Evento	Salão UFRGS 2014: SIC - XXVI SALÃO DE INICIAÇÃO CIENTÍFICA DA UFRGS
Ano	2014
Local	Porto Alegre
Título	CÓDIGOS REED-SOLOMON: CORPOS FINITOS COM APLICAÇÕES EM TEORIA DE CÓDIGOS
Autor	LUCAS GABRIEL MOTA DA SILVEIRA
Orientador	VILMAR TREVISAN

Quando transmitimos alguma informação, queremos ter certeza de que a informação enviada é igual à recebida, mas essa transmissão está sujeita a ruídos que causam erros na mensagem, como perda ou deslocamento de símbolos. A Teoria de Códigos estuda técnicas para detectar e corrigir tais erros.

A mensagem que queremos transmitir consiste de uma sequência finita de k símbolos $a=(a_1,...,a_k)$ que será codificada para uma ***palavra-código*** c de n símbolos $c=(c_1,...,c_n)$ por uma função de *codificação* f: $GF(q)^k \rightarrow GF(q)^n$, onde $n>k$. Enviamos c=f(a) pelo canal de transmissão de maneira que a mensagem recebida, $c+e$, seja tal que o erro *e* possa ser detectado e/ou corrigido. Por fim, a função de *decodificação* g: $GF(q)^n \rightarrow GF(q)^k$ que associa a mensagem recebida à mensagem decodificada é aplicada. O ***código*** é o conjunto imagem da f, ou seja, o conjunto de todas as palavras-código.

Os códigos Reed-Solomon sobre GF(q) são um tipo específico de códigos cíclicos que corrigem até *t* erros, com comprimento (das palavras-códigos) *n* igual à $q-1$. São usados na prática desde a recuperação de erros em CDs e DVDs até na comunicação pela NASA e pela Agência Espacial Européia, ou seja, são muito úteis!

Nota: **GF(q)** é o corpo finito de ordem q, também conhecido como *Galois Field*.