Cyclic Redundancy Check (CRC) Example, Part 1

Sean E. O'Connor

artifex@seanerikoconnor.freeservers.com

1. An Example with CRC-16

The CRC-16 generator polynomial is

In[22]:= $g = x^{16} + x^{15} + x^2 + 1;$

Let a sample message be 0102_{16}, which we will encode as the coefficients of the polynomial,

In[23]:= $i = x^8 + x;$

Let's assume we are encoding the message bit stream $\mathbf{0}E\,0\,000\,000\,105\,020\,063\,656\,E\,74\,757\,261\,00_{16}$. The binary digits will be the coefficients of our message polynomial i(x), with the least significant bit being the constant term of the polynomial:

In[24]:= $i = x^{123} + x^{122} + x^{121} + x^{88} + x^{82} + x^{80} + x^{73} + x^{62} + x^{61} + x^{57} + x^{56} + x^{54} + x^{53} + x^{50} + x^{48} + x^{46} + x^{45} + x^{43} + x^{42} + x^{41} + x^{38} + x^{37} + x^{36} + x^{34} + x^{30} + x^{29} + x^{28} + x^{26} + x^{24} + x^{22} + x^{21} + x^{20} + x^{17} + x^{14} + x^{13} + x^{8};$

Enter the code's blocklength n and message length k, and compute the the number of parity bits n-k.

In[25]:= $n = 2^{15} - 1$

Out[25]= 32 767

In[26]:= $k = n - 16$

Out[26]= 32 751

In[27]:= $n - k$

Out[27]= 16

For systematic encoding, the parity is p(x) = $[-x^{n-k}\, i(x)]$ mod g(x) where we do modulo 2 arithmetic on the polynomial coefficients.

In[28]:= `p = PolynomialMod[`x^{n-k}` i, {g, 2}]`

Out[28]= $1 + x + x^2 + x^3 + x^6 + x^7 + x^8 + x^{10} + x^{12} + x^{13}$

Writing the polynomial coefficients in binary we get the parity, $0011\ 0101\ 1100\ 1111\ _2 = 35CF\ _{16}$

Compute the systematically encoded codeword
c(x) = $x^{n-k}\, i(x)$ + p(x).

In[29]:= `c = Expand[`x^{n-k}` i + p]`

Out[29]= $1 + x + x^2 + x^3 + x^6 + x^7 + x^8 + x^{10} + x^{12} + x^{13} + x^{24} + x^{29} + x^{30} + x^{33} + x^{36} + x^{37} + x^{38} + x^{40} + x^{42} + x^{44} + x^{45} + x^{46} + x^{50} + x^{52} + x^{53} + x^{54} + x^{57} + x^{58} + x^{59} + x^{61} + x^{62} + x^{64} + x^{66} + x^{69} + x^{70} + x^{72} + x^{73} + x^{77} + x^{78} + x^{89} + x^{96} + x^{98} + x^{104} + x^{137} + x^{138} + x^{139}$

Compute the shifted syndrome s'(x) = $[x^{n-k}\,c(x)]$ mod g(x), modulo 2 on the polynomial coefficients. We should get zero.

```
In[30]:= p = PolynomialMod[x^(n-k) c, {g, 2}]
Out[30]= 0
```

Add error to the codeword.

```
In[31]:= cerror1 = c + x^11;
```

Compute the shifted syndrome s'(x) = $[x^{n-k}\,c(x)]$ mod g(x) modulo 2 on the polynomial coefficients. We should get a non-zero answer.

```
In[32]:= s = PolynomialMod[x^(n-k) cerror1, {g, 2}]
Out[32]= 1 + x + x^12 + x^13 + x^15
```

On the other hand, if we add a multiple of a codeword, we won't see the error.

```
In[33]:= cerror2 = c + x^2 g;

In[34]:= s = PolynomialMod[x^(n-k) cerror2, {g, 2}]
Out[34]= 0
```