Ingeniería y Ciencia
ISSN:1794-9165
ISSN-e: 2256-4314
ing. cienc., vol 8, nº16, pp. 239–255, julio-diciembre. 2012.
http://www.eafit.edu.co/ingciencia

Sobre la distancia mínima de códigos AG unipuntuales castillo

Wilson Olaya León[1] Claudia Granados Pinzón[2]

Recepción: 03-may-2012, Aceptación: 19-oct-2012
Disponible en línea: 30-nov-2012

MSC: 94.B27, 94.B65

Resumen

Presentamos una caracterización de la cota inferior d^* para la distancia mínima de códigos algebraico-geométricos unipuntuales sobre curvas castillo. Calculamos explícitamente esta cota en el caso de un semigrupo de Weierstrass generado por dos elementos consecutivos. En particular, obtenemos una caracterización más simple del valor exacto de la distancia mínima para códigos Hermitianos.

Palabras claves: Códigos correctores de errores, códigos AG, distancia mínima, códigos Hermitianos.

[1] Magíster en ciencias Matemáticas, wolaya@uis.edu.co, profesor escuela de Matemáticas, Universidad Industrial de Santander, Bucaramanga, Colombia.
[2] Magíster en ciencias Matemáticas, cigranad@uis.edu.co, profesora escuela de Matemáticas, Universidad Industrial de Santander, Bucaramanga, Colombia.

On the Minimum Distance of One-Point Castle AG Codes

Abstract
We present a characterization of the lower bound d^* for minimum distance of algebraic geometry one-point codes coming from castle curves. This article shows explicit calculations of this bound in the case of a Weierstrass semigroup generated by two consecutive elements. In particular, we obtain a simple characterization of the exact value of the minimum distance Hermitian codes.

Key words: Error-correcting codes, AG codes, minimum distance, Hermitian codes.

1 Introducción

La teoría de códigos correctores de errores tiene su génesis en el año 1948 con la publicación del artículo [15] Shannon C.E., *A Mathematical Theory of Communication* en Bell Systems Technical Journal. Inicialmente, como sucede en los trabajos de Shannon, la teoría es esencialmente probabilística y los resultados obtenidos solamente demuestran la existencia de "buenos" códigos sin mostrar cómo podrían ser construidos. La necesidad de construir estos códigos explícitamente hizo que años más tarde el álgebra y la teoría de números hicieran importantes aportes a esta teoría, con los trabajos de R. Hamming, M. Golay y otros.

La finalidad de un código corrector de errores es preservar la calidad de la información que es transmitida a través de un canal con ruido. Por lo tanto, su objetivo es detectar y corregir la mayor cantidad posible de errores que puedan ocurrir durante dicha transmisión. La idea básica para conseguir esto es la de codificar los datos del mensaje agregando una cantidad extra de símbolos (redundancia) de un modo estructurado. De esta manera, el receptor tiene la posibilidad de determinar si han ocurrido errores durante la transmisión y recobrar con suficiente certeza el mensaje original.

El propósito de la teoría de códigos correctores consiste en crear códigos con alguna estructura matemática que permita corregir el máximo número posible de errores, añadiendo la menor cantidad de redundancia (es decir,

códigos confiables y eficientes). Aunque en la práctica existen restricciones, se conocen como "buenos" códigos aquellos que mantienen un equilibrio entre estos dos aspectos.

En este sentido, la primera alternativa es considerar la 'información' como una larga secuencia de símbolos de un cuerpo finito $\mathbb{F}_q$ (alfabeto). La forma más usada que se conoce como codificación por bloques consiste en dividir la información en bloques de k símbolos (símbolos de información) y el proceso de codificación se realiza agregando la redundancia que convierten el bloque inicial de k símbolos en un bloque de n símbolos (palabra), $n \geq k$. De esta manera, al receptor llega una n-tupla y este, conociendo la técnica con la que se ha codificado, puede verificar si han ocurrido cambios en la transmisión e incluso decidir, con bastante confiabilidad, cuál fue la n-tupla enviada. Esto último, se hace utilizando el mismo principio que cuando se corrigen errores en la digitalización de un texto (es decir, suponiendo que el error cometido es pequeño). Posteriormente, realizando el proceso contrario a la codificación, que se conoce como decodificación, se pueden recobrar los primeros k símbolos de información (si la decodificación se realiza bajo el supuesto mencionado anteriormente se conoce como *decodificación de máxima verosimilitud* o por vecino próximo), ver [11].

Más aún, se puede exigir que las palabras del código formen un subespacio lineal de $\mathbb{F}_q^n$. Estos códigos (lineales) han jugado un papel importante en el desarrollo de las telecomunicaciones y de la informática. Algunas aplicaciones de gran importancia son: la transmisión de datos desde el espacio (satélites de comunicaciones, sondas espaciales de la NASA), cintas magnéticas para computadores, sistemas digitales de audio y video (CD y DVD), redes ADSL, telefonía móvil, entre otras. En la actualidad los códigos detectores-correctores de errores se usan en prácticamente todos los dispositivos de tratamiento de información.

En 1977, utilizando conceptos de geometría algebraica, Goppa introdujo una nueva forma de construir códigos lineales. Más exactamente, a partir de una curva algebraica, no singular, absolutamente irreducible, de género $g \geq 0$, definida sobre el cuerpo finito $\mathbb{F}_q$, ver [5] y [12]. Estos códigos se conocen como códigos algebraico-geométricos (AG) o códigos geométricos de Goppa. El punto clave en las construcción de Goppa radica en que se puede obtener información acerca de los parámetros de un código (longitud, dimensión y distancia mínima) en términos de información aritmética y geométrica de la

curva sobre la cual se ha construido (número de puntos racionales, género). El método de Goppa puede verse como una generalización de la construcción de códigos Reed-Solomon.

Dada una curva algebraica $\mathcal{X}$ de género $g \geq 0$ definida sobre un cuerpo finito $\mathbb{F}_q$ con $q = p^t$ elementos, p primo. Consideremos n puntos $\mathbb{F}_q$-racionales distintos $P_1, P_2, ..., P_n$. Sean $D = P_1 + P_2 + ... + P_n$ y G otro divisor racional sobre $\mathcal{X}$ con $\text{sop}(G) \cap \text{sop}(D) = \emptyset$. El código AG asociado a la terna $(\mathcal{X}, D, G)$ está definido como la imagen del espacio Riemann-Roch $\mathcal{L}(G)$ por la función evaluación en D, $ev_D : \mathcal{L}(G) \to \mathbb{F}_q^n$, $ev_D(f) = (f(P_1), f(P_2), ..., f(P_n)$. Fijados n y g, los parámetros del código $\text{C} := \text{C}(\mathcal{X}, D, G)$ solo dependen del grado del divisor G. Esto es, si $2g - 2 < \text{grad}(G) < n$, entonces C tiene longitud n, dimensión $k = \text{grad}(G) - g + 1$ y distancia mínima $d \geq n - \text{grad}(G)$, ver [16]. La elección más lógica y simple y la que mejores resultados da habitualmente, es tomar $G = mQ$ con Q un punto $\mathbb{F}_q$-racional tal que $Q \notin \text{sop}(D)$. El código $\text{C}_m := \text{C}(\mathcal{X}, D, mQ)$ se llama unipuntual (one-point). Cuando $G = mQ$ el espacio $\mathcal{L}(G)$ está íntimamente relacionado con el semigrupo de Weierstrass en Q, $H(Q) = \{-\nu_Q(f) : f \in \mathcal{L}(\infty Q)\}$ donde ν_Q es la valoración en Q.

En el año 1982, M.A. Tsfasman, S.G. Vlâdut y Th. Zink [17] utilizaron códigos AG para construir explícitamente una familia de buenos códigos cuyos parámetros asintóticos sobrepasan la cota asintótica de Gilbert-Varshamov, esta es una medida clásica para evaluar el comportamiento asintótico de una familia de códigos. En consecuencia, se obtiene un camino para dar solución al problema fundamental de la teoría de códigos que fue considerado por Shannon en términos probabilísticos, como hemos dicho, pero sin dar ninguna idea constructiva de tales familias.

En general la teoría de códigos AG sobre curvas es complicada, ya que está basada en profundos resultados de curvas algebraicas. Esto hace que en la práctica sea difícil calcular los parámetros fundamentales del código, pues están relacionados con las propiedades aritméticas y geométricas de la curva. En este sentido, los problemas de los códigos AG producen una interesante motivación en la teoría de curvas algebraicas sobre cuerpos finitos, que se traduce en obtener "buenas" curvas. Desde el punto de vista de la teoría de códigos, una buena curva debe poseer un razonable manejo (a la hora de construir los códigos y calcular sus parámetros y propiedades), así como tener muchos puntos racionales con respecto a su género. En este sentido, existe una cota que relaciona el número de puntos racionales de una curva y el semigru-

po de Weierstrass en uno de ellos, llamada la cota Lewittes-Geil-Matsumoto, $\#\mathcal{X}(\mathbb{F}_q) \leq q\rho_2 + 1$, donde ρ_2 es la multiplicidad del semigrupo, ver [4] y [10]. Las curvas que alcanzan la igualdad en dicha cota cumplen con los requisitos exigidos. Estas se conocen como curvas castillo (llamadas así por Munuera et al. [14]) y los códigos obtenidos tienen excelentes parámetros y pueden ser estudiados de manera unificada sin importar la curva.

En [3], Geil et al. consideraron el conjunto $H^* = H^*(D, G) = \{m \in \mathbb{N}_0 : \mathrm{C}_m \neq \mathrm{C}_{m-1}\}$ que establece la dimensión de todos los códigos unipuntuales C_m y permite dar una nueva cota inferior para la distancia mínima de dichos códigos, conocida como la cota d^*.

En este trabajo presentamos una caracterización de la cota inferior d^* para la distancia mínima de códigos unipuntuales sobre curvas castillo. En el caso de un semigrupo de Weierstrass generado por dos elementos consecutivos, el valor de dicha cota es calculado explícitamente. Finalmente y utilizando los resultados obtenidos damos una caracterización más sencilla que las conocidas en la literatura, para el valor exacto de la distancia mínima de los códigos Hermitianos.

2 Preliminares

2.1 Códigos AG unipuntuales sobre curvas castillo

Curvas castillo y códigos AG sobre curvas castillo fueron estudiados en [14] por Munuera et al.

Para definir las curvas castillo se utiliza la cota sobre el número de puntos racionales dada por Lewittes y mejorada recientemente por Geil y Matsumoto, que relaciona el semigrupo de Weierstrass sobre un punto racional. Las curvas que alcanzan la igualdad en esta cota combinan las propiedades de tener un razonable manejo y dar códigos unipuntuales con excelentes parámetros, es decir, donde la dimensión y la distancia mínima son grandes simultáneamente con respecto a su longitud. Muchas de las curvas bien conocidas son castillo, estas incluyen las variedades de Deligne-Lusztig de dimensión 1 (racional, Hermitiana, Suzuki y Ree) ver [6],[7] y [8], Hermitiana generalizada [1], norma-traza [2] y muchas otras.

Por una *curva punteada* $(\mathcal{X}, Q)$ sobre $\mathbb{F}_q$ entiéndase una curva algebraica

$\mathcal{X}$ no singular, absolutamente irreducible, de género $g \geq 0$, definida sobre el cuerpo finito $\mathbb{F}_q$, con un punto racional Q. Denotaremos por $H := H(Q)$ el semigrupo de Weierstrass en Q. Es decir,

$$H(Q) = \{-\nu_Q(f) : f \in \bigcup_{m=0}^{\infty} \mathcal{L}(mQ)\} = \{0 = \rho_1 < \rho_2 < ... < \rho_i < \rho_{i+1} < ...\}.$$

El número ρ_2 es usualmente llamado *multiplicidad* en Q (o multiplicidad de H). Los elementos de H son llamados *números polares*. Los números naturales que no están en H se llaman *lagunas* de H. Denotaremos por c el *conductor* de H, este es el mayor elemento de H tal que $\mathrm{c} - 1 \notin H$. Si $\mathrm{c} = 2g$, H es *simétrico*, en el sentido que $\rho \in H$ si y solo si $\mathrm{c} - 1 - \rho \notin H$.

El siguiente teorema, debido a Geil y Matsumoto [4, Teorema 1] da una cota superior sobre el número de puntos racionales, $\mathcal{X}(\mathbb{F}_q)$, de la curva $\mathcal{X}$. Este generaliza un resultado previo de Lewittes [10, Teorema 1].

Teorema 2.1 (Cota Lewittes-Geil-Matsumoto)**.** *Supongamos que* $(\mathcal{X}, Q)$ *es una curva punteada, entonces*

$$\#\mathcal{X}(\mathbb{F}_q) - 1 \leq \#(H \setminus (qH^* + H)) \leq q\rho_2,$$

donde H *es el semigrupo de Weierstrass en* Q*,* ρ_2 *su multiplicidad y* $qH^* + H = \{q\alpha + \beta : \alpha, \beta \in H, \alpha \neq 0\}$.

Definición 2.2 (Curva castillo)**.** *Una curva punteada* $(\mathcal{X}, Q)$ *sobre* $\mathbb{F}_q$ *es una* curva castillo *si* H *es simétrico y se tiene la igualdad en la cota Lewittes-Geil-Matsumoto, es decir,* $\#\mathcal{X}(\mathbb{F}_q) = q\rho_2 + 1$.

Sea $(\mathcal{X}, Q)$ una curva castillo de género $g \geq 0$ sobre $\mathbb{F}_q$ con $n + 1$ puntos $\mathbb{F}_q$-racionales. Sean $\mathcal{X}(\mathbb{F}_q) = \{Q, P_1, P_2, ..., P_n\}$, $D = P_1 + P_2 + ... + P_n$ y $G = mQ$. Consideremos la secuencia de códigos AG unipuntuales $(\mathrm{C}_m)_{m \geq 1}$, donde $\mathrm{C}_m := \mathrm{C}(\mathcal{X}, D, mQ)$. Los parámetros de los códigos C_m se pueden estudiar de manera unificada independiente de la curva $\mathcal{X}$, ver [14].

2.2 La cota d*.

Para la distancia mínima se conocen en la literatura algunas cotas inferiores. La más interesante es la *cota orden* (o cota Feng-Rao) cf.[9]. Esta cota da muy

buenos resultados, pero tiene la desventaja que solamente puede ser aplicada a los duales de códigos AG unipuntuales que en general no son unipuntuales. Más aún, en general se sabe que la distancia mínima del dual $\mathrm{C}^{\perp}$ no da información sobre la distancia mínima de C.

La cota d^* fue introducida en [3]. A diferencia de la cota orden, que sólo se aplica al dual de un código AG unipuntual, esta es aplicada directamente a códigos AG unipuntuales.

Sea $H^* = H^*(D,Q) := \{m \in \mathbb{N}_0 : \mathrm{C}_m \neq \mathrm{C}_{m-1}\}$. Es claro que H^* contiene n elementos, $H^* = \{m_1, m_2, ..., m_n\} \subset H$, $m_n \leq n + 2g - 1$ y $\dim(C_{m_i}) = i$. Más aún, para $m < n$ se tiene que $m \in H^*$ si y solo si $m \in H$. Para códigos AG sobre curvas castillo se tiene que

$$H^* = H \setminus (n + H) = (H \cap \{0, 1, 2, ..., n-1\}) \cup \{n + l_1, n + l_2, ..., n + l_g\},$$

donde l_i son las lagunas de H. Además, H^* es simétrico en el sentido que para cada entero m se tiene que $m \in H^*$ si y solo si $n + 2g - 1 - m \in H^*$.

Para $i = 1, 2, ..., n$ consideramos los conjuntos

$$\Lambda_i^* = \{m \in H^* : m - m_i \in H\} = (m_i + H) \cap H^*.$$

Definición 2.3 (la cota d*)**.** *La cota d^* para códigos AG unipuntuales es el valor*

$$d^*(i) = \min\{\#\Lambda_t^* : t \leq i\}.$$

En [3] se prueba que el valor $d^*(i)$ es una cota inferior para la distancia mínima de un código AG unipuntual, es decir, $d(\mathrm{C}_{m_i}) \geq d_i^*$.

3 Caracterización de la cota d^*.

En lo que sigue $(\mathcal{X}, Q)$ es una curva castillo de género $g \geq 0$ sobre el cuerpo finito $\mathbb{F}_q$ con $n + 1$ puntos $\mathbb{F}_q$-racionales. Sean $\mathcal{X}(\mathbb{F}_q) = \{Q, P_1, P_2, ..., P_n\}$, $D = P_1 + P_2 + ... + P_n$ y $G = m_i Q$. Para $m_i \in H^*$ consideremos los códigos AG unipuntuales C_{m_i}. Denotamos por l_i para $i = 1, 2, ..., g$ las lagunas de H.

Consideremos los conjuntos

$$D_i := \{(m_j, l_k) : m_j - l_k = n - m_i, 1 \leq j, k \leq g\}$$

y

$$\widetilde{D}_i := \{(l_k, m_j) : l_k - m_j = l_{i-n+g}, 1 \leq j, k \leq g\}.$$

Proposición 3.1.

1. *Simetría de D_i: $(m_j, l_k) \in D_i$ si y solo si $(2g-1-l_k, 2g-1-m_j) \in D_i$.*
2. *Simetría de $\widetilde{D}_i$: $(l_k, m_j) \in \widetilde{D}_i$ si y solo si $(2g-1-m_j, 2g-1-l_k) \in \widetilde{D}_i$.*
3. *Para $0 < n - m_i < c$. Si $n - m_i$ es impar (resp. par), entonces $\#D_i$ es impar (resp. par).*
4. *$\#D_{n-3g+2} = \#D_{n-3g+3} = 0$.*
5. *$(l_{i-n+g}, 0) \in \widetilde{D}_i$. Por simetría $(l_g, l_g - l_{i-n+g}) \in \widetilde{D}_i$. En consecuencia $\#\widetilde{D}_i \geq 2$ excepto para $i = n$, en este caso $\#\widetilde{D}_n = 1$.*

Demostración. 1. $(2g-1-l_k) - (2g-1-m_j) = m_j - l_k = n - m_i$.

2. $(2g-1-m_j) - (2g-1-l_k) = l_k - m_j = l_{i-n+g}$.
3. Por la simetría de D_i, basta con encontrar los elementos de D_i en el intervalo $\left[0, \alpha := \frac{2g-1-m_t}{2}\right]$. Si m_t es impar (resp. par), entonces $(m_t + \alpha, \alpha) \in D_i$ (resp. $(m_t + \alpha, \alpha) \notin D_i$). En efecto, α es una laguna, pues de lo contrario $2\alpha = 2g-1-m_t$ sería un número polar lo cual contradice la simetría de H. Por otro lado, $m_t + \alpha$ es un número polar pues $m_t + \alpha = 2g - 1 - \alpha$.
4. Para $i = n-3g+2$ se tiene que $n - m_i = 2g-1 = l_g$ y si $i = n-3g+3$, $n - m_i = 2g - 2 = m_g$.
5. $l_g - l_{i-n+g} \in H$, pues $l_g = 2g - 1$.

□

Sea ω_i la cantidad de números polares menores que $n - m_i$.

Teorema 3.2. *Con la notación anterior se tiene que*

$$\#\Lambda_i^* = \begin{cases} n - m_i & si \quad i \leq n - c - g + 1 \\ 2\omega_i + \#D_i & si \quad n - c - g + 1 < i \leq n - g \\ \#\widetilde{D}_i & si \quad i > n - g \end{cases}$$

Demostración. Si $i \leq n-c-g+1$, entonces $m_i+c \leq n$, luego $\Lambda_i^* = (m_i+H)\cap H^* = ((m_i+H)\cap(H\setminus n+\mathbb{N})\cup\{n+l_1,...,n+l_g\}$ y $\#((m_i+H)\cap(H\setminus n+\mathbb{N}) = n-m_i-g$.

Si $n-c-g+1 < i \leq n-g$, entonces $n-c < m_i < n$. Sean $X := \{x \in (m_i+H)\cap H^* : x \leq n-1\}$, $Y := \{y \in (m_i+H)\cap H^* : n < y < m_i+2g\}$ y $Z := \{z \in (m_i+H)\cap H^* : z \geq m_i+2g\}$. Por lo tanto, $\Lambda_i^* = X \cup Y \cup Z$. Note que $\#X = \omega_i$, pues $x \in X$ si y solo si $x = m_i+\rho < n$ para algún $\rho \in H$ i.e. $\rho < n-m_i$. Por simetría $\#Z = \omega_i$ puesto que $z \in Z$ si y solo si $z = n+l > m_i+c-1$ i.e. $c-1-l < n-m_i$. Finalmente $\#Y = \#D_i$ pues $y \in Y \Leftrightarrow y = m_i+m_j = n+l_k \Leftrightarrow (m_j,l_k) \in D_i$. En consecuencia, $\#\Lambda_i^* = 2\omega_i + \#D_i$.

Por último, si $i > n-g$, entonces $m_i > n$ así $m_i = n+l_{i-n+g}$. Como los elementos de $(m_i+H)\cap H^*$ son aquellos tales que $m_i+m_j = n+l_k$ esto es los pares $l_k - m_j = l_{i-n+g}$, entonces $\#\Lambda_i^* = \#\widetilde{D}_i$. □

Corolario 3.3. *Si $i \leq n-c-g+1$, entonces*

$$d_i^* = n-m_i = d_G(\mathrm{C}_{m_i})$$

donde $d_G(\mathrm{C}_{m_i})$ es la cota de Goppa.

En la siguiente sección estudiamos el caso del semigrupo de Weierstrass generado por dos elementos consecutivos. Este, entre otros, es el caso del semigrupo de Weierstrass en el punto infinito de la curva Hermitiana, la cual es una curva maximal, pues alcanza la igualdad del número de puntos racionales en la cota Hasse-Weil, ver [16].

4 Computación de d^*.

En lo que sigue suponemos que H es el semigrupo generado por dos elementos consecutivos, $H = \langle a, a+1\rangle$. Se sabe que el género es $g = \frac{a(a-1)}{2}$ y el conductor es $c = a(a-1)$. Denotamos por m_i los números polares de H y por l_i las lagunas.

Definición 4.1 (Oasis y Desiertos)**.** *Los oasis (resp. desiertos) de H son los conjuntos finitos maximales de números polares consecutivos (resp. lagunas consecutivas) de H.*

Note que cuando $H = \langle a, a+1\rangle$, existen $a-1$ oasis y $a-1$ desiertos. Más aún, se tiene una caracterización sencilla de estos conjuntos.

Observación 4.2. *Sea* $H = \langle a, a+1\rangle$.

1. *Los oasis de* H *son* $M_t = \{ta, ta+1, ..., ta+t\}$ *para* $t = 0, 1, ..., a-2$. *Además, si* $m_i \in M_t$, *entonces* $m_i = ta - \frac{t(t+1)}{2} - 1 + i$.

2. *Los desiertos de* H *son* $L_t = \{(t-1)a + t, (t-1)a + t + 1, ..., ta - 1\}$ *para* $t = 1, 2, ..., a-1$. *Además, si* $l_i \in L_t$, *entonces* $l_i = i + \frac{t(t+1)}{2} - 1$.

Existe otra caracterización de los elementos de cada oasis y desierto, esta es debida a que todo entero z tiene representación única $z = xa + y(a+1)$. Luego toda laguna $l \equiv (x, y)$, si tiene representación única $l = xa + y(a+1)$ donde $0 \leq y < a$ y $x < 0$, y todo número polar $m \equiv (x, y)$, si tiene representación única $m = xa + y(a+1)$ donde $0 \leq y < a$ y $x \geq 0$.

Proposición 4.3. *Sea* $H = \langle a, a+1\rangle$.

1. *Si* $m_i \in M_t$, *entonces* $m_i \equiv \left(\frac{(t+1)(t+2)}{2} - i, i - \frac{t(t+1)}{2} - 1\right)$.

2. *Si* $l_i \in L_t$, *entonces* $l_i \equiv \left((t-1)a - \frac{t(t-1)}{2} - i, i + \frac{t(t-1)}{2} - (a-1)(t-1)\right)$.

Demostración. 1. Note que si $m_i \equiv (x, y) \in M_t$, entonces $x + y = t$. Por otro lado, $m_i = ta - \frac{t(t+1)}{2} - 1 + i = (x+y)a + y$, luego $y = i - \frac{t(t+1)}{2} - 1$ y $x = \frac{(t+1)(t+2)}{2} - i$.

2. Note que si $l_i \equiv (x, y) \in L_t$, entonces $x + y = t - 1$. Como $l_i = i + \frac{t(t+1)}{2} - 1 = (x+y)a + y$, entonces $y = i + \frac{t(t-1)}{2} - (a-1)(t-1)$ y $x = (t-1)a - \frac{t(t-1)}{2} - i$.

□

Observación 4.4. *Utilizando la anterior representación se tiene que:*

1. *Los elementos del* t*-ésimo oasis* M_t *son*

$$ta = m_{\frac{t(t+1)}{2}+1} \quad \equiv \quad (t, 0)$$

$$\begin{aligned} ta+1 = m_{\frac{t(t+1)}{2}+2} &\equiv (t-1,1) \\ &\vdots \\ ta+t = m_{\frac{t(t+1)}{2}+(t+1)} &\equiv (0,t). \end{aligned}$$

2. Los elementos del t-ésimo desierto L_t son

$$\begin{aligned} (t-1)a+t = l_{(t-1)a-\frac{t(t-1)}{2}+1} &\equiv (-1,t) \\ (t-1)a+t+1 = l_{(t-1)a-\frac{t(t-1)}{2}+2} &\equiv (-2,t+1) \\ &\vdots \\ ta-1 = l_{ta-\frac{t(t+1)}{2}} &\equiv (-(a-t),a-1). \end{aligned}$$

4.1 Cálculo de D_i.

Primero supongamos que $n-m_i = m_s$ es un número polar. Note que $(m_j, l_k) \in D_i \Leftrightarrow m_j - l_k = m_s \Leftrightarrow m_j - m_s = l_k$. Si además $m_s \in M_t$ entonces en el mismo oasis hay $\frac{(t+1)(t+2)}{2} - s$ elementos m_j tal que $m_j - m_s$ es una laguna. En efecto, si $m_s \equiv (x,y)$ entonces todos los elementos $m_j > m_s$ en el oasis M_t satisfacen que $m_j - m_s$ es una laguna, pues si $m_j \equiv (x',y')$ entonces $x' < x$ y $y' > y$.

Ahora, en cada uno de los restantes $a-2-t$ oasis hay de dos tipos de elementos $m_j \equiv (x',y')$, aquellos donde $x' < x$ y los que $y' < y$. De cada uno hay $\frac{(t+1)(t+2)}{2} - s$ y $s - \frac{t(t+1)}{2} - 1$ elementos m_j tal que $m_j - m_s$ es una laguna. En consecuencia se tiene el siguiente resultado.

Lema 4.5. *Si $n - m_i = m_s$ es un número polar y $m_s \in M_t$, entonces*

$$\#D_i = ta - \frac{t(t+1)}{2} + 1 - s.$$

Corolario 4.6. *Si $n - m_i = m_s$ es un número polar y $m_s \in M_t$, entonces*

$$\#D_i = m_s - 2(s-1).$$

Demostración. $m_s = ta - \frac{t(t+1)}{2} - 1 + s$. □

Corolario 4.7. *Para $n-c-g+1 < i \leq n-g$. Si $n-m_i = m_s$ es un número polar, entonces*

$$\#\Lambda_i^* = n - m_i.$$

Demostración. Por el teorema 3.2, el teorema 4.6 y el hecho que $\omega_i = s-1$. □

Ahora, supongamos que $n - m_i = l_s$ es una laguna y que $l_s \in L_t$, entonces $(t-i)a+(t-1) < l_s < ta$. En el siguiente resultado probaremos que el cardinal de D_i, cuando $n - m_i = l_s$ es cualquier laguna en el desierto L_t, es mayor o igual que el cardinal de $D_{n-g+1-ta}$ para $n - m_i = ta$ (el primer número polar del oasis M_t).

Lema 4.8. *Sea $(m_j, l_k) \in D_{n-g+1-ta}$. Si $m_j \in M_\tau$, entonces existe al menos un par (x, y) con $0 \leq x \leq m_j - \tau a$ y $1 \leq y \leq (\tau - t + 1)a - 1 - l_k$ tal que para todo $1 \leq s \leq a - t$, $(m_j - x, l_k + y) \in D_{n-g+1-ta+s}$.*

Demostración. Para $1 \leq s \leq (\tau - t + 1)a - 1 - l_k$, tome $y = s$ y $x = 0$. Y para $(\tau - t + 1)a - 1 - l_k < s \leq a - t$, tome $y = (\tau - t + 1)a - 1 - l_k$ y $x = s - (\tau - t + 1)a + 1 + l_k$. □

Corolario 4.9. *Si $n - m_i = l_s$ es una laguna y $l_s \in L_t$, entonces*

$$\#D_i \geq \#D_{n-g+1-ta}.$$

Por lo anterior, se tiene probado el siguiente resultado.

Teorema 4.10. *Supongamos que H es el semigrupo de Weierstrass generado por dos elementos consecutivos. Si $i \leq n - g$, entonces*

$$d_i^* = \text{mín}\{m_t : m_t \geq n - m_i\}.$$

4.2 Cálculo de $\widetilde{D}_i$.

Sea $n - g + 1 \leq i \leq n$. Supongamos que $l_{i-n+g} \equiv (x, y) \in L_t$. Recuerde que $-a < x < 0$ y $x + y = t - 1$.

Note que si $l_{i-n+g} \in L_t$, entonces l_{i-n+g} es la única laguna de L_t que es primer elemento de una pareja de $\widetilde{D}_i$. Para los demás desiertos entre $t+1$ y $a-1$ (estos son $a-2-t$ desiertos) se tiene que $(l_k, l_k - l_{i-n+g}) \in \widetilde{D}_i$ con $l_k \equiv (x', y')$ si cumple que $x' \geq x$ y $y' \geq y$.

Considerando los conjuntos $A := \{l_k = (x', y') : l_k \geq l_{i-n+g}, x' \geq x\}$ y $B := \{l_k = (x', y') : l_k \geq l_{i-n+g}, y' < y\}$, se tiene que $\#\widetilde{D}_i = \#A - \#B$.

- Cálculo de $\#A$. Existen $x + (a-t)$ desiertos con $-x$ elementos que pertenecen a A. Para los demás $(a-1-t) - x - (a-t) = -x-1$ desiertos se tienen $(-x-1) + (-x-2) + ... + 1 = \frac{-x(-x-1)}{2}$ elementos que están en A. En consecuencia, $\#A = 1 + (-x)(x + (a-t) + \frac{-x(-x-1)}{2}$.
- Cálculo de $\#B$. Existen $y-t-1$ desiertos con $y-t-1$, $y-t-2$,...,1 elementos en B. En consecuencia $\#B = \frac{(y-t)(y-t-1)}{2}$.

Por lo tanto hemos probado el siguiente resultado.

Teorema 4.11. *Para $n-g+1 \leq i \leq n$. Si $l_{i-n+g} \equiv (x, y) \in L_t$, entonces*

$$\#\widetilde{D}_i = -x(x + a - t + 1).$$

Corolario 4.12. *Para cada $1 \leq t < a-1$*

$$\#\widetilde{D}_{n-g+(t-1)a-\frac{t(t-1)}{2}+1} = \#\widetilde{D}_{n-g+ta-\frac{t(t-1)}{2}} = a - t$$

Demostración. $m_{n-g+(t-1)a-\frac{t(t-1)}{2}+1} - n = l_{(t-1)a-\frac{t(t-1)}{2}+1} = (t-1)a + t \equiv (-1, t)$ y $m_{n-g+ta-\frac{t(t-1)}{2}} - n = l_{ta-\frac{t(t-1)}{2}} = ta - 1 \equiv (t-a, a-1)$. □

Note que el Corolario 4.12 muestra la igualdad en el cardinal de $\widetilde{D}_i$ cuando $m_i - n$ es el primer y último elemento de cada desierto L_t, para todo $t = 1, 2..., a-1$. Ahora veamos que cuando $m_i - n$ es un elemento intermedio en el desierto L_t se tiene que el cardinal de $\widetilde{D}_i$ es mayor o igual al de los extremos del desierto.

Lema 4.13. *Para cada $1 \leq t < a-1$. Si $l_{(t-1)a-\frac{t(t-1)}{2}+1} < m_i - n < l_{ta-\frac{t(t-1)}{2}}$, entonces*

$$\#\widetilde{D}_i \geq a - t.$$

Demostración. Como $m_i - n \equiv (x, y)$ es una laguna intermedia en el desierto L_t, entonces $x = -1 - k$ para algún $1 \leq k \leq a - t - 2$. Así, por el Teorema 4.11, $\#\widetilde{D}_i = a - t + k(a - t - k - 1)$ y puesto que $a - t - 1 - k > 0$ se tiene el resultado. □

Como consecuencia de los anteriores resultados hemos probado el siguiente teorema.

Teorema 4.14. *Para $i > n - g$. Si $m_i - n \in L_t$, entonces $d_i^* = a - t$.*

5 Códigos unipuntuales Hermitianos

Consideremos la curva Hermitiana $\mathcal{H} : y^q + y = x^{q+1}$ de género $g = \frac{q(q-1)}{2}$ sobre $\mathbb{F}_{q^2}$. Esta tiene $q^3 + 1$ puntos racionales y semigrupo de Weierstrass en el punto infinito $H = H(P_\infty) = \langle q, q + 1\rangle$. Claramente esta es una curva castillo.

Los códigos unipuntuales sobre la curva Hermitiana han sido estudiados por varios autores. En particular la distancia mínima de códigos unipuntuales Hermitianos fue establecida por Yang y Kumar en [18]. Nosotros utilizando los resultados de la sección anterior obtenemos una caracterización más práctica para determinar la distancia mínima de estos códigos.

Para cada $m_i \in H^*$ consideremos el código $\mathrm{C}_{m_i} := \mathrm{C}(\mathcal{H}, D, m_i P_\infty)$ donde D es la suma de todos los q^3 puntos $\mathbb{F}_q$-racionales de $\mathcal{H}$ diferentes de P_∞. Claramente la longitud de C_{m_i} es $n = q^3$ y la dimensión es $k_{m_i} = i$.

Para la distancia mínima $d_{m_i} := d(\mathrm{C}_{m_i})$ sabemos que $d_{m_i} \geq d_i^*$. Así, por el Teorema 4.10, $d_{m_i} \geq \min\{m_t : m_t \geq n - m_i\}$ para $i \leq n - g$ y por el Teorema 4.14, $d_{m_i} \geq q - t$ para $n - g < i \leq n$, donde $m_i = n + l_{i-n+g}$ y $l_{i-n+g} \in L_t$, es decir l_{i-n+g} es una laguna en el t-ésimo desierto.

Nosotros referimos a la literatura para observar que en este caso la cota d_i^* coincide con el valor exacto de la distancia mínima d_{m_i} de los códigos C_{m_i}. La nueva caracterización de los valores de la distancia mínima d_{m_i} para códigos Hermitianos son resumidos en la siguiente tabla.

i	d_{m_i}	condición
$i \leq n-g$	$n-m_i$	si $n-m_i \in H$
	qt	si $n-m_i \in L_t$
$n-g < i \leq n$	$q-t$	$m_i - n \in L_t$

Note que esta caracterización del valor exacto de la distancia mínima de códigos Hermitianos es más simple que las conocidas en la literatura (ver [18] y [9]) y resalta el hecho de que la distancia mínima sólo difiere de la cota Goppa cuando $m_i = n - l_w$ para toda laguna l_w. Observe también que se puede construir un [64,53,8]-código sobre $\mathbb{F}_{16}$ que es un nuevo récord, según las tablas MinT [13].

6 Conclusión

Los códigos AG unipuntuales castillo contienen algunos de los más importantes códigos algebraico-geométricos estudiados en la literatura hasta la fecha. La distancia mínima de estos códigos puede ser acotada aplicando la llamada cota d^*. Esta es una cota inferior para la distancia mínima que a diferencia de la cota orden se aplica sobre el código AG primario. Nosotros caracterizamos la cota d^* para los códigos castillo en general y calculamos explícitamente esta cota en el caso particular de un semigrupo de Weierstrass generado por dos elementos consecutivos. Finalmente, para ilustrar estos resultados, estudiamos los códigos Hermitianos, obteniendo una caracterización más sencilla para su distancia mínima que las conocidas actualmente.

7 Agradecimientos

Los autores expresan su agradecimiento a los árbitros de la revista por sus valiosos aportes y sugerencias.

Referencias

[1] A. Garcia, H. Stichtenoth, "A Class of Polynomials over Finite Fields", *Finite Fields and Their Applications*, vol. 5, n.o 4, pp. 424-435, oct. 1999. Referenciado en 243

[2] O. Geil, "On codes from norm-trace curves", *Finite Fields and Their Applications*, vol. 9, n.o 3, pp. 351-371, jul. 2003. Referenciado en 243

[3] F. Torres, D. Ruano, C. Munuera, O. Geil, "On the order bounds for one-point AG codes", *Advances in Mathematics of Communications*, vol. 5, n.o 3, pp. 489-504, ago. 2011. Referenciado en 243, 245

[4] O. Geil, R. Matsumoto, "Bounding the number of -rational places in algebraic function fields using Weierstrass semigroups", *Journal of Pure and Applied Algebra*, vol. 213, n.o 6, pp. 1152-1156, jun. 2009. Referenciado en 243, 244

[5] V. Goppa, "Codes on algebraic curves", *Sov. Math.-Dokl.*, vol. 24, pp. 170-172, 1981. Referenciado en 241

[6] J. Hansen, "Deligne-Lusztig varieties and group codes", in *Coding Theory and Algebraic Geometry*, vol. 1518, H. Stichtenoth y M. Tsfasman, Eds. Springer Berlin / Heidelberg, 1992, pp. 63-81. Referenciado en 243

[7] J. Pedersen, J. Hansen, "Automorphism groups of Ree type Deligne-Lusztig curves and function fields.", *J. reine angew. Math.* , n.o 440, pp. 99-109, 1993. Referenciado en 243

[8] J. Hansen, H. Stichtenoth, "Group codes on certain algebraic curves with many rational points", *Applicable Algebra in Engineering, Communication and Computing*, vol. 1, n.o 1, pp. 67-77, 1990. Referenciado en 243

[9] T. Høholdt, J. van Lint, R. Pellikaan, "Algebraic-geometry codes", in *Handbook of Coding Theory, Volume 1: Part 1: Algebraic Coding*, V. Pless y W. . Huffman, Eds. Amsterdam: Elsevier, 1998, pp. 871-961. Referenciado en 244, 253

[10] J. Lewittes, "Places of degree one in function fields over finite fields", *Journal of Pure and Applied Algebra*, vol. 69, n.o 2, pp. 177-183, dic. 1990. Referenciado en 243, 244

[11] J. van Lint, *Introduction to Coding Theory*, 2.a ed. Springer-Verlag, 1992. Referenciado en 241

[12] J. van Lint y G. V. D. Geer, *Introduction to coding theory and algebraic geometry.* Birkhauser Verlag, 1988. Referenciado en 241

[13] "MinT", *Online database for optimal parameters of (t, m, s)-nets, (t, s)-secuences, ortogonal arrays and linear codes.* [Online]. Available: http://mint.sbg.ac.at/. Referenciado en 253

[14] C. Munuera, A. Sepúlveda, F. Torres, "Algebraic Geometry Codes from Castle Curves", in *Coding Theory and Applications*, vol. 5228, Á. Barbero, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008, pp. 117-127. Referenciado en 243, 244

[15] C. Shannon, "A mathematical theory of communication", *Bell System Technical Journal*, vol. 27, pp. 656-715, 1948. Referenciado en 240

[16] H. Stichtenoth, *Algebraic Function Fields and Codes*. Springer-Verlag, 2009. Referenciado en 242, 247

[17] M. Tsfasman, S. Vlădutx, T. Zink, "Modular curves, Shimura curves, and Goppa codes, better than Varshamov-Gilbert bound", *Mathematische Nachrichten*, vol. 109, n.o 1, pp. 21-28, 1982. Referenciado en 242

[18] K. Yang, P. Kumar, "On the true minimum distance of Hermitian codes", in Coding *Theory and Algebraic Geometry*, vol. 1518, H. Stichtenoth y M. A. Tsfasman, Eds. Springer Berlin Heidelberg, pp. 99-107. Referenciado en 252, 253