Jens Andersson, Elektro- och informationsteknik, LTH
2012-09-06

Ett alternativt sätt att förklara/härleda CRC

Vi vill skicka ett meddelande i form av en följd av ettor och nollor, en bitström. Vi låter polynomet M(x) representera meddelandet. Dessutom vill vi sända med extrabitar som gör att vi kan upptäcka fel. Extrabitarna låter vi representeras av ett annat polynom som vi kallar R(x). Därför skickar vi en bitström som motsvaras av $M(x)*x^k + R(x)$. k är antalet bitar felupptäckande information vi skickar, vilket innebär att grad(R(x)) = k - 1.

Mottagaren tar emot en bitström som vi representerar med $M(x)*x^k + R(x) + E(x)$. E(x) motsvarar alla felaktiga bitar som mottagaren tar emot. Är E(x) = 0 har inga fel uppstått, är E(x) > 0 har fel uppstått.

Division av bitströmmar är lätt att implementera i nätadaptern. Låt oss således använda division! Vi tar fram en speciell bitström som motsvarare ett speciellt polynom. Vi kallar bitströmmen/polynomet för generatorn. Generatorpolynomet C(x) har vissa speciella egenskaper, bland annat är längden på generatorn k bitar vilket är samma sak som att grad(C(x)) = k.

Låt oss också hitta ett R(x) så att $M(x)*x^k + R(x)$ är jämnt delbart med C(x). Det kan vi skriva så här:

$$[M(x)*x^k + R(x)] / C(x) = f(x) + 0$$

$$M(x)*x^k / C(x) + R(x) /C(x) = f(x) + 0$$

$$R(x) / C(x) = f(x) - M(x)*x^k / C(x)$$

R(x) / C(x) är således skillnaden mellan f(x) och $M(x)*x^k / C(x)$, dvs R(x) är resten vi får om vi utför $M(x)*x^k / C(x)$.

I mottagaren utför vi följande division

$$[M(x)*x^k + R(x) + E(x)]/ C(x)$$

Det kan skrivas om

$$[M(x)*x^k + R(x)]/C(x) + E(x) / C(x)$$

Men resten vi får om vi utför $[M(x)*x^k + R(x)] / C(x)$ är ju 0; det var ju så vi definierade R(x) från början. Dvs om det uppstår någon rest vid divisionen i mottagaren måste det bero på att E(x) är skild från 0 vilket indikerar att ett fel har uppstått.