Códigos de Reed Solomon

Felipe Delfini Caetano Fidalgo **Jaime Edmundo Apaza Rodriguez**

Depto de Matemática, FEIS, UNESP,
15385-000, Ilha Solteira, SP
E-mail: felipeomat@gmail.com jaime@mat.feis.unesp.br

RESUMO

Neste trabalho apresentamos os Códigos de Reed Solomon (Códigos RS) definidos sobre um corpo finito $\mathbb{F}_q$. Os Códigos RS servem de introdução, e motivação, ao estudo dos Códigos Geométricos de Goppa. Para definir os códigos RS são usados elementos de um certo espaço vetorial de polinômios definidos sobre um corpo $\mathbb{F}_q$, enquanto que, para os Códigos de Goppa, são usados elementos de um corpo de funções algébricas, também definidas sobre um corpo do tipo $\mathbb{F}_q$. De fato, para um divisor D de um corpo de funções algébricas, o conjunto $\mathcal{L}(D)$ é um espaço vetorial. O estudo deste assunto será motivo de um trabalho posterior, dando assim continuidade a este primeiro.

A seguir, introduzimos o conceito de *distância*.

Definição 1 *Para $a, b \in \mathbb{F}_q^n$, a distância de Hamming é dada por $d(a,b) = |\{i : a_i \neq b_i\}|$, ou seja, o número de entradas em que a e b diferem.*

O peso de $a \in \mathbb{F}_q^n$ é dado por $w(a) = d(a,0)$. A distância mínima de um código $\mathcal{C}$ é definida por $d(\mathcal{C}) = min\{w(a) : a \neq 0,\ a \in C\}$.

Um $[n,k,d]$- código $\mathcal{C}$ é um subespaço de $\mathbb{F}_{q^n}$, onde $n = dim_{\mathbb{F}_q}\mathbb{F}_{q^n}$, $k = dim_{\mathbb{F}_q}\mathcal{C}$ e d, a distância mínima. Os valores n, k *e* d são os parâmetros do código $\mathcal{C}$.

Proposição 1 (Cota de Singleton) *Para um $[n,k,d]$-código $\mathcal{C}$ vale $k + d \leqslant n + 1$.*

Definição 2 (Códigos MDS) *Um código $\mathcal{C}$ é dito de Máxima Distância Separável (MDS) se atingir a Cota de Singleton.*

Agora, sejam $n = q - 1$ e $\beta \in \mathbb{F}_q$ um elemento primitivo do grupo multiplicativo $\mathbb{F}_q^* = \mathbb{F}_q - \{0\}$, isto é, $\mathbb{F}_q^* = \{\beta, \beta^2, ..., \beta^n = 1\}$. Consideremos o espaço vetorial

$$\mathcal{L}_k := \{f \in \mathbb{F}_q[X] | deg f \leqslant k-1\},$$

de dimensão k, com $1 \leqslant k \leqslant n$, e a aplicação avaliação $ev : \mathcal{L}_k \longrightarrow \mathbb{F}_q^n$ dada por

$$ev(f) := (f(\beta), f(\beta^2), ..., f(\beta^n)) \in \mathbb{F}_q^n.$$

Esta aplicação é $\mathbb{F}_q$-linear e injetiva. Logo,

$$\mathcal{C}_k := \{(f(\beta), f(\beta^2), ..., f(\beta^n) | f \in \mathcal{L}_k\}$$

é um código $[n,k]$ sobre $\mathbb{F}_q$. Este código é chamado *Código de Reed Solomon*.

O peso de uma palavra código não nula $c = ev(f) \in \mathcal{C}_k$ é dado por

$$w(c) = n - |\{i \in \{1, ..., n\}; f(\beta^i) = 0\}| \geqslant n - deg f \geqslant n - (k-1).$$

Assim, a mínima distância d de $\mathcal{C}_k$, satisfaz a relação $d \geqslant n + 1 - k$. Pela Cota de Singleton temos que $d \leqslant n+1-k$. Portanto, vale a igualdade e, então, os Códigos RS são códigos MDS sobre $\mathbb{F}_q$, ou seja, são ótimos nesse sentido.

Os códigos RS são pequenos em comparação com o tamanho do alfabeto $\mathbb{F}_q$, pois $n = q - 1$. Este é um outro bom motivo para estudar os Códigos de Goppa, além do seu interesse intrínseco e aplicações. Os códigos de Goppa são uma forma "complicada" de definir certos subespaços vetoriais de $\mathbb{F}_q^n$ e seus parâmetros são estimados usando o clássico *Teorema de Riemann-Roch*.

Referências

[1] Stichtenoth, H., Algebraic Function Fields and Codes, *Springer-Verlag*, 1993.