Note that page numbering is turned on in this template.

Application of Figure 2 to CRC .

In this little section, we replace variable z by x, the degree of polynomial H is n-k instead of k, and it is called g instead of H. The symbols n and k have the following new meaning: a set of k data symbols is used to construct a proper polynomial d(x). A set of n code symbols (known as a block) is transmitted where n > k. The block contains the k data symbols and n-k parity check symbols which are used to allow detection of errors. At the transmitting end, a polynomial divider is used to divide the polynomial $[x^{n-k}d(x)]$ by the generator polynomial g(x) of degree n-k. This division can be thought of this way

$$x^{n-k}d(x) = D(x)g(x) - \gamma(x)$$

where D(x) is the division quotient and $-\gamma(x)$ is the division remainder, which has degree ≤ n-k. The quotient D(x) has degree k, the same as that of d(x). The code word polynomial (degree n) is given by

$$C(x) \equiv D(x)g(x) = \gamma(x) + x^{n-k}d(x) \ .$$

If you write out the coefficients of C(x) (from low to high power), you find that the first n-k of them are the coefficients of γ(x), and the last k of them are the data symbols of d(x). For example, if n=5 and k=3,

$$C(x) = (\gamma_0+\gamma_1 x) + x^2(d_0+d_1x+d_2x^2) = \gamma_0+\gamma_1 x+d_0x^2+d_1x^3+d_2x^4 \rightarrow (\gamma_0, \gamma_1, d_0, d_1, d_2) \ .$$

This in this scheme, the n-k parity check symbols are the negative of the remainder coefficients obtained by doing the division $[x^{n-k}d(x)]/g(x)$. This remainder is obtained using a Figure 2 divider with n-k registers. When the proper division is completed, the registers contain the remainder $-\gamma(x)$. By grounding the feedback line in Figure 1 at this point, the next n-k clocks shift out $-\gamma(x)$ and the coefficients are then negated and appended to the data stream as shown in the example above. That data stream, which is the polynomial C(x), is then transmitted (symbol d_2 first in our example). At the receiving end, C(x) is divided by g(x). Since D(x) = C(x)/g(x), there should be no remainder! If there was an error in the transmission so that some erroneous code word C'(x) was received, one gets C'(x) = D(x) g(x) + s(x) where s(x) is an anomalous remainder (the syndrome) which is found sitting in the Figure 2 registers after the division. This scheme is known as a Cyclic Redundancy Check (CRC). Notice that both the transmitting end and receiving end have Figure 2 dividers which divide by g(x).

Application of Figure 2 to CRC .

In this little section the degree of polynomial H(z) is K ≡ n-k instead of k. This K is then the number of registers in a Figure 2 polynomial divider set up to divide a polynomial by H(z). The symbols n and k have the following new meaning: a set of k data symbols is used to construct a proper polynomial d(z). A set of n code symbols (known as a block) is transmitted where n > k. The block contains the k data symbols and n-k "parity check symbols" which are used to allow detection of errors. At the transmitting

end, a Figure 2 polynomial divider is used to divide the polynomial $[z^{n-k}d(z)]$ by the polynomial H(z) of degree K = n-k. In this context, H(z) is referred to as a "generator" polynomial. This division can be thought of this way

$$z^{n-k}d(z) = D(z)H(z) - \gamma(z)$$

where D(z) is the division quotient and $-\gamma(z)$ is the division remainder (which has degree $\leq$ n-k). The quotient D(z) has degree k, the same as that of d(z). A "code word polynomial" (degree n) is given by

$$C(z) \equiv D(z)H(z) = \gamma(z) + z^{n-k}d(z)$$

where we just use the previous line to get the right side. If we write out the coefficients of C(z) (from low to high power), we find that the first n-k of them are the coefficients of $\gamma(z)$, and the last k of them are the data symbols of d(z). For example, if n=5 and k=3,

$$C(z) = (\gamma_0+\gamma_1 z) + z^2(d_0+d_1 z+d_2 z^2) = \gamma_0+\gamma_1 z+d_0 z^2+d_1 z^3+d_2 z^4 \rightarrow (\gamma_0, \gamma_1, d_0, d_1, d_2) \ .$$

This in this scheme, the K = n-k parity check symbols are the negative of the remainder coefficients obtained by doing the division $[z^{n-k}d(z)]/H(z)$. This remainder is obtained using a Figure 2 divider with K = n-k registers. When the proper polynomial division is completed, the registers contain the remainder $-\gamma(z)$. By grounding the feedback line in Figure 2 and directly accessing the output of the rightmost register, the next n-k clocks shift out $-\gamma(z)$ and the coefficients are then negated and appended to the data stream as shown in the example above to create code polynomial C(z). That data stream, which is the polynomial C(z), is then transmitted (symbol d_2 first in our example). At the receiving end, the received C(z) is divided by H(z) by another Figure 2 divider. Since D(x) = C(x)/H(z), there should be no remainder! If there was an error in the transmission so that some erroneous code word C'(z) was received, one gets C'(z) = D(z) g(z) + s(z) where s(z) is an anomalous remainder (the syndrome) which is found sitting in the Figure 2 registers after the division. This error detection scheme is known as a Cyclic Redundancy Check (CRC). Notice that both the transmitting end (encoder) and receiving end (decoder) have Figure 2 dividers which divide by H(z).

The subject is discussed more in Chapter 8 of Ref [Galois]. There, variable z is called x, and H(z) is called g(x).