbb{F}_q)^\perp$, and in particular, generated in degree a multiple of the degree in which the ideal of $PG(k, \mathbb{F}_q)^\perp$ is generated – therefore, we will focus on A_q^k and characterizing the circuits of $AG(k, \mathbb{F}_q)^\perp$.

As before, the Stanley-Reisner ideal of a matroid complex M is generated by the circuits of M, and the complements of the circuits of M are the hyperplanes of $M^\perp$. Thus, taking M to be the matroid $AG(k, \mathbb{F}_q)^\perp$, we obtain a characterization for the Stanley-Reisner ideal of $AG(k, \mathbb{F}_q)^\perp$ analogous to 5.1.5, namely,

5.3.2 Proposition. *Assume J_k is the Stanley-Reisner ideal of the matroid*

$$\mathcal{M}(A_q^k)^\perp = AG(k, \mathbb{F}_q)^\perp.$$

Then r is a minimal monomial generator of J_k if and only if $\operatorname{supp}(r)$ *is the complement of a $AG(k, \mathbb{F}_q)$-hyperplane.*

As one deletes a hyperplane of $PG(k, \mathbb{F}_q)$ to obtain $AG(k, \mathbb{F}_q)$, a natural question to ask is whether this relationship extends in some sense to the Stanley-Reisner ideals

of $PG(k,\mathbb{F}_q)^\perp$ and $AG(k,\mathbb{F}_q)^\perp$. In fact, it does:

5.3.3 Proposition. *Let I_k be the Stanley-Reisner ideal of $PG(k,\mathbb{F}_q)^\perp$ and let J_k denote the Stanley-Reisner ideal of $AG(k,\mathbb{F}_q)^\perp$. Let x_N be the monomial supported on N, the natural inclusion of $PG(k-1,\mathbb{F}_q)$ into $PG(k,\mathbb{F}_q)$. Then $I_k\colon x_N \cong J_k$.*

Proof. Take $PG(k,\mathbb{F}_q)$ and $AG(k,\mathbb{F}_q)$ to be the vector matroids of S_q^k and A_q^k, respectively. Let m be a minimal generator of $I_k\colon x_N$ – thus, m is supported on $V^C - N$, where V is a $PG(k,\mathbb{F}_q)$-hyperplane. Since affine hyperplanes have support contained within N^C, we must show that

$$N^C - (V^C - N) = N^C - V^C$$

is an affine hyperplane in $AG(k,\mathbb{F}_q)$. Let p be a point in V which is not in N – hence $p_0 = 1$. Since $p \in V$, the coordinates of p satisfy a homogeneous linear form

$$l(x_0,\ldots,x_k) = 0.$$

Dehomogenizing l by setting $x_0 = 1$ yields an affine hyperplane in $AG(k,\mathbb{F}_q)$ on which p lies.

Conversely, if p is a point on an affine hyperplane in $AG(k,\mathbb{F}_q)$, then p satisfies a linear form

$$a_1x_1 + \cdots + a_kx_k + b = 0,$$

which homogenizes to

$$a_1x_1 + \cdots + a_kx_k + bx_0 = 0. \qquad (*)$$

Comparing these equations, $x_0 = 1$, hence $p_0 = 1$, so $p \in N^C$. Furthermore, $(1\colon p_1\colon \cdots\colon p_k)$ satisfies *, so p also lies on a $PG(k,\mathbb{F}_q)$-hyperplane. □

In the projective case, we mapped the hyperplanes of $PG(k,\mathbb{F}_q)$ to a subset of the hyperplanes of $PG(k+1,\mathbb{F}_q)$ by reconsidering their ideals as ideals in a ring with

one additional variable; we will extend this construction further in order to map the hyperplanes of $PG(k, \mathbb{F}_q)$ to a subset of the hyperplanes of $AG(k+1, \mathbb{F}_q)$. As before, assume V is a $PG(k, \mathbb{F}_q)$-hyperplane – hence V is the variety of a homogeneous linear form

$$l(x_0, \ldots, x_k) = 0.$$

Considering l as a polynomial in the variables $x_{-1}, x_0, \ldots, x_k$, one obtains the $PG(k+1, \mathbb{F}_q)$-hyperplane defined by $l(x_{-1}, x_0, \ldots, x_k)$. Since we identify the points of $AG(k+1, \mathbb{F}_q)$ with those whose first coordinate is 1, we dehomogenize l by setting $x_{-1} = 1$ to obtain the $AG(k+1, \mathbb{F}_q)$-hyperplane corresponding to

$$l(x_0, \ldots, x_k) = -a_{-1} = 0.$$

Call this hyperplane $\widetilde{V}$. For convenience, we will adhere to the notation $I_k := I(\mathcal{M}(S(k, \mathbb{F}_q))) = I(PG(k, \mathbb{F}_q)^{\perp})$ to designate the Stanley-Reisner ideal of the matroid dual to $PG(k, \mathbb{F}_q)$, and likewise $J_k := I(AG(k, \mathbb{F}_q)^{\perp})$ for the Stanley-Reisner ideal of the dual to $AG(k, \mathbb{F}_q)$.

5.3.4 Definition. Let x_{V^C} be a minimal generator of I_k, where V is a hyperplane in $PG(k, \mathbb{F}_q)$. Define $\widetilde{x_{V^C}} := x_{\widetilde{V}^C}$ and set $\widetilde{I_k}$ to be the ideal generated by the monomials $\widetilde{x_{V^C}}$.

As $\widetilde{V}$ is an $AG(k+1, \mathbb{F}_q)$-hyperplane, one has that $\widetilde{I_k}$ is contained in the Stanley-Reisner ideal of $AG(k+1, \mathbb{F}_q)^{\perp}$, J_{k+1}. Furthermore, there exists a recursive relationship between I_k and J_{k-1} analogous to that considered for the projective case:

5.3.5 Lemma. *Assume V is an $AG(k, \mathbb{F}_q)$-hyperplane, with X_{V^C} a minimal generator of J_k supported on the complement of V, and denote by $J_k - x_{V^C}$ the ideal generated by the minimal generators of J_k except for x_{V^C}. Then*

$$(J_k - x_{V^C}) : x_{V^C} \cong J_{k-1}$$

Proof. Notice that the generators of $(J_k - x_{V^C}) : x_{V^C}$ have the form $x_{U^C - V^C}$, where

U is an $AG(k, \mathbb{F}_q)$-hyperplane. Since

$$U^C - V^C = V - U \cap V,$$

one may use another dimension argument, albeit modified. If U and V are parallel hyperplanes, then since $(J_k - x_{V^C})$ doesn't have x_{V^C} as one of its minimal generators, $U \neq V$. Thus, $U \cap V = \emptyset$, so $x_{U^C - V^C} = x_V$, which is divisible by the generators of $(J_k - x_{V^C}) : x_{V^C}$ for which $U \cap V \neq \emptyset$. Thus, we only consider hyperplanes U and V which aren't parallel.

In the event that U and V are not parallel, $\dim(U \cap V) = k - 2$, so $U \cap V \cong AG(k-2, \mathbb{F}_q)$. Therefore,

$$\begin{aligned}(J_k - x_{V^C}) : x_{V^C} &= (x_{V - U\cap V} \,|\, U \cong AG(k-1, \mathbb{F}_q)) \\ &= (x_{V-L} \,|\, L \cong AG(k-2, \mathbb{F}_q)) \\ &\cong J_{k-1}\end{aligned}$$

□

5.3.6 Corollary. *Assume I_k, J_{k-1}, $J_k \subseteq R$ are the Stanley-Reisner ideals of the matroids $\mathcal{M}(S_q^k)^\perp = PG(k, \mathbb{F}_q)^\perp$, $\mathcal{M}(A_q^{k-1})^\perp = AG(k-1, \mathbb{F}_q)^\perp$, and $\mathcal{M}(A_q^k)^\perp = AG(k, \mathbb{F}_q)^\perp$, respectively. Let $\widetilde{I_k}$ be as defined above, and assume $x_{V_1^C}, \ldots, x_{V_{p+1}^C}$ are distinct minimal generators of J_k, none of which are generators of $\widetilde{I_k}$. Then*

$$(\widetilde{I_k}, x_{V_1^C}, \ldots, x_{V_p^C}) \colon x_{V_{p+1}^C} \cong J_{k-1}.$$

Proof. As in the projective case, the proof of 5.3.5 also implies that $\widetilde{I_k} \colon x_{V_{p+1}^C} \cong J_{k-1}$, via the same logic: if U is an $AG(k, \mathbb{F}_q)$-hyperplane parallel to v_{p+1}, then the exclusion of $x_{V_{p+1}^C}$ from $\widetilde{I_k}$ implies $U \neq v_{p+1}$, thus $U \cap V = \emptyset$, and therefore $x_{U^C - v_{p+1}^C} = x_{V_{p+1}^C}$, which isn't minimal. Otherwise, U and v_{p+1} intersect along an $AG(k-2, \mathbb{F}_q)$. Employing this in conjunction with 5.3.5,

$$J_{k-1} \cong \widetilde{I_{k-1}} \colon x_{V_{p+1}^C}$$

$$\subseteq (\widetilde{I_{k-1}}, x_{V_1^C}, \ldots, x_{V_p^C}) \colon x_{V_{p+1}^C}$$
$$\subseteq (J_k - x_{V_{p+1}^C}) \colon x_{V_{p+1}^C}$$
$$\cong J_{k-1}.$$

□

From [9], the $\mathbb{Z}^n$-graded Betti number $\beta_{i,\sigma}$ of the Stanley-Reisner ideal of a matroid $M = (E, \mathcal{I})$ is nonzero if and only if $\sigma \subseteq E$ is an inclusion-minimal set for which $n_M(\sigma) = i$. By the duality given in 3.1.8, this is equivalent to $E - \sigma$ being an $(r(M^\perp) - i)$-flat of $M^\perp$. In the case when $M = PG(k, \mathbb{F}_q)^\perp$, we obtain that such an $E - \sigma$ is a $(k - i)$-flat of $PG(k, \mathbb{F}_q)$, and is therefore a $PG(k - i, \mathbb{F}_q)$. Thus,

$$|E - \sigma| = \#PG(k - i, \mathbb{F}_q) = \frac{q^{k-i} - 1}{q - 1},$$

and consequently, the minimum twist (in fact, the only twist, due to 3.1.7) at the i-th position in a minimal free resolution of the Stanley-Reisner ideal of $PG(k, \mathbb{F}_q)^\perp$ is:

$$d_i(PG(k, \mathbb{F}_q)^\perp) = |\sigma| = |E| - |E - \sigma| = \frac{q^k - 1}{q - 1} - \frac{q^{k-i} - 1}{q - 1},$$

the same as derived in [10]. However, in the case when $M = AG(k, \mathbb{F}_q)^\perp$, where $|E| = q^k$ and $|E - \sigma|$ is a $(k - i)$-flat of $AG(k, \mathbb{F}_q)$, and hence has cardinality q^{k-i}, the same reasoning yields minimum twists of

$$d_i(AG(k, \mathbb{F}_q)^\perp) = q^k - q^{k-i} = (q - 1)d_i(PG(k, \mathbb{F}_q)^\perp).$$

Using 3.1.7 again and the fact that any minimal free resolution of J_k has length $k + 1$, we may compute the Betti numbers of J_k using the Herzog-Kühl equations. In the case when $i \neq k + 1$, one may compute

$$\beta_{i,d_i}(J_k) = q^i q^{\frac{i(i-1)}{2}} \binom{k}{i}_q$$
$$= q^i \beta_{i,d_i}(I_k),$$

where $\beta_{i,d_i}(I_k) = q^{\frac{i(i-1)}{2}}\binom{k}{i}_q$ was determined in [10] and $\binom{k}{i}_q$ denotes the Gaussian binomial coefficient. When $i = k+1$, one obtains

$$\beta_{k+1,d_{k+1}} = (q-1)(q^2-1)\cdots(q^k-1).$$

Since $d_i(AG(k,\mathbb{F}_q)^\perp) > d_i(AG(k-1,\mathbb{F}_q)^\perp)$, any chosen map of complexes between a minimal free resolution of $J_{k-1} \cong (\widetilde{I_{k-1}}, x_{V_1^C}, \ldots, x_{V_p^C})\colon x_{V_{p+1}^C}$ and a minimal free resolution for $(\widetilde{I_{k-1}}, x_{V_1^C}, \ldots, x_{V_p^C})$ has positive degree. Consequently, the comparison maps are minimal, so using the same model of induction as in the projective case, one obtains the following result.

5.3.7 Proposition. *There exists a minimal free resolution of J_k by mapping cones.*

Appendix: Macaulay2 Code

Some effort has gone into developing methods in the *Macaulay2* [5] computer algebra system to support research into combinatorial invariants of linear block codes. A summary of some of the more important methods developed for *Macaulay2* is included below. In the event that a function calls a secondary method which is not native to *Macaulay2*, a description of the secondary method's functionality is provided; only the essential code is included. Note that this code is compatible with version 1.7 of *Macaulay2*.

As finite affine and projective spaces arise via simplex and Reed-Muller codes, methods for computing such spaces are provided below. Due to their differing Stanley-Reisner ideals, we distinguish between finite affine spaces and finite affine geometries and provide methods for each. Note that each of the following procedures may easily be refactored to run iteratively, if one desires to produce a list of finite geometries.

```
-----------------------------------------------------------------------
-- Input: a nonnegative integer r and a GaloisField F
-- Output: a matrix whose columns are the pairwise linearly
--  independent vectors in F^r
-- Remark: block(m, n, alpha) returns an m x n matrix whose entries
--  are equal to alpha
-----------------------------------------------------------------------
finiteProjectiveGeometry = method(TypicalValue => Matrix);
finiteProjectiveGeometry(ZZ, GaloisField) := Matrix => (r, F) -> (
    if (r < -1) then (
        error "expected r to be at least -1";
    ) else if (r == -1) then (
        matrix mutableMatrix(F, 0, 0)
    ) else if (r == 0) then (
        matrix {{1_F}}
    ) else (
        aff := finiteAffineSpace(r, F);
        pg := finiteProjectiveGeometry(r-1, F);
        zeros := block(1, numCols pg, 0_F);
        ones := block(1, numCols aff, 1_F);

        ((zeros | ones) || (pg | aff))
```

```
    )
)

-----------------------------------------------------------------------
-- Input: a nonnegative integer r and a GaloisField F
-- Output: a matrix whose columns are the points in the rank r finite
--  affine geometry over F
-----------------------------------------------------------------------
finiteAffineGeometry = method(TypicalValue => Matrix);
finiteAffineGeometry(ZZ, GaloisField) := Matrix => (r, F) -> (
    if (r < 0) then (
        error "expected r to be at least 0";
    ) else if (r == 0) then (
        matrix mutableMatrix(F, 0, 0)
    ) else (
        aff := finiteAffineSpace(r, F);

        block(1, numCols aff, 1_F) || aff
    )
)

-----------------------------------------------------------------------
-- Input: a nonnegative integer k and a field F
-- Output: a matrix over F whose columns are the points in affine
--  k-space over F
-- Remark: fieldElements(F) returns a list containing the elements of
--  the field, in the order {0, a^0, a^1, a^2, ...}, where a is a
--  primitive element; blockMatrix(m, n, mat) returns a matrix
--  consisting of m x n copies of mat
-----------------------------------------------------------------------
finiteAffineSpace = method(TypicalValue => Matrix);
finiteAffineSpace(ZZ, GaloisField) := Matrix => (k, F) -> (
    if (k < 0) then (
        error "expected k to be at least 0";
    ) else (
        fldElements := fieldElements F;

        if (k == 0) then (
            matrix mutableMatrix(F, 0, 0)
        ) else if (k == 1) then (
            matrix {fldElements}
        ) else (
            aff := finiteAffineSpace(k-1, F);
            aff' := blockMatrix(1, fieldOrder F, aff);
```

```
            topRow := matrix {
                for i in fldElements list
                    (numCols aff):i
            };

            sub(topRow, ring aff') || aff'
        )
    )
)
```

One may compute the minimal 1-supports of the simplex codes – and hence the complements to hyperplanes of finite projective geometries – using the following method.

```
-----------------------------------------------------------------------
-- Input: a positive integer k and a GaloisField F
-- Output: a list of representatives of the minimal 1-supports of the
--  k-dimensional simplex code over F
-- Remark: finiteProjectiveGeometries(k, F) returns a list of the
--  finite projective geometries up to rank k
-----------------------------------------------------------------------
simplexCodeSupportCodewords = method(TypicalValue => List);
simplexCodeSupportCodewords(ZZ, GaloisField) := List => (k, F) -> (
    if (k < 1) then (
        error "expected a positive dimension";
    ) else (
        a := primitiveElement F;
        ls := toList(0 .. fieldOrder(F)-2);
        projGeometries := finiteProjectiveGeometries(k-1, F);
        suppWords := {first projGeometries};

        for i from 2 to k do (
            repSupp := for c in suppWords list (
                cols := apply(ls, z -> a^z * c);
                c' := join({c, matrix {{0_F}}}, cols);
                matrix {c'}
            );

            topRow := (projGeometries#(i-1))^{0};
            linComs := flatten for c in repSupp list (
                apply(ls, z -> c - a^z * topRow)
            );

            suppWords = join(repSupp, linComs, {topRow});
```

```
        );

        suppWords
    )
)
```

BCH codes and their duals are a particularly rich source of examples; their generator polynomials (or more generally, the generator polynomial of any cyclic code with a specified defining set) may be computed in *Macaulay2* using the following pair of methods.

```
-----------------------------------------------------------------------
-- Input: a GaloisField F, an integer n, and a list of representatives
--  of q-cyclotomic cosets mod n
-- Output: the polynomial whose defining set consists of the powers of
--  a primitive element which lie in the cyclotomic cosets specified
--  by cycCosetReps
-- Remark: minRootOfUnityExtensionDegree(n, q) returns the degree of
--  the smallest field extension over GF q which contains an n-th root
--  of unity
-----------------------------------------------------------------------
cycCosetPol = method(TypicalValue => RingElement);
cycCosetPol(GaloisField, ZZ, List) := RingElement => (F, n, reps) -> (
    q := fieldOrder F;
    x := local x;
    S := F[x];

    if (reps == {}) then (
        1_S
    ) else (
        G := GF q^(minRootOfUnityExtensionDegree(n, q));
        ord := ((fieldOrder G)-1) // n;
        minPols := apply(reps, i -> minPol(i*ord, G, S));

        product unique minPols
    )
)

-----------------------------------------------------------------------
-- Input: a nonnegative integer i, a GaloisField G, and a
--  PolynomialRing S in one variable, with a subfield of G as its
--  coefficient ring
-- Output: the minimal polynomial over a subfield F of G of the i-th
```

```
--  power of the primitive element used by M2 to represent G, returned
--  as an element of S
-- Caveat: the coefficients of the polynomial f returned by this
--  function live in the ground field F.  Thus, in order to obtain
--  f(a^i) = 0, as expected, one must map f into G[y] via iota
--  (defined in the code below).
-- Remark: primitiveElement(F) returns a primitive element of the
--  given field F; cyclotomicCoset(q, s, n) returns the q-cyclotomic
--  coset of s mod n
-----------------------------------------------------------------------
miPo = method(TypicalValue => RingElement);
miPo(ZZ, GaloisField, PolynomialRing) := RingElement => (i, G, S) -> (
    F := coefficientRing S;

    if (class F =!= GaloisField) then
        error "expected a polynomial ring over a GaloisField";
    if (numgens S != 1) then
        error "expected a polynomial ring in one variable";
    if (i < 0) then
        error "expected a nonnegative integer";
    if not isSubfield(F, G) then (
        error concatenate("expected coefficient ring of ",
            toString S, " to be a subfield of ", toString G);
    );

    y := local y;
    T := G[y];
    aF := primitiveElement F;
    aG := primitiveElement G;
    cycCoset := cyclotomicCoset(fieldOrder F, i, fieldOrder(G)-1);
    mappings := {aF => sub(aF, G), S_0 => T_0};
    iota := map(T, S, mappings);
    minPolImage := product apply(cycCoset, z -> (T_0)-aG^z);

    first (preimage(iota, ideal minPolImage))_*
)
```

Bibliography

[1] D. Bayer and B. Sturmfels. Cellular Resolutions of Monomial Modules. *Journal für die reine und angewandte Mathematik*, 502:123–140, 1998.

[2] A. Corso and U. Nagel. Specializations of Ferrers ideals. *Journal of Algebraic Combinatorics*, 28:425–437, Nov. 2008.

[3] A. Dochtermann and F. Mohammadi. Cellular resolutions from mapping cones. *Journal of Combinatorial Theory, Series A*, 128:180–206, Nov. 2014.

[4] D. Eisenbud. *Commutative Algebra with a View Toward Algebraic Geometry*. Springer, 1999.

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

[6] J. Herzog and Y. Takayama. Resolutions by mapping cones. *Homology, Homotopy, and Applications*, 4(2):277–294, 2002.

[7] C. Huffman and V. Pless. *Fundamentals of Error-Correcting Codes*. Cambridge University Press, 1st edition, 2010.

[8] T. Johnsen, J. Roksvold, and H. Verdure. A generalization of weight polynomials to matroids. 2013.

[9] T. Johnsen and H. Verdure. Hamming weights and Betti numbers of Stanley-Reisner rings associated to matroids. *Applicable Algebra in Engineering, Communication and Computing*, 24:73–93, Jan. 2013.

[10] T. Johnsen and H. Verdure. Stanley-Reisner resolution of constant weight linear codes. *Designs, Codes and Cryptography*, 72:471–481, Aug. 2014.

[11] F.J. MacWilliams and N.J.A. Sloane. *The Theory of Error-correcting Codes*. North-Holland Publishing Company, 1977.

[12] W. Massey. *Singular Homology Theory*. Springer, 2012.

[13] E. Miller and B. Sturmfels. *Combinatorial Commutative Algebra*. Springer, 2005.

[14] U. Nagel and V. Reiner. Betti numbers of monomial ideals and shifted skew shapes. *Electronic Journal of Combinatorics*, 16, 2009.

[15] I. Novik. Lyubeznik's Resolution and Rooted Complexes. *Journal of Algebraic Combinatorics*, 16:97–101, July 2002.

[16] I. Novik, A. Postnikov, and B. Sturmfels. Syzygies of oriented matroids. *Duke Mathematical Journal*, 111(2):287–317, 2002.

[17] I. Novik and E. Swartz. Face ring multiplicity via CM-connectivity sequences. *Canadian Journal of Mathematics*, 61:888–903, Aug. 2009.

[18] J. Oxley. *Matroid Theory*. Oxford University Press, 2nd edition, 2011.

[19] I. Peeva. *Graded Syzygies*. Springer, 2011.

[20] R. Stanley. *Combinatorics and Commutative Algebra*. Progress in Mathematics. Birkhäuser Boston, 2007.

[21] M. Velasco. Minimal free resolutions that are not supported by a CW-complex. *Journal of Algebra*, 319:102–114, Jan. 2008.

[22] V. Wei. Generalized Hamming Weights for Linear Codes. *IEEE Transactions on Information Theory*, 37:1412–1418, Sept. 1991.

[23] D.J.A. Welsh. *Matroid Theory*. Dover Publications, Inc., 2010.

Vita

Education

M.A. Mathematics, *University of Kentucky* *Dec. 2011*

B.S. Mathematics, *University of Dayton* *Aug. 2009*