Appendix F: Cyclic Code Error Detection Theorems (CRC)

We shall identify the term Cyclic Redundancy Check (CRC) with any error detection system based on an (n,k) cyclic code. The Facts presented in this section are all stated and proved in the original 1961 CRC paper by Peterson and Brown noted in References. The notation used in their paper is the same as ours except for the following differences:

	us	CRC paper
generator	g(x)	P(X)
data polynomial	D(x)	G(X)
code polynomial	C(x)	F(X)
semantics	g(x) has period n	P(X) belongs to exponent n

Our proofs are only slightly more general in some cases than those of the paper which deals only with GF(2). We always assume the code length is n and number of data symbols is k.

Our definition of a cyclic code includes item (8.1) (b) requiring that g(x) divides $x^n - 1$. In some of the Facts presented below, this requirement is necessary, and in others it is not. If this requirement is ignored, then a "cyclic code" so obtained won't really by cyclic because the proof of Chap 8 (f) fails. Also, the set of code words won't form an ideal in the ring A_n, and much of the theory of cyclic codes falls apart. Nevertheless, some of the Facts below will still be valid and are so noted.

It is assumed that the proofs here are read in the order presented.

Fact 1: If $g(0) \neq 0$, a cyclic code generated by g(x) over GF(p) detects all single-symbol errors. (F.1)

Proof. Suppose C'(x) and C(x) differ in one symbol position. Then $E(x) \equiv C'(x)-C(x) = \alpha x^i$ where i = 0,1..n-1 and α is some non-zero element of GF(p). We need to show that in this case the syndrome s(x) will be non-zero so the error will then be detected. But :

$$s(x) = \text{Rem}[C'(x)/g(x)] = \text{Rem}[\{C(x) + E(x)\}/g(x)] = \text{Rem}[E(x)/g(x)] = \text{Rem}[\alpha\, x^i/g(x)]$$

where we used Rem[C(x)/g(x)] = 0. Now:

- For i = 0, $\text{Rem}[\alpha x^i/g(x)] = \text{Rem}[\alpha/g(x)] = \alpha \neq 0$. Note that $g(0) \neq 0$ rules out g(x) = constant ≠ 0.
- For i > 1, $\text{Rem}[\alpha x^i/g(x)] \neq 0$ unless $g(x) = \alpha x^n$ for $n \leq i$, but $g(0) \neq 0$ rules out such a g(x).

QED. Notice that it was not required that g(x) divide evenly into $x^n - 1$.

Fact 2: If g(x) = (x-1)f(x), a cyclic code generated by g(x) over GF(2) detects all odd-number-bit errors. (F.2)

Comment: x-1 is the same as x+1 for GF(2) since -1 = +1 in GF(2).

Proof: In this case, E(x) = C'(x) - C(x) is a polynomial with an odd number of terms. We must show that in this case the syndrome does not vanish so the error will be detected. But:

$$s(x) = \text{Rem}[E(x)/g(x)] = \text{Rem}[(\text{poly with odd of terms})/g(x)]$$

Assume that this remainder is 0. Then we would haven some quotient s(x) and

poly with odd of terms (x) $= g(x)\, s(x) = (x-1)f(x)\, s(x)$.

Evaluate at x = 1 to get

odd sum of 1's $= 1 = (1-1)f(1)s(1) = 0$

Since $1 \neq 0$ we have a contradiction, so it must be that $s(x) \neq 0$ and the error is detected.

Notice that it was not required that g(x) divide evenly into $x^n - 1$.

Fact 3: If $g(0) \neq 0$ and g(x) has period n, a cyclic code generated by g(x) over GF(2) detects all double-bit errors and all single-bit errors. (F.3)

Proof: We already know from Fact 1 that single-bit errors are detected. For double-bit errors we have $E(x) = x^i + x^j$ for some $0 \leq i \leq j \leq n-1$ We need to show that the syndrome does not vanish in this case.

$$s(x) = \text{Rem}[E(x)/g(x)] = \text{Rem}[(x^i+x^j)/g(x)] = \text{Rem}[x^i(x^{j-i}+1)/g(x)] \ .$$

Since $g(0) \neq 0$, we know that g(x) has no factors of x so the x^i cancels nothing in g(x), so the only way for s(x) to be 0 is if

$$\text{Rem}[(x^{j-i}+1)/g(x)] = 0$$

which we rewrite in GF(2) as

$$\text{Rem}[(x^{j-i} - 1)/g(x)] = 0 \qquad (*)$$

The maximum value of j-i is (n-1)-(0) = n-1. If the period of g(x) is n, then (*) cannot be true, since the period s of g(x) is the smallest s such that (x^s-1) is divisible by g(x). Then we get $s(x) \neq 0$ and the double-bit error will be detected.

This proof requires that g(x) divide evenly into $x^n - 1$ *and* that n be the period of g(x).

Fact 4: If $g(0) \neq 0$ *and* $g(x) = (x-1)f(x)$ *and* g(x) has period n, a cyclic code generated by g(x) over GF(2) detects all single-bit, double-bit, triple-bit and all other odd-number-bit errors. (F.4)

Proof: Such a g(x) meets the criteria for Facts 1,2 and 3 so we can take the union of the detections of each.

Definition: A **burst error** of length (extent) r means any number of symbol errors occurring within a sequential set of powers x^i to x^{i+r-1}. For example, if a,b,c,d are non-zero elements of GF(p), the error

pattern $E(x) = ax^3 + bx^5 + cx^9$ would be the error polynomial for a burst error of length r = 7. Other E(x) of length 7: $ax^4 + bx^{10}$, $ax^2 + bx^4 + cx^6 + dx^8$. For GF(2) all coefficients are of course 1.

Fact 5: If $g(0) \neq 0$, a cyclic code generated by g(x) over GF(p) detects all burst errors of length n-k or smaller. (F.5)

Proof: The error pattern can be written $E(x) = x^i f(x)$ where f(x) has degree $r-1 \leq n-k-1$ and $f(x) \neq 0$. The syndrome is

$$s(x) = \text{Rem}[E(x)/g(x)] = \text{Rem}[x^i f(x)/g(x)] .$$

As before, x^i cancels nothing in g(x) if $g(0) \neq 0$, so the only way to get s(x) = 0 is if

$$\text{Rem}[f(x)/g(x)] = 0 .$$

But since g(x) has degree n-k and f(x) has degree $\leq$ n-k-1, this remainder is just $f(x) \neq 0$. QED.

Notice that it was not required that g(x) divide evenly into $x^n - 1$.

Fact 6: The cyclic code of Fact 5 detects all burst errors of length $r \leq n-k$. It does not detect all burst errors for r > n-k, but statistically it can detect a lot of them. For GF(2), here are the conclusions:

fraction of burst errors NOT detected for $r = (n-k) + 1$ = $1/2^{(n-k-1)}$

fraction of burst errors NOT detected for $r > (n-k) + 1$ = $1/2^{(n-k)}$ (F.6)

For example, if n-k = 32 as in CRC-32, then $1/2^{(n-k-1)} = 1/2^{31} \sim 10^{-9}$. For such a code, only one burst error out of a billion goes undetected even if the burst extent is the entire length-n packet! This means that almost all multi-symbol errors of any arrangement will be detected. And *all* burst errors of extent 32 or less are detected.

Proof: See Theorem 6 of the original Peterson and Brown CRC paper appearing in the References.