Coding theory: algebraic geometry of linear algebra

David R. Kohel

§1. Introduction.

Let \( R \) be a ring whose underlying set we call the alphabet. A linear code \( C \) over \( R \) is a free \( R \)-module \( V \) of rank \( k \), an embedding \( \iota : V \rightarrow U \) in a free module \( U \) of rank \( n \), and a choice of basis \( \mathcal{B} = \{ e_i \} \) for \( U \). The code is said to have block length \( n \) and dimension \( k \). We will also assume that the cokernel \( W \) of \( \iota \) is free over \( R \). We will be slightly sloppy and identify the image of \( V \) in \( U \) with the code \( C \). We define \( || \cdot || : U \rightarrow \mathbb{N} \) by

\[
||x|| = |\{ i : x_i \neq 0 \}|, \text{ where } x = \sum_i x_i e_i \in U.
\]

We call \( ||x|| \) the weight of \( x \), and define a distance function \( d(\cdot, \cdot) : U \times U \rightarrow \mathbb{N} \) by setting \( d(x, y) = ||x - y|| \). The minimum distance \( d \) of the code \( C \) is the minimum of \( d(x, y) \) for \( x \) and \( y \) in \( C \). By the linearity of \( C \), we have that \( d \) is the minimum weight of a nonzero codeword. We call a linear code \( C \) with parameters \( n, k \) and \( d \) a linear \([n, k, d]\)-code.

Consider the exact sequence of \( R \)-modules

\[
0 \rightarrow V \xrightarrow{\iota} U \xrightarrow{\pi} W \rightarrow 0
\]

By means of choices of bases for \( V \) and \( W \) we can represent \( \iota \) and \( \pi \) by matrices \( G \) and \( H \), the generator matrix and the parity check matrix, respectively.

The main problems of study in coding theory are:

1. Good encoding and decoding algorithms for families of codes.
2. Proving the existence, or nonexistence, of linear \([n, k, d]\)-codes over \( R \) of given parameters.
3. Construction of families of codes which are asymptotically “good” as \( n \) goes to infinity.
4. Computing the weight enumerator polynomials

\[
w(z) = w_C(z) = \sum_i A_i z^i = \sum_{x \in C} q^{||x||},
\]
for $C$ lying in a family of codes. (In some families of algebraic-geometric codes, the codewords of a given weight are points on an algebraic variety and can be effectively computed.)

§2. Equivalence of codes.

Let $C = (\iota: U \to V, \mathfrak{B})$ and $C' = (\iota': U' \to V', \mathfrak{B}')$ be codes. An isomorphism of codes is an isomorphism $\phi: U \to U'$ of $R$-modules which preserves weights and such that $\phi(\iota(V)) = \iota'(V')$. Note that $\varphi(\mathfrak{B})$ need not equal $\mathfrak{B}'$; the weight preserving condition only requires that the linear subspaces $\{R^* e_i\}$ are permuted. An automorphism of codes is an isomorphism of a code with itself. The automorphism group of $C$ is a subgroup of the semidirect product of the permutation group $S_n$ and $(R^*)^n$.

§3. Projective systems.

Let $M$ be a free $R$-module of dimension $k$ and let $S$ be a subset of $n$ points (which need not be distinct) such that $S$ lies in no hyperplane of $V$. We call the pair $(M, S)$ a linear system over $R$, and set

$n = |S|, \quad k = \text{rank}(M), \quad d = n - \max \limits_{H} |S \cap H| \geq 1,$

where $H$ runs over all hyperplanes of $M$. We define an isomorphism of linear systems $(M, S)$ and $(M', S')$ to be an $R$-module isomorphism $M \to M'$ taking $S$ onto $S'$.

**Theorem 0.1** The isomorphism classes of linear $[n, k, d]$-codes are in bijective correspondence with the isomorphism classes of $(M, S)$ with parameters $n, k$ and $d$.

Before proving the theorem, we define a projective system by letting

$\mathbb{P} = \mathbb{P}(M) = \left( M - \bigcup_{a \in R} aM \right) / R^*$,

and $\mathcal{P}$ be the image of $S$ in $\mathbb{P}$. We call $(\mathbb{P}, \mathcal{P})$ a projective system, and define

$n = |\mathcal{P}|, \quad k = \text{dim}(\mathbb{P}) + 1, \quad d = n - \max \limits_{H} |\mathcal{P} \cap H|.$

We say that a code is nondegenerate if $C$ is not contained in $U_i$ for any of the $n$ canonical hyperplanes $U_i$ of $U$ generated by $\{e_1, \ldots, \hat{e}_i, \ldots, e_n\} \subseteq \mathfrak{B}$. 2
Theorem 0.2 The set of isomorphism classes of nondegenerate $R$-linear $[n, k, d]$-codes are in bijective correspondence with projective systems over $R$ with parameters $n$, $k$, and $d$.

Proof of Theorem 0.1. Let $V = M^*$ and define $V \rightarrow U = R^n$ by

$$\varphi \mapsto (\varphi(P_1), \varphi(P_2), \ldots, \varphi(P_n)).$$

Conversely, given a code $(\iota : U \rightarrow V, \mathcal{B})$, the basis $\mathcal{B} = \{e_i\}$ determines a dual basis $\{e_i^*\}$ of $U^*$ which restricts to elements of $M = V^*$.

The second theorem follows easily. Note that the degeneracy of a code corresponding to $(M, S)$ is just the multiplicity of $(0, 0, \ldots, 0)$ in $S$.

Exercise. Set $||H|| = n - |H \cap P|$ and verify that $w(z) = 1 + (q - 1) \sum_H z^{||H||}$, where $q$ is the size of the alphabet.

Example. Let $R = F_4$ and let $E$ be the elliptic curve given by

$$Y^2Z + YZ^2 = X^3$$

in $\mathbb{P}^2$. Then

$$E(F_4) = \{(0 : 1 : 0), (0 : 0 : 1), (0 : 1, 1), (1 : \alpha : 1), (\alpha : \alpha : 1), (\alpha^2 : \alpha : 1), (\alpha : \alpha^2 : 1), (\alpha^2 : \alpha^2 : 1)\},$$

where $\alpha$ is a generator for $F_4^*$.

To turn this into a linear code, we make some ugly choices... We lift these points back to $M = F_4^3$ and set $U = F_4^9$. Then with the basis $\{x, y, z\}$ for $V = M^*$, we have $V \rightarrow U$ given by the generator matrix

$$G = \begin{bmatrix}
0 & 0 & 0 & 1 & 1 & \alpha & \alpha & \alpha^2 & \alpha^2 \\
1 & 0 & 1 & \alpha & \alpha^2 & \alpha & \alpha^2 & \alpha & \alpha^2 \\
0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1
\end{bmatrix}.$$

We now determine directly that the weight enumerator polynomial for $C$ is $1 + 4z^6 + 3z^8$. In particular, the minimum distance is 6. Thus we have constructed a linear $[9, 3, 6]$ code.

§4. Duals of codes.
The dual of a linear code $C$ is defined to be the linear subspace

$$C^\perp = \{ x \in U : x \cdot y = 0 \text{ for all } y \in C \}.$$  

The block length of the dual code is still $n$, and the dimension of the code is $n-k$. The MacWilliams identity relates the weight enumerator polynomials of $C$ and $C^\perp$. We have

$$w_{C^\perp}(z) = q^{-k} w_C \left( \frac{1 - z}{1 - (q - 1)z} \right)$$

The weight enumerator polynomial of $C^\perp$ in the example above is then

$$w_{C^\perp}(z) = 1 + 5z^3 + 11z^4 + 24z^5 + 8z^6 + 11z^7 + 4z^8,$$

and $C^\perp$ is a linear $[9,6,3]$-code.

Notice that in this example the sum $k + d$ is equal to $n$. For any linear code we have the following general bound.

**Theorem 0.3 (Singleton bound)** For any linear $[n,k,d]$-code $k + d \leq n + 1$.

**Proof.** Consider any $k - 1$ points in $\mathbb{P}(V) = \mathbb{P}^{k-1}$. Necessarily they lie in a hyperplane. Thus by definition of a projective system,

$$k - 1 \leq \max_H |P \cap H| = n - d.$$

§5. **Line bundles on X**

In order to prove the following theorem, we introduce line bundles on a variety $X$.

**Theorem 0.4** Let $X$ be a curve, let $T$ be a subset of $X(R)$ of cardinality $n$, and let $L$ be a line bundle on $X$ of degree $a$. Let $s_1, \ldots, s_k$ be a basis for the global sections of $L$, and assume that the induced morphism $\varphi : X \to \mathbb{P}^{k-1}$ is an embedding. Then the projective system $(\mathbb{P}^{k-1}(R), P)$, where $P = \varphi(T)$, determines a linear $[n,k,d]$-code with parameters

$$k \geq a - g + 1 \quad \text{and} \quad d \geq n - a.$$  

In particular, $k + d \geq n + 1 - g$.  

4
**Note 1.** Our elliptic curve example was such an example with $a = 3$, $g = 1$, and $P = E(\mathbb{F}_4)$ of cardinality 9.

**Note 2.** A line bundle $\mathcal{L}$ satisfying the conditions of the theorem is said to be very ample.

Let $\mathcal{O}_X$ be the sheaf of functions on $X$, i.e. for each open subset $U$ of $X$, $\mathcal{O}_X(U)$ is the ring of rational polynomial maps $U \to R$.

A sheaf $\mathcal{F}$ of $\mathcal{O}_X$-modules is defined to be a sheaf on $X$ such that for each open subset $U$ of $X$, the group $\mathcal{L}(U)$ is an $\mathcal{O}_X(U)$ module, and for each inclusion of open sets $V \to U$ the homomorphism $\mathcal{L}(U) \to \mathcal{L}(V)$ is compatible with the ring homomorphism $\mathcal{O}_X(U) \to \mathcal{O}_X(V)$, i.e. $\mathcal{L}(U) \to \mathcal{L}(V)$ becomes a homomorphism of $\mathcal{O}_X(U)$-modules.

A line bundle $\mathcal{L}$ (or invertible sheaf) is defined to be a sheaf of $\mathcal{O}_X$-modules on $X$ such that there exists a covering of $X$ by open sets $U$ such that $\mathcal{L}|_U$ is isomorphic to $\mathcal{O}_X|_U$.

In short, a line bundle is defined by the conditions that

1. For each open set $U$ in a covering of $X$, $\mathcal{L}(U)$ is isomorphic to an $\mathcal{O}_X(U)$-module.
2. The inclusions $\mathcal{L}(U \cap V) \subseteq \mathcal{L}(U)$ and $\mathcal{L}(U \cap V) \subseteq \mathcal{L}(V)$ determine how the modules glue together.

**Sketch of proof.** The theorem is proved with the following steps.

1. The dimension $k$ of $\mathcal{L}(X)$ over $R$ is at least $a - g + 1$ by the Riemann-Roch theorem.
2. The global sections $s_1,\ldots,s_k$ of $\mathcal{L}(X)$ determine an embedding as follows. For each set $U$ in a cover of $X$, fix an isomorphism $\mathcal{L}(U) \cong \mathcal{O}_X(U)$. Then we can define

   $$X \xrightarrow{\varphi} \mathbb{P}^{k-1}.$$  
   $$P \longmapsto (s_1(P) : \cdots : s_k(P)).$$

   Since changing the isomorphism is equivalent to multiplying each $s_i$ by a unit in $\mathcal{O}_X(U)$, this gives a well-defined map to $\mathbb{P}^{k-1}$.
3. Apply the equivalence of projective systems and codes. The minimum distance of the code is defined to be

   $$d = n - \max_H |T \cap H|.$$
Over an algebraically closed field $R$, by Bezout’s theorem the cardinality of $\varphi(X(R)) \cap H$, counted with multiplicity, is equal to $a$ for any hyperplane $H$. Over general $R$ we may get lucky and $a$ may be smaller, but we have a lower bound $d \geq n - a$. 