Cyclic Redundancy Check (CRC) Example, Part 3

Sean E. O'Connor

artifex@seanerikoconnor.freeservers.com

1. An Example with CRC-32Q

In[301]:= `g = (x + 1)` $\left(x^{31} + x^{23} + x^{22} + x^{15} + x^{14} + x^{7} + x^{4} + x^{3} + 1\right)$

Out[301]= $(1 + x)\left(1 + x^3 + x^4 + x^7 + x^{14} + x^{15} + x^{22} + x^{23} + x^{31}\right)$

In[302]:= `g = PolynomialMod[ Expand[ g ], 2 ]`

Out[302]= $1 + x + x^3 + x^5 + x^7 + x^8 + x^{14} + x^{16} + x^{22} + x^{24} + x^{31} + x^{32}$

Let a sample message be

In[303]:= `i =` $x^8 + x$

Out[303]= $x + x^8$

Enter the code's blocklength and message length.

In[304]:= `n =` $2^{32} - 1$

Out[304]= 4 294 967 295

In[305]:= `k = n - 32`

Out[305]= 4 294 967 263

In[306]:= `n - k`

Out[306]= 32

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

In[307]:= `p = PolynomialMod[` x^{n-k} `i, {g, 2}]`

Out[307]= $1 + x + x^2 + x^3 + x^6 + x^7 + x^8 + x^{12} + x^{13} + x^{14} + x^{16} + x^{17} + x^{22} + x^{23} + x^{24} + x^{25}$

Writing the polynomial coefficients in binary, we get
$0011\ 1100\ 0011\ 0111\ 0001\ 1100\ 1111\ _2 = 03C371CF\ _{16}$

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

In[308]:= `c = Expand[` x^{n-k} `i + p ]`

Out[308]= $1 + x + x^2 + x^3 + x^6 + x^7 + x^8 + x^{12} + x^{13} + x^{14} + x^{16} + x^{17} + x^{22} + x^{23} + x^{24} + x^{25} + x^{33} + x^{40}$

In[309]:=
```
s = PolynomialMod[x^(n-k) c, {g, 2}]
```
Out[309]= 0

Add error to the codeword.

In[310]:=
```
cerror1 = c + x^11
```
Out[310]= $1 + x + x^2 + x^3 + x^6 + x^7 + x^8 + x^{11} + x^{12} + x^{13} + x^{14} + x^{16} + x^{17} + x^{22} + x^{23} + x^{24} + x^{25} + x^{33} + x^{40}$

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[311]:=
```
p = PolynomialMod[x^(n-k) cerror1, {g, 2}]
```
Out[311]= $1 + x^6 + x^7 + x^8 + x^{10} + x^{11} + x^{12} + x^{14} + x^{16} + x^{17} + x^{22} + x^{23} + x^{25} + x^{26} + x^{31}$

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

In[312]:=
```
cerror2 = Expand[ PolynomialMod[ c + x^2 g, 2]]
```
Out[312]= $1 + x + x^5 + x^6 + x^8 + x^9 + x^{10} + x^{12} + x^{13} + x^{14} + x^{17} + x^{18} + x^{22} + x^{23} + x^{25} + x^{26} + x^{34} + x^{40}$

In[313]:=
```
p = PolynomialMod[x^(n-k) (cerror2), {g, 2}]
```
Out[313]= 0