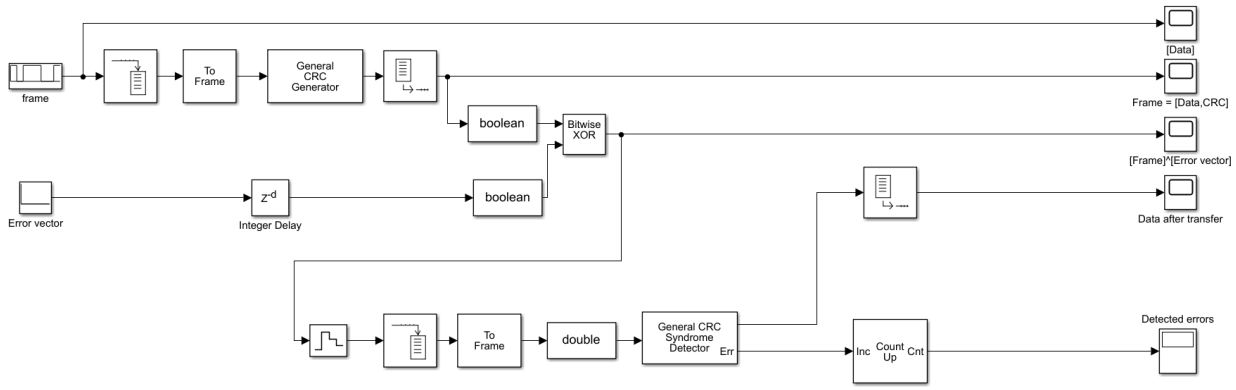
Zabezpečení datových přenosů pomocí CRC

Měření a simulace

Dmitrii Litvin (litvidmi)



A) DETEKČNÍ VLASTNOSTI

- délka rámce = 8 bitů [1 0 1 1 1 0 0 0]
- polynom CRC3 [1 0 1 1]
- crc = [1 1]
- error vector = [0 0 0 0 0 0 0 0], detected errors = 0
- error vector = [0 0 0 0 0 0 0 1], detected errors = 9

1. Hypotézy
   - Je-li chybový vektor posunem generujícího polynomu (násobení obecnou mocninou), chyba není detekována:
     error vector = [0 0 1 0 1 1 0 0], polynom = [1 0 1 1], detected errors = 0
   - Obecněji, je-li chybový vektor beze zbytku dělitelný generujícím polynomem, chyba není detekována:
     error vector = [1 0 1 1 1 0 1 1], polynom = [1 0 1 1], detected errors = 0
   - Každá jednonásobná chyba je detekována, pokud má generující polynom koeficient 1 u x 0 a zároveň má alespoň jeden další člen:
     x + 1 = [1 1] – parity check,
     pro error vector = [1 0 0 0 0 0 0 0], polynom = [1 0 0 1] detected errors = 9
   - Pokud je generující polynom beze zbytku dělitelný polynomem $x \oplus 1$, pak detekuje jakýkoliv lichý počet chyb:
     délka rámce = 12
     Pro CRC10 error vector = [1 1 1 1 1 1 1 1 1 1 1 1], polynom = [1 1 0 0 0 1 1 0 0 1 1] detected errors = 9
   - Pokud $x\ i \oplus 1$ není beze zbytku dělitelné generujícím polynomem pro všechna $i \in \langle 1, n - 1 \rangle$, kde n je délka kódového slova, pak jsou detekovány všechny dvojnásobné chyby:

Pro error vector = [0 1 1 1 1 1 1 1], polynom = [1 0 1 1], detected errors = 9

- Pokud je chybový vektor typu $x\ j\ (x\ t \oplus \ldots \oplus 1)$, kde t je menší nebo rovno stupni generujícího polynomu (shluk chyb s délkou menší nebo rovnou počtu bitů CRC), pak jsou všechny takovéto chyby detekovány:
  Pro error vector = [1 1 0 0 0 0 0 0], polynom degree = 3 (t = 1), j = 7 detected errors = 9

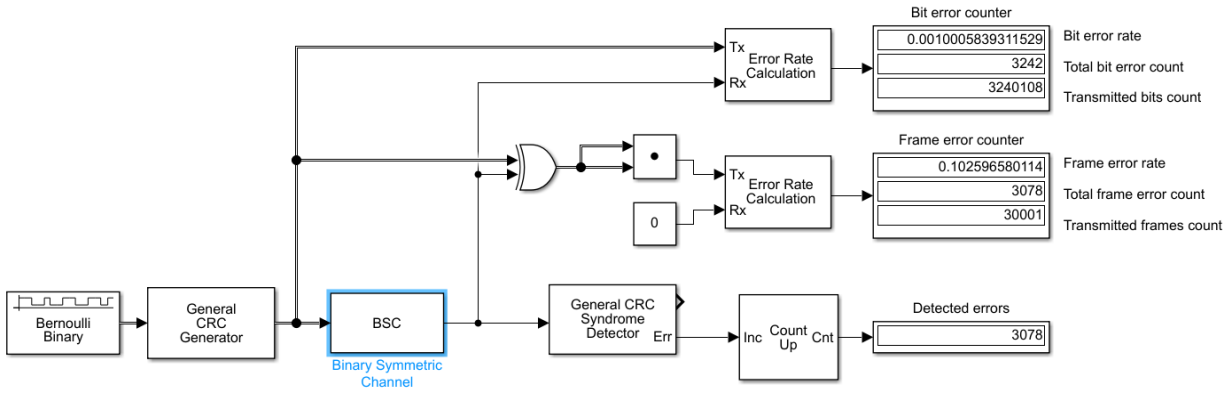
2. Dokázat obecně
   - Pokud je chybový vektor shlukovou chybou s délkou rovnou délce generujícího polynomu (vektor typu $x\ j\ (x\ t{-}1 \oplus \ldots \oplus 1)$, kde t-1 = k je rovno stupni generujícího polynomu), pak pravděpodobnost, že chyba nebude detekována, je 2^(−(k−1)).
   - Pokud je chybový vektor shlukovou chybou s délkou t vyšší než k+1, k je stupeň generujícího polynomu, pak pravděpodobnost, že chyba nebude detekována, je 2^(−k).

   - Tvrzení: lze detekovat **téměř** všechny shlukové chyby délky > *k+1*, kde *k* je stupeň G(x), pokud G(x) obsahuje nenulový konstantní člen
   - Důkaz: Nechť polynom M(x) reprezentuje *n*-bitové datové slovo. Stupeň polynomu M(x) je tedy *n-1*. Pak:
     - existuje 2^n různých datových slov, z nich 2^{n-k} má shodné CRC a jen jedno z nich je to správné (skutečně odeslané)
     - pravděpodobnost, že chyba nebude detekována je tedy:

       $(2^{(n-k)} - 1) / 2^n \approx 2^{-k}$ (pro velká n)

B) SPOLEHLIVOST

- Error probability: 0.001 (1 = 100 %)
  Detected errors = 3078, frame error count = 3078



- Error probability: 0.01 (1 = 100 %)

Detected errors = 19872, frame error count = 19885