Let $M(x)$ be the message, and $G(x)$ be the generator polynomial, both as defined in the paper and the draft. $C(x)$ also defined in the paper (it is the initial value of the CRC register). $n = \deg G(x)$ and k is the number of bits in $M(x)$.

Here is a semi-proof by contradiction that **prefixing** and **adding** *do not necessarily* lead to the same remainder, $R(x)$.

All we do is factorize the expression $M'(x)$, into an *independent* and *dependent* on the initial value of the CRC terms. Please note that the *independent* terms depend only on the message, $M(x)$, and the *dependent* term is the greatest constant[1] term in both expressions, thus we can compare them.

Prefixing: This method is also described in a paper by Williams (*A Painless Guide to Error Detection Algorithms, 1993*)

$$\begin{aligned} M'(x) &= x^n M(x) + C(x) \\ &= x^n M(x) + x^n x^k I(x) \\ &= x^n (M(x) + x^k I(x)) \\ &= x^n \left[M(x) + x^k \underbrace{I(x)} \right] \end{aligned}$$

Adding: I.e. complementing the first 32 MSb.

$$\begin{aligned} M'(x) &= x^n M(x) + x^k I(x) \\ &= x^n \left(M(x) + x^k x^{-n} I(x) \right) \\ &= x^n \left[M(x) + x^k \underbrace{x^{-n} I(x)} \right] \end{aligned}$$

This means that when a remainder is computed from $M'(x)$ it will *not* necessarily be the same for both methods. Thus, the examples for CRCs in the draft will be different if one used **adding** or **prefixing**.

This is clearly seen when $M(x) = \sum_{i=0}^{31} x^i$, i.e. 32 1's.

[1] *known*