Torres de cuerpos de funciones asintoticamente buenas

María Chara

Instituto de Matemática Aplicada del Litoral
UNL - CONICET
Santa Fe

14 de Mayo de 2010
Seminario IMAL

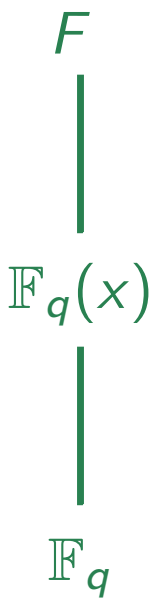
Cuerpos de Funciones

Cuerpos de Funciones

Sea $\mathbb{F}_q$ el cuerpo finito con q elementos. Un **cuerpo de funciones algebraicas** $F/\mathbb{F}_q$ sobre $\mathbb{F}_q$ es un extensión de cuerpos $F \supseteq \mathbb{F}_q$ tal que F es un extensión algebraica finita de $\mathbb{F}_q(x)$ para algún elemento $x \in F$ que sea trascendente sobre $\mathbb{F}_q$.

Cuerpos de Funciones

Sea $\mathbb{F}_q$ el cuerpo finito con q elementos. Un **cuerpo de funciones algebraicas** $F/\mathbb{F}_q$ sobre $\mathbb{F}_q$ es un extensión de cuerpos $F \supseteq \mathbb{F}_q$ tal que F es un extensión algebraica finita de $\mathbb{F}_q(x)$ para algún elemento $x \in F$ que sea trascendente sobre $\mathbb{F}_q$.



Un **anillo de valuaciones** del cuerpo de funciones $F/\mathbb{F}_q$ es un anillo $\mathcal{O} \subseteq F$ con las propiedades:

Un **anillo de valuaciones** del cuerpo de funciones $F/\mathbb{F}_q$ es un anillo $\mathcal{O} \subseteq F$ con las propiedades:

- $\mathbb{F}_q \subsetneq \mathcal{O} \subsetneq F$;

Un **anillo de valuaciones** del cuerpo de funciones $F/\mathbb{F}_q$ es un anillo $\mathcal{O} \subseteq F$ con las propiedades:

- $\mathbb{F}_q \subsetneq \mathcal{O} \subsetneq F$;
- para cualquier $z \in F$, $z \in \mathcal{O}$ o $z^{-1} \in \mathcal{O}$.

Un **anillo de valuaciones** del cuerpo de funciones $F/\mathbb{F}_q$ es un anillo $\mathcal{O} \subseteq F$ con las propiedades:

- $\mathbb{F}_q \subsetneq \mathcal{O} \subsetneq F$;
- para cualquier $z \in F$, $z \in \mathcal{O}$ o $z^{-1} \in \mathcal{O}$.

Un **place** P del cuerpo de funciones $F/\mathbb{F}_q$ es el ideal maximal de algún anillo de valuaciones $\mathcal{O}$ de $F/\mathbb{F}_q$.

El cuerpo de funciones racionales $\mathbb{F}_q(x)$

El cuerpo de funciones racionales $\mathbb{F}_q(x)$

- $p(x) \in \mathbb{F}_q[x]$ polinomio mónico irreducible

$$\mathcal{O}_{p(x)} = \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in \mathbb{F}_q[x],\ p(x) \not| g(x) \right\}$$

El cuerpo de funciones racionales $\mathbb{F}_q(x)$

- $p(x) \in \mathbb{F}_q[x]$ polinomio mónico irreducible

$$\mathcal{O}_{p(x)} = \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in \mathbb{F}_q[x],\ p(x) \not| g(x) \right\}$$

$$P_{p(x)} = \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in \mathbb{F}_q[x],\ p(x) | f(x),\ p(x) \not| g(x) \right\}$$

El cuerpo de funciones racionales $\mathbb{F}_q(x)$

- $p(x) \in \mathbb{F}_q[x]$ polinomio mónico irreducible

$$\mathcal{O}_{p(x)} = \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in \mathbb{F}_q[x],\ p(x) \not| g(x) \right\}$$

$$P_{p(x)} = \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in \mathbb{F}_q[x],\ p(x) | f(x),\ p(x) \not| g(x) \right\}$$

- Anillo de valuaciones asociado al place infinito

$$\mathcal{O}_\infty = \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in \mathbb{F}_q[x],\ \deg f(x) \leq \deg g(x) \right\}$$

El cuerpo de funciones racionales $\mathbb{F}_q(x)$

- $p(x) \in \mathbb{F}_q[x]$ polinomio mónico irreducible

$$\mathcal{O}_{p(x)} = \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in \mathbb{F}_q[x],\ p(x) \not| g(x) \right\}$$

$$P_{p(x)} = \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in \mathbb{F}_q[x],\ p(x) | f(x),\ p(x) \not| g(x) \right\}$$

- Anillo de valuaciones asociado al place infinito

$$\mathcal{O}_{\infty} = \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in \mathbb{F}_q[x],\ \deg f(x) \leq \deg g(x) \right\}$$

$$P_{\infty} = \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in \mathbb{F}_q[x],\ \deg f(x) < \deg g(x) \right\}$$

- Si P un place de $F/\mathbb{F}_q$ y $\mathcal{O}_P$ es su anillo valuaciones entonces el cociente $F_P := \mathcal{O}_P/P$ se llama el **cuerpo de clases residuales** de P y es una extensión finita de $\mathbb{F}_q$. (Es cuerpo pues P es ideal maximal)

- Si P un place de $F/\mathbb{F}_q$ y $\mathcal{O}_P$ es su anillo valuaciones entonces el cociente $F_P := \mathcal{O}_P/P$ se llama el **cuerpo de clases residuales** de P y es una extensión finita de $\mathbb{F}_q$. (Es cuerpo pues P es ideal maximal)

- $deg\ P := [F_P : \mathbb{F}_q]$ se llama el **grado** de P.

- Si P un place de $F/\mathbb{F}_q$ y $\mathcal{O}_P$ es su anillo valuaciones entonces el cociente $F_P := \mathcal{O}_P/P$ se llama el **cuerpo de clases residuales** de P y es una extensión finita de $\mathbb{F}_q$. (Es cuerpo pues P es ideal maximal)

- $deg\ P := [F_P : \mathbb{F}_q]$ se llama el **grado** de P.

- Para cada cuerpo de funciones tenemos asociado un número entero no negativo g llamado **género** de $F/\mathbb{F}_q$.

- Si P un place de $F/\mathbb{F}_q$ y $\mathcal{O}_P$ es su anillo valuaciones entonces el cociente $F_P := \mathcal{O}_P/P$ se llama el **cuerpo de clases residuales** de P y es una extensión finita de $\mathbb{F}_q$. (Es cuerpo pues P es ideal maximal)

- $deg\ P := [F_P : \mathbb{F}_q]$ se llama el **grado** de P.

- Para cada cuerpo de funciones tenemos asociado un número entero no negativo g llamado **género** de $F/\mathbb{F}_q$.

- El cuerpo de funciones racionales $\mathbb{F}_q(x)$ tiene género $g = 0$.

- Si P un place de $F/\mathbb{F}_q$ y $\mathcal{O}_P$ es su anillo valuaciones entonces el cociente $F_P := \mathcal{O}_P/P$ se llama el **cuerpo de clases residuales** de P y es una extensión finita de $\mathbb{F}_q$. (Es cuerpo pues P es ideal maximal)

- $deg\ P := [F_P : \mathbb{F}_q]$ se llama el **grado** de P.

- Para cada cuerpo de funciones tenemos asociado un número entero no negativo g llamado **género** de $F/\mathbb{F}_q$.

- El cuerpo de funciones racionales $\mathbb{F}_q(x)$ tiene género $g = 0$.

- El cuerpo de funciones elípticas $F = \mathbb{F}_2(x, y)$ con

$$y^2 + y = f(x) \in \mathbb{F}_2[x] \quad \text{y} \quad \deg f(x) = 3$$

es un cuerpo de funciones con género $g = 1$.

- Un place P se dice que es **racional** si es de grado uno.

- Un place P se dice que es **racional** si es de grado uno.

- Denotamos por $N(F)$ al número de places racionales de $F/\mathbb{F}_q$.

- Un place P se dice que es **racional** si es de grado uno.
- Denotamos por $N(F)$ al número de places racionales de $F/\mathbb{F}_q$.
- Para un entero $g \geq 0$ sea

$$N_q(g) = \text{máx}\left\{ N(F) : \begin{array}{c} F \text{ es un cuerpo de funciones} \\ \text{sobre } \mathbb{F}_q \text{ de género } g \end{array} \right\}$$

- Un place P se dice que es **racional** si es de grado uno.

- Denotamos por $N(F)$ al número de places racionales de $F/\mathbb{F}_q$.

- Para un entero $g \geq 0$ sea

$$N_q(g) = \text{máx}\left\{ N(F) : \begin{array}{c} F \text{ es un cuerpo de funciones} \\ \text{sobre } \mathbb{F}_q \text{ de género } g \end{array} \right\}$$

- La cantidad

$$A(q) := \limsup_{g \to \infty} \frac{N_q(g)}{g}$$

se llama constante de Ihara.

- Observar que si $g(F)$ denota al género de F entonces el Teorema de Hasse-Weil dice que

$$|N(F) - q - 1| \leq 2g(F)\sqrt{q}$$

y por lo tanto

$$N(F) \leq q + 1 + 2g(F)\sqrt{q}.$$

- Observar que si $g(F)$ denota al género de F entonces el Teorema de Hasse-Weil dice que

$$|N(F) - q - 1| \leq 2g(F)\sqrt{q}$$

y por lo tanto

$$N(F) \leq q + 1 + 2g(F)\sqrt{q}.$$

- Esta cota implica inmediatamente que

$$A(q) \leq 2\sqrt{q}.$$

- Observar que si $g(F)$ denota al género de F entonces el Teorema de Hasse-Weil dice que

$$|N(F) - q - 1| \leq 2g(F)\sqrt{q}$$

y por lo tanto

$$N(F) \leq q + 1 + 2g(F)\sqrt{q}.$$

- Esta cota implica inmediatamente que

$$A(q) \leq 2\sqrt{q}.$$

- Basados en ideas de Ihara, esta cota fue mejorada por Drinfeld-Vladut quienes mostraron que:

$$A(q) \leq \sqrt{q} - 1.$$

Qué sabemos de $A(q)$

Qué sabemos de $A(q)$

- $A(q) > 0$ para todas las potencias $q = p^e$ con p primo y $e \geq 1$.

Qué sabemos de $A(q)$

- $A(q) > 0$ para todas las potencias $q = p^e$ con p primo y $e \geq 1$.
- (Serre) Existe una constante $c > 0$ tal que $A(q) \geq c \cdot \log q$ para todo q.

Qué sabemos de $A(q)$

- $A(q) > 0$ para todas las potencias $q = p^e$ con p primo y $e \geq 1$.
- (Serre) Existe una constante $c > 0$ tal que $A(q) \geq c \cdot \log q$ para todo q.
- (Ihara, Tsfasman-Vladut-Zink) Si $l = q^2$ es un cuadrado entonces $A(l) \geq \sqrt{l} - 1$. Por lo tanto $A(l) = \sqrt{l} - 1$.

Qué sabemos de $A(q)$

- $A(q) > 0$ para todas las potencias $q = p^e$ con p primo y $e \geq 1$.
- (Serre) Existe una constante $c > 0$ tal que $A(q) \geq c \cdot \log q$ para todo q.
- (Ihara, Tsfasman-Vladut-Zink) Si $l = q^2$ es un cuadrado entonces $A(l) \geq \sqrt{l} - 1$. Por lo tanto $A(l) = \sqrt{l} - 1$.
- (Zink, Bezerra-García-Stichtenoth) Si $l = q^3$ es un cubo entonces $A(l) \geq 2(q^2 - 1)/(q + 2)$.

Qué sabemos de $A(q)$

- $A(q) > 0$ para todas las potencias $q = p^e$ con p primo y $e \geq 1$.
- (Serre) Existe una constante $c > 0$ tal que $A(q) \geq c \cdot \log q$ para todo q.
- (Ihara, Tsfasman-Vladut-Zink) Si $l = q^2$ es un cuadrado entonces $A(l) \geq \sqrt{l} - 1$. Por lo tanto $A(l) = \sqrt{l} - 1$.
- (Zink, Bezerra-García-Stichtenoth) Si $l = q^3$ es un cubo entonces $A(l) \geq 2(q^2 - 1)/(q + 2)$.
- Si l no es un cuadrado no se conoce el valor exacto de $A(l)$.

Una manera alternativa de obtener cotas inferiores para la constante de Ihara es a través de la construcción de torres explícitas de cuerpos de funciones sobre $\mathbb{F}_q$.

Una **torre de cuerpos de funciones sobre** $\mathbb{F}_q$ es una sucesión infinita $\mathcal{F} = (F_0, F_1, F_2, \ldots)$ de cuerpos de funciones $F_i/\mathbb{F}_q$ tales que:

Una **torre de cuerpos de funciones sobre $\mathbb{F}_q$** es una sucesión infinita $\mathcal{F} = (F_0, F_1, F_2, \ldots)$ de cuerpos de funciones $F_i/\mathbb{F}_q$ tales que:

- $F_0 \subsetneq F_1 \subsetneq F_2 \subsetneq \cdots \subsetneq F_i \subsetneq \cdots$;

Una **torre de cuerpos de funciones sobre $\mathbb{F}_q$** es una sucesión infinita $\mathcal{F} = (F_0, F_1, F_2, \ldots)$ de cuerpos de funciones $F_i/\mathbb{F}_q$ tales que:

- $F_0 \subsetneq F_1 \subsetneq F_2 \subsetneq \cdots \subsetneq F_i \subsetneq \cdots$;
- cada extensión F_{i+1}/F_i es finita y separable;

Una **torre de cuerpos de funciones sobre $\mathbb{F}_q$** es una sucesión infinita $\mathcal{F} = (F_0, F_1, F_2, \ldots)$ de cuerpos de funciones $F_i/\mathbb{F}_q$ tales que:

- $F_0 \subsetneq F_1 \subsetneq F_2 \subsetneq \cdots \subsetneq F_i \subsetneq \cdots$;
- cada extensión F_{i+1}/F_i es finita y separable;
- el género satisface que $g(F_i) \to \infty$ para $i \to \infty$;

Una **torre de cuerpos de funciones sobre $\mathbb{F}_q$** es una sucesión infinita $\mathcal{F} = (F_0, F_1, F_2, \ldots)$ de cuerpos de funciones $F_i/\mathbb{F}_q$ tales que:

- $F_0 \subsetneq F_1 \subsetneq F_2 \subsetneq \cdots \subsetneq F_i \subsetneq \cdots$;
- cada extensión F_{i+1}/F_i es finita y separable;
- el género satisface que $g(F_i) \to \infty$ para $i \to \infty$;
- $\mathbb{F}_q$ es el cuerpo total de constantes de F_i, para todo $i \geq 0$.

Una **torre de cuerpos de funciones sobre** $\mathbb{F}_q$ es una sucesión infinita $\mathcal{F} = (F_0, F_1, F_2, \ldots)$ de cuerpos de funciones $F_i/\mathbb{F}_q$ tales que:

- $F_0 \subsetneq F_1 \subsetneq F_2 \subsetneq \cdots \subsetneq F_i \subsetneq \cdots$;
- cada extensión F_{i+1}/F_i es finita y separable;
- el género satisface que $g(F_i) \to \infty$ para $i \to \infty$;
- $\mathbb{F}_q$ es el cuerpo total de constantes de F_i, para todo $i \geq 0$.

Por explícita entendemos una torre $\mathcal{F} = (F_0, F_1, F_2, \ldots)$ donde cada cuerpo de funciones F_i está dado por ecuaciones polinómicas explícitas.

Se puede demostrar que el **límite de la torre**

$$\lambda(\mathcal{F}) := \lim_{n\to\infty} \frac{N(F_n)}{g(F_n)}$$

siempre existe, y además

$$0 \leq \lambda(\mathcal{F}) \leq A(q).$$

Se puede demostrar que el **límite de la torre**

$$\lambda(\mathcal{F}) := \lim_{n\to\infty} \frac{N(F_n)}{g(F_n)}$$

siempre existe, y además

$$0 \leq \lambda(\mathcal{F}) \leq A(q).$$

La torre $\mathcal{F}$ se dice que es **asintóticamente buena** si tiene límite positivo $\lambda(\mathcal{F}) > 0$. Si $\lambda(\mathcal{F}) = 0$ entonces se dice que $\mathcal{F}$ es **asintóticamente mala.**

Qué nos interesa (Y qué hicimos..)

Qué nos interesa (Y qué hicimos..)

- Dar condiciones para definir una torre recursiva de cuerpos de funciones.

Qué nos interesa (Y qué hicimos..)

- Dar condiciones para definir una torre recursiva de cuerpos de funciones.
- Dar condiciones para estimar el número de places racionales en la torre.

Qué nos interesa (Y qué hicimos..)

- Dar condiciones para definir una torre recursiva de cuerpos de funciones.
- Dar condiciones para estimar el número de places racionales en la torre.
- Dar condiciones para acotar superiormente el género en torres moderadas.

Qué nos interesa (Y qué hicimos..)

- Dar condiciones para definir una torre recursiva de cuerpos de funciones.
- Dar condiciones para estimar el número de places racionales en la torre.
- Dar condiciones para acotar superiormente el género en torres moderadas.
- Buscar ejemplos

Torres recursivas

Sean $a(Y) \in \mathbb{F}_q(Y)$ y $b(X) \in \mathbb{F}_q(X)$ funciones racionales no constantes, y sea $\mathcal{F} = (F_0, F_1, F_2, \dots)$ una sucesión de cuerpos de funciones sobre $\mathbb{F}_q$. Supongamos que existen $x_i \in F_i$ para $i = 0, 1, 2, \dots$ tales que

(i) x_0 es trascendente sobre $\mathbb{F}_q$ y $F_0 = \mathbb{F}_q(x_0)$; es decir, F_0 es el cuerpo de funciones racionales.

(ii) $F_i = \mathbb{F}_q(x_0, x_1, \dots, x_i)$ para todo $i \geq 0$.

(iii) Para todo $i \geq 0$, los elementos x_i y x_{i+1} satisfacen $a(x_{i+1}) = b(x_i)$.

(iv) $[F_1 : F_0] = \deg a(y)$.

Entonces $\mathcal{F}$ es una sucesión **recursiva** sobre $\mathbb{F}_q$ definida por la ecuación

$$a(Y) = b(X).$$

Teorema: Condiciones para estimar el número de places racionales

Teorema: Condiciones para estimar el número de places racionales

Consideremos la sucesión $\mathcal{F} = (F_0, F_1, F_2, \ldots)$ sobre $\mathbb{F}_q$ definida recursivamente por $a(Y) = b(X)$ donde $a(T), b(T) \in \mathbb{F}_q(T)$ y $\deg a(T) = \deg b(T) = d$. Supongamos que existe $\phi(T) \in \mathbb{F}_q[T]$ tal que:

Teorema: Condiciones para estimar el número de places racionales

Consideremos la sucesión $\mathcal{F} = (F_0, F_1, F_2, \ldots)$ sobre $\mathbb{F}_q$ definida recursivamente por $a(Y) = b(X)$ donde $a(T), b(T) \in \mathbb{F}_q(T)$ y $\deg a(T) = \deg b(T) = d$. Supongamos que existe $\phi(T) \in \mathbb{F}_q[T]$ tal que:

(i) $A = \{\gamma \in \bar{\mathbb{F}}_q \, : \, \phi(a(\gamma)) = 0\} \subset \mathbb{F}_q$

Teorema: Condiciones para estimar el número de places racionales

Consideremos la sucesión $\mathcal{F} = (F_0, F_1, F_2, \ldots)$ sobre $\mathbb{F}_q$ definida recursivamente por $a(Y) = b(X)$ donde $a(T), b(T) \in \mathbb{F}_q(T)$ y $\deg a(T) = \deg b(T) = d$. Supongamos que existe $\phi(T) \in \mathbb{F}_q[T]$ tal que:

(i) $A = \{\gamma \in \bar{\mathbb{F}}_q \ : \ \phi(a(\gamma)) = 0\} \subset \mathbb{F}_q$

(ii) $\phi(b(\gamma)) = 0$ para todo $\gamma \in A$.

Teorema: Condiciones para estimar el número de places racionales

Consideremos la sucesión $\mathcal{F} = (F_0, F_1, F_2, \ldots)$ sobre $\mathbb{F}_q$ definida recursivamente por $a(Y) = b(X)$ donde $a(T), b(T) \in \mathbb{F}_q(T)$ y $\deg a(T) = \deg b(T) = d$. Supongamos que existe $\phi(T) \in \mathbb{F}_q[T]$ tal que:

(i) $A = \{\gamma \in \bar{\mathbb{F}}_q : \phi(a(\gamma)) = 0\} \subset \mathbb{F}_q$

(ii) $\phi(b(\gamma)) = 0$ para todo $\gamma \in A$.

(iii) $\sigma(T) = \pm(a_1(T) - a_2(T)b(x_i))$ es el polinomio mínimo de x_{i+1} sobre F_i para todo $i > 0$, $\sigma(T)$ es separable y $\deg \sigma(T) \geq 2$.

Teorema: Condiciones para estimar el número de places racionales

Consideremos la sucesión $\mathcal{F} = (F_0, F_1, F_2, \ldots)$ sobre $\mathbb{F}_q$ definida recursivamente por $a(Y) = b(X)$ donde $a(T), b(T) \in \mathbb{F}_q(T)$ y $\deg a(T) = \deg b(T) = d$. Supongamos que existe $\phi(T) \in \mathbb{F}_q[T]$ tal que:

(i) $A = \{\gamma \in \bar{\mathbb{F}}_q : \phi(a(\gamma)) = 0\} \subset \mathbb{F}_q$

(ii) $\phi(b(\gamma)) = 0$ para todo $\gamma \in A$.

(iii) $\sigma(T) = \pm(a_1(T) - a_2(T)b(x_i))$ es el polinomio mínimo de x_{i+1} sobre F_i para todo $i > 0$, $\sigma(T)$ es separable y $\deg \sigma(T) \geq 2$.

(iv) Para todo $\gamma \in A$ el polinomio $a_1(T) - a_2(T)b(\gamma)$ tiene d raíces simples.

Teorema: Condiciones para estimar el número de places racionales

Consideremos la sucesión $\mathcal{F} = (F_0, F_1, F_2, \ldots)$ sobre $\mathbb{F}_q$ definida recursivamente por $a(Y) = b(X)$ donde $a(T), b(T) \in \mathbb{F}_q(T)$ y $\deg a(T) = \deg b(T) = d$. Supongamos que existe $\phi(T) \in \mathbb{F}_q[T]$ tal que:

(i) $A = \{\gamma \in \bar{\mathbb{F}}_q : \phi(a(\gamma)) = 0\} \subset \mathbb{F}_q$

(ii) $\phi(b(\gamma)) = 0$ para todo $\gamma \in A$.

(iii) $\sigma(T) = \pm(a_1(T) - a_2(T)b(x_i))$ es el polinomio mínimo de x_{i+1} sobre F_i para todo $i > 0$, $\sigma(T)$ es separable y $\deg \sigma(T) \geq 2$.

(iv) Para todo $\gamma \in A$ el polinomio $a_1(T) - a_2(T)b(\gamma)$ tiene d raíces simples.

Entonces

$$N(F_i) \geq [F_i : F_0] \cdot |A|.$$

Observación

Observación

Si en lugar de (iii) y (iv) tenemos

(iii') $\sigma(T) = \pm\left(\frac{1}{b(x_i)}a_1(T) - a_2(T)\right)$ es el polinomio mínimo de x_{i+1} sobre F_i para todo $i > 0$, $\sigma(T)$ es separable y $\deg\sigma(T) \geq 2$.

(iv') Para todo $\gamma \in A$, $b(\gamma) \neq 0$ y el polinomio $\frac{1}{b(\gamma)}a_1(T) - a_2(T)$ tiene d raíces distintas.

Entonces el teorema también vale.

Observación

Si en lugar de (iii) y (iv) tenemos

(iii') $\sigma(T) = \pm\left(\frac{1}{b(x_i)}a_1(T) - a_2(T)\right)$ es el polinomio mínimo de x_{i+1} sobre F_i para todo $i > 0$, $\sigma(T)$ es separable y $\deg\sigma(T) \geq 2$.

(iv') Para todo $\gamma \in A$, $b(\gamma) \neq 0$ y el polinomio $\frac{1}{b(\gamma)}a_1(T) - a_2(T)$ tiene d raíces distintas.

Entonces el teorema también vale.

Notar que si $\phi(0) \neq 0$ entonces $b(\gamma) \neq 0$ para todo $\gamma \in A$ por (ii) con lo cual en lugar de (iv') se puede pedir

(iv'') $\phi(0) \neq 0$ y para todo $\gamma \in A$, el polinomio $\frac{1}{b(\gamma)}a_1(T) - a_2(T)$ tiene d raíces distintas.

Ejemplo: Torre BGS de Bezerra-García-Stichtenoth

Sea q una potencia de un primo y consideremos el cuerpo finito $\mathbb{F}_l$ con $l = q^3$. La torre BGS $\mathcal{G} = (G_0, G_1, G_2, \ldots)$ está definida recursivamente por la ecuación

$$\frac{1-y}{y^q} = \frac{x^q + x - 1}{x}.$$

En este caso tenemos que

$$a(T) = \frac{1-T}{T^q} \qquad \text{y} \qquad b(T) = \frac{T^q + T - 1}{T}.$$

Sea

$$\phi(T) = T^{q+1} - T + 1.$$

Se puede probar que

$$T^{q^2+q}\,\phi(a(T)) = T^{q+1}\,\phi(b(T)) = (1-T)^{q^2+q+1} + T^{q^2+q+1},$$

$A \subset \mathbb{F}_l$ y $|A| = q(q+1)$. Por lo tanto se cumplen las condiciones (i) y (ii). La condición (iii') se cumple por la forma en que está definida la torre y el hecho de que todas las extensiones satisfacen $[G_i : G_0] = q^i$ para todo $i \geq 0$.

Finalmente veamos que se cumple (iv'').

Como $\phi(0) \neq 0$ sólo tenemos que probar que $\bar{\sigma}(T) = \frac{1}{b(\gamma)}(1 - T) - T^q$ tiene q raíces distintas y esto se ve fácilmente observando que su derivada $\bar{\sigma}'(T) = \frac{-1}{b(\gamma)}$ no tiene raíces en común con $\bar{\sigma}(T)$.

Luego, como se cumplen todas las condiciones del Teorema, tenemos que

$$N(G_i) \geq [G_i : G_0] \cdot |A| = q^i \cdot q(q+1) = q^{i+1}(q+1).$$

Ejemplo: Caso particular de la torre GS de García-Stichtenoth

Considerar la torre $\mathcal{E} = (E_0, E_1, E_2, \ldots)$ de cuerpos de funciones sobre $\mathbb{F}_9$ definida por la ecuación

$$y^2 = \frac{x^2 + 1}{2x}.$$

En este caso tenemos que

$$a(T) = T^2, \qquad \text{y} \qquad b(T) = \frac{T^2 + 1}{2T}.$$

Sea

$$\phi(T) = T^2 + 1.$$

Se puede verificar que

$$\phi(a(T)) = T^2\,\phi(b(T)) = (T^2 + 2T + 2)(T^2 + T + 2).$$

Representamos al cuerpo $\mathbb{F}_9$ como $\mathbb{F}_9 = \mathbb{F}_3(\alpha)$ con $\alpha^2 = 2\alpha + 1$ y por lo tanto

$$\mathbb{F}_9 = \{0,\ 1,\ 2,\ \alpha,\ \alpha+1,\ \alpha+2,\ 2\alpha,\ 2\alpha+1,\ 2\alpha+2\}.$$

Entonces tenemos que

$$A = \{\gamma \in \bar{\mathbb{F}}_9 \ :\ \phi(a(\gamma)) = 0\} = \{\alpha,\ \alpha+1,\ 2\alpha,\ 2\alpha+2\} \subset \mathbb{F}_9.$$

Esto nos asegura que se cumplen las condiciones (i) y (ii). La condición (iii) vale por la forma en que está definida la torre.

Veamos que se cumple la condición (iv).

En este caso el polinomio que tenemos que estudiar es

$$\bar{\sigma}(T) = a(T) - b(\gamma) = T^2 - b(\gamma)$$

para todo $\gamma \in A$, y su derivada es

$$\bar{\sigma}'(T) = 2T.$$

Entonces hay que probar que $b(\gamma) \neq 0$ para todo $\gamma \in A$.

Calculemos entonces $b(\gamma)$ para todo los $\gamma \in A$.

- $b(\alpha) = \alpha + 2$
- $b(\alpha + 1) = \alpha + 2$
- $b(2\alpha) = 2\alpha + 1$
- $b(2\alpha + 2) = 2\alpha + 1$

y por lo tanto el polinomio $a(T) - b(\gamma) = T^2 - b(\gamma)$ tiene 2 raíces simples y el teorema arroja los mismos resultados que los obtenidos por G-S.

Ejemplo: La torre de var der Geer y van der Vlugt

Consideremos la torre $\mathcal{H} = (H_0, H_1, H_2, \ldots)$ de cuerpos de funciones sobre $\mathbb{F}_8$ definida recursivamente por

$$y^2 + y = \frac{x^2 + x + 1}{x}.$$

Esta torre fue considerada por var der Geer y van der Vlugt, quienes calcularon explícitamente el género y la cantidad de places racionales en cada paso de la torre y obtuvieron que

$$N(H_i) = 6 \cdot 2^i + 2$$

para todo $i \geq 0$.

En este caso usando que

$$a(T) = T^2 + T, \qquad \text{y} \qquad b(T) = \frac{T^2 + T + 1}{T},$$

considerando

$$\phi(T) = T^3 + T + 1$$

y representando al cuerpo $\mathbb{F}_8$ como $\mathbb{F}_8 = \mathbb{F}_2(\alpha)$ con $\alpha^3 = \alpha + 1$ tenemos que

$$\mathbb{F}_8 = \{0, 1, \alpha, \alpha + 1, \alpha^2, \alpha^2 + 1, \alpha^2 + \alpha, \alpha^2 + \alpha + 1\};$$

y el teorema se cumple con

$$A = \mathbb{F}_8 \setminus \mathbb{F}_2.$$

Luego

$$N(H_i) \geq 6 \cdot 2^i$$

para todo $i \geq 0$.

Ejemplo

Sea $m \geq 2$ y q una potencia de un primo de manera que $\mathbb{F}_q$ contenga al cuerpo de descomposición del polinomio $T^m + \alpha$ para algún $\alpha \in \mathbb{F}_q$ y tal que $\text{mcd}(m, \mathit{char}\, \mathbb{F}_q) = 1$.
Consideremos la sucesión $\mathcal{F} = (F_0, F_1, F_2, \ldots)$ de cuerpos de funciones sobre $\mathbb{F}_q$ definida recursivamente por la ecuación

$$y^m = \frac{x^m - \alpha f(x) + \alpha}{f(x)},$$

donde $f(T) \in \mathbb{F}_q[T]$ es un polinomio separable de grado $m - r$ con $\text{mcd}(m, r) = 1$.

Estas torres se dicen que son de tipo Kummer.

En este caso tenemos que

$$a(T) = T^m, \qquad \text{y} \qquad b(T) = \frac{T^m - \alpha f(T) + \alpha}{f(T)}.$$

Con

$$\phi(T) = T + \alpha$$

tenemos que

$$\phi(a(T)) = a(T) + \alpha = T^m + \alpha$$

y

$$\phi(b(T)) = b(T) + \alpha = \frac{T^m - \alpha f(T) + \alpha}{f(T)} + \alpha = \frac{T^m + \alpha}{f(T)}.$$

Como la torre está definida sobre el cuerpo de descomposición de $\phi(a(T))$, y el polinomio

$$\bar{\sigma}(T) = T^m - b(\gamma)$$

tiene m raíces distintas, entonces se cumplen las condiciones del Teorema y tenemos que para todo $i \geq 0$, el número de places racionales de F_i/F_0 satisface

$$N(F_i) \geq m^{i+1}.$$

Torres moderadas

Sea $\mathbb{P}(F)$ el conjunto de todos los places de un cuerpo de funciones $F/\mathbb{F}_q$.

Torres moderadas

Sea $\mathbb{P}(F)$ el conjunto de todos los places de un cuerpo de funciones $F/\mathbb{F}_q$.

- Dada una extensión E/F, un place $P \in \mathbb{P}(F)$ y $Q \in \mathbb{P}(E)$ decimos que Q divide a P o que Q está arriba de P si $P \subset Q$ y lo denotamos $Q|P$.

Torres moderadas

Sea $\mathbb{P}(F)$ el conjunto de todos los places de un cuerpo de funciones $F/\mathbb{F}_q$.

- Dada una extensión E/F, un place $P \in \mathbb{P}(F)$ y $Q \in \mathbb{P}(E)$ decimos que Q divide a P o que Q está arriba de P si $P \subset Q$ y lo denotamos $Q|P$.

- Para cada $P \in \mathbb{P}(F)$, existe una cantidad finita de places $P' \in \mathbb{P}(E)$ que están arriba de P.

Torres moderadas

Sea $\mathbb{P}(F)$ el conjunto de todos los places de un cuerpo de funciones $F/\mathbb{F}_q$.

- Dada una extensión E/F, un place $P \in \mathbb{P}(F)$ y $Q \in \mathbb{P}(E)$ decimos que Q divide a P o que Q está arriba de P si $P \subset Q$ y lo denotamos $Q|P$.

- Para cada $P \in \mathbb{P}(F)$, existe una cantidad finita de places $P' \in \mathbb{P}(E)$ que están arriba de P.

- El índice de ramificación de $Q|P$ se define como el único entero tal que

$$v_Q(x) = e(Q|P) \cdot v_P(x)$$

para todo $x \in F$.

Torres moderadas

Torres moderadas

- Si $e(Q|P) > 1$ decimos que $Q|P$ **ramifica**. Si $e(Q|P) = 1$ decimos que $Q|P$ **no ramifica**.

Torres moderadas

- Si $e(Q|P) > 1$ decimos que $Q|P$ **ramifica**. Si $e(Q|P) = 1$ decimos que $Q|P$ **no ramifica**.

- La extensión E/F se dice **moderada** si $e(Q|P)$ es coprimo con la característica de $\mathbb{F}_q$, para todos los places $P \in \mathbb{P}(F)$ y todo $Q|P$.

Torres moderadas

- Si $e(Q|P) > 1$ decimos que $Q|P$ **ramifica**. Si $e(Q|P) = 1$ decimos que $Q|P$ **no ramifica**.
- La extensión E/F se dice **moderada** si $e(Q|P)$ es coprimo con la característica de $\mathbb{F}_q$, para todos los places $P \in \mathbb{P}(F)$ y todo $Q|P$.
- Una **torre** se dice que es **moderada** si todas las extensiones F_{i+1}/F_i son moderadas para todo $i \geq 0$.

Teorema de García-Stichtenoth-Thomas para torres moderadas

Sea $\mathcal{F} = (F_0, F_1, F_2, \ldots)$ una torre sobre $\mathbb{F}_q$ tal que:

(i) Todas las extensiones F_{n+1}/F_n son moderadas.

(ii) $S = \{P \in \mathbb{P}(F_0) | P$ es ramificado en F_n/F_0 para algún $n \geq 1\}$ es finito.

(iii) $T = \{P \in \mathbb{P}(F_0) | \deg P = 1,$ y P se descom. compl. en la torre$\}$ es no vacío.

Entonces $\mathcal{F}$ es asintóticamente buena, y se obtiene que

$$\lambda(\mathcal{F}) \geq \frac{2t}{2g(F_0) - 2 + s} > 0,$$

donde $t := \#T$ y $s := \sum_{P \in S} \deg P$.

Teorema

Sea $\mathcal{F} = (F_0, F_1, F_2, \dots)$ una torre de cuerpos de funciones sobre $\mathbb{F}_q$ definida recursivamente por la ecuación

$$y^m = \frac{b_1(x)}{b_2(x)}$$

con $b_1(T)$, $b_2(T) \in \mathbb{F}_q[T]$, $\deg b_1(T) = m$, $\deg b_2(T) = m - r$ y $\mathrm{mcd}(m, r) = 1$. Supongamos que existe un subconjunto S_0 de $\mathbb{F}_q$ tal que:

(i) $0 \in S_0$;

(ii) para todo $\beta \in \bar{\mathbb{F}}_q$ tal que $b_2(\beta) = 0$ se tiene que $\beta \in S_0$; y

(iii) para todo $\alpha \in S_0$, si $b_2(\beta)\alpha^m - b_1(\beta) = 0$ entonces $\beta \in S_0$.

Entonces la torre $\mathcal{F}$ tiene un espacio de ramificación finito. Más aún, si $P \in \mathbb{P}(F_0)$ es un place ramificado en la torre entonces $P = P_\infty$ es el polo de x_0 en F_0 o P es un cero de $x_0 - \alpha$ para algún $\alpha \in S_0$.

Ejemplo

Sea $m \geq 2$ y q una potencia de un primo de manera que $\mathbb{F}_q$ contenga al cuerpo de descomposición del polinomio $T^m + \alpha$ para algún $\alpha \in \mathbb{F}_q$ y tal que $\text{mcd}(m, \mathit{char}\, \mathbb{F}_q) = 1$.
Consideremos la sucesión $\mathcal{F} = (F_0, F_1, F_2, \ldots)$ de cuerpos de funciones sobre $\mathbb{F}_q$ definida recursivamente por la ecuación

$$y^m = \frac{x^m - \alpha f(x) + \alpha}{f(x)},$$

donde $f(T) \in \mathbb{F}_q[T]$ es un polinomio separable de grado $m - r$ con $\text{mcd}(m, r) = 1$.

Ejemplo

En particular si consideramos $m = 2$, $q = 9$ y $f(x) = x$ tenemos que $\mathcal{G} = (G_0, G_1, \ldots)$ es una torre sobre $\mathbb{F}_9$ definida recursivamente por la ecuación

$$y^2 = \frac{x^2 - x + 1}{x}.$$

$S_0 = \{0, 1, 2\} \subset \mathbb{F}_9$ donde $\mathbb{F}_9 = \mathbb{F}_3(\alpha)$ con $\alpha^2 + \alpha + 2$ satisface las hipótesis del Teorema y por lo tanto el espacio de ramificación de la torre $\mathcal{G}$ es finito y está contenido en el conjunto $\{(x_0 = 0), (x_0 = 1), (x_0 = 2), (x_0 = \infty)\}$. Utilizando el Teorema de G.S.T., tenemos que

$$\lambda(\mathcal{G}) \geq \frac{4}{4 - 2} = 2$$

y como sabemos que

$$\lambda(\mathcal{G}) \leq \sqrt{9} - 1 = 2$$

entonces la torre $\mathcal{G}$ es asintóticamente óptima sobre $\mathbb{F}_9$ y $\lambda(\mathcal{G}) = 2$.

Ejemplo

Si consideramos $m = 2$, $q = 9$, $\mathbb{F}_9 = \mathbb{F}_3(\alpha)$ con $\alpha^2 + \alpha + 2 = 0$ y $f(x) = x + 1$ tenemos que $\mathcal{H} = (H_0, H_1, \ldots)$ es una torre de cuerpos de funciones sobre $\mathbb{F}_9$ definida recursivamente por la ecuación

$$y^2 = \frac{x(x-1)}{x+1}.$$

En este caso,

$$S_0 = \{0, 1, 2, \alpha, \alpha^3, \alpha^5, \alpha^7\}$$

satisface las hipótesis del Teorema. Luego, $\mathcal{H}$ es una torre asintóticamente buena sobre $\mathbb{F}_9$ y tenemos que

$$\lambda(\mathcal{H}) \geq \frac{2}{3}.$$

Ejemplo, una torre sobre $\mathbb{F}_{25}$

Escribimos $\mathbb{F}_{25} = \mathbb{F}_5(\alpha)$ con $\alpha^2 + \alpha + 2 = 0$. Consideremos la torre $\mathcal{I} = (I_0, I_1, \ldots)$ sobre $\mathbb{F}_{25}$ definida por

$$y^2 = \frac{x^2 - f(x) + 1}{f(x)}, \tag{1}$$

con $f(x) = \alpha^9 x + 1$. Como $\mathbb{F}_{25}$ contiene al cuerpo de descomposición de $T^2 + 1$, tenemos que

$$\nu(\mathcal{I}/I_0) \geq 2.$$

$S_0 = \{0, \alpha^3, \alpha^9, \alpha^{15}, \alpha^{21}\} \subset \mathbb{F}_{25}$ satisface las condiciones del Teorema.
Entonces $|\mathrm{Ram}(\mathcal{I}/I_0)| \leq 6$ y por el Teorema de G.S.T. tenemos que

$$\lambda(\mathcal{I}) \geq \frac{2 \cdot 2}{6 - 2} = 1$$

y por lo tanto la torre $\mathcal{I}$ es asintóticamente buena sobre $\mathbb{F}_{25}$.

Observar que la torre $\mathcal{I}$ puede escribirse también como la torre recursiva sobre $\mathbb{F}_{25}$ generada por la ecuación

$$y^2 = \frac{x^2 - f(x) + 1}{f(x)},$$

con $f(x) = \alpha^{21}x + 1$, utilizando el cambio de variables $X = 2x$, $Y = 2y$.

Ejemplo, una torre sobre $\mathbb{F}_{81}$

Escribimos $\mathbb{F}_{81} = \mathbb{F}_3(\alpha)$ con $\alpha^4 + 2\alpha + 2 = 0$. Consideremos la torre $\mathcal{J} = (J_0, J_1, \ldots)$ sobre $\mathbb{F}_{81}$ definida por

$$y^2 = \frac{x^2 - f(x) + 1}{f(x)}, \tag{2}$$

con $f(x) = \alpha^5 x + \alpha^{10}$. Como $\mathbb{F}_{81}$ contiene al cuerpo de descomposición de $T^2 + 1$, tenemos que

$$\nu(\mathcal{J}/J_0) \geq 2.$$

$S_0 = \{0, \alpha^5, \alpha^{15}, \alpha^{25}, \alpha^{35}, \alpha^{45}, \alpha^{55}, \alpha^{65}, \alpha^{75}, \} \subset \mathbb{F}_{81}$ satisface las condiciones del Teorema. Entonces $|\mathrm{Ram}(\mathcal{J}/J_0)| \leq 10$ y

$$\lambda(\mathcal{J}/J_0) \geq \frac{2 \cdot 2}{10 - 2} = \frac{1}{2}.$$

Luego la torre $\mathcal{J}$ es asintóticamente buena sobre $\mathbb{F}_{81}$.

La torre $\mathcal{J}$ puede definirse también utilizando $f(x) = \alpha^{45}x + \alpha^{10}$. Utilizando el cambio de variables $X = 2x$, $Y = 2y$ se muestra que ambas ecuaciones definen la misma torre sobre $\mathbb{F}_{81}$.

La torre $\mathcal{J}$ puede definirse también utilizando $f(x) = \alpha^{45}x + \alpha^{10}$. Utilizando el cambio de variables $X = 2x$, $Y = 2y$ se muestra que ambas ecuaciones definen la misma torre sobre $\mathbb{F}_{81}$.

Los mismos resultados se obtienen utilizando $f(x) = \alpha^{15}x + \alpha^{30}$ y $f(x) = \alpha^{55}x + \alpha^{30}$. Sin embargo, hasta el momento no pudimos demostrar si las torres generadas por estas ecuaciones coinciden con las del ejemplo o no.

GRACIAS!!