Schubert Calculus over Finite Fields and Random Network Codes

Anna-Lena Trautmann

Institute of Mathematics
University of Zurich

ALCOMA10
Thurnau, April 12-17 2010

Outline

Plücker Embedding

Let M^* be the $k \times n$-matrix representation of $M \in G(k,n)$. The maximal minors of M^* constitute the *Plücker coordinates* of the subspace M. They embed $G(k,n)$ into the projective space $\mathbb{P}^{\binom{n}{k}-1}$.

Plücker coordinates in $G(2,4)$

$$M^* = \begin{bmatrix} a_0 & a_1 & a_2 & a_3 \\ b_0 & b_1 & b_2 & b_3 \end{bmatrix}$$

$$x_{i,j} := a_i b_j - a_j b_i$$

the Plücker coordinates are $[x_{1,2} : x_{1,3} : x_{1,4} : x_{2,3} : x_{2,4} : x_{3,4}]$.

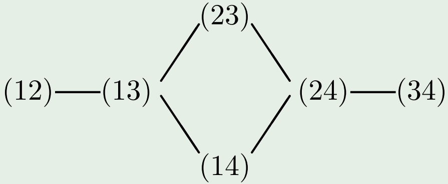
Bruhat Order

Let $\binom{[n]}{k}$ denote the set of all ordered multiindices of length k of the numbers between 1 and n and let $\alpha, \beta \in \binom{[n]}{k}$. The *Bruhat order*

$$\alpha \leq \beta \ \Leftrightarrow \ \alpha_i \leq \beta_i \quad \forall\, i = 1, ..., k$$

is a partial order on $\binom{[n]}{k}$.

Bruhat order on $\binom{[4]}{2}$



The *straightening syzygies* form a minimal Gröbner basis for the Plücker ideals (i.e. the Grassmann variety embedded in projective space via the Plücker coordinates).

Gröbner basis of $G(2,4)$:

$$x_{14}x_{23} - x_{13}x_{24} + x_{12}x_{34}$$

Gröbner basis of $G(2,5)$:

$$x_{14}x_{23} - x_{13}x_{24} + x_{12}x_{34}$$

$$x_{15}x_{24} - x_{14}x_{25} + x_{12}x_{45}$$

$$x_{15}x_{34} - x_{14}x_{35} + x_{13}x_{45}$$

$$x_{15}x_{23} - x_{13}x_{25} + x_{12}x_{35}$$

$$x_{25}x_{34} - x_{23}x_{45} + x_{24}x_{35}$$

Schubert Cells

A *Schubert cell* C_α is the set of all subspaces such that the leading ones (pivots) of the reduced row-echelon form of the matrix representations are in positions $x_{\bar{\alpha}} := n+1-\alpha_k, ..., n+1-\alpha_1$ (i.e. positions α_i counted from right to left).
This is equivalent to saying that all minors $x_{\bar{\beta}}$ where β is greater than or not comparable to α in the Bruhat order have to be zero:

Definition

$$C_\alpha := \{M \in G_{k,n} : x_{\bar{\alpha}} = 1, x_{\bar{\beta}} = 0 \; \forall \beta \not\leq \alpha\}$$

Schubert cells in $G(2,4)$

$$C_{1,3} = \begin{bmatrix} 0 & 1 & * & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \qquad C_{2,3} = \begin{bmatrix} 0 & 1 & 0 & * \\ 0 & 0 & 1 & * \end{bmatrix}$$

Theorem

The size of a Schubert cell is

$$|(C_\alpha)| = q^{\sum_{i=1}^{k} \alpha_i - i}$$

Schubert Systems

Let $A_1, ..., A_d$ be a flag of linear subspaces of $\mathbb{F}_q^n$ with respective dimensions $\alpha_1, ..., \alpha_d$:

$$A_1 \subset A_2 \subset ... \subset A_d$$

$$0 \leq \alpha_1 < \alpha_2 < ... < \alpha_d \leq n$$

Definition

Schubert system:

$$\Omega_{A_1,...,A_k} := \{B \in G(k,n) | \dim(B \cap A_j) \geq j\}$$

If we choose the flag to be of standard form (from the right), i.e. $A_i = E_i := \langle e_{n-i+1}, ..., e_n \rangle$, we may write

$$\Omega_{\alpha_1,...,\alpha_k} := \Omega_{E_{\alpha_1},...,E_{\alpha_k}}$$

Theorem

$$\Omega_\alpha = \bigcup_{\beta \leq \alpha} C_\beta = \{M \in G_{k,n} : x_{\bar{\beta}} = 0 \ \forall \beta \not\leq \alpha\}$$

i.e. the Schubert system Ω_α is the union of all reduced row-echelon forms with leading ones in positions $n+1-\beta_k, ..., n+1-\beta_1$, where $\beta \leq \alpha$.

Corollary

A Schubert system is an algebraic projective variety of size

$$|\Omega_\alpha| = \frac{1}{q^{k(k+1)/2}} \sum_{\beta \leq \alpha} q^{\sum_{i=1}^{k} \beta_i}$$

Schubert Varieties in Network Coding

Theorem

Let $A = \langle e_{n-k+1}, \ldots, e_n \rangle$ *(standard flag) and*

$$\alpha_1 = d+1, \alpha_2 = d+2, \ldots, \alpha_{k-d-1} = k-1$$

$$\alpha_{k-d} = k$$

$$\alpha_{k-d+1} = n-d+1, \ldots, \alpha_{k-1} = n-1, \alpha_k = n$$

Then

$$B_{2d}(A) = \Omega_{\alpha_1, \ldots, \alpha_k}$$

Example in $G(2,4)$

Let $A = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$ and $d = 1$. Then

$$\alpha_1 = \alpha_{k-d} = k = 2 \qquad \alpha_2 = \alpha_k = n = 4$$

$$\begin{aligned} B_2(A) = \Omega_{2,4} &= \{B \in G(2,4) | x_{\bar{\beta}} = 0, \beta \not\leq (2,4)\} \\ &= \{B \in G(2,4) | x_{\bar{3}\bar{4}} = 0\} \\ &= \{B \in G(2,4) | x_{12} = 0\} \end{aligned}$$

For $d = 2$ we get

$$\alpha_1 = \alpha_{k-1} = n - 1 = 3 \qquad \alpha_2 = \alpha_k = n = 4$$

$$B_4(A) = \{B \in G(2,4) | x_{\bar{\beta}} = 0, \beta \not\leq (3,4)\} = G(2,4)$$

$B_2(A)$ in Plücker coordinates (RREF):

$$[0:0:0:0:0:1], [0:0:0:0:1:*], [0:0:0:1:*:*'],$$

$$[0:0:1:0:*:*'], [0:1:*:*':-(*\cdot *'):*'']$$

$B_2(A)$ in representation matrices (RREF):

$$\begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & * & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 & * \\ 0 & 0 & 1 & *' \end{pmatrix}$$

$$\begin{pmatrix} 1 & * & *' & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & * & 0 & *' \\ 0 & 0 & 1 & *'' \end{pmatrix}$$

Question: How can we describe balls around non-standard-subspaces?

Theorem

The subspace distance remains the same under $GL(n,q)$-action, i.e.

$$d_S(U,V) = d_S(U \cdot T, V \cdot T)$$

for an invertible $n \times n$-matrix T.

Thus, if we know $B_{2d}(U)$ we also know $B_{2d}(V)$ for $V = U \cdot T$:

$$B_{2d}(U) = \{M : \dim(U \cap M) \geq k-d\}$$

$$\Leftrightarrow \; B_{2d}(V) = \{M \cdot T : \dim(U \cap M) \geq k-d\}$$

$GL(n)$-actions in Plücker coordinates

Let $U \in G(k,n)$, $\hat{U}$ its corresponding element in $\mathbb{P}^{\binom{n}{k}-1}$ (i,e. its Plücker coordinates) and $T \in GL(n)$. Define

$$\hat{T} := \begin{bmatrix} \hat{t}_{11} & \dots & \hat{t}_{1\binom{n}{k}} \\ \vdots & & \vdots \\ \hat{t}_{\binom{n}{k}1} & \dots & \hat{t}_{\binom{n}{k}\binom{n}{k}} \end{bmatrix}$$

where $\hat{t}_{ij}$ is the $k \times k$-minor of T with rows denoted by the i-th element of $\binom{[n]}{k}$ and columns denoted by the j-th element of $\binom{[n]}{k}$. Then it holds that

Theorem

$$V = U \cdot T \;\;\Rightarrow\;\; \hat{V} = \hat{U} \cdot \hat{T}$$

This implies that

Corollary

$$x_\alpha^V = \sum_{l \in \binom{[n]}{k}} x_l^U x_\alpha^{T_l}$$

where $x_\alpha^{T_l}$ denotes the $k \times k$-minor of T involving rows $l_1, ..., l_k$ and columns $\alpha_1, ..., \alpha_k$.

This way one can translate the linear conditions of $B_{2d}(A)$ (for A standard) to arbitrary elements of $G(k, n)$.

Example in $G(2,5)$

$$A = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$$B_4(A) = \Omega_{25} = \{M \in G(k,n) : x_{12} = x_{13} = x_{23} = 0\}$$

We choose

$$B = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

We compute S fulfilling $A = B \cdot S$:

$$S = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

We use the formula for the Plücker coordinates:

$$x_{12}^A = \sum_{l \in \binom{[5]}{2}} x_l^A x_{12}^{S_l} = x_{45}^B$$

$$x_{13}^A = \sum_{l \in \binom{[5]}{2}} x_l^A x_{13}^{S_l} = x_{14}^B$$

$$x_{23}^A = \sum_{l \in \binom{[5]}{2}} x_l^A x_{23}^{S_l} = x_{15}^B$$

hence

$$B_4(B) = \{M \in G(k,n) : x_{14} = x_{15} = x_{45} = 0\}$$

Code Construction

Construction 1

1. choose $A_1 =< e_1, ..., e_k >$
2. construct $B_{2d}(A_1)$
3. choose $A_2 \notin B_{2d}(A_1)$
4. construct $B_{2d}(A_2)$
5. choose $A_3 \notin B_{d2}(A_1) \cup B_{2d}(A_2)$

$\vdots$

6. until $B_{2d}(A_1) \cup B_{2d}(A_2) \cup ... \cup B_{2d}(A_l) = G(2, n)$

Construction 2

For constructing a code with minimum distance $2d$ we have to find elements such that the balls around these of radius $d-1$ do not intersect pairwise.

This construction only works for $d \equiv 1 \mod 2$ and $k \geq 3$, because

- The radius of a ball is a multiple of 2 and is equal to $d-1$.
- It holds that $k \geq d$, thus $d = 1$ and the ball of radius $d - 1 = 0$ is just the element itself.

For any $A, B \in G(k,n)$ there exists a (non-unique) $T \in GL(n)$ such that $B = A \cdot T$. The Grassmannian $G(k,n)$ is an orbit of any of its elements under $GL(n)$.

Theorem

$$Stab(A) := \{g \in GL(n) | A \cdot g = A\}$$

$$G(k,n) \cong GL(n)/Stab(A)$$

Similarly a Schubert cell is an orbit under the action of upper triangular matrices. Let C_α^0 be the matrix with pivots in positions $\bar{\alpha}$ and all other entries 0,

$$C_\alpha = \{C_\alpha^0 \cdot g | g \in UT(n) \subset GL(n)\}$$

$$C_\alpha \cong UT(n)/Stab(C_\alpha^0)$$

Orbit Codes

Definition

Let $A \in G(k,n)$ be fixed and G a (multiplicative) subgroup of $GL(n)$. Then

$$C = \{A \cdot g | g \in G\}$$

is called an *orbit code* and it holds

$$d_S(C) = \min_{g \in G \setminus Stab(A)} d_S(A, A \cdot g)$$

Theorem

The dual code of an orbit code is an orbit code.

$$C = \{A \cdot g | g \in G\} \subseteq G(k,n) \Leftrightarrow C^{\perp} = \{A^{\perp} \cdot g | g \in G\} \subseteq G(n-k,n)$$

Cyclic Orbit Codes

Example over $\mathbb{F}_2$

Let G be the group generated by

$$g := \begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix}$$

and

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

Then $C = \{A \cdot g | g \in G\} = \{A \cdot g^i\}$ is an $[4, 4, 4, 2]$-code.

Reed-Solomon-like Codes

Let $U = \{U_i\}$ be an additive subgroup of $Mat_{k\times n-k}$ such that all elements are of rank $\geq 2\delta - k$ and

$$G_i = \left(\begin{array}{c|c} I_{k\times k} & U_i \\ \hline 0 & I_{n-k\times n-k} \end{array}\right)$$

and G be the group generated (multiplicatively) by all G_i.

Theorem

$$C = \{A \cdot g | g \in G\}$$

is a $[n, 2\delta, |U|, k]$-code. If $U = GAB(k \times n - k)$ (Gabidulin rank-metric-codes) it is exactly the Reed-Solomon-like code (Koetter and Kschischang).

Proof.
Any element of G has the shape of G_i

$$\left(\begin{array}{c|c} I & U_{i_1} \\ \hline 0 & I \end{array}\right) \cdot \left(\begin{array}{c|c} I & U_{i_2} \\ \hline 0 & I \end{array}\right) = \left(\begin{array}{c|c} I & U_{i_1} + U_{i_2} \\ \hline 0 & I \end{array}\right)$$

Then

$$A \cdot G_i = \left[\begin{array}{cc} I & U_i \end{array}\right]$$

and

$$d_S(A, A \cdot G_i) = rank \left[\begin{array}{cc} I_{k\times k} & 0 \\ I_{k\times k} & U_i \end{array}\right] = k + rank(U_i)$$

Known result: The RS-like codes correspond to the lifting of Gabidulin codes. $\square$

Spread Codes

Let $n = 2k$ and $U = F_q[P]$ be the F_q-algebra of a companion matrix of an irreducible polynomial.

$$G_1^i = \left(\begin{array}{c|c} I & U_i \\ \hline 0 & I \end{array}\right) \qquad G_2 = \left(\begin{array}{c|c} 0 & I \\ \hline I & 0 \end{array}\right)$$

and G be the group generated (multiplicatively) by all G_1^i and G_2.

Theorem

$$C = \{A \cdot g | g \in G\}$$

is exactly the $[n, n, \frac{q^n-1}{q^{n/2}-1}, n/2]$-spread code. (Manganiello, Gorla, Rosenthal)

Proof.
The blocks are always a linear combination of $0, I$ and elements of U, thus each block is again an element of U. Letting G act on A we get elements of the shape

$$\begin{bmatrix} U_i & U_j \end{bmatrix}$$

If U_i is non-zero

$$\text{rowspace}\begin{bmatrix} U_i & U_j \end{bmatrix} = \text{rowspace}\begin{bmatrix} I & U_i^{-1} \cdot U_j \end{bmatrix}$$

$\square$

Remark

The construction can be generalized to $n = j \cdot k$ and works for U being any subgroup of $GL(n/j)$ with field structure.

Thank you for your attention!