Computer Networks

Lecture 2: The Ethernet

Marcin Bieńkowski

2.1 CRC Checksum

2.1.1 Polynomials

CRC is based on dividing polynomials whose coefficients are $\{0, 1\}$ (modulo 2). First, we present some examples on how to operate on such polynomials. Take $A(x) = x^5 + x^3 + x^2 + 1$ and $B(x) = x^3 + x$. Their sum is $A(x) + B(x) = x^5 + x^2 + x + 1$. Note that $A(x) + A(x) \equiv 0$ and hence $-A(x) = A(x)$. Thus, subtracting is the same as adding: $B(x) - A(x) = B(x) + A(x)$. One may also multiply polynomials (as we would multiply "ordinary" polynomials, but remembering that their coefficients are taken modulo 2). For example, $(x + 1) \cdot (x + 1) = x^2 + x + x + 1 = x^2 + 1$.

One may also divide such polynomials. In particular, take any polynomials $A(x)$ and $B(x) \not\equiv 0$. and let k be the degree of $B(x)$. Then there exists exactly one pair of polynomials $Q(x)$ and $R(x)$, such that

$$A(x) = Q(x) \cdot B(x) + R(x) \ ,$$

where $R(x)$ is a polynomial of degree at most $k - 1$. For example, if $A(x) = x^{10} + x^8 + x^3$ and $B(x) = x^3 + x^2 + 1$, then $Q(x) = x^7 + x^6 + x^4 + x$ and $R(x) = x$.

2.1.2 Computing CRC

For computing CRC, we change the transmitted bit string $\overline{m}$ into a polynomial $M(x)$ (for example $10100001 \rightarrow x^7 + x^5 + 1$). Assume that we want to generate r-bit control sum. For this we need a polynomial $G(x)$ of degree r known to sender and receiver.[1] Our goal is to create a r-bit checksum $\overline{s}$, such that the polynomial corresponding to $\overline{ms}$ is divisible by $G(x)$. We send $\overline{ms}$ over the wire, and the receiver checks whether it is divisible by $G(x)$. If it is not, then certainly, there were errors during transmission. If it is divisible, then there is still small chance that there were errors, but usually the data is intact.

How can we compute $\overline{s}$? Let $S(x)$ be a polynomial (of degree $r - 1$) corresponding to $\overline{s}$. Then $\overline{ms}$ corresponds to $x^r \cdot M(x) + S(x)$. Recall that $G(x)$ has to divide $x^r \cdot M(x) + S(x)$. Let $S(x)$ be the remainder of dividing $x^r \cdot M(x)$ over $G(x)$, i.e., $x^r \cdot M(x) = G(x) \cdot Q(x) + S(x)$. Clearly, $S(x)$ has degree at most $r - 1$. Moreover, $x^r \cdot M(x) + S(x) = G(x) \cdot Q(x) + S(x) + S(x) = G(x) \cdot Q(x)$, i.e., is divisible by $G(x)$!

For example, assume we want to transmit a message $\overline{m} = 10100001$ and the CRC polynomial is $G(x) = x^3 + x^2 + 1$. Then, the checksum will have 3 bits, i.e., $r = 3$. Thus, $x^r \cdot M(x) = x^{10} + x^8 + x^3 = (x^7 + x^6 + x^4 + x) \cdot G(x) + x$. The remainder $S(x) = x$ corresponds to the 3-bit string $\overline{s} = 010$, which is appended at the end of the message.

[1] For example, in the Ethernet we use 32-bit control sum whose polynomial is $G(x) = x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$.