Cuestiones asintóticas de torres y códigos

R. Toledano

Universidad Nacional del Litoral e Instituto de Matemática Aplicada del Litoral

FaMAF (CBA) 2017

Códigos lineales

Sea $\mathbb{F}_q$ un cuerpo finito con q elementos. Un [n,k]-código sobre $\mathbb{F}_q$ de longitud n es un $\mathbb{F}_q$-subespacio vectorial $\mathcal{C}$ de $\mathbb{F}_q^n$ de dimensión k.

Códigos lineales

Sea $\mathbb{F}_q$ un cuerpo finito con q elementos. Un [n,k]-código sobre $\mathbb{F}_q$ de longitud n es un $\mathbb{F}_q$-subespacio vectorial $\mathcal{C}$ de $\mathbb{F}_q^n$ de dimensión k.

La distancia de Hamming en $\mathbb{F}_q^n$ se define como

$$d(\mathbf{x}, \mathbf{y}) = \#\{i : x_i \neq y_i\}$$

donde $\mathbf{x} = (x_1, \ldots, x_n)$ e $\mathbf{y} = (y_1, \ldots, y_n)$

Códigos lineales

Sea $\mathbb{F}_q$ un cuerpo finito con q elementos. Un [n,k]-código sobre $\mathbb{F}_q$ de longitud n es un $\mathbb{F}_q$-subespacio vectorial $\mathcal{C}$ de $\mathbb{F}_q^n$ de dimensión k.

La distancia de Hamming en $\mathbb{F}_q^n$ se define como

$$d(\mathbf{x}, \mathbf{y}) = \#\{i : x_i \neq y_i\}$$

donde $\mathbf{x} = (x_1, \ldots, x_n)$ e $\mathbf{y} = (y_1, \ldots, y_n)$

Un [n,k,d]-código sobre $\mathbb{F}_q$ es un [n,k]-código $\mathcal{C}$ sobre $\mathbb{F}_q$ con distancia mínima d, i.e.

$$d = \min\{d(\mathbf{x}, \mathbf{y}) : \mathbf{x} \neq \mathbf{y} \in \mathcal{C}\}$$

Códigos lineales

Sea $\mathbb{F}_q$ un cuerpo finito con q elementos. Un [n,k]-código sobre $\mathbb{F}_q$ de longitud n es un $\mathbb{F}_q$-subespacio vectorial $\mathcal{C}$ de $\mathbb{F}_q^n$ de dimensión k.

La distancia de Hamming en $\mathbb{F}_q^n$ se define como

$$d(\mathbf{x}, \mathbf{y}) = \#\{i : x_i \neq y_i\}$$

donde $\mathbf{x} = (x_1, \ldots, x_n)$ e $\mathbf{y} = (y_1, \ldots, y_n)$

Un [n,k,d]-código sobre $\mathbb{F}_q$ es un [n,k]-código $\mathcal{C}$ sobre $\mathbb{F}_q$ con distancia mínima d, i.e.

$$d = \min\{d(\mathbf{x}, \mathbf{y}) : \mathbf{x} \neq \mathbf{y} \in \mathcal{C}\}$$

En un [n,k,d]-código sobre $\mathbb{F}_q$ la dimensión k mide la capacidad de transmisión de información del código mientras que la distancia mínima d mide la capacidad de detección y corrección de errores del mismo.

Códigos lineales

Por lo tanto se quiere tener [n,k,d]-códigos con dimensión y distancia mínima lo más grandes posible.

Códigos lineales

Por lo tanto se quiere tener [n,k,d]-códigos con dimensión y distancia mínima lo más grandes posible.

Sin embargo, hay un balance entre ambos parámetros:

$$\text{(Cota de Singleton)} \quad k + d \leq n + 1$$

Códigos lineales

Por lo tanto se quiere tener [n,k,d]-códigos con dimensión y distancia mínima lo más grandes posible.

Sin embargo, hay un balance entre ambos parámetros:

$$\text{(Cota de Singleton)} \quad k + d \leq n + 1$$

Esto quiere decir que para lograr códigos con altas capacidades de transmisión y detección-corrección de errores hay que considerar códigos de gran longitud.

Códigos lineales

Por lo tanto se quiere tener [n,k,d]-códigos con dimensión y distancia mínima lo más grandes posible.

Sin embargo, hay un balance entre ambos parámetros:

$$\text{(Cota de Singleton)} \quad k + d \leq n + 1$$

Esto quiere decir que para lograr códigos con altas capacidades de transmisión y detección-corrección de errores hay que considerar códigos de gran longitud.

Las cantidades

$$0 \leq R(\mathcal{C}) = \frac{k}{n}, \quad \delta(\mathcal{C}) = \frac{d}{n} \leq 1$$

se denominan tasa de información y distancia mínima relativa respectivamente del código $\mathcal{C}$.

Códigos lineales

Con esta terminología nos preguntamos si dados $0 < \delta, R < 1$ existen códigos sobre $\mathbb{F}_q$ cuyas tasas de información y distancias mínimas relativas se encuentren arbitrariamente cerca de δ y R.

Códigos lineales

Con esta terminología nos preguntamos si dados $0 < \delta, R < 1$ existen códigos sobre $\mathbb{F}_q$ cuyas tasas de información y distancias mínimas relativas se encuentren arbitrariamente cerca de δ y R.

Formalmente se define el conjuntos

$$V_q = \{(\delta(\mathcal{C}), R(\mathcal{C})) \in [0,1]^2 \ : \mathcal{C} \text{ es un código sobre } \mathbb{F}_q\}$$

y nos preguntamos cómo es $U_q \subset [0,1]^2$, el conjunto de los puntos límite de V_q.

Códigos lineales

Con esta terminología nos preguntamos si dados $0 < \delta, R < 1$ existen códigos sobre $\mathbb{F}_q$ cuyas tasas de información y distancias mínimas relativas se encuentren arbitrariamente cerca de δ y R.

Formalmente se define el conjuntos

$$V_q = \{(\delta(\mathcal{C}), R(\mathcal{C})) \in [0,1]^2 \ : \mathcal{C} \text{ es un código sobre } \mathbb{F}_q\}$$

y nos preguntamos cómo es $U_q \subset [0,1]^2$, el conjunto de los puntos límite de V_q.

Teorema (Manin) Existe una función continua y decreciente

$$\alpha_q : [0,1] \to [0,1]$$

tal que

$$U_q = \{(\delta, R) \ : 0 \leq R \leq \alpha_q(\delta)\}$$

y $\alpha_q(0) = 1$ y $\alpha_q(\delta) = 0$ para $1 - q^{-1} \leq \delta \leq 1$.

Códigos lineales

El valor exacto de $\alpha_q(\delta)$ es desconocido para $0 < \delta < 1 - q^{-1}$.
Sólo se conocen cotas inferiores.

Códigos lineales

El valor exacto de $\alpha_q(\delta)$ es desconocido para $0 < \delta < 1 - q^{-1}$.
Sólo se conocen cotas inferiores.

La función q-aria de entropía $H_q \colon [0, 1 - q^{-1}] \to \mathbb{R}$ se define como

$$H_q(x) = x \log_q(q-1) - x \log_q(x) - (1-x) \log_q(1-x)$$

para $x > 0$ y $H_q(0) = 0$.

Códigos lineales

El valor exacto de $\alpha_q(\delta)$ es desconocido para $0 < \delta < 1 - q^{-1}$.
Sólo se conocen cotas inferiores.

La función q-aria de entropía $H_q \colon [0, 1 - q^{-1}] \to \mathbb{R}$ se define como

$$H_q(x) = x \log_q(q-1) - x \log_q(x) - (1-x) \log_q(1-x)$$

para $x > 0$ y $H_q(0) = 0$.

Teorema (Cota de Gilbert-Varshamov)

$$\alpha_q(\delta) \geq 1 - H_q(\delta)$$

para $0 \leq \delta \leq 1 - q^{-1}$.

Códigos lineales

El valor exacto de $\alpha_q(\delta)$ es desconocido para $0 < \delta < 1 - q^{-1}$. Sólo se conocen cotas inferiores.

La función q-aria de entropía $H_q \colon [0, 1 - q^{-1}] \to \mathbb{R}$ se define como

$$H_q(x) = x \log_q(q-1) - x \log_q(x) - (1-x) \log_q(1-x)$$

para $x > 0$ y $H_q(0) = 0$.

Teorema (Cota de Gilbert-Varshamov)

$$\alpha_q(\delta) \geq 1 - H_q(\delta)$$

para $0 \leq \delta \leq 1 - q^{-1}$.

La cota de Gilbert-Varshamov es la mejor cota inferior para $\alpha_q(\delta)$ que se puede obtener desde la teoría elemental de códigos. La demostración no es constructiva.

Códigos asintóticamente buenos

Una sucesión $\{\mathcal{C}_i\}$ de $[n_i,\ k_i,\ d_i]$-códigos sobre $\mathbb{F}_q$ se dice que es asintóticamente buena si

Códigos asintóticamente buenos

Una sucesión $\{\mathcal{C}_i\}$ de $[n_i,\ k_i,\ d_i]$-códigos sobre $\mathbb{F}_q$ se dice que es asintóticamente buena si

$$\liminf_{i\to\infty} \frac{k_i}{n_i} = R > 0 \quad \text{y} \quad \liminf_{i\to\infty} \frac{d_i}{n_i} = \delta > 0$$

Códigos asintóticamente buenos

Una sucesión $\{\mathcal{C}_i\}$ de $[n_i,\ k_i,\ d_i]$-códigos sobre $\mathbb{F}_q$ se dice que es asintóticamente buena si

$$\liminf_{i\to\infty} \frac{k_i}{n_i} = R > 0 \quad \text{y} \quad \liminf_{i\to\infty} \frac{d_i}{n_i} = \delta > 0$$

En este caso tenemos que

$$\alpha_q(\delta) \geq R$$

Códigos asintóticamente buenos

Una sucesión $\{\mathcal{C}_i\}$ de $[n_i,\ k_i,\ d_i]$-códigos sobre $\mathbb{F}_q$ se dice que es asintóticamente buena si

$$\liminf_{i\to\infty} \frac{k_i}{n_i} = R > 0 \quad \text{y} \quad \liminf_{i\to\infty} \frac{d_i}{n_i} = \delta > 0$$

En este caso tenemos que

$$\alpha_q(\delta) \geq R$$

Con la construcción de este tipo de sucesiones se logran códigos de longitud arbitrariamente grande cuyos parámetros relativos se acercan tanto como uno quiera a un punto de acumulacíon de V_q.

Códigos asintóticamente buenos

Una sucesión $\{\mathcal{C}_i\}$ de $[n_i, k_i, d_i]$-códigos sobre $\mathbb{F}_q$ se dice que es asintóticamente buena si

$$\liminf_{i\to\infty} \frac{k_i}{n_i} = R > 0 \quad \text{y} \quad \liminf_{i\to\infty} \frac{d_i}{n_i} = \delta > 0$$

En este caso tenemos que

$$\alpha_q(\delta) \geq R$$

Con la construcción de este tipo de sucesiones se logran códigos de longitud arbitrariamente grande cuyos parámetros relativos se acercan tanto como uno quiera a un punto de acumulacíon de V_q.

Es aquí en donde la teoría de torres de cuerpos de funciones muestra su utilidad para la construcción de tales sucesiones de códigos.

Códigos AG

Sea F un cuerpo de funciones sobre $\mathbb{F}_q$ (i.e. F es una extensión finita del cuerpo de funciones racionales $\mathbb{F}_q(x)$).

Códigos AG

Sea F un cuerpo de funciones sobre $\mathbb{F}_q$ (i.e. F es una extensión finita del cuerpo de funciones racionales $\mathbb{F}_q(x)$).

Para cada entero $g \geq 0$ se define

$$N_q(g) = \max\{N(F) : F \text{ cuerpo de funciones sobre } \mathbb{F}_q \text{ de género } g\}$$

donde $N(F)$ es el número de lugares racionales de F.

Códigos AG

Sea F un cuerpo de funciones sobre $\mathbb{F}_q$ (i.e. F es una extensión finita del cuerpo de funciones racionales $\mathbb{F}_q(x)$).

Para cada entero $g \geq 0$ se define

$$N_q(g) = \max\{N(F) : F \text{ cuerpo de funciones sobre } \mathbb{F}_q \text{ de género } g\}$$

donde $N(F)$ es el número de lugares racionales de F.

La constante de Ihara se define como

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

Códigos AG

Sea F un cuerpo de funciones sobre $\mathbb{F}_q$ (i.e. F es una extensión finita del cuerpo de funciones racionales $\mathbb{F}_q(x)$).

Para cada entero $g \geq 0$ se define

$$N_q(g) = \max\{N(F) : F \text{ cuerpo de funciones sobre } \mathbb{F}_q \text{ de género } g\}$$

donde $N(F)$ es el número de lugares racionales de F.

La constante de Ihara se define como

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

El valor exacto de $A(q)$ es desconocido excepto cuando $q = p^{2n}$:

$$A(p^{2n}) = p^n - 1$$

Códigos AG

Teorema (Tsfasman, Vladut y Zink)

$$\alpha_q(\delta) \geq 1 - \frac{1}{A(q)} - \delta$$

En particular si $q = p^2$ entonces

$$\alpha_q(\delta) \geq 1 - \frac{1}{p-1} - \delta$$

para $0 \leq \delta \leq 1 - (p-1)^{-1}$.

Esta cota supera a la cota de Gilbert-Varshamov en un subintervalo de $[0, 1 - (p-1)^{-1}]$ cuando $p \geq 7$.

Torres de cuerpos de funciones

Una manera de conseguir cotas inferiores para la constante de Ihara $A(q)$ es mediante la construcción de torres de cuerpos de funciones asintóticamente buenas.

Torres de cuerpos de funciones

Una manera de conseguir cotas inferiores para la constante de Ihara $A(q)$ es mediante la construcción de torres de cuerpos de funciones asintóticamente buenas.

Una torre $\mathcal{F}$ de cuerpos de funciones sobre $\mathbb{F}_q$ es una sucesión $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ de cuerpos de funciones sobre $\mathbb{F}_q$ tal que

(a) $F_i \subsetneq F_{i+1}$ para todo $i \geq 0$.

(b) La extensión F_{i+1}/F_i es finita y separable para todo $i \geq 1$.

(c) $\mathbb{F}_q$ es algebraicamente cerrado en F_i, para todo $i \geq 0$.

(d) $g(F_i) \to \infty$ a medida que $i \to \infty$.

Torres de cuerpos de funciones

El género $\gamma(\mathcal{F})$ de $\mathcal{F}$ sobre F_0 se define como

$$\gamma(\mathcal{F}) := \lim_{i \to \infty} \frac{g(F_i)}{[F_i : F_0]} .$$

Torres de cuerpos de funciones

El género $\gamma(\mathcal{F})$ de $\mathcal{F}$ sobre F_0 se define como

$$\gamma(\mathcal{F}) := \lim_{i\to\infty} \frac{g(F_i)}{[F_i : F_0]}\,.$$

La tasa de descomposición $\nu(\mathcal{F})$ de $\mathcal{F}$ sobre F_0 se define como

$$\nu(\mathcal{F}) := \lim_{i\to\infty} \frac{N(F_i)}{[F_i : F_0]}.$$

Torres de cuerpos de funciones

Una torre $\mathcal{F}$ de cuerpos de funciones sobre $\mathbb{F}_q$ se dice que es asintóticamente buena si

$$\nu(\mathcal{F}) > 0 \qquad \text{y} \qquad \gamma(\mathcal{F}) < \infty.$$

Torres de cuerpos de funciones

Una torre $\mathcal{F}$ de cuerpos de funciones sobre $\mathbb{F}_q$ se dice que es asintóticamente buena si

$$\nu(\mathcal{F}) > 0 \qquad \text{y} \qquad \gamma(\mathcal{F}) < \infty.$$

Caso contrario se dice que es asintóticamente mala. De manera equivalente, $\mathcal{F}$ es asintóticamente buena si y sólo si el límite de la torre es positivo, i.e.

$$\lambda(\mathcal{F}) := \lim_{i \to \infty} \frac{N(F_i)}{g(F_i)} = \frac{\nu(\mathcal{F})}{\gamma(\mathcal{F})} > 0.$$

Torres de cuerpos de funciones

Una torre $\mathcal{F}$ de cuerpos de funciones sobre $\mathbb{F}_q$ se dice que es asintóticamente buena si

$$\nu(\mathcal{F}) > 0 \qquad \text{y} \qquad \gamma(\mathcal{F}) < \infty.$$

Caso contrario se dice que es asintóticamente mala. De manera equivalente, $\mathcal{F}$ es asintóticamente buena si y sólo si el límite de la torre es positivo, i.e.

$$\lambda(\mathcal{F}) := \lim_{i\to\infty} \frac{N(F_i)}{g(F_i)} = \frac{\nu(\mathcal{F})}{\gamma(\mathcal{F})} > 0.$$

Notar que

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

con lo cual $\alpha_q(\delta) \geq 1 - 1/\lambda(\mathcal{F}) - \delta$.

Torres de cuerpos de funciones

Una torre $\mathcal{F}$ de cuerpos de funciones sobre $\mathbb{F}_q$ se dice que es asintóticamente buena si

$$\nu(\mathcal{F}) > 0 \qquad \text{y} \qquad \gamma(\mathcal{F}) < \infty.$$

Caso contrario se dice que es asintóticamente mala. De manera equivalente, $\mathcal{F}$ es asintóticamente buena si y sólo si el límite de la torre es positivo, i.e.

$$\lambda(\mathcal{F}) := \lim_{i \to \infty} \frac{N(F_i)}{g(F_i)} = \frac{\nu(\mathcal{F})}{\gamma(\mathcal{F})} > 0.$$

Notar que

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

con lo cual $\alpha_q(\delta) \geq 1 - 1/\lambda(\mathcal{F}) - \delta$.

Una torre $\mathcal{F}$ de cuerpos de funciones sobre $\mathbb{F}_q$ se dice que es óptima si $\lambda(\mathcal{F}) = A(q)$.

Códigos AG

Sea F un cuerpo de funciones sobre $\mathbb{F}_q$, G y $D = P_1 + \cdots + P_n$ divisores disjuntos de F, donde $P_1, \ldots, P_n$ son lugares racionales de F.

Códigos AG

Sea F un cuerpo de funciones sobre $\mathbb{F}_q$, G y $D = P_1 + \cdots + P_n$ divisores disjuntos de F, donde $P_1, \ldots, P_n$ son lugares racionales de F.

Consideremos el espacio de Riemann-Roch

$$\mathcal{L}(G) = \{u \in F \setminus \{0\} : (u) \geq -G\} \cup \{0\}$$

asociado a G, donde (u) representa el divisor principal de $u \in F$.

Códigos AG

Sea F un cuerpo de funciones sobre $\mathbb{F}_q$, G y $D = P_1 + \cdots + P_n$ divisores disjuntos de F, donde $P_1, \ldots, P_n$ son lugares racionales de F.

Consideremos el espacio de Riemann-Roch

$$\mathcal{L}(G) = \{u \in F \setminus \{0\} : (u) \geq -G\} \cup \{0\}$$

asociado a G, donde (u) representa el divisor principal de $u \in F$.

El código AG asociado a F, D y G se define como

$$C_{\mathcal{L}}(D, G) = \{(u(P_1), u(P_2), \ldots, u(P_n)) \in \mathbb{F}_q^n : u \in \mathcal{L}(G)\},$$

donde $u(P_i)$ representa la clase residual de u módulo P_i.

Códigos AG

Sea F un cuerpo de funciones sobre $\mathbb{F}_q$, G y $D = P_1 + \cdots + P_n$ divisores disjuntos de F, donde $P_1, \ldots, P_n$ son lugares racionales de F.

Consideremos el espacio de Riemann-Roch

$$\mathcal{L}(G) = \{u \in F \setminus \{0\} : (u) \geq -G\} \cup \{0\}$$

asociado a G, donde (u) representa el divisor principal de $u \in F$.

El código AG asociado a F, D y G se define como

$$C_{\mathcal{L}}(D, G) = \{(u(P_1), u(P_2), \ldots, u(P_n)) \in \mathbb{F}_q^n : u \in \mathcal{L}(G)\},$$

donde $u(P_i)$ representa la clase residual de u módulo P_i.

Se tiene que

$$k \geq deg\ G + 1 - g \quad \text{si } deg\ G < n \quad \text{y} \quad d \geq n - deg\ G$$

Además $2g - 2 < deg\ G < n$ entonces $k = deg\ G + 1 - g$.

Códigos AG buenos

Sea $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ una sucesión de cuerpos de funciones sobre $\mathbb{F}_q$ tal que para cada $i \geq 0$ existan n_i lugares racionales $P_{i,1}, \ldots, P_{i,n_i}$ en F_i.

Códigos AG buenos

Sea $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ una sucesión de cuerpos de funciones sobre $\mathbb{F}_q$ tal que para cada $i \geq 0$ existan n_i lugares racionales $P_{i,1}, \ldots, P_{i,n_i}$ en F_i. Sea $\lambda \in (0,1)$ y supongamos que vale lo siguiente:

(a) $n_i \to \infty$ a medida que $i \to \infty$;

(b) existe i_0 tal que $\frac{n_i}{g(F_i)} \geq \lambda^{-1}$ para todo $i \geq i_0$; y

(c) para cada $i > 0$ existe un divisor G_i de F_i disjunto de $D_i := P_{i,1} + \cdots + P_{i,n_i}$ tal que

$deg\ G_i \leq n_i \cdot \alpha(i)$,

donde $\alpha : \mathbb{N} \to \mathbb{R}$ con $\alpha(i) \to 0$ mientras $i \to \infty$.

Códigos AG buenos

Sea $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ una sucesión de cuerpos de funciones sobre $\mathbb{F}_q$ tal que para cada $i \geq 0$ existan n_i lugares racionales $P_{i,1}, \ldots, P_{i,n_i}$ en F_i. Sea $\lambda \in (0,1)$ y supongamos que vale lo siguiente:

(a) $n_i \to \infty$ a medida que $i \to \infty$;

(b) existe i_0 tal que $\frac{n_i}{g(F_i)} \geq \lambda^{-1}$ para todo $i \geq i_0$; y

(c) para cada $i > 0$ existe un divisor G_i de F_i disjunto de $D_i := P_{i,1} + \cdots + P_{i,n_i}$ tal que

$deg\ G_i \leq n_i \cdot \alpha(i)$,

donde $\alpha : \mathbb{N} \to \mathbb{R}$ con $\alpha(i) \to 0$ mientras $i \to \infty$.

Entonces la sucesión $\mathcal{F}$ induce una sucesión de códigos AG $\mathcal{G} = \{\mathcal{C}_i\}_{i=N}^{\infty}$ asintóticamente buenos tal que

$$\liminf_{i\to\infty} \frac{k_i}{n_i} = 1 - \lambda - \delta > 0 \quad \text{y} \quad \liminf_{i\to\infty} \frac{d_i}{n_i} = \delta > 0$$

para $0 < \delta < 1 - \lambda$.

Códigos AG buenos

Sea $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ una sucesión de cuerpos de funciones sobre $\mathbb{F}_q$ tal que para cada $i \geq 0$ existan n_i lugares racionales $P_{i,1}, \ldots, P_{i,n_i}$ en F_i. Sea $\lambda \in (0,1)$ y supongamos que vale lo siguiente:

(a) $n_i \to \infty$ a medida que $i \to \infty$;

(b) existe i_0 tal que $\frac{n_i}{g(F_i)} \geq \lambda^{-1}$ para todo $i \geq i_0$; y

(c) para cada $i > 0$ existe un divisor G_i de F_i disjunto de $D_i := P_{i,1} + \cdots + P_{i,n_i}$ tal que

$deg\ G_i \leq n_i \cdot \alpha(i)$,

donde $\alpha : \mathbb{N} \to \mathbb{R}$ con $\alpha(i) \to 0$ mientras $i \to \infty$.

Entonces la sucesión $\mathcal{F}$ induce una sucesión de códigos AG $\mathcal{G} = \{\mathcal{C}_i\}_{i=N}^{\infty}$ asintóticamente buenos tal que

$$\liminf_{i\to\infty} \frac{k_i}{n_i} = 1 - \lambda - \delta > 0 \quad \text{y} \quad \liminf_{i\to\infty} \frac{d_i}{n_i} = \delta > 0$$

para $0 < \delta < 1 - \lambda$.
De esto se deduce que $\alpha_q(\delta) \geq 1 - \lambda - \delta$.

Códigos AG buenos

Una manera de encontrar una sucesión de cuerpos de funciones sobre $\mathbb{F}_q$ que satisfaga las condiciones anteriores es construyendo torres de cuerpos de funciones sobre $\mathbb{F}_q$ asintóticamente buenas con límite superiores a uno.

Códigos AG buenos

Una manera de encontrar una sucesión de cuerpos de funciones sobre $\mathbb{F}_q$ que satisfaga las condiciones anteriores es construyendo torres de cuerpos de funciones sobre $\mathbb{F}_q$ asintóticamente buenas con límite superiores a uno.

En particular, si la clausura galosiana de una torre asintóticamente buena sobre $\mathbb{F}_q$ es también asintóticamente buena sobre $\mathbb{F}_q$, entonces es posible demostrar la existencia de buenos códigos AG con mayor estructura que solamente la linealidad.

Códigos AG buenos

Una manera de encontrar una sucesión de cuerpos de funciones sobre $\mathbb{F}_q$ que satisfaga las condiciones anteriores es construyendo torres de cuerpos de funciones sobre $\mathbb{F}_q$ asintóticamente buenas con límite superiores a uno.

En particular, si la clausura galosiana de una torre asintóticamente buena sobre $\mathbb{F}_q$ es también asintóticamente buena sobre $\mathbb{F}_q$, entonces es posible demostrar la existencia de buenos códigos AG con mayor estructura que solamente la linealidad.

Bajo ciertas condiciones, el grupo de Galois de las extensiones que aparecen en la clausura galosiana de una torre dada, actúa sobre los lugares racionales que definen el código AG y esa acción se traduce, por ejemplo, en que los códigos AG así obtenidos son transitivos (pues la acción es transitiva sobre los lugares racionales que están sobre otro lugar racional.)

Buenos códigos AG transitivos por bloques

Sea $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ o bien una torre moderada o bien una torre 2-acotada sobre $\mathbb{F}_q$ con pasos de Galois tal que los espacios de descomposición $Sp(\mathcal{F})$ y de ramificicación $R(\mathcal{F})$ sean no vacíos.

Buenos códigos AG transitivos por bloques

Sea $\mathcal{F} = \{F_i\}_{i=0}^{\infty}$ o bien una torre moderada o bien una torre 2-acotada sobre $\mathbb{F}_q$ con pasos de Galois tal que los espacios de descomposición $Sp(\mathcal{F})$ y de ramificicación $R(\mathcal{F})$ sean no vacíos.

Supongamos que existen conjuntos finitos Γ y Ω de lugares racionales de F_0 tales que: $R(\mathcal{F}) \subset \Gamma$ y $\Omega \subset Sp(\mathcal{F})$ con

$$0 < g_0 - 1 + \epsilon t < r,$$

donde $g_0 = g(F_0)$, $t = |\Gamma|$, $r = |\Omega|$ y $\epsilon = 1/2$ si $\mathcal{F}$ es moderada o $\epsilon = 1$ en otro caso.

Buenos códigos AG transitivos por bloques

Supongamos además que existe un lugar $P_0 \in R(\mathcal{F})$ que es absolutamente μ-ramificado en $\mathcal{F}$ para algún $\mu > 1$.

Buenos códigos AG transitivos por bloques

Supongamos además que existe un lugar $P_0 \in R(\mathcal{F})$ que es absolutamente μ-ramificado en $\mathcal{F}$ para algún $\mu > 1$.

Entonces existe una sucesión $\mathcal{G} = \{\mathcal{C}_i\}_{i=0}^{\infty}$ de códigos AG r-bloque transitivos sobre $\mathbb{F}_q$ asintóticamente buenos para los cuales se tiene que

$$\liminf_{i\to\infty} \frac{k_i}{n_i} = 1 - \frac{g_0 - 1 + \epsilon t}{r} - \delta > 0 \quad \text{y} \quad \liminf_{i\to\infty} \frac{d_i}{n_i} = \delta > 0$$

para $0 < \delta < 1 - (g_0 - 1 + \epsilon t)/r$.

Buenos códigos AG transitivos por bloques

Supongamos además que existe un lugar $P_0 \in R(\mathcal{F})$ que es absolutamente μ-ramificado en $\mathcal{F}$ para algún $\mu > 1$.

Entonces existe una sucesión $\mathcal{G} = \{\mathcal{C}_i\}_{i=0}^{\infty}$ de códigos AG r-bloque transitivos sobre $\mathbb{F}_q$ asintóticamente buenos para los cuales se tiene que

$$\liminf_{i\to\infty} \frac{k_i}{n_i} = 1 - \frac{g_0 - 1 + \epsilon t}{r} - \delta > 0 \quad \text{y} \quad \liminf_{i\to\infty} \frac{d_i}{n_i} = \delta > 0$$

para $0 < \delta < 1 - (g_0 - 1 + \epsilon t)/r$. En particular

$$\alpha_q(\delta) \geq 1 - \frac{g_0 - 1 + \epsilon t}{r} - \delta$$

Muchas gracias!!!