Technical Evaluation Report
"COS DCE FSW CRC Memo"

Date:	October 25, 2001
Document Number:	COS-11-0035
Revision:	Initial Release
Contract No.:	NAS5-98043
CDRL No.:	

Prepared By: _____ _____

W. Clement, Clement Engineering, Inc. Date

Reviewed By: _____ _____

K. Brownsberger, COS Sr. Software Scientist, CU/CASA Date

Reviewed By: _____ _____

J. Andrews, COS Experiment Manager, CU/CASA Date

Center for Astrophysics & Space Astronomy
University of Colorado
Campus Box 593
Boulder, Colorado 80309

REVISIONS

Letter	ECO No.	Description	Check	Approved	Date
-		Initial Release			

Original Release Name	Date
Drawn: W. Clement	10-25-01
Reviewed:	
Approved:	

THE UNIVERSITY OF COLORADO
At Boulder
The Center for Astrophysics and Space Astronomy

Technical Evaluation Report
"COS DCE FSW CRC Memo"

Size	Code Indent No.	Document No.	Rev
A		COS-11-0035	-
Scale: N/A			

Table of Contents

1. 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 C:

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

and the next 16 bits of data to be processed as D:

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

and the CRC value after these 16 data bits have been processed as X:

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

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 D which, combined with the known C, yields a desired 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 B which yields a desired X and then, using known C, solving for the required data word D using the relationship

$$B = C \oplus D \quad \rightarrow \quad D = C \oplus B$$

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 B and finding those which yield values of X in which only one bit is '1' and all else are '0'. This is equivalent to saying we are finding those values of B that toggle individual bits of X. Then,

given C we can solve for the data value D which produces that X. Exhaustive search of these 2^{16} possibilities results in an interesting finding. There are exactly 16 values of B which uniquely serve our purposes – 16 values which each toggle a different bit in X. (Also, to produce X = **0**, the necessary and sufficient condition is B = **0** which, in turn, requires D = C.) The table below shows the 16 values of B which toggle individual bits in X.

X Bit Toggled	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 X ($X_{15}…X_0$) are formed by XORing terms of B ($B_{15}…B_0$), it can be shown that to toggle multiple bits in X, simply XOR the corresponding values of B found in the above table. Thus, any of the 2^{16} possible values of X may be obtained by combination of the corresponding values of 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, X = **1234**, WRITTEN IN BINARY IS 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 B FROM THE TABLE (THOSE FOR X_2, X_4, X_5, X_9, AND X_{12}), WE HAVE

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

FROM THIS, WE SOLVE FOR THE DATA WORD D WHICH PRODUCES THIS B

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

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 X = **1234**, AS DESIRED.