mathematics

MDPI

Article

A Topological View of Reed–Solomon Codes

Alberto Besana and Cristina Martínez *

Department of Physics and Mathematics, University of Alcalá, 28871 Madrid, Spain; albertobesana@gmail.com
* Correspondence: Cristina.martinezram@uah.es

Abstract: We studied a particular class of well known error-correcting codes known as Reed–Solomon codes. We constructed RS codes as algebraic-geometric codes from the normal rational curve. This approach allowed us to study some algebraic representations of RS codes through the study of the general linear group $GL(n,q)$. We characterized the coefficients that appear in the decompostion of an irreducible representation of the special linear group in terms of Gromov–Witten invariants of the Hilbert scheme of points in the plane. In addition, we classified all the algebraic codes defined over the normal rational curve, thereby providing an algorithm to compute a set of generators of the ideal associated with any algebraic code constructed on the rational normal curve (NRC) over an extension $\mathbb{F}_{q^n}$ of $\mathbb{F}_q$.

Keywords: 2000 mathematics subject classification; 05E10 (primary); 05A15 (secondary); algebraic code; symmetric group; partitions

Citation: Besana, A.; Martínez, C. A Topological View of Reed–Solomon Codes. *Mathematics* **2021**, *9*, 578. https://doi.org/10.3390/math9050578

Academic Editor: Askar Tuganbaev

Received: 28 January 2021
Accepted: 28 February 2021
Published: 9 March 2021

1. Introduction

Let us denote by $\mathbb{F}_q$ the finite field of q elements with q a power of prime number p. One can consider field extensions $\mathbb{F}_q$ of $\mathbb{F}_p$ as q varies through powers of the prime p. Any $\mathbb{F}_{p^n}$ field extension of $\mathbb{F}_p$ is a vector space over $\mathbb{F}_p$ of dimension n and an $(n-1)-$dimensional projective space $PG(n-1,p)$.

Let V be an $n+1$ dimensional vector space over the field $\mathbb{F}_q$; we denote by $PG(n,q)$ or $\mathbb{P}(V)$ the n-dimensional projective space over V and by $\mathbb{P}^1$, the projective line. The set of all subspaces of dimension r in V is a Grassmannian, and it is denoted by $\mathcal{G}_{r,n}(\mathbb{F}_q)$ or by $PG^r(n,q)$. The dual of an $r-$space in $PG(n,q)$ is an $(n-r-1)-$space.

Consider the $\mathbb{F}_q-$rational points of $\mathcal{G}_{r,n}(\mathbb{F}_q)$ as a projective system; we obtain a q-ary linear code, called the Grassmann code, which we denote $[n,r]_q$ code. The length l and the dimension k of $G(r,n)$ are given by the q binomial coefficient $l = \begin{bmatrix} n \\ r \end{bmatrix}_q = \frac{(q^{n+1}-1)(q^{n+1}-q)\ldots(q^{n+1}-q^r)}{(q^{r+1}-1)(q^{r+1}-q)\ldots(q^{r+1}-q^r)}$, and $k = \binom{n}{r}$, respectively.

We study the relation between codes constructed from vector bundles and the representation theory of the general linear group $GL(n,\mathbb{F}_q)$. Following [1], we consider the right action of the general linear group $GL(n,\mathbb{F}_q)$ on $\mathcal{G}_{k,n}(\mathbb{F}_q)$:

$$\begin{array}{rcl} \mathcal{G}_{k,n}(\mathbb{F}_q) \times GL(n,\mathbb{F}_q) & \to & \mathcal{G}_{k,n}(\mathbb{F}_q) \\ (\mathcal{U}, A) & \to & \mathcal{U}A. \end{array} \tag{1}$$

Observe that the action is defined independently of the choice of the representation matrix $\mathcal{U} \in \mathbb{F}_q^{k\times n}$.

Let $\mathcal{U} \in \mathcal{G}_{k,n}(\mathbb{F}_q)$ and $G < GL(n,\mathbb{F}_q)$ be a subgroup; then $C = \{\mathcal{U}A |\ A \in G\}$ is an orbit in $\mathcal{G}_{k,n}(\mathbb{F}_q)$ of the induced action.

In order to classify all the orbits, we need to classify all the conjugacy classes of subgroups of $GL(n,\mathbb{F}_q)$. In [2], we studied cyclic coverings of the projective line that correspond to orbits defined by a cyclic subgroup of order p as the multiplicative group of

p^{th} roots of unity or the additive group of integers modulo p for some prime number p. In particular, we showed that any irreducible cyclic plane cover of the projective line can be given by a prime ideal

$$(y^m - (x-a_1)^{d_1} \dots (x-a_n)^{d_n}) \subset \mathbb{F}_q[x,y].$$

This ideal defines an affine curve in $\mathbb{A}^2(\mathbb{F}_q)$ which has singularities, if $d_k > 1$ for some $1 \leq k \leq n$. There exists a unique projective curve birationally equivalent to this affine curve obtained by homogenization of the polynomial. Here we study the connection between ideal sheaves on $\mathbb{F}_q[x,y]$ and its numerical invariants together with the combinatorics of partitions of n and the representation theory of the general linear group $GL(\mathbb{F}_q, n)$. In other words, we want to understand which subspaces are invariant by the action of elements of the general linear group or finite subgroups of $GL(n, \mathbb{F}_q)$ and how the $GL(n, \mathbb{F}_q)$ group's action on the Grassmannian changes the Grassmann code, as this action simply permutes basis elements of the Grassmann code.

When one considers as an alphabet a set $\mathcal{P} = \{P_1, \dots, P_N\}$ of $\mathbb{F}_q-$rational points lying on a smooth projective curve defined over a finite field, algebraic codes are constructed by evaluation of the global sections of a line bundle or a vector bundle on the curve. Any cyclic cover of $\mathbb{P}^1$ which is simply ramified corresponds to an unordered tuple of n points on $\mathbb{P}^1$. More generally, in Section 4 we consider configurations of n points in a $d-$dimensional projective space $PG(d,q)$ which generically lies on a rational normal curve (NRC) and we study the algebraic codes defined on it, providing a complete classification in terms of divisors defined over the NRC; see Theorem 2. These are the so called Reed–Solomon codes. Moreover, in the last section as an application of the Horn problem, we provide a set of generators of the ideal associated with any algebraic code constructed on the NRC over an extension $\mathbb{F}_q^n$ of $\mathbb{F}_q$.

From now on, $\mathbb{F}_q$ will be a field with $q = p^n$ elements and $\mathcal{C}$ a non-singular, projective, irreducible curve defined over $\mathbb{F}_q$ with q elements.

Notation

For d a positive integer, $\alpha = (\alpha_1, \dots, \alpha_m)$ is a partition of d into m parts if the α_i are positive and decreasing integers summing to n. We will denote as $\mathcal{P}(d)$ the set of all partitions of d. We set $l(\alpha) = m$ for the length of α, that is, the number of cycles in α, and l_i for the length of α_i. The notation $(a_1, \dots, a_k)$ stands for a permutation in S_d that sends a_i to a_{i+1}. For $\lambda \in \mathcal{P}(d)$, we write $[\lambda]$ for the corresponding character of S_n. We write $PGL(2,k) = GL(2,k)/k^*$, where k is field of arbitrary characteristic and elements of $PGL(2,k)$, which will be represented by equivalence classes of matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, with $ad - bc \neq 0$. A $q-$ary constant weight code of length n, distance d and weight w will be denoted as an $[n,d,w]_q$ code.

2. Horn Problem: An Application to Convolutional Codes

In this section we present a description of the Horn problem, i.e., the study of the eigenvalues of the sum $C = A + B$ of two matrices, given the spectrum of A and B, in the context of polynomial matrices with polynomial entries associated with torsion modules or dually submodules of a polynomial ring with coefficients in a field. Next, we introduce some important matrices that define a linear error-correcting code.

Let R be any complete valued field R with a closed coefficient field k of an arbitrary characteristic, for example, a finite field or the ring $R = \mathbb{C}\{x\}$ of convergent power series. If $f \in R$ is a nonzero divisor, then we define the encoder A as the matrix associated with the corresponding torsion module R/fR. The matrix A can be diagonalized by elementary row and column operations with diagonal entries $x^{\alpha_1}, x^{\alpha_2}, \dots, x^{\alpha_n}$, for unique non-negative integers $\alpha_1 \geq \dots \geq \alpha_n$. More precisely, these matrices are in correspondence

with endomorphisms of R^n, with cokernels being torsion modules with at most n generators. Such a module is isomorphic to a direct sum

$$R/x^{\alpha_1}R \oplus R/x^{\alpha_2}R \oplus \ldots \oplus R/x^{\alpha_n}R, \;\; \alpha_1 \geq \ldots \geq \alpha_n.$$

The set $(\alpha_1, \ldots, \alpha_n)$ of invariant factors of A defines a partition α of size $d = |\lambda|$. Reciprocally, when $R = \mathbb{C}\{x\}$ is the ring of convergent power series, any partition λ defines a rank one torsion-free sheaf on $\mathbb{C}$ by setting $\mathcal{I}_\lambda = (x^{\lambda_1}, x^{\lambda_2}, x^{\lambda_3}, \ldots, x^{\lambda_n})$. In particular, the ideal sheaf corresponding to the identity partition $(1)^n$, defines a maximal ideal $\mathcal{I}_{(1)^n} = (x, \overbrace{\ldots}^{n \text{ times}}, x)$ in $\mathbb{C}[x]$. The Horn problem is then equivalent to the following question: which partitions α, β, γ can be the invariant factors of matrices A, B and C if $C = A \cdot B$?

In the case of convergent power series, this problem was proposed by I. Gohberg and M.A. Kaashoek. By denoting the cokernels of A, B and C as $\mathcal{A}, \mathcal{B}$ and $\mathcal{C}$, respectively, one has a short exact sequence:

$$0 \to \mathcal{A} \to \mathcal{B} \to \mathcal{C} \to 0,$$

i.e., $\mathcal{B}$ is a submodule of $\mathcal{C}$ with $\mathcal{C}/\mathcal{B} \cong \mathcal{A}$; such an exact sequence corresponds to matrices A, B and C with $A \cdot B = C$.

If we specialize C to be the identity matrix I, by the correspondence between partitions and ideal sheaves above, the invariant factors of the identity matrix are defined by the partition $(1)^n$, then the question becomes: which partitions α, β can be the invariant factors of matrices A, B if $A \cdot B = I$? The case of interest for us will be the case in which R is an $\mathbb{F}_q[x]$-module with q a prime power of p.

Duly, the code can be defined as an $R-$submodule of R^n, where $R = \mathbb{F}[z]$ is a polynomial ring with coefficients in a field $\mathbb{F}$ and z is a uniformizing parameter in R (see [3]). When $\mathbb{F}$ is a finite field, these are known as convolutional codes which have been very well studied; see, for example, [4]. A full row rank matrix $G(z) \in \mathbb{F}[z]^{k \times n}$ with the property that

$$\mathcal{C} = \mathrm{Im}_{\mathbb{F}[z]} G(z) = \{f(z)g(z) : \, f(z) \in [\mathbb{F}^k(z)]\}$$

is called a generator matrix. The degree d of a convolutional code $\mathcal{C}$ is the maximum of the degrees of the determinants of the $k \times k$ submatrices of one, and hence any generator matrix of $\mathcal{C}$. The main difference between block and convolutional codes is that at the encoder, in a convolutional code we may have different states. Linear block codes may be considered as a particular case of convolutional codes with only one state. In next section we describe an example of block codes known as Reed–Solomon codes.

Remark 1. *The set of convolutional codes of a fixed degree is parametrized by the Grothendieck Quot scheme of degree d, rank $n-k$ coherent sheaf quotients of $\mathcal{O}^n$ on a curve X defined over $\mathbb{F}$. If the degree is zero, these schemes describe a Grassmann variety and constitute the so called class of block codes of parameters (n, k). Namely, the space of all matrix divisors $\mathcal{D}_k(r, d)$ of rank r and degree d can be identified with the set of rational points of $\mathrm{Quot}^m_{\mathcal{O}_X(D)^n/X/k}$ parametrizing torsion quotients of $\mathcal{O}_X(D)^n$ and having degree $m = r \cdot \deg\, D - d$, see [5].*

An Example with Algebraic-Geometric Codes: Reed–Solomon Codes

Let X be a smooth projective curve defined over a finite field $\mathbb{F}_q$ with q elements. The classical algebraic-geometric (AG) code due to Goppa is defined by evaluating rational functions associated with a divisor D at a finite set of $\mathbb{F}_q$-rational points. From another point of view, we are considering the evaluation of sections of the corresponding line bundle $\mathcal{O}_X(D)$ on X. Namely, let $\mathcal{P} := \{P_1, \ldots, P_n\}$ be a configuration of distinct $\mathbb{F}_q$-

rational points of X, the usual algebraic-geometric code is defined to be the image of the evaluation map:

$$\begin{aligned} \varphi_D : L(D) &\to \mathbb{F}_q^n \\ f &\mapsto (f(P_1), \ldots, f(P_n)), \end{aligned} \tag{2}$$

where $L(D)$ denotes the vector space of sections associated with the line bundle $\mathcal{O}_X$. The parameters of these codes, the length n, the dimension k and the minimum distance d are determined by the theorem of Riemann-Roch and it is easy to see that they satisfy the following bound $k + d \geq n + 1 - g$, where g is the genus of the curve X. Using this definition, the notion of AG codes is easily generalized for varieties of higher dimension.

Namely, let E be a vector bundle of rank r on X defined over $\mathbb{F}_q$. The Goppa code $C(X, D, G)$ takes as input a divisor D supported on the finite set $\mathcal{P}$ of $\mathbb{F}_q$-rational points and a divisor G associated with the vector bundle E and evaluates each section $\sigma \in \mathcal{L}(G)$ in the linear series attached to the divisor G:

$$C(X, D, G) = \{(\sigma(P_i))_{i=1}^n : \sigma \in \mathcal{L}(G)\} \subseteq \mathbb{F}_q^n.$$

Observe that $C(X, \mathcal{P}, E)$ is an $\mathbb{F}_q$-linear subspace of $\mathbb{F}_{q^r}^n$ and thus a point of the Grassmannian $\mathcal{G}_{r,n}(\mathbb{F}_q)$. Moreover, for the same subset of evaluation points and any $r \leq k$, we have $G(r, n) \subseteq G(k, n) \subseteq \mathbb{F}_q^n$, where $r \leq k$. Further, we get a partial flag of $\mathbb{F}_q-$vector spaces $\{0\} = E^k \subset E^{k-1} \subset \ldots \subset E^1 \subset E^0 = \mathbb{F}_q^n$ such that $\dim (\mathrm{E}^{\mathrm{i}-1}/\mathrm{E}^{\mathrm{i}}) = \lambda_i$, to which we associate the partition $\lambda = (\lambda_1, \ldots, \lambda_r)$ of n. In this way, each partition λ of n determines a variety $\mathcal{F}_\lambda = \mathcal{F}_\lambda(\mathbb{F}_q)$ of partial flags of $\mathbb{F}_q$-vector spaces.

The representation theory of the special linear group $SL(n, \mathbb{F}_q)$ can be viewed as a form of Gale duality first proven by Goppa in the context of algebraic coding theory.

Let D and G be effective divisors supported over a smooth projective curve X defined over $\mathbb{F}_q$ such that $\mathrm{Supp(G)} \cap \mathrm{Supp(D)} = \emptyset$, then the geometric Goppa code associated with the divisors D and G is defined by

$$\mathcal{C}(D, G) = \{(x(P_1), \ldots, x(P_n)), x \in \mathcal{L}(G)\} \subseteq \mathbb{F}_q^n,$$

where $\mathcal{L}(G)$ denotes the linear system associated with the divisor G.

Definition 1. *Let C_1 and C_2 be the corresponding codes obtained by evaluating non-constant rational functions $f(x)$ and $g(x)$ with non common roots on X over the support of the divisor D. We define the quotient code of C_1 and C_2 to be the code associated with the quotient rational function $\varphi = f/g$.*

Since f and g take the value ∞, they are defined by non constant polynomials $f(x)$ and $g(x)$ in $\overline{\mathbb{F}_q}[x]$. Here $\overline{\mathbb{F}_q}$ denotes the algebraic closure of $\mathbb{F}_q$. The degree of φ is defined to be $\deg(\varphi) = \max\{\mathrm{deg(f)}, \mathrm{deg(g)}\}$.

As φ is a finite morphism, one may associate to each rational point $x \in X(\mathbb{F}_q)$ a local degree or multiplicity $m_\varphi(x)$ defined as:

$$m_\varphi(x) = ord_{z=0}\psi(z),$$

where $\psi = \sigma_2 \circ \varphi \circ \sigma_1$, $y = \varphi(x)$, and $\sigma_1, \sigma_2 \in PGL(2, \mathbb{F}_q)$ such that $\sigma_1(0) = x$ and $\sigma_2(y) = 0$.

With each non-constant rational function φ over X, one can associate a matrix A with entries in the ring $\mathbb{F}_q[x]$. Namely, let us call $f_0 := f(x)$ and call f_1 the divisor polynomial $g(x)$, and f_2 the remainder polynomial; then by repeated use of the Euclid's algorithm, we construct a sequence of polynomials $f_0, f_1, \ldots, f_k$, and quotients $q_1, \ldots q_k$, $K \leq n$. Then the quotient matrix A is defined to be the diagonal matrix with entries $q_1, \ldots, q_k$ corresponding to the continued fraction expansion of the rational function φ.

Here we include a SAGE code [6] which implements the algorithm.

```
def euclid(f, g):
r = f % g
q = f // g
while r.degree() >= 0:
yield q
f = g
g = r
r = f % g
q = f // g
```

Let λ_i be the partition of the integer k, defining the degree multiplicities of the polynomial q_i. Then the Horn problem applied to this situation reads:

Which partitions α, β and γ can be the degree multiplicities of polynomials q_A, q_B and q_C such that the corresponding diagonal matrices A, B, and C satisfy $C = A \cdot B$?

Another important family of Goppa codes is obtained considering the normal rational curve $\mathcal{C}^n$ defined over $\mathbf{F}_q$:

$$\mathcal{C}^n := \{\mathbb{F}_q(1, \alpha, \ldots, \alpha^n) : \alpha \in \mathbb{F}_q \cup \{\infty\}\}.$$

The points are distinct elements of $\mathbf{F}_q$ and L is the vector space of polynomials of degree at most $k-1$ and with coefficients in $\mathbf{F}_q$. Such polynomials have at most $k-1$ zeros, so nonzero codewords have at least $n-k+1$ non-zeros. Hence, this is a $[n, k, n-k+1]_q$ code whenever $k \leq n$. Any codeword $(c_0, c_1, \ldots, c_{n-1})$ can be expressed into a q-ary k-vector with respect to the basis $\{1, \alpha, \ldots, \alpha^{k-1}\}$.These codes are just generalized Reed–Solomon codes of parameters $[n, k, d]_q$ over $\mathbf{F}_q$ with parity check polynomial $h(x) = \prod_{i=1}^{k-1}(x - \alpha^i)$ where α is a primitive root of $\mathbf{F}_q$ such that $\alpha^k = \alpha + 1$. In other words, the GRS code is an ideal in the ring $\mathbf{F}_q[x]/(x^k - x - 1)$ generated by a polynomial $g(x)$ with roots in the splitting field $\mathbf{F}_q^l$ of $x^k - x - 1$, where $k|q^l - 1$. Since the NRC is a genus 0 curve, it is easy to see that these codes satisfy the Singleton bound $d \geq n - k + 1$.

Construction of Reed–Solomon codes over $\mathbb{F}_q$ only employs elements of $\mathbb{F}_q$, hence their lengths are at most q. In order to get longer codes, one can make use of elements of an extension of $\mathbb{F}_q$, for instance considering subfield subcodes of Reed–Solomon codes.

As in [2], where we considered a variant of the Horn problem in the context of cyclic coverings of the projective line defined over an arbitrary field k, the problem is reduced to study the representation theory of the general linear group $GL(n, \mathbb{F}_q)$.

3. Representation Theory of $GL(n, \mathbb{F}_q)$

We focus on Grassman codes $\mathcal{G}_{k,n}(\mathbb{F}_q)$ that were described in the introduction as $[n, k]_q-$codes by considering an action (1) of the general linear group $GL(n, q)$ on the Grassmannian. The study of the representation theory of $GL(n, q)$ will allow us to understand better the orbits of this action that will be characterized in Section 5.

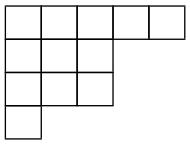
The multiplication in the finite field $\mathbb{F}_{q^n}$ is a bilinear map from $\mathbb{F}_{q^n} \times \mathbb{F}_{q^n}$ into $\mathbb{F}_{q^n}$. Thus it corresponds to a linear map from the tensor product $m : \mathbb{F}_{q^n} \otimes \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$. The symmetric group S_n acts on $\mathbb{F}_{q^n}$ via the permutation matrix:

$$\sigma \cdot v_i = v_{\sigma(i)}, \quad v_i \in \mathbb{F}_{q^n}. \tag{3}$$

The d-Veronese embedding of $\mathbb{P}^n(\mathbb{F}_q)$ maps the line spanned by the vector $v \in \mathbb{F}_{q^n}$ to the line spanned by $v^{\otimes d} = v \otimes \ldots \otimes v$. Thus the symmetric group S_n acts diagonally on the basis of simple tensors of $\mathbb{F}_{q^n}$.

$$\sigma \cdot (v_{i_1} \otimes \ldots \otimes v_{i_r}) = v_{\sigma(i_1)} \otimes \ldots \otimes v_{\sigma(i_r)}. \tag{4}$$

For each partition $\lambda = (\lambda_1, \ldots, \lambda_k)$ we consider its Young diagram. The diagram of λ is an array of boxes, lined up at the left, with λ_i boxes in the i^{th} row, with rows arranged from top to botton. For example,



is the Young diagram of the partition $\lambda = (5,3,3,1)$ with $l(\lambda) = 4$ and $|\lambda| = 12$. We define the Schur projection:

$$c_\lambda : \bigotimes^d \mathbb{F}_{q^n} \to \bigotimes^d \mathbb{F}_{q^n}.$$

Let S_n be the symmetric group of permutations over d elements. Any permutation $\sigma \in S_n$ acts on a given Young diagram by permuting the boxes. Let $R_\lambda \subseteq S_n$ be the subgroup of permutations preserving each row. Let $C_\lambda \subseteq S_n$ be the subgroup of permutations preserving each column, let $c_\lambda = \sum_{\sigma \in R_\lambda} \sum_{\tau \in C_\lambda} \epsilon(\tau)\sigma\tau$.

The image of c_λ is an irreducible $GL(n, \mathbb{F}_q)$-module, which is nonzero iff the number of rows is less or equal than $\dim V_\lambda$. All irreducible $GL(n, \mathbb{F}_q)$-modules can be obtained in this way. Every $GL(n, \mathbb{F}_q)-$module is a sum of irreducible ones.

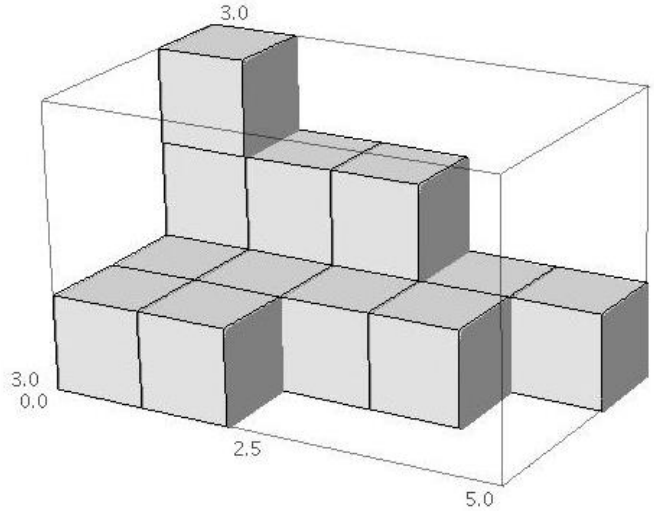
In terms of irreducible representations of $GL(n, \mathbb{F}_q)$, a partition η corresponds to a finite irreducible representation that we denote as $V(\eta)$. Since $GL(n, \mathbb{F}_q)$ is reductive, any finite dimensional representation decomposes into a direct sum of irreducible representations, and the structure constant $c^\eta_{\lambda,\mu}$ is the number of times that a given irreducible representation $V(\eta)$ appears in an irreducible decomposition of the tensor product of the representations $V(\lambda) \otimes V(\mu)$. These are known as Littlewood–Richardson coefficients, since they were the first to give a combinatorial formula encoding these numbers (see [7]). In terms of the Hopf algebra Λ of Schur functions, let s_λ be the Schur function indexed by the partition λ, we have $s_\lambda \cdot s_\mu = \sum_\nu k^\nu_{\lambda\mu} s_\nu$ for the product and we get the coefficients $k^\eta_{\lambda\mu}$ as the structure constants of the dual Hopf algebra Λ^*. These are known as Kronecker coefficients (see [8,9]) since they appear as expansion coefficients in the Kronecker product $[\lambda][\mu] = \sum_\nu k_{\lambda\mu}[\nu]$ of characters of the symmetric group S_n, as the authors proved in Proposition 4.3 of [2]. Recall that the Schur function s_λ attached to the partition $\lambda = (\lambda_1, \ldots, \lambda_n)$ of length less or equal than n is defined by the quotient:

$$s_\lambda(x_1, \ldots, x_n) = \frac{det(x_i^{\lambda_i + n - j})_{1 \le i,j, \le n}}{det(x_i^{n-j})_{1 \le i,j \le 0}}.$$

It is a homogeneous polynomial of degree $|\lambda|$ in $x_1, \ldots, x_n$. It easily seen that $s_\lambda(x_1, \ldots, x_n, 0) = s_\lambda(x_1, \ldots, x_n)$. Moreover we can define the Schur function s_λ as the unique symmetric function with this property for all $n \ge l(\lambda)$. It is well known that the Schur functions constitute a basis for the ring Λ of symmetric functions. In addition, there are at least other three well known bases for the ring Λ of symmetric functions. The basis e_k of k-elementary symmetric functions, the h_k complete homogeneous symmetric functions of degree k and the power sums $p_k = z_1^k + z_2^k + \ldots$. This has been applied in Reed–Solomon coding, that is, for AG codes defined on the projective line $\mathbb{P}^1$, as a way to encode information words. Namely, for each codeword $a = (a_0, a_1, \ldots, a_n)$, $a_i \in \mathbb{F}_q$, let us define $a_{n+1} = \sum_{i=1}^n a_i \in \mathbb{F}_q$ which is nothing but the first elementary symmetric function e_1. If we consider the variables $x_1, \ldots, x_r$ as a fixed list of nonzero elements in $\mathbb{F}_q$, then the information word a can be encoded into the codeword $d = (d_1, \ldots, d_r)$, where $d_i = \sum_{j=1}^n a_j x_i^j$. The secret is $a_0 = -\sum_{i=1}^r d_i$, while the pieces of the secret are the d_is.

3.1. Relation between Littlewood–Richardson Coefficients and Kronecker Coefficients

One can stack Littlewood–Richardson coefficients $c^{\nu}_{\lambda\mu}$ in a 3D matrix or 3-dimensional matrix. Intuitively a 3D matrix is a stacking of boxes in the corner of a room. The elements of the principal diagonal are called rectangular coefficients and are indexed by triples $(\lambda, \mu, \nu) = ((i^n), (i^n), (i^n))$ of partitions (i^n) with all their parts equal to the same integer $1 \leq i \leq n$.



Consider $\mathcal{B}$ and $\mathcal{C}$, two 3D matrices, then we define the product matrix $\mathcal{B} \cdot \mathcal{C}$ as the 3D matrix

$$\mathcal{B} \cdot \mathcal{C} = \prod_{\nu \in \mathcal{P}(n), B^{\nu}, C^{\nu} \in M_{p(n)\times p(n)}(\mathbb{Q})} B^{\nu} \cdot C^{\nu}.$$

Namely, for each index ν fixed, λ and μ run over all partitions $\mathcal{P}(n)$ of n. Thus the coefficients $\left(c^{\nu}_{\lambda,\mu}\right)_{\lambda,\mu\in\mathcal{P}(n)}$ are encoded in a matrix of order $p(n) \times p(n)$, where $p(n)$ denotes the number of unrestricted partitions of n, that is, the number of ways of writing the integer n as a sum of positive integers without regard to order. Thus the product matrix $B^{\nu} \cdot C^{\nu}$ is the standard product of square matrices in $M_{p(n)\times p(n)}(\mathbb{Q})$. In particular, the property of associativity follows easily from the associativity in the vector space $M_{p(n)\times p(n)}(\mathbb{Q})$.

Proposition 1. *Let $\mathcal{C}$ be the 3D matrix whose entries are the Littlewood–Richardson coefficients, and $\mathcal{K}$ the 3D matrix of Kronecker coefficients. Then the matrices are inverse one to each other.*

Proof. Since $c^{\nu}_{\lambda\mu}$ and $k^{\nu}_{\lambda\mu}$ correspond to the structure constants of the Hopf algebra of Schur functions and its dual one respectively (see Proposition 4.3 of [2]), and the Hopf algebra of Schur functions is self-dual (see [9]), one gets that the product matrix $\mathcal{C} \cdot \mathcal{K}$ is the identity 3D matrix $\mathcal{I}$, that is, the matrix whose rectangular coefficients are identically 1. Thus both matrices are inverse one to each other. □

3.2. The Polytope of Triples (λ, μ, η) for Which $c^{\eta}_{\lambda,\mu}$ Is Positive

The convex hull in $\mathbb{R}^3$ of all triples (λ, μ, ν) with $c^{\nu}_{\lambda,\mu} > 0$ is the Newton polytope of $f(x, y, z) = \sum_{\lambda,\mu,\nu} c^{\nu}_{\lambda,\mu} x^{\lambda} y^{\mu} z^{\nu} \in \mathbb{C}[x, y, z]$. Here x^{λ} denotes the monomial $x^{\lambda_1} \cdots x^{\lambda_n}$ of partition degree λ. In particular, when $\lambda = (1^r)$, we have $x^{(1)^r} = e_r = \sum_{i_1<\ldots<i_r} x_{i_1} \ldots x_{i_r}$, the $r-$th elementary symmetric function. At the other extreme, when $\lambda = (r)$ we have $x^{(r)} = p_r = \sum x_i^r$, the $r-$power sum. As we have seen in the previous section, it is clear that every symmetric function $f \in \Lambda$ is uniquely expressible as a finite linear combination of the $(x^{\lambda})_{\lambda\in\mathcal{P}}$. Moreover, the following theorem shows that f is the the generating series

for the Gromov–Witten invariant $N_{d,g}(\lambda,\mu,\nu)$ counting irreducible plane curves of given degree and genus g passing through a generic configuration of $3d-1+g$ points on $\mathbb{P}^2(\mathbb{C})$ with ramification type at $0,\infty$ and 1 described by the partitions λ,μ and ν and simple ramification over other specified points with $|\lambda|+|\mu|+|\nu| = d$, and these have been computed by Fomin and Mikhalkin in [10].

Theorem 1. *The power series $f(x,y,z) = \sum_{\lambda,\mu,\nu} c^{\nu}_{\lambda,\mu} x^{\lambda} y^{\mu} z^{\nu} \in \mathbb{C}[x,y,z]$, is the generating series for the Gromov–Witten invariants $N_{d,g}(\lambda,\mu,\nu)$, counting irreducible plane curves of given degree d and genus g passing through a generic configuration of $3d-1+g$ points on $\mathbb{P}^2(\mathbb{C})$ with ramification type at $0,\infty$ and 1 described by the partitions λ,μ and ν and simple ramification over other specified points with $|\lambda|+|\mu|+|\nu| = d$.*

Proof. Whenever the coefficient $c^{\nu}_{\lambda,\mu} > 0$ is positive consider the corresponding ideal sheaves $\mathcal{I}_{\lambda}$, $\mathcal{I}_{\mu}$ and $\mathcal{I}_{\nu}$ in $\mathbb{C}[x,y,z]$ associated with the partitions λ,μ and ν respectively. Each ideal sheaf determines a curve in $\mathbb{C}[x,y]$ via homogenization of the corresponding monomial ideals. Thus each coefficient represents the number of ideal sheaves on $\mathbb{C}^3$ of colength n and degree d equal to the size of the partition, that is the corresponding 3-point Gromov–Witten invariant $\langle\lambda,\mu,\nu\rangle_{0,3,d}$ of the Hilbert scheme Hilb_n of $n = 2d-1+|\nu|+|\mu|+|\lambda|+g$ distinct points in the plane, or the relative Gromov–Witten invariant $N_{d,g}(\lambda,\mu,\nu)$ counting irreducible plane curves of given degree d and genus g passing through a generic configuration of $3d-1+g$ points on $\mathbb{P}^2(\mathbb{C})$ with ramification type at $0,\infty$ and 1 respectively, described by the partitions λ,μ and ν of n (see section 4 of [2]). □

Remark 2. *The Euler characteristic of each ideal sheaf is fixed and coincides with the Euler characteristic χ of the polyhedra described in $\mathbb{R}^3$ by the convex hull of all triples (λ,μ,ν) with $c^{\nu}_{\lambda,\mu} > 0$, that is, the Newton polytope of $f(x,y,z) = \sum_{\lambda,\mu,\nu} c^{\nu}_{\lambda,\mu} x^{\lambda} y^{\mu} z^{\nu} \in \mathbb{R}[x,y,z]$. Thus each coefficient represents the number of ideal sheaves on $\mathbb{C}^3$ of fixed Euler characteristic $\chi = n$ and degree d equal to the size of the partition, that is the corresponding Donaldson-Thomas invariant of the blow-up of the plane $\mathbb{P}^1 \times (\mathbb{C}^2)$ with discrete invariants $\chi = n$ and degree d.*

Remark 3. *The Hilbert scheme Hilb_n of n points in the plane $\mathbb{C}^2$ parametrizing ideals $\mathcal{J} \subset \mathbb{C}[x,y]$ of colength n contains an open dense set in the Zariski topology parametrizing ideals associated with configurations of n distinct points. Moreover there is an isomorphism $\mathrm{Hilb}_n \cong (\mathbb{C}^2)^n/S_n$. In particular, as we showed in [2], any conjugacy class in the symmetric group S_n determines a divisor class in the $T-$equivariant cohomology $H^{4n}_T(\mathrm{Hilb}_n,\mathbb{Q})$, for the standard action of the torus $T = (\mathbb{C}^*)^2$ on $\mathbb{C}^2$. The $T-$equivariant cohomology of Hilb_n has a canonical Nakajima basis indexed by $\mathcal{P}(n)$. The map $\lambda \to \mathcal{J}_{\lambda}$ is a bijection between the set of partitions $\mathcal{P}(n)$ and the set of $T-$fixed points $\mathrm{Hilb}^T_n \subset \mathrm{Hilb}_n$.*

Denote the series $\langle\lambda,\mu,\nu\rangle^{\mathrm{Hilb}_n}$ of 3-point invariants by a sum over curve degrees:

$$\langle\lambda,\mu,\nu\rangle^{\mathrm{Hilb}_n} = \sum_{d\geq 0} q^d \langle\lambda,\mu,\nu\rangle^{\mathrm{Hilb}_n}_{0,3,d}.$$

Corollary 1. *Let H be the divisor class in the Nakajima basis corresponding to the tautological rank n bundle $\mathcal{O}/\mathcal{J} \to \mathrm{Hilb}_n$ with fiber $\mathbb{C}[x,y]/\mathcal{J}$ over $\mathcal{J} \in \mathrm{Hilb}_n$ and ν the corresponding partition.Then we can recover inductively in the degree d, all the Littlewood–Richardson coefficients $(c^{\nu}_{\lambda,\mu})_{\lambda,\mu\in\mathcal{P}(n)}$.*

Proof. The non-negative degree of a curve class $\beta \in H_2(\mathrm{Hilb}_n,\mathbb{Z})$ is defined by $d = \int_{\beta} H$. Then via the identification of $c^{\nu}_{\lambda,\mu}$ with the 3-point Gromov–Witten invariant $\langle\lambda,H,\mu\rangle^{\mathrm{Hilb}_n}_{0,3,d}$ where $[\lambda]$, $[\mu]$ are the corresponding classes in $H^{4n}_T(\mathrm{Hilb}_n,\mathbb{Q})$ associated with the partitions λ and μ in $\mathcal{P}(n)$, we proceed by induction on the degree d as in section 3.6 of [11]. □

Remark 4. *If we choose the partition ν to be the empty partition $\emptyset$, we recover the relative Gromov–Witten invariants $N_{d,g}(\lambda, \mu)$ studied by Fomin and Mikhalkin in [10], and by Caporaso and Harris in [12].*

4. Configurations of Points over a Normal Rational Curve

In this section, we study codes defined from a linear series attached to a divisor on the normal rational curve NRC or equivalently Goppa codes on $\mathbb{P}^1$ and hence generalized Reed–Solomon codes. Assume V is a vector space of dimension $n+1$ over a field k equipped with a linear action, that is, G acts via a representation $G \to GL(V)$. We denote by $S^d V$ the d-th symmetric power of V.

Consider the d-Veronese embedding of $\mathbb{P}^n$

$$\begin{aligned} \mathbb{P}V^* &\to \mathbb{P}S^d V^* \\ v &\mapsto v^d, \end{aligned} \tag{5}$$

mapping the line spanned by $v \in V^*$ to the line spanned by $v^d \in S^d V^*$. In coordinates, if we choose bases $\{\alpha, \beta\}$ for V and $\{[\frac{n!}{k!(n-k)!}]\alpha^k \beta^{d-k}\}$ for $S^d V^*$ and expanding out $(x\alpha + y\beta)^d$, we see that in coordinates this map may be given as

$$[x, y] \to [x^d, x^{d-1}y, x^{d-2}y^2, \ldots, xy^{d-1}, y^d].$$

In particular, the homogeneous coordinate ring for the natural projective embedding of the geometric invariant theory (GIT) quotient $(\mathbb{P}^d)^n //SL_{d+1}$ is the ring of invariants for n ordered points in the projective space up to, projectivity, i.e, if one considers the function field $k(x_1, \ldots, x_d)$ of the projective space $(\mathbb{P})^d$, the ring of invariants is defined by:

$$\{f \in k(x_1, \ldots, x_d) \,|\, \forall \sigma \in SL_{d+1}, \sigma \cdot f = f\}.$$

Generators for this ring are given by tableau functions, which appear in many areas of mathematics, particularly representation theory and Schubert calculus. Consider the hypersimplex:

$$\triangle(d+1, n) = \{(c_1, \ldots, c_n) \in \mathbb{Q}^n | 0 \leq c_i \leq 1, \sum c_i = d+1\},$$

for any $1 \leq d \leq n-3$ and choose a linearization $c \in \triangle(d+1, n)$, there is a morphism

$$\varphi : \bar{M}_{0,n} \to (\mathbb{P}^d)^n //_c SL_{d+1},$$

sending a configuration of distinct points on $\mathbb{P}^1$ to the corresponding configuration under the d^{th} Veronese map.

The symmetric power $\mathrm{Sym}^n C_d$ of the curve C_d is the quotient of the configuration space $\mathcal{C}_d^n$ of n unordered tuples of points on the normal rational curve C_d by the symmetric group S_n. Furthermore, we can identify the set of effective divisors of degree d on C_d with the set of k-rational points of the symmetric power $\mathrm{Sym}^n C$, that is, $\mathrm{Sym}^n C$ represents the functor of families of effective divisors of degree n on C.

Lee-Sullivan List-Decoding Algorithm of Reed–Solomon Codes

By definition, the rational normal curve C_d is the image by the $d-$Veronese embedding of $\mathbb{P}V^* = \mathbb{P}^1$ where V is a 2-dimensional vector space, therefore it is isomorphic to any curve of genus 0. The action of $PGL(2, k)$ on $\mathbb{P}^d$ preserves the rational normal curve C_d. Conversely, any automorphism of $\mathbb{P}^d$ fixing C_d pointwise is the identity. It follows that the group of automorphisms of $\mathbb{P}^d$ that preserves C_d is precisely $PGL(2, k)$. These codes are just generalized RS codes and they come with efficient decoding algorithms once we choose a metric consistent with channel errors and search of a set of vectors with given metric properties as a correcting code. In particular, these codes are consistent with the Hamming metric ([13,14]). Recall that given two vectors of length n, say U and V, the

Hamming distance $d_H(U, V)$ between U and V is the number of coordinates in which they differ.

Given a $[n, k]$ RS code C of length n and dimension k, we call d the minimum (Hamming distance) which attains the Singleton bound $n - k + 1$. We shall identify the code with the set of its codewords. A codeword of C is viewed as a polynomial $c_0 + c_1 x + \ldots + c_{n-1} x^{n-1}$ in the $\mathbb{F}-$vector space $\mathbb{F}[x]$, where $\mathbb{F}$ is a finite field. In the communication process, when a codeword is transmitted, it can be affected by errors and erasures. An error occurs when one codeword component is changed into another field element and an erasure occurs when the received component has an unknown value. The problem of minimum distance decoding is to find, for any given vector v, the set C_v of all codewords $c \in C$ at minimum distance from v. If C_v contains just one element c, then the sent codeword coincides with the received codeword and no decoding is needed. The codewords of minimum weight are the points lying in the intersection of any line and the curve. K. Lee and M.E. O'Sullivan in [15] describe a list decoding algorithm consisting of two steps: the interpolation step and the root-finding step. Starting with a set of generators of the module induced from the ideal for the n points $\{P_1, \ldots, P_n\}$, they convert the generators to a Gröbner basis of the module in which the minimal polynomial is found. This results in an efficient algorithm solving the interpolation problem.

Let v be the received vector, and fix n distinct points $\alpha_1, \ldots, \alpha_n$ from $\mathbb{F}$, for each $1 \leq i \leq n$, let P_i denote the point (α_i, v_i) by Lagrange interpolation we get the polynomial $h_v = \sum_{i=1}^{n} v_i h_i \in \mathbb{F}[x]_n$, where $h_i = \prod_{j=1}^{n} (x - \alpha_j)$, $j \neq i$ so that $h_i(\alpha_j) = 1$ if $j = 1$, and 0 otherwise. Now for $m \geq 1$, we define the ideal

$$I_{v,m} = \{f \in \mathbb{F}[x, y] | \, mult_{P_i}(f) \ \geq m \ \text{ for } 1 \leq i \leq n\} \cup \{0\}.$$

For $f \in \mathbb{F}[x, y]$ and $u \geq 1$, denoted by $deg_u(f)$, the $(1, u)-$weighted degree of f, that is, the variables x and y, are assigned weights 1 and u, respectively, and for a monomial $x^i y^j$, we define $deg_u(x^i y^j) = i + uj$.

The goal of the interpolation step is to find a polynomial in $I_{v,m}$ having the smallest $(1, k-1)-$weighted degree. The codewords of minimum weight are the points lying in the intersection of any line and the curve. Moreover if $wt(v - c) < n - \frac{w}{m}$, where $w = deg_{k-1}(f)$ and f is the polynomial representing the word c, then the polynomial h_c is a root of f as a polynomial in y over $\mathbb{F}[x]$. Moreover the set of polynomials $(y - h_c)^i \eta^{m-i}$, $0 \leq i \leq m$, where $\eta = \prod_{j=1}^{n} (x - \alpha_j)$ is a set of generators of $I_{v,m}$.

Let Q be the minimal polynomial of $I_{v,m}$ with respect to the monomial order $>_{k-1}$ of $\mathbb{F}[x, y]$. We can find Q by computing a Gröbner basis of $I_{v,m}$ with respect to $>_{k-1}$. In Appendix A, we provide Horn's algorithm to compute sets of indices which are admissible for the Horn problem. As a result, we provide a set of generators for the algebraic code induced on the NRC.

Proposition 2. *If we consider the set of orbits of C_d^n by the action of finite subgroups of the symmetric group S_n, we get all possible divisor classes in the group* $\mathrm{Div}^n(C_d)$ *of degree n divisors on C_d.*

Proof. Since the symmetric group S_n is generated by 3 elements, a reflection of order 2, a symmetry of order 3 and a rotation of order n, we get all the divisor classes by quotienting the configuration space $\mathcal{C}_d^n$ of n points on the normal rational curve, by the cyclic group generated by the rotation, or one of the triangle groups, the dihedral group D_n, the alternated groups A_4, A_5 or the symmetric group S_4. □

5. Notion of Collinearity on the Normal Rational Curve

A permutation matrix $\sigma \in GL(n, \mathbb{F}_q)$ acts on the Grassmannian by multiplication on the right of the corresponding representation matrix. In particular, we are interested in understanding the orbits by the action of any permutation matrix of $GL(n, \mathbb{F}_q)$ and moreover of any subgroup G contained in $GL(n, \mathbb{F}_q)$. Further, it is possible to count the

orbits of the action in several cases and this is established by the correspondence given in Theorem 2 between sets of points satisfying certain geometrical conditions and partitions.

Definition 2. *An incidence structure $\mathcal{S}$ on V is a triple $(\mathcal{P}, \mathcal{B}, I)$, where $\mathcal{P}$ is a set whose elements are smooth, reduced points in V, $\mathcal{B}$ is a set whose elements are subsets of points called blocks (or lines in several specific cases) endowed with a relation of collinearity, and an incidence relation $I \subset \mathcal{P} \times \mathcal{B}$. If $(P, L) \in I$, then we say that P is incident with L or L is incident with P, or P lies in L or L contains P.*

When the collinearity relation is a symmetric ternary relation defined on triples $(p, q, r) \in \mathcal{P} \times \mathcal{P} \times \mathcal{P}$ by the geometric condition $(p, q, r) \in \mathcal{B}$ if either $p + q + r$ is the full intersection cycle of C_d with a k-line $l \subset \mathbb{P}^n(k)$ with the right multiplicities, or else if there exists a k-line $l \subset V$ such that, $p, q, r \in l$, then the triple (p, q, r) is called a plane section.

1. For any $(p, q) \in \mathcal{P}^2(V^*)$, there exists an $r \in \mathcal{P}(S^d V^*)$ such that $(p, q, r) \in l$. The triple (p, q, r) is strictly collinear if r is unique with this property, and p, q, r are pairwise distinct. The subset of strictly collinear triples is a symmetric ternary relation. When k is a field algebraically closed of characteristic 0, then r is unique with this property, and we recover the euclidean axioms.
2. Assume that $p \neq q$ and that there are two distinct $r_1, r_2 \in \mathcal{P}$ with $(p, q, r_1) \in \mathcal{B}$ and $(p, q, r_2) \in \mathcal{B}$. Denote by $l = l(p, q)$ the set of all such rs, then $l^3 \in \mathcal{B}$—that, is any triple (r_1, r_2, r_3) of points in which l is collinear. Such sets l are called lines in $\mathcal{B}$.

If V is a 3-dimensional vector space defined over the finite field $\mathbb{F}_p$, then the projective plane $\mathbb{P}^2(\mathbb{F}_p)$ on V is defined by the incidence structure $PG(2, p) = (\mathcal{P}(V), \mathcal{L}(V), I)$.

Definition 3.

1. *A $(k; r)$-arc $\mathcal{K}$ in $PG(2, p)$ is a set of k points such that some r, but not $r + 1$ of them are collinear. In other words, some line of the plane meets $\mathcal{K}$ in r points and no more than r points. A $(k; r)-$arc is complete if there is no $(k + 1; r)$ arc containing it.*
2. *A k-arc is a set of k points, such that, every subset of s points with $s \leq n$ points is linearly independent.*

Let q denote some power of the prime p and $PG(n, p)$ be the n-dimensional projective space $(\mathbb{F}_p)^{n+1} \cong \mathbb{F}_q$, where $n \geq 2$.The normal rational curve C is defined as:

$$\mathcal{V}_1^n := \left\{ \mathbb{F}_q(1, x, x^2, \ldots, x^n) |\ x \in \mathbb{F}_q \bigcup \{\infty\} \right\}.$$

If $q \geq n + 2$, the NRC is an example of a $(q + 1)-$arc. It contains $q + 1$ rational points, and every set of $n + 1$ points are linearly independent. For each $a \in (\mathbb{F}_p)^{n+1}$, the mapping:

$$\mathbb{F}_p(x_0, \ldots, x_n) \to \mathbb{F}_p(a^0 x_0, \ldots, a^n x_n),$$

describes an automorphic collineation of the NRC.

All invariant subspaces form a lattice with the operations of "join" and "meet".

For $j \in \mathbb{N}$, let $\Omega(j) = \{m \in \mathbb{N} | 0 \leq m \leq n, \binom{m}{j} \neq 0 \, mod \, p\}$. Given $J \subset \{0, 1, \ldots, n\}$, put $\Omega(J) = \bigcup_{j \in J} \Omega(j)$, $\Psi(J) := \bigcup_{j \in J} \{j, n - j\}$.

Both Ω and Ψ are closure operators on $\{0, 1, \ldots, n\}$. Likewise the projective collineation $\mathbb{F}_p(x_0, x_1, \ldots, x_n) \to \mathbb{F}_p(x_n, x_{n-1}, \ldots, x_0)$ leaves the NRC invariant whence Λ has to be closed with respect to Ψ. Any algebraic-geometric code constructed by evaluation of a function over the NRC with values in $\mathbb{F}_q$ is a generalized Reed–Solomon code of length at most q. In order to get longer codes, one needs to use elements from any finite extension $\mathbb{F}_q^r$ of $\mathbb{F}_q$.

Proposition 3. *Each subspace invariant under collineation of the NRC is indexed by a partition in $\mathcal{P}(t)$. If the ground field k is sufficiently large, then every subspace which is invariant under all collineations of the NRC is spanned by base points kc_λ, where $\lambda \in \mathcal{P}(t)$.*

Proof. Let

$$E_n^t := \{(e_0, e_1, \ldots, e_n) \in \mathbb{N}^{n+1} | \, e_0 + e_1 + \ldots + e_n = t\},$$

be the set of partitions of t of n parts and let Y be the $\binom{n}{t}-$dimensional vector space over $\mathbb{F}_p$ with basis

$$\{c_{e_0,e_1,\ldots,e_n} \in \mathbb{F}_q : (e_0, e_1, \ldots, e_n) \in E_n^t\}.$$

Let us call $\mathcal{V}_n^t$ the Veronese image under the Veronese mapping given by:

$$\mathbb{F}_p(\sum_{i=0}^{n} x_i b_i) \to \mathbb{F}_p(\sum_{E_n^t} c_{e_0,\ldots,e_n} x^{e_0} x_1^{e_1} \cdots c_n^{e_n}), \quad x_i \in \mathbb{F}_p.$$

The Veronese image of each r-dimensional subspace of $PG(n, p)$ is a sub-Veronesean variety $\mathcal{V}_r^t$ of $\mathcal{V}_n^t$, and all those subspaces are indexed by partitions in $\mathcal{P}(t)$. Thus by a Theorem due to Gmainer are invariant under the collineation group of the normal rational curve (see [16]).

The k-rational points $(p_0, p_1, \cdots, p_n)$ of the normal rational curve C correspond to collinear points on C that are defined over some Galois extension l of k and permuted by $\mathrm{Gal}(l/k)$. □

5.1. An Application: Three-Point Codes on the Normal Rational Curve

As we showed in Proposition 3, each subspace invariant under collineation of the NRC is indexed by a partition $\lambda \in \mathcal{P}(d)$. Let us call the base point associated with the partition λ as P_λ. As we are considering that the ground field is $\mathbb{F}_q$, the $\mathbb{F}_q$-points might be defined over a finite extension $\mathbb{F}_{q^r}$ of $\mathbb{F}_q$. Observe that for any divisor r of n, one easily obtains a extension field of $\mathbb{F}_q$ of degree r. Namely, let ξ a non-trivial $r-$root of unity, one can consider the symbols $\xi^{q^r}, \ldots, \xi^q, \xi$ and the polynomial which has them as roots, $q(x) = \prod_{i=0}^{i=r}(1 - \xi^{q^i})$ gives an extension field of $\mathbb{F}_q$ of degree r.

Theorem 2. *Let $\sigma_1, \sigma_2, \sigma_3$ be three generators for the symmetric group S_d and let λ_1, λ_2 and λ_3 be the partitions of d indexing the corresponding irreducible representations in the special linear group $SL(n, \mathbb{F}_q)$. Then any algebraic code defined over the NRC is covered by a divisor defined as linear combination of the base points $(P_{\lambda_i})_{1 \le i \le 3}$ on the NRC, where the λ_i are LR coefficients.*

Proof. Consider the divisors associated with the rational maps $f(x, y, z) = nx + my + lz$ defined over the normal rational curve C_d defined over $\mathbb{F}_q$, with n, m and l integer numbers. In particular, if $d | \, q^2 - 1$, the points $P = (\alpha, 0, 0)$, $Q = (0, \beta, 0)$ and $R = (0, 0, \gamma)$ with $\alpha^d = 1$, $\beta^d = 1$ and $\gamma^d = 1$, are $\mathbb{F}_{q^2}-$rational points on C_d, and the divisors nP, mQ and lR define codes on it. Reciprocally, given a code on the NRC, by Proposition 2, the corresponding divisor defining the code is defined by a finite subgroup in the symmetric group. Since the symmetric group is generated by the 3 elements σ_1, σ_2 and σ_3, the divisor is a linear combination of the base points $(P_{\lambda_i})_{1 \le i \le 3}$ on the NRC. □

5.2. Conclusions

In [17], the authors considered a particular class of block codes known as quasi-cyclic codes as orbit codes in the Grassmannian parameterizing constant dimension codes. In the present paper we have focused on RS codes that can also be viewed as orbit codes in the Grassmannian through the action of $PGL(n, q)$, the collineation group of the NRC. This approach could be extended to study a wide class of codes, including convolutional codes with two states known as 2D finite support convolutional codes of rate $\frac{k}{n}$, which are defined as free $\mathbb{F}[z_1, z_2]-$submodules of $\mathbb{F}[z_1.z_2]^n$ with rank k.

Author Contributions: Writing—original draft, C.M.; Writing–review—editing, A.B. All authors have read and agreed to the published version of the manuscript.

Funding: This research received external funding from University of Alcalá.

Acknowledgments: We thank Diego Napp for very useful comments during the preparation of this manuscript and the referee for valuable observations.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A. Explicit Presentation of 3-Point Codes

In this section, we provide Horn's algorithm to compute sets of indices which are admissible for the Horn problem. As a result, we provide a set of generators for the algebraic code induced on the NRC. Given sets $I, J, K \subset \{0, 1, \ldots, n\}$, of cardinality r, we can associate to them partitions λ, μ and ν as follows. Let $I = \{i_1 < \ldots, < i_r\} \subset \{1, \ldots, n\}$; then the corresponding partition is defined as $\lambda = (i_r - r, \ldots, i_1 - 1)$. We consider the corresponding codes defined by the base points c_λ, c_μ and c_ν, whenever the corresponding Littlewood–Richardson coefficient $c^\nu_{\lambda,\mu}$ is positive. Next, we give an algorithm to compute the Littlewood–Richardson coefficients $c^\nu_{\lambda,\mu}$. Horn defined sets of triples (I, J, K) by the following inductive procedure (see [7]):

$$U_r^n = \{(I, J, K) | \sum_{i\in I} + \sum_{j\in J} = \sum_{k\in K} k + r(r+1)/2\},$$

$$T_r^n = \{(I, J, K) \in U_r^n | \, for\ all\ p < r\ and\ all\ (F, G, H) \in T_p^r,$$
$$\sum_{f\in F} i_f + \sum_{g\in G} j_g \leq \sum_{h\in H} k_h + p(p+1)/2\}.$$

Note that Horn's algorithm produces all the triples from the lowest values. Even if it is possible to start with a random generator set I, you need first to compute the lower values. As a consequence of the classification Theorem 2, for any triple (I, J, K) of indices admissible for the Horn problem the polynomials defined by $f(x) = \prod_{j\in J}(x - \alpha^j), g(x) = \prod_{i\in I}(x - \alpha^i)$, and $h(x) = \prod_{k\in K}(x - \alpha^k)$ where α is a primitive element of $\mathbb{F}_{q^m}$ and m is the least integer such that $n + 1 | \, p^m - 1$ constitute a set of generators for the ideal of the corresponding algebraic code in the module of $n + 1$ $\mathbb{F}_{q^m}$-rational points lying on the NRC.

Here we present a Sage [6] code calculating the U_r^n and T_r^n index sets, followed by a table containing all the cases till $n = 4$ and $r = 3$. The algorithm is implemented using Python: this involves calculate and iterate through $r-$combination of $n-$element. The running time is $O(\binom{n}{r}^3)$.

```
from sage.combinat.subset import Subsets

def simple_cache(func):
cache = dict()
def cached_func(*args):
if args not in cache:
cache[args] = func(*args)
return cache[args]
cached_func.cache = cache
return cached_func
```

```
@simple_cache
def getUnr(n, r):
if r >= n:
raise ValueError(‘‘r must be less than n: (n, r) =
(%d, %d)’’ %(n, r))
s = Subsets(range(1, n + 1), r)
candidates = [(x, y, z) for x in s for y in s for z in s]
return [tuple(map(sorted, (x, y, z))) for (x, y, z) in candidates if (
sum(x) + sum(y)) == (sum(z) + r * (r + 1)/2)]



def index_filter(sub_index, index):
if max(sub_index) > len(index):
raise ValueError(‘‘%s must be valid indexes for %s’’
% (sub_index, index))
# our indexes lists start at 1
return [index[i - 1] for i in sub_index]



def condition((f, g, h), (i, j, k)):
p = len(f)
return sum(index_filter(f, i)) + sum(index_filter(g, j)) <= sum(
index_filter(h, k)) + p*(p + 1)/2

def genTillR(r):
return [getTnr(r, p) for p in range(1, r)]

@simple_cache
def getTnr(n, r):
if r == 1:
return getUnr(n, 1)
else:
return [(i, j, k) for (i, j, k) in getUnr(n, r) if all(
all(condition((f, g, h), (i, j, k)) for (f, g, h) in triplets)
for triplets in genTillR(r))]
```

Here we list code's remarks

- The `sorted()` mapping function in `getUnr()` is necessary because the order of elements in `Subsets` is unknown;
- There is a 1-offset between index in Python lists and index sets we use;
- The recursion in `getTnr()` is factored out in `getTillR()` call;
- The cache decorator mitigates the perils of performing the same calculation several times in a function that is already heavily recursive;
- Results are limited by constraints Python has on recursive function calls;
- The filtering performed on U_r^n to get T_r^n is implemented by two nested calls to `all()`.

(n, r)	U_r^n	T_r^n
(2, 1)	$(\{1\},\{1\},\{1\}), (\{1\},\{2\},\{2\}),$ $(\{2\},\{1\},\{2\})$	$(\{1\},\{1\},\{1\}), (\{1\},\{2\},\{2\}),$ $(\{2\},\{1\},\{2\})$
(3, 1)	$(\{1\},\{1\},\{1\}), (\{1\},\{2\},\{2\}),$ $(\{1\},\{3\},\{3\}), (\{2\},\{1\},\{2\}),$ $(\{2\},\{2\},\{3\}), (\{3\},\{1\},\{3\})$	$(\{1\},\{1\},\{1\}), (\{1\},\{2\},\{2\}),$ $(\{1\},\{3\},\{3\}), (\{2\},\{1\},\{2\}),$ $(\{2\},\{2\},\{3\}), (\{3\},\{1\},\{3\})$
(3, 2)	$(\{1,2\},\{1,2\},\{1,2\}),$ $(\{1,2\},\{1,3\},\{1,3\}),$ $(\{1,2\},\{2,3\},\{2,3\}),$ $(\{1,3\},\{1,2\},\{1,3\}),$ $(\{1,3\},\{1,3\},\{2,3\}),$ $(\{2,3\},\{1,2\},\{2,3\})$	$(\{1,2\},\{1,2\},\{1,2\}),$ $(\{1,2\},\{1,3\},\{1,3\}),$ $(\{1,2\},\{2,3\},\{2,3\}),$ $(\{1,3\},\{1,2\},\{1,3\}),$ $(\{1,3\},\{1,3\},\{2,3\}),$ $(\{2,3\},\{1,2\},\{2,3\})$
(4, 1)	$(\{1\},\{1\},\{1\}), (\{1\},\{2\},\{2\}),$ $(\{1\},\{3\},\{3\}), (\{1\},\{4\},\{4\}),$ $(\{2\},\{1\},\{2\}), (\{2\},\{2\},\{3\}),$ $(\{2\},\{3\},\{4\}), (\{3\},\{1\},\{3\}),$ $(\{3\},\{2\},\{4\}), (\{4\},\{1\},\{4\})$	$(\{1\},\{1\},\{1\}), (\{1\},\{2\},\{2\}),$ $(\{1\},\{3\},\{3\}), (\{1\},\{4\},\{4\}),$ $(\{2\},\{1\},\{2\}), (\{2\},\{2\},\{3\}),$ $(\{2\},\{3\},\{4\}), (\{3\},\{1\},\{3\}),$ $(\{3\},\{2\},\{4\}), (\{4\},\{1\},\{4\})$
(4, 2)	$(\{1,2\},\{1,2\},\{1,2\}),$ $(\{1,2\},\{1,3\},\{1,3\}),$ $(\{1,2\},\{1,4\},\{1,4\}),$ $(\{1,2\},\{1,4\},\{2,3\}),$ $(\{1,2\},\{2,3\},\{1,4\}),$ $(\{1,2\},\{2,3\},\{2,3\}),$ $(\{1,2\},\{2,4\},\{2,4\}),$ $(\{1,2\},\{3,4\},\{3,4\}),$ $(\{1,3\},\{1,2\},\{1,3\}),$ $(\{1,3\},\{1,3\},\{1,4\}),$ $(\{1,3\},\{1,3\},\{2,3\}),$ $(\{1,3\},\{1,4\},\{2,4\}),$ $(\{1,3\},\{2,3\},\{2,4\}),$ $(\{1,3\},\{2,4\},\{3,4\}),$ $(\{1,4\},\{1,2\},\{1,4\}),$ $(\{1,4\},\{1,2\},\{2,3\}),$ $(\{1,4\},\{1,3\},\{2,4\}),$ $(\{1,4\},\{1,4\},\{3,4\}),$ $(\{1,4\},\{2,3\},\{3,4\}),$ $(\{2,3\},\{1,2\},\{1,4\}),$ $(\{2,3\},\{1,2\},\{2,3\}),$ $(\{2,3\},\{1,3\},\{2,4\}),$ $(\{2,3\},\{1,4\},\{3,4\}),$ $(\{2,3\},\{2,3\},\{3,4\}),$ $(\{2,4\},\{1,2\},\{2,4\}),$ $(\{2,4\},\{1,3\},\{3,4\}),$ $(\{3,4\},\{1,2\},\{3,4\})$	$(\{1,2\},\{1,2\},\{1,2\}),$ $(\{1,2\},\{1,3\},\{1,3\}),$ $(\{1,2\},\{1,4\},\{1,4\}),$ $(\{1,2\},\{2,3\},\{2,3\}),$ $(\{1,2\},\{2,4\},\{2,4\}),$ $(\{1,2\},\{3,4\},\{3,4\}),$ $(\{1,3\},\{1,2\},\{1,3\}),$ $(\{1,3\},\{1,3\},\{1,4\}),$ $(\{1,3\},\{1,3\},\{2,3\}),$ $(\{1,3\},\{1,4\},\{2,4\}),$ $(\{1,3\},\{2,3\},\{2,4\}),$ $(\{1,3\},\{2,4\},\{3,4\}),$ $(\{1,4\},\{1,2\},\{1,4\}),$ $(\{1,4\},\{1,3\},\{2,4\}),$ $(\{1,4\},\{1,4\},\{3,4\}),$ $(\{2,3\},\{1,2\},\{2,3\}),$ $(\{2,3\},\{1,3\},\{2,4\}),$ $(\{2,3\},\{2,3\},\{3,4\}),$ $(\{2,4\},\{1,2\},\{2,4\}),$ $(\{2,4\},\{1,3\},\{3,4\}),$ $(\{3,4\},\{1,2\},\{3,4\})$
(4, 3)	$(\{1,2,3\},\{1,2,3\},\{1,2,3\}),$ $(\{1,2,3\},\{1,2,4\},\{1,2,4\}),$ $(\{1,2,3\},\{1,3,4\},\{1,3,4\}),$ $(\{1,2,3\},\{2,3,4\},\{2,3,4\}),$ $(\{1,2,4\},\{1,2,3\},\{1,2,4\}),$ $(\{1,2,4\},\{1,2,4\},\{1,3,4\}),$ $(\{1,2,4\},\{1,3,4\},\{2,3,4\}),$ $(\{1,3,4\},\{1,2,3\},\{1,3,4\}),$ $(\{1,3,4\},\{1,2,4\},\{2,3,4\}),$ $(\{2,3,4\},\{1,2,3\},\{2,3,4\})$	$(\{1,2,3\},\{1,2,3\},\{1,2,3\}),$ $(\{1,2,3\},\{1,2,4\},\{1,2,4\}),$ $(\{1,2,3\},\{1,3,4\},\{1,3,4\}),$ $(\{1,2,3\},\{2,3,4\},\{2,3,4\}),$ $(\{1,2,4\},\{1,2,3\},\{1,2,4\}),$ $(\{1,2,4\},\{1,2,4\},\{1,3,4\}),$ $(\{1,2,4\},\{1,3,4\},\{2,3,4\}),$ $(\{1,3,4\},\{1,2,3\},\{1,3,4\}),$ $(\{1,3,4\},\{1,2,4\},\{2,3,4\}),$ $(\{2,3,4\},\{1,2,3\},\{2,3,4\})$

References

1. Manganiello, F.; Trautmann, A.L.; Rosenthal, J. On conjugacy classes of subgroups of the general linear group and cyclic orbit codes. In Proceedings of the IEEE International Symposium on Information Theory proceedings (ISIT), St. Petersburg, Russia, 31 July–5 August 2011.
2. Besana, A.; Martínez, C. Combinatorial enumeration of cyclic covers of $\mathbb{P}^1$. *Turk. J. Math.* **2018**, *42*, 2018–2034. [CrossRef]
3. Martínez, C. On the cohomology of Brill-Noether loci over Quot schemes. *J. Algebra* **2008**, *319*, 391–403. [CrossRef]
4. Climent, J.; Napp, D.; Pinto, R.; Simoes, R. Decoding of 2D convolutional codes over an erasure Channel. *Adv. Math. Commun.* **2016**, *10*, 179–193. [CrossRef]
5. Bifet, E.; Ghione, F.; Leticia, M. On the Abel-Jacobi map for divisors of higher rank on a curve. *Math. Ann.* **1994**, *299*, 641–672. [CrossRef]
6. SageMath. Available online: http://www.sagemath.org/ (accessed on 20 October 2020).
7. Fulton, W. Eigenvalues, invariant factors, highest weights and Schubert calculus. *Bull. Am. Math. Soc.* **2000**, *37*, 209–249. [CrossRef]
8. Manivel, L. On rectangular Kronecker coefficients. *J. Algebr. Comb.* **2011**, *33*, 153–162. [CrossRef]
9. Sottile, F.; Lam, T.; Lauve, A. A skew Littlewood-Richardson rule from Hopf algebras. *Int. Math. Res. Not.* **2011**, *2011*, 1205–1219.
10. Fomin, S.; Milkhalkin, G. Label floor diagrams for plane curves. *J. Eur. Math. Soc.* **2009**, *12*, 1453–1496.
11. Okounkov, A.; Pandharipande, P. Quantum cohomology of the Hilbert scheme of points in the plane. *Invent. Math.* **2010**, *179*, 523–557. [CrossRef]
12. Caporaso, L.; Harris, J. Counting plane curves of any genus. *Invent. Math.***1998**, *131* , 345–392. [CrossRef]
13. Bezzateev, S.V.; Shekhunova, N. Class of generalized Goppa codes perfect in weighted Hamming metric. *Des. Codes Criptogr*. **2013**, *66*, 391–399. [CrossRef]
14. Bezzateev, S.V.; Shekhunova, N.A. Subclass of cyclic Goppa codes. *IEEE Trans. Inf. Theory* **2013**, *59*, 11. [CrossRef]
15. Lee, K.; O'Sullivan, M.E. List decoding of RS codes from a Gröbner basis perspective. *J. Symb. Comput.* **2008**, *43*, 645–658. [CrossRef]
16. Gmainer, J. Pascal's Triangle, Normal Rational Curves, and their Invariant Subspaces. *Eur. J. Comb.* **2001**, *22*, 37–49. [CrossRef]
17. Besana, A.; Martínez, C. A Geometrical Realisation of Quasi-Cyclic Codes. In *Combinatorics, Probability and Control*; IntechOpen: London, UK, 2020; pp. 259–271.