Spread codes and the Klein correspondence

Klara Stokes

Joint work with Axel Hultman

Classical coding theory: a code is a set of vectors over a finite field $\mathbb{F}_q$.

Subspace code: a code is a set of subspaces of a vector space over $\mathbb{F}_q$.

This talk is on error-correction in certain subspace codes.

Notation.

- **Rank** will denote the dimension of a vector space, and
- **Dimension** will denote the dimension of a projective space.

Let $V = V(n+1, \mathbb{F}_q)$ be a vector space of rank $n+1$ over the finite field $\mathbb{F}_q$.

The Grassmannian $Gr_q(k+1, n+1)$ is the set of subspaces of rank $k+1$ of V.

A subspace of $V(n+1, \mathbb{F}_q)$ of rank $k+1$ corresponds to a projective subspace of dimension k of the projective geometry $PG(n, \mathbb{F}_q) := \mathbb{P}(V(n+1, \mathbb{F}_q))$.

Example. $V(4, \mathbb{F}_q)$ and $PG(3, \mathbb{F}_q)$

Grassmannian	In $V(4, \mathbb{F}_q)$	In $PG(3, \mathbb{F}_q)$
$Gr_q(1, 4)$	Rank 1	Dim 0 (Points)
$Gr_q(2, 4)$	Rank 2	Dim 1 (Lines)
$Gr_q(3, 4)$	Rank 3	Dim 2 (Planes).

The Plücker embedding is a map

$$
\begin{array}{rcl}
Pl: \quad Gr(n+1, k+1) & \rightarrow & \mathbb{P}\left(\bigwedge^{k+1} V(n+1, \mathbb{F}_q)\right) \\
\langle v_1, \ldots, v_{k+1} \rangle & \mapsto & [v_1 \wedge \cdots \wedge v_{k+1}]
\end{array}
$$

embedding the Grassmannian in the projectivisation of the exterior algebra $\bigwedge^{k+1} V(n+1, \mathbb{F}_q)$.

$\bigwedge^{k+1} V(n+1, \mathbb{F}_q)$ is a vector space of rank $\binom{n+1}{k+1}$, and its non-zero directions is $PG(\binom{n+1}{k+1} - 1, \mathbb{F}_q)$.

It is well-known that the Plücker embedding makes the Grassmannian a smooth algebraic variety of $PG(\binom{n+1}{k+1} - 1, \mathbb{F}_q)$ defined by the intersection of quadrics.

Its points are the totally decomposable vectors of $\bigwedge^{k+1} V(n+1, \mathbb{F}_q)$.

Example.
The Grassmannian

$$Gr_q(2,4) = \{\langle u, v\rangle : u \neq v \in V(4, \mathbb{F}_q)\},$$

of lines in $PG(3, \mathbb{F}_q)$, is embedded in $PG(5, \mathbb{F}_q)$ with Plücker coordinates

$$Q = \left\{ (x_{01} : x_{02} : x_{03} : x_{12} : x_{13}, x_{23}) : x_{ij} = \det \begin{pmatrix} u_i & u_j \\ v_i & v_j \end{pmatrix} \right\}.$$

The points in Q are the points on the Klein quadric defined by

$$x_{01}x_{23} - x_{02}x_{13} + x_{03}x_{12} = 0.$$

This is a hyperbolic quadric in $PG(5, \mathbb{F}_q)$.

A subspace code is a set of projective subspaces of $PG(n, \mathbb{F}_q)$.

A **constant-dimension subspace code** of rank (vector dimension) $k+1$ is a subspace code contained in the Grassmannian $Gr_q(k+1, n+1)$, (i.e. a set of projective subspaces of dimension k).

As in classical coding theory, error-correction in subspace codes requires the codewords to be taken well-separated according to some distance.

The subspace distance between two subspaces A, B in a vector space V:

$$d(A, B) = \dim(A) + \dim(B) - 2\dim(A \cap B).$$

It measures the shortest distance between A and B in the inclusion lattice of projective subspaces of $PG(n, \mathbb{F}_q)$.

Example. In $V = PG(3, \mathbb{F}_q)$ the maximal possible distance between two codewords is 4, and this bound is attained by a set of lines with pairwise empty intersection.

A *spread* in $PG(3, \mathbb{F}_q)$ is a set of lines such every point belongs to exactly one of the lines.

In general, a spread (*t-spread*) in $PG(n, \mathbb{F}_q)$ is a set of subspaces of dimension t forming a partition of the point set.

There is a t-spread in $PG(n, \mathbb{F}_q)$ if and only if $(t+1)|(n+1)$.

Spreads (and partial spreads) have been used as subspace codes for network coding [Manganiello-Gorla-Rosenthal 2008].

There exist several decoding algorithms.

A planar spread is a t-spread in $PG(n, \mathbb{F}_q)$ such that $2(t+1) = (n+1)$.

A planar spread defines a translation plane. If this plane is Desarguesian, then the spread is called Desarguesian.

Desarguesian spreads make good codes.

It is "well-known" that a Desarguesian spread is represented in the Grassmannian by a complete intersection of $Gr_q(t+1, n+1)$ with a linear subspace of $\bigwedge^{t+1} V(n+1, \mathbb{F}_q)$ of rank 2^t [i.e. Havlicek, or Lunardon].

Projectively this intersection is a **cap** in the intersecting subspace $U \cong PG(2^t - 1, \mathbb{F}_q)$: a set of points of which no three are collinear.

As we saw before, a line L in $PG(3, \mathbb{F}_q)$ corresponds to a point p_L in the Grassmannian $Gr_q(2,4)$, which is a projective algebraic variety known as the *Klein quadric* defined by

$$x_{01}x_{23} - x_{02}x_{13} + x_{03}x_{12} = 0.$$

The coordinates of the point p_L is given by the Plücker embedding

$$Pl(\langle u, v\rangle) = (x_{01} : x_{02} : x_{03} : x_{12} : x_{13}, x_{23})$$

where

$$x_{ij} = \det \begin{pmatrix} u_i & u_j \\ v_i & v_j \end{pmatrix}.$$

A spread S in $PG(3, \mathbb{F}_q)$ is represented through this embedding as a smooth intersection between $Pl(Gr_q(2,4))$ and a linear subspace $U \cong PG(3, \mathbb{F}_q)$.

Let $Q : x_{01}x_{23} - x_{02}x_{13} + x_{03}x_{12} = 0$ and $U : \begin{cases} x_{01} + x_{23} = 0 \\ x_{02} - x_{13} = 0. \end{cases}$

If $q = 3$ then $Q \cap U$ consists of the following points in $PG(5, 3)$:

$$\begin{array}{ll} p_{L_1} = (0:0:2:0:0:0) & p_{L_2} = (1:0:1:1:0:2) \\ p_{L_3} = (1:1:2:1:1:2) & p_{L_4} = (1:2:2:1:2:2) \\ p_{L_5} = (1:0:2:2:0:2) & p_{L_6} = (1:1:1:2:1:2) \\ p_{L_7} = (1:2:1:2:2:2) & p_{L_8} = (0:2:2:2:2:0) \\ p_{L_9} = (0:2:1:1:2:0) & p_{L_{10}} = (0:0:0:2:0:0) \end{array}$$

which are the Plücker coordinates of the following lines in $PG(3, 3)$:

$$\begin{array}{l} L_1 = \{(1:0:0:0),(0:0:0:1),(1:0:0:1),(2:0:0:1)\}, \\ L_2 = \{(2:1:1:1),(2:0:1:0),(0:1:0:1),(1:1:2:1)\}, \\ L_3 = \{(1:2:1:0),(0:2:2:1),(2:0:1:1),(1:1:0:1)\}, \\ L_4 = \{(2:1:0:1),(0:2:1:1),(1:1:1:0),(1:0:2:1)\}, \\ L_5 = \{(0:2:0:1),(1:0:1:0),(1:2:1:1),(2:2:2:1)\}, \\ L_6 = \{(2:2:1:0),(1:2:0:1),(2:0:2:1),(0:1:1:1)\}, \\ L_7 = \{(0:1:2:1),(2:2:0:1),(1:0:1:1),(2:1:1:0)\}, \\ L_8 = \{(1:1:1:1),(2:2:1:1),(0:0:1:1),(1:1:0:0)\}, \\ L_9 = \{(2:1:2:1),(1:2:2:1),(0:0:2:1),(2:1:0:0)\}, \\ L_{10} = \{(0:0:1:0),(0:1:0:0),(0:1:1:0),(0:2:1:0)\} \end{array}$$

The Klein quadric, being a hyperbolic quadric in five dimensions, contains points, lines and planes (but no 3-spaces). The planes can be partitioned into two classes (called Greek and Latin) using the relation:

$$\pi_1 \sim \pi_2 \quad \Leftrightarrow \quad \pi_1 = \pi_2 \text{ or } \pi_1 \cap \pi_2 \text{ is a point}$$

- The set of lines through a given a point p in $PG(3, \mathbb{F}_q)$ defines a Latin plane.
- The set of lines contained in a given plane P in $PG(3, \mathbb{F}_q)$ defines a Greek plane.

The Klein correspondence

In $PG(3, \mathbb{F}_q)$		**In** $PG(5, \mathbb{F}_q)$
Lines	$\Leftrightarrow$	Points contained in the Klein quadric
Points	$\Leftrightarrow$	Latin planes contained in the Klein quadric
Planes	$\Leftrightarrow$	Greek planes contained in the Klein quadric

Let Q be the Klein quadric and let U be the 3-dimensional subspace defining the Plücker coordinates of the spread $Q \cap U$.

Decoding algorithm

$PG(3, \mathbb{F}_q)$		$PG(5, \mathbb{F}_q)$
Send a spread line L	$\Leftrightarrow$	Point $p_L \in Q \cap U$
Receive L with 1 error (point or plane)	$\Rightarrow$	Plane $\pi \subseteq Q$.
Line L that was sent.	$\Leftarrow$	Calculate $\pi \cap U = P_L$

Let Q be the Klein quadric and let U be the 3-dimensional subspace defining the Plücker coordinates of the spread $Q \cap U$.

Decoding algorithm

$PG(3, \mathbb{F}_q)$		$PG(5, \mathbb{F}_q)$
Send a spread line L	$\Leftrightarrow$	Point $p_L \in Q \cap U$
Receive L with 1 error (point or plane)	$\Rightarrow$	Plane $\pi \subseteq Q$.
Line L that was sent.	$\Leftarrow$	Calculate $\pi \cap U = P_L$

How? Just solve a system of two linear equations.

Sent data: spread line L.

Received data: L with "one error down in dimension", i.e. a point $p = (p0 : p_1 : p_2 : p_3) \in L$, represented by the vector $(p_0, p_1, p_2, p_3) \in V(F_q, 4) = \langle e_0, e_1, e_2, e_3 \rangle$.

How do we send the **point** p to the Grassmannian of **lines**?

Send the 4 lines through p in the directions of the base vectors!

$$\begin{aligned} q_0 &= p \wedge e_0 = (-p_1 : -p_2 : -p_3 : 0 : 0 : 0) \\ q_1 &= p \wedge e_1 = (p_0 : 0 : 0 : -p_2 : -p_3 : 0) \\ q_2 &= p \wedge e_2 = (0 : p_0 : 0 : p_1 : 0 : -p_3) \\ q_3 &= p \wedge e_3 = (0 : 0 : p_0 : 0 : p_1 : p_2) \end{aligned}$$

Only 3 points are linearly independent, so their span $X = \langle q_0, q_1, q_2, q_3 \rangle$ is a **plane** in $PG(5, \mathbb{F}_q)$ contained in the Grassmannian.

Let $x \in X = \langle q_0, q_1, q_2, q_3 \rangle$, then

$$x = (bp_0 - ap_1 : cp_0 - ap_2 : dp_0 - ap_3 : cp_1 - bp_2 : dp_1 - bp_3 : dp_2 - cp_3)$$

for some a, b, c, d.

Apply the equations definining U:

$$\begin{cases} bp_0 - ap_1 + dp_2 - cp_3 = 0 \\ cp_0 - dp_1 - ap_2 + bp_3 = 0 \end{cases}$$

But these are the defining equations (in a, b, c, d) of the sent line L!

What have we done?

We used the coordinates of the received point $p = (p_0 : p_1 : p_2 : p_3) \in L$ as coefficients of the equations defining L following the rules given by the defining equations of the spread.

No need passing over Plücker coordinates. Just plug in p_1, p_2, p_3, p_4.

In the lattice of subspaces of $PG(n, \mathbb{F}_q)$ two t-spread elements only meet in the empty set. Therefore their distance is twice their height in the lattice, i.e. $2t + 2$.

A t-spread subspace code in $PG(n, \mathbb{F}_q)$ can correct at most t errors.

A line spread in $PG(3, \mathbb{F}_q)$ can only correct one error. To correct more errors we need more dimension.

We would like an incidence correspondence in $Gr_q(t+1, 2(t+1))$, analogous to the Klein correspondence, for generalizing the decoding algorithm to t-spreads.

Note:

- Let A be a subspace of rank $m+1 \leq t+1$ of $V(2(t+1), \mathbb{F}_q)$.
- Let $\Omega(A)$ be the space of subspaces of rank $t+1$ intersecting A in a subspace of rank $x > 0$.
- Then $\Omega(A)$ is a Schubert variety.
- A Schubert variety is a linear section of the Plücker embedding of the Grassmannian.
  OBS! In general not a linear variety!

Let S be a t-spread code of $PG\left(\binom{2(t+1)}{t+1} - 1, \mathbb{F}_q\right)$, represented in the Grassmannian by the intersection of the linear subspace $U \cong PG(2^t, \mathbb{F}_q)$ and $Pl(Gr(t+1, 2(t+1)))$.

Decoding algorithm

To decode a codeword sent as $C \in S$ and received as a subspace A satisfying $d(C, A) < t+1$:

- Send A to $Pl(A) \subseteq Pl(Gr(t+1, 2(t+1))) \subseteq PG\left(\binom{2(t+1)}{t+1} - 1, \mathbb{F}_q\right)$ and consider its span $\langle Pl(A) \rangle$.
- Calculate $H = \langle Pl(A) \rangle \cap U$. Then H will be a linear subspace of $PG(\binom{2(t+1)}{t+1} - 1, \mathbb{F}_q)$.
- Calculate $H \cap Pl(Gr(t+1, 2(t+1))))$ (if necessary).

In practice, to send a subspace $A = \langle v_0, \dots, v_m \rangle$ of rank $m+1 \leq t+1$ of $V(2(t+1), t+1)$ to $Pl(Gr(2(t+1), t+1))$:

- take the $2(t+1)$ basis vectors $e_1, \dots, e_{2(t+1)}$ of V, and
- calculate (if non-zero)

$$Q_i = v_0 \wedge \cdots \wedge v_m \wedge e_{i_1} \wedge \cdots \wedge e_{i_{t-m}}$$

where the multiindexes $i = (i_1, \dots, i_{t-m})$ run over all $\binom{2(t+1)}{t-m}$ combinations of $(t-m)$ of the basis vectors.

In practice, to send a subspace $A = \langle v_0, \dots, v_m \rangle$ of rank $m+1 \leq t+1$ of $V(2(t+1), t+1)$ to $Pl(Gr(2(t+1), t+1))$:

- take the $2(t+1)$ basis vectors $e_1, \dots, e_{2(t+1)}$ of V, and
- calculate (if non-zero)

  $$Q_i = v_0 \wedge \cdots \wedge v_m \wedge e_{i_1} \wedge \cdots \wedge e_{i_{t-m}}$$

  where the multiindexes $i = (i_1, \dots, i_{t-m})$ run over all $\binom{2(t+1)}{t-m}$ combinations of $(t-m)$ of the basis vectors.

These points span the linear subspace $\langle Pl(A) \rangle$ intersecting $Pl(Gr(2(t+1), t+1))$.

By precalculating the points Q_i for a generic subspace A (as we did for the Klein quadric), we can calculate $H = \langle Pl(A) \rangle \cap U$ by solving a set of

$$\dim(U^{\perp}) = \binom{2t+2}{t+1} - 2^t$$

linear equations with coefficients from the vectors spanning A.

Only one of the points in H is totally decomposable.
That is the sent spread-codeword C.

Thank you for listening!