Cyclic Code Redundancy (CCR Separável)

CRC – Código de Redundância Cíclica Separável

Para a transmissão de longos blocos de informação é mais eficiente empregar a codificação separável, que irá permitir o dado recebido já ser utilizado na recepção.

Seja $D(x) = d_{K-1} \cdot x^{K-1} + d_{K-2} \cdot x^{K-2} + \dots + d_0$ (grau $K-1$)

Seja $G(x)$ de grau $(n-K)$.

Seja $\overline{D(x)} = d_{K-1} \cdot x^{n-1} + d_{K-2} \cdot x^{n-2} + \dots + d_0 \cdot x^{n-K}$

(desloca $D(x)$ para a esquerda deixando $(n-K)$ zeros na posições menos significativos)

Em seguida divide-se $\overline{D(x)}$ por $G(x)$, obtendo um resto $R(x)$ com grau $< (n-K)$.

$$\Rightarrow \boxed{\overline{D}(x) = Q(x) \cdot G(x) + R(x)}$$

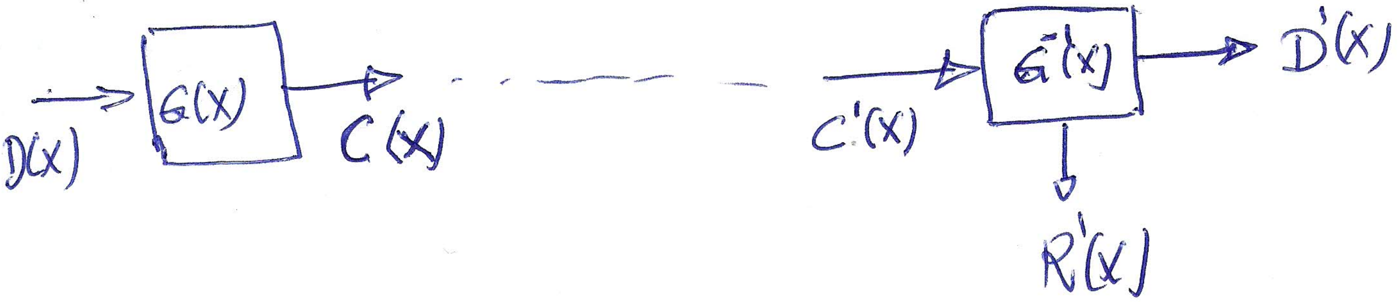
$$\boxed{C(x) = \overline{D}(x) + R(x) = Q(x) \cdot G(x)}$$

que será o polinômio a ser transmitido.

(modulo-2)

$\overline{D}(x)$ e $R(x)$ não tem termos (informações) em mesma posição.

Sendo que os primeiros K bits de $C(x)$ correspondem à informação original.



$$\text{Se } \underline{R'(x)} \begin{cases} = \emptyset; & \text{mensagem correta} \\ \neq \emptyset; & \text{mensagem incorreta.} \end{cases}$$