Códigos (I)

XXVII Escuela Venezolana de Matemáticas – EMALCA

Edgar Martínez-Moro

Sept. 2014

Instituto de Investigación en Matemáticas
Universidad de Valladolid

Códigos correctores

Un código corrector de errores es un subconjunto $\mathcal{C} \subseteq \mathcal{A}^n$, siendo $\mathcal{A}$ un alfabeto finito y n un entero positivo. Los elementos de $\mathcal{C}$ son llamados palabras y n es su longitud.

Cada palabra de $\mathcal{C}$ contiene k símbolos de información y $n-k$ símbolos redundantes: el número k/n se llama tasa de transmisión de $\mathcal{C}$.

Dados $\mathbf{x}, \mathbf{y} \in \mathcal{A}^n$, llamamos distancia de Hamming entre $\mathbf{x}$ e $\mathbf{y}$ al número de coordenadas distintas que poseen,

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

Códigos correctores

Un código corrector de errores es un subconjunto $\mathcal{C} \subseteq \mathcal{A}^n$, siendo $\mathcal{A}$ un alfabeto finito y n un entero positivo. Los elementos de $\mathcal{C}$ son llamados palabras y n es su longitud.

Cada palabra de $\mathcal{C}$ contiene k símbolos de información y $n-k$ símbolos redundantes: el número k/n se llama tasa de transmisión de $\mathcal{C}$.

Dados $\mathbf{x}, \mathbf{y} \in \mathcal{A}^n$, llamamos distancia de Hamming entre $\mathbf{x}$ e $\mathbf{y}$ al número de coordenadas distintas que poseen,

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

Códigos correctores

Un código corrector de errores es un subconjunto $\mathcal{C} \subseteq \mathcal{A}^n$, siendo $\mathcal{A}$ un alfabeto finito y n un entero positivo. Los elementos de $\mathcal{C}$ son llamados palabras y n es su longitud.

Cada palabra de $\mathcal{C}$ contiene k símbolos de información y $n-k$ símbolos redundantes: el número k/n se llama tasa de transmisión de $\mathcal{C}$.

Dados $\mathbf{x}, \mathbf{y} \in \mathcal{A}^n$, llamamos distancia de Hamming entre $\mathbf{x}$ e $\mathbf{y}$ al número de coordenadas distintas que poseen,

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

Obsérvese que la función d es realmente una distancia en $\mathcal{A}^n$. El hecho de que d no sea invariante por cambios de base, hace que la teoría de códigos no sea una parte trivial del álgebra lineal.

La capacidad de corrección de errores de $\mathcal{C}$ viene determinada por su distancia mínima, definida como

$$d = d(\mathcal{C}) = \text{mín}\{d(\mathbf{x}, \mathbf{y}) \mid \mathbf{x}, \mathbf{y} \in \mathcal{C},\ \mathbf{x} \neq \mathbf{y}\}.$$

El objetivo principal (o mejor, uno de los objetivos principales) de la teoría de códigos correctores de errores es encontrar *buenos* códigos, es decir, códigos que maximicen solidariamente los parámetros k/n y d/n. Sin embargo estas demandas son mutuamente contradictorias.

Otro requerimiento importante para un buen código es que posea algún método de descodificación computacionalmente efectivo. Relativamente pocos códigos permiten estos métodos efectivos. En el lenguaje de la Teoría de la Complejidad Computacional, el problema de descodificar un código (arbitrario) es NP-Completo.

Códigos lineales sobre cuerpos finitos

Un código lineal q-ario de longitud n es un subespacio vectorial $\mathcal{C} \subseteq \mathbb{F}_q^n$.

Para abreviar, de un código lineal de longitud n, dimensión k y distancia mínima d, diremos que es de tipo $[n, k, d]$. Los códigos utilizados en la práctica (excepto algunos de pequeño tamaño) son siempre lineales.

Llamaremos matriz generatriz de $\mathcal{C}$ a la matriz de una aplicación lineal biyectiva $c : \mathbb{F}_q^k \longrightarrow \mathcal{C} \subset \mathbb{F}_q^n$, es decir, a una matriz $k \times n$ cuyas filas son una base de $\mathcal{C}$.

Códigos lineales sobre cuerpos finitos

Un código lineal q-ario de longitud n es un subespacio vectorial $\mathcal{C} \subseteq \mathbb{F}_q^n$.

Para abreviar, de un código lineal de longitud n, dimensión k y distancia mínima d, diremos que es de tipo $[n, k, d]$. Los códigos utilizados en la práctica (excepto algunos de pequeño tamaño) son siempre lineales.

Llamaremos matriz generatriz de $\mathcal{C}$ a la matriz de una aplicación lineal biyectiva $c : \mathbb{F}_q^k \longrightarrow \mathcal{C} \subset \mathbb{F}_q^n$, es decir, a una matriz $k \times n$ cuyas filas son una base de $\mathcal{C}$.

Diremos que dos códigos $\mathcal{C}_1, \mathcal{C}_2$, de la misma longitud, n, sobre $\mathbb{F}_q$, son equivalentes si existe una permutación σ del conjunto $\{1, \cdots, n\}$ tal que $\mathcal{C}_2 = \{\sigma(\mathbf{c}) \mid \mathbf{c} \in \mathcal{C}_1\}$.

Una permutación σ, actúa realmente sobre los índices $\{1, \cdots, n\}$ y no sobre los elementos de $\mathbb{F}_q^n$. Cuando por abuso de notación escribimos $\sigma(\mathbf{x})$, deberíamos escribir $(x_{\sigma(1)}, \cdots, x_{\sigma(n)})$.

– Proposición –

Todo código es equivalente a uno sistemático.

Diremos que dos códigos $\mathcal{C}_1, \mathcal{C}_2$, de la misma longitud, n, sobre $\mathbb{F}_q$, son equivalentes si existe una permutación σ del conjunto $\{1, \cdots, n\}$ tal que $\mathcal{C}_2 = \{\sigma(\mathbf{c}) \mid \mathbf{c} \in \mathcal{C}_1\}$.

Una permutación σ, actúa realmente sobre los índices $\{1, \cdots, n\}$ y no sobre los elementos de $\mathbb{F}_q^n$. Cuando por abuso de notación escribimos $\sigma(\mathbf{x})$, deberíamos escribir $(x_{\sigma(1)}, \cdots, x_{\sigma(n)})$.

– Proposición –

Todo código es equivalente a uno sistemático.

Diremos que una matriz H es una matriz de control del código $\mathcal{C}$ si para todo vector $\mathbf{x} \in \mathbb{F}_q^n$ se verifica que $\mathbf{x} \in \mathcal{C}$ si y sólo si $H\mathbf{x}^t = \mathbf{0}$.

– Proposición –

Si G y H son matrices generatriz y de control de $\mathcal{C}$, entonces

$$GH^t = 0.$$

Diremos que una matriz H es una matriz de control del código $\mathcal{C}$ si para todo vector $\mathbf{x} \in \mathbb{F}_q^n$ se verifica que $\mathbf{x} \in \mathcal{C}$ si y sólo si $H\mathbf{x}^t = \mathbf{0}$.

– Proposición –

Si G y H son matrices generatriz y de control de $\mathcal{C}$, entonces

$$GH^t = 0.$$

Sea $\mathbf{x} = (x_1, \cdots, x_n) \in \mathbb{F}_q^n$. Llamaremos soporte de $\mathbf{x}$ al conjunto $\mathrm{sop}(\mathbf{x}) = \{i \mid 1 \leq i \leq n, x_i \neq 0\}$. Llamaremos peso de Hamming de $\mathbf{x}$ a $w(\mathbf{x}) = |\mathrm{sop}(\mathbf{x})| = d(\mathbf{x}, \mathbf{0})$ siendo $\mathbf{0}$ el vector $\mathbf{0} = (0, 0, \cdots, 0)$.

El peso mínimo de $\mathcal{C}$ se define como

$$w(\mathcal{C}) = \text{mín}\{w(\mathbf{c}) \mid \mathbf{c} \in \mathcal{C}, \mathbf{c} \neq \mathbf{0}\}.$$

– Lema –

En un código lineal, la distancia mínima es igual al peso mínimo.

Sea $\mathbf{x} = (x_1, \cdots, x_n) \in \mathbb{F}_q^n$. Llamaremos soporte de $\mathbf{x}$ al conjunto $\mathrm{sop}(\mathbf{x}) = \{i \mid 1 \leq i \leq n, x_i \neq 0\}$. Llamaremos peso de Hamming de $\mathbf{x}$ a $w(\mathbf{x}) = |\mathrm{sop}(\mathbf{x})| = d(\mathbf{x}, \mathbf{0})$ siendo $\mathbf{0}$ el vector $\mathbf{0} = (0, 0, \cdots, 0)$.

El peso mínimo de $\mathcal{C}$ se define como

$$w(\mathcal{C}) = \mathrm{mín}\{w(\mathbf{c}) \mid \mathbf{c} \in \mathcal{C}, \mathbf{c} \neq \mathbf{0}\}.$$

– Lema –

En un código lineal, la distancia mínima es igual al peso mínimo.

– Proposición –

Sea $\mathcal{C}$ un código lineal de matriz de control H y distancia mínima d. Entonces $d > r$ si y sólo si cualesquiera r columnas de H son linealmente independientes. Por tanto, la distancia mínima de $\mathcal{C}$ coincide con el menor cardinal de un conjunto de columnas linealmente dependientes en H.

– Corolario (Cota de Singleton) –

La distancia mínima de un código lineal $[n, k]$ verifica

$$d \leq n - k + 1.$$

Esta cota también se puede probar en el caso de códigos no lineales. Los códigos lineales para los que se alcanza la igualdad en la cota anterior, $d = n - k + 1$, son llamados de máxima distancia de separación.

– Corolario (Cota de Singleton) –

La distancia mínima de un código lineal $[n, k]$ verifica

$$d \leq n - k + 1.$$

Esta cota también se puede probar en el caso de códigos no lineales. Los códigos lineales para los que se alcanza la igualdad en la cota anterior, $d = n - k + 1$, son llamados de máxima distancia de separación.

Dualidad

La matriz de control, H, de un código lineal $\mathcal{C}$, puede ser interpretada como matriz generatriz de otro código sobre $\mathbb{F}_q$, llamado dual de $\mathcal{C}$ y denotado $\mathcal{C}^\perp$. Obviamente, si $\mathcal{C}$ tiene dimensión k, entonces $\mathcal{C}^\perp$ tiene dimensión $n-k$. Además, si G es una matriz generatriz de $\mathcal{C}$, como la igualdad $GH^t = 0$ implica $HG^t = 0$, se deduce que G es una matriz de control para $\mathcal{C}^\perp$.

– Proposición –

Si $\mathcal{C}$ es un código lineal, entonces su dual $\mathcal{C}^\perp$ es el ortogonal de $\mathcal{C}$ con respecto a la forma bilineal

$$\langle \mathbf{u}, \mathbf{v} \rangle = \sum_{i=1}^{n} u_i v_i \in \mathbb{F}_q.$$

Dualidad

La matriz de control, H, de un código lineal $\mathcal{C}$, puede ser interpretada como matriz generatriz de otro código sobre $\mathbb{F}_q$, llamado dual de $\mathcal{C}$ y denotado $\mathcal{C}^\perp$. Obviamente, si $\mathcal{C}$ tiene dimensión k, entonces $\mathcal{C}^\perp$ tiene dimensión $n-k$. Además, si G es una matriz generatriz de $\mathcal{C}$, como la igualdad $GH^t = 0$ implica $HG^t = 0$, se deduce que G es una matriz de control para $\mathcal{C}^\perp$.

– Proposición –

Si $\mathcal{C}$ es un código lineal, entonces su dual $\mathcal{C}^\perp$ es el ortogonal de $\mathcal{C}$ con respecto a la forma bilineal

$$\langle \mathbf{u}, \mathbf{v} \rangle = \sum_{i=1}^{n} u_i v_i \in \mathbb{F}_q.$$

Como la forma bilineal $\langle \cdot, \cdot \rangle$ es simétrica y no degenerada, se verifica que $(\mathcal{C}^{\perp})^{\perp} = \mathcal{C}$, es decir, el dual del dual de un código es el propio código. Obsérvese que puede darse la situación $\mathcal{C} \cap \mathcal{C}^{\perp} \neq \{\mathbf{0}\}$. El caso extremo se presenta cuando $\mathcal{C} = \mathcal{C}^{\perp}$. En dicho caso llamaremos al código autodual.

A diferencia de lo que ocurre con la dimensión, no es posible, en general, determinar la distancia mínima de $\mathcal{C}^{\perp}$ únicamente en términos de la distancia mínima de $\mathcal{C}$.

Códigos cíclicos

Un código lineal $\mathcal{C}$ de longitud n sobre $\mathbb{F}_q$, es cíclico si para cada $(c_0, c_1, \cdots, c_{n-1}) \in \mathcal{C}$ se verifica que $(c_{n-1}, c_0, \cdots, c_{n-2}) \in \mathcal{C}$.

Sean $\mathbb{F}_q[x]_{(n-1)}$ el espacio vectorial de los polinomios sobre $\mathbb{F}_q$ con grado menor que n y A el anillo cociente $A = \mathbb{F}_q[x]/\langle x^n - 1\rangle$. En virtud de los isomorfismos de espacios vectoriales

$$\mathbb{F}_q^n \cong \mathbb{F}_q[x]_{(n-1)} \cong A$$

podemos identificar cada vector $(a_0, \cdots, a_{n-1})$ con el polinomio $a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$ y con la clase, en A, $a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + \langle x^n - 1\rangle$. Consecuentemente, un código sobre $\mathbb{F}_q$ puede considerarse como un subconjunto de A.

Por otra parte, impondremos la restricción adicional $\mathrm{mcd}(q, n) = 1$. Esto garantiza que el polinomio $x^n - 1$ tiene todos sus factores irreducibles distintos y sus raíces forman un grupo cíclico de orden n. La propiedad fundamental de los códigos cíclicos es la siguiente.

– Teorema –

Sea $\mathcal{C}$ un código lineal no nulo de longitud n sobre el cuerpo finito $\mathbb{F}_q$. $\mathcal{C}$ es cíclico si y sólo si, considerado inmerso en A, es un ideal.

Por otra parte, impondremos la restricción adicional $\mathrm{mcd}(q, n) = 1$. Esto garantiza que el polinomio $x^n - 1$ tiene todos sus factores irreducibles distintos y sus raíces forman un grupo cíclico de orden n. La propiedad fundamental de los códigos cíclicos es la siguiente.

– Teorema –

Sea $\mathcal{C}$ un código lineal no nulo de longitud n sobre el cuerpo finito $\mathbb{F}_q$. $\mathcal{C}$ es cíclico si y sólo si, considerado inmerso en A, es un ideal.

– Corolario –

Dado un código cíclico no nulo $\mathcal{C}$ de longitud n, existe un único polinomio mónico $g(x) \in \mathbb{F}_q[x]$ divisor de $x^n - 1$, tal que $\mathcal{C} = \langle g(x) \rangle$. En consecuencia, los elementos de $\mathcal{C}$ pueden identificarse con los polinomios de grado menor que n múltiplos de $g(x)$.

– Proposición –

Sea $\mathcal{C}$ un código cíclico de longitud n sobre $\mathbb{F}_q$ con polinomio generador $g(x)$ de grado $n-k$. El conjunto

$$\{g(x), xg(x), \cdots, x^{k-1}g(x)\}$$

es una base de $\mathcal{C}$. En particular, $\mathcal{C}$ tiene dimensión k.

– Corolario –

Un codigo cíclico de longitud n y polinomio generador $g(x) = g_0 + g_1 x + \cdots + g_{n-k} x^{n-k}$ tiene matriz generatriz

$$G = \begin{pmatrix} g_0 & g_1 & g_2 & \cdots & g_{n-k} & & & & \\ & g_0 & g_1 & \cdots & g_{n-k-1} & g_{n-k} & & & \\ & & \ddots & \ddots & & \ddots & \ddots & & \\ & & & & & & & & \\ & & & & \ddots & \ddots & \ddots & \ddots & \\ & & & & & g_0 & g_1 & \cdots & g_{n-k-1} & g_{n-k} \end{pmatrix}.$$

Si $\mathcal{C}$ es un código cíclico de longitud n, con polinomio generador $g(x)$ de grado $n-k$, llamaremos polinomio de control de $\mathcal{C}$ a

$$h(x) = \frac{x^n - 1}{g(x)} = h_0 + h_1 x + \cdots + h_k x^k.$$

– Proposición –

Con las notaciones de la definición anterior, la matriz (de tamaño $(n-k)\times n$)

$$H = \begin{pmatrix} & & & & h_k & h_{k-1} & \dots & h_1 & h_0 \\ & & & h_k & h_{k-1} & h_{k-2} & \dots & h_0 & \\ & & . & . & . & . & . & & \\ & & & & & & & & \\ & . & . & . & . & & & & \\ h_k & h_{k-1} & \dots & h_1 & h_0 & & & & \end{pmatrix}$$

es una matriz de control de $\mathcal{C}$.

Ceros de un código cíclico

Sea $x^n-1 = f_1(x)f_2(x)\cdots f_m(x)$ la descomposición de x^n-1 en factores irreducibles y sea α_i una raíz de $f_i(x)$. Para el código cíclico $\mathcal{C}_i$ engendrado por $f_i(x)$, se verifica $\mathcal{C}_i = \langle f_i(x)\rangle = \{c(x) \in A \mid c(\alpha_i) = 0\}$. En general, para el código cíclico $\mathcal{C}$ engendrado por $g(x) = f_{i_1} f_{i_2} \cdots f_{i_r}$, se tendrá

$$\mathcal{C} = \langle g(x)\rangle = \{c(x) \mid c(\alpha_{i_1}) = c(\alpha_{i_2}) = \cdots = c(\alpha_{i_r}) = 0\},$$

lo que muestra que los códigos cíclicos pueden definirse, alternativamente, como conjuntos de polinomios con ciertas raíces n-ésimas de 1 como ceros.

Códigos BCH y RS

Fijemos un cuerpo $\mathbb{F}_q$ y números naturales n, b y δ, $2 \leq \delta \leq n$. Sean m el orden multiplicativo de q módulo n (es decir, el menor número natural tal que $q^m \equiv 1 \mod n$) y $\alpha \in \mathbb{F}_{q^m}$ una raíz primitiva n-ésima de la unidad.

Llamaremos código BCH de longitud n y distancia mínima prevista δ, al código cíclico de longitud n cuyo polinomio generador tiene por raíces $\alpha^b, \alpha^{b+1}, \cdots, \alpha^{b+\delta-2}$.

Si se toma $b = 1$, el código se denominar BCH en sentido estricto. Si la longitud n es de la forma $n = q^m - 1$, entonces se hablar de códigos BCH primitivos (en este caso el exponente m coincide con el orden multiplicativo de q módulo n y α es un elemento primitivo de $\mathbb{F}_{q^m}$); si, además, $m = 1$, (es decir, $n = q - 1$ y por tanto $\alpha \in \mathbb{F}_q$) el código se denomina Reed-Solomon.

Códigos BCH y RS

Fijemos un cuerpo $\mathbb{F}_q$ y números naturales n, b y δ, $2 \leq \delta \leq n$. Sean m el orden multiplicativo de q módulo n (es decir, el menor número natural tal que $q^m \equiv 1 \mod n$) y $\alpha \in \mathbb{F}_{q^m}$ una raíz primitiva n-ésima de la unidad.

Llamaremos código BCH de longitud n y distancia mínima prevista δ, al código cíclico de longitud n cuyo polinomio generador tiene por raíces $\alpha^b, \alpha^{b+1}, \cdots, \alpha^{b+\delta-2}$.

Si se toma $b = 1$, el código se denominar BCH en sentido estricto. Si la longitud n es de la forma $n = q^m - 1$, entonces se hablar de códigos BCH primitivos (en este caso el exponente m coincide con el orden multiplicativo de q módulo n y α es un elemento primitivo de $\mathbb{F}_{q^m}$); si, además, $m = 1$, (es decir, $n = q - 1$ y por tanto $\alpha \in \mathbb{F}_q$) el código se denomina Reed-Solomon.

Códigos BCH y RS

Fijemos un cuerpo $\mathbb{F}_q$ y números naturales n, b y δ, $2 \leq \delta \leq n$. Sean m el orden multiplicativo de q módulo n (es decir, el menor número natural tal que $q^m \equiv 1 \mod n$) y $\alpha \in \mathbb{F}_{q^m}$ una raíz primitiva n-ésima de la unidad.

Llamaremos código BCH de longitud n y distancia mínima prevista δ, al código cíclico de longitud n cuyo polinomio generador tiene por raíces $\alpha^b, \alpha^{b+1}, \cdots, \alpha^{b+\delta-2}$.

Si se toma $b = 1$, el código se denominar BCH en sentido estricto. Si la longitud n es de la forma $n = q^m - 1$, entonces se hablar de códigos BCH primitivos (en este caso el exponente m coincide con el orden multiplicativo de q módulo n y α es un elemento primitivo de $\mathbb{F}_{q^m}$); si, además, $m = 1$, (es decir, $n = q - 1$ y por tanto $\alpha \in \mathbb{F}_q$) el código se denomina Reed-Solomon.

– Proposición –

Un código BCH de distancia prevista δ, posee distancia mínima $d \geq \delta$.

Un polinomio generador del código puede obtenerse del modo siguiente: para $i = b, \cdots, b+\delta-2$, sea $m_i(x)$ el polinomio irreducible de α^i sobre $\mathbb{F}_q$. Entonces

$$g(x) = \text{ mcm}\{m_b(x), \cdots, m_{b+\delta-2}(x)\} \tag{1}$$

es el polinomio generador buscado. La dimensión del código es, como en todos los códigos cíclicos, $n - \deg g(x)$.

– Proposición –

Un código BCH de distancia prevista δ, posee distancia mínima $d \geq \delta$.

Un polinomio generador del código puede obtenerse del modo siguiente: para $i = b, \cdots, b+\delta-2$, sea $m_i(x)$ el polinomio irreducible de α^i sobre $\mathbb{F}_q$. Entonces

$$g(x) = \text{ mcm}\{m_b(x), \cdots, m_{b+\delta-2}(x)\} \tag{1}$$

es el polinomio generador buscado. La dimensión del código es, como en todos los códigos cíclicos, $n - \deg g(x)$.

Códigos de Reed-Solomon

Un código Reed-Solomon sobre $\mathbb{F}_q$ es un código BCH primitivo de longitud $n = q - 1$. Su característica distintiva más notable es que la raíz n-ésima, α, es un elemento de $\mathbb{F}_q$ y, por tanto, todas las manipulaciones con el código implican sólo operaciones en el propio cuerpo $\mathbb{F}_q$. Como contrapartida a esta simplicidad de manejo, queda limitada a $q - 1$ la longitud de un código Reed-Solomon sobre $\mathbb{F}_q$.

– Proposición –

Los códigos Reed-Solomon son MDS.

Códigos de Reed-Solomon

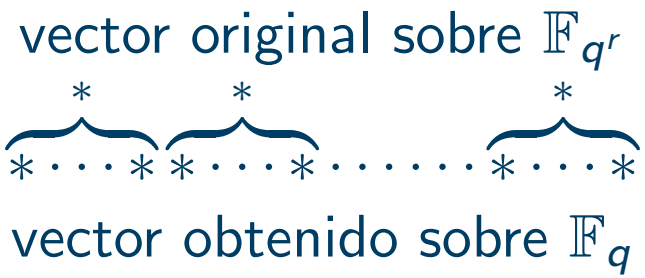
Un código Reed-Solomon sobre $\mathbb{F}_q$ es un código BCH primitivo de longitud $n = q - 1$. Su característica distintiva más notable es que la raíz n-ésima, α, es un elemento de $\mathbb{F}_q$ y, por tanto, todas las manipulaciones con el código implican sólo operaciones en el propio cuerpo $\mathbb{F}_q$. Como contrapartida a esta simplicidad de manejo, queda limitada a $q - 1$ la longitud de un código Reed-Solomon sobre $\mathbb{F}_q$.

– Proposición –

Los códigos Reed-Solomon son MDS.

Descenso del cuerpo

Dado un cuerpo finito $\mathbb{F}_{q^r}$, extensión de $\mathbb{F}_q$, fijemos una base $\{1, \alpha, \cdots, \alpha^{r-1}\}$ de $\mathbb{F}_{q^r}$ sobre $\mathbb{F}_q$. Como sabemos, cada elemento de $\mathbb{F}_{q^r}$ puede identificarse con el vector de $\mathbb{F}_q^r$ de sus coordenadas en la base anterior. Aplicando este procedimiento a cada componente de un vector de $\mathbb{F}_{q^r}^n$, obtenemos un vector de $\mathbb{F}_q^{rn}$



En particular, si $\mathcal{C}$ es un código de longitud n sobre $\mathbb{F}_{q^r}$, a partir de él podemos conseguir un código sobre $\mathbb{F}_q$ de longitud rn; se dice que este cuerpo se obtiene del original por descenso de cuerpo.

– Proposición –

Sea $\mathcal{C}$ un código de Reed-Solomon sobre $\mathbb{F}_{2^r}$ con distancia $d = 2t + 1$. Entonces, el código binario obtenido por descenso de cuerpo sobre $\mathbb{F}_2$ corrige todos los errores a ráfagas de longitud $l \leq (t-1)r + 1$.