La construccion de codigos Goppa y codigos MDS formado por curvas algebraicas encima de superficies cubicas con 27 rectas sobre campos finitos de caracteristica p impar

Joel Barraza Nava

Colorado State University

March 21, 2024

Projective space: $\mathbf{PG(n, q)}$

- Dado V un espacio vectorial de dimension $(n+1)$ sobre un campo (field) F, el espacio proyectivo $\mathrm{PG}(n, F)$ de dimension n es el espacio cociente $V \backslash \{0\}$ definido por la relacion de equivalencia
$$x \sim y \Leftrightarrow x = \lambda y,$$
por un escalar $\lambda \in F \backslash \{0\}$.
- Por ejemplo, si $n = 2$, $\mathrm{PG}(2, F)$ es el plano proyectivo.
- Suponga que el campo F es un campo finito F_q de caracteristica impar (odd).

Points, lines, and planes in $\mathbf{PG(n, q)}$

- Los elementos de $\mathrm{PG}(n, q)$ son los puntos $\mathrm{P}(X)$ cuales son clases de equivalencia de un vector $X = (x_0, x_1, \ldots, x_n)$.
- Dos puntos $\mathrm{P}(X)$ y $\mathrm{P}(Y)$ determinan una recta (line) representada por un matriz,

$$\mathrm{L}\begin{bmatrix} X \\ Y \end{bmatrix}.$$

- Tres puntos $\mathrm{P}(X)$, $\mathrm{P}(Y)$, y $\mathrm{P}(Z)$ cuales no son colineales (collinear) determinan un plano representado por el matriz,

$$\pi\begin{bmatrix} X \\ Y \\ Z \end{bmatrix}.$$

Conics in $\mathbf{PG(2, q)}$

- Una conica en $\mathrm{PG}(2, q)$ es el conjunto de ceros de un polinomio homogeneo de grado 2 cual es dado por la ecuacion

$$a_0x_0^2 + a_1x_1^2 + a_2x_2^2 + a_3x_0x_1 + a_4x_0x_2 + a_5x_1x_2 = 0.$$

- Un $(5, 2)$-arco en el plano proyectivo es un conjunto de 5 puntos tal que cada recta interseca el conjunto en como maximo (at most) 2 puntos.
- Una conica por un $(5, 2)$-arco es una conica no degenerada (non-degenerate).

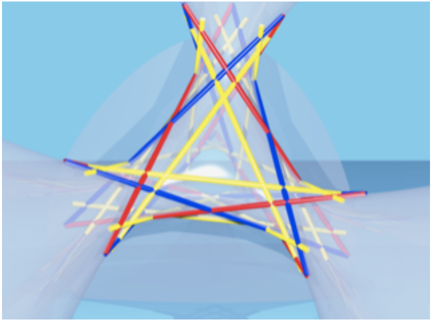
Conics from $(5,2)$-arcs on the projective plane $\mathbf{PG(2,q)}$

- Se sabe que una conica por 5 puntos $\{\mathrm{P}(U), \mathrm{P}(V), \mathrm{P}(X), \mathrm{P}(Y), \mathrm{P}(Z)\}$ impone (imposes) 5 condiciones linealmente independientes sobre el espacio de formas cuadraticas.
- Obtenemos un matriz de tamaño 5×6.

$$\begin{bmatrix} u_0^2 & u_1^2 & u_2^2 & u_0 u_1 & u_0 u_2 & u_1 u_2 \\ v_0^2 & v_1^2 & v_2^2 & v_0 v_1 & v_0 v_2 & v_1 v_2 \\ x_0^2 & x_1^2 & x_2^2 & x_0 x_1 & x_0 x_2 & x_1 x_2 \\ y_0^2 & y_1^2 & y_2^2 & y_0 y_1 & y_0 y_2 & y_1 y_2 \\ z_0^2 & z_1^2 & z_2^2 & z_0 z_1 & z_0 z_2 & z_1 z_2 \end{bmatrix}$$

- Calculamos el espacio nulo (nullspace) para obtener el sexto condicion linealmente independiente que determina la ecuacion del conico.

Cubic Surfaces with 27 lines



27 rectas del superficie Eckardt sobre los numeros reales

Superficie Eckardt

Cubic surfaces with 27 lines in $\mathbf{PG(3, q)}$

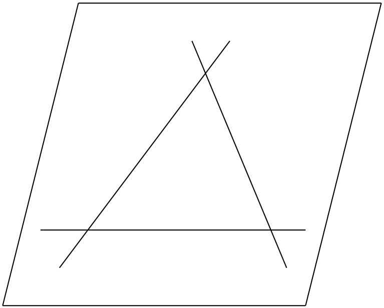
- Una superficie (surface) cubica suave $\mathcal{F}$ con 27 rectas es el conjunto de ceros de un polinomio homogeneo de grado 3 en 4 variables x_0, x_1, x_2, x_3.
- Una superficie $\mathcal{F}$ es determinada univocamente (uniquely) por un *6-doble de Schläfli* cual es una conjunto de 12 rectas repartidas entre dos conjuntos de 6 rectas.

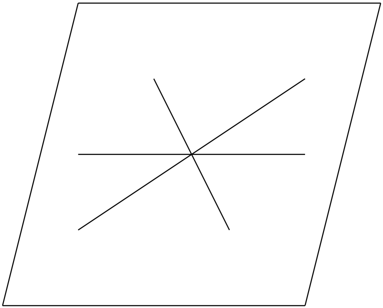
$$\begin{array}{cccccc} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ b_1 & b_2 & b_3 & b_4 & b_5 & b_6 \end{array}$$

- Cada par de lineas rectas de una fila son lineas sesgadas (skew lines) y la recta a_i interseca b_j cuando $i \neq j$.
- Del 6-doble obtenemos las otras 15 rectas del superficie $\mathcal{F}$ denotadas por c_{ij}

Tritangent planes

- Un *plano tres-tangente* (tritangent plane) es formado por 3 rectas del superficie $\mathcal{F}$, que ademas son coplanares.
- Las 3 lineas intersecan en tal manera que forman un triangulo o intersecan en un solo punto.
- Una superficie cubica $\mathcal{F}$ puede tener como maximo 45 planos tres-tangentes.

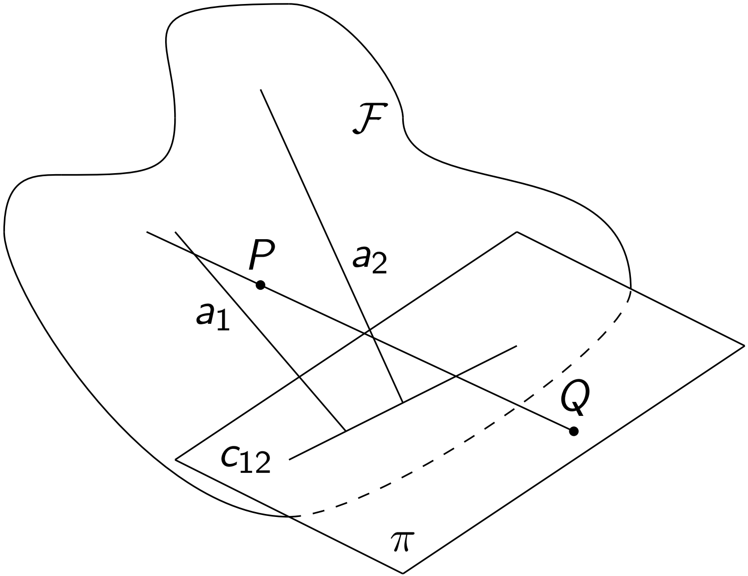




Birational maps

- Un $(6,2)$-arco denotado por $\mathcal{S}$ es no conica si el arco tiene como minimo un punto que no esta contenido en un conico.
- Una superficie cubica $\mathcal{F}$ es la explosion (blow-up) del plano proyectivo en 6 puntos cuales son $\mathcal{S}$.
- Dado dos rectas sesgadas y un plano tres-tangente, tal que las rectas no estan contenidas completamente en el plano, podemos construir una mapa racional $\Phi : \mathcal{F} \to \mathrm{PG}(2,q)$.
- Con las dos rectas sesgadas y el plano tres-tangente de $\mathcal{F}$ podemos construir la mapa racional inversa $\Phi^{-1} : \mathrm{PG}(2,q) \to \mathcal{F}$.
- Φ es una map biracional desde $\mathrm{PG}(2,q)$ al superficie cubica $\mathcal{F}$ menos el *conjunto excepcional* (exceptional locus) donde dicho mapa es indeterminado. Referimos al Φ como el mapa *Clebsch*.

Illustration of Φ



Constructing Φ and Φ^{-1}

- Sin perdida de generalidad, dado las rectas sesgadas a_1 y a_2, ecojemos la recta transversal c_{12} de cuales ay 5 que interseca a_1 y a_2. Existen 3 tres-tangentes que contienen la transversal c_{12} sin contener a_1 y a_2.
- Suponga que $\mathrm{P}(X) = P \in \mathcal{F}$ y no esta contenido en a_1 o a_2. Obtenemos los planos $\langle a_1, P\rangle = \pi_1$ y $\langle a_2, P\rangle = \pi_2$.
- La interseccion $\pi_1 \cap \pi_2$ es una recta l que interseca π en un punto $Q = \mathrm{P}(Y)$.
- Resulta que Φ es determinada por la recta l tal que $\Phi(P) = Q$.

Constructing Φ and Φ^{-1}

- En la otra direccion, suponga que tenemos a_1, a_2, c_{12}, y π.
- Existe un punto $Q \in \pi$ cual no esta contenido en las rectas a_1, a_2, o c_{12}.
- La interseccion $\langle a_1, Q\rangle \cap \langle a_2, Q\rangle$ es una recta l_i tal que no esta completamente contenida en $\mathcal{F}$.
- La recta l_i interseca $\mathcal{F}$ en tres puntos; $l_i \cap a_1 = P_i$, $l_i \cap a_2 = P_2$, y un tercer punto $P \in \mathcal{F}$.
- Obtenemos el imagen de Q cual es P si parametrizamos la recta l_i tal que tambien determina Φ^{-1}.

Conics in $\mathbf{PG(2, q)}$ mapped to curves on $\mathcal{F}$

- Dado una superficie cubica $\mathcal{F}$, suponga que hemos construido la mapa Clebsch Φ.
- Si $\mathcal{A}$ es un $(5, 2)$-arco, de los 5 puntos obtenemos una conica $\mathcal{C}_{\mathcal{A}}$ sobre el plano tres-tangente π.
- Transformamos la conica $\mathcal{C}_{\mathcal{A}}$ a una curva en $\mathcal{F}$ bajo Φ.
- Mas general, queremos identificar (identify) todos los $(5, 2)$-arcos sobre el plano π mientras evitamos (avoid) el conjunto excepcional.
- Para tal fin, utilizamos $\text{Aut}(\mathcal{F})$ para obtener $\text{stab}_{\text{Aut}(\mathcal{F})}(\pi)$.
- Actuamos (we act) sobre los puntos restringidos de π con el estabilizador (stabilizer).

Coding Theory

- Un codigo lineal (linear code) $\mathcal{C}$ de longitud n sobre los elementos de F es un subespacio lineal de V.
- Los elementos de $\mathcal{C}$ son las *palabras de codigos* (*codewords*) $c = (c_0, c_1, \ldots, c_{n-1}) \in V$.
- La *distancia* $d(a, b)$ de dos palabras a y b es el numero de elementos en los que difieren, $a_i \neq b_i$.
- El *peso* (weight) $w(c)$ de una palabra de codigo c es el numero de elementos en los que difieren al cero, $w(c) = d(c, 0)$.
- La *distancia minima* de un codigo lineal $\mathcal{C}$ es el *peso minimo*, $\min(w(\mathcal{C})) = \min(d(\mathcal{C}))$.
- Insertamos puntos en las columnas de un matriz para construir una *matriz generadora* $g_{\mathcal{C}}$ de un codigo lineal $\mathcal{C}$ cuyas filas forman una base de $\mathcal{C}$.

Lower bounds of linear codes

- Un codigo lineal $\mathcal{C}$ puede ser descrito por los parametros $[n, k, d]_q$ tal que n es la longitud, k la dimension, d la distancia minima, y q se refiere al campo finito F_q.
- Codigos lineales pueden detectar $d-1$ errores y corregir (correct) $\lfloor \frac{d-1}{2} \rfloor$ errores. Por lo tanto, queremos aumentar (increase) la distancia minima d.
- Por lo tanto, utilizamos el *Limite de Singleton* (Singleton bound) cual es $d \leq n-k+1$. Un codigo $\mathcal{C}$ cuyos parametros satisface $d = n-k+1$ se conoce como *distancia maxima separable*.
- Ademas, utilizamos la *cota Griesmer* (Griesmer bound) $n \geq \displaystyle\sum_{i=0}^{k-1} \left\lceil \frac{d}{q^i} \right\rceil$. Un codigo optimo satisface la cota con igualdad.

Creating linear codes

- Para la calculacion de $(5, 2)$-arcos y superficies cubicas utilizamos Orbiter, cual es una sistema de algebra computacional escrito en C++.
- Orbiter fue creado por Anton Betten. https://github.com/abetten/orbiter
- Calculaciones simbolicas hechas con Maple.

Creating linear codes, ex. q=13

- Suponga que $\mathcal{F}$ es una superficie cubica en $\mathrm{PG}(3,13)$ definido por la ecuacion,

$$12x_0^2x_3 + 12x_1^2x_3 + 12x_2^2x_3 + 9x_0x_1x_2 + x_3^3 = 0$$

- Sea $a_1 = \begin{bmatrix} 1 & 2 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}$, y $a_2 = \begin{bmatrix} 1 & 11 & 0 & 0 \\ 0 & 0 & 1 & 12 \end{bmatrix}$ dos rectas sesgadas.
- La recta $c_{12} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$ es la linea transversal de a_1 y a_2.
- El plano tres-tangente $\pi = V(x_3)$ contiene c_{12}.

Creating linear codes, ex. q =13

- Obtenemos la mapa biracional Φ,

$$
\begin{aligned}
y_0 &= x_0\, x_2 + 6\, x_1\, x_3\\
y_1 &= 11\, x_0\, x_3 + x_1\, x_2\\
y_2 &= {x_2}^2 + 12\, {x_3}^2\\
y_3 &= 0
\end{aligned}
$$

- Cuya mapa inversa Φ^{-1},

$$
\begin{aligned}
x_0 &= 3\, {y_0}^3 + 9\, y_0\, {y_1}^2 + 9\, y_0\, {y_2}^2\\
x_1 &= 9\, {y_0}^2 y_1 + {y_1}^3 + 9\, y_1\, {y_2}^2\\
x_2 &= 3\, {y_0}^2 y_2 + {y_1}^2 y_2 + 9\, {y_2}^3\\
x_3 &= 3\, y_0\, y_1\, y_2
\end{aligned}
$$

Creating linear codes, ex. q =13

- Sea $\mathcal{A} = \{\mathrm{P}(5,2,1),\ \mathrm{P}(7,4,1),\ \mathrm{P}(10,4,1),\ \mathrm{P}(2,8,1),\ \mathrm{P}(6,9,1)\}$ un $(5,2)$-arco sobre el plano π.
- La conica $C_{\mathcal{A}}$ cual corresponde al arco $\mathcal{A}$ es definida por la ecuacion,

$$11\,x_0^2 + 5\,x_1^2 + 5\,x_2^2 + 8\,x_0\,x_2 + 12\,x_1\,x_2 = 0.$$

- $|C_{\mathcal{A}}| = 14$, transformamos los puntos a una curva $\Phi(C_{\mathcal{A}}) = \mathcal{C}$ sobre $\mathcal{F}$.

Creating linear codes, ex. q =13

- Insertamos los puntos $P \in \mathcal{C}$, menos el punto cero $P(0,0,0,0)$, en las columnas del matriz generadora $g_{\mathcal{C}}$,

$$\begin{bmatrix} 4 & 9 & 3 & 2 & 4 & 7 & 6 & 12 & 2 & 11 & 6 & 8 & 2 & 5 \\ 4 & 4 & 0 & 8 & 5 & 5 & 8 & 8 & 12 & 1 & 8 & 3 & 4 & 6 \\ 0 & 0 & 8 & 10 & 3 & 3 & 0 & 3 & 9 & 7 & 3 & 11 & 1 & 9 \\ 0 & 0 & 0 & 4 & 7 & 6 & 3 & 12 & 8 & 9 & 6 & 11 & 8 & 6 \end{bmatrix}$$

$$\Rightarrow \begin{bmatrix} 1 & 0 & 0 & 0 & 5 & 1 & 10 & 12 & 2 & 5 & 11 & 11 & 3 & 1 \\ 0 & 1 & 0 & 0 & 9 & 7 & 10 & 10 & 10 & 7 & 1 & 7 & 7 & 4 \\ 0 & 0 & 1 & 0 & 12 & 5 & 8 & 8 & 10 & 7 & 5 & 2 & 9 & 9 \\ 0 & 0 & 0 & 1 & 5 & 8 & 4 & 3 & 2 & 12 & 8 & 6 & 2 & 8 \end{bmatrix}.$$

- Con $g_{\mathcal{C}}$ en forma reducida escalonada (RREF), observa que $\min(d(\mathcal{C})) = 11$.
- Obtenemos un $[14,4,11]_{13}$-codigo cual es MDS y optimo porque satisface la cota, $\sum_{i=0}^{3} \left\lceil \frac{11}{13^i} \right\rceil = 14 = n$.

Classification

- Number of distinct linear codes?
- Number of conics is associated with the number of linear codes.
- For classification, we use Orbiter's interface for Nauty.
- Linear codes classified for $q \leq 9$.
- Markus Grassl, http://www.codetables.de/