

1

Introdução

Quando armazenamos ou transmitimos dados por um canal de comunicação, ocorrem erros que não podemos prever. Isto ocorre pela própria natureza do canal de comunicação. A Teoria de Códigos, que foi iniciada pelo matemático norte-americano Claude Elwood Shannon do laboratório Bell em um trabalho publicado em 1948, se preocupa em detectar e corrigir erros.

Os códigos corretores de erros estão presentes em vários momentos de nosso cotidiano sem que percebamos; por exemplo quando enviamos um email, quando ouvimos música em um CD, quando assistimos a um programa de televisão ou ouvimos rádio, na verdade todas as vezes que fazemos uso de informações digitalizadas. Pois bem, de vez em quando pode ocorrer de um email aparecer corrompido, ou a televisão com problemas de recepção (o comum “chuvisco”), ou a estação de rádio que você está ouvindo aparecer com um chiado. Esses pequenos incômodos ocorrem porque aconteceram alguns erros durante a transmissão. Esses erros não são intencionais e geralmente não podem ser controlados.

Um código corretor de erros permite detectar e corrigir certos erros de forma que a mensagem original possa ser recuperada, isto geralmente é feito adicionando dados de controle na informação transmitida.

Com o aumento da confiabilidade nas comunicações digitais e o surgimento dos computadores digitais como ferramenta essencial da sociedade tecnológica, os códigos corretores de erros vêm conquistando uma posição proeminente. Para ilustrar a praticidade e importância do uso de códigos corretores de erros temos:

- a) uso do bit de paridade como um mecanismo detetor de erro - é um dos esquemas mais simples e conhecidos na comunicação computacional;
- b) armazenamento em discos - estão sendo muito utilizados devido ao

aumento de densidade. Quanto maior a densidade, a probabilidade de ocorrer erros também aumenta;

c) transmissão de informações pelas naves espaciais:

- em 1972 a espaçonave Mariner transmitiu figuras de Marte para a Terra com 64 tonalidades de cinza. Atividade solar e outras condições atmosféricas podem introduzir erros em sinais fracos vindo do espaço. O código utilizado foi o Reed-Muller;

- em 1979 a espaçonave Voyager começou a enviar imagens com 4096 tonalidades de cores. O código utilizado foi o de Gollay;

d) áudio digital - o aumento da popularidade do áudio digital deve-se ao desenvolvimento dos códigos corretores de erros que facilita o processo de digitalização. Ao iniciar a leitura do CD, o sistema corrige os erros produzidos por marcas de dedos, arranhões e outras imperfeições, para logo em seguida transformar em sinais sonoros. O código utilizado é o de Reed-Solomon.

O presente trabalho é focado nos códigos geométricos de Goppa, que possuem propriedades particulares que os fazem uma classe extremamente importante de códigos.

Os códigos de Goppa foram introduzidos no trabalho (Goppa), também são conhecidos como códigos de Reed-Solomon generalizados e a maioria dos códigos utilizados na prática podem ser representados como subcódigos de um código de Reed-Solomon generalizado de maneira natural.

Os códigos de Goppa são interessantes pois para este tipo de código o comprimento, a dimensão e a distância mínima (estes parâmetros serão definidos no capítulo 2), podem ser calculados ou pelo menos estimados e sempre podemos obter uma cota inferior para a distância mínima o que é importante na hora de corrigir erros.

Também para estes códigos existem algoritmos eficientes de decodificação (em (Pel4) pode ser encontrado um survey sobre a história destes algoritmos).

Como veremos nos próximos capítulos, para construir códigos de Goppa com bons parâmetros, é necessário que a curva sobre a qual estão definidos tenha gênero pequeno e muitos pontos racionais. Este fato fez com que o estudo da teoria de curvas sobre corpos finitos saísse do esquecimento e hoje é uma linha de pesquisa importante na área da geometria algébrica.