MEMO
Rev B, 20 January 2001
William I. Clement, Ph.D.

COS DCE Cyclic Redundancy Code Computations

Standard Cyclic Redundancy Codes are based on polynomial division. The data for which a CRC is being calculated are treated as the coefficients of a large polynomial. This polynomial is divided by a "generator polynomial" of some modest order (e.g. 8, 16, 32), resulting in a remainder polynomial of order less than the generator. The coefficients of this remainder polynomial are collectively known as the CRC. This is a linear operation and, as such, it is a simple matter to pad the data stream with some additional data values in order to yield a specified CRC.

Due to the nonlinear nature of the CRC algorithm used for COS DCE (it is not true polynomial division), one cannot use this standard method of generating a desired CRC. Instead, the following analysis indicates how such a computation is made.

Designating the current value of the 16-bit CRC as $\mathbb{C}$:

$$\mathbb{C} = (C_{15}, C_{14}, C_{13}, C_{12}, C_{11}, C_{10}, C_9, C_8, C_7, C_6, C_5, C_4, C_3, C_2, C_1, C_0)$$

and the next 16 bits of data to be processed as $\mathbb{D}$:

$$\mathbb{D} = (D_{15}, D_{14}, D_{13}, D_{12}, D_{11}, D_{10}, D_9, D_8, D_7, D_6, D_5, D_4, D_3, D_2, D_1, D_0)$$

and the CRC value after these 16 data bits have been processed as $\mathbb{X}$:

$$\mathbb{X} = (X_{15}, X_{14}, X_{13}, X_{12}, X_{11}, X_{10}, X_9, X_8, X_7, X_6, X_5, X_4, X_3, X_2, X_1, X_0)$$

we find that:

X_{15}	=	$C_{11} \oplus C_{10} \oplus C_7 \oplus C_3 \oplus D_{11} \oplus D_{10} \oplus D_7 \oplus D_3$
X_{14}	=	$C_{10} \oplus C_9 \oplus C_6 \oplus C_2 \oplus D_{10} \oplus D_9 \oplus D_6 \oplus D_2$
X_{13}	=	$C_9 \oplus C_8 \oplus C_5 \oplus C_1 \oplus D_9 \oplus D_8 \oplus D_5 \oplus D_1$
X_{12}	=	$C_{15} \oplus C_8 \oplus C_7 \oplus C_4 \oplus C_0 \oplus D_{15} \oplus D_8 \oplus D_7 \oplus D_4 \oplus D_0$
X_{11}	=	$C_{15} \oplus C_{14} \oplus C_{11} \oplus C_{10} \oplus C_6 \oplus D_{15} \oplus D_{14} \oplus D_{11} \oplus D_{10} \oplus D_6$
X_{10}	=	$C_{14} \oplus C_{13} \oplus C_{10} \oplus C_9 \oplus C_5 \oplus D_{14} \oplus D_{13} \oplus D_{10} \oplus D_9 \oplus D_5$
X_9	=	$C_{15} \oplus C_{13} \oplus C_{12} \oplus C_9 \oplus C_8 \oplus C_4 \oplus D_{15} \oplus D_{13} \oplus D_{12} \oplus D_9 \oplus D_8 \oplus D_4$
X_8	=	$C_{15} \oplus C_{14} \oplus C_{12} \oplus C_{11} \oplus C_8 \oplus C_7 \oplus C_3 \oplus D_{15} \oplus D_{14} \oplus D_{12} \oplus D_{11} \oplus D_8 \oplus D_7 \oplus D_3$
X_7	=	$C_{15} \oplus C_{14} \oplus C_{13} \oplus C_{11} \oplus C_{10} \oplus C_7 \oplus C_6 \oplus C_2 \oplus D_{15} \oplus D_{14} \oplus D_{13} \oplus D_{11} \oplus D_{10} \oplus D_7 \oplus D_6 \oplus D_2$
X_6	=	$C_{14} \oplus C_{13} \oplus C_{12} \oplus C_{10} \oplus C_9 \oplus C_6 \oplus C_5 \oplus C_1 \oplus D_{14} \oplus D_{13} \oplus D_{12} \oplus D_{10} \oplus D_9 \oplus D_6 \oplus D_5 \oplus D_1$
X_5	=	$C_{13} \oplus C_{12} \oplus C_{11} \oplus C_9 \oplus C_8 \oplus C_5 \oplus C_4 \oplus C_0 \oplus D_{13} \oplus D_{12} \oplus D_{11} \oplus D_9 \oplus D_8 \oplus D_5 \oplus D_4 \oplus D_0$
X_4	=	$C_{15} \oplus C_{12} \oplus C_8 \oplus C_4 \oplus D_{15} \oplus D_{12} \oplus D_8 \oplus D_4$
X_3	=	$C_{15} \oplus C_{14} \oplus C_{11} \oplus C_7 \oplus C_3 \oplus D_{15} \oplus D_{14} \oplus D_{11} \oplus D_7 \oplus D_3$
X_2	=	$C_{14} \oplus C_{13} \oplus C_{10} \oplus C_6 \oplus C_2 \oplus D_{14} \oplus D_{13} \oplus D_{10} \oplus D_6 \oplus D_2$
X_1	=	$C_{13} \oplus C_{12} \oplus C_9 \oplus C_5 \oplus C_1 \oplus D_{13} \oplus D_{12} \oplus D_9 \oplus D_5 \oplus D_1$

X_0	=	$C_{12} \oplus C_{11} \oplus C_8 \oplus C_4 \oplus C_0 \oplus D_{12} \oplus D_{11} \oplus D_8 \oplus D_4 \oplus D_0$

Our task is to find the data $\mathbb{D}$ which, combined with the known $\mathbb{C}$, yields a desired $\mathbb{X}$.

Notice the symmetry in this solution. In every expression, wherever a bit from the current CRC (C_x) exists, the corresponding data bit (D_x) is also present. Thus, defining $B_x = C_x \oplus D_x$, the table may be rewritten:

X_{15}	=	$B_{11} \oplus B_{10} \oplus B_7 \oplus B_3$
X_{14}	=	$B_{10} \oplus B_9 \oplus B_6 \oplus B_2$
X_{13}	=	$B_9 \oplus B_8 \oplus B_5 \oplus B_1$
X_{12}	=	$B_{15} \oplus B_8 \oplus B_7 \oplus B_4 \oplus B_0$
X_{11}	=	$B_{15} \oplus B_{14} \oplus B_{11} \oplus B_{10} \oplus B_6$
X_{10}	=	$B_{14} \oplus B_{13} \oplus B_{10} \oplus B_9 \oplus B_5$
X_9	=	$B_{15} \oplus B_{13} \oplus B_{12} \oplus B_9 \oplus B_8 \oplus B_4$
X_8	=	$B_{15} \oplus B_{14} \oplus B_{12} \oplus B_{11} \oplus B_8 \oplus B_7 \oplus B_3$
X_7	=	$B_{15} \oplus B_{14} \oplus B_{13} \oplus B_{11} \oplus B_{10} \oplus B_7 \oplus B_6 \oplus B_2$
X_6	=	$B_{14} \oplus B_{13} \oplus B_{12} \oplus B_{10} \oplus B_9 \oplus B_6 \oplus B_5 \oplus B_1$
X_5	=	$B_{13} \oplus B_{12} \oplus B_{11} \oplus B_9 \oplus B_8 \oplus B_5 \oplus B_4 \oplus B_0$
X_4	=	$B_{15} \oplus B_{12} \oplus B_8 \oplus B_4$
X_3	=	$B_{15} \oplus B_{14} \oplus B_{11} \oplus B_7 \oplus B_3$
X_2	=	$B_{14} \oplus B_{13} \oplus B_{10} \oplus B_6 \oplus B_2$
X_1	=	$B_{13} \oplus B_{12} \oplus B_9 \oplus B_5 \oplus B_1$
X_0	=	$B_{12} \oplus B_{11} \oplus B_8 \oplus B_4 \oplus B_0$

Our task becomes one of finding the $\mathbb{B}$ which yields a desired $\mathbb{X}$ and then, using known $\mathbb{C}$, solving for the required data word $\mathbb{D}$ using the relationship

$$\mathbb{B} = \mathbb{C} \oplus \mathbb{D} \qquad \rightarrow \qquad \mathbb{D} = \mathbb{C} \oplus \mathbb{B}$$

Unfortunately, analytical solution to this set of simultaneous nonlinear equations in B_x is difficult. However, a simple computational solution involves generating the 2^{16} possible values of $\mathbb{B}$ and finding those which yield values of $\mathbb{X}$ in which only one bit is '1' and all else are '0'. This is equivalent to saying we are finding those values of $\mathbb{B}$ that toggle individual bits of $\mathbb{X}$. Then, given $\mathbb{C}$ we can solve for the data value $\mathbb{D}$ which produces that $\mathbb{X}$. Exhaustive search of these 2^{16} possibilities results in an interesting finding. There are exactly 16 values of $\mathbb{B}$ which uniquely serve our purposes – 16 values which each toggle a different bit in $\mathbb{X}$. (Also, to produce $\mathbb{X} = \mathbf{0}$, the necessary and sufficient condition is $\mathbb{B} = \mathbf{0}$ which, in turn, requires $\mathbb{D} = \mathbb{C}$.) The table below shows the 16 values of $\mathbb{B}$ which toggle individual bits in $\mathbb{X}$.

$\mathbb{X}$ Bit Toggled	$\mathbb{B}$ Value Producing the Bit Change (hex)
X_0	9D71
X_1	2AC3
X_2	5586
X_3	AB0C
X_4	4639
X_5	8C72
X_6	08C5
X_7	118A
X_8	2314
X_9	4628
X_{10}	8C50
X_{11}	0881
X_{12}	1102
X_{13}	2204
X_{14}	4408
X_{15}	8810

Because all terms in $\mathbb{X}$ ($X_{15}\ldots X_0$) are formed by XORing terms of $\mathbb{B}$ ($B_{15}\ldots B_0$), it can be shown that to toggle multiple bits in $\mathbb{X}$, simply XOR the corresponding values of $\mathbb{B}$ found in the above table. Thus, any of the 2^{16} possible values of $\mathbb{X}$ may be obtained by combination of the corresponding values of $\mathbb{B}$ from the table. An example illustrates the procedure.

Example: For a block of 'N' bytes, compute a new value for the last two bytes so that the overall CRC for the block is **1234** (hexadecimal). Assume the CRC for the first 'N-2' bytes is **93C5**.

Solution: The desired CRC, $\mathbb{X}$ = **1234**, written in binary is $\mathbb{X}$ = 0001001000110100. Thus, bits 2, 4, 5, 9, and 12 need to be set to '1' and all others to '0'. Forming the XOR of the five corresponding values of $\mathbb{B}$ from the table (those for X_2, X_4, X_5, X_9, and X_{12}), we have

$$\mathbb{B} = 5586 \oplus 4639 \oplus 8C72 \oplus 4628 \oplus 1102 = \mathbf{C8E7}$$

From this, we solve for the data word $\mathbb{D}$ which produces this $\mathbb{B}$

$$\mathbb{D} = \mathbb{C} \oplus \mathbb{B} = 93C5 \oplus C8E7 = \mathbf{5B22}$$

Since the COS DCE CRC algorithm processes a byte at a time, data byte **5B** is processed first (after the 'N-2' bytes, of course), followed by data byte **22**. The result is $\mathbb{X}$ = **1234**, as desired.