Programa de Doctorado en Matemáticas
Departamento de Álgebra, Geometría y Topología
Universidad de Valladolid

Estructura Métrica de los Códigos Lineales
Códigos Tóricos Generalizados

Diego Ruano Benito

Tesis doctoral, diciembre de 2006

UNIVERSIDAD DE VALLADOLID
Departamento de Álgebra, Geometría y Topología

Estructura Métrica de los Códigos Lineales. Códigos Tóricos Generalizados

Memoria presentada bajo la dirección de Antonio Campillo López y José Ignacio Farrán Martín para la obtención del título de Doctor en Matemáticas.

ANTONIO CAMPILLO LÓPEZ, CATEDRÁTICO DE UNIVERSIDAD DEL DEPARTAMENTO DE ÁLGEBRA, GEOMETRÍA Y TOPOLOGÍA DE LA UNIVERSIDAD DE VALLADOLID

CERTIFICA:

Que la presente Memoria titulada "Estructura Métrica de los Códigos Lineales. Códigos Tóricos Generalizados" ha sido realizada bajo mi dirección y la de José Ignacio Farrán Martín en el Departamento de Álgebra, Geometría y Topología de la Universidad de Valladolid por Diego Ruano Benito para optar al grado de Doctor en Matemáticas, y para que así conste en cumplimiento de la presente legislación, autoriza su presentación ante el departamento de Álgebra, Geometría y Topología de dicha Universidad.

En Valladolid a 4 de diciembre de 2006.

Fdo: Antonio Campillo López

JOSÉ IGNACIO FARRÁN MARTÍN, PROFESOR TITULAR DE UNIVERSIDAD DEL DEPARTAMENTO DE MATEMÁTICA APLICADA DE LA UNIVERSIDAD DE VALLADOLID

CERTIFICA:

Que la presente Memoria titulada "Estructura Métrica de los Códigos Lineales. Códigos Tóricos Generalizados" ha sido realizada bajo mi dirección y la de Antonio Campillo López en el Departamento de Álgebra, Geometría y Topología de la Universidad de Valladolid por Diego Ruano Benito para optar al grado de Doctor en Matemáticas, y para que así conste en cumplimiento de la presente legislación, autoriza su presentación ante el departamento de Álgebra, Geometría y Topología de dicha Universidad.

En Segovia a 4 de diciembre de 2006.

Fdo: José Ignacio Farrán Martín

Agradecimientos

Quiero agradecer la labor docente de mis directores de tesis Antonio Campillo y José Ignacio Farrán.

Estoy especialmente agradecido a mis compañeros Fernando Hernando y Julio J. Moyano. Las experiencias, alegrías y desesperanzas que hemos compartido son el mejor recuerdo de esta etapa. Vuestros ánimos y apoyo han sido muy valiosos.

Agradezco a Ana Núñez su orientación y apoyo, sobre todo al inicio del doctorado. Estoy agradecido a Paco Monserrat por todas las dudas que me ha resuelto y su apoyo en los malos momentos. También agradezco la ayuda y las conversaciones tomando café a los compañeros del grupo de investigación Singacom, del departamento de Álgebra, Geometría y Topología y así como a otros estudiantes de doctorado de Matemáticas de la Universidad de Valladolid, como Lolo Ruiz.

Quiero agradecer el trabajo y colaboración de los compañeros con los que he organizado los encuentros YMIS, Young Mathematicians in Sedano, de los años 2005, 2006 y 2007: Rocío Blanco, Eugenia Ellis, Fernando Hernando, Ann Lemahieu y Julio J. Moyano.

I thank Gert-Martin Greuel and the Department of Mathematics of Kaiserslautern University for giving me the opportunity to start and finish my PhD studies there. I am also grateful to Roberto Notari for his teaching and hospitality during my stay at Politecnico di Torino. I want to express my gratefulness to Tom Høholdt for his teaching, hospitality and advices during my stay at Technical University of Denmark, I learned a lot with you (not just mathematics!). My thanks further go to Johan P. Hansen for two very nice days working together with Tom Høholdt at DTU.

Mis estudios de doctorado han sido financiados por la beca FPU AP2002-0087 del Ministerio de Educación y Ciencia. Los proyectos de investigación MTM 2004-00958 del Ministerio de Educación y Ciencia y VA068/04 de la Junta de Castilla y León me han permitido asistir a cursos y conferencias. Además, la Universidad de Valladolid ha financiado mi participación en varios congresos internacionales.

Finalmente, quiero agradecer muy especialmente a mi familia y amigos todo el apoyo que me habéis dado. También quiero disculparme con todos vosotros por el tiempo extra que la tesis me ha tenido secuestrado y la

paciencia que siempre habéis tenido. A mis padres Inés y Jesús, a mi hermana Irene y a María por quererme y apoyarme en todo momento y por animarme y echarme un cable siempre que lo he necesitado. Sin vosotros no estaría ahora, ni de lejos, escribiendo estas líneas. A mis abuelos Meles, Pepita y Román que han seguido con ilusión la evolución de esta tesis. A mis amigos de Pucela, en especial a Cris, Erika, Fer, Javi y Nacho y muy especialmente a José Luis, y a la panda de Mave por escuchar mis problemas y por los buenos ratos que hemos pasado juntos.

Índice general

Introducción

La teoría de los códigos correctores de errores nació en 1948 de la mano de C.E. Shannon [60], trabajador de Bell Laboratories. Los códigos correctores de errores se utilizan en la industria cuando se quiere enviar una información a través de un canal sujeto a ruido. El ruido en un canal es la alteración de parte de la información producida por interferencias en las telecomunicaciones o por la degradación del medio de almacenamiento de la información (por ejemplo, el compact-disc). Un código corrector añade información extra al mensaje que queremos transmitir con el fin de recuperar la información enviada, al igual que en el lenguaje natural la redundancia de éste nos permite corregir de manera automática ciertos errores e imprecisiones que cometemos cuando hablamos o escribimos. C.E. Shannon demostró que, manteniendo la probabilidad de corregir errores tan alta como se quiera, es posible codificar mensajes de tal forma que el número de bits de información extra que se transmiten sea tan pequeño como permita el canal. La demostración del resultado anterior no es constructiva, por lo que no hay un método explícito para construir una familia óptima de códigos.

En 1950 R.W. Hamming, también trabajador de Bell Laboratories, empezó a estudiar códigos correctores con tasa de transmisión mejor que el código de repetición. Su primer intento produjo los conocidos códigos de Hamming que permiten corregir fácilmente un error en la transmisión [27]. En 1965 el NASA Mariner 4 envió a la Tierra las primeras imágenes del planeta Marte, fue un gran avance, aunque las fotografías fueron de una calidad decepcionante. Poco después (1969-73) los Mariner 6, 7 y 9 repetían el experimento, sin embargo en este caso las imágenes fueron mucho mejores. Los Mariner 6, 7 y 9 usaron un potente código de Reed-Muller capaz de corregir 7 errores de 32 bits transmitidos, que consistía en 6 bits de datos y 26 bits de control. Los códigos cíclicos son códigos lineales cuyas palabras son invariantes por permutaciones cíclicas. Permiten, además de la corrección de múltiples errores aleatorios, la corrección de errores a ráfagas (por ejemplo rayones en un CD o DVD). Una familia importante de códigos cíclicos son los códigos de BCH, introducidos de forma independiente por R.C. Bose y D.K. Ray-Chaudhuri y por A. Hocquenghem. Los códigos BCH permiten estimar la capacidad correctora del código a priori y son ampliamente utilizados en la industria (por ejemplo los CD o DVD). Los códigos álgebro-geométricos son una generalización de los códigos

clásicos de Goppa, permiten estimar la capacidad correctora de los mismos de manera análoga a los BCH, y serán detallados posteriormente. Otras familias de códigos utilizadas en la industria son los códigos LDPC, que permiten una decodificación mediante grafos, y los turbocódigos, utilizados en las comunicaciones móviles. Los códigos convolucionales han sido también utilizados en las telecomunicaciones, usualmente junto con un código cíclico, y son fácilmente implementables en un circuito integrado.

Los denominados códigos de bloque transmiten la información en palabras de la misma longitud, contrariamente a los códigos convolucionales que realizan un cifrado en flujo (se codifica a la vez que se transmite), y que tienen por tanto longitud variable. Dentro de los códigos de bloque, los códigos lineales son los más estudiados y utilizados en la práctica, debido a que su estructura lineal permite utilizar las herramientas del álgebra lineal tanto para obtener resultados teóricos como para su manejo práctico. Los códigos lineales son subespacios vectoriales de dimensión k de un espacio vectorial de dimensión finita n sobre un cuerpo finito $\mathbb{F}_q$ (alfabeto) con q elementos. Un código lineal tiene tres parámetros: longitud n, dimensión k y distancia mínima d. Las palabras de tamaño k que contienen la información a transmitir (símbolos de información) se codifican en palabras de longitud n (palabras código) con una redundancia $n-k$. Normalmente la codificación se realiza de manera que los k primeros símbolos de la palabra código coincidan con los símbolos de información (codificación sistemática), en cuyo caso los $n-k$ símbolos redundantes se denominan símbolos de control. Si en la transmisión se cometen "pocos" errores, podemos corregirlos (teóricamente) o al menos detectar que la palabra recibida es errónea. De manera más precisa, si d es la distancia mínima del código, éste es capaz de detectar t errores si $t < d$ y corregir t errores si $2t < d$. Así pues, cuanto mayor sea la distancia mínima del código, mayor será la capacidad correctora del mismo, es decir, mayor número de errores podremos detectar y corregir. En el caso particular de los códigos lineales, la detección de errores se realiza mediante el cálculo del síndrome, que consiste en multiplicar la palabra recibida por la llamada matriz de control. En general, el proceso de decodificación es un problema NP, y su eficiencia depende de la estructura particular de cada código.

Una familia importante de códigos lineales son los códigos álgebro-geométricos, introducidos por Goppa a principios de los 80. La aplicación de métodos de la geometría algebraica fue la clave para la construcción de dichos códigos. Se hicieron notables en 1982 cuando Tsfasman, Vlăduţ y Zink construyeron una sucesión de códigos que excedía, por primera vez en 30 años, la cota de Gilbert-Varshamov, es decir, con un buen comportamiento de sus parámetros asintóticos $R = k/n$ y $\delta = d/n$.

En estos códigos es posible aplicar resultados de la geometría algebraica (tales como el teorema de Riemann-Roch o el algoritmo de Brill-Noether) tanto para la construcción efectiva de los códigos como para la estimación

de sus parámetros. Esto último, aunque parezca trivial no lo es, y es fundamental para conocer de antemano la capacidad correctora de los códigos, como era el caso de los códigos BCH. Por otro lado, desde el punto de vista de la implementación práctica de un código es interesante que se pueda decodificar de manera eficiente (es decir, con complejidad polinomial), y en este sentido, para los códigos álgebro-geométricos se han diseñado a partir de los años 90 algoritmos de decodificación con una complejidad $\mathcal{O}(n^3)$ o menor, debidos entre otros a Porter, Pellikaan, Feng, Rao, Høholdt, Justensen, Sudan, ... La idea básica de tales algoritmos es hallar un conjunto "pequeño" de posiciones que contenga las posiciones erróneas y entonces el problema se reduce a resolver un sistema lineal.

Los códigos álgebro-geométricos se definen evaluando funciones algebraicas sobre una curva proyectiva lisa definida sobre un cuerpo finito. Evaluamos las funciones racionales de $\mathcal{L}(D)$ en ciertos puntos racionales de la curva, donde D es un divisor cuyo soporte no contiene ninguno de los puntos racionales en los que evaluamos. Las funciones de $\mathcal{L}(D)$ tienen ceros y polos acotados por D. Los parámetros de los códigos se estiman fácilmente gracias al teorema de Riemann-Roch, ya que los puntos pueden ser vistos como divisores. Este método para definir códigos puede extenderse a variedades proyectivas de dimensión arbitraria. Podemos evaluar funciones racionales, pero construir una base de $\mathcal{L}(D)$ y estimar la distancia mínima no es factible en general.

J.P. Hansen en 1998 consideró códigos álgebro-geométricos definidos sobre superficies tóricas [28]; gracias a las técnicas combinatorias de dichas superficies pudo estimar los parámetros de los códigos así definidos. La geometría tórica estudia variedades que contienen un toro algebraico como subconjunto denso y donde además el toro actúa sobre la variedad. La importancia de dichas variedades, llamadas tóricas, reside en que éstas se corresponden con objetos combinatorios, lo que hace que las técnicas para el estudio de variedades (tales como la cohomología, la teoría de intersección, resolución de singularidades, etc) sean más precisas y los cálculos más asequibles.

Una variedad tórica puede ser definida mediante un abanico, que es una colección de conos que verifican ciertas propiedades de contención e intersección. Los divisores de la variedad también pueden ser descritos de forma combinatoria, de tal forma que un politopo racional convexo es el mismo dato que una variedad tórica y un divisor de Cartier. J.P. Hansen definió los código tóricos a partir de politopos convexos planos. Es decir, considerando la superficie tórica y el divisor de Cartier D que define un politopo P y evaluando las funciones de $\mathcal{L}(D)$ en los puntos del toro $T = (\mathbb{F}_q^*)^r$; son por tanto códigos álgebro-geométricos. Una base de $\mathcal{L}(D)$ son los monomios cuyos exponentes son los puntos racionales del politopo P. La distancia mínima se estima usando teoría de intersección. D. Joyner en [38] calculó ejemplos de códigos tóricos con buenos parámetros, propuso

varias preguntas y enunció dos conjeturas sobre los parámetros de un código tórico.

La presente memoria consta de cuatro capítulos. En el *capítulo 1*, de carácter introductorio, presentamos los códigos lineales y sus duales, es decir, consideramos su subespacio ortogonal con respecto a la forma bilineal B con matriz asociada igual a la identidad. También tratamos el concepto de matriz generatriz y de control y presentamos la decodificación por distancia mínima y algunos resultados asociados. Finalmente, introducimos los códigos álgebro-geométricos para curvas y, posteriormente, para variedades de dimensión arbitraria.

En el *capítulo 2* consideramos una introducción a la geometría tórica. Presentamos las variedades tóricas a partir de conos, abanicos y politopos. También presentamos sus principales propiedades. Introducimos los códigos tóricos de la misma forma que fueron definidos por J.P. Hansen, pero consideramos códigos definidos a partir de un politopo de dimensión arbitraria r. Calculamos el núcleo de la aplicación de evaluación, y por tanto la dimensión del código (ver Teorema 2.14). Dicho resultado permite responder a una de las preguntas de D. Joyner sobre la inyectividad de la aplicación de evaluación [38]. Estimamos la distancia mínima de un código tórico calculando una cota inferior, usando teoría de intersección (ver Sección 2.1). Calculamos los números de intersección por medio de volúmenes mixtos, dichos cálculos extienden los cálculos de J.P. Hansen para códigos definidos a partir de una superficie tórica. También obtenemos una cota superior de la distancia mínima (ver Proposición 2.17). Finalmente presentamos algunos ejemplos y damos respuesta a las conjeturas de D. Joyner (ver Contraejemplos 2.21 y 2.23).

En el *capítulo 3* definimos una extensión de los códigos tóricos, los denominados códigos tóricos generalizados. Éstos se definen considerando un álgebra polinomial arbitraria y evaluando sus elementos en los puntos del toro T. Por tanto, un código tórico es un código tórico generalizado y en particular todos los resultados existentes para códigos tóricos generalizados son válidos para códigos tóricos. Comprobamos (ver Proposición 3.2) que para definir la familia de códigos tóricos generalizados es suficiente considerar polinomios cuyos exponentes tengan grado menor o igual que $q-2$ en cada variable, es decir subálgebras de $\mathbb{F}_q[H] = \langle Y^u \mid u \in H \rangle$ donde $H = (\{0, \ldots, q-2\})^r$. En este capítulo estudiamos su estructura cíclica y métrica. Probamos que los códigos tóricos generalizados son multicíclicos (ver Proposición 3.3). Un código multicíclico es un código cuyas palabras son invariantes por ciertas permutaciones cíclicas, una forma alternativa de verlos es como ideales de $\mathbb{F}_q[X_1, \ldots, X_r]/(X_1^{N_1} - 1, \ldots, X_r^{N_r} - 1)$, con $N_1, \ldots, N_r \in \mathbb{N}$. Recíprocamente, probamos cómo toda una clase de códigos multicíclicos son códigos tóricos generalizados (ver Teorema 3.5). Es decir, probamos que todos los ideales de $\mathbb{F}_q[X_1, \ldots, X_r]/(X_1^{q-1} - 1, \ldots, X_r^{q-1} - 1)$ son códigos tóricos generalizados.

Mediante el estudio de la estructura métrica dada por la forma bilineal B, que define el código dual de un código lineal, calculamos el código dual de un código tórico generalizado (ver Teorema 3.6), que es un código tórico generalizado. Precisamente, el dual del código definido por $U \subset H$ es $\mathcal{C}_U^{\perp} = \mathcal{C}_{U^{\perp}}$, donde $U^{\perp} = H \setminus U'$ y $U' = \{(-u_1 \mod (q-1), \ldots, -u_r \mod (q-1)) \mid u \in U\}$. Sin embargo, el dual de un código tórico no es un código tórico en general. Consideramos una matriz generatriz y una matriz de control dadas por un subconjunto de filas de la matriz de evaluación M, que es la matriz cuadrada de tamaño n asociada a la aplicación de evaluación de $\mathbb{F}_q[H]$ en los puntos del toro. El conocimiento del dual de un código tórico generalizado nos permite obtener un método para calcular la distancia mínima (ver Proposición 3.8); dicho resultado es análogo a [45, Proposition 2.1]. Ordenando la base de monomios de $\mathbb{F}_q[H]$ se tiene que MM^t es la matriz de una involución, que tiene la forma siguiente

$$\begin{pmatrix} 1 & & & & & & & \\ & \ddots & & & & & & \\ & & 1 & & & & & \\ & & & 0 & 1 & & & \\ & & & 1 & 0 & & & \\ & & & & & \ddots & & \\ & & & & & & 0 & 1 \\ & & & & & & 1 & 0 \end{pmatrix}$$

Además, determinamos el número de unos en la diagonal principal de la matriz anterior, 1 si la característica de $\mathbb{F}_q$ es 2 y 2^r si no lo es, y deducimos que no existen códigos tóricos generalizados autoduales (ver Proposición 3.9). Finalmente, en la sección tercera de este capítulo mostramos cómo los cálculos con códigos tóricos generalizados pueden implementarse fácilmente en un sistema de álgebra computacional como SINGULAR [26].

La estructura métrica de los códigos tóricos generalizados motivó el capítulo 4 de esta memoria, obtener una estructura similar para un código lineal arbitrario. Para ello, en el *capítulo 4* se estudian las formas bilineales definidas en un espacio vectorial sobre un cuerpo finito. Una parte de la bibliografía de geometría sobre cuerpos finitos suele restringirse a característica distinta de dos, pero en el caso de los códigos es igualmente interesante y por ello se estudia en este capítulo. La demostraciones son diferentes en característica dos, pero se desarrollan de forma paralela.

Para $\mathbb{F}_q$ de característica distinta de dos, decimos que $\mathbb{F}_q^n$ tiene una descomposición geométrica de tipo r, s si

$$\mathbb{F}_q^n = H_1 \perp \cdots \perp H_r \perp L_1 \perp \cdots \perp L_s$$

donde $H_1, \ldots, H_r$ son planos hiperbólicos y $L_1, \ldots, L_s$ son variedades lineales unidimensionales no isótropas. Cada plano hiperbólico está generado por

dos generadores geométricos $H_i = \langle x_{2i-1}, x_{2i}\rangle$, tales que $B(x_{2i-1}, x_{2i-1}) = 0$, $B(x_{2i}, x_{2i}) = 0$, $B(x_{2i-1}, x_{2i}) = 1$, para $i = 1, \ldots, r$. Cada variedad de dimensión 1 esta generada por $L_i = \langle x_{2r+i}\rangle$, para $i = 1, \ldots, s$. Se tiene que $\{x_1, \ldots, x_n\}$ es una base de $\mathbb{F}_q^n$ que denominamos base de la descomposición geométrica.

Sea M la matriz de B en dicha base, entonces se tiene que $MM^t = J_{r,s}$

$$J_{r,s} = \begin{pmatrix} 0 & 1 & & & & & & \\ 1 & 0 & & & & & & \\ & & \ddots & & & & & \\ & & & 0 & 1 & & & \\ & & & 1 & 0 & & & \\ & & & & & \varepsilon_1 & & \\ & & & & & & \ddots & \\ & & & & & & & \varepsilon_s \end{pmatrix}$$

donde ε_i es o bien 1 o bien un no cuadrado fijo de $\mathbb{F}_q^*$.

Decimos que un código lineal es compatible con una descomposición geométrica de tipo $J_{r,s}$ si existe una base $\{x_1, \ldots, x_n\}$ de $\mathbb{F}_q^n$ compatible con dicha descomposición, de tal forma que existe $I \subset \{1, \ldots, n\}$ tal que $\{x_i \mid i \in I\}$ es una base del código. Probamos que todo código lineal sobre un cuerpo de característica distinta de 2 es compatible con una descomposición geométrica con $s \leq 4$ (ver Teorema 4.10).

Para $\mathbb{F}_q$ de característica 2, decimos que $\mathbb{F}_q^n$ tiene una descomposición geométrica de tipo r, s, t si

$$\mathbb{F}_q^n = H_1 \perp \cdots \perp H_r \perp L_1 \perp \cdots \perp L_s, \text{ con } t = 0$$

$$\mathbb{F}_q^n = H_1 \perp \cdots \perp H_r \perp L_1 \perp \cdots \perp L_s \perp E, \text{ con } t = 1$$

donde $H_1, \ldots, H_r$ son planos hiperbólicos, $L_1, \ldots, L_s$ son variedades lineales unidimensionales no isótropas y E es un plano elíptico. Cada plano hiperbólico está generado por dos generadores geométricos $H_i = \langle x_{2i-1}, x_{2i}\rangle$, tales que $B(x_{2i-1}, x_{2i-1}) = 0$, $B(x_{2i}, x_{2i}) = 0$, $B(x_{2i-1}, x_{2i}) = 1$, para $i = 1, \ldots, r$. Cada variedad de dimensión 1 esta generado por $L_i = \langle x_{2r+i}\rangle$, tales que $B(x_{2r+i}, x_{2r+i}) = 1$ para $i = 1, \ldots, s$ y el plano elíptico está generado por dos generadores geométricos $E = \langle x_{n-1}, x_n\rangle$ si $t = 1$, tales que $B(x_{n-1}, x_{n-1}) = 0$, $B(x_n, x_n) = 1$, $B(x_{n-1}, x_n) = 1$. Se tiene que $\{x_1, \ldots, x_n\}$ es una base de $\mathbb{F}_q^n$ que denominamos base de la descomposición geométrica.

Sea M la matriz de B en dicha base, entonces se tiene que $MM^t = J_{r,s,t}$

$$J_{r,s,0} = \begin{pmatrix} 0 & 1 & & & & & & \\ 1 & 0 & & & & & & \\ & & \ddots & & & & & \\ & & & 0 & 1 & & & \\ & & & 1 & 0 & & & \\ & & & & & 1 & & \\ & & & & & & \ddots & \\ & & & & & & & 1 \end{pmatrix}$$

$$J_{r,s,1} = \begin{pmatrix} 0 & 1 & & & & & & & \\ 1 & 0 & & & & & & & \\ & & \ddots & & & & & & \\ & & & 0 & 1 & & & & \\ & & & 1 & 0 & & & & \\ & & & & & 1 & & & \\ & & & & & & \ddots & & \\ & & & & & & & 1 & \\ & & & & & & & & 0 & 1 \\ & & & & & & & & 1 & 1 \end{pmatrix}$$

Decimos que un código lineal es compatible con una descomposición geométrica de tipo $J_{r,s,t}$ si existe una base $\{x_1, \ldots, x_n\}$ de $\mathbb{F}_q^n$ compatible con dicha descomposición, de tal forma que existe $I \subset \{1, \ldots, n\}$ tal que $\{x_i \mid i \in I\}$ es una base del código. Probamos que todo código lineal sobre un cuerpo de característica 2 es compatible con una descomposición geométrica con $s \leq 4$ y $t = 0$ ó, si el código es autodual, $s = 0$ y $t = 1$ (Teorema 4.19).

La descomposición geométrica permite escribir las matrices generatriz y de control como un subconjunto de filas de la matriz que tiene por filas los elementos de la base de la descomposición geométrica de $\mathbb{F}_q^n$ (ver Proposición 4.23). Extendemos los resultados para calcular la distancia mínima de códigos tóricos generalizados de [45, Proposition 2.1] y proposición 3.8 para un código lineal arbitrario (ver Teorema 4.24).

De esta forma $\mathcal{M}_{r,s,t} = \{M \in \mathcal{M}_{n\times n} \mid MM^t = J_{r,s,t}\}$ con $(s,t) \in \{0,1,2,3,4\} \times \{0\} \cup \{0\} \times \{1\}$ y $2r = n - s - 2t$, permite definir la familia de códigos lineales por medio de sus submatrices. Finalmente, mostramos cómo el grupo ortogonal actúa sobre $\mathcal{M}_{r,s,t}$ (ver Proposición 4.25). Por tanto, tenemos un nuevo paradigma para los códigos lineales que, junto con la correspondencia con el grupo ortogonal, abre una vía alternativa para estudiar problemas clásicos de códigos lineales en términos de teoría de grupos.

Introduction

The theory of error-correcting codes started up in 1948 with C.E. Shannon [60], worker of Bell Laboratories. Error-correcting codes are used in the industry when one sends information through a noisy channel. The noise in a channel is the corruption of a part of the information due to interferences in the telecommunications or to degradation of the information storing support (for instance, compact disc). An error-correcting code adds extra information to the message to be transmitted with the aim to recover the sent information, in the same way as redundancy in the natural language allows us to correct some errors or imprecisions made while speaking or writing. C.E. Sannon proved that, keeping the probability of correcting errors as high as one wants, it is possible to codify the messages so that the number of extra bits transmitted is as small as the channel allows. The proof of the previous result is not constructive, therefore there is no explicit method to construct an optimal family of codes.

In 1950 R.W. Hamming, who also worked for Bell Laboratories, started to study error-correcting codes which had a better transmission rate than the repetition code. His first attempt produced the well-known Hamming codes which easily correct one error occurred during transmission [27]. In 1965 NASA Mariner 4 sent to the Earth the first images of Mars, which was a big progress, nevertheless the quality of the photographs was disappointing. Later (1969-73) Mariner 6, 7 and 9 repeated the experiment, but the images were much better this time. Mariner 6, 7 and 9 used a potent Reed-Muller code able to correct 7 errors in each 32 transmitted bits, consisting of 6 data bits and 26 control bits. Cyclic codes are linear codes whose words stay invariant by cyclic permutations. They allow, besides of correcting random multiple errors, to correct streak errors (for instance scratches on a CD or a DVD). An important family of cyclic codes are the BCH codes, independently introduced by R.C. Bose and D.K. Ray-Chaudhuri and by A. Hocquenghem. These codes allow to estimate the error-correcting code capacity and they are widely used in the industry (for instance CD or DVD). Algebraic-geometry codes are a generalization of the Classic Goppa codes, the error-correcting code capacity can be estimated in a similar way to that of BCH codes, and they will be later detailed. Some other families of codes that are used in the industry are LDPC codes, which can be decoded using graphs, and turbocodes, used in mobile telecommunications. Convolutional

codes have been also used in telecommunications, usually together with a cyclic code, and they can be easily implemented in an integrated circuit.

The so-called block codes transmit the information in words of the same length, oppositely to convolutional codes which uses stream codification (codification and transmission happen at the same time), and therefore have variable length. From the family of block codes, the most studied and used in practice are the linear ones, because of their linear structure, which allows to use tools of linear algebra both to obtain theoretical results and to use them in practice. Error-correcting codes are vector subspaces of dimension k of a finite n-dimensional vector space over a finite field $\mathbb{F}_q$ (alphabet) with q elements. A linear code has three parameters: length n, dimension k and minimum distance d. The words of length k which contain the information to be transmitted (information symbols) are codified in words of length n (code words) with redundancy $n-k$. Usually the codification is carried out so that the first k symbols of a code word are the same as the information ones (systematic codification), where the $n-k$ redundant symbols are called control symbols. If during the transmission occur only "few" errors, we can (theoretically) correct them or at least detect that the received word is incorrect. Namely, if the minimum distance of the code is d, it will be able to detect t errors if $t < d$ and correct t errors if $2t < d$. Therefore, the larger the minimum distance of the codes is, the larger its error-correcting capacity is, that is, more errors can be detected and corrected. In the particular case of linear codes, the detection of errors is achieved computing the syndrome, which consists of multiplying the received word by the so-called control matrix. In general, the decoding process is a NP problem, and its efficiency depends on the particular structure of each code.

An important family of linear codes are algebraic-geometry codes, introduced by Goppa at the early 80's. The key for their construction was the application of algebraic geometry methods. They became important in 1982 when Tsfasman, Vlăduţ and Zink constructed a sequence of codes which exceeded, for the first time in 30 years, the Gilbert-Varshamov bound, that is, with a good behaviour of their asymptotic parameters $R = k/n$ and $\delta = d/n$.

In these codes it is possible to apply results from algebraic geometry (such as the Riemann-Roch theorem or the Brill-Noether algorithm) both for the effective construction of the codes and for estimating their parameters. Although estimating the parameters may seem trivial, it is not and it is basic to know in advance the error-correcting capacity of the codes, as in the case of BCH codes. On the other hand, from the point of view of the practical implementation of a code it is interesting that it can be efficiently decoded (that is, with polinomial complexity), and in this sense, from the 90's decoding algorithms with complexity $\mathcal{O}(n^3)$ or lower have been designed by for example Porter, Pellikaan, Feng, Rao, Høholdt, Justensen, Sudan, ... among others. The basic idea of such algorithms is to compute a "small" set

of positions which contains the wrong positions and then the problem is reduced to solving a linear system.

Algebraic-geometry codes are defined evaluating algebraic functions over a smooth projective curve defined over a finite field. The rational functions of $\mathcal{L}(D)$ are evaluated at certain rational points of the curve, where D is a divisor whose support does not contain any of the rational evaluation points. The zeros and poles of the functions of $\mathcal{L}(D)$ are bounded by D. The parameters of the codes are easily estimated using the Riemann-Roch theorem, since points can be seen as divisors. This method can be extended to define codes over varieties of arbitrary dimension. It is possible to evaluate rational functions, but in general hard to compute a basis of $\mathcal{L}(D)$ and estimate its minimum distance.

In 1998 J.P. Hansen considered algebraic-geometry codes defined over toric surfaces [28]. Thanks to combinatorial technics of such varieties he was able to estimate the parameters of the codes defined in that way. Toric geometry studies varieties which contain an algebraic torus as a dense subset and where moreover the torus acts over the variety. The importance of such varieties, called toric varieties, resides in their correspondence with combinatorial objects, which makes the technics to study the varieties (such as cohomology, intersection theory, resolution of singularities, etc) more precise and the computations reachable.

A toric variety can be defined by a fan, which is a set of cones that verify some properties of inclusion and intersection. The divisors of the variety can be also described in a combinatorial way, in such a way that a rational convex polytope is the same datum as a toric variety and a Cartier divisor. J.P. Hansen defined toric codes from convex plane polytopes. That is, he considered a toric surface and the Cartier divisor D which defines a polytope P, and he evaluated the functions of $\mathcal{L}(D)$ at the points of the torus $T = (\mathbb{F}_q^*)^r$, they are therefore algebraic-geometry codes. A basis of $\mathcal{L}(D)$ is given by the monomials whose exponents are the rational points of the polytope P. The minimum distance is estimated using intersection theory. D. Joyner in [38] computed some examples of toric codes with good parameters, he asked several questions and formulated two conjectures about the parameters of a toric code.

This essay consists of four chapters. In *chapter 1*, preparatory, we introduce linear codes and their duals, which means we consider their orthogonal subspace with respect to the bilinear form B whose associated matrix is the identity one. We also deal with the concept of generator and control matrices and introduce the minimum distance decoding and some associated results. We last present algebraic-geometry codes for curves and, afterwards, for arbitrary dimensional varieties.

In *chapter 2* we consider an introduction to toric geometry. We bring forward toric varieties from cones, fans and polytopes. We also present their

main properties. We introduce toric codes in the same way as they were defined by J.P. Hansen, but we consider codes defined from an arbitrary r-dimensional polytope. We compute the kernel of the evaluation map, and so the dimension of the code (see Theorem 2.14). This result allows us to answer one of Joyner's questions about the injectivity of the evaluation map [38]. We estimate the minimum distance of a toric code computing a lower bound, using intersection theory (see Section 2.1). We compute the intersection numbers using mixed volumes, such computations extend those of J.P. Hansen for codes defined from a toric surface. We also obtain an upper bound of the minimum distance (see Proposition 2.17). We last present some examples and we answer D. Joyner's conjectures (see Counterexamples 2.21 and 2.23).

In *chapter 3* we define an extension of toric codes, the so-called generalized toric codes. They are defined considering an arbitrary polynomial algebra and evaluating its elements at the points of the torus T. Therefore, a toric code is a generalized toric code and in particular every result for generalized toric codes is valid for toric codes. We determine (see Proposition 3.2) that in order to define the family of generalized toric codes it suffices to consider polynomials whose exponents have degree lower than or equal to $q-2$ in each variable, that is, subalgebras of $\mathbb{F}_q[H] = \langle Y^u \mid u \in H \rangle$ where $H = (\{0, \ldots, q-2\})^r$. In this chapter we study their multicyclic and metric structure. We prove that generalized toric codes are multicyclic (see Proposition 3.3). A multicyclic code is a code whose words stay invariant by certain cyclic permutations, an alternative way to think of them is as ideals of $\mathbb{F}_q[X_1, \ldots, X_r]/(X_1^{N_1} - 1, \ldots, X_r^{N_r} - 1)$, with $N_1, \ldots, N_r \in \mathbb{N}$. Reciprocally, we prove that a whole class of multicyclic toric codes are generalized toric codes (see Theorem 3.5), which means that we prove that every ideal of $\mathbb{F}_q[X_1, \ldots, X_r]/(X_1^{q-1} - 1, \ldots, X_r^{q-1} - 1)$ is a generalized toric code.

Through the study of the metric structure given by the bilinear form B, which defines the dual code of a linear code, we compute the dual code of a generalized toric code (see Theorem 3.6), which is a generalized toric code. Namely, the dual of the code defined by $U \subset H$ is $\mathcal{C}_U^{\perp} = \mathcal{C}_{U^{\perp}}$, where $U^{\perp} = H \setminus U'$ and $U' = \{(-u_1 \mod (q-1), \ldots, -u_r \mod (q-1)) \mid u \in U\}$. However, the dual of a toric code is not in general a toric code. We consider a generator matrix and a control matrix given by a subset of rows of the evaluation matrix M, which is the square n-sized matrix associated to the evaluation map of $\mathbb{F}_q[H]$ at the points of the torus. The knowledge of the dual of a generalized toric code allows us to obtain a method to compute the minimum distance (see Proposition 3.8). This result is similar to [45, Proposition 2.1]. Ordering the monomial basis of $\mathbb{F}_q[H]$ one has that MM^t is the matrix of an involution, which has the following form

$$\begin{pmatrix} 1 & & & & & & & \\ & \ddots & & & & & & \\ & & 1 & & & & & \\ & & & 0 & 1 & & & \\ & & & 1 & 0 & & & \\ & & & & & \ddots & & \\ & & & & & & 0 & 1 \\ & & & & & & 1 & 0 \end{pmatrix}$$

Moreover, we determine the number of ones in the main diagonal of the previous matrix, 1 if the characteristic of $\mathbb{F}_q$ is 2 and 2^r if it is not, and we deduce there exist no self-dual generalized toric code (see Proposition 3.9). Last, in the third section of this chapter we show how the computations with generalized toric codes can be easily implemented in a computer algebra system as SINGULAR [26].

The metric structure of generalized toric codes gave rise to the fourth chapter of this essay, which obtains a similar structure for an arbitrary linear code. Therefore, the bilinear forms defined on a vector space over a finite field are studied in *chapter 4*. Part of the bibliography about geometry over finite fields does not usually take into account characteristic equal to two, but for codes this characteristic is as interesting and thus it is studied in this chapter. The proofs for characteristic 2 are different, but they will be developed parallel.

If the characteristic of $\mathbb{F}_q$ is not equal to 2, we say that $\mathbb{F}_q^n$ has a geometric decomposition of type r, s if

$$\mathbb{F}_q^n = H_1 \perp \cdots \perp H_r \perp L_1 \perp \cdots \perp L_s$$

where $H_1, \ldots, H_r$ are hyperbolic planes and $L_1, \ldots, L_s$ are non isotropic one-dimensional linear varieties. Each hyperbolic plane is generated by two geometric generators $H_i = \langle x_{2i-1}, x_{2i} \rangle$, such that $B(x_{2i-1}, x_{2i-1}) = 0$, $B(x_{2i}, x_{2i}) = 0$, $B(x_{2i-1}, x_{2i}) = 1$, when $i = 1, \ldots, r$. Each one-dimensional variety is generated by $L_i = \langle x_{2r+i} \rangle$, when $i = 1, \ldots, s$. One has that $\{x_1, \ldots, x_n\}$ is a basis of $\mathbb{F}_q^n$ that we call basis of the geometric decomposition.

Let M be the matrix of B in this basis, then one has that $MM^t = J_{r,s}$

$$J_{r,s} = \begin{pmatrix} 0 & 1 & & & & & & \\ 1 & 0 & & & & & & \\ & & \ddots & & & & & \\ & & & 0 & 1 & & & \\ & & & 1 & 0 & & & \\ & & & & & \varepsilon_1 & & \\ & & & & & & \ddots & \\ & & & & & & & \varepsilon_s \end{pmatrix}$$

where ε_i is either 1 or a fixed non-square element of $\mathbb{F}_q^*$.

A linear code is said to be compatible with a geometric decomposition of type $J_{r,s}$ if there exists a basis $\{x_1, \ldots, x_n\}$ of $\mathbb{F}_q^n$ compatible with such decomposition, in such a way that exists $I \subset \{1, \ldots, n\}$ such that $\{x_i \mid i \in I\}$ is a basis of the code. We prove that every linear code over a field of characteristic different from 2 is compatible with a geometric decomposition with $s \leq 4$ (see Theorem 4.10).

If the characteristic of $\mathbb{F}_q$ is equal to 2, we say that $\mathbb{F}_q^n$ has a geometric decomposition of type r, s, t if

$$\mathbb{F}_q^n = H_1 \perp \cdots \perp H_r \perp L_1 \perp \cdots \perp L_s, \text{ with } t = 0$$

$$\mathbb{F}_q^n = H_1 \perp \cdots \perp H_r \perp L_1 \perp \cdots \perp L_s \perp E, \text{ with } t = 1$$

where $H_1, \ldots, H_r$ are hyperbolic planes, $L_1, \ldots, L_s$ are isotropic one-dimensional linear varieties and E is an elliptic plane. Each hyperbolic plane is generated by two geometric generators $H_i = \langle x_{2i-1}, x_{2i} \rangle$, such that $B(x_{2i-1}, x_{2i-1}) = 0$, $B(x_{2i}, x_{2i}) = 0$, $B(x_{2i-1}, x_{2i}) = 1$, when $i = 1, \ldots, r$. Each one-dimensional variety is generated by $L_i = \langle x_{2r+i} \rangle$, such that $B(x_{2r+i}, x_{2r+i}) = 1$ when $i = 1, \ldots, s$ and the elliptic plane is generated by two geometric generators $E = \langle x_{n-1}, x_n \rangle$ if $t = 1$, such that $B(x_{n-1}, x_{n-1}) = 0$, $B(x_n, x_n) = 1$, $B(x_{n-1}, x_n) = 1$. One has that $\{x_1, \ldots, x_n\}$ is a basis of $\mathbb{F}_q^n$ that we call basis of the geometric decomposition.

Let M be the matrix of B in this basis, then one has that $MM^t = J_{r,s,t}$

$$J_{r,s,0} = \begin{pmatrix} 0 & 1 & & & & & & \\ 1 & 0 & & & & & & \\ & & \ddots & & & & & \\ & & & 0 & 1 & & & \\ & & & 1 & 0 & & & \\ & & & & & 1 & & \\ & & & & & & \ddots & \\ & & & & & & & 1 \end{pmatrix}$$

$$J_{r,s,1} = \begin{pmatrix} 0 & 1 & & & & & & & & \\ 1 & 0 & & & & & & & & \\ & & \ddots & & & & & & & \\ & & & 0 & 1 & & & & & \\ & & & 1 & 0 & & & & & \\ & & & & & 1 & & & & \\ & & & & & & \ddots & & & \\ & & & & & & & 1 & & \\ & & & & & & & & 0 & 1 \\ & & & & & & & & 1 & 1 \end{pmatrix}$$

A linear code is said to be compatible with a geometric decomposition of type $J_{r,s,t}$ if there exists a basis $\{x_1, \ldots, x_n\}$ of $\mathbb{F}_q^n$ compatible with such decomposition, in such a way that exists $I \subset \{1, \ldots, n\}$ such that $\{x_i \mid i \in I\}$ is a basis of the code. We prove that every linear code over a field of characteristic 2 is compatible with a geometric decomposition with $s \leq 4$ and $t = 0$ or, if the code is self-dual, $s = 0$ and $t = 1$ (see Theorem 4.19).

The geometric decomposition allows us to write the generator and control matrices as subsets of the rows of the matrix whose rows are the elements of the basis of the geometric decomposition of $\mathbb{F}_q^n$ (see Proposition 4.23). We extend the methods to compute the minimum distance of generalized toric codes of [45, Proposition 2.1] and proposition 3.8 to an arbitrary linear code (see Theorem 4.24)

In this way $\mathcal{M}_{r,s,t} = \{M \in \mathcal{M}_{n\times n} \mid MM^t = J_{r,s,t}\}$ with $(s,t) \in \{0,1,2,3,4\} \times \{0\} \cup \{0\} \times \{1\}$ and $2r = n - s - 2t$, allows us to define the family of linear codes throughout their submatrices. Last, we show how the orthogonal group acts over $\mathcal{M}_{r,s,t}$ (see Proposition 4.25). Therefore, we have obtained a new paradigm for linear codes which, along with the correspondence with the orthogonal group, gives rise to study classic problems of linear codes in terms of group theory.

CAPÍTULO 1

Códigos Lineales Correctores de Errores

En este capítulo introductorio presentamos los conceptos básicos sobre códigos lineales y sobre códigos álgebro-geométricos. Introducimos los códigos correctores de errores lineales y mostramos sus principales resultados asociados. Posteriormente, presentamos los códigos álgebro-geométricos.

1. Códigos Lineales

Presentamos los conceptos básicos sobre códigos lineales, necesarios en la presente memoria. Un estudio detallado de los códigos lineales puede encontrarse en [39, 47, 48]. Sea $\mathbb{F}_q$ el cuerpo finito con q elementos.

Un **código lineal** $\mathcal{C}$ de longitud n sobre $\mathbb{F}_q$ es un subespacio vectorial de $\mathbb{F}_q^n$, sus elementos se denominan palabras y $\mathbb{F}_q$ alfabeto del código. Se denota la dimensión de $\mathcal{C}$ como $k = \dim\ \mathcal{C}$ (en particular $\#\mathcal{C} = q^k$).

Consideramos dos aplicaciones lineales: la aplicación de codificación g y la aplicación síndrome h (que sirve para detectar errores) dadas, respectivamente, por G, denominada **matriz generatriz**, y por la matriz transpuesta H^t de la denominada **matriz de control** H, ambas de rango máximo, de forma que

$$\mathbb{F}_q^k \xrightarrow{\ g\ } \mathbb{F}_q^n \xrightarrow{\ h\ } \mathbb{F}_q^{n-k}$$

donde $\mathrm{Im}(g) = \mathcal{C}$ y $\mathrm{Ker}(h) = \mathcal{C}$. Se tiene entonces que $GH^t = 0$. Las filas de G son una base del código. H se deduce en la práctica mediante álgebra lineal, calculando una base de soluciones de un sistema lineal indeterminado.

Si se recibe una palabra $x \in \mathbb{F}_q^n$ tal que $h(x) = 0$ entonces la palabra recibida es correcta. En cambio si $h(x) \neq 0$ entonces $x \notin \mathcal{C}$ y en principio decodificaremos esta palabra por el criterio de máxima verosimilitud o mínima distancia que describimos posteriormente. Dicho criterio minimiza además la probabilidad de error en la decodificación.

La **distancia de Hamming** es la dada por

$$d(x, y) = \#\{i \mid 1 \leq i \leq n, x_i \neq y_i\}$$

para $x, y \in \mathbb{F}_q^n$, que dota a $\mathbb{F}_q^n$ de estructura de espacio métrico.

El **peso de Hamming** $w(x)$ de x se define como

$$w(x) = d(x, 0)$$

La **distancia mínima** $d(\mathcal{C})$ de un código lineal se define por

$$d \equiv d(\mathcal{C}) = \min\{d(x,y) \mid x,y \in \mathcal{C}, x \neq y\} = \min\{w(x) \mid x \in \mathcal{C},\ x \neq 0\}$$

Se denominan a $[n,k,d]$ los parámetros del código lineal $\mathcal{C}$. A veces se escribe $[n,k,d]_q$ para indicar el alfabeto.

PROPOSICIÓN 1.1. *Un código lineal $\mathcal{C}$ puede corregir $\left\lfloor \frac{d-1}{2} \right\rfloor$ errores, y detectar t errores si $t < d$.*

DEMOSTRACIÓN. Las bolas euclídeas con centro en cada palabra del código $\mathcal{C}$ y radio $\left\lfloor \frac{d-1}{2} \right\rfloor$ son disjuntas. Así, para una palabra recibida x con $\left\lfloor \frac{d-1}{2} \right\rfloor$ o menos errores, se tiene que x pertenece a una única bola de centro una palabra código y radio $\left\lfloor \frac{d-1}{2} \right\rfloor$. Por lo tanto decodificamos x por la palabra código que es el centro de dicha bola (es decir, decodificamos por mínima distancia).

Podemos detectar t errores, con $t < d$, porque si en x se han producido $1 < t < d$ errores entonces x no es una palabra del código. Además, podemos comprobarlo usando la matriz de control del código, puesto que $xH^t \neq 0$. □

EJEMPLO 1.2. Hay dos ejemplos triviales:

$\mathcal{C} = \mathbb{F}_q^n$. No se puede ni detectar ni corregir ningún error, puesto que $d = 1$.

El código de repetición:

$$\begin{array}{ccc} \mathbb{F}_2 & \xrightarrow{g} & \mathbb{F}_2^n \\ 0 & \mapsto & (\underbrace{0,\ldots,0}_{n}) \\ 1 & \mapsto & (\underbrace{1,\ldots,1}_{n}) \end{array}$$

obviamente $d = n$. Por ejemplo si $n = 4$, únicamente se puede corregir $[\frac{4-1}{2}] = 1$ error, si bien pueden detectarse hasta 3 errores.

Sea $\mathcal{C}$ un código lineal y sea H una matriz de control de $\mathcal{C}$. Podemos considerar H como la matriz generatriz de otro código sobre $\mathbb{F}_q$. Este código es el denominado **código dual** de $\mathcal{C}$, y se denota por $\mathcal{C}^\perp$.

De hecho, $\mathcal{C}^\perp$ es el código que consiste en el subespacio ortogonal de $\mathcal{C}$ respecto de la forma bilineal simétrica $B : \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q$ dada por $B(x,y) = \sum_{i=1}^n x_i y_i$. Como dicha forma es no degenerada, se tiene que $\mathcal{C}^\perp$ tiene dimensión $n-k$ si $\mathcal{C}$ tiene dimensión k. Además, si G es una matriz generatriz de $\mathcal{C}$, la igualdad $GH^t = 0$ implica que G es una matriz de control de $\mathcal{C}^\perp$.

El siguiente resultado permite calcular la distancia mínima a partir de la matriz de control del código, en lugar de calcular el peso de todas sus palabras.

PROPOSICIÓN 1.3. *Sea $\mathcal{C}$ un código lineal, sean G una matriz generatriz y H una matriz de control de $\mathcal{C}$. Entonces*

$\mathcal{C}$ tiene distancia mínima d si cualesquiera $d-1$ columnas de H son linealmente independientes y existen d linealmente dependientes.

$\mathcal{C}$ tiene distancia mínima d si para cualesquiera $n-d+1$ columnas de de G existen k columnas que son linealmente independientes y existen $n-d$ columnas que no contienen a k columnas linealmente independientes.

DEMOSTRACIÓN. Se tiene que $x \in \mathbb{F}_q^n$ pertenece a $\mathcal{C}$ si y sólo si $xH^t = 0$, por tanto existe una palabra de peso d si y sólo si xH^t da una combinación lineal de d columnas que son linealmente dependientes.

Sea $x \in \mathcal{C}$, se tiene que x es combinación lineal de las k filas de G. Por tanto x tiene peso d si y sólo si tiene $n-d$ coordenadas igual a cero, que definen un sistema homogéneo de k ecuaciones. □

EJEMPLO 1.4. Sea $n = (q^k - 1)/(q-1)$. El $[n, n-k]$ **código de Hamming** sobre $\mathbb{F}_q$ es un código cuya matriz de control tiene columnas linealmente independientes dos a dos. Por tanto, la distancia mínima de un código de Hamming es 3, independientemente de q.

Por ejemplo, el $[7, 4, 3]$ código binario de Hamming $\mathcal{C}$ tiene la siguiente matriz de control

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

2. Códigos Álgebro-Geométricos

V.D. Goppa introdujo los códigos álgebro-geométricos a principios de los 80 [24]. Son una generalización de las ideas sobre los denominados códigos clásicos de Goppa, que son una extensión de los códigos BCH.

En principio fueron obtenidos evaluando funciones racionales sobre una curva proyectiva lisa definida sobre un cuerpo finito $\mathbb{F}_q$, posteriormente esta definición se extendió a variedades de dimensión arbitraria. En esta sección se introducen los códigos álgebro geométricos y se muestran algunos resultados asociados. Dichos resultados pueden encontrase en [63] y para códigos definidos a partir de una curva en [33].

Sea X una curva proyectiva no singular y absolutamente irreducible definida sobre $\mathbb{F}_q$.

Sea G un divisor racional sobre X. Sea $\mathcal{L}(G)$ el espacio vectorial de funciones racionales sobre X con polos y ceros acotados por G

$$\mathcal{L}(G) = \{f \in \mathbb{F}_q(X)^* \mid (f) + G \succeq 0\} \cup \{0\}$$

El **código álgebro-geométrico** $\mathcal{C}_L(D,G)$ de longitud n sobre $\mathbb{F}_q$ es la imagen de la aplicación de evaluación $\mathbb{F}_q$-lineal dada por

$$\begin{array}{rccc} \text{ev}: & \mathcal{L}(G) & \to & \mathbb{F}_q^n \\ & f & \mapsto & (f(P_1),\ldots,f(P_n)) \end{array}$$

donde $P_1,\ldots,P_n$ son puntos racionales de X, $D=\sum_{i=1}^n P_i$(divisor), y G es cualquier divisor racional tal que $\sup(D)\bigcap\sup(G)=\emptyset$. Aunque no es necesario, se considera sobre G la restricción $2g-2<\deg(G)<n$. De esta forma la aplicación ev es inyectiva y se tiene el siguiente resultado que hace uso del teorema de Riemann-Roch.

TEOREMA 1.5. *El código $\mathcal{C}_L(D,G)$, de longitud n sobre $\mathbb{F}_q$, tiene dimensión $k=\deg(G)-g+1$ y distancia mínima $d\geq n-\deg(G)$. La cota $n-\deg(G)$ se denomina* ***distancia de Goppa*** *de $\mathcal{C}_L(D,G)$.*

DEMOSTRACIÓN. Si f pertenece al núcleo de ev, entonces $f\in\mathcal{L}(G-D)$, y por lo tanto $f=0$ (pues $\deg(G-D)<0$). Esto prueba que ev es inyectiva, y aplicando el teorema de Riemann-Roch se tiene que $k=\dim(\mathcal{L}(G))$ que es igual a $\deg(G)-g+1$, ya que $\deg(D)>2g-2$.

Por otra parte, si $\text{ev}(f)$ tiene peso d, con f no nula, existen $n-d$ puntos P_i, denotados $P_{i_1},P_{i_2},\ldots,P_{i_{n-d}}$, que verifican $f(P_i)=0$. En consecuencia, $f\in\mathcal{L}(G-E)$, donde $E=P_{i_1}+P_{i_2}+\cdots+P_{i_{n-d}}$, y se tiene $\deg(G)-n+d\geq 0$, al ser $\mathcal{L}(G-E)\neq 0$. □

EJEMPLO 1.6. Sea X la recta proyectiva sobre $\mathbb{F}_{q^m}$. Sean $n=q^m-1$, $P_0=(0:1)$, $P_\infty=(1:0)$, $D=\sum_{j=1}^n P_j$, donde $P_j=(\beta^j:1)$, $1\leq j\leq n$, β raíz primitiva $n-$ésima de 1. Sea $G=aP_0+bP_\infty$, con $a\geq 0, b\geq 0$.

Por el teorema de Riemann-Roch sabemos que:

$$\dim(\mathcal{L}(G))=l(G)=a+b-0+1=a+b+1$$

El conjunto $\{(\frac{x}{y})^i \mid -a\leq i\leq b\}$ es una base de $\mathcal{L}(G)$, porque $f\in\mathcal{L}(G)$ sólo tiene polos en P_0 y P_∞ con orden a lo sumo a o b, respectivamente.

En consecuencia $\text{ev}((\frac{x}{y})^i)=((\frac{\beta}{1})^i,\ldots,(\frac{\beta^n}{1})^i)$. Una matriz generatriz para este código es

$$G=\begin{pmatrix} \beta^{-a} & \beta^{-a+1} & \cdots & \cdots & \beta^b \\ \vdots & \vdots & & & \vdots \\ \vdots & \vdots & \cdots & \cdots & \vdots \\ \vdots & \vdots & & & \vdots \\ (\beta^n)^{-a} & (\beta^n)^{-a+1} & \cdots & \cdots & (\beta^n)^b \end{pmatrix}$$

Se puede ver que $(c_1,\ldots,c_n)$ es una palabra del código $\mathcal{C}_L(D,G)$ si y sólo si $\sum_{j=1}^n c_j(\beta^l)^j=0$ para todo $a<l<n-b$. Se deduce que $\mathcal{C}_L(D,G)$ es un código de Reed-Solomon [45, section 6.8] y el código subcuerpo con coordenadas en $\mathbb{F}_q$ es un código BCH [45, section 6.6].

En 1982, Tsfasman, Vlăduţ y Zink [62], construyeron una sucesión de códigos álgebro-geométricos que mejoran la cota de Gilbert-Varshamov [45, section 5.1]. Fue la primera vez en 30 años que se superó dicha cota de manera efectiva. Habitualmente se trabaja con la familia dual de los códigos anteriormente definidos, i.e., se considera la matriz generatriz de un código $\mathcal{C}_L(D,G)$ como la matriz de control de un nuevo código $\mathcal{C}_\Omega(D,G)$, que puede ser descrito, gracias al teorema de los residuos, por medio de las formas diferenciales racionales sobre X. Dentro de éstos últimos se considera una familia especial, los denominados **códigos álgebro-geométricos sobre un punto**, en los cuales $G = mP$, donde P es un punto racional extra. Para estos códigos se conocen métodos de decodificación eficientes, como el algoritmo de Feng-Rao, con complejidad menor que $\mathcal{O}(n^3)$.

Finalmente, damos la definición de código álgebro-geométrico para una variedad de dimensión arbitraria. Sea X una variedad normal proyectiva sobre $\mathbb{F}_q$. Sean $P_1, \ldots, P_n$ puntos de X racionales sobre $\mathbb{F}_q$, y consideramos $\mathcal{P} = \{P_1, \ldots, P_n\}$. Sea D un divisor de Cartier con soporte disjunto con $\mathcal{P}$. El **código álgebro-geométrico** $\mathcal{C}(X, D, \mathcal{P})$ de longitud n es la imagen de la aplicación de evaluación $\mathbb{F}_q$-lineal

$$\begin{array}{rccc} \mathrm{ev}: & \mathcal{L}(D) & \to & \mathbb{F}_q^n \\ & f & \mapsto & (f(P_1), \ldots, f(P_n)) \end{array}$$

Si la aplicación de evaluación ev es inyectiva la dimensión de $\mathcal{C}(X, D, \mathcal{P})$ es igual a $k = \dim(\mathcal{L}(D))$. En caso contrario, la dimensión de $\mathcal{C}(X, D, \mathcal{P})$ es igual a $k = \dim(\mathcal{L}(D)) - \dim(\ker(\mathrm{ev}))$. Además en la codificación se tiene que el número de filas no coincide con la dimensión, por lo tanto se deben eliminar las filas que sean linealmente dependientes para tener una matriz generatriz, que es la que se usaría en la práctica para codificar.

No es sencillo trabajar con un código álgebro-geométrico sobre una variedad de dimensión arbitraria, concretamente, salvo en pocos casos, se desconocen métodos para calcular una base de $\mathcal{L}(D)$ y sobre todo su distancia mínima. En el capítulo siguiente estudiamos los códigos álgebro-geométricos para variedades tóricas, denominados códigos tóricos, donde se aprovecha su estructura combinatoria para definirlos y estimar sus parámetros.

CAPÍTULO 2

Códigos Tóricos

J.P. Hansen presentó los códigos tóricos en 1998 [28], los códigos tóricos son códigos álgebro-geométricos sobre variedades tóricas. En este capítulo introducimos los códigos tóricos y calculamos sus parámetros. Primero presentamos una introducción a la geometría tórica que contiene las definiciones y resultados necesarios para el estudio de los códigos tóricos.

1. Geometría Tórica

Sea $\mathbb{K}$ un cuerpo. Una **variedad tórica** X es una variedad normal que contiene al toro algebraico $T = \mathbb{K}^* \times \cdots \times \mathbb{K}^*$ como subconjunto denso, junto con la acción $T \times X \to X$ de T sobre X que extiende la acción natural de T sobre sí mismo. La importancia de las variedades tóricas reside en su correspondencia con objetos combinatorios como los conos y politopos. Todos los resultados de esta sección se encuentran en [8] para un cuerpo base arbitrario, y en [21, 50] para $\mathbb{K} = \mathbb{C}$. Para los conceptos de geometría tórica usamos principalmente la notación de [21].

1.1. Conos, abanicos, politopos y variedades tóricas. Sea N un retículo isomorfo a $\mathbb{Z}^r$ para algún $r \geq 1$. Sea $M = \mathrm{Hom}(N, \mathbb{Z})$ el retículo dual de N. Se tiene la aplicación $\mathbb{Z}$-bilineal $\langle\ ,\ \rangle : M \times N \to \mathbb{Z}$, $(u, v) \mapsto u(v)$. Sean $N_{\mathbb{R}} = N \otimes \mathbb{R}$ y $M_{\mathbb{R}} = M \otimes \mathbb{R}$, donde $M_{\mathbb{R}}$ es el espacio vectorial dual de $N_{\mathbb{R}}$. Se tiene la aplicación $\mathbb{R}$-bilineal $\langle\ ,\ \rangle : M_{\mathbb{R}} \times N_{\mathbb{R}} \to \mathbb{R}$, $(u, v) \mapsto u(v)$.

Un **cono poliédrico convexo** σ es un conjunto

$$\sigma = \{s_1 v_1 + \cdots + s_k v_k \in N_{\mathbb{R}} \mid s_i \geq 0\}$$

generado por un conjunto finito de elementos $v_1, \ldots, v_s \in N_{\mathbb{R}}$. La **dimensión** de σ, $\dim(\sigma)$, es la dimensión del espacio vectorial

$$\sigma + (-\sigma) = \mathbb{R}\sigma$$

El **cono dual** $\sigma^\vee \subset M_{\mathbb{R}}$ de un cono poliédrico convexo, se define como

$$\sigma^\vee = \{u \in M_{\mathbb{R}} \mid \langle u, v\rangle \geq 0 \ \forall\ v \in \sigma\}$$

Una **cara** τ de un cono σ es la intersección de σ con un hiperplano definido por una forma lineal que es no negativa en σ, es decir se tiene que $\tau = \sigma \cap u^\perp = \{v \in \sigma \mid \langle u, v\rangle = 0\}$ para un $u \in \sigma^\vee$. El propio cono convexo σ es una cara ya que es la intersección con la forma lineal definida por 0. Además cada cara es un cono poliédrico convexo, generado por los

vectores de σ tal que $\langle u, v_i\rangle = 0$. Las caras unidimensionales se denotan por ρ y se denominan **bordes**. El **elemento primitivo** $v(\rho) \in N$ de un borde ρ es el único generador de $\rho \cap N$ como semigrupo aditivo. Se tiene un orden parcial en las caras de σ, sean τ y τ' dos caras de σ, si $\tau \subset \tau'$ se denota $\tau < \tau'$.

Un cono poliédrico convexo σ se dice que es **racional** si sus generadores pueden tomarse en el retículo N. Un cono poliédrico convexo σ es **fuertemente convexo** si $\sigma \cap (-\sigma) = \{0\}$ o, equivalentemente, si $\sigma^\vee$ genera $M_\mathbb{R}$. Cualquier cono racional está generado por un conjunto minimal de elementos de N, cuando el cono es fuertemente convexo, los generadores minimales son los elementos primitivos de los bordes. Además si σ es un cono poliédrico racional fuertemente convexo entonces $\sigma^\vee$ es un cono racional poliédrico en $M_\mathbb{R}$ [50, Proposition 1.3]. Por simplicidad llamaremos únicamente **cono** a un cono poliédrico racional fuertemente convexo en este trabajo.

Sea σ un cono, entonces $S_\sigma = \sigma^\vee \cap M$ es un semigrupo finitamente generado por el lema de Gordan [50, Proposition 1.1]. Consideramos la $\mathbb{K}$-álgebra asociada a S_σ, $\mathbb{K}[S_\sigma] = \bigoplus_{u \in S_\sigma} \mathbb{K}\chi^u$ (donde $\chi^u\chi^{u'} = \chi^{u+u'}$, la unidad es χ^0). Por lo tanto podemos definir la variedad afín U_σ como $U_\sigma = \mathrm{Spec}(\mathbb{K}[S_\sigma])$ que denominamos **variedad tórica afín asociada a** σ.

Un álgebra conmutativa finitamente generada A determina una variedad afín que se denota $\mathrm{Spec}(A)$. Si se escogen los generadores de A entonces A se puede presentar como $\mathbb{K}[X_1, \ldots, X_r]/I$, donde I es un ideal. Por tanto se identifica la variedad afín $V(I)$ con $\mathrm{Spec}(A)$, en concreto a cada punto de $V(I)$ le corresponde un ideal maximal de $\mathrm{Spec}(A)$, que se denominan puntos cerrados de la variedad y se denotan como $\mathrm{Specm}(A)$. Un homomorfismo $A \to B$ de álgebras determina un morfismo $\mathrm{Spec}(B) \to \mathrm{Spec}(A)$ de variedades y en particular los puntos cerrados corresponden a morfismos de álgebras de A a $\mathbb{K}$.

En el caso de variedades tóricas, los puntos cerrados corresponden a homomorfismos de semigrupos de S_σ a $\mathbb{K}$, donde se considera $\mathbb{K} = \mathbb{K}^* \cup \{0\}$ como semigrupo multiplicativo y se tiene $\mathrm{Specm}(\mathbb{K}[\mathrm{S}_\sigma]) \simeq \mathrm{Hom}(S_\sigma, \mathbb{K})$.

Se puede considerar χ^u como un monomio de Laurent, $\chi^u(t) = t_1^{u_1} \cdots t_r^{u_r} \in \mathbb{K}[t_1, \ldots, t_r]_{(t_1 \cdots t_r)}$, además define una aplicación $T \to \mathbb{K}^*$. En la teoría de grupos algebraicos χ^u se conoce como un **carácter**.

Denominamos **toro algebraico** de dimensión r a $T = (\mathbb{K}^*)^r$. Se tiene que T está contenido en toda variedad tórica afín y que además actúa sobre la variedad extendiendo la acción sobre sí mismo. De hecho, estas dos propiedades caracterizan las variedades tóricas [40].

Veamos que el toro $T = \mathbb{K}^* \times \cdots \times \mathbb{K}^*$ está incluido en U_σ. Se tiene que S_σ es un subsemigrupo de $S_{\{0\}} = M$. Sea $v_1, \ldots, v_r$ una base de N y $u_1 = v_1^*, \ldots, u_r = v_r^*$ su base dual de M. Como semigrupo, M

tiene como generadores $u_1^*, \ldots, u_r^*, -u_1^*, \ldots, -u_r^*$, por lo que si escribimos $x_i = \chi^{u_i^*} \in \mathbb{K}[M]$, se tiene

$$\mathbb{K}[M] = \mathbb{K}[x_1, x_2, \ldots, x_r, x_1^{-1}, x_2^{-1}, \ldots, x_r^{-1}] = \mathbb{K}[x_1, x_2, \ldots, x_r]_{(x_1 x_2 \cdots x_r)}$$

que es el anillo de polinomios de Laurent con r indeterminadas y se tiene que $U_0 = \mathrm{Spec}(\mathbb{K}[M]) = \mathbb{K}^* \times \cdots \times \mathbb{K}^* = (\mathbb{K}^*)^r = T$. En consecuencia, como todos los semigrupos S_σ son subsemigrupos de M, se tiene que $\mathbb{K}[S_\sigma]$ es una subálgebra de $\mathbb{K}[M]$. Por consiguiente, $\mathbb{K}[S_\sigma]$ es un dominio y $T \subset U_\sigma$.

Además podemos describir el toro T intrínsecamente como

$$T = \mathrm{Spec}(\mathbb{K}[M]) = \mathrm{Hom}(M, \mathbb{K})$$

Sea σ un cono en N, el toro T actúa sobre U_σ de la manera siguiente: hemos visto que un punto $t \in T$ es identificado con un homomorfismo $M \to \mathbb{K}$ de grupos y que un punto $x \in U_\sigma$ es identificado con un homomorfismo $S_\sigma \to \mathbb{K}$ de semigrupos. Entonces

$$\begin{array}{ccc} T \times U_\sigma & \to & U_\sigma \\ (t, x) & \mapsto & t \cdot x \end{array}$$

donde $t \cdot x$ es el homomorfismo de semigrupos

$$\begin{array}{rccc} t \cdot x : & S_\sigma & \to & \mathbb{K} \\ & u & \mapsto & t(u)x(u) \end{array}$$

Ejemplo 2.1. Sea σ el cono generado por $v_1, \ldots, v_l$ con $1 \leq l \leq r$. Se tiene

$$S_\sigma = \mathbb{Z}_{\geq 0} u_1 + \cdots + \mathbb{Z}_{\geq 0} u_l + \mathbb{Z} u_{l+1} + \cdots + \mathbb{Z} u_r$$

Por consiguiente se tiene que $\mathbb{K}[\sigma] = \mathbb{K}[x_1, \ldots, x_l, x_{l+1}, x_{l+1}^{-1}, \ldots, x_r, x_r^{-1}]$ y $U_\sigma = \mathbb{K}^l \times (\mathbb{K})^{r-l}$.

Por tanto, podemos deducir que si σ está generado por l elementos que se pueden completar a una base de N, entonces U_σ es producto de un espacio afín de dimensión l y de un toro $(r-l)$-dimensional, que es una variedad no singular (como veremos en el teorema 2.6).

Un **abanico** $\triangle$ en N es un conjunto finito de conos en $N_\mathbb{R}$ tales que: cada cara de los conos en $\triangle$ es también un cono de $\triangle$ y la intersección de dos conos en $\triangle$ es una cara de cada uno de ellos. Para un abanico $\triangle$ la **variedad tórica** $X_\triangle$ se construye tomando la unión disjunta de variedades tóricas afines U_σ con $\sigma \in \triangle$, y pegando dichas variedades afines por las caras comunes: para conos σ, $\sigma' \in \triangle$ se tiene que $\sigma \cap \sigma'$ es una cara de cada uno de ellos, y por lo tanto podemos identificar $U_{\sigma \cap \sigma'}$ como variedad abierta de U_σ y de $U_{\sigma'}$.

Las identificaciones son compatibles debido a que en la correspondencia entre conos y variedades afines se mantiene el orden. Además el pre-esquema resultante es un esquema debido al siguiente lema [21, Section 1.4].

LEMA 2.2. *Si σ y σ' son dos conos que se intersecan en una cara común entonces la aplicación diagonal $U_{\sigma\cap\sigma'} \to U_\sigma \times U_{\sigma'}$ es una inmersión cerrada.*

En particular, se tiene:

- Para dos conos σ y σ' en un abanico se verifica que $U_\sigma \cap U_{\sigma'} = U_{\sigma\cap\sigma'}$.
- Sea σ un cono en N y sea $\triangle$ el abanico formado por todas las caras de σ. Entonces $X_\triangle = U_\sigma$.

Veamos un ejemplo en el que construimos una variedad tórica a partir de un abanico.

EJEMPLO 2.3. Sea $\triangle$ el abanico de la Figura 1. Los conos de dimensión uno son las 4 semirrectas desde el origen sobre los ejes, y los conos de dimensión 2 son los 4 cuadrantes $\sigma_i,\ i = 1, \ldots, 4$.

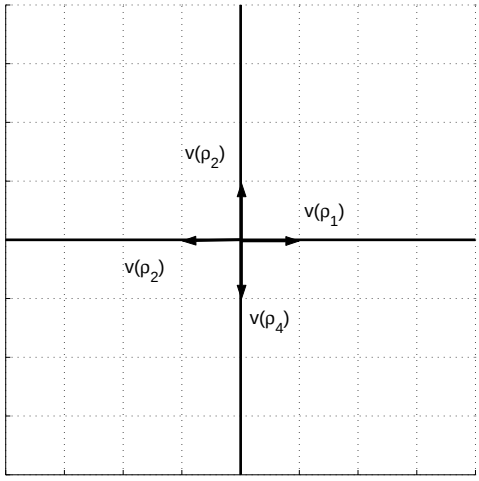

FIGURA 1. Abanico $\triangle$, ejemplo 2.3

Las variedades tóricas afines $U_{\sigma_i} \simeq \mathbb{K}^2$ (que corresponden a las álgebras $\mathbb{K}[x_1, x_2]$, $\mathbb{K}[x_1^{-1}, x_2]$, $\mathbb{K}[x_1^{-1}, x_2^{-1}]$, $\mathbb{K}[x_1, x_2^{-1}]$) se pegan de la manera usual para dar $\mathbb{P}^1 \times \mathbb{P}^1$ (fijando coordenadas, $x_1 = t_1/t_0$, y $x_2 = t_1'/t_0'$ donde $(t_1 : t_0) \times (t_1' : t_0')$ son las coordenadas de $\mathbb{P}^1 \times \mathbb{P}^1$).

Un politopo racional convexo en $M_\mathbb{R}$ es el cierre convexo de un conjunto finito de puntos en M, por simplicidad diremos únicamente **politopo**. Podemos representar un politopo como intersección de semiespacios. Al igual que en $N_\mathbb{R}$ podemos considerar caras de politopos en $M_\mathbb{R}$. Una **faceta** F de un politopo P es una cara de P de codimensión 1 en M, por tanto existe un subespacio normal a esa cara que está generado por dos elementos primitivos en el retículo N, uno interno al politopo y otro externo. Sea $v_F \in N$ el

elemento interno y primitivo que genera la cara normal a F y a_F un entero tal que

$$P = \bigcap_{F \text{ faceta de } P} \{u \in M_{\mathbb{R}} \mid \langle u, v_F \rangle \geq -a_F\}$$

Dada una cara τ de P, sea σ_τ el cono generado por v_F para todas las facetas F que contienen a τ. Entonces

$$\triangle_P = \{\sigma_\tau \mid \tau \text{ es una cara de } P\}$$

es un abanico que denominamos **abanico asociado a** P, la variedad tórica que define se denota por X_P.

Ejemplo 2.4. Sea P el politopo plano de $M_{\mathbb{R}}$ con vértices $(0,0)$, $(1,0)$, $(1,1)$, $(0,1)$, i.e. la envolvente convexa de esos puntos.

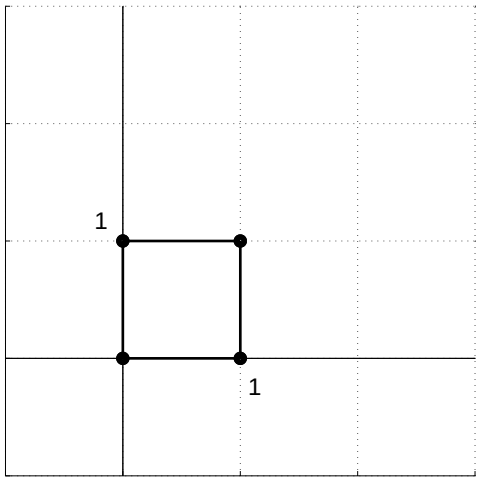

Figura 2. Politopo P, ejemplo 2.4

P es la intersección de los siguientes semiespacios,

$$P = \{u_1 \geq 0\} \cap \{-u_1 \geq -1\} \cap \{u_2 \geq 0\} \cap \{-u_2 \geq -1\}$$

Los elementos primitivos internos de N normales a las facetas son $v_1, -v_1, v_2, -v_2$. Cada vértice del politopo da lugar a un cono de dimensión 2 en el abanico normal (por ejemplo $(0,0)$ da lugar al cono generado por v_1 y v_2). Por lo tanto, se tiene que el abanico normal $\triangle_P$ es el del ejemplo 2.3, y en consecuencia $X_P = \mathbb{P}^1 \times \mathbb{P}^1$.

1.2. Propiedades de las variedades tóricas. Se tiene una caracterización de las variedades tóricas definidas mediante un politopo [6, Theorem 12.2].

TEOREMA 2.5. *Sea $\triangle$ un abanico. La variedad tórica $X_\triangle$ asociada a $\triangle$ es proyectiva si y sólo si $\triangle$ es el abanico normal asociado a un politopo.*

Se dice que un **abanico $\triangle$ es no singular** si para cada cara $\sigma \in \triangle$ existe una $\mathbb{Z}$-base $\{v_1, \ldots, v_r\}$ de N tal que σ está generado por $\{v_1, \ldots, v_s\}$, donde $s \leq r$ es la dimensión de σ. Se tiene de esta forma un criterio combinatorio para determinar si una variedad tórica es **singular** [21, section 2.1], [50, theorem 1.10].

TEOREMA 2.6. *La variedad tórica $X_\triangle$ asociada a un abanico $\triangle$ es no singular si y sólo si $\triangle$ es no singular.*

Sea $\triangle$ un abanico, un abanico $\triangle'$ es un **refinamiento** de $\triangle$ si cada cono de $\triangle$ es unión de conos de $\triangle'$. El morfismo $X'_\triangle \to X_\triangle$ inducido por la aplicación identidad de N en N es birracional y propio. De hecho, es un isomorfismo sobre el toro contenido en ambas variedades [21, section 2.4].

Así, esta construcción puede usarse para comprender las resoluciones de singularidades de variedades tóricas. Al abanico $\triangle'$, que es no singular y es un refinamiento de $\triangle$, lo denominamos **abanico refinado de** $\triangle$. En el caso de superficies, esta construcción es computable en términos de fracciones continuas con la complejidad del algoritmo de Euclides [21, section 2.6].

EJEMPLO 2.7. Sea P el politopo de vértices $(0,0)$, $(2,2)$ y $(0,4)$.

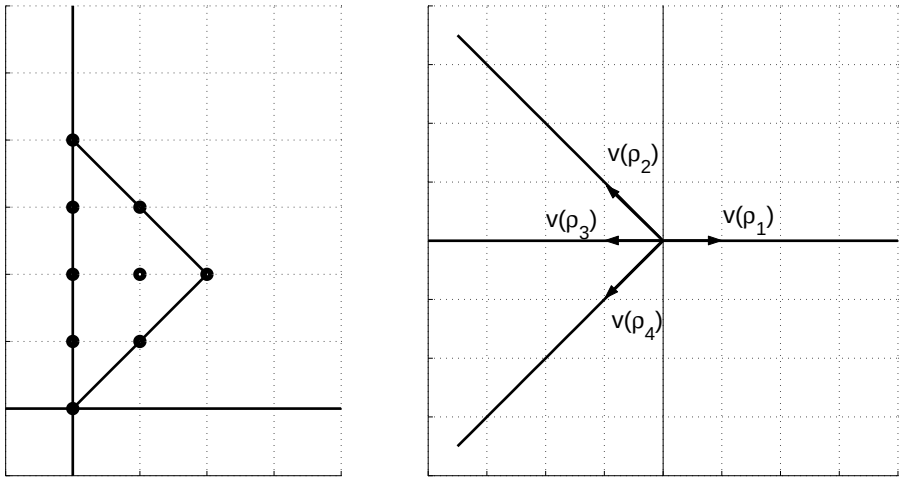

FIGURA 3. P y su abanico normal refinado.

$$P = \{u_1 \geq 0\} \cap \{-u_1 + u_2 \geq 0\} \cap \{-u_1 - u_2 \geq -4\}$$

Se tiene que los bordes de $\triangle_P$ son $(1,0)$, $(-1,1)$ y $(-1,-1)$ por lo que $\triangle_P$ es un abanico singular ya que $(-1,1)$ y $(-1,-1)$ no generan el retículo N.

Refinamos el abanico $\triangle_P$ considerando el borde $(-1,0)$, es decir el abanico refinado $\triangle'$ tiene los bordes $(1,0)$, $(-1,1)$, $(-1,0)$ y $(-1,-1)$ y

los 4 conos de dimensión 2 generados por dos bordes consecutivos. Se tiene que $\triangle'$ es un refinamiento de $\triangle$ y $X'_{\triangle}$ es una variedad no singular por el teorema 2.6.

Las variedades tóricas definidas anteriormente son variedades **normales**, también denominadas variedades tóricas normales. Es decir, todos sus anillos locales son dominios íntegramente cerrados en sus cuerpos de fracciones [21, section 2.1]. El motivo por el que las variedades tóricas que consideramos son normales es que hemos utilizado todos los puntos del retículo del cono dual para definir la variedad [6, theorem 7.2].

Sea σ un cono generado por $u_1, \ldots, u_t$ entonces $\mathbb{K}[S_\sigma] = \mathbb{K}[\chi^{u_1}, \ldots, \chi^{u_t}]$. Se tiene que $\mathbb{K}[S_\sigma] = \mathbb{K}[Y_1, \ldots, Y_t]/I$ donde I está generado por binomios de la forma $Y_1^{a_1} \cdots Y_t^{a_t} - Y_1^{b_1} \cdots Y_t^{b_t}$, con $a_1, \ldots, a_t,\ b_1, \ldots, b_t$ enteros no negativos que verifican la ecuación

$$a_1 u_1 + \cdots + a_t u_t = b_1 u_1 + \cdots + b_t u_t$$

Sin embargo, no toda álgebra cociente definida por un ideal generado por binomios define una variedad tórica normal [61].

Se dice que un abanico $\triangle$ es **completo** si la unión de todas sus caras es $N_{\mathbb{R}}$. Se tiene el siguiente resultado que caracteriza las variedades tóricas completas [21, Section 2.4], [50, Section 1.4].

TEOREMA 2.8. *Una variedad tórica $X_{\triangle}$ es completa si y sólo si $\triangle$ es completo.*

Al haber supuesto en la definición de politopo que el origen está incluido, se tiene que el abanico normal $\triangle_P$ definido por un politopo P es completo y por tanto la variedad X_P es completa.

1.3. Órbitas y divisores. Sea P un politopo y $\triangle_P$ su abanico normal. Como X_P es una variedad proyectiva normal, podemos considerar el grupo conmutativo $\mathrm{Div}(X_P)$ de **divisores de Weil** de X. Un divisor de Weil es una suma finita de combinaciones lineales sobre $\mathbb{Z}$ de variedades irreducibles de codimensión 1. Denotamos por T–$\mathrm{Div}(X_P)$ el subgrupo de divisores de Weil que son invariantes por la acción de T.

El siguiente teorema caracteriza las T-órbitas, órbitas por la acción de T, en función de $\triangle_P$ [50, proposition 1.6]

TEOREMA 2.9. *Sea P un abanico y $\triangle_P$ su abanico normal. Para cada $\sigma \in \triangle_P$ se considera*

$$\mathrm{orb}(\sigma) = \mathrm{Hom}(M \cap \sigma^{\perp}, \mathbb{K}^*)$$

Toda T-órbita de X_P es de esta forma y se tiene una correspondencia biunívoca entre $\triangle_P$ y las T-órbitas de X_P. Además se verifica:

- $\mathrm{orb}(\{0\}) = T$.

- *Sea* $\sigma \in \triangle$. *Entonces* $\mathrm{orb}(\sigma)$ *es un abierto en su propia clausura que denotamos por* $V(\sigma)$. *La variedad* $V(\sigma)$ *es una subvariedad tórica cerrada de* X_P *de codimensión* $\dim(\sigma)$, *es decir* $\dim \sigma + \dim V(\sigma) = r$.
- *Si* X_P *es no singular entonces* $V(\sigma)$ *es no singular.*

Por el resultado anterior, $\{V(\rho) \mid \rho \in \triangle_P(1)\}$ es una base de T–$\mathrm{Div}(X_P)$ sobre $\mathbb{Z}$. Denotamos por $\mathrm{PDiv}(X_P)$ el subgrupo de **divisores principales de** $\mathrm{Div}(X_P)$, i.e., los divisores de la forma

$$\mathrm{div}(f) = \sum_V v_V(f) V$$

con f una función racional en X_P distinta de cero, y $v_V(f)$ el orden de f en las subvariedades cerradas V de X_P de codimensión 1. Cada $u \in M$ corresponde a un carácter χ^u que es una función regular en T, que da lugar a una función racional en X_P.

El subgrupo $\mathrm{CDiv}(X_P)$ de **divisores de Cartier** de $\mathrm{Div}(X_P)$ son los divisores de Weil localmente principales, i.e., existe un recubrimiento abierto $X_P = \cup U_j$ y funciones racionales distintas de cero f_j, tales que el divisor de Cartier se escribe como el divisor $\mathrm{div}(f_j^{-1})$ en U_j. Si X_P es regular todo divisor de Weil es un divisor de Cartier, i.e. $\mathrm{CDiv}(X_P) = \mathrm{Div}(X_P)$ [32, proposition 6.11].

Un politopo define el siguiente divisor de Cartier T-invariante

$$D_P = \sum_{F \text{ faceta de } P} a_F V(\rho_F)$$

y dado $u \in P$

$$\mathrm{div}(\chi^u) = \sum_{F \text{ faceta de } P} \langle u, v_F \rangle V(\rho_F)$$

Ejemplo 2.10. Dos politopos con los mismos vectores normales internos definen la misma variedad tórica. Por ejemplo, los politopos $P_{a,b}$ con vértices $(0,0)$, $(a,0)$, (a,b) y $(0,b)$ definen la misma variedad tórica $\mathbb{P}^1 \times \mathbb{P}^1$ para todo $a, b \in \mathbb{N}$. En particular para $a = b = 1$ se tiene el politopo del ejemplo 2.4. En cambio, definen divisores de Cartier diferentes

$$D_{P_{a,b}} = aV(\rho) + bV(\rho')$$

donde ρ y ρ' son los conos generados por $(-1,0)$ y $(0,-1)$ respectivamente.

Un abanico completo $\triangle$ y $D = \sum a_\rho V(\rho)$ un divisor de Cartier T-invariante definen un politopo,

$$P_D = \{u \in M_{\mathbb{R}} \mid \langle u, v(\rho) \rangle \geq -a_\rho \ \forall\ \rho \text{ borde de } \triangle\}$$

Además, $P_{D_P} = P$. Por tanto, un politopo es el mismo dato que una variedad tórica completa normal y un divisor de Cartier.

El siguiente lema permite calcular una base de $\mathrm{H}^0(X_P, \mathcal{O}(D_P)) = \mathcal{L}(D_P)$, i.e., funciones racionales f sobre X_P tales que $\mathrm{div}(f) + D_P \succeq 0$.

LEMA 2.11. *Sea X_P una variedad tórica asociada a un politopo P. El conjunto $\mathrm{H}^0(X_P, \mathcal{O}(D_P))$ de secciones globales de $\mathcal{O}(D_P)$ es un $\mathbb{K}$-espacio vectorial de dimensión finita que tiene a $\{\chi^u \mid u \in P \cap M\}$ como base.*

2. Códigos Tóricos

Sea $\mathbb{F}_q$ el cuerpo finito con q elementos. Sea P un politopo racional de dimensión $r \geq 2$, X_P su variedad tórica refinada asociada y D_P su divisor de Cartier asociado sobre X_P como en la sección anterior. Por tanto, se tiene que X_P es una variedad regular.

Para $t \in T = (\mathbb{F}_q^*)^r$, las funciones racionales de $\mathrm{H}^0(X_P, \mathcal{O}(D_P))$ pueden evaluarse en t

$$\begin{array}{ccc} \mathrm{H}^0(X_P, \mathcal{O}(D_P)) & \to & \mathbb{F}_q \\ f & \mapsto & f(t) \end{array}$$

puesto que f es una combinación lineal de caracteres χ^u que pueden ser considerados monomios de Laurent en virtud del lema 2.11. Esta aplicación es simplemente la evaluación de un polinomio de Laurent cuyos monomios tienen exponentes en $P \cap M$ en un punto cuyas coordenadas son distintas de cero.

Introducimos los códigos tóricos de la misma forma que fueron definidos por J.P. Hansen en [28]. Evaluando las funciones racionales de $\mathrm{H}^0(X_P, \mathcal{O}(D_P))$ en los $(q-1)^r$ puntos de $T = (\mathbb{F}_q^*)^r$ obtenemos el **código tórico $\mathcal{C}_P^t$ asociado a** P, que es un código álgebro-geométrico, como los presentados en la sección 1.2. Por consiguiente, $\mathcal{C}_P^t$ es la imagen de la aplicación de evaluación $\mathbb{F}_q$-lineal dada por

$$\begin{array}{ccc} \mathrm{ev} : \mathrm{H}^0(X_P, \mathcal{O}(D_P)) & \to & (\mathbb{F}_q)^{\#T} \\ f & \mapsto & (f(t))_{t \in T} \end{array}$$

Como evaluamos en $\#T$ puntos, $\mathcal{C}_P^t$ tiene **longitud** $n = \#T = (q-1)^r$.

Del lema 2.11 se deduce que $\mathrm{H}^0(X_P, \mathcal{O}(D_P))$ es un $\mathbb{F}_q$-espacio vectorial de dimensión finita con base $\{\chi^u \mid u \in P \cap M\}$, por tanto un sistema de generadores del código $\mathcal{C}_P^t$ es $\{(\chi^u(t))_{t \in T} \mid u \in P \cap M\}$. Dicho sistema de generadores es una base del código si y sólo si la aplicación de evaluación ev es inyectiva.

NOTA 2.12. D. Joyner, en [38], define un código tórico a partir de una variedad tórica proveniente de un abanico completo, un divisor de Cartier y un 1-ciclo. El 1-ciclo se usa para evaluar las funciones racionales en su soporte. Además, se considera el caso particular en el que el 1-ciclo tiene a T como soporte, denominando a esta familia **códigos tóricos estándar** [38, definition 4.5]. Como hemos visto en la sección anterior, un abanico completo y un divisor de Cartier es el mismo dato que un politopo P. Por

tanto, los códigos tóricos definidos aquí y en el resto de la bibliografía de códigos tóricos son tan generales como los códigos tóricos estándar de [38].

El siguiente resultado se usa para calcular el núcleo de la aplicación de evaluación y la dimensión del código que se dan en el teorema 2.14.

LEMA 2.13. *Sea P un politopo tal que $P \cap M$ está contenido en $H = \{0, \dots, q-2\} \times \cdots \times \{0, \dots, q-2\} \subset M$. Consideremos*

$$f = \sum_{u \in P \cap M} \lambda_u \chi^u, \quad \lambda_u \in \mathbb{F}_q$$

Entonces $(f(t))_{t \in T} = (0)_{t \in T}$ ($f \in \ker(\mathrm{ev})$ para algún D) si y sólo si $\lambda_u = 0$, $\forall\, u \in P \cap M$.

DEMOSTRACIÓN. Sea $f = \sum_{u \in P \cap M} \lambda_u \chi^u$, podemos escribir f como

$$f(t_1, \dots, t_r) = \sum_{0 \le u_1, \dots, u_r \le q-2} \lambda_{u_1, \dots, u_r} t_1^{u_1} \cdots t_r^{u_r} \in \mathbb{F}_q[t_1, \dots, t_r]$$

con $\lambda_{u_1, \dots, u_r} \in \mathbb{F}_q$. Veamos que $f = 0$.

Probamos el resultado por inducción en el número de variables. Si $r = 1$, $f = \sum_{0 \le u_1 \le q-2} \lambda_{u_1} t_1^{u_1}$, como f se anula para todos los valores de $\mathbb{F}_q^*$ entonces pertenece al ideal generado por $t_1^{q-1} - 1$, y por tanto $f = 0$ (por cuestión de grados).

Supongamos el resultado cierto para $r-1$ variables. Sea $t_1, \dots, t_{r-1} \in \mathbb{F}_q^*$ entonces

$$f(t_1, \dots, t_r) = g_{q-2}(t_1, \dots, t_{r-1}) t_r^{q-2} + \cdots + g_1(t_1, \dots, t_{r-1}) t_r + g_0(t_1, \dots, t_{r-1})$$

con $g_i(t_1, \dots, t_{r-1}) \in \mathbb{F}_q[t_1, ..., t_{r-1}]$.

El polinomio $f(t_1, \dots, t_{r-1}, t_r) \in \mathbb{F}_q[t_r]$ se anula para todo $t_r \in \mathbb{F}_q^*$. Por consiguiente f pertenece al ideal generado por $t_r^{q-1} - 1$, y se tiene $f = 0$ (por cuestión de grados). Por tanto $g_i = 0$ para todo $i = 1, \dots, q-2$ y podemos aplicar la hipótesis de inducción a g_i para obtener $f = 0$. □

El siguiente resultado permite calcular el núcleo de la aplicación de evaluación, una base del código y por tanto su dimensión.

TEOREMA 2.14. *Sea P un politopo y $\mathcal{C}_P^t$ su código tórico asociado.*

Para todo $u \in P \cap M$ escribimos $u = c_u + b_u$ donde $c_u \in H = \{0, \dots, q-2\} \times \cdots \times \{0, \dots, q-2\} \subset M$, y $b_u \in ((q-1)\mathbb{Z})^r$. También denotaremos $\overline{u} = c_u$. Sea $\overline{P}$ el conjunto, $\overline{P} = \{c_u \mid u \in P\} \subset P \cap M$.

Se tiene que,

(1) *El núcleo de la aplicación de evaluación* ev *es el $\mathbb{F}_q$-espacio vectorial generado por*

$$\{\chi^u - \chi^{u'} \mid u, u' \in P \cap M,\ c_u = c_{u'}\}$$

(2) *Una base del código* $\mathcal{C}_P^t$ *es*

$$\{(\chi^{c_u}(t))_{t\in T} \mid u \in P \cap M\}$$

Y por tanto la ***dimensión*** *de* $\mathcal{C}_P^t$

$$k = \#\{\overline{u} \mid u \in P \cap M\} = \#\overline{P}$$

Demostración.

(1) Sean $u, u' \in P \cap M$ tales que $c_u = c_{u'}$. Entonces $\mathrm{ev}(\chi^u) = \mathrm{ev}(\chi^{u'})$ y se tiene por tanto que $\mathrm{ev}(\chi^u - \chi^{u'}) \in \ker(\mathrm{ev})$.

Por otro lado sea $f \in \mathrm{H}^0(X_P, \mathcal{O}(D_P))$, con $\mathrm{ev}(f) = 0$.

$$f = \sum_{u\in P\cap M} \lambda_u \chi^u = \sum_{u\in P\cap M} \lambda_u(\chi^u - \chi^{c_u}) + \sum_{u\in P\cap M} \lambda_u \chi^{c_u}$$

Se tiene para todo $t \in T$

$$f(t) = \sum_{u\in P\cap M} \lambda_u(\chi^u(t) - \chi^{c_u}(t)) + \sum_{u\in P\cap M} \lambda_u \chi^{c_u}(t)$$

Como el primer término de la igualdad y el primer sumando del segundo término de la igualdad anterior son cero, se tiene que $\sum_{u\in P\cap M} \lambda_u \chi^{c_u}(t) = 0$ para todo $t \in T$, y por el lema 2.13 ($c_u \in H\ \forall\ u$) se tiene que $\sum_{u\in P\cap M} \lambda_u \chi^{c_u}$ es la función cero. Por tanto, f pertenece al espacio vectorial generado por $\{\chi^u - \chi^{u'} \mid u, u' \in P \cap M,\ c_u = c_{u'}\}$.

(2) Sea $f \in \mathrm{H}^0(X_P, \mathcal{O}(D_P))$, y sea $t \in T$,

$$f(t) = \sum_{u\in P\cap M} \lambda_u \chi^u(t) = \sum_{u\in P\cap M} \lambda_u \chi^{c_u+b_u}(t) = \sum_{u\in P\cap M} \lambda_u \chi^{c_u}(t)$$

Por tanto $(f(t))_{t\in T} \in \{(\chi^{c_u}(t))_{t\in T} \mid u \in P \cap M\}$.

Y además $\{(\chi^{c_u}(t))_{t\in T} \mid u \in P \cap M\}$ es un conjunto linealmente independiente por el lema 2.13 ($c_u \in H\ \forall\ u$). □

Dos politopos P, P' tales que $\overline{P} = \overline{P'}$ tienen el mismo código tórico asociado ($\mathcal{C}_P^t = \mathcal{C}_{P'}^t$). Calcular χ^{c_u} es equivalente a calcular la clase de χ^u en $\mathbb{F}_q[X_1, \ldots, X_r]/J$, donde $J = (X_1^{q-1} - 1, \ldots, X_r^{q-1} - 1)$. En [11] se prueba que un código tórico definido mediante un politopo plano es multicíclico usando una representación matricial de las palabras del código. Considerando la clase de χ^u en $\mathbb{F}_q[X_1, \ldots, X_r]/J$, puede comprobarse que $\mathcal{C}_P^t$ es un código multicíclico para un politopo de dimensión arbitraria. La demostración de este fenómeno se presenta en el capítulo 3 para códigos tóricos generalizados que incluyen en particular los códigos tóricos.

En [38, Question 3.4] D. Joyner pregunta *"under what conditions (if any) is the map* ev *an injection?"*. Nuestro teorema 2.14 responde a esta pregunta completamente para códigos tóricos estándar.

Decimos que un politopo P verifica la **condición de inyectividad** si para todo $u, u' \in P \cap M$ con $u \neq u'$ se tiene que $c_u \neq c_{u'}$. Por el teorema anterior, P verifica la condición de inyectividad si y sólo si la aplicación de evaluación ev es inyectiva y $\mathcal{C}_P^t$ tiene por tanto dimensión $k = \#(P \cap M)$, que es el número de puntos racionales del politopo. En [28, 29] se restringe el tamaño de los politopos considerando la cota de la distancia mínima para hacer inyectiva la aplicación de evaluación. Por tanto, en sus ejemplos la dimensión del código es el número de puntos racionales del politopo.

Se puede encontrar en [9] y sus referencias una discusión de los algoritmos para calcular el número de puntos en el retículo de un politopo, tales algoritmos tienen complejidad polinómica. Además, para politopos planos se tiene la fórmula de Pick [21]:

LEMA 2.15. *Sea P un politopo plano en $M_{\mathbb{R}}$. Entonces*

$$\#(P \cap M) = \mathrm{vol}_2(P) + \frac{\text{Perímetro}(P)}{2} + 1$$

donde vol_2 *es el volumen plano de Lebesgue.*

2.1. Cálculo de la distancia mínima. En esta sección estimamos la distancia mínima de los códigos tóricos y calculamos una cota inferior y una superior de la distancia mínima. Primero extendemos las técnicas de [28] para politopos de dimensión r=2 a dimensión arbitraria, calculando los números de intersección usando volúmenes mixtos. Posteriormente, presentamos los cálculos de [28] para politopos planos.

Para calcular la distancia mínima d del código lineal $\mathcal{C}_P^t$ debemos calcular el peso mínimo de una palabra no nula, i.e. el máximo número de ceros de una función f en $\mathrm{H}^0(X_P, \mathcal{O}(D_P)) \setminus \{0\}$ en T. Resolveremos este problema usando teoría de intersección [19].

Sea $u_1 = (1, 0, \ldots, 0), u_2 = (0, 1, 0, \ldots, 0), \ldots, u_r = (0, \ldots, 0, 1)$ una base de M. Cada punto de $T = (\mathbb{F}_q^*)^r$ está contenido en una de las $(q-1)^{r-1}$ rectas

$$C_{\eta_1,\ldots,\eta_{r-1}} = \mathrm{V}(\{\chi^{u_i} - \eta_i \mid i = 1, \ldots, r-1\}),\ \eta_i \in \mathbb{F}_q^*\ \forall i$$

Sea $f \in \mathrm{H}^0(X_P, \mathcal{O}(D_P)) \setminus \{0\}$. Supongamos que f se anula completamente, es decir se anula en todos sus puntos, a lo largo de a de las rectas anteriormente definidas y denotemos por A el conjunto de subíndices de las a rectas donde f es cero.

Siguiendo [31, proposition 3.2], en las otras rectas el número de ceros está dado por el número de intersección de un divisor de Cartier con un 1-ciclo, el entero $D_P \cdot C_{\eta_1,\ldots,\eta_{r-1}}$. Por lo que el número de ceros de f en T está acotado por

$$a(q-1) + \sum_{\eta_i \in \mathbb{F}_q^*, (\eta_1,\ldots,\eta_{r-1}) \notin A} D_P \cdot C_{\eta_1,\ldots,\eta_{r-1}}$$

Para conocer el máximo número de ceros de f tenemos que calcular el número de intersección correspondiente al divisor de Cartier D_P y el 1-ciclo $C_{\eta_1,\ldots,\eta_{r-1}}$, además de acotar el número de rectas en las que f puede ser 0.

Siguiendo [42] $D_P \cdot C_{\eta_1,\ldots,\eta_{r-1}} = D_P \cdot C$ para cualquier recta C definida anteriormente. Por tanto el número de ceros de f está acotado por

$$a(q-1) + ((q-1)^{r-1} - a)(D_P \cdot C)$$

y por tanto la distancia mínima está acotada por

$$d(\mathcal{C}_P^t) \geq n - (a(q-1) + ((q-1)^{r-1} - a)(D_P \cdot C))$$

Se tiene que

$$D_P \cdot C = D_P \cdot (\mathrm{div}(\chi^{u_1}))_0 \cdot \ldots \cdot (\mathrm{div}(\chi^{u_{r-1}}))_0$$

donde $(\mathrm{div}(\chi^{u_1}))_0$ es el divisor de ceros del divisor principal definido por el carácter χ^{u_1}. Siguiendo [21] se tiene que este número de intersección es el volumen mixto de sus politopos asociados

$$D_P \cdot C = r! V_r(P, P_{(\mathrm{div}(\chi^{u_1}))_0}, \ldots, P_{(\mathrm{div}(\chi^{u_{r-1}}))_0})$$

El **volumen mixto** V_r de r politopos $P_1, \ldots, P_r$ es

$$V_r(P_1, \ldots, P_r) = \frac{1}{r!} \sum_{j=1}^{r} (-1)^{r-j} \sum_{1 \leq i_1 < \cdots < i_j \leq r} \mathrm{vol}_r(P_{i_1} + \cdots + P_{i_j})$$

donde vol_r es el volumen de Lebesgue. Un algoritmo para calcular el volumen de Lebesgue de un politopo se encuentra en [3]. Además, bajo ciertas hipótesis extra, el volumen mixto puede ser calculado directamente [41].

Sea $f \in \mathrm{H}^0(X_P, \mathcal{O}(D_P))$; como $\mathcal{C}_P^t = \mathcal{C}_{P'}^t$ si y sólo si $\overline{P} = \overline{P'}$, podemos suponer sin pérdida de generalidad que $\deg_{t_i} f \leq q-2$.

$$f(t_1, \ldots, t_r) = f_0(t_1, \ldots, t_{r-1}) + f_1(t_1, \ldots, t_{r-1}) t_r + \cdots + f_{q-2}(t_1, \ldots, t_{r-1}) t_r^{q-2}$$

Sea $C_{\eta_1,\ldots,\eta_{r-1}}$ una recta donde f se anula, $f(\eta_1, \ldots, \eta_{r-1}, t_r) \in \mathbb{F}_q[t_r]$, y $\deg f(\eta_1, \ldots, \eta_{r-1}, t_r) < t_r^{q-1}$. Por tanto, como se tiene que $f(\eta_1, \ldots, \eta_{r-1}, t_r)$ es cero para todo $t_r \in \mathbb{F}_q^*$, se tiene que $f_i(\eta_1, \ldots, \eta_{r-1}) = 0 \ \forall \ i$.

Por consiguiente el entero a es menor o igual que el máximo número de ceros de una función no nula $f \in \mathrm{H}^0(X_{P'}, \mathcal{O}(D_{P'}))$, donde P' es la proyección r-ésima del politopo P. Repetimos este proceso hasta obtener un politopo de dimensión 2.

Para un **politopo plano** calculamos la distancia mínima como en [29]:

Sea P un politopo plano. Se puede mejorar el cálculo anterior de la cota de la distancia mínima. Sea $f \in \mathrm{H}^0(X_P, \mathcal{O}(D_P)) \setminus \{0\}$, y supongamos que f es idénticamente cero en a de esas rectas. Por tanto, siguiendo [31, proposition 3.2], en las otras $(q-1-a)$ rectas el máximo número de ceros de f es $D_P \cdot \mathrm{div}(\chi^{u_1})$.

En dimensión 2 un 1-ciclo es un divisor de Weil y como f se anula en a de las rectas anteriores se tiene que

$$\operatorname{div}(f) + D_P - a(\operatorname{div}(\chi^{u_1}))_0 \succeq 0$$

Equivalentemente, $f \in \mathrm{H}^0(X_P, \mathcal{O}(D_P - a(\operatorname{div}(\chi^{u_1}))_0))$, y por tanto el máximo número de ceros de f en las otras $(q-1-a)$ rectas es $(D_P - a(\operatorname{div}(\chi^{u_1}))_0) \cdot (\operatorname{div}(\chi^{u_1}))_0$, que es menor o igual que el número anterior para un politopo de dimensión mayor que 2. Esto probablemente permitirá dar una cota más ajustada.

Del lema 2.11 se deduce que

$$a \leq \text{máx}\{u_2 - u_2' \mid u_1 = u_1', (u_1, u_2) \in P, (u_1', u_2') \in P\}$$

Finalmente, calculamos el número de intersección de los dos divisores de Cartier de la misma manera que para dimensión $r > 2$, usando el volumen mixto de los politopos asociados:

$$(D_P - a(\operatorname{div}(\chi^{u_1}))_0) \cdot (\operatorname{div}(\chi^{u_1}))_0 = 2V_2(P_{D_P - a(\operatorname{div}(\chi^{u_1}))_0}, P_{(\operatorname{div}(\chi^{u_1}))_0})$$

Nota 2.16. Para un politopo P suficientemente grande se pueden obtener cotas triviales para la distancia mínima, lo que no es el caso cuando la condición de inyectividad se verifica. Por ejemplo, si consideramos un rectángulo P con una base mayor que $q-1$, obtenemos una cota negativa para la distancia mínima. Otra posibilidad puede ser aplicar los cálculos anteriores a $\overline{P}$ para obtener una cota no trivial pero, desafortunadamente, $\overline{P}$ no es en general el conjunto de puntos racionales de un politopo convexo. Este fenómeno es similar a la situación en la que se considera un código álgebro-geométrico $\mathcal{C}_L(D, G)$ con $\deg(G) \geq n$ [63].

El siguiente resultado proporciona una **cota superior** de la distancia mínima que puede ser usada para comprobar si la cota anterior es ajustada. Este resultado extiende los ejemplos de [29] y los cálculos de [38].

Proposición 2.17. *Sea P un politopo y $\mathcal{C}_P^t$ su código lineal asociado.*

Sean $u \in M$ y $Q = \{0, 1, \ldots, l_1\} \times \cdots \times \{0, 1, \ldots, l_r\} \subset M$, donde $0 \leq l_i \leq q-2$ (algunos l_i pueden ser igual a cero). Si $\overline{u+Q}$ está contenido en el conjunto $\overline{P}$, (donde $u = c_u + b_u$, $c_u \in H$, $b_u \in ((q-1)\mathbb{Z})^r$, $\overline{P} = \{c_u \mid u \in P \cap M\}$ como en el teorema 2.14) entonces

$$d \leq n - \sum_{j=1}^{r} (-1)^{j+1} \sum_{i_1 < \cdots < i_j} l_{i_1} \cdots l_{i_j} (q-1)^{r-j}$$

Demostración. Sean $a_1^i, a_2^i, \ldots, a_{l_i}^i \in \mathbb{F}_q^*$ diferentes dos a dos para $i = 1, \ldots, r$.

Sea $f(t_1, \ldots, t_r) = t_1^{u_1} \cdots t_r^{u_r} \prod (t_i - a_1^i) \cdots (t_i - a_{l_i}^i)$. El número de ceros de f en T es igual a $\sum_{j=1}^{r} (-1)^{j+1} \sum_{i_1 < \cdots < i_j} l_{i_1} \cdots l_{i_j} (q-1)^{r-j}$ (por el principio de inclusión-exclusión).

Como f es una combinación lineal de monomios con exponentes en $(u+Q)\cap M$ y $\overline{u+Q}\subset\overline{P}$, se tiene que para cada monomio χ^{c_u} en f existe $b_u\in((q-1)\mathbb{Z})^r$ tal que $\chi^{c_u+b_u}\in \mathrm{H}^0(X_P,\mathcal{O}(D_P))$, además ambos monomios toman los mismos valores en T. Procediendo de la misma manera con todos los monomios de f se obtiene una función f' tal que $f'(t)=f(t)$, $\forall t\in T$ y $f'\in \mathrm{H}^0(X_P,\mathcal{O}(D_P))$. Por tanto una cota superior para la distancia mínima es

$$d\leq n-\sum_{j=1}^{r}(-1)^{j+1}\sum_{i_1<\cdots<i_j} l_{i_1}\cdots l_{i_j}(q-1)^{r-j}$$

□

3. Ejemplos y Conjeturas de Joyner

Consideramos dos ejemplos. El primero ilustra el cálculo de los parámetros de una sucesión de politopos $(P_r)_{r\geq 2}$ con $\dim(P_r)=r$ en los que la r-proyección de P_r es P_{r-1}. El segundo ejemplo muestra que la cota inferior de la distancia mínima usando teoría de intersección y la cota superior de la proposición 2.17 no siempre coinciden.

Ejemplo 2.18. Sea P_2 el politopo plano con vértices $(0,0)$, $(b_1,0)$, (b_1,b_2), $(0,b_2)$ con $b_1,b_2<q-1$. Este código es estudiado en [28, proposition 3.2].

El abanico normal $\triangle_{P_2}$ definido por P_2 tiene como bordes los conos generados por $v(\rho_1)=(1,0)$, $v(\rho_2)=(0,1)$, $v(\rho_3)=(-1,0)$ y $v(\rho_4)=(0,-1)$, el abanico del ejemplo 2.3. La variedad tórica X_{P_2} es regular.

$$P_2=\bigcap_{i=1}^{4}\{\langle u,\rho_i\rangle\geq -a_i\}$$

donde $a_1=0$, $a_2=0$, $a_3=b_1$, $a_4=b_2$. Por lo que se tiene que $D_P=\sum a_iV(\rho_i)=b_1V(\rho_3)+b_2V(\rho_4)$.

Como P_2 es un politopo plano el código $\mathcal{C}_{P_2}^t$ tiene longitud $n=(q-1)^2$. La aplicación de evaluación ev es inyectiva ya que verifica la restricción de inyectividad puesto que $b_1,b_2<q-1$ (teorema 2.14). Por tanto la dimensión del código $\mathcal{C}_{P_2}^t$ es

$$k=\dim \mathrm{H}^0(X_{P_2},\mathcal{O}(D_{P_2}))=\#P_2\cap M=(b_1+1)(b_2+1)$$

De la sección 2.1 se deduce que el máximo número de ceros de una función no nula f de $\mathrm{H}^0(X_{P_2},\mathcal{O}(D_{P_2}))$ es menor o igual que

$$a(q-1)+(q-1-a)(D_{P_2}-a(\mathrm{div}(\chi^{u_1}))_0\cdot(\mathrm{div}(\chi^{u_1}))_0)$$

donde $a\leq b_1$.

Se tiene $\mathrm{div}(\chi^{u_1})=\sum\langle u_1,v(\rho_i)\rangle V(\rho_i)=V(\rho_1)-V(\rho_3)$. Por lo que $(\mathrm{div}(\chi^{u_1}))_0=V(\rho_1)$.

Calculamos el número de intersección de los dos divisores usando volúmenes mixtos

$$\begin{aligned} D_{P_2} - a(\mathrm{div}(\chi^{u_1}))_0 \cdot (\mathrm{div}(\chi^{u_1}))_0 &= 2V_2(P_{D_{P_2}-a(\mathrm{div}(\chi^{u_1}))_0}, P_{(\mathrm{div}(\chi^{u_1}))_0}) \\ &= \mathrm{vol}_2(P_{D_{P_2}-a(\mathrm{div}(\chi^{u_1}))_0} + P_{(\mathrm{div}(\chi^{u_1}))_0}) \\ &\quad -\mathrm{vol}_2(P_{D_{P_2}-a(\mathrm{div}(\chi^{u_1}))_0}) \\ &\quad -\mathrm{vol}_2(P_{(\mathrm{div}(\chi^{u_1}))_0}) \\ &= ((b_1 - a + 1)b_2) - ((b_1 - a)b_2) - (0) \\ &= b_2 \end{aligned}$$

Porque

- $P_{D_{P_2}-a(\mathrm{div}(\chi^{u_1}))_0} + P_{(\mathrm{div}(\chi^{u_1}))_0}$ es el politopo de vértices $(a-1,0)$, $(b_1,0)$, (b_1,b_2) y $(a-1,b_2)$.
- $P_{D_{P_2}-a(\mathrm{div}(\chi^{u_1}))_0}$ es el politopo de vértices $(a,0)$, $(b_1,0)$, (b_1,b_2) y (a,b_2).
- $P_{(\mathrm{div}(\chi^{u_1}))_0}$ es el politopo de vértices $(-1,0)$ y $(0,0)$.

Por tanto el número de ceros de $f \in \mathrm{H}^0(X_{P_2}, \mathcal{O}(D_{P_2}))$ está acotado superiormente por

$$a(q-1-b_2) + (q-1)b_2 \leq b_1(q-1-b_2) + (q-1)b_2$$

y por consiguiente la distancia mínima está acotada por

$$d(\mathcal{C}_{P_2}^t) \geq (q-1)^2 - (b_1(q-1-b_2) + (q-1)b_2) = (q-1-b_1)(q-1-b_2)$$

Aplicando la proposición 2.17, con $u = 0$, $l_1 = b_1$ y $l_2 = b_2$, obtenemos que $u + Q \subset P_2$, de hecho $u + Q = P_2$, y obtenemos

$$d(\mathcal{C}_{P_2}^t) \leq (q-1)^2 - b_1(q-1) - b_2(q-1) + b_1b_2 = (q-1-b_1)(q-1-b_2)$$

Considerando ambas cotas, se tiene $d(\mathcal{C}_{P_2}^t) = (q-1-b_1)(q-1-b_2)$

Sea P_3 el politopo tridimensional con vértices $(0,0,0)$, $(b_1,0,0)$, $(b_1,b_2,0)$, $(0,b_2,0)$, $(0,0,b_3)$, $(b_1,0,b_3)$, (b_1,b_2,b_3), $(0,b_2,b_3)$ donde además $b_1, b_2, b_3 < q-1$. Es decir, el prisma rectangular de lados b_1, b_2, b_3.

El abanico normal $\triangle_{P_3}$ definido por P_3 tiene como bordes los conos generados por $v(\rho_1) = (1,0,0)$, $v(\rho_2) = (-1,0,0)$, $v(\rho_3) = (0,1,0)$, $v(\rho_4) = (0,-1,0)$, $v(\rho_5) = (0,0,1)$ y $v(\rho_6) = (0,0,-1)$. La variedad tórica X_{P_3} es regular.

$$P_3 = \bigcap_{i=1}^{6} \{\langle u, \rho_i \rangle \geq -a_i\}$$

donde $a_1 = 0$, $a_2 = b_1$, $a_3 = 0$, $a_4 = b_2$, $a_5 = 0$, $a_6 = b_3$. Por tanto $D_P = \sum a_i V(\rho_i) = b_1 V(\rho_2) + b_2 V(\rho_4) + b_3 V(\rho_6)$.

Como P_3 es un cono tridimensional, el código $\mathcal{C}^t_{P_3}$ tiene longitud $n = (q-1)^3$. La aplicación de evaluación ev es inyectiva ya que P_3 verifica la restricción de inyectividad puesto que $b_1, b_2, b_3 < q-1$ (teorema 2.14). Por tanto se tiene que la dimensión de $\mathcal{C}^t_{P_3}$ es

$$k = \dim \mathrm{H}^0(X_{P_3}, \mathcal{O}(D_{P_3})) = \#P_3 \cap M = (b_1+1)(b_2+1)(b_3+1)$$

De la sección 2.1 se deduce que el máximo número de ceros de una función no nula $f \in \mathrm{H}^0(X_{P_3}, \mathcal{O}(D_{P_3}))$ es menor o igual que

$$a(q-1) + ((q-1)^2 - a)(D_{P_3} \cdot C)$$

donde $C = \mathrm{V}(\{\chi^{u_1}, \chi^{u_2}\})$ y a es menor o igual que el máximo número de ceros de una función racional definida por la 3-proyección de P_3, i.e. P_2. Entonces $a \leq b_1(q-1-b_2) + (q-1)b_2$.

Se tiene que $\mathrm{div}(\chi^{u_1}) = \sum \langle u_1, v(\rho_i)\rangle V(\rho_i) = V(\rho_1) - V(\rho_2)$. Por tanto $(\mathrm{div}(\chi^{u_1}))_0 = V(\rho_1)$. $\mathrm{div}(\chi^{u_2}) = \sum \langle u_1, v(\rho_i)\rangle V(\rho_i) = V(\rho_3) - V(\rho_4)$. Por lo que $(\mathrm{div}(\chi^{u_2}))_0 = V(\rho_3)$.

Calculamos el número de intersección $D_{P_3} \cdot C$ usando volúmenes mixtos

$$\begin{aligned}
D_{P_3} \cdot C &= D_{P_3} \cdot (\mathrm{div}(\chi^{u_1}))_0 \cdot (\mathrm{div}(\chi^{u_2}))_0 \\
&= 3! V_3(P, P_{(\mathrm{div}(\chi^{u_1}))_0}, P_{(\mathrm{div}(\chi^{u_2}))_0}) \\
&= \mathrm{vol}_3(P_3 + P_{(\mathrm{div}(\chi^{u_1}))_0} + P_{(\mathrm{div}(\chi^{u_2}))_0}) - \mathrm{vol}_3(P_3 + P_{(\mathrm{div}(\chi^{u_1}))_0}) \\
&\quad -\mathrm{vol}_3(P_3 + P_{(\mathrm{div}(\chi^{u_2}))_0}) - \mathrm{vol}_3(P_{(\mathrm{div}(\chi^{u_1}))_0} + P_{(\mathrm{div}(\chi^{u_2}))_0}) \\
&\quad +\mathrm{vol}_3(P_3) + \mathrm{vol}_3(P_{(\mathrm{div}(\chi^{u_1}))_0}) + \mathrm{vol}_3(P_{(\mathrm{div}(\chi^{u_2}))_0}) \\
&= ((b_1+1)(b_2+1)(b_3)) - ((b_1+1)b_2b_3) - (b_1(b_2+1)b_3) - (0) \\
&\quad +(b_1b_2b_3) + (0) + (0) \\
&= b_3
\end{aligned}$$

Porque

- $P_3 + P_{(\mathrm{div}(\chi^{u_1}))_0} + P_{(\mathrm{div}(\chi^{u_2}))_0}$ es el politopo de vértices $(-1,-1,0)$, $(b_1,-1,0)$, $(b_1,b_2,0)$, $(-1,b_2,0)$, $(-1,-1,b_3)$, $(b_1,-1,b_3)$, (b_1,b_2,b_3) y $(-1,b_2,b_3)$.
- $P_3 + P_{(\mathrm{div}(\chi^{u_1}))_0}$ es el politopo de vértices $(-1,0,0)$, $(b_1,0,0)$, $(b_1,b_2,0)$, $(-1,b_2,0)$, $(-1,0,b_3)$, $(b_1,0,b_3)$, (b_1,b_2,b_3) y $(-1,b_2,b_3)$.
- $P_3 + P_{(\mathrm{div}(\chi^{u_2}))_0}$ es el politopo de vértices $(0,-1,0)$, $(b_1,-1,0)$, $(b_1,b_2,0)$, $(0,b_2,0)$, $(0,-1,b_3)$, $(b_1,-1,b_3)$, (b_1,b_2,b_3) y $(0,b_2,b_3)$.
- $P_{(\mathrm{div}(\chi^{u_1}))_0} + P_{(\mathrm{div}(\chi^{u_2}))_0}$ es el politopo de vértices $(0,0,0)$, $(-1,0,0)$, $(-1,-1,0)$ y $(0,-1,0)$.
- P_3 es el politopo de vértices $(0,0,0)$, $(b_1,0,0)$, $(b_1,b_2,0)$, $(0,b_2,0)$, $(0,0,b_3)$, $(b_1,0,b_3)$, (b_1,b_2,b_3) y $(0,b_2,b_3)$.
- $P_{(\mathrm{div}(\chi^{u_1}))_0}$ es el politopo de vértices $(-1,0,0)$ y $(0,0,0)$.
- $P_{(\mathrm{div}(\chi^{u_2}))_0}$ es el politopo de vértices $(0,-1,0)$ y $(0,0,0)$

Por tanto el máximo número de ceros $f \in \mathrm{H}^0(X_{P_3}, \mathcal{O}(D_{P_3}))$ está acotado superiormente por

$$a(q-1-b_3)+(q-1)^2b_3 \leq (b_1(q-1-b_2)+(q-1)b_2)(q-1-b_3)+(q-1)^2b_3$$

y por consiguiente la distancia mínima está acotada por

$d(\mathcal{C}_{P_3}^t) \geq n - ((b_1(q-1-b_2)+(q-1)b_2)(q-1-b_3)+(q-1)^2b_3) = (q-1-b_1)(q-1-b_2)(q-1-b_3)$.

Aplicando la proposición 2.17, con $u=0$, $l_1=b_1$, $l_2=b_2$ y $l_3=b_3$, se tiene que $u+Q \subset P_3$, de hecho $u+Q=P_3$, y obtenemos

$$d(\mathcal{C}_{P_3}^t) \leq (q-1-b_1)(q-1-b_2)(q-1-b_3)$$

Considerando ambas cotas, se tiene

$$d(\mathcal{C}_{P_3}^t) = (q-1-b_1)(q-1-b_2)(q-1-b_3)$$

Calculando la cota superior e inferior de un hipercubo P_r de dimensión r de lados $b_1, \ldots, b_r < q-1$ se obtiene que la distancia mínima $d_r = d(\mathcal{C}_{P_r}^t)$ de $\mathcal{C}_{P_r}^t$ es

$$d_2 = (q-1-b_1)(q-1-b_2)$$

$$d_r = (q-1)^r - ((q-1)^{r-1} - d_{r-1})(q-1-b_r) - b_r(q-1)^{r-1}, \ \forall\ r \geq 3$$

y se comprueba por inducción en r que es igual a

$$d_r = (q-1-b_1)\cdots(q-1-b_r)$$

Por tanto, el código $\mathcal{C}_{P_r}^t$ asociado al hipercubo de lados $b_1, \ldots, b_r$ tiene parámetros $[(q-1)^r, \prod(b_i+1), \prod(q-1-b_i)]$. En [45] usando una generalización de determinantes de Vandermonde en varias variables se estudia esta misma sucesión de códigos.

En todos los ejemplos de J.P. Hansen [28, 29] para politopos planos, así como en el ejemplo anterior se tiene que la cota inferior de la distancia mínima, usando teoría de intersección, y la cota superior de la proposición 2.17 coinciden. El siguiente ejemplo muestra que ambas cotas no siempre coinciden.

Ejemplo 2.19. Sea P el politopo plano de vértices $(0,0)$, $(b,0)$, $(2b,b)$, $(2b,2b)$, $(b,2b)$, $(0,b)$ con $b < q-1$.

El abanico normal $\triangle_P$ definido por P tiene como bordes los conos generados por $v(\rho_1)=(1,0)$, $v(\rho_2)=(0,1)$, $v(\rho_3)=(-1,1)$, $v(\rho_4)=(-1,0)$, $v(\rho_5)=(0,-1)$, $v(\rho_6)=(1,-1)$. La variedad tórica X_P es regular.

$$P = \bigcap_{i=1}^{6} \{\langle u, v(\rho_i)\rangle \geq -a_i\}$$

donde $a_1=0$, $a_2=0$, $a_3=b$, $a_4=2b$, $a_5=2b$, $a_6=b$. Por lo que $D_P = \sum a_i V(\rho_i) = bV(\rho_3) + 2bV(\rho_4) + 2bV(\rho_5) + V(\rho_6)$.

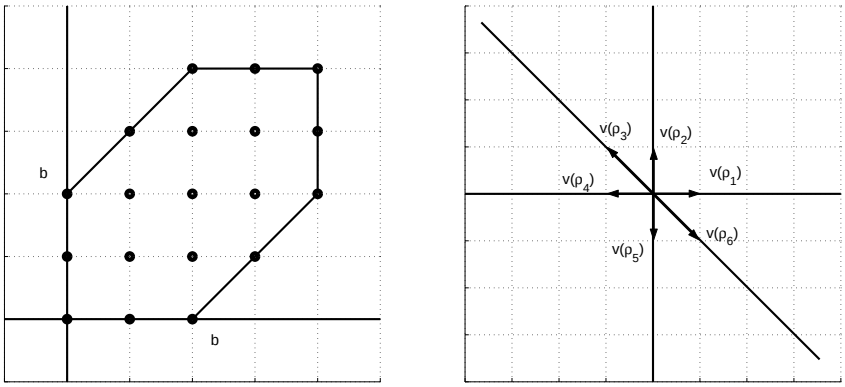

FIGURA 4. P y su abanico normal.

Como P es un politopo plano el código $\mathcal{C}_P$ tiene longitud $n = (q-1)^2$. La aplicación de evaluación ev es inyectiva ya que P verifica la restricción de inyectividad puesto que $b < q-1$. Por tanto se tiene que la dimensión de $\mathcal{C}_P^t$ usando la fórmula de Pick (lema 2.15) es

$$k = \dim \mathrm{H}^0(X_P, \mathcal{O}(D_P)) = \mathrm{vol}_2(P) + \frac{\text{Perímetro}(P)}{2} + 1 = 3b^2 + 3b + 1$$

De la sección 2.1 se deduce que el máximo número de ceros de una función no nula $f \in \mathrm{H}^0(X_P, \mathcal{O}(D_P))$ es menor o igual que

$$a(q-1) + (q-1-a)(D_P - a(\mathrm{div}(\chi^{u_1}))_0 \cdot (\mathrm{div}(\chi^{u_1}))_0)$$

donde $a \leq 2b$.

Se tiene que $\mathrm{div}(\chi^{u_1}) = \sum \langle u_1, v(\rho_i)\rangle V(\rho_i) = V(\rho_1) - V(\rho_3) - V(\rho_4) + V(\rho_6)$. Por lo que $(\mathrm{div}(\chi^{u_1}))_0 = V(\rho_1) + V(\rho_6)$.

Calculamos el número de intersección de los dos divisores usando volúmenes mixtos

$$\begin{aligned} D_P - a(\mathrm{div}(\chi^{u_1}))_0 \cdot (\mathrm{div}(\chi^{u_1}))_0 &= 2V_2(P_{D_P - a(\mathrm{div}(\chi^{u_1}))_0}, P_{(\mathrm{div}(\chi^{u_1}))_0}) \\ &= \mathrm{vol}_2(P_{D_P - a(\mathrm{div}(\chi^{u_1}))_0} + P_{(\mathrm{div}(\chi^{u_1}))_0}) \\ &\quad -\mathrm{vol}_2(P_{D_P - a(\mathrm{div}(\chi^{u_1}))_0}) \\ &\quad -\mathrm{vol}_2(P_{(\mathrm{div}(\chi^{u_1}))_0}) \\ &= (3b^2 - 2ab + 2b) - (3b^2 - 2ab) - (0) \\ &= 2b \end{aligned}$$

Porque

- $P_{D_P - a(\mathrm{div}(\chi^{u_1}))_0} + P_{(\mathrm{div}(\chi^{u_1}))_0}$ es el politopo de vértices $(a-1, 0)$, $(b, 0)$, $(2b, b)$, $(2b, 2b)$, $(b + a - 1, 2b)$ y $(a-1, b-a)$.

- $P_{D_P - a(\mathrm{div}(\chi^{u_1}))_0}$ es el politopo de vértices $(a,0)$, $(b,0)$, $(2b,b)$, $(2b,2b)$, $(b+a,2b)$ y $(a,b-a)$.
- $P_{(\mathrm{div}(\chi^{u_1}))_0}$ es el politopo de vértices $(-1,0)$ y $(0,0)$.

Por tanto el número de ceros de $f \in \mathrm{H}^0(X_P, \mathcal{O}(D_P))$ está acotado superiormente por

$$a(q-1-2b) + (q-1)2b \leq 2b(q-1-2b) + (q-1)2b = 4b(q-1) - 4b^2$$

y por consiguiente la distancia mínima está acotada por

$$d \geq n - (4b(q-1) - 4b^2) = (q-1)^2 - 4b(q-1) + 4b^2$$

Aplicamos la proposición 2.17 para obtener una cota superior de la distancia mínima, consideramos un segmento de longitud $2b$ y un cuadrado de lado b en P.

Sea $u = (0,b)$ y $Q = \{0,1,\ldots,2b\} \times \{0\}$, $u + Q \subset P$. Por lo que $d \leq (q-1)^2 - 2b(q-1)$.

Sea $u = (0,0)$ y $Q = \{0,1,\ldots,b\} \times \{0,1,\ldots,b\}$, $u + Q \subset P$. Por lo que $d \leq (q-1)^2 - (2b(q-1) - b^2)$. Entonces

$$(q-1)^2 - 4b(q-1) + 4b^2 < (q-1)^2 - 2b(q-1) < (q-1)^2 - (2b(q-1) - b^2)$$

y por tanto la cota inferior calculada usando teoría de intersección no coincide con ninguna de las cotas superiores.

A continuación probamos que las conjeturas 4.2 y 4.3 de [38] no son ciertas. Como contraejemplos consideramos un código del teorema 1.2 de [29] y un código del teorema 1.3 de [29] respectivamente.

CONJETURA 2.20. *[38, Conjecture 4.2]: Sea $\mathcal{C}(E,D,X)$ [38, definition (5), section 3.1] un código tórico asociado al 1-ciclo E, el divisor de Cartier T-invariante D y la variedad tórica X. Sea*

- *X una variedad tórica no singular de dimensión r.*
- *n lo suficientemente grande de tal manera que exista un entero $N > 1$ tal que $2N\mathrm{vol}_r(P_D) \leq n \leq 2N^2\mathrm{vol}_r(P_D)$*

Si q es "suficientemente grande" entonces todo $f \in \mathrm{H}^0(X, \mathcal{O}(D))$ tiene a lo sumo n ceros en los puntos racionales de X. Consecuentemente,

$$d \geq n - 2N\mathrm{vol}_r(P_D)$$

Aquí "suficientemente grande" puede depender de X, C y D pero no de f.

CONTRAEJEMPLO 2.21. Damos un contraejemplo a la conjetura anterior. Sea $\mathcal{C}_P$ un código asociado al politopo plano P de vértices $(0,0)$, $(1,1)$, $(0,2)$. En [29] se muestra que $\mathcal{C}_P$ tiene longitud $n = (q-1)^2$ y distancia mínima $d = (q-1)^2 - 2(q-1)$. La variedad tórica no singular X es $X_\triangle$, donde $\triangle$ es el abanico cuyos bordes están generados por $v(\rho_1) = (1,0)$, $v(\rho_2) = (-1,1)$,

$v(\rho_3) = (-1, 0)$, $v(\rho_4) = (-1, -1)$. E es la suma formal de todos los puntos de T porque $\mathcal{C}_P$ es un código tórico estándar. Consideramos $D = D_P$, es decir el divisor de Cartier que define P, $D = V(\rho_3) + V(\rho_4)$ y se tiene $\mathrm{vol}_r(P_D) = \mathrm{vol}_r(P) = 1$.

Por el teorema 2.14 sabemos q "suficientemente grande" significa $q \geq 3$. Probaremos que la conjetura es falsa para $q \geq 5$ en este ejemplo, sea q mayor o igual que 5 y $N = q - 2$.

$$2N\mathrm{vol}_r(P_D) \leq n \leq 2N^2\mathrm{vol}_r(P_D) \Leftrightarrow 2(q-2) \leq (q-1)^2 \leq 2(q-2)^2$$

que se verifica para $q \geq 5$.

La conjetura dice que la distancia mínima satisface la desigualdad

$$d \geq n - 2N\mathrm{vol}_r(P_D) = (q-1)^2 - 2(q-2) > (q-1)^2 - 2(q-1) = d$$

por tanto para $q \geq 5$ la conjetura da una cota inferior de la distancia mínima estrictamente mayor que la distancia mínima, por lo tanto la conjetura es falsa.

Conjetura 2.22. *[38, Conjecture 4.3]: Sea $\mathcal{C}(E, D, X)$ [38, definition (5), section 3.1] el código tórico asociado al 1-ciclo E, el divisor de Cartier T-invariante D y la variedad tórica X. Sea*

- *X una variedad tórica no singular de dimensión r.*
- *$\psi_D(v) = \mathrm{mín}_{u \in P_D \cap M} \langle u, v \rangle$ estrictamente convexa*
- *$\deg(E) > \deg(D^r)$*

Si q es "suficientemente grande" entonces cualquier $f \in \mathrm{H}^0(X, \mathcal{O}(D))$ tiene a lo sumo n ceros en los puntos racionales de X. Consecuentemente,

$$k \geq \dim \mathrm{H}^0(X, \mathcal{O}(D)) = \#P_D \cap M$$

$$d \geq n - r!(\#P_D \cap M)$$

Además si $n > r!(\#P_D \cap M)$ entonces $\dim \mathrm{H}^0(X, \mathcal{O}(D)) = \#P_D \cap M$

Contraejemplo 2.23. Damos un contraejemplo a la conjetura anterior. Sea $\mathcal{C}_P$ el código asociado al politopo P de vértices $(0, 0)$, $(1, 0)$, $(0, 1)$. En [29] se muestra que el código $\mathcal{C}_P$ tiene longitud $n = (q-1)^2$ y distancia mínima igual a $d = (q-1)^2 - (q-1)$. La variedad tórica no singular X es $X_\triangle$, donde $\triangle$ es el abanico cuyos bordes están generados por $v(\rho_1) = (1, 0)$, $v(\rho_2) = (0, 1)$, $v(\rho_3) = (-1, -1)$, i.e. $X = \mathbb{P}^2$. E es la suma formal de todos los puntos de T porque $\mathcal{C}$ es un código tórico estándar. Consideramos $D = D_P$, es decir el divisor de Cartier que define P, $D = V(\rho_3)$, por tanto se tiene que ψ_D es estrictamente convexa [21, pag 70]. Para $P = P_D$ se tiene que $\#P \cap M = 3$. Y $(q-1)^2 = \deg(E) > \deg(D) = 1$

Por el teorema 2.14 sabemos que "suficientemente grande" significa $q \geq 3$. Probaremos que la conjetura no se verifica en este ejemplo para $q \geq 8$, sea q mayor o igual que 8.

La conjetura dice que la distancia mínima verifica la desigualdad

$$d \geq n - r!(\#P_D \cap M) = (q-1)^2 - 2 \cdot 3 > (q-1)^2 - (q-1) = d$$

por tanto para $q \geq 8$ la conjetura da una cota inferior estrictamente mayor que la distancia mínima, por lo tanto la conjetura es falsa.

CAPÍTULO 3

Códigos Tóricos Generalizados

En este capítulo definimos y estudiamos los códigos tóricos generalizados que son una extensión de los códigos tóricos estudiados en el capítulo 2. Los códigos tóricos generalizados son códigos de evaluación en el toro algebraico, la extensión consiste en evaluar elementos de un álgebra de polinomios arbitraria en lugar de polinomios con monomios cuyos exponentes son los puntos del retículo de un politopo. Los códigos tóricos generalizados son multicíclicos, el propósito de este capítulo es estudiar su estructura multicíclica y métrica. Dicho estudio nos va a permitir calcular su dual y estimar su distancia mínima.

Sea $U \subset H = \{0, \ldots, q-2\} \times \cdots \times \{0, \ldots, q-2\}$, $T = (\mathbb{F}_q^*)^r$ y $\mathbb{F}_q[U]$ el $\mathbb{F}_q$-espacio vectorial

$$\mathbb{F}_q[U] = \langle Y^u = Y_1^{u_1} \cdots Y_r^{u_r} \mid u = (u_1, \ldots, u_r) \in U \rangle \subset \mathbb{F}_q[Y_1, \ldots, Y_r]$$

El **código tórico generalizado** $\mathcal{C}_U$ es la imagen de la aplicación $\mathbb{F}_q$-lineal

$$\begin{array}{rccc} \text{ev} : \mathbb{F}_q[U] & \to & \mathbb{F}_q^n \\ f & \mapsto & (f(t))_{t \in T} \end{array}$$

Donde $n = \#T = (q-1)^r$. Algunos resultados de códigos tóricos son válidos para códigos tóricos generalizados. Concretamente, el siguiente resultado permite concluir que la aplicación de evaluación ev es inyectiva y por tanto la dimensión del código tórico $\mathcal{C}_U$ es $k = \#U$.

LEMA 3.1. *Sea $U \subset H$, consideramos*

$$f = \sum_{u \in U} \lambda_u Y^u, \quad \lambda_u \in \mathbb{F}_q$$

Entonces $(f(t))_{t \in T} = (0)_{t \in T}$ si y sólo si $\lambda_u = 0, \ \forall \ u \in H$.

La demostración del resultado anterior es la misma que la del lema 2.13 de códigos tóricos por lo que no la reproducimos. Esto se debe a que el lema 2.13 demuestra que un polinomio no nulo que es combinación lineal de monomios con exponentes en H no se anula completamente en T y no hace uso de que los exponentes sean puntos del retículo de un politopo.

Aunque hemos definido los códigos tóricos generalizados para $U \subset H$ como la evaluación de $\mathbb{F}_q[U]$ en T, esta familia de códigos incluye todos los códigos definidos como la evaluación de polinomios de una subálgebra

$\mathbb{F}_q[Y_1, \ldots, Y_r]$ en T. El siguiente resultado muestra este fenómeno que habíamos anunciado al comienzo del capítulo.

PROPOSICIÓN 3.2. *Sea $V \subset \mathbb{Z}^r$, $\mathbb{F}_q[V] = \langle Y^v \mid v \in V \rangle$ y $\mathcal{C}_V$ el código definido por la imagen de la aplicación de evaluación en T*

$$\begin{array}{rccc} \mathrm{ev} : \mathbb{F}_q[V] & \to & \mathbb{F}_q^n \\ f & \mapsto & (f(t))_{t \in T} \end{array}$$

Sea $v \in \mathbb{Z}^r$, como en el capítulo anterior escribimos $V = c_v + b_v$ donde $c_v \in H$ y $b_v \in ((q-1)\mathbb{Z})^r$. También denotamos $\overline{v} = c_v$. Entonces $\mathcal{C}_U = \mathcal{C}_V$, donde $U = \overline{V} \subset H$.

DEMOSTRACIÓN. Sea $f = \sum_{v \in V} \lambda_v Y^v \in \mathbb{F}_q[V]$ y $t \in T$. Entonces

$$f(t) = \sum_{v \in V} \lambda_v t^{c_v + b_v} = \sum_{v \in V} \lambda_v t^{c_v}$$

Y se tiene el resultado. □

Sea P un politopo en $M_{\mathbb{R}}$, por la proposición 3.2 se tiene que $\mathcal{C}_P^t = \mathcal{C}_U$ con $U = \overline{P}$. Por tanto todos los resultados para códigos tóricos generalizados serán válidos en particular para códigos tóricos.

Una extensión no tan general pero análoga a la que se da entre los códigos tóricos y los códigos tóricos generalizados se da entre los códigos de Reed-Muller y los códigos hiperbólicos de [22] y sus referencias.

1. Estructura Multicíclica de los Códigos Tóricos Generalizados

Los códigos multicíclicos pueden entenderse como palabras invariantes por ciertas permutaciones cíclicas o bien como ideales de una cierta álgebra polinomial. En [11] se prueba que un código tórico definido a partir de una superficie tórica ($r = 2$) es multicíclico usando una representación matricial de las palabras del código, aunque se conjeturó el resultado para dimensión arbitraria. Dicha prueba es difícil de extender para politopos o superficies tóricas de dimensión arbitraria porque se deben considerar arreglos r-dimensionales, es decir el análogo r-dimensional del concepto de matriz que se considera bidimensional. Mediante una representación polinómica del código veremos que un código tórico generalizado con r arbitraria es multicíclico.

Sea $\mathcal{C} \subset \mathbb{F}_q^n$ un código lineal. Se dice que $\mathcal{C}$ es un **código cíclico** si se verifica que $\mathcal{C}$ es invariante por permutaciones cíclicas, es decir si $c = (c_0, c_1, \ldots, c_{n-1}) \in \mathcal{C}$ entonces $(c_{n-1}, c_0, c_1, \ldots, c_{n-2}) \in \mathcal{C}$.

Sea $\mathbb{F}_q[X]_{\leq n-1}$ el $\mathbb{F}_q$-espacio vectorial de polinomios con grado menor que n y A en anillo cociente $\mathbb{F}_q[X]/(X^n - 1)$. Dado que $\mathbb{F}_q^n$, $\mathbb{F}_q[X]_{\leq n-1}$ y A son espacios vectoriales sobre el mismo cuerpo de la misma dimensión

finita n, se tiene que son isomorfos. Y por tanto podemos considerar los isomorfismos

$$\mathbb{F}_q^n \simeq \mathbb{F}_q[X]_{\leq n-1} \simeq \mathbb{F}_q[X]/(X^n - 1)$$

podemos identificar $(c_0, c_1, \ldots, c_{n-1})$, el polinomio $c_0 + c_1X + \cdots + c_{n-1}X^{n-1}$ y la clase $c_0 + c_1X + \cdots + c_{n-1}X^{n-1} + (X^n - 1)$. En la práctica se usa la notación más conveniente en cada momento. La notación polinómica en el álgebra A permite considerar las permutaciones cíclicas mediante la multiplicación por polinomios, ya que un código $\mathcal{C} \subset A$ es cíclico si y sólo si es un ideal en A.

Los códigos cíclicos han sido ampliamente estudiados y utilizados en la práctica [47]. Una extensión de los códigos cíclicos son los códigos multicíclicos [54]. Un código $\mathcal{C} \subset A = \mathbb{F}_q[X_1, \ldots, X_r]/(X_1^{N_1} - 1, \ldots, X_r^{N_r} - 1)$ es **multicíclico o r-D cíclico** si es un ideal en A, con $N_1, \ldots, N_r \in \mathbb{N}$. Sea $\mathbb{F}_q[X_1, \ldots, X_r]_{\leq (N_1-1,\ldots,N_r-1)}$ el $\mathbb{F}_q$ espacio vectorial de polinomios en las variables $X_1, \ldots, X_r$ con grado en la variable X_i menor que N_i para todo i. Al igual que en los códigos cíclicos podemos considerar los isomorfismos de espacios vectoriales

$$\mathbb{F}_q^n \simeq \mathbb{F}_q[X_1, \ldots, X_r]_{\leq (N_1-1,\ldots,N_r-1)} \simeq A$$

donde $n = N_1 \cdots N_r$. Además, podemos identificar sus elementos como en los códigos cíclicos.

Sea $\mathcal{C}_U$ el código tórico generalizado con $U \subset H$. Sea α un elemento primitivo de $\mathbb{F}_q$, i.e. $\mathbb{F}_q^* = \{\alpha^0, \alpha^1, \ldots, \alpha^{q-2}\}$ y por tanto se tiene que $T = \{\alpha^i = (\alpha^{i_1}, \ldots, \alpha^{i_r}) \mid i \in H\}$. De esta forma el código $\mathcal{C}_U$ es el subespacio vectorial de $\mathbb{F}_q^n$ generado por $\{(Y^u(\alpha^i))_{i\in H} \mid u \in U\}$, donde se tiene que $Y^u(\alpha^i) = \alpha^{\langle u,i\rangle} = \alpha^{u_1 i_1 + \cdots + u_n i_n}$. Para estudiar su estructura multicíclica, en virtud del isomorfismo anterior, vamos a considerar las palabras como polinomios o clases de polinomios en A en lugar de como n-uplas y denotamos el código $\mathcal{C}_U$ en A como C_U^A. Concretamente, representamos

$$(\alpha^{\langle u,i\rangle})_{i\in H} \in \mathcal{C}_U \text{ por } \sum_{i\in H} \alpha^{\langle u,i\rangle} X^i \in \mathcal{C}_U^A$$

Sea $U \subset H$, $A = \mathbb{F}_q[X_1, \ldots, X_r]/(X_1^{q-1} - 1, \ldots, X_r^{q-1} - 1)$, el código $\mathcal{C}_U^A \subset A$ que es isomorfo a $\mathcal{C}_U \subset \mathbb{F}_q^n$ es

$$\mathcal{C}_U^A = \{\sum_{u\in U} \lambda_u \sum_{i\in H} \alpha^{\langle u,i\rangle} X^i \mid \lambda_u \in \mathbb{F}_q\} \subset A$$

PROPOSICIÓN 3.3. *Sea $U \subset H = (\{0, \ldots, q-2\})^r$, $\mathcal{C}_U^A$ es un código r-D cíclico con $N_1 = q - 1$, ..., $N_r = q - 1$.*

DEMOSTRACIÓN. Sea $u \in U$, $\sum_{i\in H} \alpha^{\langle u,i\rangle} X^i \in \mathcal{C}_U^A$.

$$X^a \sum_{i\in H} \alpha^{\langle u,i\rangle} X^i = \sum_{i\in H} \alpha^{u_1(i_1-a_1)+\cdots+u_r(i_r-a_r)} X^i = \alpha^{-\langle u,a\rangle} \sum_{i\in H} \alpha^{\langle u,i\rangle} X^i$$

Y se tiene el resultado por la linealidad de $\mathcal{C}_U^A$. □

Además del producto de polinomios en $\mathbb{F}_q[H]$ que denotamos por $\cdot$, $Y^u \cdot Y^v = Y^{u+v}$, podemos considerar la estructura multiplicativa del álgebra A en $\mathbb{F}_q[H]$. Para la base de A dada por $\{X^i\}_{i\in H}$ consideramos producto $X^i * X^j = X^{i+j}$. El siguiente resultado describe la operación $*$ en $\mathbb{F}_q[H]$ que será utilizada en el teorema 3.5.

PROPOSICIÓN 3.4. *Denotamos* $\mathrm{ev}^{-1}(X^i)$ *como* X^i *en* $\mathbb{F}_q[H]$*, entonces*

$$X^i * Y^u = \alpha^{-\langle u,i\rangle} * Y^u$$

$$Y^u * Y^v = \begin{cases} 0 & \text{si } u \neq v \\ (-1)^r Y^u & \text{si } u = v \end{cases}$$

DEMOSTRACIÓN. Por los siguientes isomorfismos considerados anteriormente

$$\begin{array}{ccccc} \mathbb{F}_q[H] & \longleftrightarrow & \mathbb{F}_q^n & \longleftrightarrow & A \\ Y^u & \mapsto & (\alpha^{\langle u,i\rangle})_{i\in H} & \leftrightarrow & \sum_{i\in H} \alpha^{\langle u,i\rangle} X^i \end{array} \tag{1}$$

se tiene que

$$X^i * Y^u = X^i * \sum \alpha^{\langle u,j\rangle} X^j = \alpha^{-\langle u,i\rangle} Y^u$$

$$Y^u * Y^v = \sum \alpha^{\langle u,i\rangle} X^i * Y^v = \sum \alpha^{\langle u-v,i\rangle} Y^v =$$

$$= \begin{cases} \sum_{i\in H} \alpha^{\langle u-v,i\rangle} Y^v = \frac{q(q-1)}{2}(\sup(u-v)) = 0 & \text{si } u \neq v \\ \sum_{i\in H} Y^u = (-1)^r Y^u & \text{si } u = v \end{cases}$$

donde $\sup(u-v)$ es el número de coordenadas de $u-v$ distintas de cero.

□

Del resultado anterior se deduce que $\mathbb{F}_q[H]$ puede representarse por

$$\mathbb{F}_q[H] = \mathbb{F}_q[Y^u, u \in H]/\langle Y^u * Y^u - (-1)^r Y^u, Y^u * Y^v (u \neq v)\rangle$$

donde además

$$X^i = (-1)^r \sum_{u\in H} \alpha^{-\langle u,i\rangle} Y^u$$

En particular, $\mathrm{ev}(1_Y) = \sum_{i\in H} X^i$ y $\mathrm{ev}^{-1}(1_X) = -\sum_{u\in H} Y^u$.

El siguiente resultado muestra que todo código lineal sobre un cuerpo finito con q elementos que es r-D cíclico con $N_1 = q-1, \ldots, N_r = q-1$ es un código tórico generalizado. Por tanto, los códigos tóricos generalizados y los los r-D códigos cíclicos con $N_1 = q-1, \ldots, N_r = q-1$ son la misma familia de códigos

TEOREMA 3.5. *Sea* $J \subset \mathbb{F}_q[X_1, \ldots, X_r]/(X_1^{q-1} - 1, \ldots, X_r^{q-1} - 1)$ *un ideal, entonces existe* $U \subset H$ *tal que* $J = \mathcal{C}_U^A$.

DEMOSTRACIÓN. Puesto que A es isomorfo a $\mathbb{F}_q[H]$ por (1) y que $\{Y^u \mid u \in H\}$ es una base de $\mathbb{F}_q[H]$, tenemos que $\{\mathrm{ev}(Y^u) \mid u \in H\}$ es una base de A, donde $\mathrm{ev}(Y^u) = \sum_{i \in H} \alpha^{\langle u,i \rangle} X^i \in A$.

Sean $\sum_{v \in H} \lambda_v \mathrm{ev}(Y^v) \in J$ y $u \in H$, por la proposición 3.4 se tiene que $\mathrm{ev}(Y^u) \sum_{v \in H} \lambda_v \mathrm{ev}(Y^v) = (-1)^r \lambda_u ev(Y^u) \in J$. Por lo que $\mathrm{ev}(Y^u) \in J$ si $\lambda_u \neq 0$. Procediendo de la misma manera con todos los generadores de J y u en H, obtenemos U tal que $J = (\mathrm{ev}(Y^u) \mid u \in U)$.

2. Estructura Métrica de los Códigos Tóricos Generalizados

En esta sección estudiamos la estructura métrica dada por la forma bilineal B introducida en la sección 1, $B(x,y) = \sum_{i=1}^n x_i y_i$ con $x, y \in \mathbb{F}_q^n$. El siguiente resultado permite considerar la estructura métrica de $\mathcal{C}_U \subset \mathbb{F}_q^n$ en $\mathbb{F}_q[H]$ y calcular explícitamente su código dual.

TEOREMA 3.6. *Conservando la notación anterior, sean* $u, v \in H$, *se tiene que*

$$B(\mathrm{ev}(Y^u), \mathrm{ev}(Y^v)) = \begin{cases} 0 & \text{si } \overline{u+v} \neq 0 \\ (-1)^r & \text{si } \overline{u+v} = 0 \end{cases}$$

Sean $u \in H$, $u' = \overline{-u}$ *con* $\overline{u}$ *como en la proposición 3.2 y* $U' = \{u' \mid u \in U\}$, $\#U = \#U'$. *Sea* $U \subset H$ *y* $U^\perp = H \setminus U' = (H \setminus U)'$, *entonces el código dual de* $\mathcal{C}_U$ *es* $\mathcal{C}_U^\perp = \mathcal{C}_{U^\perp}$

DEMOSTRACIÓN. Sea $u \in U$, $v \in U^\perp$, entonces se tiene que $B((\alpha^{\langle u,i \rangle})_{i \in H}, (\alpha^{\langle v,i \rangle})_{i \in H}) = \sum_{i \in H} \alpha^{\langle u+v,i \rangle}$

$$\sum_{i \in H} \alpha^{\langle u+v,i \rangle} = \sum_{i \in H} \alpha^{\langle \overline{u+v},i \rangle} = \begin{cases} \frac{q(q-1)}{2}(\sup(\overline{u+v})) = 0 & \text{si } \overline{u+v} \neq 0 \\ \sum_{i \in H} 1 = (-1)^r & \text{si } \overline{u+v} = 0 \end{cases}$$

donde $\sup(\overline{u+v})$ es el número de coordenadas de $\overline{u+v}$ distintas de cero.

Entonces $B(\mathrm{ev}(Y^u), \mathrm{ev}(Y^v)) = 0$ para todo $u \in U$, $v \in U^\perp$ puesto que $\overline{u+v} \neq 0$. Y se tiene el resultado por las dimensiones de $\mathbb{F}_q[U]$ y $\mathbb{F}_q[U^\perp]$ y la linealidad de los códigos. □

Como puede observarse en el resultado anterior, en general el dual de un código tórico $\mathcal{C}_{P_1}$ no es un código tórico, únicamente lo es cuando existe un politopo P_2 tal que $\overline{P_1}^{\perp} = \overline{P_2}$. En cambio el dual de un código tórico generalizado sí que es un código tórico generalizado.

NOTA 3.7. Los resultados de este capítulo pueden encontrarse en [56, 57]. Un resultado similar al del teorema 3.6 ha sido obtenido de forma independiente en [4].

Se tiene que la matriz M del morfismo de evaluación $\mathrm{ev} : \mathbb{F}_q[H] \to \mathbb{F}_q^n$ es

$$\begin{pmatrix} \alpha^{\langle u_1,i_1\rangle} & \alpha^{\langle u_1,i_2\rangle} & \dots & \dots & \alpha^{\langle u_1,i_n\rangle} \\ \alpha^{\langle u_2,i_1\rangle} & \alpha^{\langle u_2,i_2\rangle} & \dots & \dots & \alpha^{\langle u_2,i_n\rangle} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \alpha^{\langle u_n,i_1\rangle} & \alpha^{\langle u_n,i_2\rangle} & \dots & \dots & \alpha^{\langle u_n,i_n\rangle} \end{pmatrix}$$

donde $\{u_1, \dots, u_n\} = \{i_1, \dots, i_n\} = H$ y si además $u_j = i_j$ entonces M es una matriz simétrica, por tanto suponemos que $u_j = i_j \ \forall j = 1, \dots, n$.

Por tanto, una matriz generatriz del código $\mathcal{C}_U$ con $U \subset H$, $k = \#U$, es la $(k \times n)$-matriz compuesta por las k filas $\alpha^{\langle u,i_1\rangle}, \dots, \alpha^{\langle u,i_n\rangle}$ de M con $u \in U$ y una matriz de control es la $(n-k \times n)$-matriz compuesta por las $n-k$ filas $\alpha^{\langle u,i_1\rangle}, \dots, \alpha^{\langle u,i_n\rangle}$ de M con $u \in U^{\perp}$. O, equivalentemente, la matriz traspuesta de la matriz de control es la $(n \times n-k)$-matriz compuesta por las $n-k$ columnas $\alpha^{\langle u_1,i\rangle}, \dots, \alpha^{\langle u_n,i\rangle}$ de M con $i \in U^{\perp}$ puesto que suponemos $u_j = i_j \ \forall j = 1, \dots, n$.

Del conocimiento del código dual se deduce el siguiente resultado para estimar la distancia mínima. Esta proposición es análoga a [45, Proposition 2.1] para códigos tóricos pero cuya prueba es también válida para códigos tóricos generalizados. Usando la matriz de control se simplifican los cálculos con respecto a la matriz generatriz.

PROPOSICIÓN 3.8. *Sea $U \subset H$ y d un entero positivo. Si $\forall\ S \subset H$ con $\#S = d-1$ existe $V \subset U^{\perp}$ con $\#V = d-1$ tal que la submatriz de $M(S,V)$ tiene determinante distinto de cero entonces $d(\mathcal{C}_U) \geq d$, donde $M(S,V)$ es la submatriz de la matriz de evaluación M correspondiente a las filas de S y las columnas de V, i.e. $M(S,V) = (\alpha^{\langle u_S,i_V\rangle})_{u_S \in S, i_V \in V}$.*

DEMOSTRACIÓN. Por la proposición 1.3, se tiene que la distancia mínima de un código lineal es mayor o igual que d si $d-1$ columnas cualesquiera de una matriz de control son linealmente independientes. Una matriz de control de $\mathcal{C}_U$ es $M(U^{\perp})$. Por lo que la distancia mínima de $\mathcal{C}_U$ es mayor o igual que d si $d-1$ columnas de $M(U^{\perp})$ cualesquiera son linealmente independientes, que es equivalente a que haya una submatriz cuadrada de tamaño $d-1$ de $M(U^{\perp})$ con determinante distinto de cero. □

Sea $\sigma(u) = u'$, como $\sigma^2 = \mathrm{Id}$, se tiene que σ es una involución. Además vamos a considerar un orden en los elementos de H de forma que la matriz de la involución tenga una expresión particular. Por el teorema 3.6 se tiene que $B(\mathrm{ev}(Y^u), \mathrm{ev}(Y^v)) = 0$ si y sólo si $\overline{u+v} \neq 0$. Por tanto, primero consideramos los elementos $u \in H$ tales que $\sigma(u) = u' = u$, y por tanto $\overline{u+u} = 0$, se tiene $B(\mathrm{ev}(Y^u), \mathrm{ev}(Y^u)) = (-1)^r$ y $B(\mathrm{ev}(Y^u), \mathrm{ev}(Y^v)) = 0$ para todo $v \in H \setminus \{u\}$. Posteriormente, consideramos en H los pares de elementos u y $\sigma(u) = u'$, con $u \neq \sigma(u)$ y por tanto $\overline{u+u'} = 0$, se tiene $B(\mathrm{ev}(Y^u), \mathrm{ev}(Y^{u'})) = (-1)^r$, $B(\mathrm{ev}(Y^u), \mathrm{ev}(Y^v)) = 0$ para todo $v \in H \setminus \{u'\}$ y $B(\mathrm{ev}(Y^{u'}), \mathrm{ev}(Y^v)) = 0$ para todo $v \in H \setminus \{u\}$. Sea $H = \{u_1, \ldots, u_n\}$ ordenado de la forma anterior, y sea M la matriz asociada a la aplicación de evaluación $\mathrm{ev} : \mathbb{F}_q[H] \to \mathbb{F}_q^n$. Entonces se tiene que la matriz I_σ asociada a la involución σ se escribe como

$$(-1)^r I_\sigma = \begin{pmatrix} 1 & & & & & & & \\ & \ddots & & & & & & \\ & & 1 & & & & & \\ & & & 0 & 1 & & & \\ & & & 1 & 0 & & & \\ & & & & & \ddots & & \\ & & & & & & 0 & 1 \\ & & & & & & 1 & 0 \end{pmatrix}$$

y por tanto $MM^t = (-1)^r I_\sigma$, y como $M^t = M$ se tiene que

$$M^{-1} = (-1)^r I_\sigma M$$

Con esta notación, el siguiente resultado establece el número de 1's que se tienen en la diagonal principal de la matriz $(-1)^r I_\sigma$ y permite deducir que no existen códigos tóricos generalizados autoduales ($\mathcal{C}^\perp = \mathcal{C}$).

PROPOSICIÓN 3.9. *Con la notación anterior, sea σ la involución $\sigma(u) = u'$ para los elementos de H. El número de elementos $u \in H$ tales que $\sigma(u) = u$ es 2^r si q es impar y 1 si q es par. Además no existen códigos tóricos autoduales.*

DEMOSTRACIÓN. Sea $u = (u_1, \ldots, u_r)$ en H, $\sigma(u) = u$ si y sólo si $2u_i \equiv 0 \mod (q-1)$, $i = 1, \ldots, r$.

Sea q impar entonces $q-1$ es impar y se tiene $2u_i \equiv 0 \mod (q-1)$ si y sólo si u_i es igual a 0 o $(q-1)/2$. Por tanto, se tienen 2^r elementos con $\sigma(u) = u$. En cambio, si q es par, $q-1$ es impar y se tiene que el único elemento de H tal que $2u_i \equiv 0 \mod (q-1)$ para todo i es $(0, \ldots, 0)$.

Un código $\mathcal{C}$ es autodual si y sólo si $\mathcal{C}^\perp = \mathcal{C}$, en particular n debe ser par y $k = n/2$. Sea q par, entonces $n = (q-1)^r$ es impar y por tanto no existen códigos tóricos autoduales con q par. Si consideramos q impar, puesto que existen $u_1, \ldots, u_{2^r} \in H$ tales que $B(\mathrm{ev}(Y_i^u), \mathrm{ev}(Y_i^u)) \neq 0$, la dimensión

máxima de un código autoortogonal ($\mathcal{C}^\perp \subset \mathcal{C}$) es $n/2 - 2^{r-1} < n/2$, y por tanto no existen códigos tóricos autoduales. □

EJEMPLO 3.10. Sea $\mathbb{F}_5$ el cuerpo finito con 5 elementos y $r = 2$. Por tanto, $H = \{0,1,2,3\} \times \{0,1,2,3\}$. La longitud de un código tórico generalizado $\mathcal{C}_U$ con $U \subset H$ es $n = 4^2 = 16$.

Ordenamos los elementos de H para obtener $(-1)^r I_\sigma$ de la forma anterior. Como el cuerpo base tiene 5 elementos se tiene $\sigma(u) = u$ para $2^2 = 4$ elementos $u_1 = (0,0)$, $u_2 = (2,0)$, $u_3 = (0,2)$ y $u_4 = (2,2)$. Para el resto de los elementos de H se tiene $\sigma(u) \neq u$ y consideramos $u_j = u$ y $u_{j+1} = \sigma(u)$, por ejemplo $\sigma(0,1) = (0,3)$ y $\sigma(0,3) = (0,1)$. Por tanto escribimos $u_5 = (0,1)$, $u_6 = (0,3)$, $u_7 = (1,0)$, $u_8 = (3,0)$, $u_9 = (1,1)$, $u_{10} = (3,3)$, $u_{11} = (1,2)$, $u_{12} = (3,2)$, $u_{13} = (1,3)$, $u_{14} = (3,1)$, $u_{15} = (2,1)$, $u_{16} = (2,3)$. La ordenación de H no es única. Sea $i_j = u_j \ \forall j \in \{1,\dots,n\}$. La matriz de evaluación M de la aplicación $\mathbb{F}_5[H] \to \mathbb{F}_5^n$ en la base anterior es

$$M = \begin{pmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 4 & 4 & 1 & 1 & 4 & 4 & 1 & 1 & 4 & 4 & 4 & 4 \\
1 & 1 & 1 & 1 & 1 & 1 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 1 & 1 \\
1 & 1 & 1 & 1 & 4 & 4 & 4 & 4 & 1 & 1 & 4 & 4 & 1 & 1 & 4 & 4 \\
1 & 4 & 1 & 4 & 2 & 3 & 1 & 1 & 2 & 3 & 4 & 4 & 3 & 2 & 2 & 3 \\
1 & 4 & 1 & 4 & 3 & 2 & 1 & 1 & 3 & 2 & 4 & 4 & 2 & 3 & 3 & 2 \\
1 & 1 & 4 & 4 & 1 & 1 & 2 & 3 & 2 & 3 & 2 & 3 & 2 & 3 & 4 & 4 \\
1 & 1 & 4 & 4 & 1 & 1 & 3 & 2 & 3 & 2 & 3 & 2 & 3 & 2 & 4 & 4 \\
1 & 4 & 4 & 1 & 2 & 3 & 2 & 3 & 4 & 4 & 3 & 2 & 1 & 1 & 3 & 2 \\
1 & 4 & 4 & 1 & 3 & 2 & 3 & 2 & 4 & 4 & 2 & 3 & 1 & 1 & 2 & 3 \\
1 & 1 & 4 & 4 & 4 & 4 & 2 & 3 & 3 & 2 & 2 & 3 & 3 & 2 & 1 & 1 \\
1 & 1 & 4 & 4 & 4 & 4 & 3 & 2 & 2 & 3 & 3 & 2 & 2 & 3 & 1 & 1 \\
1 & 4 & 4 & 1 & 3 & 2 & 2 & 3 & 1 & 1 & 3 & 2 & 4 & 4 & 2 & 3 \\
1 & 4 & 4 & 1 & 2 & 3 & 3 & 2 & 1 & 1 & 2 & 3 & 4 & 4 & 3 & 2 \\
1 & 4 & 1 & 4 & 2 & 3 & 4 & 4 & 3 & 2 & 1 & 1 & 2 & 3 & 2 & 3 \\
1 & 4 & 1 & 4 & 3 & 2 & 4 & 4 & 2 & 3 & 1 & 1 & 3 & 2 & 3 & 2
\end{pmatrix}$$

Sea $U = \{(0,0),(1,0),(2,0),(0,1),(1,1),(2,1)\}$ y $\mathcal{C}_U$ su código asociado de longitud $n = 16$ y dimensión $k = 6$, el código tórico generalizado $\mathcal{C}_U$ es también un código tórico, en concreto el estudiado en el ejemplo 2.18 con $b_1 = 2, b_2 = 1$. Una matriz generatriz de $\mathcal{C}_U$ es la submatriz formada por las filas 1, 3, 5, 7, 9 y 15 de M

$$\begin{pmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 4 & 1 & 1 \\
1 & 4 & 1 & 4 & 2 & 3 & 1 & 1 & 2 & 3 & 4 & 4 & 3 & 2 & 2 & 3 \\
1 & 1 & 4 & 4 & 1 & 1 & 2 & 3 & 2 & 3 & 2 & 3 & 2 & 3 & 4 & 4 \\
1 & 4 & 4 & 1 & 2 & 3 & 2 & 3 & 4 & 4 & 3 & 2 & 1 & 1 & 3 & 2 \\
1 & 4 & 1 & 4 & 2 & 3 & 4 & 4 & 3 & 2 & 1 & 1 & 2 & 3 & 2 & 3
\end{pmatrix}$$

Una matriz de control de $\mathcal{C}_U$, o equivalentemente una matriz generatriz de $\mathcal{C}_U^{\perp}$, es la submatriz formada por las filas 2, 4, 5, 7, 9, 11, 12, 13, 14 y 15 de M

$$\begin{pmatrix}
1 & 1 & 1 & 1 & 4 & 4 & 1 & 1 & 4 & 4 & 1 & 1 & 4 & 4 & 4 & 4 \\
1 & 1 & 1 & 1 & 4 & 4 & 4 & 4 & 1 & 1 & 4 & 4 & 1 & 1 & 4 & 4 \\
1 & 4 & 1 & 4 & 2 & 3 & 1 & 1 & 2 & 3 & 4 & 4 & 3 & 2 & 2 & 3 \\
1 & 1 & 4 & 4 & 1 & 1 & 2 & 3 & 2 & 3 & 2 & 3 & 2 & 3 & 4 & 4 \\
1 & 4 & 4 & 1 & 2 & 3 & 2 & 3 & 4 & 4 & 3 & 2 & 1 & 1 & 3 & 2 \\
1 & 1 & 4 & 4 & 4 & 4 & 2 & 3 & 3 & 2 & 2 & 3 & 3 & 2 & 1 & 1 \\
1 & 1 & 4 & 4 & 4 & 4 & 3 & 2 & 2 & 3 & 3 & 2 & 2 & 3 & 1 & 1 \\
1 & 4 & 4 & 1 & 3 & 2 & 2 & 3 & 1 & 1 & 3 & 2 & 4 & 4 & 2 & 3 \\
1 & 4 & 4 & 1 & 2 & 3 & 3 & 2 & 1 & 1 & 2 & 3 & 4 & 4 & 3 & 2 \\
1 & 4 & 1 & 4 & 2 & 3 & 4 & 4 & 3 & 2 & 1 & 1 & 2 & 3 & 2 & 3
\end{pmatrix}$$

Se tiene que la matriz $M \cdot M^t = I_\sigma$ es

$$I_\sigma = \begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0
\end{pmatrix}$$

3. Códigos Tóricos Generalizados en Singular

La implementación de los códigos tóricos en un lenguaje de cálculo simbólico como SINGULAR [26] es sencilla. Una introducción a SINGULAR puede encontrarse en [25]. Este lenguaje permite trabajar sobre el cuerpo finito $\mathbb{F}_q$ con elemento primitivo α. En el siguiente ejemplo definimos $F = \mathbb{F}_8[X]$ que contiene a $\mathbb{F}_8$, cuyo elemento primitivo es `a`.

```
                     SINGULAR                                /
 A Computer Algebra System for Polynomial Computations   /   version 3-0-2
                                                       0<
     by: G.-M. Greuel, G. Pfister, H. Schoenemann        \   July 2006
FB Mathematik der Universitaet, D-67653 Kaiserslautern    \
> ring F=(2^3,a),X,lp;
> basering;
//   # ground field : 8
//   primitive element : a
//   minpoly        : 1*a^3+1*a^1+1*a^0
//   number of vars : 1
//        block   1 : ordering lp
//                  : names    X
//        block   2 : ordering C
```

Podemos definir otro polinomio mínimo de la extensión, pero si consideramos el dado por SINGULAR, los cálculos son más rápidos.

Definimos H como una lista de vectores de enteros, además podemos ordenar sus elementos como en la sección anterior. Podemos ordenar $H = \{0, \ldots, q-2\} \times \{0, \ldots, q-2\}$ para un cuerpo de característica par usando el siguiente procedimiento

```
proc generarHchdos(int q)
{
  list H;
  intvec tmp;
  int ii,jj;
  tmp=0,0;
  H[1]=tmp;
  int cont=2;
  for(ii=1;ii<=(q-2)/2;ii++)
    {tmp=ii,0;
    H[cont]=tmp;
    tmp=q-1-ii,0;
    H[cont+1]=tmp;
    cont=cont+2;
    }
  for(ii=1;ii<=(q-2)/2;ii++)
    {tmp=0,ii;
    H[cont]=tmp;
    tmp=0,q-1-ii;
    H[cont+1]=tmp;
    cont=cont+2;
    }
  for(ii=1;ii<=q-2;ii++)
    {for(jj=1;jj<=(q-2)/2;jj++)
      {tmp=ii,jj;
      H[cont]=tmp;
      tmp=q-1-ii,q-1-jj;
      H[cont+1]=tmp;
      cont=cont+2;
```

```
      }
    }
  return(H);
}
```

En cambio, para un cuerpo de característica impar usamos el siguiente

```
proc generarHchNOdos(int q)
{
  list H;
  intvec tmp;
  int ii,jj;
  tmp=0,0; H[1]=tmp;
  tmp=(q-1)/2,0;H[2]=tmp;
  tmp=0,(q-1)/2; H[3]=tmp;
  tmp=(q-1)/2,(q-1)/2; H[4]=tmp;
  int cont=5;
  for(ii=1;ii<(q-1)/2;ii++)
    {tmp=ii,0;
    H[cont]=tmp;
    tmp=q-1-ii,0;
    H[cont+1]=tmp;
    cont=cont+2;
    }
  for(ii=1;ii<(q-1)/2;ii++)
    {tmp=0,ii;
    H[cont]=tmp;
    tmp=0,q-1-ii;
    H[cont+1]=tmp;
    cont=cont+2;
    }
  for(ii=1;ii<(q-1)/2;ii++)
    {for(jj=1;jj<=q-2;jj++)
      {tmp=ii,jj;
      H[cont]=tmp;
      tmp=q-1-ii,q-1-jj;
      H[cont+1]=tmp;
      cont=cont+2;
      }
    }
  for(jj=1;jj<(q-1)/2;jj++)
    {tmp=(q-1)/2,jj;
    H[cont]=tmp;
    tmp=(q-1)/2,q-1-jj;
    H[cont+1]=tmp;
    cont=cont+2;
    }
  return(H);
}
```

Calculamos H para $\mathbb{F}_5$

```
> ring F=5,x,lp;
```

```
> list H=generarHchNOdos(5);
> H;
[1]:    [2]:    [3]:    [4]:    [5]:    [6]:    [7]:    [8]:
   0,0     2,0     0,2     2,2     1,0     3,0     0,1     0,3


[9]:    [10]:    [11]:    [12]:    [13]:    [14]:    [15]:    [16]:
   1,1      3,3      1,2      3,2      1,3      3,1      2,1      2,3
```

Definimos la matriz M de la aplicación de evaluación lineal ev elevando el elemento primitivo a las diferentes potencias de H

```
proc MatrizEvaluacion(int q, poly a, list H)
{
  int ii,jj;
  matrix M[(q-1)^2][(q-1)^2];
  for(ii=1;ii<=(q-1)^2;ii++)
    {for(jj=1;jj<=(q-1)^2;jj++)
      {
    M[ii,jj]=a^(H[ii][1]*H[jj][1] + H[ii][2]*H[jj][2]);
      }
    }
return(M)
}
```

Para $\mathbb{F}_5$ obtenemos M y la matriz de la involución I_σ.

```
> ring F=5,x,lp;
> list H=generarHchNOdos(5);
> poly a=2;
> matrix M=MatrizEvaluacion(5,a,H);
> show(M);
// matrix, 16x16
1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1,
1,1, 1, 1, -1,-1,1, 1, -1,-1,-1,-1,-1,-1,1, 1,
1,1, 1, 1, 1, 1, -1,-1,-1,-1,1, 1, -1,-1,-1,-1,
1,1, 1, 1, -1,-1,-1,-1,1, 1, -1,-1,1, 1, -1,-1,
1,-1,1, -1,2, -2,1, 1, 2, -2,2, -2,2, -2,-1,-1,
1,-1,1, -1,-2,2, 1, 1, -2,2, -2,2, -2,2, -1,-1,
1,1, -1,-1,1, 1, 2, -2,2, -2,-1,-1,-2,2, 2, -2,
1,1, -1,-1,1, 1, -2,2, -2,2, -1,-1,2, -2,-2,2,
1,-1,-1,1, 2, -2,2, -2,-1,-1,-2,2, 1, 1, -2,2,
1,-1,-1,1, -2,2, -2,2, -1,-1,2, -2,1, 1, 2, -2,
1,-1,1, -1,2, -2,-1,-1,-2,2, 2, -2,-2,2, 1, 1,
1,-1,1, -1,-2,2, -1,-1,2, -2,-2,2, 2, -2,1, 1,
1,-1,-1,1, 2, -2,-2,2, 1, 1, -2,2, -1,-1,2, -2,
1,-1,-1,1, -2,2, 2, -2,1, 1, 2, -2,-1,-1,-2,2,
1,1, -1,-1,-1,-1,2, -2,-2,2, 1, 1, 2, -2,2, -2,
1,1, -1,-1,-1,-1,-2,2, 2, -2,1, 1, -2,2, -2,2
```

```
>show(M*transpose(M));
// matrix, 16x16
1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,1,0,0,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,1,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,1,0,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,1,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,1,0,0,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,1,0,0,0,0,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,
0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,0
```

Una forma alternativa de definir la matriz de evaluación M es considerar una matriz de polinomios $(X^i)_{i\in H}$ en el anillo $\mathbb{F}_q[X_1,\ldots,X_n]$

```
ring B=q,X(1..n),lp
```

y después utilizar la función `subst` para obtener M.

Se pueden obtener submatrices de M con la función `submat`, a continuación calculamos la matriz generatriz y la matriz de control del código [38, Example 3.9]. Dicho código tiene parámetros $[49,11,28]_8$ y mejora la distancia mínima del anterior código lineal conocido que tenía parámetros $[49,11,27]_8$.

Sea P el politopo de vértices $(0,0)$, $(4,1)$ y $(1,4)$. Los bordes del abanico normal $\triangle_P$ están generados por $v(\rho_1)=(5,-1)$, $v(\rho_2)=(-1,5)$, $v(\rho_3)=(-1,-1)$. En `U` tenemos los puntos racionales del politopo P y en `Uort` los puntos de H que definen el código ortogonal a $\mathcal{C}_U$.

```
> ring F=(2^3,a),x,lp;
> list H=generarHchdos(8)
> matrix M=MatrizEvaluacion(2,H);
> intvec U=1,14,16,18,20,22,24,26,28,32,49;
> intvec Uort=2,3,4,5,6,7,8,9,10,11,12,13,14,16,18,20,22,24,26,28,30,
31,32,34,35,36,37,38,39,40,41,42,43,44,45,46,47,49;
> matrix MatrizGeneratriz=submat(M,U,1..49);
> matrix MatrizDeControl=submat(M,Uort,1..49);
> show(MatrizGeneratriz);
// matrix, 11x49
1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,
1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,
```

```
1,a,a6,a2,a5,a3,a4,a,a6,a2,a5,a3,a4,a2,a5,a3,a4,a4,a3,a3,a4,a4,a3,
a5,a2,a4,a3,a5,a2,a6,a,a5,a2,a6,a,1,1,a6,a,1,1,a,a6,1,1,a,a6,a2,a5,
1,a,a6,a2,a5,a3,a4,a2,a5,a4,a3,a6,a,a3,a4,a5,a2,1,1,a4,a3,a6,a,a,
a6,a5,a2,1,1,a2,a5,a6,a,a,a6,a3,a4,1,1,a2,a5,a4,a3,a,a6,a3,a4,a5,a2,
1,a,a6,a2,a5,a3,a4,a3,a4,a6,a,a2,a5,a4,a3,1,1,a3,a4,a5,a2,a,a6,a4,
a3,a6,a,a2,a5,a5,a2,1,1,a3,a4,a6,a,a,a6,a4,a3,1,1,a2,a5,a5,a2,a,a6,
1,a2,a5,a4,a3,a6,a,a,a6,a2,a5,a3,a4,a3,a4,a4,a3,a5,a2,a5,a2,a6,a,
1,1,1,1,a,a6,a2,a5,a2,a5,a3,a4,a4,a3,a4,a3,a5,a2,a6,a,a6,a,1,1,a,a6,
1,a2,a5,a4,a3,a6,a,a2,a5,a4,a3,a6,a,a4,a3,a6,a,a,a6,a6,a,a,a6,a3,
a4,a,a6,a3,a4,a5,a2,a3,a4,a5,a2,1,1,a5,a2,1,1,a2,a5,1,1,a2,a5,a4,a3,
1,a2,a5,a4,a3,a6,a,a3,a4,a6,a,a2,a5,a5,a2,a,a6,a4,a3,1,1,a3,a4,a6,
a,a2,a5,a5,a2,a,a6,a4,a3,1,1,a3,a4,a6,a,a2,a5,a5,a2,a,a6,a4,a3,1,1,
1,a3,a4,a6,a,a2,a5,a,a6,a2,a5,a3,a4,a4,a3,a5,a2,a6,a,1,1,a,a6,a2,
a5,a3,a4,a4,a3,a5,a2,a6,a,1,1,a,a6,a2,a5,a3,a4,a4,a3,a5,a2,a6,a,1,1,
1,a3,a4,a6,a,a2,a5,a2,a5,a4,a3,a6,a,a5,a2,1,1,a2,a5,a,a6,a3,a4,a5,
a2,a4,a3,a6,a,a,a6,1,1,a2,a5,a4,a3,a3,a4,a5,a2,1,1,a6,a,a,a6,a3,a4,
1,a4,a3,a,a6,a5,a2,a,a6,a2,a5,a3,a4,a5,a2,a6,a,1,1,a2,a5,a3,a4,a4,
a3,a6,a,1,1,a,a6,a3,a4,a4,a3,a5,a2,1,1,a,a6,a2,a5,a4,a3,a5,a2,a6,a,
1,a,a6,a2,a5,a3,a4,a4,a3,a,a6,a5,a2,a5,a2,a2,a5,a6,a,a6,a,a3,a4,1,
1,1,1,a4,a3,a,a6,a,a6,a5,a2,a2,a5,a2,a5,a6,a,a3,a4,a3,a4,1,1,a4,a3
```

Para trabajar con la notación polinomial de un código tórico, también podemos considerar en SINGULAR el álgebra polinomial

$$A = \mathbb{F}_q[X_1, \ldots, X_r]/(X_1^{N_1} - 1, \ldots, X_r^{N_r} - 1)$$

En el siguiente ejemplo construimos A para $r = 2$ sobre $\mathbb{F}_8$

```
> ring R=(2^3,a),X(1..2),lp;
> ideal J= X(1)^7 -1,X(2)^7 -1;
> qring Q=groebner(J);
> Q;
//   # ground field : 8
//   primitive element : a
//   minpoly        : 1*a^3+1*a^1+1*a^0
//   number of vars : 2
//        block   1 : ordering lp
//                  : names    X(1) X(2)
//        block   2 : ordering C
// quotient ring from ideal
_[1]=X(2)^7+1 _[2]=X(1)^7+1
```

Para obtener la forma reducida de un elemento de A debemos considerar lo siguiente

```
> X(1)^8;
X(1)^8
> reduce(X(1)^8,std(0));
X(1)
```

```
> reduce(X(1)^8-X(1),std(0));
0
```

Una alternativa a trabajar en el anillo cociente es utilizar el álgebra $R = \mathbb{F}_q[X_1, \ldots, X_r]$ y trabajar módulo el ideal $J = (X_1^{q-1} - 1, \ldots, X_r^{q-1} - 1)$, que además es una base de Gröbner universal, i.e. es una base de Gröbner para cualquier orden monomial.

CAPÍTULO 4

Estructuras Métricas sobre Códigos Lineales

En el capítulo 1 hemos definido el código dual de un código lineal, éste es el ortogonal del código como subespacio vectorial de $\mathbb{F}_q^n$ con respecto a la forma bilineal dada por la matriz identidad. En este capítulo estudiamos las formas bilineales sobre un cuerpo finito y lo usamos para dar una descomposición similar a la obtenida para códigos tóricos generalizados al final del capítulo 3. Dicha descomposición denominada descomposición geométrica de un código lineal puede darse para un código lineal arbitrario de forma constructiva; permite expresar fácilmente el dual de un código lineal y dar un método para calcular la distancia mínima que extiende para códigos lineales la proposición 3.8 de códigos tóricos generalizados. Dicho estudio es diferente para cuerpos de característica 2, pero se desarrolla de forma paralela.

1. Estructuras Métricas de $\mathbb{F}_q^n$

Puede encontrarse una introducción a la geometría sobre cuerpos finitos, y en particular a las formas bilineales, en [34, 58]. Referimos los resultados sobre formas bilineales y cuadráticas en característica distinta de 2 a [1]. Un estudio detallado del grupo ortogonal y de las formas cuadráticas en característica arbitraria puede consultarse en [12, 13, 14]. Aplicaciones de la geometría sobre cuerpos finitos a códigos autoduales y autoortogonales pueden encontrarse en [51, 52, 53].

Una estructura métrica sobre $\mathbb{F}_q^n$ viene dada por una forma bilineal no degenerada. Cuando la forma bilineal es simétrica y la característica es distinta de dos, una estructura métrica viene dada alternativamente por la forma cuadrática asociada a la forma bilineal que proporciona la estructura. En esta sección introducimos y comentamos las estructuras métricas sobre $\mathbb{F}_q^n$.

Una forma bilineal sobre el espacio vectorial $\mathbb{F}_q^n$ es una aplicación bilineal $B : \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{F}_q$. Se dice que es simétrica si $B(x, y) = B(y, x)\ \forall x, y \in \mathbb{F}_q^n$ y que es no degenerada si se verifica que

$$B(x, y) = 0\ \forall y \in \mathbb{F}_q^n \Rightarrow x = 0$$
$$B(x, y) = 0\ \forall x \in \mathbb{F}_q^n \Rightarrow y = 0$$

Una forma cuadrática sobre $\mathbb{F}_q^n$ es una aplicación $Q : \mathbb{F}_q^n \to \mathbb{F}_q$ tal que

$$\begin{array}{l} Q(ax) = a^2 Q(x) \\ b(x,y) = Q(x+y) - Q(x) - Q(y) \text{ es bilineal} \end{array}$$

Es decir, una forma cuadrática puede ser considerada como un polinomio homogéneo de grado 2 en el anillo $\mathbb{F}_q[x_1, \ldots, x_n]$ que da lugar a la forma cuadrática evaluando las coordenadas de los vectores de $\mathbb{F}_q^n$. Además, una forma bilineal simétrica $B(x,y)$ define una forma cuadrática $Q(x) = B(x,x)$. Y por otro lado, como la aplicación $b(x,y)$ anterior es simétrica, siempre que la característica de $\mathbb{F}_q^n$ sea distinta de dos, una forma cuadrática define una forma bilineal simétrica denominada polaridad de Q

$$B(x,y) = \frac{1}{2}(Q(x+y) - Q(x) - Q(y))$$

Por tanto, si la característica de $\mathbb{F}_q^n$ es distinta de 2, la polaridad define una correspondencia biyectiva y recíproca entre las formas bilineales simétricas y las formas cuadráticas. En cambio, si la característica de $\mathbb{F}_q^n$ es dos, no se pueden recuperar todas las formas cuadráticas a partir de las formas bilineales. En el estudio posterior de la métrica sobre característica 2 mostraremos este fenómeno.

Sea $\mathcal{B} = \{x_1, \ldots, x_n\}$ una base de $\mathbb{F}_q^n$, la matriz asociada a la forma bilineal B en la base $\mathcal{B}$ es

$$M = \begin{pmatrix} B(x_1,x_1) & \cdots & B(x_1,x_n) \\ \vdots & & \vdots \\ B(x_n,x_1) & \cdots & B(x_n,x_n) \end{pmatrix}$$

Además, si $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n)$ en la base $\mathcal{B}$, se tiene que $B(x,y) = xMy^t$, donde y^t denota la transpuesta de y. Si M es la matriz de B en la base $\{x_1, \ldots, x_n\}$ y N es la matriz de paso de la base $\{y_1, \ldots, y_n\}$ a $\{x_1, \ldots, x_n\}$, es decir $y_i N = x_i$, entonces NMN^t es la matriz de B en la base $\{y_1, \ldots, y_n\}$. Al determinante de la matriz M se le denomina **discriminante** de B. A la vista del cambio de base dicho determinante está bien definido módulo un cuadrado de $\mathbb{F}_q^*$ puesto que $\det(NMN^t) = \det(N)^2 \det(M)$.

A partir de ahora todas las formas bilineales que consideramos son simétricas. Las formas bilineales simétricas permiten definir el concepto geométrico de ortogonalidad. Sean $x, y \in \mathbb{F}_q^n$, se dice que x e y son **ortogonales** si $B(x,y) = 0$ y se denota $x \perp y$. Sean U, W dos subespacios vectoriales de $\mathbb{F}_q^n$, se dice que U y W son **ortogonales** si $x \perp y$ para todo $x \in U$, $y \in W$ y se denota $U \perp W$.

Sea $U \subset \mathbb{F}_q^n$ un subespacio vectorial, el radical de U son los vectores de U que son ortogonales a U, es decir

$$\operatorname{rad}(U) = U \cap U^{\perp}$$

Se dice que U es **no singular** si $\mathrm{rad}(U) = (0)$ y que es singular en caso contrario. Se tiene que U es no singular si y sólo si la forma bilineal restringida a U es no degenerada.

Sea $\mathbb{F}_q^n$ suma directa de subespacios dos a dos ortogonales

$$\mathbb{F}_q^n = U_1 \oplus \cdots \oplus U_r$$

entonces decimos que $\mathbb{F}_q^n$ es la suma ortogonal de $U_1, \ldots, U_r$ y lo denotamos

$$\mathbb{F}_q^n = U_1 \perp \cdots \perp U_r$$

Si $\mathbb{F}_q^n$ es no singular y U es un subespacio vectorial de $\mathbb{F}_q^n$ se tiene que $n = \dim(\mathbb{F}_q^n) = \dim(U) + \dim(U^\perp)$. Además si U es no singular se tiene que $\mathbb{F}_q^n = U \perp U^\perp$ y $U^\perp$ es no singular.

Se dice que $x \in \mathbb{F}_q^n$ es **isótropo** si $B(x,x) = 0$, es decir si $\langle x \rangle \subset \mathrm{rad}(\langle x \rangle)$. Un subespacio vectorial $U \subset \mathbb{F}_q^n$ se dice que es isótropo si $B(x,y) = 0$ para todo $x, y \in U$, es decir, si $U \subset \mathrm{rad}(U)$.

Los subespacios isótropos satisfacen por tanto $\dim(U) \leq \left\lfloor \frac{n}{2} \right\rfloor$. Un subespacio isótropo $U \subset \mathbb{F}_q^n$ se denomina maximal si no es subespacio propio de ningún otro subespacio isótropo. Además todos los subespacios isótropos maximales de un subespacio no singular tienen la misma dimensión, que denominamos **índice** de U. En particular, el propio espacio $\mathbb{F}_q^n$ tiene su propio índice, menor o igual que la parte entera de $n/2$.

Sea $H \subset \mathbb{F}_q^n$ un subespacio vectorial de dimensión 2, se dice que H es un **plano hiperbólico** si existen x_1, x_2 que generan H tales que

$$\begin{aligned} B(x_1, x_1) &= 0 \\ B(x_2, x_2) &= 0 \\ B(x_1, x_2) &= 1 \end{aligned}$$

y por tanto H es no singular. Los dos generadores ordenados x_1, x_2 se denominan **generadores geométricos o base geométrica de** H, la matriz de B restringida a H en la base geométrica es

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

PROPOSICIÓN 4.1. *Sea $\mathbb{F}_q$ de característica distinta de dos, un subespacio no singular de dimensión 2 que contiene a un vector isótropo es un plano hiperbólico.*

DEMOSTRACIÓN. Sea x_1 un vector isótropo no nulo. Sea y un vector del subespacio de dimensión 2 considerado linealmente independiente de x_1 y sea $x_2 = \lambda_1 x_1 + \lambda_2 y$. Determinemos los valores λ_1, $\lambda_2 \in \mathbb{F}_q$ para obtener un base geométrica. Se tiene que $B(x_1, x_2) = \lambda_2 B(x_1, y)$, además $B(x_1, y) \neq 0$ puesto que un plano hiperbólico es no singular. Por tanto, $\lambda_2 = B(x_1, y)^{-1} \neq 0$ y $B(x_1, x_2) = 1$.

Por otro lado, $B(x_2, x_2) = 0$ si y sólo si $2\lambda_1\lambda_2 B(x_1, y) + \lambda_2^2 B(y, y) = 0$. Puesto que $\lambda_2 \neq 0$ y $B(x_1, y) \neq 0$ se tiene que

$$\lambda_1 = \frac{-\lambda_2 B(y, y)}{2B(x_1, y)} = \frac{-B(y, y)}{2B(x_1, y)^2}$$

y x_2 es isótropo. □

En este primer resultado se puede observar cómo el estudio para característica 2 es diferente. En particular, este resultado no es cierto en característica 2 como muestra el siguiente ejemplo.

EJEMPLO 4.2. Sea $\mathbb{F}_q$ un cuerpo de característica 2 y sea B la forma bilineal que viene dada por la matriz identidad. Sea $x = (x_1, x_2) \in \mathbb{F}_q^2$, x es un vector isótropo si y sólo si $x_1^2 + x_2^2 = 0$, es decir, si y sólo si $(x_2/x_1)^2 = 1$. Luego $(1, 1)$ es un vector isótropo, además únicamente los vectores del subespacio lineal generado por $(1, 1)$ son isótropos, puesto que elevar al cuadrado es un isomorfismo en característica 2. Por tanto, $\mathbb{F}_q^2$ contiene a un vector isótropo pero no es un plano hiperbólico.

En la base $\{(1, 1), (0, 1)\}$ de $\mathbb{F}_q^2$ la matriz asociada de B es

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

y por tanto decimos que $\mathbb{F}_q^2$ es un plano elíptico.

Más concretamente, decimos que un subespacio no singular $E \subset \mathbb{F}_q^n$ de dimensión 2 es un **plano elíptico** si existen x_1, x_2 que generan E tales que

$$\begin{aligned} B(x_1, x_1) &= 0 \\ B(x_2, x_2) &= 1 \\ B(x_1, x_2) &= 1 \end{aligned}$$

y por tanto E es no singular. Los dos generadores ordenados x_1, x_2 se denominan **generadores geométricos o base geométrica de** E, la matriz de B restringida a E en la base geométrica es

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

2. Descomposiciones Geométricas en Característica Distinta de 2

A partir de ahora consideramos únicamente la estructura métrica dada por la forma bilineal $B(x, y) = \sum_{i=1}^n x_i y_i$, que fue introducida en el capítulo 1 para definir el código dual de un código lineal. A partir de ahora $\mathbb{F}_q^n$ es el espacio vectorial sobre $\mathbb{F}_q$ dotado de la forma bilineal simétrica no degenerada B que tiene asociada la matriz identidad. Primero presentamos B con característica distinta de 2 y, posteriormente en la sección 4, con característica 2 puesto que, como hemos indicado, dicho estudio es diferente.

Consideramos primero $\mathbb{F}_q^2$, que será de utilidad para la discusión de $\mathbb{F}_q^n$. Distinguiremos dos casos dependiendo de si -1 es un cuadrado de $\mathbb{F}_q$, $-1 \in \mathbb{F}_q^{*2}$, o no lo es. Sea $q = p^l$, se tiene que -1 es un cuadrado en $\mathbb{F}_q$ (con q impar) si y sólo si $q \equiv 1 \mod 4$. Para $q = p$ se tiene el resultado por la ley de reciprocidad cuadrática [59, sección 1.3]. Si $l > 1$ sea $\mathbb{K}$ la clausura algebraica de $\mathbb{F}_p$, entonces $\mathbb{F}_{p^l}$ se realiza como el subcuerpo de $\mathbb{K}$ formado por los elementos de $\mathbb{K}$ tales que $x^{p^l} = x$. Además se tiene que $\mathbb{F}_{p^l} \cap \mathbb{F}_{p^{l'}} = \mathbb{F}_{p^d}$, donde d es el máximo común divisor de l, l'. Luego si -1 es un cuadrado en $\mathbb{F}_p$ se tiene que $p \equiv 1 \mod 4$, luego $p^l \equiv 1 \mod 4$ para todo l, pero si -1 tiene una raíz en $\mathbb{F}_p$ también la tiene en $\mathbb{F}_{p^l}$ para todo l. Si -1 no es un cuadrado en $\mathbb{F}_p$ se tiene $p \equiv 3 \mod 4$, entonces -1 sí es un cuadrado en $\mathbb{F}_{p^2}$. Entonces, como $\mathbb{F}_{p^l} \cap \mathbb{F}_{p^2}$ es igual a $\mathbb{F}_p$ ó $\mathbb{F}_{p^2}$ según l sea impar o par, se tiene que $q = p^l \equiv 1 \mod 4$ si l es par y $q = p^l \equiv 3 \mod 4$ si l es impar y de aquí se deduce el resultado.

Un vector no nulo $x = (x_1, x_2) \in \mathbb{F}_q^2$ es un vector isótropo, si y sólo si $x_1^2 + x_2^2 = 0$, es decir, si y sólo si $(x_2/x_1)^2 = -1$. Si -1 es un cuadrado en el cuerpo, la ecuación anterior tiene solución y existen por tanto vectores isótropos. Como B es no degenerada se tiene que $\mathbb{F}_q^2$ es un plano hiperbólico. En cambio si -1 no es un cuadrado no existen vectores isótropos y por tanto $\mathbb{F}_q^2$ no es un plano hiperbólico (ni plano elíptico).

Entonces si $q \equiv 1 \mod 4$ en $\mathbb{F}_q^2$ existe al menos un vector isótropo. Podemos obtener los dos generadores geométricos del plano hiperbólico usando la proposición 4.1, concretamente $x = (x_1, x_2)$, $y = \frac{1}{2x_1x_2}(x_2, x_1)$ con $(x_2/x_1)^2 = -1$ verifican $B(x,x) = 0$, $B(y,y) = 0$ y $B(x,y) = 1$ si $(x_2/x_1)^2 = -1$. Además ambos vectores son diferentes puesto que si $x = y$ se tendría que $2x_1^2 = 1$, $2x_2^2 = 1$ que implicaría $1 = (x_2/x_1)^2 = -1$ y linealmente independientes puesto que si no lo fueran se tendría que $1 = (x_2/x_1)^2 = -1$.

EJEMPLO 4.3. Se tiene que $\mathbb{F}_5^2$ es un plano hiperbólico porque $5 \equiv 1 \mod 4$, además $(4/2)^2 = -1$ y se tiene que $x_1 = (2,4)$, $x_2 = (4,2)$ verifican $B(x_1, x_1) = 0$, $B(x_2, x_2) = 0$, $B(x_1, x_2) = 1$. En cambio en $\mathbb{F}_3^2$ no hay vectores isótropos ya que $3 \not\equiv 1 \mod 4$.

El siguiente lema [59, section 1.7] se utiliza a continuación para la discusión de un plano que no es hiperbólico.

LEMA 4.4. *Sean $a, b, c \in \mathbb{F}_q$ no nulos, entonces la siguiente ecuación tiene solución en $\mathbb{F}_q$*

$$aX^2 + bY^2 = c$$

DEMOSTRACIÓN. Sea A el conjunto de elementos de $\mathbb{F}_q$ de la forma aX^2 con $X \in \mathbb{F}_q$ y sea B el conjunto de elementos de $\mathbb{F}_q$ de la forma $c - bY^2$ con $Y \in \mathbb{F}_q$. A y B tienen $(q+1)/2$ elementos por lo que A y B no pueden ser disjuntos y se tiene el resultado. □

En un plano no singular sin vectores isótropos existen dos generadores ortonormales.

PROPOSICIÓN 4.5. *Sea $U \subset \mathbb{F}_q^n$ de dimensión 2 sin vectores isótropos $\mathbb{F}_q$. Entonces existen dos generadores ortonormales x_1, x_2 de U, es decir, tales que $B(x_1, x_1) = B(x_2, x_2) = 1$ y $B(x_1, x_2) = 0$.*

DEMOSTRACIÓN. Sea $U = \langle y_1, y_2 \rangle$, $x_1 = \lambda_1 y_1 + \lambda_2 y_2$. Se tiene que $B(x_1, x_1) = \lambda_1^2 B(y_1, y_1) + \lambda_2^2 B(y_2, y_2)$. Por el lema 4.4 existe un vector x_1 en U con $B(x_1, x_1) = 1$ ya que $B(y_1, y_1) \neq 0$ y $B(y_2, y_2) \neq 0$.

Sea $z \in U$ no nulo ortogonal a x_1, $B(\lambda_1 x_1 + \lambda_2 z, \lambda_1 x_1 + \lambda_2 z) = \lambda_1^2 + \lambda_2^2 B(z, z)$. Como no hay vectores isótropos se tiene que $-B(z, z)$ es un no cuadrado y por tanto $B(z, z)$ es un cuadrado, por lo que existe $\lambda \in \mathbb{F}_q^*$ tal que $B(\lambda z, \lambda z) = 1$ y x_1 y x_2 son ortonormales. □

En la proposición 4.8 escribimos $U \subset \mathbb{F}_q^n$ de dimensión mayor o igual que 3 como suma ortogonal de planos hiperbólicos y un subespacio de dimensión menor o igual que 2. Pero para probar este resultado necesitamos dos lemas, el primero calcula un vector isótropo y el segundo, dado un vector isótropo, calcula el segundo generador geométrico de un plano hiperbólico.

LEMA 4.6. *Sea $U \subset \mathbb{F}_q^n$ no singular de dimensión mayor o igual que 3, entonces existe al menos un vector isótropo no nulo en U.*

DEMOSTRACIÓN. Sea P un plano no singular de U y $x_1 \in P^\perp$, supongamos que $B(x_1, x_1) \neq 0$ (en caso contrario x_1 es isótropo).

Por el lema 4.4 se tiene que existe $x_2 \in P$ tal que $B(x_2, x_2) = -B(x_1, x_1)$. Por tanto $x_1 + x_2 \neq 0$ y $B(x_1 + x_2, x_1 + x_2) = 0$. □

LEMA 4.7. *Sea x_1 un vector isótropo del subespacio $U \subset \mathbb{F}_q^n$ de dimensión mayor o igual que 3, entonces existe un vector isótropo x_2 de U tal que $B(x_1, x_2) = 1$.*

DEMOSTRACIÓN. Sea y un vector de U que no está en la variedad ortogonal a x_1 y sea $x_2 = \alpha_1 x_1 + \alpha_2 y$, con $\alpha_1, \alpha_2 \in \mathbb{F}_q$ tales que

$$\begin{cases} B(x_2, x_2) = 0 \\ B(x_1, x_2) = 1 \end{cases}$$

es decir

$$\begin{cases} 2\alpha_1\alpha_2 B(y, x_2) + \alpha_2^2 B(y, y) = 0 \\ \alpha_2 B(x_1, y) = 1 \end{cases}$$

que tiene solución debido a que la forma cuadrática es no degenerada y podemos despejar α_2 de la segunda ecuación. □

Usando estos dos lemas podemos probar el siguiente resultado

PROPOSICIÓN 4.8. *Sea $U \subset \mathbb{F}_q^n$ un espacio vectorial de dimensión m no singular con característica de $\mathbb{F}_q$ distinta de dos. Se puede descomponer U de la siguiente forma:*

Para m impar

(1) *$U = H_1 \perp \cdots \perp H_{(m-1)/2} \perp L$, donde cada H_i es un plano hiperbólico y L es un subespacio lineal de dimensión 1.*

Para m par

(2) *Si el índice de U es $m/2$: $U = H_1 \perp \cdots \perp H_{m/2}$, donde cada H_i es un plano hiperbólico.*
(3) *Si el índice de U es $m/2 - 1$: $U = H_1 \perp \cdots \perp H_{(m-2)/2} \perp L_1 \perp L_2$, donde cada H_i es un plano hiperbólico y L_1 y L_2 son dos subespacios lineales de dimensión 1 generados por dos vectores ortonormales.*

La forma cuadrática $Q(x)$ asociada a la forma bilineal B restringida a U es equivalente en cada caso a

(1) $2x_1x_2 + \cdots + 2x_{m-2}x_{m-1} + \varepsilon x_m^2$ *(Q de tipo parabólico en U)*
(2) $2x_1x_2 + \cdots + 2x_{m-1}x_m$ *(Q de tipo hiperbólico en U)*
(3) $2x_1x_2 + \cdots + 2x_{m-3}x_{m-2} + x_{m-1}^2 + x_m^2$ *(Q de tipo elíptico en U)*

DEMOSTRACIÓN. Sea m impar, podemos aplicar los lemas 4.6 y 4.7 para obtener un plano hiperbólico H_1 y $U = H_1 \perp (H_1^\perp \cap U)$. De la misma forma, podemos obtener en $H_1^\perp \cap U$ más planos hiperbólicos ortogonales dos a dos iterando el proceso hasta tener U como suma ortogonal de $(m-1)/2$ planos hiperbólicos y una variedad lineal de dimensión 1.

Del mismo modo, en el caso de m par, podemos aplicar los lemas 4.6 y 4.7 sucesivamente hasta que se obtienen $(m-2)/2$ planos hiperbólicos ortogonales dos a dos y una variedad lineal W de dimensión 2.

Por la proposición 4.1 se tiene que, o bien W es un plano hiperbólico y por tanto el índice de U es $m/2$, o W no contiene vectores isótropos y el índice de U es $m/2 - 1$.

En el caso de que W contenga algún vector isótropo se tiene por la proposición 4.1 que W es un plano hiperbólico, y usando el lema 4.7 obtenemos un plano hiperbólico. De esta forma tenemos U como suma ortogonal de $m/2$ planos hiperbólicos.

En el caso de que W no contenga ningún vector isótropo usando la proposición 4.5 se obtienen dos generadores ortonormales de W de forma que se tiene U como suma ortogonal de $(m-2)/2$ planos hiperbólicos y dos variedades lineales de dimensión 1. Notesé que este último caso únicamente se tiene cuando $q \equiv 3 \mod 4$. □

Además hemos probado que el índice U de un subespacio vectorial de dimensión m es: $(m-1)/2$ si m es impar y $m/2$ o $m/2 - 1$ si m es par.

Como corolario deducimos cuándo $\mathbb{F}_q^n$, con n par, es de tipo hiperbólico o elíptico.

COROLARIO 4.9. *Para $U = \mathbb{F}_q^n$, con n par se tiene que el índice de $\mathbb{F}_q^n$ es*

- *$n/2$ (y por tanto B es de tipo hiperbólico), si -1 es un cuadrado de $\mathbb{F}_q$ o bien si -1 no es un cuadrado de $\mathbb{F}_q$ y $4 \mid n$.*
- *$n/2-1$ (y por tanto B es de tipo elíptico), si -1 no es un cuadrado de $\mathbb{F}_q$ y $4 \nmid n$.*

DEMOSTRACIÓN. Usando el resultado anterior podemos escribir $\mathbb{F}_q^n$ como suma ortogonal de $n/2-1$ planos hiperbólicos y una variedad lineal W de dimensión 2 que o bien es un plano hiperbólico si contiene vectores isótropos o bien es un subespacio lineal sin espacios isótropos generado por dos vectores ortonormales. Sea M la matriz de B en la base de $\mathbb{F}_q^n$ dada por los generadores geométricos de los planos hiperbólicos y la base correspondiente de W.

Sea -1 un cuadrado de $\mathbb{F}_q$ y supongamos que W está generado por x_1, x_2 ortonormales. Sea $y = a_1x_1 + a_2x_2$, y es isótropo si $B(y,y) = 0$, es decir si $a_1^2B(x_1,x_1) + a_2^2B(x_2,x_2) = a_1^2 + a_2^2 = 0$ o, equivalentemente, si $(a_1/a_2)^2 = -1$. Como -1 es un cuadrado se tiene que existe un vector isótropo en W y por tanto W es un plano hiperbólico.

Sea -1 un no cuadrado de $\mathbb{F}_q$ y $4 \mid n$. Supongamos que W está generado por dos vectores ortonormales, entonces se tiene que $\det(M) = -1$, lo que contradice que el discriminante de B es 1 modulo un cuadrado de $\mathbb{F}_q$, por lo que W es un plano hiperbólico.

Sea -1 un no cuadrado de $\mathbb{F}_q$ y $4 \nmid n$. Supongamos que W es un plano hiperbólico, entonces se tiene que $\det(M) = -1$, lo que contradice que el discriminante de B es 1 modulo un cuadrado de $\mathbb{F}_q$, por lo que W no tiene vectores isótropos. □

En $\mathbb{F}_q^n$ existen bases ortonormales para la forma bilineal B, por ejemplo la base canónica. Sin embargo, no siempre a partir de una base ortogonal podemos obtener una base ortonormal multiplicando por el inverso de la norma, únicamente lo podremos hacer cuando los vectores tengan un producto que es un cuadrado en $\mathbb{F}_q$. Por tanto, dada una variedad lineal $L = \langle x \rangle$ tenemos que $B(x,x)$ es igual a a^2 o a^2g donde g es un no cuadrado de $\mathbb{F}_q$, además multiplicando x por a^{-1} podemos suponer que $B(x,x) = 1$ o bien que $B(x,x) = g$ y diremos que x es una base geométrica de L.

Por los resultados anteriores podemos escribir $\mathbb{F}_q^n$ como suma ortogonal de planos hiperbólicos y de variedades lineales de dimensión uno. Además, los planos hiperbólicos están generados por dos vectores isótropos cuyo producto es uno y la variedades lineales están generadas por vectores no isótropos.

Decimos que $\mathbb{F}_q^n$ tiene **descomposición geométrica de tipo** r, s si

$$\mathbb{F}_q^n = H_1 \perp \cdots \perp H_r \perp L_1 \perp \cdots \perp L_s$$

donde $H_1, \ldots, H_r$ son planos hiperbólicos y $L_1, \ldots, L_s$ son variedades lineales unidimensionales no isótropas. Cada plano hiperbólico está generado por dos generadores geométricos $H_i = \langle x_{2i-1}, x_{2i} \rangle$, $i = 1, \ldots, r$. Cada variedad de dimensión 1 está generada por $L_i = \langle x_{2r+i} \rangle$, $i = 1, \ldots, s$. Se tiene que $\{x_1, \ldots, x_n\}$ es una base de $\mathbb{F}_q^n$ y se dice que es una **base de la descomposición geométrica**.

Sea M la matriz de B en dicha base, entonces se tiene que $MM^t = J_{r,s}$

$$J_{r,s} = \begin{pmatrix} 0 & 1 & & & & & & \\ 1 & 0 & & & & & & \\ & & \ddots & & & & & \\ & & & 0 & 1 & & & \\ & & & 1 & 0 & & & \\ & & & & & \varepsilon_1 & & \\ & & & & & & \ddots & \\ & & & & & & & \varepsilon_s \end{pmatrix}$$

donde ε_i es o bien 1 o bien un no cuadrado fijo de $\mathbb{F}_q^*$.

Decimos que una base $\{x_1, \ldots, x_n\}$ de $\mathbb{F}_q^n$ es una **base de compatible con la descomposición** $J_{r,s}$ si $\{x_{2i-1}, x_{2i}\}$, con $i = 1, \ldots, r$, son una base geométrica de planos hiperbólicos; x_{2r+i}, con $i = 1, \ldots s$, generan una variedades lineales de dimensión 1 y de tal forma que son ortogonales dos a dos. O equivalentemente, si la matriz de B en dicha base, M, verifica $MM^t = J_{r,s}$.

Una descomposición es mínima si es de tipo $0, n$; se tiene que $J_{0,n}$ es igual la matriz identidad $n \times n$. La base canónica es una base compatible con una descomposición mínima. Decimos que una descomposición es maximal si es como la dada en la proposición 4.8.

3. Códigos Lineales Compatibles con Descomposiciones Geométricas en Característica Distinta de 2

Sea $\mathcal{C} \subset \mathbb{F}_q^n$ un código lineal, decimos que $\mathcal{C}$ es **compatible con una descomposición geométrica de tipo** $J_{r,s}$ si existe una base $\{x_1, \ldots, x_n\}$ de $\mathbb{F}_q^n$ compatible con dicha descomposición, de tal forma que existe $I \subset \{1, \ldots, n\}$ tal que $\{x_i \mid i \in I\}$ es una base de $\mathcal{C}$.

El siguiente resultado muestra que todo código lineal es compatible con una descomposición geométrica. Este resultado permite estudiar cualquier código lineal dando una descomposición geométrica, y así extender el estudio de [53] de códigos autoortogonales y autoduales a códigos lineales arbitrarios.

TEOREMA 4.10. *Sea $\mathbb{F}_q$ de característica distinta de 2. Todo código lineal $\mathcal{C} \subset \mathbb{F}_q^n$ es compatible con al menos una descomposición geométrica.*

DEMOSTRACIÓN. Sea $\mathcal{C} = \text{rad}(\mathcal{C}) \perp \mathcal{C}_1$, donde $\text{rad}(\mathcal{C}) = \langle x_1, \ldots, x_l \rangle$

Podemos calcular $x'_1, \ldots, x'_l \in \mathcal{C}_1$ de forma que x_i, x'_i son los generadores geométricos de un plano hiperbólico y además los planos hiperbólicos $H_i = \langle x_i, x'_i \rangle$ son ortogonales dos a dos y ortogonales a $\mathcal{C}_1$. Es decir, se tiene que

$$\mathcal{C}' = H_1 \perp \cdots \perp H_l \perp \mathcal{C}_1$$

donde $\mathcal{C}'$ contiene a $\mathcal{C}$ y es no singular. Probemos la construcción de $\mathcal{C}'$ por inducción en l, que es parte del teorema 3.8 de [1].

Para $l = 0$ no hay nada que probar. El subespacio $\mathcal{C}_0 = \langle x_1, \ldots, x_{l-1} \rangle \perp \mathcal{C}_1$ es ortogonal a x_l pero no lo contiene, por tanto existe $y \in \mathcal{C}_0^\perp$ tal que $B(x_l, y) \neq 0$. El plano generado por x_l, y es no singular y está contenido en $\mathcal{C}_0^\perp$ y por la proposición 4.1 está generado por una base geométrica $H_l = \langle x_l, x'_l \rangle$. Como $H_l \subset \mathcal{C}_0^\perp$, entonces $\mathcal{C}_0 \perp H_l$ y $\mathcal{C}_0 \subset H_l^\perp$. Como el radical de $\mathcal{C}_0$ tiene dimensión $l - 1$ por la hipótesis de inducción podemos encontrar bases geométricas x_i, x'_i de H_i en $H_l^\perp$, para $i = 1, \ldots, l-1$ que sean ortogonales dos a dos y a $\mathcal{C}_1$ y puesto que son ortogonales a H_l y H_l es ortogonal a $\mathcal{C}_1$ se tiene probada la construcción de $\mathcal{C}'$.

Por tanto, tenemos $\mathcal{C}' = H_1 \perp \cdots \perp H_l \perp \mathcal{C}_1$, donde $H_i = \langle x_i, x'_i \rangle$, con $x'_i \notin \mathcal{C}$. Además $\mathcal{C}'$ es no singular y por tanto $\mathbb{F}_q^n = H_1 \perp \cdots \perp H_l \perp \mathcal{C}_1 \perp \mathcal{C}'^\perp$.

Como $\mathcal{C}_1$ es no singular podemos usar la proposición 4.8 para escribir $\mathcal{C}'$ como suma de planos hiperbólicos y un subespacio vectorial W de dimensión 1 o 2 (si la dimensión de $\mathcal{C}'$ es menor de 3 entonces no consideramos ningún plano hiperbólico y $\mathcal{C}' = W$). Por tanto obtenemos $\mathcal{C}' = H_{l+1} \perp \cdots \perp H_m \perp W$, donde $H_{l+i} = \langle x_{l+i}, x'_{l+i} \rangle$.

Por la proposición 4.8 podemos tener 3 tipos de geometría para W

(a) Si $\dim(W) = 1$, escribimos $W = \langle x \rangle$. Además x no es isótropo puesto que B es no degenerada. Podemos considerar $x \in W$ de forma que $B(x, x)$ es igual a 1 o g, donde g es un no cuadrado fijo y $W = L_1 = \langle x_{m+1} \rangle$.
(b) Si $\dim(W) = 2$ y W contiene algún vector isótropo, entonces W es un plano hiperbólico, $W = H_{m+1} = \langle x_{m+1}, x'_{m+1} \rangle$, por la proposición 4.1.
(c) Si $\dim(W) = 2$ y W no contiene ningún vector isótropo entonces W puede generarse por dos vectores ortonormales $L_1 = \langle x_{m+1} \rangle$, $L_2 = \langle x_{m+2} \rangle$, donde $W = L_1 \perp L_2$, por la proposición 4.5.

Descomponemos $\mathcal{C}'^\perp$ de la misma forma que $\mathcal{C}$ y obtenemos

$$\mathcal{C}'_1 = H'_1 \perp \cdots \perp H'_{m'} \perp W'$$

Por consiguiente, conservando notaciones, tenemos la descomposición geométrica de $\mathbb{F}_q^n$

(a) $\mathbb{F}_q^n = H_1 \perp \cdots \perp H_m \perp L_1 \perp H_1' \perp \cdots \perp H_{m'}' \perp W'$ y
$\mathcal{C} = \langle x_1, \ldots, x_l, x_{l+1}, x_{l+1}', \ldots, x_m, x_m', x_{m+1} \rangle$
(b) $\mathbb{F}_q^n = H_1 \perp \cdots \perp H_m \perp H_{m+1} \perp H_1' \perp \cdots \perp H_{m'}' \perp W'$ y
$\mathcal{C} = \langle x_1, \ldots, x_l, x_{l+1}, x_{l+1}', \ldots, x_{m+1}, x_{m+1}' \rangle$
(c) $\mathbb{F}_q^n = H_1 \perp \cdots \perp H_m \perp L_1 \perp L_2 \perp H_1' \perp \cdots \perp H_{m'}' \perp W'$ y
$\mathcal{C} = \langle x_1, \ldots, x_l, x_{l+1}, x_{l+1}', \ldots, x_m, x_m', x_{m+1}, x_{m+2} \rangle$ □

Decimos que un código lineal $\mathcal{C}$ dado por los generadores $\mathcal{C} = \langle x_1, \ldots, x_k \rangle$ está dado en la **forma geométrica estándar** si la matriz de B restringida a $x_1, \ldots, x_k$ es la misma matriz que la de B restringida a los generadores de $\mathcal{C}$ de la base obtenida en el teorema 4.10.

De la construcción de la base de $\mathbb{F}_q^n$ del teorema 4.10 se deduce que un código lineal puede darse como el subespacio lineal generado por parte de una base geométrica de tipo r, s con $s \leq 4$, puesto que generamos planos hiperbólicos hasta obtener un subespacio sin vectores isótropos de dimensión menor o igual que dos. El siguiente ejemplo ilustra una descomposición geométrica estándar con $s = 4$.

Ejemplo 4.11. La descomposición geométrica de un código lineal $\mathcal{C}$ dada por el teorema 4.10 consiste en una suma ortogonal de planos hiperbólicos y a lo sumo dos subespacios unidimensionales. A su vez el complemento de $\mathcal{C}$ tiene también una descomposición equivalente. Por tanto, la descomposición geométrica de $\mathbb{F}_q^n$ obtenida es una suma ortogonal de planos hiperbólicos y a lo sumo 4 subespacios unidimensionales. Sea $\mathcal{C} = \langle (3,2,0,0), (4,4,0,0) \rangle$ contenido en $\mathbb{F}_7^4$, como -1 no es un cuadrado se tiene que $\mathcal{C} = \langle (1,0,0,0), (0,1,0,0) \rangle$ y $\mathcal{C}' = \langle (0,0,1,0), (0,0,0,1) \rangle$ es la descomposición geométrica dada por el teorema 4.10. Por tanto, la forma bilineal B en esta base tiene por matriz

$$\begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & 1 \end{pmatrix}$$

El siguiente ejemplo ilustra una descomposición geométrica de $\mathbb{F}_3^{12}$ compatible con el código de Golay $\mathcal{G}_{12}$.

Ejemplo 4.12. El código de Golay $\mathcal{G}_{12}$ es un código autodual sobre $\mathbb{F}_3$ que tiene matriz generatriz [47]:

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 2 & 2 & 1 & 2 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 2 & 2 & 2 \\ 0 & 0 & 0 & 1 & 0 & 0 & 2 & 1 & 0 & 1 & 2 & 2 \\ 0 & 0 & 0 & 0 & 1 & 0 & 2 & 2 & 1 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 2 & 2 & 1 & 0 & 2 \end{pmatrix}$$

Se tiene que $\mathcal{G}_{12} \subset \mathbb{F}_3^{12}$ y, aunque -1 no es un cuadrado en $\mathbb{F}_3$, 4 divide a $n = 12$ y por tanto la descomposición maximal de $\mathbb{F}_3^{12}$ compatible con $\mathcal{G}_{12}$ es la suma ortogonal de 8 planos hiperbólicos, donde el primer generador pertenece al código y el segundo no. La matriz M de la descomposición geométrica es

$$M = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 2 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 2 & 2 & 1 & 2 \\ 0 & 2 & 0 & 0 & 0 & 0 & 0 & 1 & 2 & 2 & 1 & 2 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 2 & 2 & 2 \\ 0 & 0 & 2 & 0 & 0 & 0 & 1 & 0 & 1 & 2 & 2 & 2 \\ 0 & 0 & 0 & 1 & 0 & 0 & 2 & 1 & 0 & 1 & 2 & 2 \\ 0 & 0 & 0 & 2 & 0 & 0 & 2 & 1 & 0 & 1 & 2 & 2 \\ 0 & 0 & 0 & 0 & 1 & 0 & 2 & 2 & 1 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 & 2 & 0 & 2 & 2 & 1 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 2 & 2 & 1 & 0 & 2 \\ 0 & 0 & 0 & 0 & 0 & 2 & 1 & 2 & 2 & 1 & 0 & 2 \end{pmatrix}$$

Una base del código son las filas 1,3,5,7,9,11. Se tiene

$$MM^t = J_{8,0} = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

4. Descomposiciones Geométricas en Característica 2

La situación en el caso de que la característica de $\mathbb{F}_q$ sea igual a 2, es decir $q = 2^l$, es muy diferente y en su mayoría las demostraciones anteriores no son válidas, aunque obtendremos una descomposición geométrica análoga.

En el caso de característica distinta de 2, se tiene una correspondencia entre las forma bilineales simétricas y las formas cuadráticas. Podemos definir una forma cuadrática a partir de la forma bilineal $Q(x) = B(x, x)$ que da una correspondencia biunívoca entre las formas bilineales simétricas y las formas cuadráticas por medio de la polaridad. En cambio, en característica 2 no se tiene esta propiedad.

En característica 2 se llama una forma cuadrática a una aplicación Q de $\mathbb{F}_q^n$ en $\mathbb{F}_q$ que verifica

$$Q(\lambda x + \mu y) = \lambda^2 Q(x) + \mu^2 Q(y) + \lambda\mu F(x, y)$$

donde F es una forma bilineal sobre $\mathbb{F}_q^n$. Se tiene que F está determinada por Q puesto que

$$F(x, y) = Q(x + y) + Q(x) + Q(y)$$

Si definimos $Q(x) = \sum x_i^2$ tenemos que $F = 0$.

Como hemos visto en el ejemplo 4.2, $\mathbb{F}_q^2$ es un plano no singular que contiene un vector isótropo pero no puede estar generado por dos vectores isótropos. En cambio en característica distinta de 2 sí hay un vector isótropo, entonces siempre existe otro vector isótropo que junto con el primero genera un plano hiperbólico.

El siguiente resultado permite calcular y obtener una base de los vectores isótropos de $\mathbb{F}_q^n$.

PROPOSICIÓN 4.13. *Sea $x \in \mathbb{F}_q^n$, se tiene que x es isótropo si y sólo si $\sum_{i=1}^n x_i = 0$. Los $n-1$ vectores $y_1 = (1, 1, 0, \ldots, 0)$, $y_2 = (0, 1, 1, 0, \ldots, 0)$, $\ldots$, $y_n = (0, \ldots, 0, 1, 1)$ consituyen una base del subespacio vectorial de vectores isótropos de $\mathbb{F}_q^n$.*

DEMOSTRACIÓN. Se tiene que x es isótropo si y sólo si $B(x, x) = 0$. Es decir $\sum_{i=1}^n x_i^2 = 0$ si y sólo si $(\sum_{i=1}^n x_i)^2 = 0$ o, equivalentemente, si $\sum_{i=1}^n x_i = 0$.

Los vectores isótropos de $\mathbb{F}_q^n$ forman un subespacio vectorial. Se tiene trivialmente que y_i es isótropo $\forall$ i y que $y_1, \ldots, y_n$ son linealmente independientes. Veamos que $\{y_1, \ldots, y_n\}$ es un sistema generador del subespacio vectorial de vectores isótropos. Sea $x = (x_1, \ldots, x_n)$ isótropo,

definimos los coeficientes de la combinación lineal

$$\begin{cases} \lambda_1 = x_1 \\ \lambda_2 = x_2 + x_1 \\ \lambda_3 = x_3 + x_2 + x_1 \\ \quad \vdots \\ \lambda_n = x_{n-1} + x_{n-2} + \cdots + x_1 \end{cases}$$

Se tiene que $\sum_{i=1}^{n-1} \lambda_i y_i = (x_1, \ldots, x_{n-1}, \sum_{i=1}^{n-1} x_i) = (x_1, \ldots, x_{n-1}, x_n)$. La última igualdad se deduce de la ecuación $x_n = \sum_{i=1}^{n-1} x_i$ debido a que x es isótropo. □

Como corolario de este resultado deducimos que $\mathbb{F}_q^n$ con n par no puede descomponerse en suma ortogonal de $n/2$ planos hiperbólicos. Nótese la diferencia con el caso de característica distinta de dos.

El siguiente resultado se deduce trivialmente de la proposición anterior, pero no de forma constructiva, por lo que presentamos una prueba constructiva que es útil para calcular una base geométrica en la práctica.

LEMA 4.14. *Sea $U \subset \mathbb{F}_q^n$ un subespacio vectorial de dimensión mayor o igual que 2, entonces existe al menos un vector isótropo en U.*

DEMOSTRACIÓN. Sean x_1, x_2 dos vectores linealmente independientes de U que no son isótropos. Sea $y = \lambda_1 x_1 + \lambda_2 x_2$, donde calculamos los coeficientes λ_1 y λ_2 para que y sea isótropo.

Se tiene que $B(y, y) = \lambda_1^2 B(x_1, x_1) + \lambda_2^2 B(x_2, x_2) = 0$, si y sólo si $(\lambda_1/\lambda_2)^2 = B(x_2, x_2)/B(x_1, x_1)$. Y como en un cuerpo de característica 2 todo elemento es un cuadrado, se tiene que $\lambda_1 = \sqrt{B(x_2, x_2)}$ y $\lambda_2 = \sqrt{B(x_1, x_1)}$ □

El siguiente resultado muestra que todo subespacio vectorial de dimensión 2 no singular es o bien un plano hiperbólico o bien un plano elíptico.

PROPOSICIÓN 4.15. *Sea $U \subset \mathbb{F}_q^n$ un subespacio vectorial no singular de dimensión 2. Entonces U es un plano hiperbólico o un plano elíptico.*

DEMOSTRACIÓN. Por la proposición 4.13 se tiene que o bien hay dos rectas diferentes de vectores isótropos o bien únicamente una. Veamos que en el primer caso se tiene un plano hiperbólico y en el segundo un plano elíptico.

Sean x_1, $x_2 \in U$ isótropos y linealmente independientes. Por tanto $\lambda = B(x_1, x_2)$ es distinto de cero, sean $y_1 = \lambda^{-1} x_1$, $y_2 = x_2$. Se tiene que y_1, y_2 son los generadores de un plano hiperbólico, es decir $B(y_1, y_1) = 0$, $B(y_2, y_2) = 0$ y $B(y_1, y_2) = 1$.

Sean x_1, $x_2 \in U$ linealmente independientes, con x_1 isótropo y x_2 no isótropo. Sea $\lambda = B(x_1, x_2)$ y $\mu = B(x_2, x_2) \neq 0$. Se tiene que

$y_1 = \lambda^{-1}\sqrt{\mu}x_1$, $y_2 = \sqrt{\mu^{-1}}x_2$ son los generadores de un plano elíptico $B(y_1, y_1) = 0$ y $B(y_1, y_2) = B(y_2, y_2) = 1$. □

Como veremos en la sección 4.6 los planos elípticos no son apropiados para calcular el dual de un código lineal. El siguiente lema permite trabajar con un plano ortonormal en lugar de con un plano elíptico.

LEMA 4.16. *Sea $E \subset \mathbb{F}_q^n$ un plano elíptico con generadores geométricos $E = \langle x_1, x_2\rangle$, entonces existen dos generadores de E ortonormales.*

DEMOSTRACIÓN. Sean $y_1 = x_1 + x_2$, $y_2 = x_2$. Puesto que son linealmente independientes, son una base de E y $B(y_1, y_1) = B(x_1, x_1) + B(x_2, x_2) = 1$ y $B(y_1, y_2) = B(x_1, x_2) + B(x_2, x_2) = 0$. □

En la proposición 4.18 escribimos $U \subset \mathbb{F}_q^n$ de dimensión mayor o igual que 3 como suma ortogonal de planos hiperbólicos y un subespacio de dimensión menor o igual que 2. Para demostrar este resultado necesitamos el siguiente lema que escribe un subespacio vectorial de dimensión mayor o igual que 3 como suma ortogonal de un plano hiperbólico y su ortogonal.

LEMA 4.17. *Sea $U \subset \mathbb{F}_q^n$ un subespacio vectorial no singular de dimensión mayor o igual que 3. Entonces existen x, y generadores de un plano hiperbólico H de forma que $U = H \perp U'$ donde U' es un subespacio vectorial no singular.*

DEMOSTRACIÓN. Usando el lema 4.14, se obtiene $x \in U$ isótropo y tenemos que $U = \langle x\rangle \perp U_1$, donde $U_1 = \langle x\rangle^{\perp} \cap U$. Como U_1 es un subespacio vectorial no singular de dimensión mayor o igual que dos, por el lema 4.14 se obtiene $y \in U$ isótropo. Y por tanto x, y generan un plano hiperbólico H y $U = H \perp U'$ donde $U' = H^{\perp} \cap U$. □

Usando el lema previo podemos probar el siguiente resultado.

PROPOSICIÓN 4.18. *Sea $U \subset \mathbb{F}_q^n$ un espacio vectorial no singular de dimensión m con $\mathbb{F}_q$ de característica igual a dos. Se puede descomponer U de la siguiente forma:*

Para m impar

(1) *$U = H_1 \perp \cdots \perp H_{(m-1)/2} \perp L$, donde cada H_i es un plano hiperbólico y L es un subespacio lineal de dimensión 1.*

Para m par

(2) *$U = H_1 \perp \cdots \perp H_{m/2}$, donde cada H_i es un plano hiperbólico.*
(3) *$U = H_1 \perp \cdots \perp H_{m/2-1} \perp L_1 \perp L_2$, donde cada H_i es un plano hiperbólico y L_1, L_2 son subespacios lineales de dimensión 1.*

DEMOSTRACIÓN. Sea m impar, podemos aplicar el lema 4.17 sucesivamente para generar planos hiperbólicos hasta que se obtienen $(m-1)/2$

planos hiperbólicos ortogonales dos a dos y una variedad lineal de dimensión 1.

Del mismo modo, en el caso de m par, podemos aplicar el lema 4.17 sucesivamente hasta que se obtienen $m/2-1$ planos hiperbólicos ortogonales dos a dos y una variedad lineal de dimensión 2. Esta variedad lineal de dimensión 2 es o bien un plano elíptico o bien un plano hiperbólico, dependiendo de si tiene dos vectores isótropos linealmente independientes o no (proposición 4.15). En el caso de que sea un plano elíptico éste puede ser generado por dos vectores ortonormales usando la proposición 4.16 □

Sea $U = \mathbb{F}_q^n$ con n par, entonces U necesariamente tiene una descomposición de tipo (3), ya que en $\mathbb{F}_q^n$ hay únicamente $n-1$ vectores isótropos linealmente independientes (proposición 4.13).

Sea x un vector no isótropo, entonces podemos suponer que $B(x,x)=1$ puesto que todos los elementos de $\mathbb{F}_q^*$ son cuadrados y diremos que x es una **base geométrica de** $L=\langle x\rangle$.

Por los resultados anteriores podemos escribir $\mathbb{F}_q^n$ como suma ortogonal de planos hiperbólicos, variedades lineales de dimensión uno y, a lo sumo, un plano elíptico.

Decimos que $\mathbb{F}_q^n$ tiene una **descomposición geométrica de tipo** r,s,t si

$$\mathbb{F}_q^n = P_1 \perp \cdots \perp P_r \perp L_1 \perp \cdots \perp L_s, \text{ con } t=0$$

$$\mathbb{F}_q^n = P_1 \perp \cdots \perp P_r \perp L_1 \perp \cdots \perp L_s \perp E, \text{ con } t=1$$

donde $H_1,\ldots,H_r$ son planos hiperbólicos, $L_1,\ldots,L_s$ son variedades lineales unidimensionales no isótropas y E es un plano elíptico. Cada plano hiperbólico está generado por dos generadores geométricos $H_i=\langle x_{2i-1},x_{2i}\rangle$, $i=1,\ldots,r$, cada variedad de dimensión 1 está generada por un generador geométrico $L_i=\langle x_{2r+i}\rangle$, $i=1,\ldots,s$ y el plano elíptico está generado por dos generadores geométricos $E=\langle x_{n-1},x_n\rangle$ si $t=1$. Se tiene que $\{x_1,\ldots,x_n\}$ es una base de $\mathbb{F}_q^n$ y se dice que es una **base de la descomposición geométrica**.

Sea M la matriz de B en dicha base, entonces se tiene que $MM^t = J_{r,s,t}$

$$J_{r,s,0} = \begin{pmatrix} 0 & 1 & & & & & & \\ 1 & 0 & & & & & & \\ & & \ddots & & & & & \\ & & & 0 & 1 & & & \\ & & & 1 & 0 & & & \\ & & & & & 1 & & \\ & & & & & & \ddots & \\ & & & & & & & 1 \end{pmatrix}$$

$$J_{r,s,1} = \begin{pmatrix} 0 & 1 & & & & & & & \\ 1 & 0 & & & & & & & \\ & & \ddots & & & & & & \\ & & & 0 & 1 & & & & \\ & & & 1 & 0 & & & & \\ & & & & & 1 & & & \\ & & & & & & \ddots & & \\ & & & & & & & 1 & \\ & & & & & & & & 0 & 1 \\ & & & & & & & & 1 & 1 \end{pmatrix}$$

Decimos que una base $\{x_1, \ldots, x_n\}$ de $\mathbb{F}_q^n$ es una **base compatible con la descomposición** $J_{r,s,t}$ si $\{x_{2i-1}, x_{2i}\}$, con $i = 1, \ldots, r$, son una base geométrica de planos hiperbólicos; x_{2r+i}, con $i = 1, \ldots, s$, son una base geométrica de variedades lineales de dimensión 1; $\{x_{2r+s+1}, x_{2r+s+2}\}$ son una base geométrica de un plano elíptico (si $t = 1$) y de tal forma que son ortogonales dos a dos. O, equivalentemente, si la matriz de B en dicha base, M, verifica $MM^t = J_{r,s,t}$.

Una descomposición es mínima si es de tipo $0, n, 0$; se tiene que $J_{0,n,0}$ es igual la matriz identidad $n \times n$. La base canónica es una base compatible con una descomposición mínima. Decimos que una descomposición es maximal si es como la dada en la proposición 4.18.

5. Códigos Lineales Compatibles con Descomposiciones Geométricas en Característica 2

Sea $\mathcal{C} \subset \mathbb{F}_q^n$ un código lineal, decimos que $\mathcal{C}$ es **compatible con una descomposición geométrica de tipo** $J_{r,s,t}$ si existe una base $\{x_1, \ldots, x_n\}$ de $\mathbb{F}_q^n$ compatible con dicha descomposición, de tal forma que existe $I \subset \{1, \ldots, n\}$ tal que $\{x_i \mid i \in I\}$ es una base de $\mathcal{C}$.

El siguiente resultado muestra que todo código lineal es compatible con una descomposición geométrica. Este resultado permite estudiar cualquier código lineal dando una descomposición geométrica, y así extender el estudio de [52] de códigos autoortogonales y autoduales a códigos lineales arbitrarios.

TEOREMA 4.19. *Sea $\mathbb{F}_q$ de característica 2. Todo código lineal $\mathcal{C} \subset \mathbb{F}_q^n$ es compatible con al menos una descomposición geométrica.*

DEMOSTRACIÓN. Sea $\mathcal{C} = \mathrm{rad}(\mathcal{C}) \perp \mathcal{C}_1$, donde $\mathrm{rad}(\mathcal{C}) = \langle x_1, \ldots, x_l \rangle$. Distinguimos dos casos, $l = n/2$ con n par y el resto de los casos. Primero probamos el caso general y, posteriormente, el caso particular $l = n/2$ con n par.

Podemos calcular $x_1', \ldots, x_l' \in \mathcal{C}_1$ de forma que x_i, x_i' sean los generadores geométricos de un plano hiperbólico y además los planos hiperbólicos $H_i =$

$\langle x_i, x_i' \rangle$ sean ortogonales dos a dos y ortogonales a $\mathcal{C}_1$. Es decir, se tiene que

$$\mathcal{C}' = H_1 \perp \cdots \perp H_l \perp \mathcal{C}_1$$

donde $\mathcal{C}'$ contiene a $\mathcal{C}$ y es no singular. Probemos la construcción de $\mathcal{C}'$ por inducción en l.

Para $l = 0$ no hay nada que probar. El subespacio $\mathcal{C}_0 = \langle x_1, \ldots, x_{l-1} \rangle \perp \mathcal{C}_1$ es ortogonal a x_l pero no lo contiene, por tanto existe $y \in \mathcal{C}_0^{\perp}$ isótropo tal que $B(x_l, y) \neq 0$ puesto que el subespacio vectorial de vectores isótropos tiene dimensión $n-1$ (proposición 4.13). El plano generado por x_l, y es no singular y está contenido en $\mathcal{C}_0^{\perp}$ y por la proposición 4.15 está generado por una base geométrica $H_l = \langle x_l, x_l' \rangle$. Como $H_l \subset \mathcal{C}_0^{\perp}$ entonces $\mathcal{C}_0 \perp H_l$ y $\mathcal{C}_0 \subset H_l^{\perp}$. Como el radical de $\mathcal{C}_0$ tiene dimensión $l-1$ por la hipótesis de inducción podemos encontrar bases geométricas x_i, x_i' de H_i en $H_l^{\perp}$, para $i = 1, \ldots, l-1$ que sean ortogonales dos a dos y a $\mathcal{C}_1$ y puesto que son ortogonales a H_l y H_l es ortogonal a $\mathcal{C}_1$, se tiene probada la construcción de $\mathcal{C}'$.

Como $\mathcal{C}_1$ es no singular, podemos usar la proposición 4.18 para escribir $\mathcal{C}'$ como suma de planos hiperbólicos y un subespacio vectorial W de dimensión 1 o 2 (si la dimensión de $\mathcal{C}'$ es menor de 3 entonces no consideramos ningún plano hiperbólico y $\mathcal{C}' = W$). Por tanto, obtenemos $\mathcal{C}' = H_{l+1} \perp \cdots \perp H_m \perp W$, donde $H_{l+i} = \langle x_{l+i}, x_{l+i}' \rangle$.

Por la proposición 4.18 podemos tener 3 tipos de geometría para W

(a) Si $\dim(W) = 1$, escribimos $W = \langle x \rangle$. Además x no es isótropo puesto que B es no degenerada. Podemos considerar $x \in W$ de forma que $B(x, x)$ es igual a 1 y $W = L_1 = \langle x_{m+1} \rangle$.
(b) Si $\dim(W) = 2$ y W contiene dos vectores isótropos linealmente independientes entonces por la proposición 4.15 W es un plano hiperbólico, $W = H_{m+1} = \langle x_{m+1}, x_{m+1}' \rangle$, .
(c) Si $\dim(W) = 2$ y W no contiene dos rectas de vectores isótropos entonces W es un plano elíptico por la proposición 4.15. Usando el lema 4.16 dicho plano elíptico puede generarse por dos vectores ortonormales $L_1 = \langle x_{m+1} \rangle$, $L_2 = \langle x_{m+2} \rangle$, donde $W = L_1 \perp L_2$.

Descomponemos $\mathcal{C}'^{\perp}$ de la misma forma que $\mathcal{C}$ y obtenemos

$$\mathcal{C}_1' = H_1' \perp \cdots \perp H_{m'}' \perp W'$$

Por consiguiente, conservando notaciones tenemos la descomposición geométrica de $\mathbb{F}_q^n$

(a) $\mathbb{F}_q^n = H_1 \perp \cdots \perp H_m \perp L_1 \perp H_1' \perp \cdots \perp H_{m'}' \perp W'$ y
$\mathcal{C} = \langle x_1, \ldots, x_l, x_{l+1}, x_{l+1}', \ldots, x_m, x_m', x_{m+1} \rangle$
(b) $\mathbb{F}_q^n = H_1 \perp \cdots \perp H_m \perp H_{m+1} \perp H_1' \perp \cdots \perp H_{m'}' \perp W'$ y
$\mathcal{C} = \langle x_1, \ldots, x_l, x_{l+1}, x_{l+1}', \ldots, x_{m+1}, x_{m+1}' \rangle$
(c) $\mathbb{F}_q^n = H_1 \perp \cdots \perp H_m \perp L_1 \perp L_2 \perp H_1' \perp \cdots \perp H_{m'}' \perp W'$ y
$\mathcal{C} = \langle x_1, \ldots, x_l, x_{l+1}, x_{l+1}', \ldots, x_m, x_m', x_{m+1}, x_{m+2} \rangle$

Sea $l = n/2$ con n par. Podemos calcular $x'_1, \ldots, x'_{n/2} \in \mathcal{C}_1$ de forma que x_i, x'_i sean los generadores geométricos de un plano hiperbólico para $i = 1, \ldots, n/2-1$ y $x_{n/2}, x'_{n/2}$ sean los generadores geométricos de un plano elíptico. Además los planos hiperbólicos $H_i = \langle x_i, x'_i \rangle$ y el plano elíptico $E = \langle x_{n/2}, x'_{n/2} \rangle$ son ortogonales dos a dos. Es decir, se tiene que

$$\mathbb{F}_q^n = H_1 \perp \cdots \perp H_{n/2-1} \perp E$$

Por el apartado anterior podemos construir $H_1 \perp \cdots \perp H_{n/2-1}$, con $H_i = \langle x_i, x'_i \rangle$, puesto que su índice es menor que $n/2$. Consideramos $E = (H_1 \perp \cdots \perp H_{n/2-1})^\perp$. Se tiene que $x_{n/2} \in E$ y no está contenido en $H_1 \perp \cdots \perp H_{n/2-1}$, por tanto no existe ningún vector isótropo en E linealmente independiente de $x_{n/2}$ puesto que el subespacio de vectores isótropos tiene dimensión $n-1$. Por la proposición 4.15, podemos considerar $y \in E$ tal que $x_{n/2}, y$ son los generadores geométricos del plano elíptico E.

Por tanto, tenemos la siguiente descomposición geométrica de $\mathbb{F}_q^n$

(d) $\mathbb{F}_q^n = H_1 \perp \cdots \perp H_{n/2-1} \perp E$ y
$\mathcal{C} = \langle x_1, \ldots, x_{n/2} \rangle$ □

Decimos que un código lineal $\mathcal{C}$ dado por los generadores $\mathcal{C} = \langle x_1, \ldots, x_k \rangle$ está dado en la **forma geométrica estándar** si la matriz de B restringida a $x_1, \ldots, x_k$ es la misma matriz que la de B restringida a los generadores de $\mathcal{C}$ de la base obtenida en el teorema 4.19.

De la construcción de la base de $\mathbb{F}_q^n$ del teorema 4.19 se deduce que un código lineal puede darse como el subespacio lineal generado por una parte de una base geométrica de tipo r, s, t con $s \leq 4$ y $t = 0$ o bien $s = 0$ y $t = 1$. Este segundo caso ($s = 0, t = 1$) se considera únicamente para códigos autoduales.

El siguiente ejemplo ilustra cómo evitamos emplear un plano elíptico cuando no se considera un código autodual.

EJEMPLO 4.20. Sea $\mathcal{C}$ el código lineal sobre $\mathbb{F}_2$ que tiene matriz generatriz

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

Sean $x_1 = (1,1,0,0)$ y $x_2 = (0,0,0,1)$. Se tiene que x_1 es un vector isótropo y que x_2 no lo es. Sea $x'_1 = (0,1,1,0)$, se tiene que x_1, x'_1 son una base geométrica de un plano hiperbólico $H_1 = \langle x_1, x'_1 \rangle$ que es ortogonal a x_2. Un vector ortogonal a H_1 y linealmente independiente de x_2 es $y = (1,1,1,1)$. Trivialmente, y es un vector isótropo, además y, x_2 forman una base geométrica de un plano elíptico. Pero, por otro lado, podemos considerar $x_3 = x_2 + y = (1,1,1,0)$ de forma que $L_2 = \langle x_2 \rangle$ y $L_3 = \langle x_3 \rangle$ son dos variedades lineales no isótropas. Por tanto, tenemos la descomposición geométrica de $\mathbb{F}_2^4$ de tipo $1, 2, 0$ compatible con $\mathcal{C}$ dada por $\mathbb{F}_2^4 = H_1 \perp L_1 \perp L_2$.

El siguiente ejemplo ilustra la descomposición geométrica de un código autodual en característica 2.

EJEMPLO 4.21. Sea $\mathcal{C}$ el código de $\mathbb{F}_2^6$ que tiene por matriz generatriz

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

Se trata de un código autodual, la suma de las coordenadas de los generadores del código, es decir las filas de la matriz generatriz, es 0 (proposición 4.13).

La descomposición maximal, por tanto, está dada por 2 planos hiperbólicos y un plano elíptico. En particular, se tiene que la matriz M de una descomposición geométrica maximal es

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

Una base del código son las filas 1, 3 y 5 de la matriz M, que en este caso forman la misma base que habíamos considerado previamente. La descomposición geométrica obtenida es $\mathbb{F}_2^6 = H_1 \perp H_2 \perp E$. Es decir, una descomposición de tipo 2,0,1

$$MM^t = J_{2,0,1} = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$

NOTA 4.22. La construcción de la base geométrica estándar de un código lineal viene dada por el teorema 4.10 en característica distinta de dos y 4.19 en característica 2. Dicha base puede ser calcularse en la práctica usando técnicas de álgebra y geometría lineales como muestran las demostraciones de los resultados.

6. Dual y Distancia Mínima de un Código Lineal

Una vez probado que en cualquier característica se tiene que todo código lineal es compatible con una descomposición geométrica, trabajamos en

una característica positiva arbitraria. Cuando la característica sea distinta de dos, tomamos $t = 0$ ya que no consideramos planos elípticos en la descomposición geométrica.

En esta sección extendemos dos resultados del capítulo 3, el cálculo del dual y el de la distancia mínima, de códigos tóricos generalizados para códigos lineales arbitrarios.

Sea $\{x_1, \ldots, x_n\}$ un base geométrica de una descomposición geométrica de tipo r, s, t. Sea $i \in \{1, \ldots, n\}$, definimos i' como

- $i + 1$ si x_i es el primer generador de un plano hiperbólico H
- $i - 1$ si x_i es el segundo generador de un plano hiperbólico H
- i si x_i genera un subespacio lineal L
- $i + 1$ si x_i es el primer generador de un plano elíptico E

No es necesario definir i' con x_i siendo el segundo generador de un plano elíptico porque únicamente consideramos descomposiciones geométricas con a lo sumo un plano elíptico en el que únicamente el primer generador pertenece al código, puesto que en el caso en que los dos generadores del plano elíptico pertenezcan al código, consideramos dos generadores ortonormales de subespacios lineales L, usando el lema 4.16.

Para $I \subset \{1, \ldots, n\}$ definimos $I' = \{i' \mid i \in I\}$ y $I^\perp = \{1, \ldots, n\} \setminus I'$. De esta forma podemos calcular el dual de un código lineal usando el siguiente resultado.

PROPOSICIÓN 4.23. *Sea $\mathcal{C}$ un código lineal con una descomposición geométrica de tipo r, s, t dada por la base $\{x_1, \ldots, x_n\}$ de $\mathbb{F}_q^n$ e $I \subset \{1, \ldots, n\}$ tal que $\mathcal{C} = \langle x_i \mid i \in I \rangle$. Entonces el dual del código $\mathcal{C}$ es $\mathcal{C}^\perp = \langle x_i \mid i \in I^\perp \rangle$.*

DEMOSTRACIÓN. De la matriz $J_{r,s,t}$ del producto bilineal de los vectores de la base se deduce que $\langle x_i \rangle^\perp = \langle x_j \mid j \neq i' \rangle$. Por tanto

$$\mathcal{C}^\perp = \langle x_j \mid j \notin I' \rangle = \langle x_i \mid i \in I^\perp \rangle$$

□

De esta forma, tenemos en una matriz un código lineal y su código ortogonal. Sea $\mathcal{C}$ un código lineal con una descomposición geométrica de tipo r, s, t dada por la base $\{x_1, \ldots, x_n\}$ de $\mathbb{F}_q^n$ e $I \subset \{1, \ldots, n\}$ tal que $\mathcal{C} = \langle x_i \mid i \in I \rangle$. Además, sea M la matriz $n \times n$ que tiene por filas los elementos de la base $\{x_1, \ldots, x_n\}$, por tanto se tiene $MM^t = J_{r,s,t}$. Sea $M(I)$ la matriz $k \times n$ formada por las filas $i \in I$, entonces $M(I)$ es una matriz generatriz de $\mathcal{C}$. Del mismo modo, $M(I^\perp)$ es una matriz de control de $\mathcal{C}$, es decir, $M(I^\perp)$ es una matriz generatriz del código dual $\mathcal{C}^\perp$.

El motivo por el que consideramos únicamente un plano elíptico en las descomposiciones geométricas cuando el primer generador pertenece al código y el segundo no, se fundamenta en lo siguiente: si x_i es el segundo generador de un plano elíptico $\langle x_i \rangle^\perp = \langle x_j \mid j \neq i, i-1 \rangle + \langle x_i + x_{i-1} \rangle$,

lo cual obligaría a cambiar la base geométrica de $\mathbb{F}_q^n$ para calcular el dual. Pero esto no es un problema, debido a que si el segundo generador geométrico pertenece al código entonces también pertenece el primero, como comprobamos en el teorema 4.19, y por tanto podemos considerar dos vectores ortonormales que generan el plano elíptico usando el lema 4.16.

El siguiente resultado extiende para códigos lineales arbitrarios [45, Proposition 2.1] y la proposición 3.8 de códigos tóricos generalizados. Además, probamos que ambas formas de calcular la distancia mínima son duales.

TEOREMA 4.24. *Sea $\mathcal{C}$ un código lineal con una descomposición de tipo r, s, t dada por la base $\{x_1, \ldots, x_n\}$ de $\mathbb{F}_q^n$ e $I \subset \{1, \ldots, n\}$ tal que $\mathcal{C} = \langle x_i \mid i \in I \rangle$. Sea M la matriz $n \times n$ tal que $MM^t = J_{r,s,t}$, donde una matriz generatriz de $\mathcal{C}$ es $M(I)$ y $M(I, J)$ es la submatriz de M formada por los elementos que están en las filas $i \in I$ y en las columnas $j \in J$.*

(a) *Sea d el menor entero positivo tal que para todo conjunto $J \subset \{1, \ldots, n\}$ con $\#J = n-d+1$ existe algún $K \subset J$ con $\#K = k$ tal que $\det M(I, K) \neq 0$. Entonces la distancia mínima de $\mathcal{C}$ es d.*
(b) *Sea d el mayor entero positivo tal que para todo $J \subset \{1, \ldots, n\}$ con $\#J = d-1$ existe $D \subset I^\perp$ con $\#D = d-1$ tal que $\det(D, J) \neq 0$. Entonces la distancia mínima de $\mathcal{C}$ es d.*

Además, las dos formas de calcular la distancia mínima anteriores son equivalentes.

DEMOSTRACIÓN.

(a) Por la proposición 1.3, se tiene que la distancia mínima de un código lineal es d si para cualesquiera $n-d+1$ columnas de una matriz generatriz existen k columnas que son linealmente independientes y existen $n-d$ columnas que no contienen a k columnas linealmente independientes. Una matriz generatriz de $\mathcal{C}$ es $M(I)$, por lo que la distancia mínima de $\mathcal{C}$ es el mayor entero positivo d tal que cualesquiera $n-d+1$ columnas de $M(I)$ contienen k columnas que son linealmente independientes, que es equivalente al resultado.

(b) Por la proposición 1.3, se tiene que la distancia mínima de un código lineal es d si $d-1$ columnas cualesquiera de una matriz de control son linealmente independientes y existen d columnas que son linealmente dependientes. Una matriz de control de $\mathcal{C}$ es $M(I^\perp)$, por lo que la distancia mínima de $\mathcal{C}$ es el mayor entero positivo d tal que $d-1$ columnas de $M(I^\perp)$ cualesquiera sean linealmente independientes, que es equivalente a que haya un menor de tamaño $d-1$ con determinante distinto de cero $M(I^\perp, J)$ para todo $J \subset \{1, \ldots, n\}$, $\#J = d-1$, por lo que se tiene el resultado.

La equivalencia entre los dos resultados anteriores es clara porque ambos calculan la distancia mínima del código lineal $\mathcal{C}$, pero además ambas formas de calcular la distancia mínima son duales. Para probarlo usaremos la geometría de Plücker.

Sea M la matriz que tiene por filas la base $\{x_1, \ldots, x_n\}$ de $\mathbb{F}_q^n$, es decir la matriz de paso de la base canónica $\{e_1, \ldots, e_n\}$ a $\{x_1, \ldots, x_n\}$, $N = \{1, \ldots, n\}$ y M^* la matriz de paso del dual de la base canónica $\{e_1^*, \ldots, e_n^*\}$ a $\{x_1^*, \ldots, x_n^*\}$. Por tanto, $x_1 \wedge \cdots \wedge x_k = \sum_{j_i \in N} \det(M(I, K)) e_{j_1} \wedge \cdots \wedge e_{j_k}$, donde $K = j_1, \ldots, j_k$. Además, como $MM^t = J_{r,s,t}$, se tiene que $M^* = J_{r,s,t} M$.

Sea $\zeta(x_1 \wedge \cdots \wedge x_k) = x_{k+1}^* \wedge \cdots \wedge x_n^*$. Luego

$$\zeta(x_1 \wedge \cdots \wedge x_k) = \sum_{j_i \in N \setminus K} \det(M^*(N \setminus I, N \setminus K)) e_{j_1}^* \wedge \cdots \wedge e_{j_{n-k}}^*$$

pero como ζ es lineal también se tiene que $\zeta(x_1 \wedge \cdots \wedge x_k) =$

$$\sum_{j_i \in K} \det(M(I, K)) \zeta(e_{j_1} \wedge \cdots \wedge e_{j_k}) = \sum_{j_i \in K} \det(M(I, K)) e_{j_1}^* \wedge \cdots \wedge e_{j_k}^*$$

Por lo que se tiene que $\det(M(I, K)) = \det(M^*(N \setminus I, N \setminus K)) = \det(J_{r,s,t} M(N \setminus I, N \setminus K)) = \det(M(I \setminus I', N \setminus K)) = \det(M(I^{\perp}, N \setminus K))$ □

En [45, Proposition 2.1], que extiende el resultado anterior, se usa la estructura de matriz de Vandermonde en varias variables de la matriz generatriz de un código tórico para calcular explícitamente la distancia de dos familias de códigos. Para un código lineal arbitrario no se tiene dicha estructura, pero la descomposición geométrica de un código puede dar lugar al cálculo explícito de ciertas familias. Esto será objeto de estudio posterior a la finalización de esta memoria.

7. Grupo Ortogonal y Códigos Lineales

En esta sección desarrollamos más aplicaciones de esta estructura geométrica de los códigos lineales, en particular su relación con el grupo ortogonal.

La descomposición geométrica de un código lineal dada por los teoremas 4.10 y 4.19 permite obtener una matriz generatriz y una matriz de control de un código lineal mediante subconjuntos de filas de una matriz que verifica que su producto por su transpuesta es igual a $J_{r,s,t}$ con (s, t) en $\{0, 1, 2, 3, 4\} \times \{0\} \cup \{0\} \times \{1\}$ y $2r = n - s - 2t$, siempre consideraremos r, s, t en este conjunto. Recíprocamente, todo subconjunto de filas de una matriz de este tipo puede ser considerado como una matriz generatriz de un código lineal. Por tanto, tenemos una descripción de los códigos lineales y sus duales en términos de una nueva familia de matrices. A continuación,

mostramos la relación entre esta nueva forma de definir los códigos lineales y el grupo ortogonal.

Para una forma bilineal $B : \mathbb{F}_q^n \to \mathbb{F}_q^n$ el **grupo ortogonal** es el grupo de aplicaciones lineales $L : \mathbb{F}_q^n \to \mathbb{F}_q^n$, que verifican $B(L(x), L(y)) = B(x, y)$ para todo $x, y \in \mathbb{F}_q^n$, junto con la operación composición de transformaciones lineales. El elemento neutro es la transformación lineal $L(x) = x$, para todo $x \in \mathbb{F}_q^n$.

Para la forma bilineal B con matriz asociada igual a la matriz identidad el grupo ortogonal se denota por $\mathcal{O}(n)$ y es isomorfo a las matrices cuadradas de tamaño n, $\mathcal{M}_{n\times n}$, cuyo producto por su transpuesta es igual a la matriz identidad. Es decir,

$$\mathcal{O}(n) = \{A \in \mathcal{M}_{n\times n} \mid AA^t = Id\}$$

La operación de grupo en $\mathcal{O}(n)$ es el producto de matrices y el elemento neutro es la matriz identidad Id.

Existe una correspondencia biyectiva entre las matrices del grupo ortogonal, $\mathcal{O}(n)$, y las matrices de $\mathcal{M}_{r,s,t} = \{M \in \mathcal{M}_{n\times n} \mid MM^t = J_{r,s,t}\}$. Dicha correspondencia biyectiva viene dada por una matriz cualquiera $T \in \mathcal{M}_{r,s,t}$, para cada $N \in \mathcal{O}(n)$ consideramos $\phi(N) = TN$, por lo que para cada $M \in \mathcal{M}_{r,s,t}$, $\phi^{-1}(M) = T^{-1}N$. Es claro que ϕ da una correspondencia biyectiva de conjuntos entre $\mathcal{O}(n)$ y $\mathcal{M}_{r,s,t}$ pero no es un isomorfismo de grupos debido a que el producto de dos matrices $M_1, M_2 \in \mathcal{M}_{r,s,t}$ no verifica $(M_1M_2)(M_1M_2)^t = J_{r,s,t}$.

Aunque no tengamos un isomorfismo de grupos entre $\mathcal{O}(n)$ y $\mathcal{M}_{r,s,t}$, podemos presentar el grupo ortogonal de forma que actúe sobre $\mathcal{M}_{r,s,t}$. Para r, s, t fijos consideramos el grupo formado por el conjunto de matrices $O \in \mathcal{M}_{n\times n}$ tales que $OJ_{r,s,t}O^t = J_{r,s,t}$, junto con la multiplicación de matrices, es decir $\mathcal{O}_{J_{r,s,t}} = \{O \in \mathcal{M}_{n\times n} \mid OJ_{r,s,t}O^t = J_{r,s,t}\}$.

PROPOSICIÓN 4.25. *Sea $J = J_{r,s,t}$ fija, entonces $\mathcal{O}_J$ es un grupo con la multiplicación de matrices, isomorfo al grupo ortogonal $\mathcal{O}(n)$.*

DEMOSTRACIÓN. Sean $O_1, O_2 \in \mathcal{O}_J$, entonces se tiene que

$$(O_1O_2)J(O_1O_2)^t = O_1O_2JO_2^tO_1^t = O_1JO_1^t = J$$

por lo que $\mathcal{O}_J$ es un grupo cuyo elemento neutro es la matriz identidad.

Como J y la matriz identidad Id son las matrices de la forma bilineal B en bases diferentes, existe una matriz T inversible tal que $TT^t = J$.

Para $O \in \mathcal{O}_J$ sea $\phi(O) = T^{-1}OT$. Veamos que $\phi(O) \in \mathcal{O}(n)$, $\phi(O)(\phi(O))^t = (T^{-1}OT)(T^tO^t(T^{-1})^t) = T^{-1}OJO^t(T^{-1})^t = T^{-1}J(T^{-1})^t$, que es igual a la matriz identidad.

Y la inversa de ϕ para $N \in \mathcal{O}(n)$, $\phi^{-1}(N) = TNT^{-1}$. Se verifica que $\phi^{-1}(N)J(\phi^{-1})^t = TNT^{-1}J(T^{-1})^tN^tT^t = TNT^t(T^{-1})^tN^tT^t = TNN^tT^t$,

que es igual a $TT^t = J$. Por lo que ϕ es claramente una aplicación biyectiva entre $\mathcal{O}_J$ y $\mathcal{O}(n)$.

Se tiene que ϕ además es isomorfismo de grupos ya que para $O_1, O_2 \in \mathcal{O}_J$, se tiene que $\phi(O_1)\phi(O_2) = T^{-1}O_1TT^{-1}O_2T = T^{-1}O_1O_2T = \phi(O_1O_2)$. □

Por tanto, se tiene que el grupo ortogonal tiene el mismo cardinal que $\mathcal{M}_{r,s,t}$ y además actúa sobre él, puesto que $MN \in \mathcal{M}_{r,s,t}$ y $OM \in \mathcal{M}_{r,s,t}$, con $N \in \mathcal{O}(n)$ y $O \in \mathcal{O}_{J_{r,s,t}}$. Es decir, el grupo ortogonal en las dos versiones isomorfas que hemos presentado actúa sobre el conjunto de matrices de $M \in \mathcal{M}_{r,s,t}$, $\mathcal{O}(n)$ por la derecha y $\mathcal{O}_{J_{r,s,t}}$ por la izquierda.

Este nuevo paradigma de los códigos lineales desarrollado en este capítulo, junto con la acción del grupo ortogonal, abre una nueva vía de estudio en la que se pueden utilizar resultados de teoría de grupos para resolver, o al menos en principio reformular, problemas clásicos de teoría de códigos, como por ejemplo la conjetura MDS o el teorema principal de la teoría de códigos [47].

Bibliografia

[1] E. Artin. *Algèbre Géométrique*. Cahiers Scientifiques. Paris Gauthier-Villars, Editeur, 1967.

[2] M.F. Atiyah and I.G. MacDonald. *Introduction to Commutative Algebra*, volume 16 of *Addison-Wesley Series in Mathematics*. 1969.

[3] A.I. Barvinok. Computing the volume, counting integral points, and exponential sums. *Discrete Comput. Geom.*, 10:123–141, 1993.

[4] M. Bras-Amorós and M. O'Sullivan. Duality for several families of evaluation codes. *ArXiv:cs.IT/0609159*, 2006.

[5] C. Chevalley. *The Algebraic Theory of Spinors and Clifford Algebras*. Collected Works of Claude Chevalley, Vol. 2. Springer-Verlag, 1996.

[6] D. Cox. What is a toric variety? In R. Krasauskas R. Goldman, editor, *Topics in Algebraic Geometry and Geometric Modeling*, volume 334. AMS Contemporary Mathematics, 2003.

[7] D. Cox, J. Little, and D. O'Shea. *Ideals, Varieties and Algorithms: an Introduction to Computational Algebraic Geometry and Commutative Algebra*. Undergraduate Texts in Mathematics. Springer-Verlag, 1992.

[8] V.I. Danilov. The geometry of toric varieties. *Russian Math. Surverys*, 33(2):97–154, 1978.

[9] J.A. De Loera. The many aspects of counting lattice points in polytopes. *Math. Semesterber*, 52(2):175–195, 2005.

[10] O. Debarre. *Higher-Dimensional Algebraic Geometry*. Universitext. Springer-Verlag, 2001.

[11] V. Díaz, C. Guevara, and M. Vath. Codes from n-dimensional polyhedra and n-dimensional cyclic codes. *Proceedings of SIMU summer institute*, 2001.

[12] L.E. Dickson. *Linear Groups. With an Exposition of the Galois Field Theory*. Dover Publications, 1958.

[13] J. Dieudonné. *La Géométrie des Groupes Classiques (Troisième édition)*. Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 5. Springer-Verlag, 1971.

[14] J. Dieudonné. *Sur les Groupes Classiques (Troisième édition)*. Publications de L'Institut de Mathématique de L'Université de Strasbourg. Hermann Paris, 1981.

[15] M. Eichler. *Quadratische Formen und orthogonale Gruppen (zweite Auflage)*, volume 63 of *Die Grundlehren der mathematischen Wissenschaften in Einzeldarstellungen*. Springer-Verlag, 1974.

[16] D. Eisenbud. *Commutative Algebra with a View Toward Algebraic Geometry*, volume 150 of *Graduate Texts in Math.* Springer-Verlag, 1994.

[17] D. Eisenbud and J. Harris. *The Geometry of Schemes*, volume 197 of *Graduate Texts in Math.* Springer-Verlag, 2000.

[18] G. Ewald. *Combinatorial Convexity and Algebraic Geometry*, volume 168 of *Graduate Texts in Math.* Springer-Verlag, 1996.

[19] W. Fulton. *Intersection Theory.* Ergebnisse der Mathematik und ihrer Grenzgebiete 3. Folge, Band 2. Springer-Verlag, 1984.

[20] W. Fulton. *Introduction to Intersection Theory in Algebraic Geometry*, volume 54 of *Conference Board of the Mathematical Sciences.* AMS, 1984.

[21] W. Fulton. *Introduction to Toric Varieties.* Annals of Mathematics Studies. Princeton University Press, 1993.

[22] O. Geil and T. Høholdt. On hyperbolic codes. In S. Boztaş and I.E. Shparlinski, editors, *AAECC-14, LNCS 2227*, pages 159–171. Springer-Verlag, 2001.

[23] I.M. Gelfand, M.M. Kapranov, and A.V. Zelevinsky. *Discriminants, Resultants and Multidimensional Determinants.* Mathematics: Theory & Applications. Birkhäuser, 1994.

[24] V.D. Goppa. Codes on algebraic curves. *Soviet. Math. Dokl*, 24 (1):170–172, 1981.

[25] G.-M. Greuel and G. Pfister. *A SINGULAR Introduction to Commutative Algebra.* Springer-Verlag, 2002.

[26] G.-M. Greuel, G. Pfister, and H. Schönemann. SINGULAR 3.0. A Computer Algebra System for Polynomial Computations, Centre for Computer Algebra, University of Kaiserslautern, 2005. `http://www.singular.uni-kl.de`.

[27] R.W. Hamming. Error detecting and error correcting codes. *Bell Syst. Tech. J.*, 29:147–160, 1950.

[28] J.P. Hansen. Toric surfaces and error-correcting codes. *Coding theory, cryptography and related areas (Guanajuato,1998)*, pages 132–142, 2000.

[29] J.P. Hansen. Toric varieties Hirzebruch surfaces and error-correcting codes. *Appl. Algebra Engrg. Comm. Comput.*, 13:289–300, 2002.

[30] J.P. Hansen. Toric surfaces and codes, techniques and examples. *DMF Preprint: DMF-2004-01-27*, 2004.

[31] S.H. Hansen. Error-correcting codes from higher-dimensional varieties. *Finite Fields Appl.*, 7:530–552, 2001.

[32] R. Hartshorne. *Algebraic Geometry*, volume 52 of *Graduate Texts in Math.* Springer-Verlag, 1977.

[33] T. Høholdt, J.H. van Lint, and R. Pellikaan. Algebraic geometry codes. In V. Pless, W.C. Huffman, and R.A. Brualdi, editors, *Handbook of Coding Theory*, volume 1, chapter 10. Elsevier, 1998.

[34] J.W.P. Hirschfeld. *Projective Geometry over Finite Fields, second edition.* Oxford Mathematical Monographs. Oxford University Press,

1998.

[35] W.C. Huffman. On the classification and enumeration of self-dual codes. *Finite Fields Appl.*, 11:451–490, 2005.

[36] W.C. Huffman and V. Pless. *Fundamentals of Error Correcting Codes*. Cambridge University Press, 2003.

[37] J.E. Humphreys. *Linear Algebraic Groups*, volume 21 of *Graduate Texts in Math.* Springer-Verlag, 1975.

[38] D. Joyner. Toric codes over finite fields. *Appl. Algebra Engrg. Comm. Comput.*, 15:63–79, 2004.

[39] J. Justesen and T. Høholdt. *A Course in Error Correcting Codes*. EMS Textbooks in Mathematics. European Mathematical Society, 2004.

[40] G. Kempf, F. Knudsen, D. Mumford, and B. Saint-Donat. *Toroidal Embeddings I*, volume 339 of *Lectures Notes in Mathematics*. Springer-Verlag, 1973.

[41] A.G. Khovanskii. Newton polyhedra, a new formula for mixed volume, product of roots of a system equations. *Fields Inst. Commun.*, 24:325–364, 1999.

[42] S.L. Kleiman. Toward a numerical theory of ampleness. *Ann. of Math. (2)*, 84(3):293–344, 1966.

[43] J.H. van Lint. *Introduction to Coding Theory. Third edition*, volume 86 of *Graduate Texts in Math.* Springer-Verlag, 1999.

[44] J. Little and H. Schenck. Toric surface codes and Minkowski sums. *To appear in SIAM J. Discrete Math.*, 2005.

[45] J. Little and R. Schwarz. On m-dimensional toric codes. *ArXiv:cs.IT/0506102*, 2005.

[46] W. Lütkebohmert. *Codierungstheorie. Algebraisch-geometrische Grundlagen und Algorithmen*. Vieweg studium-Aufbaukurs Mathematik. Vieweg Studium, 2003.

[47] F.J. Macwilliams and N.J.A. Sloane. *The Theory of Error-Correcting Codes*, volume 16 of *North-Holland mathematical library*. North-Holland, 1977.

[48] C. Munuera and J. Tena. *Codificación de la Información*. Secretariado de Publicaciones e Intercambio Científico, Univ. Valladolid, 1997.

[49] T. Oda. *Lectures on Torus Embedings and applications*. Published for the TATA institute of fundamental research, Bombay. Springer-Verlag, 1978.

[50] T. Oda. *Convex Bodies and Algebraic Geometry. An Introduction to the Theory of Toric Varieties*. Ergebnisse der Mathematik und ihrer Grenzgebiete, 3. Folge, Band 15. Springer-Verlag, 1984.

[51] V. Pless. On the uniqueness of the Golay codes. *J. Combin. Theory*, 5:215–228, 1968.

[52] V. Pless. A classification of self-orthogonal codes over GF(2). *Discrete Math.*, 3:209–246, 1972.

[53] V. Pless and N.J.A. Sloane. On the cassification and enumeration of self-dual codes. *J. Combin. Theory Ser. A*, 18:313–335, 1975.

[54] A. Poli and L.I. Huget. *Codes Correcteurs. Théorie et Appliacations*. Logique Mathématiques Informatique. Masson, 1989.

[55] D. Ruano. On the parameters of r-dimensional toric codes. *Accepted in Finite Fields Appl.*, 2005. ArXiv:math.AG/0512285.

[56] D. Ruano. Generalized toric codes. In J.M. Ucha-Enríquez F.J. Castro-Jiménez, editor, *Actas del Décimo encuentro de Álgebra Computacional y Aplicaciones, 7-9 septiembre*, pages 151–154, 2006.

[57] D. Ruano. On the structure of generalized toric codes. *ArXiv:cs.IT/0611010*, 2006.

[58] B. Segre. Le geometrie di Galois. *Ann. Mat. Pura Appl. Ser. 4a*, 48:1–96, 1959.

[59] J.-P. Serre. *Cours D'Arithmétique*. Le Mathématicien. Presses Universitaires de France, 1970.

[60] C.E. Shannon. A mathematical theory of communication. *Bell Syst. Tech. J.*, 27:379–423 and 623–656, 1948.

[61] B. Sturmfels. *Gröbner Bases and Convex Polytopes*, volume 8 of *AMS University Lecture Series*. American Mathematical Society, 1996.

[62] M.A. Tsfasman, S.G. Vlăduţ, and T. Zink. Modular curves, shimura curves and goppa codes, better than varshamov-gilbert bound. *Math. Nachr.*, 109:21–28, 1982.

[63] M.A. Tsfasman and S.G. Vlăduţ. *Algebraic Geometry Codes*, volume 58 of *Mathematics and its applications*. Kluwer Dordrecht, 1991.