SOBRE CURVAS ALGEBRAICAS Y CÓDIGOS CORRECTORES

CARLOS MUNUERA Y FERNANDO TORRES

Resumen. El estudio de las curvas ha atraído desde siempre la atención de los matemáticos. Posiblemente el episodio más reciente de esta historia lo constituye el caso de las curvas definidas sobre cuerpos finitos, que se ha desarrollado de manera espectacular en los últimos años, a raíz de sus interesantes aplicaciones en la la ingeniería y en la técnica. En este trabajo describimos la evolución y situción actual del estudio de las curvas algebraicas sobre cuerpos finitos en conexión con sus aplicaciones a la teoría de Códigos Correctores de Errores.

1. Introducción: Curvas Algebraicas

Los orígenes del estudio sistemático de las *curvas* se remontan a los trabajos de matemáticos de la antigua Grecia, y están ligados a los nombres de Pitágoras, Euclides o Diofanto. Estos y otros, se plantearon -y resolvieron- cuestiones sobre un buen número de curvas, muchas de las cuales caen en la categoría de lo que hoy conocemos como *curvas algebraicas*, como las cónicas, la cisoide de Diocles, la concoide de Nicomedes, etc. En particular, estas dos últimas fueron introducidas para estudiar problemas de naturaleza 'polinomial': la duplicación del cubo y la trisección del ángulo respectivamente. Por otro lado, los orígenes del estudio formal de los polinomios, podemos encontrarlos en los resultados de un libro del matématico árabe al-Khwärizmi, que fue escrito en el siglo IX. Como se sabe, del título del libro "Hisab al-jabr wa-al muqabala"[1], procede la palabra *álgebra* y del de su autor, la palabra *algoritmo*. Hagamos notar que las pruebas de varias propiedades 'polinomiales' estudiadas en ese texto, usaban implícitamente propiedades de la geometría de Euclides. No es, por tanto, sorprendente que existan profundas relaciones entre esta geometría y los polinomios. Sin embargo, estas relaciones no se establecieron de forma clara hasta el siglo XVII, con la introducción de las coordenadas en el plano real a raíz de los trabajos de Descartes y Fermat. Luego una curva (definición primaria) será el conjunto de puntos cuyas coordenadas anulan un polinomio.

Cuando el cuerpo base es $\mathbf{R}$ pueden ocurrir situaciones 'extrañas'; por ejemplo los ceros de un polinomio pueden no existir, o reducirse a un único punto, lo que va contra nuestra intución de lo que debería ser una curva. Este es el caso del polinomio $X^2+Y^2=0$. Puesto que la definición de curva como conjunto de ceros de un polinomio puede ser formulada sobre un cuerpo arbitrario $\mathbf{K}$, la forma en que estas dificultades fueron superadas consistió considerar la curva sobre el cuerpo de los números complejos, $\mathbf{K}=\mathbf{C}$. Esta primera generalización abrió la puerta a utilizar cuerpos cada vez más generales, y

Aparecerá en la Gaceta RSME.

[1] "Sobre las operaciones de restablecimiento y reducción". Curiosamente, el nombre *al-Khwärizmi* con que su autor ha pasado a la posteridad es en realidad un apodo, que podríamos traducir como *'el números'*. Su nombre real era Muhammad ibn Musa.

denomimar 'curvas' a objetos aparentemente muy alejados de los de la primitiva intuicion geometrica de los griegos.

En esta línea, sea $F = F(X, Y)$ un polinomio irreducible con coeficientes complejos (es decir, tal que no es posible escribir F como el producto de dos polinomios no constantes). Podemos preguntarnos por la existencia de soluciones en Y en de la ecuación $F = 0$ sobre el cuerpo $\mathbf{K}(X)$. Por ejemplo consideremos la ecuación $Y^2 - f(X) = 0$, siendo $f(X)$ un polinomio de grado impar, d, con raíces diferentes dos a dos. Esta ecuación no tiene solución en $\mathbf{K}(X)$ luego Y, visto como una función de X, no está definida como función clásica. Sin embargo, sí puede estarlo como una función d-valuada. Riemann (aproximadamente en 1850) construyó un espacio topológico compacto S con estructura compleja (llamado hoy *superficie de Riemann compacta*), donde Y puede definirse como función. En nuestro ejemplo, el género topológico de la correspondiente superficie es $(d-1)/2$. El cuerpo de funciones meromorfas de S es presisamente el cuerpo cociente, $\mathbf{K}(S)$, del anillo $\mathbf{K}[X, Y]/(F)$, donde $\mathbf{K}$ es algebraicamente cerrado en $\mathbf{K}(S)$, y este cuerpo tiene trascendencia uno sobre $\mathbf{K}$.

Alrededor de 1870, Brill y Noether mostraron que existen un entero $n \in \mathbf{N}$ y una aplicación biholomorfa $\pi : S \to \pi(S) \subseteq \mathbf{P}^n(\mathbf{K})$ (siendo $\mathbf{P}^n(\mathbf{K})$ el espacio proyectivo de dimensión n sobre $\mathbf{K}$), de manera que $\pi(S)$ es no-singular y queda descrito por los ceros comunes de un cierto conjunto de polinomios homogeneos en $(n+1)$ variables. Dado que el grado de trascendencia del cuerpo de funciones meromorfas de $\pi(S)$ es uno, es natural ver este objeto como una curva algebraica; por lo tanto S puede ser obtenida de una curva 'proyectiva, irreducible, no-singular' inmersa en algun especio proyectivo.

Un poco más tarde (aproximadamente en 1880), Dedenkind y Weber observaron que los dominios de valoración discreta de $\mathbf{K}(S)$ están en correspondencia biyectiva con los puntos de S. Esta observación les llevo a definir una curva (abstracta) como el conjunto de subíndices necesario para describir los dominios de valoración discreta de un cuerpo de funciones algebraicas dado, con grado de trascendencia uno sobre un cuerpo algebraicamente cerrado $\mathbf{K}$. Como en el caso de las superficies de Riemann compactas, se demuestra que esta curva abstracta se puede sumergir en un cierto espacio proyectivo, donde está descrita como el conjunto de soluciones comunes de un número finito de ecuaciones homogóneas. En consecuencia, son equivalentes

- el estudio de curvas proyectivas irreducibles no-singulares;
- el estudio de las superficies compactas de Riemann;
- el estudio de cuerpos con grado de trascendencia uno sobre $\mathbf{K}$ en los que $\mathbf{K}$ sea algebraicamente cerrado.

A pesar de todas estas generalizaciones, hasta tiempos bastante recientes el espacio ambiente 'natural' para el estudio de las curvas era el cuerpo de los números complejos, $\mathbf{C}$. Sin embargo, durante la segunda mitad del siglo XX han ido apareciendo aplicaciones técnicas de las curvas, principalmente relacionados con problemas de ingeniería electrónica digital (Códigos Correctores de Errores, Criptografía, Diseño y Análisis de Circuitos, etc.) que por su naturaleza precisan ambientes discretos. Por consiguiente, para estas aplicaciones, el cuerpo base $\mathbf{K}$ debe ser la clausura algebraica de un cuerpo finito $\mathbf{F}_q$. Si bien este caso ya habia sido considerado con anterioridad, no ha sido –como decimos– sino hasta la segunda mitad del pasado siglo cuando se le ha dedicado una atención especial.

En este artículo vamos a describir la evolución y situción actual del estudio de las curvas algebraicas sobre cuerpos finitos en conexión con sus aplicaciones a la teoría de Códigos Correctores de Errores.

Una descripción muy completa de la historia del estudio de las curvas (en general) puede encontrarse en [3],[9] y [50]. Las referencias básicas para el resto del trabajo son [1],[12],[13],[14],[26, Cap. IV],[30],[36],[45] y [46].

2. ... y Cuerpos Finitos

Los orígenes del estudio de los cuerpos finitos se remontan a los siglos XVII y XVIII. En efecto, ya antes de Galois (1811-1832), matemáticos como Fermat (1601-1665), Euler (1707-1783), Lagrange (1736-1813) o Gauss (1777-1855) habían trabajado con ecuaciones en congruencias módulo un número primo p. En particular, se debe principalmente a Fermat y Euler el estudio de la famosa ecuación $x^m \equiv 1 \pmod{p}$. A propósito de ella, el primero estableció lo que hoy conocemos como *Teorema Pequeño de Fermat*, a saber, si p no divide a x, entonces $x^{p-1} \equiv 1 \pmod{p}$. Por su parte, Euler fué capaz de calcular el número de soluciones de la ecuación general y ampliar el resultado de Fermat, probando que si $(m, x) = 1$, entonces $x^{\phi(m)} \equiv 1 \pmod{m}$, siendo ϕ el indicador de Euler (en notación moderna, $\phi(m) = \#(\mathbf{Z}/m\mathbf{Z})^*$). Estos resultados juegan hoy en día un papel importante en el estudio de los números primos y los test de primalidad; ver e.g. [29], [34].

No obstante, ninguno de estos matemáticos llegó a establecer de forma explícita el concepto de cuerpo finito. Si bien el estudio sistemático de las propiedades de estas estructuras comienza ya en los trabajos de Gauss, ese mérito corresponde a Galois, quien además fué capaz de construir cuerpos finitos con cardinal arbitrario (potencia de un primo), mediante sistemas de raíces de ecuaciones algebraicas. El hecho –casi trivial– de que sólo existen cuerpos finitos con estos cardinales no fué establecido sino hasta finales del XIX (casi un siglo despues de los trabajos de Galois) por Moore mediante su teorema de existencia y unicidad: *Para cada potencia $q := p^n$ de un primo p, existe, salvo isomorfismo, un único cuerpo $\mathbf{F}_q$ de orden q*. Así pues $\mathbf{F}_q$ es isomorfo al cuerpo de descomposición del polinomio $X^q - X \in \mathbf{Z}/p\mathbf{Z}$. Este resultado se complementa con el importante teorema de Wedderburn (de 1905): *todo anillo con división finito es commutativo.*

3. Puntos racionales de las Curvas sobre Cuerpos Finitos

Por supuesto, las curvas algebraicas pueden definirse y tratarse sobre un cuerpo finito de modo similar al de cualquier otro cuerpo (por ejemplo, el 'clásico' complejo). Claro está, que en este caso de cuerpos finitos, poseen peculiaridades propias. Así, una de las características más importantes de una curva definida sobre un cuerpo finito, es el número de puntos (racionales) que posee. Recordemos que dada $\mathcal{X}$ una curva algebraica, geométricamente irreducible, proyectiva y no singular, $\mathcal{X}$, definida sobre $\mathbf{F}_q$ (o simplemente, una 'curva' sobre $\mathbf{F}_q$), contenida en un espacio proyectivo $\mathbf{P} := \mathbf{P}^n(\bar{\mathbf{F}}_q)$, un punto de $\mathcal{X}$ es *racional* (sobre $\mathbf{F}_q$) si posee unas coordenadas $(x_0 : \ldots : x_n)$ tales que $x_0, \ldots, x_n \in \mathbf{F}_q$. La racionalidad de un punto $P \in \mathcal{X}(\bar{\mathbf{F}}_q)$ puede detectarse mediante el morfismo de Frobenius $\mathbf{\Phi}$ sobre $\mathbf{F}_q$, $\mathbf{\Phi}(x_0 : \ldots : x_n) = (x_0^q : \ldots : x_n^q)$, ya que los puntos racionales son precisamente los puntos fijos de $\mathbf{\Phi}$.

El estudio del cálculo número de puntos racionales de una curva no es nuevo para los matemáticos. Ya Gauss, en sus *Disquisitiones* de 1801, se ocupó de contar los puntos $\mathbf{F}_p$-racionales de la *curva de Fermat* $X^3 + Y^3 + Z^3 \equiv 0 \pmod{p}$, siendo p un primo impar, demostrando –por ejemplo– que si $p \not\equiv 1 \pmod{3}$, la curva tiene $p+1$ puntos $\mathbf{F}_p$-racionales (la solución general puede verse en [43, p. 111]).

Desde la época de Gauss hasta nuestros días, el problema de contar puntos ha sobrevivido de manera más o menos latente, aunque ciertamente nunca ha sido uno de los temas destacados de las matemáticas. Un poco más adelante bosquejaremos algunas de las líneas principales de esta historia. Ahora bien, en tiempos recientes esta cuestión ha resurgido con fuerza, hasta convertirse en un punto central dentro del estudio de las curvas. Las razones de este interés hay que buscarlas en sus aplicaciones prácticas que desbordan el marco puramente 'teórico' del estudio de las curvas.

Recordemos, por ejemplo, que la calidad de un sistema criptográfico construido a partir de una curva elíptica, depende de forma esencial de la estructura del grupo de puntos de la curva, lo que en definitiva está en función de la cantidad de puntos racionales que posee.[2] Otro ejemplo significativo es el de los Códigos Correctores de Errores construidos a partir de curvas. De forma análoga al caso anterior, la calidad de estos códigos depende del número de puntos racionales de la curva utilizada (grosso-modo, crece al hacerlo el número de puntos). En las Secciones 4 y 5 de este trabajo, profundizaremos en esta relación entre curvas y códigos (veáse tambien [37]).

Estas y otras aplicaciones prácticas han reavivado el interés por el estudio del cardinal de las curvas algebraicas sobre cuerpos finitos. Entre los objetivos centrales de este estudio podemos señalar los siguientes:

- desarrollar métodos que permitan contar los puntos racionales de una curva, o al menos
- obtener fórmulas que proporcionen acotaciones de este número; y
- encontrar curvas con muchos puntos (idealmente con los máximos permitidos por las fórmulas citadas en el punto anterior).

En las siguientes secciones expondremos algunos de los métodos y resultados relevantes en este estudio.

3.1. La función Zeta. Una de las herramientas más importantes en el estudio del número de puntos racionales de una curva $\mathcal{X}$ es su *función zeta*, estrechamente relacionada con la que Riemann introdujo en su tesis doctoral de 1859 y que lleva su nombre. Recordemos que para cada $s \in \mathbf{C}$ con $\Re(s) > 1$, se define

$$\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p} \frac{1}{1 - p^{-s}}\,,$$

estando el producto de la derecha (*identidad de Euler*) extendido a todos los números primos. Como se sabe, esta función admite prolongación analítica a todo el plano complejo, resultando una función meromorfa con un único polo en $s = 1$. En el semiplano $\Re(s) < 0$, la función tiene ceros en los puntos $s = -2m, m = 1, 2, \ldots$. Estos ceros son llamados

[2]Veáse a este respecto el artículo de Gómez Pardo en La Gaceta 5, núm. 3, [22].

triviales. Riemann conjeturó que todos los ceros no triviales de $\zeta(s)$ están sobre la recta $\Re(s) = 1/2$. Esta es su célebre *hipótesis*, no demostrada hasta el presente.[3]

La función de Riemann 'clásica' (podemos decir, relativa al cuerpo $\mathbf{Q}$) fué generalizada por Dedekind a cualquier cuerpo de números, es decir a una extensión finita de $\mathbf{Q}$: dado el cuerpo de números $\mathbf{K}$, se define la función $\zeta_{\mathbf{K}}(s)$ en el semiplano complejo $\Re(s) > 1$, como

$$\zeta_{\mathbf{K}}(s) := \sum_{\mathfrak{a}} \frac{1}{N(\mathfrak{a})^s} = \prod_{\mathfrak{p}} \frac{1}{1 - N(\mathfrak{p})^{-s}}\,,$$

estando la suma extendida a todos los ideales $\mathfrak{a}$ del anillo de enteros $\mathcal{O}$ de $\mathbf{K}$, el producto a todos los ideales primos $\mathfrak{p}$ de $\mathcal{O}$ y donde $N(\mathfrak{a}) := \#(\mathcal{O}/\mathfrak{a})$ es la norma de $\mathfrak{a}$. En el caso de la función de Riemann original, $\mathcal{O} = \mathbf{Z}$ cuyos ideales son los $n\mathbf{Z}$ y donde $N(n\mathbf{Z}) = \#(\mathbf{Z}/n\mathbf{Z}) = n$.

Dada la equivalencia entre curvas algebraicas y cuerpos de funciones algebraicas de una variable, no había más que un paso para definir funciones zeta de curvas algebraicas. Este paso fué dado por Artin (también en su tesis doctoral, de 1924) teniendo como modelo la función zeta de Dedekind. Antes de describir esta adaptación recordemos brevemente algunos conceptos. Sea $\mathcal{X}$ una curva sobre $\mathbf{F}_q$. Para cada entero positivo ℓ, denotamos por $\mathcal{X}(\mathbf{F}_{q^\ell})$ el conjunto de puntos $\mathbf{F}_{q^\ell}$-racionales de $\mathcal{X}$. Dado un punto $P \in \mathcal{X}$, el menor entero r tal que $\mathbf{\Phi}^r(P) = P$, es el *grado* de P, $\mathrm{grad}(P)$, sobre $\mathbf{F}_q$. Por la compatibilidad del morfismo de Frobenius con la acción sobre $\mathbf{P}$ del grupo de Galois, $G = \mathrm{Gal}(\bar{\mathbf{F}}_q|\mathbf{F}_q)$, se deduce que $\mathbf{\Phi}^2(P), \ldots, \mathbf{\Phi}^{r-1}(P)$ son conjugados de P mediante G. El conjunto $\{P, \mathbf{\Phi}(P), \mathbf{\Phi}^2(P), \ldots, \mathbf{\Phi}^{r-1}(P)\}$ recibe el nombre de *punto cerrado* de $\mathcal{X}$ de grado r (sobre $\mathbf{F}_q$). Diremos que un divisor $D = \sum n_P P$ de $\mathcal{X}$ es $\mathbf{F}_q$-*racional* si es suma de puntos cerrados; su grado será $\mathrm{grad}(D) := \sum n_P \mathrm{grad}(P)$.

Definimos ya la función zeta de $\mathcal{X}$ sobre $\mathbf{F}_q$, como

$$\zeta_{\mathcal{X}}(s) := \sum_{D \geq 0} \frac{1}{N(D)^s} = \prod_{P} \frac{1}{1 - N(P)^{-s}}\,, \tag{3.1}$$

estando la suma extendida a todos los divisores efectivos $\mathbf{F}_q$-racionales D sobre $\mathcal{X}$, y el producto a todos los puntos cerrados de $\mathcal{X}$, y siendo $N(P) := q^{\mathrm{grad}(P)}$.

Mediante el cambio de variable $t = q^{-s}$, podemos escribir $\zeta_{\mathcal{X}}(s) = Z_{\mathcal{X}}(t)$. Siendo esta última una serie de potencias convergente en $|t| < q^{-1}$ (es decir, en $\Re(s) > 1$), define una función racional de la forma

$$Z_{\mathcal{X}}(t) = \frac{L(t)}{(1-t)(1-qt)}\,.$$

$L(t)$ es un polinomio de grado $2g$, donde g es el género de la curva $\mathcal{X}$. Sus coeficientes son enteros y satisfacen ciertas propiedades de simetría. Un estudio detallado de esta función puede encontrarse, por ejemplo, en [45, Cap. V].

[3]Debido a la identidad de Euler, la hipótesis de Riemann posee profundas implicaciones sobre la distribución de los números primos. En 1914, Hardy probó que en la recta crítica hay infinitos ceros de $\zeta(s)$. Otras conjeturas de Riemann sobre $\zeta(s)$ fueron probadas por Hadamard y Mangoldt. La hipótesis de Riemann fué propuesta en la lista de Hilbert como problema 8 y es actualmente considerada como uno de los desafios del presente milenio (ver S. Smale, La Gaceta 3, núm. 3, [44].)

3.2. Contando puntos racionales. Artin propuso para $Z_{\mathcal{X}}(t)$ una conjetura similar a la hipótesis de Riemann, a saber, *los recíprocos de las raíces de* $L(t)$ *son números complejos de módulo* $\sqrt{q}$. Esto implicaría una escritura de la forma

$$L(t) = \prod_{i=1}^{g}(1-\alpha_i t)(1-\overline{\alpha}_i t)\,, \tag{3.2}$$

siendo los α_i enteros algebraicos con $|\alpha_i| = \sqrt{q}$. Esta conjetura fué probada en 1934 por Hasse para $g = 1$, y en 1940 por Weil para género arbitrario. Ahora, a partir de la identidad de Euler (segunda igualdad en (3.1)), se obtiene inmediatamente

$$\log(Z_{\mathcal{X}}(t)) = \sum_{r=1}^{\infty} \#\mathcal{X}(\mathbf{F}_{q^r})\frac{t^r}{r}\,,$$

fórmula que relaciona la función Zeta de $\mathcal{X}$ con el número de puntos racionales de $\mathcal{X}$ sobre toda extensión de $\mathbf{F}_q$. Ahora bien, por la racionalidad de $Z_{\mathcal{X}}(t)$,

$$\log(Z_{\mathcal{X}}(t)) = \sum_{i=1}^{g}\log(1-\alpha_i t) + \sum_{i=1}^{g}\log(1-\overline{\alpha}_i t)) - \log(1-t) - \log(1-qt).$$

Combinando las dos últimas igualdades, fácilmente se deduce que para cada entero positivo r,

$$\#\mathcal{X}(\mathbf{F}_{q^r}) = q^r + 1 - \sum_{i=1}^{g}(\alpha_i^r + \overline{\alpha}_i^r)\,. \tag{3.3}$$

De esta ecuación podemos deducir dos importantes propiedades. En primer lugar, conocido el cardinal de $\mathcal{X}(\mathbf{F}_{q^r})$ sobre g extensiones de $\mathbf{F}_q$, podemos calcular el valor de los α_i y, en consecuencia, el cardinal de $\mathcal{X}(\mathbf{F}_{q^r})$ para cualquier r. En segundo lugar, en virtud de la hipótesis de Riemann, se verifica la acotación

$$|\#\mathcal{X}(\mathbf{F}_{q^r}) - (q^r+1)| = |\sum_{i=1}^{g}(\alpha_i^r + \overline{\alpha_i}^r)| \leq 2g\sqrt{q^r}\,,$$

desigualdad que se conoce como *cota de Hasse-Weil* y que es la principal restricción conocida sobre el número de puntos racionales de una curva. Como se ve, asegura que este número es aproximadamente el de una recta, con una posibilidad de variación que depende del género de $\mathcal{X}$. Por supuesto no es la única conocida. Por ejemplo, Serre [42], observó que de hecho

$$|\#\mathcal{X}(\mathbf{F}_{q^r}) - (q^r+1)| \leq g\lfloor 2\sqrt{q^r}\rfloor\,. \tag{3.4}$$

Por otro lado, usando (3.3), de una forma simple y elegante, Ihara [28] mostró que

$$\#\mathcal{X}(\mathbf{F}_{q^r}) \leq q^r + 1 + \lfloor\frac{1}{2}\sqrt{(8q^r+1)g^2 + 4(q^2r - q^r)g} - g\rfloor\,. \tag{3.5}$$

Si $r = 1$ y $g > \frac{1}{2}(q - \sqrt{q})$, esta cota es mejor que la de Hasse-Weil-Serre.

4. Códigos Correctores y Curvas Algebraicas

Vamos a describir, con algún detalle, la relación entre las curvas algebraicas sobre cuerpos finitos y los códigos correctores de errores. En buena medida esta relación ha determinado las líneas de investigación actuales sobre curvas. Las referencias básicas para esta sección son [4], [32], [33] y [47]. No nos detendremos a explicar qué son y cómo funcionan los Códigos Correctores, puesto que estos temas han sido ya detallados en artículos anteriores de La Gaceta (ver [37]).

La relación entre curvas y códigos correctores viene dada por una construcción introducida por el matemático ruso V.D. Goppa en 1977 ([23]), y que permite definir códigos con buenos parámetros a partir de curvas definidas sobre cuerpos finitos. Recordemos brevemente como se lleva a cabo.

Sea $\mathcal{X}$ una curva (algebraica proyectiva, geométricamente irreducible y no-singular) de género g definida sobre $\mathbf{F}_q$. Para cada divisor $\mathbf{F}_q$-racional, E, sobre $\mathcal{X}$, el conjunto

$$\mathcal{L}(E) := \{f \in \mathbf{F}_q(\mathcal{X})^* : E + \mathrm{div}(f) \succeq 0\} \cup \{0\}$$

(siendo $\mathrm{div}(f)$ el divisor de f), es un espacio vectorial sobre $\mathbf{F}_q$ cuya dimensión, $\ell(E)$, es finita (ver e.g [45]). Sea $\mathcal{P} := \{P_1, \ldots, P_n\}$ un conjunto de n puntos racionales y distintos de $\mathcal{X}$. Sean finalmente $D =: P_1 + \cdots + P_n$ y G otro divisor racional sobre $\mathcal{X}$ con soporte disjunto del de D. La aplicación de evaluación

$$ev = ev_{\mathcal{P}} : \mathcal{L}(G) \longrightarrow \mathbf{F}_q^n\,; \quad ev(f) := (f(P_1), \ldots, f(P_n))$$

está bien definida y es lineal. En efecto, como $P_i \notin \mathrm{sop}(G)$, P_i no puede ser un polo de $f \in \mathcal{L}(G)$. Por otro lado, tanto P_i como G son $\mathbf{F}_q$-racionales, luego $f(P_i) \in \mathbf{F}_q$. En consecuencia, la imagen C de ev es un código lineal [4] sobre $\mathbf{F}_q$ llamado *código algebraico-geométrico* ó *código geométrico de Goppa* [24]. La dimensión, k, y la distancia mínima, d, de C pueden estimarse mediante las relaciones

$$k = \ell(G) - \ell(G - D) \quad \text{y} \quad d \geq n - \mathrm{grad}(G)\,.$$

Consecuentemente puede utilizarse el Teorema de Riemann-Roch para calcular estos parámetros. Recordemos que según este teorema, existe un divisor racional W (llamado *canónico*) con grado $2g-2$ y $\ell(W) = g$, tal que para cualquier divisor E sobre $\mathcal{X}$ se verifica que $\ell(E) = \mathrm{grad}(E) + 1 - g + \ell(W - E)$. Utilizando este teorema, y si por simplificar nos situamos en el caso más simple,

$$2g - 2 < \mathrm{grad}(G) < n\,,$$

resulta $k = \ell(G) = \mathrm{grad}(G) + 1 - g$. En este caso es muy fácil comprobar la calidad de los códigos obtenidos, ya que basta comparar con la cota de Singleton para obtener

$$n + 1 - g \leq k + d \leq n + 1\,. \tag{4.1}$$

Cuando la curva $\mathcal{X}$ es la recta proyectiva (ésto es, $g = 0$), el código C posee los mejores parámetros permitidos, $k + d = n + 1$ (decimos que es de *máxima distancia de separación,*

[4] Para una introducción a la teoría de Códigos Lineales Correctores de Errores puede consultarse [37].

MDS). Observamos que la acotación inferior en (4.1) va empeorando a medida que crece el género de la curva. Esta acotación puede expresarse también como

$$R + \delta \geq 1 + \frac{1-g}{n}\,, \tag{4.2}$$

donde $R = k/n$ y $\delta = d/n$ son los *parámetros relativos* de C. Según esta fórmula, la calidad de los códigos obtenidos crece al hacerlo el valor n/g, lo que en definitiva depende de la proporción $\#\mathcal{X}(\mathbf{F}_q)/g$.

5. Curvas con Muchos Puntos y Códigos Correctores

5.1. La función $N_q(g)$. En virtud de esta última observación, la calidad de un código algebraico-geométrico depende de que la curva a partir de la cual ha sido construido tenga un número de puntos racionales 'grande' comparado con su género (un poco más adelante –en el apartado 5.2– definiremos con más precisión lo que entendemos por *calidad*). Este hecho ha reavivado el interés por el estudio del número de puntos racionales de una curva. En este marco, son de destacar las cuestiones siguientes:

- fijados el cuerpo $\mathbf{F}_q$ y el género g, calcular

$$N_q(g) := \text{máx}\{\#\mathcal{Y}(\mathbf{F}_q) : \mathcal{Y} \text{ es una curva de género } g \text{ sobre } \mathbf{F}_q \text{ de género } g\}\,;$$

- caracterizar y describir explícitamente las *curvas optimales*, es decir, aquellas curvas $\mathcal{X}$ sobre $\mathbf{F}_q$ de género g, tales que $\#\mathcal{X}(\mathbf{F}_q) = N_q(g)$.

Obviamente $N_q(0) = q + 1$. El estudio del valor exacto de $N_q(g)$ para géneros mayores fué iniciado por Serre, [42], quien obtuvo los valores de $N_q(1)$ y $N_q(2)$ (junto con algunos casos esporádicos para $g = 3$). En general, hallar una fórmula cerrada para $N_q(g)$ es un desafío no trivial que parece actualmente fuera de nuestras posibilidades.

El método práctico actualmente utilizado es calcular las cotas superiores más ajustadas disponibles para $N_q(g)$ y comparar los resultados obtenidos con las mejores curvas que conocemos. De entre las cotas superiores, algunas han sido ya citadas en este trabajo: las de Hasse-Weil-Serre (3.4) y de Ihara (3.5). Existen, por supuesto, otras a las que no nos hemos referido con anterioridad, como son las "fórmulas explícitas de Weil"(formalizadas por Oesterlé) [42], [45, V.3], o el método aritmético-geométrico de Stöhr y Voloch, [46]. En la dirección electrónica [20] puede obtenerse una tabla actualizada de los mejores resultados conocidos sobre $N_q(g)$, para algunos valores pequeños de q y g.

Para acotar inferiormente $N_q(g)$ se construyen curvas con la mayor cantidad de posible de puntos. Entre éstas podemos citar las *curvas de Suzuki* definidas por la ecuación $y^\ell - y = x^{\ell_0}(x^\ell - x)$, donde $\ell_0 > 1$ es una potencia de 2 y $\ell := 2\ell_0^2$; la curva de Ree, definida en $\mathbf{P}^3$ por las ecuaciones $y^\ell - y = x^{\ell_0}(x^\ell - x)$ y $z^\ell - z = x^{2\ell_0}(x^\ell - x)$), siendo ahora $\ell_0 > 1$ una potencia de 3 y $\ell = 3\ell_0^2$; o las curvas Hermitianas (a la que nos referiremos un poco más adelante)[5].

[5]De hecho, las curvas de Suzuki, de Ree y las Hermitianas alcanzan los valores máximos permitidos por $N_q(g)$.

5.2. Contando puntos racionales asintóticamente y la cota de Gilbert-Varshamov. Por ciertos motivos, teóricos y prácticos, más interés aún que encontrar códigos particulares con buenos parámetros, lo tiene obtener sucesiones de códigos cuyos parámetros sean asintóticamente buenos. Este interés nos motiva para considerar la función

$$A(q) := \limsup_{\mathcal{Y}} \frac{\#\mathcal{Y}(\mathbf{F}_q)}{g(\mathcal{Y})} = \limsup_{g\to\infty} \frac{N_q(g)}{g}\,,$$

donde $\mathcal{Y}$ varía en el conjunto de todas las curvas definidas sobre $\mathbf{F}_q$. Las cotas superiores sobre $\#\mathcal{Y}(\mathbf{F}_q)$ pueden traducirse inmediatamente en cotas sobre $A(q)$. Así, la cota de Hasse-Weil-Serre (3.4) implica que $A(q) \le 2\lfloor\sqrt{q}\rfloor$ y la de Ihara (3.5) que $A(q) \le \frac{1}{2}(\sqrt{8q+1}-1)$. En cuanto a las cotas inferiores, usando *curvas modulares*, Ihara demostró que $A(q) \ge \sqrt{q}-1$ cuando q es un cuadrado. Además, Serre, [42], estableció $A(q) > c\log(q)$, donde $c>0$ es cierta constante independiente de q.

Posteriormente Vladut y Drinfeld, [49], mejorarón la cota superior de Ihara mostrando que $A(q) \le \sqrt{q}-1$. En particular,

$$\text{si } q \text{ es un cuadrado, entonces } A(q) = \sqrt{q}-1\,. \tag{5.1}$$

Para la demostración de este resultado, Vladut y Drinfeld mostraron que cuando q es un cuadrado, existe una sucesión de curvas modulares $(\mathcal{X}_i)_i$ sobre $\mathbf{F}_q$, con géneros $g_i \to \infty$ y tales que $\lim_{g_i} \#\mathcal{X}_i(\mathbf{F}_q)/g_i = \sqrt{q}-1$. Los códigos construidos sobre estas curvas tienen –asíntoticamente– los mejores parámetros que ha sido posible obtener hasta el presente (notemos que estos parámetros no han podido ser calculados exáctamente, sino estimados usando (4.2)):

Teorema 5.1. (Tsfasman, Vladut y Zink, 1982) *Sea q un cuadrado. Existe una sucesión (C_i) de códigos algebraico-geométricos sobre $\mathbf{F}_q$ cuyos parámetros relativos (R_i,δ_i) tienen un punto límite (R',δ') tal que*

$$R'+\delta' = 1 - \frac{1}{\sqrt{q}-1}\,. \tag{5.2}$$

(ver [48], [47, Ch. 4]). Este resultado asombró en su momento a los especialistas en Teoría de Códigos y fué una de las razones que motivaron el auge de los códigos algebraico geométricos. Para ser un poco más precisos, digamos que los parámetros la sucesión de códigos aludida anteriormente superan asintóticamente la llamada *cota de Gilbert-Varshamov* (ver [37]). Era bien conocido que esta cota podía ser superada, pero hasta 1982 nadie habia mostrado como hacerlo. Por ello, este problema se convirtió en uno de los más importantes de la teoría. Aún hoy en día, todas las sucesiones que superan esa cota (o parecen tener probabilidades de hacerlo), están formadas por códigos algebriaco geométricos.

Por otro lado, para obtener aplicaciones prácticas de este resultado, es preciso construir de forma explícita los códigos correspondientes. Dada la complejidad de la sucesión de curvas consideradas inicialmente por Tsfasman, Vladut y Zink, esta no es una tarea fácil. Claro está que este trabajo se simplificaría si dispusiesemos de ecuaciones lo más explícitas y simples posibles para las curvas $\mathcal{X}_i$. Desafortunadamente, a priori no es claro que esas curvas satisfagan nuestras expectativas. Un avance en esta línea se debe a Garcia y Stichtenoth, quienes en una serie de trabajos ([15], [16], [17]) mostraron que es posible

obtener $A(q) = \sqrt{q} - 1$ para una sucesión de curvas con fácil descripción. Curiosamente, más tarde Elkies [10] mostró que las curvas que aparecen en la sucesión introducida en [15] son de nuevo curvas modulares; en [11], el mismo Elkies especula sobre la posibilidad de que toda sucesión de curvas tal que $A(q) = \sqrt{q} - 1$ (siendo q un cuadrado) esté compuesta por curvas modulares. Una evidencia para esta especulación es que todas las sucesiones de curvas con $A(q) = \sqrt{q} - 1$ conocidas hasta el presente son obtenidas mediante recubrimientos apropiados de las que definen la sucesión en [15].

Una línea de investigación actual es la construcción explícita de los códigos asintóticamente buenos obtenidos a partir de las curvas de Garcia y Stichtenoth. Para ello se consideran los códigos más simples posibles, es decir, los unipuntuales $C_i = C_i(G_i, D_i)$ donde $G_i = n_i Q_i$. En este caso, para definir C_i es necesario y suficiente conocer el semigrupo de Weierstrass $H(Q_i)$ y las funciones racionales que proporcionan sus elementos. Así, por ejemplo, para la sucesión de curvas introducida en [16], los semigrupos han sido ya calculados, pero no se conoce aún la totalidad de las funciones racionales que los definen, [39].

En los resultados anteriores hemos asumido q cuadrado. El caso $q = p^{2m+1}$ parece ser más complicado aún. Inicialmente Manin [35], conjeturó que $A(q) = p^m - 1$. Recientemente van der Geer y van der Vlugt, [21], probarón que $A(8) \geq \frac{3}{2}$ (mediante ecuaciones explícitas de curvas) lo cual invalida esta conjetura. En general, Zink ,[52], probo que $A(p^3) \geq \frac{2(p^2-1)}{p+2}$ (sin ecuaciones explítas de las curvas); esta cota inferior fue generalizada por Bezerra, Garcia y Stichtenoth, [4], para potencias cúbicas de q arbitrario (ahora sí con ecuaciones explícitas).

6. Curvas Maximales

En secciones anteriores hemos descrito de forma somera el interés del estudio sobre las curvas con muchos puntos y su situación actual. Naturalmente es imposible dar todos los detalles de las técnicas utilizadas. En esta sección vamos a ocuparnos de analizar el caso límite de las curvas maximales. Contrariamente a lo hecho antes, vamos a ofrecer más detalles, con lo que la exposición será en ocasiones más técnica (lo que esperamos que quede compensado con la belleza del tema). Los lectores interesados en profundizar en este tópico pueden consultar [30] y sus referencias.

Como hemos visto en la Sección 3, el número de puntos racionales de una curva $\mathcal{X}$ sobre $\mathbf{F}_q$ esta acotado por

$$\#\mathcal{X}(\mathbf{F}_q) \leq q + 1 + 2g\sqrt{q}\,.$$

Las curvas para las que se alcanza la igualdad son llamadas *maximales* (sobre $\mathbf{F}_q$). Por ejemplo, toda curva de género 0 es maximal. Veamos que sucede para género $g > 0$.

En primer lugar observamos quer sólo pueden existir curvas maximales sobre el cuerpo $\mathbf{F}_q$ si q es un un cuadrado. Pongamos $q = \ell^2$ y denotemos $\mathbf{K} = \mathbf{F}_{\ell^2}$. Sea $\mathcal{X}$ una curva sobre $\mathbf{K}$ de género g y sean $\alpha_1, \ldots, \alpha_g$ los números definidos en (3.2). La ecuación (3.3) proporciona una primera condición de maximalidad:

$$\mathcal{X} \text{ es } \mathbf{K}\text{-maximal si y sólo si} \quad \alpha_i = -\ell,\ i = 1, \ldots, g\,.$$

La igualdad (3.3) también muestra que no todos géneros son posibles para una curva maximal. En efecto, si $\mathcal{X}$ es maximal sobre $\mathbf{F}_{\ell^2}$, entonces la condición $\alpha_i = -\ell$, llevada a

la ecuación (3.3), implica que $\mathcal{X}$ tiene el menor número de puntos $\mathbf{F}_{\ell^4}$-racionales permitido por la cota de Hasse-Weil (es *minimal*); por lo tanto, como $\mathcal{X}(\mathbf{F}_{\ell^2}) \subseteq \mathcal{X}(\mathbf{F}_{\ell^4})$,

$$\ell^2 + 1 + 2g\ell \leq \ell^4 + 1 - 2g\ell^2$$

y se verifica que

$$g \leq g_1 = g_1(\ell) := \frac{1}{2}(\ell - 1)\ell$$

con lo que los géneros permitidos para una curva maximal se encuentran en el intervalo $[0, g_1]$ (hecho que fué notado por Ihara; ver (3.5)). Esta observación sugiere de forma natural la pregunta ¿para qué números naturales g entre 1 y g_1, existe una curva $\mathbf{K}$-maximal de género g? A continuación vamos a aportar algunas respuestas (parciales) a esta pregunta, hasta donde lo permite el estado actual de la investigación sobre el tema.

Denotemos $\mathbf{M} = \mathbf{M}_\ell = \{g : \text{existe una curva maximal de género } g \text{ sobre } \mathbf{F}_{\ell^2}\}$. En primer lugar veremos que $g_1 \in \mathbf{M}$. En efecto, consideremos la famosa curva Hermitiana $\mathcal{H}$, definida por la equación $Y^\ell Z + Y Z^\ell = X^{\ell+1}$. Esta curva es no-singular y tiene género g_1. Fácilmente se comprueba que $\mathcal{H}$ posee ℓ^3 puntos afines más un punto en el infinito, luego es maximal. Aún más, Rück y Stichtenoth, [41], probarón que $\mathcal{H}$ es, salvo isomorfismo, la única curva $\mathbf{K}$-maximal de género g_1. Un poco más adelante esbozaremos otra demostración de este resultado.

Veamos ahora que sucede si $g \in \mathbf{M}$ y $g < g_1$. Como comprobaremos, la curva $\mathcal{H}$ sigue jugando un importante papel también en este caso.

Teorema 6.1. ([41], [51], [13], [14]) *Sea $\mathcal{X}$ una curva $\mathbf{K}$-maximal de género g. Si $g > g_2 := \lfloor (\ell-1)^2/4 \rfloor$ entonces $\mathcal{X}$ es $\mathbf{K}$-isomorfa a la curva Hermitiana $\mathcal{H}$. En consecuencia, o bien $g = g_1$, o $g \leq g_2$.*

Por lo tanto, en, aproximadamente, la mitad superior del intervalo $[0, g_1]$ existe una única curva maximal. Para dar una idea de los métodos empleados en el estudio de las curvas maximales, vamos a ofrecer la prueba de este resultado. Para ello previamente recordaremos, sin demostración, algunos hechos sobre:

(1) La existencia de un sistema lineal $\mathcal{D}$ de dimensión $N \geq 2$ sobre una curva maximal ([41], [13]);
(2) Tópicos de semigrupos de Weierstrass (en el caso del Teorema 6.1); y
(3) Tópicos de la teoría de Stöhr y Voloch para $\mathcal{D}$ ([46]).

(1) Como recordamos de (3.2), el numerador de la función Zeta de $\mathcal{X}$ es $L(t) = (1+\ell t)^{2g}$. Sean $h(t) := t^{2g} L(t^{-1})$ y $\tilde{\mathbf{\Phi}}$ el morfismo de Frobenius inducido por $\mathbf{\Phi}$ en la variedad Jacobiana $\mathcal{J}$ de $\mathcal{X}$. Se verifica que $h(t) = (t + \ell)^{2g}$ es el polinomio característico de $\tilde{\mathbf{\Phi}}$; más aun, puede demostrarse que $\tilde{\mathbf{\Phi}} + qI = 0$, siendo I (resp. 0) la identidad (resp. operador nulo) sobre $\mathcal{J}$. Fijemos ahora un punto racional $P_0 \in \mathcal{X}$ y para $P \in \mathcal{X}$ denotemos por $i(P) = [P - P_0]$ la clase de P en $\mathcal{J}$. Entonces, en virtud de la igualdad $\tilde{\mathbf{\Phi}} + qI = 0$, y como $\tilde{\Phi} \circ i = i \circ \Phi$, se obtiene la equivalencia de divisores

$$\ell P + \mathbf{\Phi}(P) \sim (\ell + 1) P_0 \,. \tag{6.1}$$

Esta equivalencia sugiere estudiar el sistema lineal $\mathcal{D} = \mathcal{D}_{\mathcal{X}} := |(\ell + 1)P_0|$, $P_0 \in \mathcal{X}(\mathbf{K})$. Sea N la dimensión de $\mathcal{D}$; como consecuencia de (6.1) deducimos que $N \geq 2$. En efecto, basta considerar una función asociada a un punto racional diferente de P_0 y otra asociada

a un punto P no racional. El sistema lineal $\mathcal{D}$ es *simple* en el sentido que algún morfismo asociado a $\mathcal{D}$ es biracional de $\mathcal{X}$ sobre su imágen (esto se seguirá del punto (2)). En particular, podemos aplicar la fórmula de Castelnuovo para acotar superiormente el género g de $\mathcal{X}$ (ver [5], [2, p. 116], [26, IV Thm. 6.4], [40, Cor. 2.8]), obteniendo

$$g \leq M(q+1-N+e)/2\,,$$

donde $M = \lfloor \frac{q}{N} - 1 \rfloor$ y $e = q - M(N-1)$.

(2) Dado un punto $P \in \mathcal{X}$, el semigrupo de Weierstrass, $H(P)$, de $\mathcal{X}$ en P se define como

$$H(P) := \{n \in \mathbf{N} : \exists f \in \mathbf{K}(\mathcal{X})/\operatorname{div}_\infty(f) = nP\}$$

siendo $\operatorname{div}_0(f)$ y $\operatorname{div}_\infty(f)$ los divisores de ceros y polos, respectivamente, de la función racional f. En el caso de una curva maximal, de (6.1) se deduce que $\ell + 1 \in H(P)$ para todo $P \in \mathcal{X}(\mathbf{K})$. Para probar que $\mathcal{D}$ es simple, bastará probar que $\ell \in H(P)$ al menos para algún punto $\mathbf{K}$-racional P (de hecho esto será cierto para todo punto $\mathbf{K}$-racional). Sea $y : \mathcal{X} \to \mathbf{P}^1(\bar{\mathbf{K}})$ con $\operatorname{div}_\infty(y) = (\ell+1)P_0$. Existe $P_1 \in \mathcal{X}(\mathbf{K})$ tal que $\operatorname{div}_0(y - y(P_1)) = P_1 + D$ con $P_1 \notin \operatorname{sop}(D)$, pues de lo contrario llegaríamos a una contradicción usando la maximalidad de la curva al aplicar a y la fórmula de Riemann-Hurwitz. Sea $y_1 \in \mathbf{K}(\mathcal{X})$ tal que $\operatorname{div}(y_1) = (\ell+1)P_0 - (\ell+1)P_1$. Entonces $\operatorname{div}_\infty(y_1(y - y(P_1))) = \ell P$ y $\ell \in H(P_1)$. Ahora, de la hipótesis $g > \frac{1}{4}(\ell-1)^2$ y la cota de Castelnuevo, concluimos que $N = 2$.

(3) Sean $1, x, y$, las secciones que generan $\mathcal{D}$. Como $\ell, \ell+1 \in P_0$, podemos suponer que $\operatorname{div}_\infty(x) = \ell P_0$ y $\operatorname{div}_\infty(y) = (\ell+1)P_0$. Sean $\pi := (1 : x : y) : \mathcal{X} \to \mathbf{P}^2 := \mathbf{P}^2(\bar{\mathbf{K}})$ y $L : ax + by + c$ una recta en $\mathbf{P}^2$. Los elementos de $\mathcal{D}$ son de la forma

$$\pi^{-1}(L) := \operatorname{div}(ax + by + c) + (\ell+1)P_0\,;$$

luego para $P \in \mathcal{X}$ existen tres rectas, L_0, L_1, L_2, tales que si $j_i = j_i(P) := v_{P_i}(\pi^{-1}(L_i))$, entonces

$$j_0 < j_1 < j_2\,.$$

Para un divisor D, escribimos $D = \sum_P v_P(D)P$. Se verifica que

- La terna (j_0, j_1, j_2) es constante (y digamos igual a $(\epsilon_0, \epsilon_1, \epsilon_2)$) con la excepción de un número finito de puntos. Los $\epsilon_0, \epsilon_1, \epsilon_2$, son los *órdenes* de $\mathcal{D}$ (o π) y los puntos excepcionales son llamados $\mathcal{D}$*-puntos de Weierstrass*. En ellos $j_i \geq \epsilon_i$ para cada i (pero nótese que, en virtud de (6.1), se verifica que $j_2 = \ell + 1$ para todo punto $\mathbf{K}$-racional). Por otro lado, los ϵ_i satisfacen ciertas propiedades aritméticas, una de las cuales es la siguiente: si p es la característica de $\mathbf{K}$ y η es p-ádicamente menor que algún ϵ_i, entonces η pertenece a la sucesion de ordenes.
- En nuestro caso, $\epsilon_0 = 0$, $\epsilon_1 = 1$ y $\epsilon_2 = \ell$. Para ver esto basta considerar los divisores $\pi^{-1}(a + bx)$ y $\pi^{-1}(a + cy)$, $b, c \neq 0$, para obtener en P_0 los valores $j_1 = 1$ y $j_0 = 0$. Por otro lado, a partir de (6.1), ℓ es un orden para infinitos puntos, luego $\epsilon_2 = \ell$.
- Existe un divisor R sobre $\mathcal{X}$ cuyo soporte es exáctamente el conjunto de $\mathcal{D}$-puntos de Weierstrass. Este divisor R tiene dos propiedades relevantes a saber:

  $$\operatorname{grad}(R) = (\epsilon_0 + \epsilon_1 + \epsilon_2)(2g-2) + 3(q+1)$$

  y $v_P(R) \geq \sum_{i=0}^{2}(j_i - \epsilon_i)$; en particular $v_P(R) \geq 1$ para todo punto $\mathbf{K}$-racional P.

Prueba del Teorema 6.1. Primero veremos que $g = g_1 = \frac{1}{2}(\ell-1)\ell$. De la fórmula para $\mathrm{grad}(R)$ y de la maximalidad de la curva,

$$(1+\ell)(2g-2) + 3(\ell+1) \geq \ell^2 + 1 + 2g\ell = (\ell+1)^2 + \ell(2g-2)\,;$$

luego $g \geq g_1$. Como $g \leq g_1$, $g = g_1$. Se sigue que $\mathrm{grad}(R) = q^3+1$ y por lo tanto concluimos que $j_1 = 1$ para todo punto P.

A continuación probaremos que la curva $\mathcal{X}$ es $\mathbf{K}$-isomorfa a la curva Hermitiana. Para $P \in \mathcal{X}$, sea $L = L_P$ la recta de $\mathbf{P}^2$ asociada al invariante j_2. De los cálculos realizados anteriormente y de (6.1), deducimos que $\mathcal{X} := \pi(\mathcal{X})$ intersecta a L solamente en $\pi(P)$, con multiplicidad $\ell+1$, si P es $\mathbf{K}$-racional; en otro caso, la intersección se produce en dos puntos, $\pi(P)$ y $\pi(\mathbf{\Phi}(P))$, siendo ℓ la multiplicidad en el primero y 1 en el del segundo. Sea P un punto distinto de P_0. La ecuación de $L = L_P$ se obtiene a partir del determinante de una matriz cuyas filas son $(X,Y,Z), (1,x,y)$ y $(0,1,Dy)$, siendo $D = D^1$ la derivada respecto de x definida sobre el cuerpo $\mathbf{K}(\mathcal{X})$. Como $\pi(\mathbf{\Phi}(P)) = (1 : x^{\ell^2} : y^{\ell^2})$, se tiene la identidad

$$y^{\ell^2} - y = Dy(x^{\ell^2} - x)\,. \tag{6.2}$$

Ahora bien, debe ser $Dy = f^\ell$ para algun $f \in \mathbf{K}(\mathcal{X})$; en efecto, como $\epsilon_2 = \ell$, existe una relación de la forma $1 + z_1^\ell x + z_2^\ell y = 0$ con $z_1, z_2 \in \mathbf{K}(\mathcal{X})$ (ver [19]). Por tanto el orden de f en P es $-\ell$ y, ya que esta función no tiene otros polos, $f = a + bx$ con $a, b \in \mathbf{K}$ (aquí estamos aplicando el hecho de que tanto x como f definen al primer elemento positivo del semigrupo de Weierstrass en P_0). Finalmente de (6.2)

$$(y_1^\ell + y_1 - x_1^{\ell+1})^\ell = y_1^\ell + y_1 - x_1^{\ell+1}\,,$$

donde $y_1 := by$ y $x_1 := a + bx$. Con esto la prueba del teorema está completa.

El Teorema 6.1 se puede extender para analizar la existencia de curvas maximales en el intervalo $[0, g_2]$. En este caso, la demostración es técnicamente más complicada a pesar de que esencialmente se utilizan las mismas técnicas de series lineales aplicadas a $\mathcal{D}$ (ver [30] y las referencias en ese artículo).

Teorema 6.2. ([1], [12], [30]) *Sea $\mathcal{X}$ una curva $\mathbf{K}$-maximal de género $g \leq g_2$. Entonces*

1. *Si ℓ es impar entonces $g = g_2$ si y sólo si la curva admite un modelo plano del tipo $y^\ell + y = x^{\frac{1}{2}(\ell+1)}$;*
2. *Si ℓ es par entonces $g = g_2$ si y sólo si la curva admite un modelo plano del tipo $y^{\frac{\ell}{2}} + y^{\frac{\ell}{4}} + \cdots + y = x^{\ell+1}$;*
3. *Si $g < g_2$, entonces $g \leq g_3 := \lfloor \frac{1}{6}(\ell^2 - \ell + 4) \rfloor$.*

La cota del apartado (3) no puede mejorarse puesto que disponemos de los siguientes ejemplos, que son modelos planos de curvas maximales de género g_3 .

- Si $\ell \equiv 2 \pmod 3$ la curva $y^{\ell+1} + x^{\frac{1}{3}(\ell+1)} + x^{\frac{2}{3}(\ell+1)} = 0$;
- Si $\ell \equiv 1 \pmod 3$ la curva $y^\ell - yx^{\frac{2}{3}(\ell-1)} + x^{\frac{1}{3}(\ell-1)} = 0$;
- Si $\ell = 3^t$ la curva $y^\ell + y + (\sum_{i=1}^t x^{\frac{\ell}{3^i}})^2 = 0$.

Para demostrar que estas ecuaciones definen curvas $\mathbf{K}$-maximales usamos una observación de Serre (que aparece en el trabajo de Lachaud [31, Prop. 6]): dado un morfismo no constante entre dos curvas $\mathcal{X} \to \mathcal{Y}$ (definido sobre $\mathbf{K}$), si $\mathcal{X}$ es $\mathbf{K}$-maximal entonces

también lo será $\mathcal{Y}$. En particular, toda curva cociente de la Hermitiana, $\mathcal{H}/G$ (siendo G un subgrupo del grupo de automorfismos, $PG(3,\mathbf{K})$, de $\mathcal{H}$) es $\mathbf{K}$-maximal. Pues bien, todas las curvas maximales mencionadas hasta ahora en este trabajo han resultado ser de este tipo. Como $PG(3,\mathbf{K})$ tiene una gran cantidad de subgrupos no conjugados, obtenemos de este modo una gran cantidad de elementos de $\mathbf{M}$ (ver [6],[7],[18]). De hecho, todos los ejemplos conocidos actualmente de curvas $\mathbf{K}$-maximales o bien son cocientes de la curva Hermitiana, o bien no se sabe si lo son. Ejemplos de esta última situación son las curvas de Suzuki y de Ree definidas en la Sección 5 (usando (3.3) se observa que una curva de Suzuki es maximal sobre $\mathbf{F}_{\ell^4}$ con $\ell = 2\ell_0^2 > 2$, y la de Ree sobre $\mathbf{F}_{\ell^6}$ con $\ell = 3\ell_0^2 > 3$). Por lo tanto, por lo que sabemos, bien pudiera ser que la curva Hermitiana fuera, en cierto sentido, el único ejemplo 'significativo' de curva maximal. En definitiva, caracterizar las curvas maximales en el intervalo $[0, g_3]$ es, hoy por hoy, un problema abierto.

Referencias

[1] M. Abdón y F. Torres, *Maximal curves in characteristic two*, Manuscripta Math. **99** (1999), 39–53.

[2] E. Arbarello, M. Cornalba, P.A. Griffiths, y J. Harris, "Geometry of Algebraic Curves", Vol. I, Springer-Verlag, New York, 1985.

[3] J.K. Baumgart, "Tópicos de História da Matemática: Algebra", Atual Editora Ltda., Campinas, 1993.

[4] J. Bezerra, A. Garcia y H. Stichtenoth, *An explicit tower on function fields over cubic finite fields and Zink's lower bound*, pre-print, 2004.

[5] G. Castelnuovo, *Ricerche di geometria sulle curve algebriche*, Atti. R. Acad. Sci. Torino **24** (1889), 196–223.

[6] A. Cossidente, G. Korchmáros y F. Torres, *On curves covered by the Hermitian curve*, J. Algebra **216** (1999), 56–76.

[7] A. Cossidente, G. Korchmáros y F. Torres, *Curves of large genus covered by the Hermitian curve*, Comm. Algebra **28**(10) (2000), 4707–4728.

[8] P. Deligne y G. Lusztig, *Representations of reductive groups over finite fields*, Ann. of Math. **103** (1976), 103–161.

[9] L.E. Dickson, "History of the Theory of Numbers", Vol. II, Chelsea Publishing Company, New York, 1971.

[10] N. D. Elkies, *Explicit modular towers*, Proceedings of the Thirty-Fifth Annual Allerton Conference on Communication, Control and Computing, (T. Basar y A. Vardy, eds.), Uni. of Illinois at Urbana-Champaign (1998), 23–32.

[11] N.D. Elkies, *Explicit towers of Drinfeld modular curves*, European Congress of Mathematics (Barcelona 2000), **Vol. II** (C. Casacuberta et all., eds.), Birkhäuser, Basel (2001), 189–198.

[12] R. Fuhrman, A. Garcia y F. Torres, *On maximal curves*, J. Number Theory **67**(1) (1997), 29–51.

[13] R. Fuhrmann y F. Torres, *The genus of curves over finite fields with many rational points*, Manuscripta Math. **89** (1996), 103–106.

[14] R. Fuhrmann y F. Torres, *On Weierstrass points and optimal curves*, Rend. Circ. Mat. Palermo **51** (1998), 25–46.

[15] A. Garcia y H. Stichtenoth, *A tower of Artin-Schreier extensions of functions fields attaining the Drinfeld-Vladut bound*, Invent. Math. **121**(1) (1995), 211–233.

[16] A. Garcia y H. Stichtenoth, *On the asymptotic behaviour of some towers of functions fields over finite fields*, J. Number Theory **6** (1996), 248–273.

[17] A. Garcia y H. Stichtenoth, *On tame towers over finite fields*, J. Reine Angew. Math. **557** (2003), 53–80.

[18] A. Garcia, H. Stichtenoth y C.P. Xing, *On subfields of the Hermitian function field*, Compositio Math. **120** (2000), 137–170.

[19] A. Garcia y J.F. Voloch, *Wronskians and independence in fields of prime characteristic*, Manuscripta Math. **59** (1987), 457-469.
[20] G. van der Geer y M. van der Vlugt, *Tables of curves with many points*, `www.wins.uva.nl/~geer`.
[21] G. van der Geer y M. van der Vlugt, *An asymptotically good tower of curves over the finiete field with eight elements*, Bull. London Math. Soc. **24** (2002), 291–300.
[22] J.L. Gómez Pardo, *Criptografía y curvas elípticas*, La Gaceta de la RSME **5**, núm. 3 (2002), 738-777.
[23] V.D. Goppa, *Codes associated with divisors*, Problems of Information Transmission **1** (1977).
[24] V.D. Goppa, "Geometry and Codes", Kluwer, 1988.
[25] J.P. Hansen, *Deligne-Lusztig varieties and group codes*, Lect. Notes Math. **1518** (1992), 63–81.
[26] R. Hartshorne, "Algebraic Geometry", Springer-Verlag, New York-Heidelberg-Berlin, 1977.
[27] J.P. Hansen y J.P. Pedersen, *Automorphism group of Ree type, Deligne-Lusztig curves and function fields*, J. Reine Angew. Math. **440** (1993), 99–109.
[28] Y. Ihara, *Some remarks on the number of rational points of algebraic curves over finite fields*, J. Fac. Sci. Tokyo, Sec. Ia, **28**(3) (1981), 721–724.
[29] N. Koblitz, "A course in number theory and cryptography", Springer-Verlag, 1987.
[30] G. Korchmáros y F.Torres, *On the genus of a maximal curve*, Math. Ann. **323** (2002), 589–608.
[31] G. Lachaud, *Sommes d'Eisenstein et nombre de points de certaines courbes algébriques sur les corps finis*, C.R. Acad. Sci. Paris Série I **305** (1987), 729–732.
[32] J.H. van Lint, "Introduction to Coding Theory", Springer-Verlag, third edition, 1999.
[33] J.H. van Lint y G. van der Geer, "Introduction to Coding Theory and Algebraic Geometry", Birkhäuser, Basel-Boston-Berlin, 1988.
[34] F. López y J. Tena, "Introducción a la teoría de números primos", Publicaciones de la Universidad de Valladolid, 1990.
[35] Yu.L. Manin, *What is the maximal number of points on a curve over* $\mathbf{F}_2$*?*, J. Fac. Sci. Univ. Tokio, Sec. Ia , **28**(3) (1982), 715–720.
[36] C. Moreno, "Algebraic Curves over Finite Fields", Cambridge Tracts in Maths. **97**, Cambridge Univ. Press, Cambridge, 1991.
[37] C. Munuera, *Códigos correctores de errores*, La Gaceta de la RSME 6, núm. 3 (2003), 714-731.
[38] C. Munuera y J. Tena, "Codificación de la información", Serie: Manuales y textos universitarios **25**, Universidad de Valladolid, 1997.
[39] R. Pellikaan, H. Stichtenoth y F. Torres, *Weierstrass semigroups in an asymptotically good tower of functions fields*, Finite Fields Appls. **4** (1998), 381–392.
[40] J. Rathmann, *The uniform position principle for curves in characteristic p*, Math. Ann. **276** (1987), 565-579.
[41] H.G. Rück y H. Stichtenoth, *A characterization of Hermitian function fields over finite fields*, J. Reine Angew. Math. **457** (1994), 185–188.
[42] J.P. Serre, *Sur le nombre de points rationnels d'une courbe algébrique sur un corps fini*, C.R. Acad. Sci. Paris **296** (1983) 397–402.
[43] J.H. Silverman y J. Tate, "Rational points on elliptic curves", Springer, 1992.
[44] S. Smale, *Problemas matemáticos para el próximo siglo*, La Gaceta de la RSME **3**, núm. 3 (2000), 413-434.
[45] H. Stichtenoth, "Algebraic Function Fields and Codes", Springer-Verlag, New York, 1993.
[46] K.O. Stöhr y J.F. Voloch, *Weierstrass points and curves over finite fields*, Proc. London Math. Soc. **52** (1986), 1-19.
[47] M.A. Tsfasman y S.G. Vladut, "Algebraic-Geometric Codes", Kluwer, 1991.
[48] M.A. Tsfasman, S.G. Vladut y Th. Zink, *On Goppa codes which are better than the Varshamov-Gilbert bound*, Math. Nachr. **109** (1982), 21–28.
[49] S.G. Vladut y V.G. Drinfeld, *Number of points of an algebraic curve*, Funct. Anal. **17**(1) (1983), 68–69.
[50] B.L. van der Waerden, "Geometry and Algebra in Ancient Civilizations", Springer-Verlag, Berlin, Heidelberg, 1983.

[51] C. Xing y H. Stichtenoth, *The genus of maximal functions fields*, Manuscripta Math. **86** (1995), 217–224.
[52] Th. Zink, *Degeneration of Shimura surfaces and a problem in coding theory*, Fundamentals of Computation Theory (L.Budach, ed.) Springer-Verlag, New York (1985), 503–511.

Universidad de Valladolid, Dep. Matemática Aplicada, Avda. Salamanca SN, 47014 Valladolid, España
E-mail address: cmunuera@modular.arq.uva.es

IMECC-UNICAMP, Cx. 6065, 13083-970, Campinas SP–Brasil
E-mail address: ftorres@ime.unicamp.br