Resumo do Capítulo 1

Neste capítulo foram estabelecidos três limites fundamentais em diferentes aspectos de um sistema de comunicações digitais através do *teorema da codificação da fonte*, do *teorema da codificação de canal* e do *teorema da capacidade do canal*, todos devidos a Claude Shannon.

O *teorema da codificação da fonte* fornece-nos um padrão pelo qual podemos medir a informação proveniente de uma *fonte discreta sem memória*. Diz-nos o teorema que podemos tornar o número médio de elementos binários (binits) por símbolo da fonte tão pequeno como, mas não menor que, a *entropia* da fonte medida em bits. A entropia de uma fonte é uma função das probabilidades dos símbolos que a fonte produz. Visto a entropia ser uma medida de incerteza, é máxima quando a distribuição de probabilidades associadas gera a máxima incerteza, ou seja, quando os símbolos são equiprováveis.

Os objectivos do teorema da codificação da fonte são perseguidos e aproximados se, antes da codificação, os símbolos produzidos pela fonte forem agrupados em blocos de N símbolos – teremos então uma *extensão de ordem N* – e se os códigos forem de *comprimento variável*. Destes só nos interessam *códigos unicamente descodificáveis*, em especial um seu subconjunto, o dos *códigos sem prefixos*, definidos através de *árvores*. Ambos obedecem à *desigualdade de Kraft-McMillan*, que relaciona entre si os comprimentos de cada palavra de código. Os códigos de *Shannon-Fano* e *Huffman* são dois exemplos de códigos sem prefixos cujo comprimento médio das palavras de código se aproxima da entropia da fonte.

Uma outra abordagem foi feita através da *codificação aritmética*, embora também baseada em modelos probabilísticos da fonte, tal como os dois códigos precedentes; completamente diferente são as codificações de *Lempel-Ziv* (LZ77 e LZ78). Nesta última, por exemplo, vai-se construindo um dicionário à medida que a codificação se realiza.

O *teorema da codificação de canal* é o resultado mais surpreendente e talvez o mais importante da Teoria da Informação. Por exemplo, para um *canal binário simétrico* (BSC), o teorema da codificação de canal diz-nos que para qualquer *taxa de informação* menor ou igual à *capacidade do canal* existem *códigos* tais que a probabilidade de erro média é tão pequena quanto quisermos. Um canal binário simétrico é a forma mais simples de um *canal discreto sem memória*; é simétrico se a probabilidade de se receber um 1 se se tiver enviado um 0 for igual à probabilidade de se receber um 0 se se tiver enviado um 1. Esta probabilidade, chamada *probabilidade de transição*, define univocamente a capacidade do canal.

O terceiro teorema de Shannon, provavelmente o mais famoso, é o *teorema da capacidade do canal*, ou *lei de Shannon-Hartley*, e aplica-se a canais contínuos. Diz-nos o teorema que em qualquer canal de comunicação limitado em potência existe uma velocidade máxima de transmissão de informação sem erros, dependente da largura de banda do canal e da relação sinal-ruído. Esta velocidade, ou taxa, máxima chama-se *capacidade do canal* e mede-se em bits/s. Se o sistema funcionar a uma taxa superior à capacidade do canal está condenado a uma probabilidade de erro elevada, independentemente do receptor ou da técnica de transmissão usada.

A codificação de canal (ou codificação com controlo de erros), referida no teorema da codificação de canal, vai ser objecto do nosso estudo em seguida.