16-bit CRC polynomial selection.

Pat Thaler
Agilent Technologies
28 August 2003

The following summarizes the reasons behind the choice of the polynomial 0x18bb7 for the 16-bit CRC in data integrity. The selection of this code was done in a similar manner to the selection of the 32-bit CRC used by iSCSI and SCTP. The results are summarized here. These results rely on literature cited below and to understand them in depth, that literature should be studied. These results of these papers are also summarized in RFC 3385 iSCSI CRC Considerations which can be found on the IETF site.

From [1]: "Often, it is assumed that the probability of undetected error for error detection codes is upper bounded by 2^{-r} where r is the number of redundant (parity [CRC]) bits. This upper bound is not correct for many codes, however, especially shortened cyclic codes."

They go on to show that for some polynomials, the error performance is significantly reduced when used as shortened cyclic codes [1]. The cycle length of a 16-bit primitive polynomial is $2^{16} - 1$. When used to protect data shorter than this length, the polynomial is being used as a shortened cyclic code. For instance, when we protect a 512 byte data block with a 16-bit CRC we are using a shortened cyclic code. As is shown in [1], the reduction in probability of error detection for some codes when used as a shortened cyclic code can be orders of magnitude. Fortunately, some codes, termed "proper" codes, do not have this problem.

A code is termed "proper" if it retains the desired behavior of

$P_{ud}(N,p) \leq P_{ud}(N,0.5)$ for any p $0 \leq p \leq 0.5$

where $P_{ud}(N,p)$ is the probability of an undetected error for block length, N, and probability of bit error, p.

It is conjectured [1] that polynomials that produce proper codes are those that have approximately m/2 non-zero coefficients where m is the degree of the polynomial. Polynomials with few non-zero terms do not appear to perform as well.

[2] reports on hardware developed to identify proper polynomials. It contains a table of polynomials from degree 7 to degree 38 that were found. The proposed polynomial, 0x18bb7, was taken from this table. The table shows the polynomials in octal rather than hex notation and the parity bits column assumes the polynomial will be multiplied by 1+x so the 16-bit primitive polynomial is in the row with Parity Bits (R) equal to 17 and it is shown as 305667 octal which is

18bb7 hex. The behavior of the polynomial as proper does not require the multiplication by 1+x.

[3] shows that proper behavior is also important for burst error detection. Specifically, it contains a proof that the probability of burst error detection given a burst of length b with probability of error p for each bit within the burst is equal to the probability of undetected errors for the same code shortened to b, the length of the burst, with probability of bit error, p. Thus a code that is not proper also exhibits diminished ability to detect burst errors.

The figure below is as an example from [3] which compares the P_{ud} of a proper 16-bit CRC and two other 16-bit CRCs given a burst of 20 bits with probability of bit error within the burst between 0 and 1.

IEEE TRANSACTIONS ON COMMUNICATIONS, VOL. 42, NO. 1, JANUARY 1994

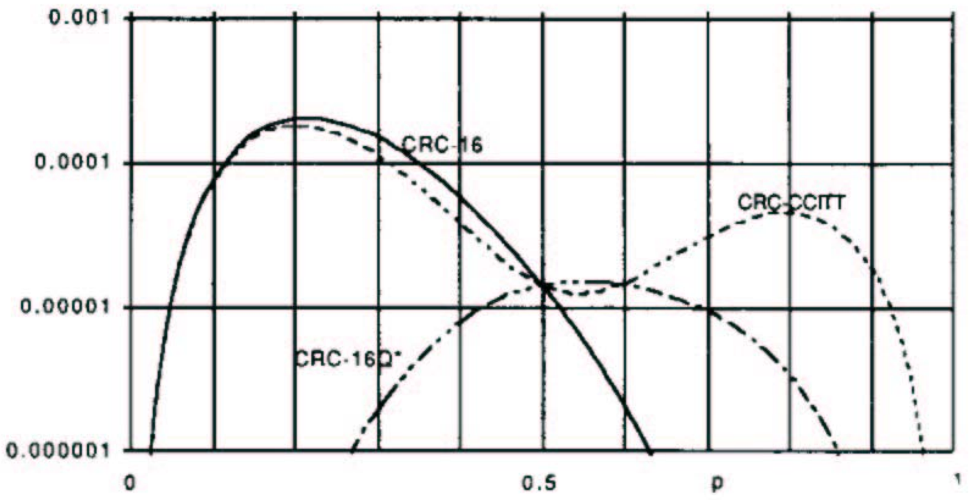

Fig. 1. $P_{ud}(p|b = 20)$ for CRC-16, CRC-CCITT, and CRC-16Q*.

A proper CRC polynomial was chosen for Data Integrity to give predictable performance for error detection for burst and bit errors for all BERs.

[1] J.K. Wolf, R.D. Blackeney, "An Exact Evaluation of the Probability of Undetected Error for Certain Binary CRC Codes", Proc. MILCOM – IEEE 1988.

[2] J.K. Wolf, R.D. Blackeney, "An Exact Evaluation of the Probability of Undetected Error for Certain Shortened Binary CRC Codes", Proc. MILCOM – IEEE 1988.

[3] J.K. Wolf and Dexter Chun, "The single burst error performance of binary cyclic codes", IEEE Transactions on Communications COM-42:11-13, January 1994.

[4] D. Sheinwald, J. Satran, P. Thaler, V. Cavanna, “Internet Protocol Small Computer System Interface (iSCSI) Cyclic Redundancy Check (CRC)/Checksum Considerations”, IETF RFC 3385, September 2002