CS3200: Computer Networks

Lecture 9

IIT Palakkad

19 Aug, 2019

Cyclic Redundancy Check (CRC)

- Sender and receiver must agree upon a **generator polynomial**, $G(x)$, in advance.
- Both the high- and low-order bits of the generator must be 1.
- To compute the CRC for some frame with m bits corresponding to the polynomial $M(x)$, the frame must be longer than the generator polynomial.
- The idea is to append a CRC to the end of the frame in such a way that the polynomial represented by the checksummed frame is divisible by $G(x)$.

Cyclic Redundancy Check (CRC)

Algorithm for computing CRC

1. Let r be the degree of $G(x)$. Append r zero bits to the low-order end of the frame so it now contains $m + r$ bits and corresponds to the polynomial $x^r M(x)$.
2. Divide the bit string corresponding to $G(x)$ into the bit string corresponding to $x^r M(x)$, using modulo 2 division.
3. Subtract the remainder (which is always r or fewer bits) from the bit string corresponding to $x^r M(x)$ using modulo 2 subtraction. The result is the checksummed frame to be transmitted. Call its polynomial $T(x)$.

Cyclic Redundancy Check (CRC)

- Why show the low-order bits of $G(x)$ be 1?
- Why do we consider $x^r M(x)$ instead of $M(x)$?
- What kind of errors will be detected?

CRC Error Detection

- Imagine that a transmission error occurs, so that instead of the bit string for $T(x)$ arriving, $T(x) + E(x)$ arrives.
- Each 1 bit in $E(x)$ corresponds to a bit that has been inverted.
- Upon receiving the checksummed frame, the receiver divides it by $G(x)$; that is, it computes $[T(x) + E(x)]/G(x)$.
- $T(x)/G(x)$ is 0, so the result of the computation is simply $E(x)/G(x)$.

CRC Error Detection

- Suppose the i^{th} bit was received in error. Then, $E(x) = x^i$.
- When will this be detected?
- What about two isolated single-bit errors, i.e., $E(x) = x^i + x^j$, where $i > j$?
- For example, $x^15 + x^14 + 1$ will not divide $x^k + 1$ for any value of k below 32,768.

CRC Error Detection

- What about odd number of errors? Then, $E(X)$ contains an odd number of terms (e.g., $x^5 + x^2 + 1$)?
- Interestingly, no polynomial with an odd number of terms has $x + 1$ as a factor in the modulo 2 system.
- What about burst errors?
- A burst error of length k can be represented by $x^i(x^{k-1} + \cdots + 1)$.
- Can detect burst errors of length $\leq r$, where r is the degree of $G(x)$.