CODES, HORN'S PROBLEM AND GROMOV-WITTEN INVARIANTS

ALBERTO BESANA AND CRISTINA MARTÍNEZ

Abstract. We study the Horn problem in the context of algebraic codes on a smooth projective curve defined over a finite field, reducing the problem to the representation theory of the special linear group $SL(2, \mathbb{F}_q)$. We characterize the coefficients that appear in the Kronecker product of symmetric functions in terms of Gromov-Witten invariants of the Hilbert scheme of points in the plane. In addition we classify all the algebraic codes defined over the rational normal curve.

1. Introduction

Finite fields have a remarkable property that finite dimensional vector spaces over them are naturally endowed with a canonical and compatible field structure. This leads to some interesting notions where the field structure and the linear structure are intertwined. Let denote by $\mathbb{F}_p$ the Galois field of $p$ elements. Any other field $\mathbb{F}$ of characteristic $p$ contains a copy of $\mathbb{F}_p$. Any $V = \mathbb{F}_p^n$ field extension of $\mathbb{F}_p$ is a $\mathbb{F}_p$ vector space of dimension $n$ and an $(n-1)$-dimensional projective space $PG(n-1, p)$. One can consider field extensions $\mathbb{F}_q$ of $\mathbb{F}_p$ as $q$ varies through powers of the prime $p$.

Let us now consider the finite field $\mathbb{F}_q$ with $q$ elements. When the finite field $\mathbb{F}_q^m$ is generated as a vector space over $\mathbb{F}_q$ by a unique element $\alpha \in \mathbb{F}_q$, then the set $\{1, \alpha, \alpha^2, \ldots, \alpha^{m-1}\}$ forms a basis of $\mathbb{F}_q^m$. In particular $\mathbb{F}_q^{mn} = \mathbb{F}_q(\alpha)$. If $W$ is generated by $v_1, \ldots, v_m$ as an $\mathbb{F}_q$ vector space then $\alpha W$ is generated by $mn$ elements: $\alpha v_1, \ldots, \alpha v_m, \ldots, \alpha^{n-1} v_1, \ldots, \alpha^{n-1} v_m$. There is a $\mathbb{F}_q$-basis $B$ of $\mathbb{F}_q^{mn}$ such that each element of $B$ generates $\mathbb{F}_q^{mn}$ over $\mathbb{F}_q$.

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 it. The set of all subspaces of dimension $r$ is called the Grassmannian and it is denoted by $G_{\mathbb{F}_q}(r, n)$ 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 $G_{\mathbb{F}_q}(r, n)$ as a projective system, we obtain a $q$-ary linear code, called the Grassmann code, which we denote $C(r, n)$. The length $l$ and the dimension $k$ of $C(r, n)$ are given by the $q$-binomial coefficient $l = \binom{n}{r}_q = \frac{(q^{n+1}-1)(q^{n+1}-q)\cdots(q^{n+1}-q^r)}{(q^{r+1}-1)(q^{r+1}-q)\cdots(q^{r+1}-q^r)}$, and $k = \binom{n}{r}$, respectively.

There is a right action of the general linear group $GL(n, \mathbb{F}_q)$ on $G_{\mathbb{F}_q}(k, n)$:

2000 Mathematics Subject Classification. 05E10 (primary) ; 05A15 (secondary) .

Key words and phrases. Algebraic code, symmetric group, partitions.
2 ALBERTO BESANA AND CRISTINA MARTÍNEZ

\[ \mathcal{G}_{\mathbb{F}_q}(k,n) \times GL(n,\mathbb{F}_q) \to \mathcal{G}_{\mathbb{F}_q}(k,n) \]

\[ \langle U, A \rangle \to UA. \]

Observe that the action is defined independent of the choice of the representation matrix \( U \in \mathbb{F}_q^{k \times n} \).

**Definition 1.1.** Let \( U \in \mathcal{G}_{\mathbb{F}_q}(k,n) \) and \( G < GL(n,\mathbb{F}_q) \) a subgroup, then \( C = \{UA| A \in G \} \) is an orbit in \( \mathcal{G}_{\mathbb{F}_q}(k,n) \) 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 [BM2] we studied cyclic coverings of the projective line that correspond to orbits defined by a cyclic subgroup, that is a subgroup in \( GL(n,\mathbb{F}_q) \) containing a cyclic subgroup \( \mathbb{Z}_p \) for some prime number. In particular, we showed that any irreducible cyclic cover can be given by a prime ideal

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

This ideal defines an affine curve in \( \mathbb{A}^2(\mathbb{F}_q) \) which has singularities, if there are some \( d_k > 1 \) for some \( 1 \leq k \leq n \). But there exists an unique smooth 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 special linear group \( SL(\mathbb{F}_q,n) \).

Any cyclic cover of \( \mathbb{P}^1 \) which is simply ramified corresponds to an unordered tuple of \( n \) points on \( \mathbb{P}^1 \). We will consider more generally, configurations of \( n \) points in \( d \)-dimensional projective space \( \mathbb{P}^d(\mathbb{F}_q) \) which generically lie on a rational normal curve and we study the algebraic codes defined on it.

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

**Conventions.** For \( d \) a positive integer, \( \alpha = (\alpha_1, \ldots, \alpha_m) \) is a partition of \( d \) into \( m \) parts if the \( \alpha_i \) are positive and non-decreasing. We set \( l(\alpha) = m \) for the length of \( \alpha \), that is the number of cycles in \( \alpha \), and \( l_i \) for the length of \( \alpha_i \). The notation \( (a_1, \ldots, a_k) \) stands for a permutation in \( S_d \) that sends \( a_i \) to \( a_{i+1} \). A curve is an integral scheme of dimension 1, proper over \( k \). A homogeneous symmetric function of degree \( n \) over a commutative ring \( R \) (with identity) is a formal power series \( f(x) = \sum \alpha c_\alpha x^\alpha \), where \( \alpha \) ranges over all weak compositions of \( \alpha = (\alpha_1, \ldots, \alpha_m) \) of \( n \), \( c_\alpha \in R \) and \( x^\alpha \) stands for the monomial \( x^{\alpha_1} \cdot x^{\alpha_2} \cdots x^{\alpha_m} \). We write \( PGL(2,k) = GL(2,k)/k^* \), and elements of \( PGL(2,k) \) will be represented by equivalence classes of matrices

\[
\begin{pmatrix}
    a & b \\
    c & d
\end{pmatrix},
\]

with \( ad - bc \neq 0 \).

2. Algebraic codes over finite fields

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 to 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 $\{P_1, \ldots, P_n\}$ 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:

$$\varphi_D : L(D) \to \mathbb{F}_q^n$$

$$f \mapsto (f(P_1), \ldots, f(P_n)).$$

Using this definition, the notion of AG codes is easily generalized for varieties of higher dimension.

Let $E$ be a vector bundle of rank $r$ on $X$ defined over $\mathbb{F}_q$. One can define the code $C(X, \mathcal{P}, E)$ to be the image of the evaluation map:

$$\varphi_E : H^0(X, E) \to \bigoplus_{i=1}^n E_{P_i} \cong \mathbb{F}_q^n$$

$$s \mapsto (s(P_1), \ldots, s(P_n)).$$

Observe that $C(X, \mathcal{P}, E)$ is an $\mathbb{F}_q$-linear subspace of $\mathbb{F}_q^n$ and thus a point of the Grassmannian $\mathcal{G}_{r,n}(\mathbb{F}_q)$.

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.

One can study linear systems defined over a finite field. A convolutional code is essentially a linear system defined over a finite field. Convolutional codes have been studied by graph theoretic methods. In doing so, convolutional codes can be viewed as submodules of $R^n$ where $R := \mathbb{F}[z]$ is a polynomial ring (see [MTR]). The set of convolutional codes of a fixed degree is parametrized by the Grothendieck Quot scheme. If the degree is zero, these schemes describe a Grassmann variety.

3. Convolutional codes

Let $\mathcal{O}_X$ be the structure sheaf of the curve $X$ defined over a field $k$ and let $K$ be its field of rational functions, considered as a constant $\mathcal{O}_X$-module. Following [BGL], we define a divisor of rank $r$ and degree $d$ or $(r, d)$ divisor as a coherent sub $\mathcal{O}_X$-module of $K^r = K^\oplus r$, having rank $r$ and degree $d$. This set can be identified with the set of rational points of an algebraic variety $\text{Div}^{r,d}_X/k$ which may be described as follows. For any effective ordinary divisor $D$, set:

$$\text{Div}^{r,d}_X/(D) = \{E \in \text{Div}^{r,d}_X/k : E \subset \mathcal{O}_X(D)^r\},$$

where $\mathcal{O}_X(D)$ is considered as a submodule of $K^r$.

The space of all matrix divisors of rank $r$ and degree $d$ can be identified with the set of rational points of $\text{Quot}_{\mathcal{O}_X(D)^r/X/k}^{m}$ parametrizing torsion quotients of $\mathcal{O}_X(D)^r$ and having degree $m = r \cdot \deg D - d$. It is a smooth projective irreducible variety. Tensoring by $\mathcal{O}_X(-D)$ defines an isomorphism between $\mathcal{Q}_{r,d}(D) = \text{Quot}_{\mathcal{O}_X(D)^r/X/k}^{m}$ and $\text{Quot}_{\mathcal{O}_X/X/k}^{m}$. 


Since the whole construction is algebraic, it can be performed over any complete valued field, for example, a $p$–adic field or the ring $R = \mathbb{C}\{x\}$ of convergent power series. The matrix code $A$ can be diagonalized by elementary row and column operations with diagonal entries $x^{\alpha_1}, x^{\alpha_2}, \ldots, x^{\alpha_n}$, for unique non-negative integers $\alpha_1 \geq \ldots \geq \alpha_n$, where $x$ is a uniformizing parameter in $R$.

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 $\lambda$ of size $d = |\lambda|$. Reciprocally, when $R = \mathbb{C}\{x\}$ is the ring of convergent power series, any partition $\lambda$ defines a rank one torsion-free sheaf on $\mathbb{C}$ by setting $I_\lambda = (x^{\lambda_1}, x^{\lambda_2}, x^{\lambda_3}, \ldots, x^{\lambda_n})$. In particular, the ideal sheaf corresponding to the identity partition $(1)^n$, defines a maximal ideal $I_{(1)^n} = (x, \ldots, x)$ in $\mathbb{C}[x]$.

**Question.** Which partitions $\alpha, \beta, \gamma$ 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. Denoting the cokernels of $A, B$ and $C$ by $A, B$ and $C$ respectively, one has a short exact sequence:

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

i.e. $B$ is a submodule of $C$ with $C/B \cong A$, then 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 $\alpha, \beta$ can be the invariant factors of matrices $A, B$ if $A \cdot B = I$?

**AN EXAMPLE WITH ALGEBRAIC CODES**

**Definition 3.1.** Let $D$ be an effective divisor with disjoint support defined over a smooth projective curve $X$ and $C_1$ and $C_2$ be the corresponding codes obtained evaluating non-constant rational functions $f(x)$ and $g(x)$ with non common roots on $X$ over the support of the divisor $D$.

Then we define the quotient code of $C_1$ and $C_2$ to be the code associated to the quotient rational function $\varphi = f/g$.

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

As $\varphi$ 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:

$$m_\varphi(x) = \text{ord}_{z=0} \psi(z),$$

where $\psi = \sigma_2 \circ \varphi \circ \sigma_1$, $y = \varphi(x)$, and $\sigma_1, \sigma_2 \in \text{PGL}(2, \mathbb{F}_q)$ such that $\sigma_1(0) = x$ and $\sigma_2(y) = 0$. 
To each non-constant rational function $\varphi$ 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 $\varphi$.

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

```python
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 $\lambda_i$ 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 $\alpha, \beta, \gamma$ 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 $C = A \cdot B$?*

As in [BM1] and [BM2], 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 special linear group $SL(n, \mathbb{F}_q)$.

**Representation theory of $SL(n, \mathbb{F}_q)$**

To a partition $\alpha = (\alpha_1, \ldots, \alpha_k)$ is associated a Young diagram. The diagram of $\alpha$ is an array of boxes, lined up at the left, with $\alpha_i$ boxes in the $i^{th}$ row, with rows arranged from top to bottom. For example,

```
+-----+-----+-----+
|     |     |     |
|     |     |     |
|     |     |     |
|     |     |     |
+-----+-----+-----+
```

is the Young diagram of the partition $\alpha = (5, 3, 3, 1)$ with $l(\alpha) = 4$ and $|\alpha| = 12$. Every Young diagram $\lambda$ defines four objects which give four different isomorphic theories:

1. A representation $V_\lambda$ of $SL(n, \mathbb{F}_q)$.
2. A representation $[\lambda]$ of the symmetric group.
3. A symmetric function $s_\lambda(x_1, \ldots, x_n)$ which is the Schur function of shape $\lambda$ in the variables $(x_1, \cdots, x_n)$.
4. A Schubert cell $X_\lambda$ in the Grassmannian.

We define the Schur projection $c_\lambda : \otimes^d V \to \otimes^d V$. 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 \( c_\lambda \) is a irreducible \( SL(n, \mathbb{F}_q) \)-module, which is nonzero iff the number of rows is \( \leq \dim V_\lambda \). All irreducible \( SL(n, \mathbb{F}_q) \)-modules can be obtained in this way. Every \( SL(n, \mathbb{F}_q) \)-module is a sum of irreducible ones.

In terms of irreducible representations of \( SL(n, \mathbb{F}_q) \), a partition \( \eta \) corresponds to a finite irreducible representation that we denote as \( V(\eta) \). Since \( SL(n, \mathbb{F}_q) \) is reductive, any finite dimensional representation decomposes into a direct sum of irreducible representations, and the structure constant \( c_{\lambda,\mu}^\eta \) is the number of times that a given irreducible representation \( V(\eta) \) appears in an irreducible decomposition of \( V(\lambda) \otimes V(\mu) \). These are known as Littlewood-Richardson coefficients, since they were the first to give a combinatorial formula encoding these numbers (see [Fu]). In terms of the Hopf algebra \( \Lambda \) of Schur functions, let \( s_\lambda \) be the Schur function indexed by the partition \( \lambda \), we have \( s_\lambda \cdot s_\mu = \sum_\nu c_{\lambda,\mu}^\nu s_\nu \) for the product and we get the coefficients \( k_{\lambda,\mu}^\eta \) as the structure constants of the dual Hopf algebra \( \Lambda^* \). These are known as Kronecker coefficients, (see [Ma] and [SLL]).

One can stack Kronecker coefficients \( c_{\lambda,\mu}^\nu \) 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 \( 1 \leq i \leq n \).

Proposition 3.2. Let \( C \) be the 3D matrix whose entries are the Littlewood-Richardson coefficients, and \( K \) the 3D matrix of Kronecker coefficients. Then the matrices are inverse one to each other.

Proof. Since \( c_{\lambda,\mu}^\nu \) and \( k_{\lambda,\mu}^\nu \) correspond to the structure constants of the Hopf algebra of Schur functions and its dual one respectively, and the Hopf algebra of Schur functions is self-dual (see [SLL]), one gets that the product matrix \( C \cdot K \) is the identity 3D matrix \( I \), that is, the matrix whose rectangular coefficients are identically 1. Thus both matrices are inverse one to each other, that is, \((c_{\lambda,\mu}^\nu)^{-1} = k_{\lambda,\mu}^\nu\). \( \square \)
Remark 3.3. How we define the product of two 3D matrices? For each index \( \nu \) fixed, \( \lambda \) and \( \mu \) run over all partitions \( \mathcal{P}(n) \) of \( n \). Thus the coefficients \( \left( c_{\lambda,\mu}^\nu \right)_{\lambda,\mu \in \mathcal{P}(n)} \) are encoded in a matrix of order \( p(n) \times p(n) \), where \( p(n) \) denotes the number of partitions of \( n \). Thus the product matrix \( C^\nu \cdot K^\nu \) is the standard product of matrices in \( M_{p(n) \times p(n)}(\mathbb{R}) \).

3.1. Effective computation of Littlewood-Richardson coefficients. The convex hull in \( \mathbb{R}^3 \) of all triples \( (\lambda, \mu, \nu) \) with \( c_{\lambda,\mu}^\nu > 0 \) is the Newton polytope of \( f(x, y, z) = \sum_{\lambda, \mu, \nu} c_{\lambda,\mu}^\nu x^\lambda y^\mu z^\nu \in \mathbb{C}[x, y, z] \). Here \( x^\lambda \) denotes the monomial \( x^{\lambda_1} \cdots x^{\lambda_n} \) of partition degree \( \lambda \).

Theorem 3.4. The polynomial \( f(x, y, z) = \sum_{\lambda, \mu, \nu} c_{\lambda,\mu}^\nu x^\lambda y^\mu z^\nu \in \mathbb{C}[x, y, z] \), 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 \( \lambda, \mu \) and \( \nu \) and simple ramification over other specified points with \( |\lambda| + |\mu| + |\nu| = d \).

Proof. Whenever the coefficient \( c_{\lambda,\mu}^\nu > 0 \) is positive consider the corresponding ideal sheaves \( I_\lambda, I_\mu \) and \( I_\nu \) in \( \mathbb{C} \) associated to the partitions \( \lambda, \mu \) and \( \nu \) 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 \( C \) of colength \( \lambda \) 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 \( \lambda, \mu \) and \( \nu \) of \( n \), (see [BM1]).

Remark 3.5. The Euler characteristic of each ideal sheaf is fixed and coincides with the Euler characteristic \( \chi \) of the polyhedra described in \( \mathbb{R}^3 \) by the convex hull of all triples \( (\lambda, \mu, \nu) \) with \( c_{\lambda,\mu}^\nu > 0 \), that is, the Newton polytope of \( f(x, y, z) = \sum_{\lambda, \mu, \nu} c_{\lambda,\mu}^\nu x^\lambda y^\mu z^\nu \in \mathbb{R}[x, y, z] \). 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 3.6. The Hilbert scheme Hilb\(_n\) of \( n \) points in the plane \( \mathbb{C}^2 \) parametrizing ideals \( J \subset \mathbb{C}[x, y] \) of colength \( n \) contains an open dense set in the Zariski topology parametrizing ideals associated to configurations of \( n \) distinct points. Moreover there is an isomorphism \( \text{Hilb}_n \cong (\mathbb{C}^2)^n / S_n \). In particular, as we showed in [BM1], any conjugacy class in the symmetric group \( S_n \) determines a divisor class in the \( T \)-equivariant cohomology \( H^*_T(\text{Hilb}_n, \mathbb{Q}) \), for the standard action of the torus \( T = (\mathbb{C}^\ast)^2 \) 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 \( \text{Hilb}_n^T \subset \text{Hilb}_n \).
Denote the series \( \langle \lambda, \mu, \nu \rangle_{\text{Hilb}_n} \) of 3-point invariants by a sum over curve degrees:

\[
\langle \lambda, \mu, \nu \rangle_{\text{Hilb}_n} = \sum_{d \geq 0} q^d \langle \lambda, \mu, \nu \rangle_{0,3,d}.
\]

**Corollary 3.7.** Let \( H \) be the divisor class in the Nakajima basis corresponding to the tautological rank \( n \) bundle \( \mathcal{O} / J \to \text{Hilb}_n \) with fiber \( \mathbb{C}[x, y] / J \) over \( J \in \text{Hilb}_n \) and \( \nu \) 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 \( \beta \in H_2(\text{Hilb}_n, \mathbb{Z}) \) is defined by \( d = \int_\beta H. \) Then via the identification of \( c^\nu_{\lambda, \mu} \) with the 3-point Gromov-Witten invariant \( \langle \lambda, H, \mu \rangle_{\text{Hilb}_n, 0,3,d} \) where \([\lambda], [\mu] \) are the corresponding classes in \( H^2(\text{Hilb}_n, \mathbb{Q}) \) associated to the partitions \( \lambda \) and \( \mu \) in \( \mathcal{P}(n) \), we proceed by induction on the degree \( d \) as in section 3.6 of [OP]. \( \square \)

**Remark 3.8.** If we choose the partition \( \nu \) to be the empty partition \( \emptyset \), we recover the relative Gromov-Witten invariants \( N_d, g(\lambda, \mu) \) studied by Fomin and Mikhalkin in [FM], and by Caporaso and Harris in [CH].

## 4. Configurations of points over a rational normal curve

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 \( G \to \text{GL}(V) \). We denote by \( S^d V \) the \( d \)-th symmetric power of \( V \).

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

\[
P^V* \to \mathbb{P} S^d V^*
\]

\( v \mapsto v^d, \)

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 \( \left\{ \frac{n!}{k!(n-k)!} \alpha^k \beta^{d-k} \right\} \) for \( S^d V^* \) and expanding out \((x\alpha + y\beta)^d\), we see that in coordinates this map may be given as

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

Goppa recognized that the Gale transform of a configuration of \( n \) distinct points supported on a rational normal curve in \( \mathbb{P}^d \) is a configuration of points supported on a rational normal curve on \( \mathbb{P}^{n-d-2} \).

In particular, the homogeneous coordinate ring for the natural projective embedding of the GIT quotient \( (\mathbb{P}^d)^n / \text{SL}_{d+1} \) is the ring of invariants for \( n \) ordered points in the projective space up to projectivity. 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:

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

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

\[
\varphi : \tilde{M}_{0,n} \to (\mathbb{P}^d)^n / c \text{SL}_{d+1},
\]
sending a configuration of distinct points on \( \mathbb{P}^1 \) to the corresponding configuration under the \( d^{th} \) Veronese map.

The symmetric power \( \text{Sym}^n C_d \) of the curve \( C_d \) is the quotient of the configuration space \( C_n^d \) of \( n \) unordered tuples of points on the rational normal 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 \( \text{Sym}^n C \), that is, \( \text{Sym}^n C \) represents the functor of families of effective divisors of degree \( n \) on \( C \).

**Why codes on the rational normal curve?** By definition, the rational normal curve \( C_d \) is the image by the \( d-1 \)-Veronese embedding of \( \mathbb{P}V^* = \mathbb{P}^1 \) where \( V \) is a 2-dimensional vector space. The action of \( \text{PGL}(2,k) \) 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 \( \text{PGL}(2,k) \). Thus the problem of classifying codes on the rational normal curve is reduced to study finite groups of the projective linear group \( \text{PG}(2,k) \) or the symmetric group \( S_n \).

In more concrete terms, one can consider the action of finite subgroups of \( S_n \) on configuration of points on the rational normal curve \( C_d \).

**Proposition 4.1.** If we consider the set of orbits of \( C_n^d \) by the action of finite subgroups of the symmetric group \( S_n \), we get all possible divisor classes in the group \( \text{Div}^n(C_d) \) 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 \( C_n^d \) of \( n \) points on the rational normal 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 \( S_4 \).

\[ \square \]

5. Notion of collinearity on the rational normal curve

**Definition 5.1.** An incidence structure \( S \) 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 \( (p, q) \in \mathbb{P}^2(V^*) \), there exists an \( r \in \mathcal{P}(\mathbb{P}^dV^*) \) 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.
Definition 5.2. (1) A \((k; r)\)-arc \(K\) in \(\text{PG}(2, p)\) 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 \(K\) 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 \(\text{PG}(n, p)\) 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:

\[
\mathcal{V}_1^n := \left\{ \mathbb{F}_q(1, x, x^2, \ldots, x^n) \mid x \in \mathbb{F}_q \cup \{ \infty \} \right\}.
\]

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

\[
\mathbb{F}_p(x_0, \ldots, x_n) \rightarrow \mathbb{F}_p(a^0 x_0, \ldots, a^n x_n),
\]
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 \(\Omega(j) = \{ m \in \mathbb{N} \mid 0 \leq m \leq n, \binom{n}{m} \equiv 0 \mod p \}\). Given

\[
J \subset \{0, 1, \ldots, n\}, \text{ put } \Omega(J) = \bigcup_{j \in J} \Omega(j), \text{ and } \Psi(J) := \bigcup_{j \notin J} \{j, n - j\}.
\]

Both \(\Omega\) and \(\Psi\) are closure operators on \(\{0, 1, \ldots, n\}\). Likewise the projective collineation \(\mathbb{F}_p(x_0, x_1, \ldots, x_n) \rightarrow \mathbb{F}_p(x_n, x_{n-1}, \ldots, x_0)\) leaves the NRC invariant whence \(\Lambda\) has to be closed with respect to \(\Psi\).

Proposition 5.3. 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 \(kc\lambda\), where \(\lambda \in \mathcal{P}(t)\).

Proof. Let

\[
E^t_n := \{(e_0, e_1, \ldots, e_n) \in \mathbb{N}^{n+1} \mid e_0 + e_1 + \ldots + e_n = t \},
\]

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

\[
\{c_{e_0, e_1, \ldots, e_n} \in \mathbb{F}_q : (e_0, e_1, \ldots, e_n) \in E^t_n\}.
\]

Let’s call \(\mathcal{V}^t_n\) the Veronese image under the Veronese mapping given by:

\[
\mathbb{F}_p \left( \sum_{i=0}^{n} x_i b_i \right) \rightarrow \mathbb{F}_p \left( \sum_{E^t_n} c_{e_0, e_1, \ldots, e_n} x^{e_0} x_1^{e_1} \cdots x_n^{e_n} \right), \quad x_i \in \mathbb{F}_p.
\]
The Veronese image of each \( r \)-dimensional subspace of \( PG(n, p) \) is a sub-Veronesean variety \( V^d_r \), and all those subspaces are indexed by partitions in \( P(t) \). Thus by a Theorem due to Gmainer are invariant under the collineation group of the normal rational curve, (see \([\text{Hav1}]\)).

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 \( \text{Gal}(l/k) \).

\[
\square
\]

5.1. An application: three-point codes on the rational normal curve.
As we showed in Proposition 5.3, each subspace invariant under collineation of the NRC is indexed by a partition \( \lambda \in P(d) \). Let us call the base point associated to the partition \( \lambda \) as \( P_\lambda \).

**Theorem 5.4.** Let \( \sigma_1, \sigma_2, \sigma_3 \) be three generators for the symmetric group \( S_3 \) and let \( \lambda_1, \lambda_2 \) and \( \lambda_3 \) be the partitions of \( d \) indexing the corresponding irreducible representations in \( SL(\mathbb{F}_q, n) \). Then we can recover all the algebraic codes defined over the NRC as linear combination of the base points \((P_\lambda_1)_{1 \leq i \leq 3}\) on the NRC.

**Proof.** Consider the divisors associated to the rational maps \( f(x, y, z) = nx + my + lz \) defined over the rational normal curve \( C_d \) defined over \( \mathbb{F}_q \), with \( n, m \) and \( l \) integer numbers. In particular, if \( d|q^2 - 1 \), the points \( P = (\alpha, 0, 0), Q = (\beta, 0, 0) \) 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 4.1 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 \( \sigma_1, \sigma_2 \) and \( \sigma_3 \), the divisor is a linear combination of the base points \((P_\lambda_i)_{1 \leq i \leq 3}\) on the NRC.

\[
\square
\]

6. APPENDIX A: Explicit presentation of 3-point codes
Given sets \( I, J, K \subset \{0, 1, \ldots, n\} \), of cardinality \( r \), we can associate to them partitions \( \lambda, \mu \) and \( \nu \) 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 \( c_\lambda, c_\mu \) and \( c_\nu \), whenever the corresponding Littlewood-Richardson coefficient \( c^k_{\lambda, \mu} \) is positive. Next, we give an algorithm to compute the Littlewood-Richardson coefficients \( c^k_{\lambda, \mu} \). Horn defined sets of triples \((I, J, K)\) by the following inductive procedure (see \([\text{Fu}]\)):

\[
U^p_I = \{(I, J, K) | \sum_{i \in I} + \sum_{j \in J} + \sum_{k \in K} = k + r(r + 1)/2\},
\]

\[
T^p_I = \{(I, J, K) \in U^p_I | \text{ for all } p < r \text{ and all } (F, G, H) \in T^p_p, \sum_{f \in F} i_f + \sum_{g \in G} j_g = \sum_{h \in H} k_h + p(p + 1)/2\}.
\]

Here we present a **Sage-Python** code calculating the \( U^n_I \) and \( T^n_I \) index sets. Then we provide some presentations.
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))]

• the sorted() mapping function in getUnr() is necessary because the order of elements in Subsets is unknown;
• in index_filter() 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 downside of calculating a function that is already heavily recursive;
• results are limited by constraints Python has on recursive function calls;
• the filtering performed on $U^n_r$ to get $T^n_r$ is implemented by two nested calls to all()
\[
\begin{array}{|c|c|c|}
\hline
(n, r) & U^n_r (\# denotes the cardinality of U^n_r) & T^n_r (\# denotes the cardinality of T^n_r) \\
\hline
(2, 1) & ([1], [1], [1]), ([1], [2], [2]), \# = 3 & ([1], [1], [1]), ([1], [2], [2]), \# = 3 \\
\hline
(3, 1) & ([1], [1], [1]), ([1], [2], [2]), ([1], [3], [3]), \# = 3 & ([1], [1], [1]), ([1], [2], [2]), ([1], [3], [3]), \# = 3 \\
\hline
(3, 2) & ([1], [1], [1]), ([1], [2], [2]), ([1], [3], [3]), \# = 6 & ([1], [1], [1]), ([1], [2], [2]), ([1], [3], [3]), \# = 6 \\
\hline
(4, 1) & ([1], [1], [1]), ([1], [2], [2]), ([1], [3], [3]), \# = 6 & ([1], [1], [1]), ([1], [2], [2]), ([1], [3], [3]), \# = 6 \\
\hline
(4, 2) & ([1], [1], [1]), ([1], [2], [2]), ([1], [3], [3]), \# = 10 & ([1], [1], [1]), ([1], [2], [2]), ([1], [3], [3]), \# = 10 \\
\hline
(4, 3) & ([1], [1], [1]), ([1], [2], [2]), ([1], [3], [3]), \# = 14 & ([1], [1], [1]), ([1], [2], [2]), ([1], [3], [3]), \# = 14 \\
\hline
\end{array}
\]
References

[BGL] E. Bifet, F. Ghione and M. Leticia, On the Abel-Jacobi map for divisors of higher rank on a curve, Math. Ann. 299 (1994), no. 4, 641-672.

[BM1] A. Besana, C. Martínez, Enumerative geometry of the curves defined by $y^d = f(x)$, arXiv:1111.6456.

[BM2] A. Besana, C. Martínez, Some remarks on cyclic covers of the projective line over finite fields, arXiv:1202.5221.

[CT] M. Chara, R. Toledano, Rational places in extensions and sequences of function fields of Kummer type, Journal of Pure and Applied Algebra 215 (2011) 2603-2614.

[CH] L. Caporaso and J. Harris, Counting plane curves of any genus, Invent. Math. 131 (1998), 345392.

[FM] S. Fomin, G. Mikhalkin, Label floor diagrams for plane curves, J. Eur. Math. Soc. 12, 1453-1496.

[Fu] W. Fulton, Eigenvalues, invariant factors, highest weights and Schubert calculus, math.AG/9908012.

[GT] M. Giulietti and F. Torres, On dense sets related to plane algebraic curves, Arxiv. Combin. LXII (2004), 33-40.

[Hav1] H. Havlicek, Veronese varieties over fields with non-zero characteristic: a survey, Discrete Mathematics, 267 (2003), 159-173

[Hav2] H. Havlicek, The Veronese surface in $PG(5,3)$ and Witt’s $5-(12,6,1)$-design, J. Comb. Theory Ser. A 84 (1998), 87-94.

[Hirs] J. W. P. Hirschfeld, Projective Geometries over finite fields, (1998) Oxford Mathematical Monographs.

[MTR] F. Manganiello, A. L. Trautmann, J. Rosenthal, On conjugacy classes of subgroups of the general linear group and cyclic orbit codes, IEEE International Symposium on Information Theory proceedings (ISIT), 2011 : July 31, 2011 - Aug. 5, 2011, St. Petersburg, Russia.

[Man] Y. Manin, Combinatorial cubic surfaces and reconstruction theorems, arXiv: 1001.0223.

[Ma] L. Manivel, On rectangular Kronecker coefficients, Journal of Algebraic Combinatorics 33 (2011), 153-162.

[OP] A. Okounkov, P. Pandharipande, Quantum cohomology of the Hilbert scheme of points in the plane, Invent. Math. 179 (2010), 523-557.

[S] http://www.sagemath.org/

[SLL] F. Sottile, T. Lam, A. Lauve, A skew Littlewood-Richardson rule from Hopf algebras, IMRN 2010.