Investigating Linear Codes Via Commutative Algebra

Susan Cooper (University of Manitoba),
Alexandra Seceleanu (University of Nebraska–Lincoln),
Ştefan Tohăneanu (University of Idaho),
Adam Van Tuyl (McMaster University)

July 22 –July 29, 2018

1 Overview of the Field

The importance of coding theory to the digital era that we live in cannot be overstated. Our research meeting aimed to explore the relationship between the theory of error-correcting codes and the more classically studied fields commutative algebra and algebraic geometry, with the goal of establishing a toolset of joint relevance.

A *linear code* of length s is a linear subspace $\mathcal{C}$ of a finite dimensional vector space K^s over a finite or infinite field K. A linear code of length s and dimension $\dim_K(\mathcal{C}) = n$ is often viewed as the row space of a $n \times s$ matrix G. The *Hamming distance* d of $\mathcal{C}$ is the minimum number of nonzero entries in a nonzero element (codeword) in $\mathcal{C}$. The numbers s, n and d are called the parameters of $\mathcal{C}$, and the code with these parameters is termed an $[s, n, d]$-code. A central theme to the study of codes is the determination of their minimum Hamming distance, which is a measure of the code's error correction capability.

Hamming distance has a nice geometric interpretation: if the columns of the generating matrix G are viewed as coordinates for a set of points $X = \{P_1, \ldots, P_s\}$ in projective space $\mathbb{P}^{n-1}$ and if these points are distinct, then, setting $\mathrm{hyp(X)} =$ the maximum number of points among $P_1, \ldots, P_s$ that are contained in a hyperplane, gives $d = n - \mathrm{hyp(X)}$. This description of Hamming distance gives a first glimpse at the crucial role that the geometry of zero-dimensional projective schemes plays in coding theory.

It may be the case, however, that some of the columns of the generating matrix G are proportional vectors. Note that adding proportional columns does not change the set of points X, however it does change the row space of G and hence the code $\mathcal{C}$. In this situation, one must keep track both of the set of distinct points arising from the columns of the generating matrix and their respective multiplicities. This data is represented algebraically by means of a *fat* (non-reduced) *point scheme* $Y = m_1P_1 + \cdots + m_sP_s$, where m_i is the multiplicity of the point P_i, i.e., the number of columns of G proportional to the coordinate vector of P_i.

Evaluation codes are a class of codes of great practical importance which can be defined in the language of polynomials. Let $S = K[t_1, \ldots, t_n] = \oplus_{d=0}^{\infty} S_d$ be a polynomial ring over K with the standard grading and let X be a finite subset of $\mathbb{P}^{n-1}$ as above. The *vanishing ideal* of X is the ideal generated by the homogeneous polynomials vanishing on X. For each $d \geq 0$ there is a linear map of K vector spaces

$$\mathrm{ev}_d : K[t_1, \ldots, t_n]_d \to K^s \quad f \mapsto \left(\frac{f(P_1)}{f_0(P_1)}, \ldots, \frac{f(P_s)}{f_0(P_s)} \right), \quad \text{where } f_0(t_1 \ldots, t_n) = t_1^d.$$

The kernel of ev_d is precisely the set of degree d polynomials in $I(X)$, denoted $I(X)_d$, and the image of ev_d is a linear code denoted by $\mathcal{C}_d(X)$ and termed an evaluation code. The case $d = 1$ gives the linear code associated to the matrix G whose columns are the points in X; this represents the K-linear map ev_1.

2 Recent Developments and Open Problems

The correspondence between reduced point schemes in projective spaces and codes has been established and studied from a commutative algebra point of view in [7] and [5]. In [11], numerical invariants of point schemes are used to bound invariants of the corresponding linear codes and vice-versa. Specifically Tohăneamu and Van Tuyl prove the following bounds hold true in the case $Y = m_1P_1 + \cdots + m_sP_s$: $d \geq \alpha(Y) - m(Y)$. Here $\alpha(Y)$ is the smallest degree of a hypersurface passing through $P_1, \dots, P_s$ with multiplicities $m_1, \dots, m_s$ respectively and $m(Z) = \max\{m_1, \dots, m_s\}$. A natural generalization is the following

Problem 1. *Investigate whether the stronger inequality $d \geq \mathrm{reg(X)} - \mathrm{m(X)} + 1 \geq \alpha(\mathrm{X}) - \mathrm{m(X)}$ holds, where $\mathrm{reg(X)}$ (the Castelnuovo-Mumford regularity) is the least degree in which the Hilbert function of X agrees with the number of points of X (counted with multiplicity).*

The classical notion of Hamming distance, which is central to coding theory, has been generalized to a family of *generalized Hamming weights* in [12]. One can ask

Problem 2. *Is there a characterization for generalized Hamming distances for evaluation ideals in terms of the geometry of the set of reduced points X or the fat point scheme Y analogous to the complement to the maximum number of points contained in a hyperplane characterization given in section 1?*

We have seen in section 1 how generator matrices and evaluation maps produce codes, but in turn these matrices and maps respectively can be produced from graphs or, more generally, from simplicial complexes. Let $G = (V, E)$ be a simple graph on vertex set $V = \{1, \dots, n\}$, and with $s = |E|$ edges. We assume that G is connected. A *cutset* of G is a set of edges in E such that when it is removed it disconnects the graph. Consider the linear code with generating matrix of size $n \times s$, where each column corresponds to an edge $[i, j] \in E(G)$ and the entries of that column are zeros, except for the i-th and j-th entries which are 1 and -1 respectively. By [11], the minimum distance d of the linear code generated in this manner is equal to the size of the smallest cutset of G. If G is a planar graph, then this is equal to the smallest size of a simple cycle in the dual graph of G. We ask

Problem 3. 1. *When is the linear code constructed from the a graph as described above a minimum distance separable (MDS) code? That is, when is $d = s - n + 2$, where n is the number of vertices, s the number of edges and d is the size of the smallest cutset?*

2. *Is the code associated to the dual graph $G^\perp$ the dual to the code constructed from the graph G?*

When K is a finite field, the basic parameters (length, dimension, and minimum distance) of the evaluation codes $\mathcal{C}_d$ associated to the set $\mathbb{T}^{s-1} = \{[(x_1, \dots, x_s)] \in \mathbb{P}^{s-1} : x_i \in K^* \text{ for all } i\}$ are known for each $d \geq 0$ (see [6] and [9]). The finite set $\mathbb{T}^{s-1}$ is called the *projective torus* of dimension $s-1$ over K and $I(\mathbb{T}^{s-1}) = (t_2^{q-1} - t_1^{q-1}, \dots, t_s^{q-1} - t_1^{q-1})$. In general, when considering evaluation codes for proper subsets $X \subset \mathbb{T}^{s-1}$, the basic parameters of $\mathcal{C}_d$, especially the minimum distance, can be hard to determine even when $d = 1$. Let G be a simple graph with p vertices $V = \{1, \dots, p\}$ and q edges, and let $\mathbb{X}$ be the algebraic toric set parameterized by all monomials y_iy_j such that $[i, j]$ is an edge of G, that is the coordinates of every point in $\mathbb{X}$ are given by evaluating all the monomials y_iy_j corresponding to edges of the graph at a point in $\mathbb{T}^{s-1}$. In this case, we say that $\mathcal{C}_d(\mathbb{X})$ is the *parameterized linear code* of order d associated to $\mathbb{X}$.

Problem 4. *For certain families of graphs, determine the generators of $I(\mathbb{X})$, the regularity of $S/I(\mathbb{X})$, and the minimum distance of the linear codes $C_d(\mathbb{X})$ associated to the given graphs (the length of the codes, $|\mathbb{X}|$, is already known by [8]).*

3 Presentation Highlights

Susan Cooper introduced the paradigm that relates linear codes and the geometry of zero-dimensional schemes in projective space, as described in the first section. The focus of her talk was on obtaining bounds of the Hamming distance for linear codes using algebraic parameters of homogeneous ideals in polynomial rings. In particular, she highlighted two results from [11] which give bounds for a linear code with generating matrix G whose columns correspond to a fat point scheme $Y = m_1P_1 + \cdots + m_sP_s$ on a set of points $X = \{P_1, \ldots, P_s\}$. On one hand, if $m_1 \geq m_2 \geq \cdots \geq m_s$ then the following inequalities hold for the Hamming distance d

$$m_1 + \cdots + m_{d(X)} \geq d \geq m_{\mathrm{hyp(X)}} + \cdots + m_s.$$

On the other hand, if $m_1 = \cdots = m_s = m$ (the case of a uniform fat point scheme), then d can be bounded in terms of $\alpha(X)$, the minimum degree of a hypersurface passing through all the points in X and in terms of a homological invariant of $I(X)$ termed the minimum socle degree. The speaker proposed several strategies, such as trimming, a procedure originating in the paper [1], which gives a good handle on the Hilbert function of a fat point scheme and asked how minimum distance behaves under this operation.

Ştefan Tohăneanu talked about interpreting the Hamming distance of a code in terms of ideals generated by products of linear forms. Let $\ell_1, \ldots, \ell_s \in R := \mathbb{K}[x_1, \ldots, x_n]$ be linear forms such that $\langle \ell_1, \ldots, \ell_s \rangle = \langle x_1, \ldots, x_n \rangle$ and let $\mathcal{C}$ be the code whose generating matrix has as columns the coefficients of the linear forms. For $1 \leq a \leq s$, we define the ideal generated by $a-$fold products of these forms to be the ideal of R

$$I(a) := \langle \{\ell_{i_1} \cdots \ell_{i_a} | 1 \leq i_1 < \cdots < i_a \leq s\} \rangle.$$

De Boer-Pellikaan [4, Exercise 3.25] noticed that $d(\mathcal{C}) = \max\{a | \mathrm{ht}(I(a)) = k\}$ (here ht denotes the height of an ideal), a fact which can be extended to recover the generalized Hamming weights as well. The speaker presented a conjecture from [10] which states that the ideals $I(a)$ have linear graded minimal free resolutions, as well as partial results which support this conjecture.

Maria Vaz Pinto talked about evaluation codes on toric sets. When K is a finite field and

$$\mathbb{X} = \{ \, [(x_1^{v_{11}} \ldots x_p^{v_{1p}}, \ldots, x_1^{v_{s1}} \ldots x_p^{v_{sp}})] : x_i \in K^* \text{ for all } i \, \} \subseteq \mathbb{P}^{s-1},$$

one says that $\mathbb{X}$ is the algebraic toric set parameterized by $y^{v_1}, \ldots, y^{v_s}$ (s monomials in n variables, $y^{v_i} = y_1^{v_{i1}} \ldots y_n^{v_{in}}, \ v_{ij} \in \mathbb{N}$). The speaker considered the parameterized linear code of order d associated to $\mathbb{X}$, $\mathcal{C}_d(\mathbb{X})$. She highlighted some remarkable properties of these parametrized linear codes, such as the dictionary establishing equivalences between the length of the code and the degree (multiplicity) of the vanishing ideal $I(\mathbb{X})$ or the dimension of the code and the value of the Hilbert function for $S/I(\mathbb{X})$ in degree d. She pointed out that a good description for the Hamming distance is still elusive in many important cases.

Rafael Villarreal proposed in his talk a broad generalization for the notion of Hamming distance. Instead of studying the distance of a linear code by converting the generating matrix into a set of points X in projective space and using the linear aspects of the geometry of these points, as encoded by the $\mathrm{hyp(X)}$, one can start with any homogeneous ideal I in a polynomial ring and define a generalized $\mathrm{hyp_I(d,r)}$ function that encodes the maximum degree of a subscheme $X \subset V(I)$ that is also supported on the intersection of r hypersurfaces of degree d which are linearly independent modulo the ideal I. The talk was dedicated to exploring properties of this new function and the way they generalize previously known results. The speaker also presented a computer program designed to efficiently approximate the generalized Hamming distances for a code based on the use of initial ideals (Gröbner bases).

4 Scientific Progress Made

A substantial amount of algebraic and homological techniques are available to commutative algebraists in order to analyze properties of varieties embedded in affine or projective space. Familiarity with these techniques has allowed the participants of this focused research group to bring their expertise to bear on several issues of current interest in coding theory introduced in section 2. By recasting some central notions of coding theory into algebraic language we were able to strengthen and generalize them to many new settings. Our main contributions consist of: (1) developing a notion of *generalized minimum distance functions* motivated by the generalized Hamming weights of [12] and (2) analyzing several families of codes built from graphs, which include linear codes whose generator matrix is a signed incidence matrix of a simple graph and toric codes parametrized by monomials encoding edges of a graph.

4.1 Generalized minimum distance functions

This new notion generalizes the notions of distance existent in coding theory using the algebraic-geometric invariant of a scheme called *degree* (or multiplicity). Let $S = K[t_1, \ldots, t_n] = \oplus_{d=0}^{\infty} S_d$ be a polynomial ring over a field K with the standard grading and let $I \neq (0)$ be a graded ideal of S. We denote the degree of S/I by $\deg(S/I)$. The function $\delta_I \colon \mathbb{N}_+ \times \mathbb{N}_+ \to \mathbb{Z}$ given by

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

is called the *generalized minimum distance* function of I, where $\mathcal{F}_{d,r}$ is the set

$$\mathcal{F}_{d,r} := \{\, \{f_1, \ldots, f_r\} \subset S_d \,|\, f_1, \ldots, f_r \text{ are linearly independent modulo } I, (I \colon (f_1, \ldots, f_r)) \neq I\}.$$

To compute $\delta_I(d,r)$ is a difficult problem, hence one of our aims is to introduce lower bounds for $\delta_I(d,r)$ which are easier to compute. One of our main results shows that there exists a function $\mathrm{fp}_I(d,r)$ termed the *footprint function* which is a lower bound for $\delta_I(d,r)$ and is easier to compute. We also explore other notions of generalized minimum distance such as the *generalized minimum Loewy distance*, which is better behaved with respect to non-reduced scheme structures and could provide a satisfactory answer to problems 1 and 2 of section 2. Moreover, since we make use of computational algebra programs in our research, we have programmed routines compatible with the computational algebra system *Macaulay 2* for computing and analyzing these new invariants.

4.2 Codes from graphs

In our second project, we analyze codes arising from graphs $G = (V(G), E(G))$ with n vertices and s edges. Let A_G be the matrix whose columns correspond to the oriented edges of G: if $\{k, l\}$ is the j-th edge then the jth column of A_G has zeros in all of its positions, except in the entries (k, j) and (l, j) of A_G, wich are equal to 1 and -1, respectively. If G is connected, $\mathrm{rank(A_G) = n - 1}$ and the rows of A_G span a $[\,q,\, n-1,\, d_1(C)\,]$-linear code $\mathcal{C}$. We prove that, if G is a connected graph that is not a tree and X is the set of points whose coordinates are given by the columns of A_G, then the Castelnuovo-Mumford regularity of $I(X)$ is 2. We also classify the graphs that give rise to MDS codes, partially answering problems 3 and 4 of section 2.

5 Outcome of the Meeting

Although there are many meetings devoted to general advances in coding theory, there have been no opportunities to date for mathematicians specifically interested in commutative algebraic methods applied to coding theory to get together and exchange ideas for collaboration purposes. We feel that our meeting has marked an important first step in this regard and we thank BIRS for its support.

We expect that our collaboration will give rise to two research articles [2, 3], one for each of the projects described in sections 4.1 and 4.2 of this report.

References

[1] S. Cooper, B. Harbourne, Z. Teitler, Combinatorial bounds on Hilbert functions of fat points in projective space, *J. Pure Appl. Algebra* **215** (2011), no. 9, 2165–2179.

[2] S. Cooper, A. Seceleanu, Ş. Tohăneanu, M. Vaz Pinto, R. Villarreal, Asymptotic properties of generalized minimum distance functions, *preprint*, **2018**.

[3] S. Cooper, A. Seceleanu, Ş. Tohăneanu, M. Vaz Pinto, R. Villarreal, Linear codes associated to graphs, *preprint*, **2018**.

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

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

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

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

[8] J. Neves, M. Vaz Pinto, and R. Villarreal, Vanishing ideals over graphs and even cycles, *Communications in Algebra*, Volume 43, Issue 3, 1050-1075 (2015).

[9] E. Sarmiento, M. Vaz Pinto and R. H. Villarreal, The minimum distance of parameterized codes on projective tori, *Appl. Algebra Engrg. Comm. Comput.* **22** (2011), no. 4, 249–264.

[10] Ş. Tohăneanu, On the de Boer-Pellikaan method for computing minimum distance, *J. Symbolic Comput.* **45** (2010), no. 10, 965–974.

[11] Ş. Tohăneanu, A. Van Tuyl, Bounding invariants of fat points using a coding theory construction, *J. Pure Appl. Algebra* **217** (2013) 269–279.

[12] V. K. Wei, Generalized Hamming weights for linear codes, *IEEE Trans. Inform. Theory* **37** (1991), no. 5, 1412–1418.