Analýza spolehlivosti CRC při detekci chyb

Vít Knobloch, Filip Krul

Květen 2021

1 Příprava simulace

Jako rámec užitečných dat jsem zvolil následující rámec délky deset:

```
[1 0 1 1 1 0 1 0 0 1]
```

Jako generující polynom jsem zvolil polynom stupně tři, reprezentovaný vektorem:

```
[1 0 1 1]
```

Poté jsem nastavil vektor reprezentující chybový polynom na nulový vektor o 13 prvcích a ověřil funkčnost modelu bez chyby.

2 Výsledky simulace a důkazy

2.1 Chybový vektor posunem generujícího

Postupně jsem nastavil chybový vektor na několik různých posunů generujícího polynomu a ani v jednom případě nebyla odhalena chyba.

Platí, že pokud je chybový polynom posunem generujícího (jeho násobkem po vynásobení nějakou mocninou), tak generující polynom dělí chybový beze zbytku. (Výsledek bude právě mocnina použitá k posunu.)

$$E(x) = x^j C(x) \quad \Rightarrow \quad \frac{E(x)}{C(x)} = x^j \tag{1}$$

Důkazem se tak odkáži na další bod.

2.2 Generující polynom dělí chybový beze zbytku

Postupně jsem nastavil chybový polynom na:

```
[0 0 0 0 0 0 0 1 1 1 0 1 0]
[0 0 0 0 0 1 0 1 1 1 0 1 1]
```

Oboje jsou násobky generujícího polynomu, v jednom případě (x^2+x) násobek, v druhém (x^4+1) násobek. Ani v jednom případě nebyla chyba detekována.

Důkaz, že CRC skutečně nemůže odhalit chybu, jejíž polynom je násobkem generujícího, je následující:

Označme $P(x)$ polynom užitečných dat, $C(x)$ generující polynom a $E(x)$ chybový polynom. Platí, že

$$P(x) = C(x)Q(x) + R(x) \tag{2}$$

kde $Q(x)$ je nějaký polynom a $R(x)$ je zbytek po dělení polynomu užitečných dat generujícím polynomem. Při přnosu se k přenášeným datům přičte (modulo 2) chybový polynom

$$P(x) + E(x) = C(x)Q(x) + R(x) + E(x) \tag{3}$$

ten je ale dělitelný generujícím polynomem (z předpokladu), proto platí

$$P(x) + E(x) = C(x)Q(x) + R(x) + C(x)Q'(x) \tag{4}$$

pro nějaký polynom $Q'(x)$. Nyní můžeme vytknout $C(x)$

$$P(x) + E(x) = C(x)[Q(x) + Q'(x)] + R(x) \tag{5}$$

Je zřejmé, že zbytek po dělění polynomu polynomu $P(x) + E(x)$ je $R(x)$, tedy stejný jako v případě $P(x)$, chyba proto nebude detekována. (Pozn.: Z tohoto důkazu také vyplývá, že pokud $E(x)$ není beze zbytku dělitelný $C(x)$, potom změní zbytek po dělení a chyba je odhalena.)

2.3 Jednonásobná chyba u polynomu s alespoň dvěma nenulovými členy

Simulace skutečně odhaluje všechny jednonásobné chyby. V důkazu využijeme důsledku předchodího důkazu a dokážeme, že jednonásobná chyba není beze zbytku dělitelná polynomem s dvěma členy.

Řekneme, že $E(x) = x^k$ a $C(x) = x^j + x^i$, kde $j > i$. Při dělení mohou nastat dva případy:

- $k < j$:
$$\frac{E(x)}{C(x)} = 0 + \frac{R(x)}{C(x)}, R(x) = x^k \tag{6}$$
- $k \leq j$:
$$\frac{E(x)}{C(x)} = x^{k-j} + \frac{x^{k-j+i}}{C(x)} \tag{7}$$

Pokud je stupeň x^{k-j+i} stále větší nebo roven j tak dělení opakujeme. To děláme, tak dlouho až nastane případ kdy kdy zbylý polynom má stupeň nižší než j, a v takovém případě je zbytek nenulový a chyba tedy bude odhalena.

2.4 Chyba liché násobnosti u generujícího polynomu dělitelného polynomem $(x + 1)$

Původní generující polynom nebyl dělitený $(x + 1)$, proto jsem jej nahradil v simulaci vektorem

```
[1 1 1 1]
```

a zkoušel jsem zadávat různé chyby liché násobnosti, v žádném případě nezůstala chyba bez odhalení. Důkaz (převzatý z přednášky) sporem:

Přepokládejme, že $E(x)$ má lichý počet nenulových prvků a zároveň je dělitelný polynomem $(x + 1)$, potom

$$E(x) = Q(x)(x + 1) \tag{8}$$

pro nějaký polynom Q(x). Pokud vyhodnotíme E(x) v 1, dostaneme:

$$E(1) = Q(1)(1 + 1) = Q(1) \cdot (0) = 0 \tag{9}$$

Protože má ale E(x) lichý počet nenulových členů, tak při jeho vyhodnocení v bodě 1 sčítáme lichý počet jedniček ve světě modulo 2, tedy

$$E(1) = 1 \tag{10}$$

a to je spor.

2.5 Odhalení dvojnásobné chyby při nedělitelnosti $(x^i + 1)$ generujícím polynomem

Pokud $x^i + 1$ 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. Simulace s několika pokusy opět neodhalila protipříklad. Důkaz je následující:

Libovolnou dvojnásobnou chybu lze napsat jako $(x^j + x^k)$, což lze přepsat jako $x^l(x^i + 1)$ pro nějaké i a l. Z předpokladu víme, že $(x^i + 1)$ není dělitelné generujícím polynomem. Pokud je generující polynom dělitelný $(x + 1)$, tak má určitě alespoň dva nenulové členy, z důkazu bodu 2.3 potom plyne, že x^l není dělitelné generujícím polynomem. Chybový polynom tedy není dělitelný generujícím a chyba je odhalena.

2.6 Shluková chyba délky kratší než je délka generujícího polynomu

Pokud je chybový vektor typu $x^j(x^t + ... + 1)$ 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.

Za celou dobu zpracovávání cvičení se nestalo, že by nějaký generující polynom neodhalil chybu kratší délky než je jeho délka. Důkaz:

(Předpokládejme, že generující polynom má alespoň dva členy, jinak věta neplatí.) Podle důkazu v sekci 2.3 není x^j dělitelné generujícím polynomem. Dále platí, že polynom nemůže dělit polynom nižšího řádu beze zbytku, tedy generující polynom nedělí ani $(x^t + ... + 1)$, protože t je z předpokladu menší než stupeň generujícího polynomu. Generující polynom proto nedělí beze zbytku ani jeden činitel chybového polynomu $x^j(x^t + ... + 1)$ a chyba bude odhalena.

3 Pravděpodobnost odhalení shlukové chyby

3.1 Shluková chyba délky shodné s generujícím polynomem

Pokud je chybový vektor shlukovou chybou s délkou rovnou délce generujícího polynomu (vektor typu $x^j(x^{t-1} + ... + 1)$, kde $t - 1 = k$ je rovno stupni generujícího polynomu), pak pravděpodobnost, že chyba nebude detekována, je $2^{-(k-1)}$. (Poznámka: Tvrzení platí pouze v případě, kdy generující polynom má nenulový konstantní člen.) Důkaz:

Už jsem dokázal, že aby chyba nebyla detekována tak generující polynom musí dělit chybový polynom beze zbytku, dále jsem dokázal, že pokud má generující polynom alespoň konstantní a jeden další člen, tak nedělí x^j. Stačí tedy ukázat, že $C(x)$ dělí $(x^{t-1} + ... + 1)$ s pravděpodobností $2^{-(k-1)}$.

Polynomy mají stejný stupeň $(t-1 = k)$ a nenulový konstantní člen. Protože uvažujeme polynomy ze světa modulo 2, tak aby jeden polynom dělil jiný polynom stejného stupně, tak musí být polynomy stejné. Tyto polynomy se určitě shodují v konstantním členu a v $xt - 1$ respektive x^k, zbývá tedy $k - 1$ členů ve kterých se buď liší, nebo shodují, v každém s pravděpodobností $\frac{1}{2}$. Pravděpodobnost, že se shodují ve všech členech je proto $(\frac{1}{2})^{k-1} = 2^{-(k-1)}$.

3.2 Shluková chyba větší délky než je délka generujícího polynomu

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}. Důkaz:

Chybový polynom je opět typu $x^j(x^{t-1} + ... + 1)$, víme, že x^j není dělitelné generujícím polynomem $C(x)$, pokud má $C(x)$ alespoň dva nenulové členy. Proto, pokud CRC chybu neodhalí, tak platí

$$(x^{t-1} + ... + 1) = C(x)Q(x) \tag{11}$$

kde Q(x) je libovolný polynom stupně $t - 1 - k$. Možných polynomů stupně $t-1$ s nenulovým absolutním členem je ve světě modulo 2 přesně 2^{t-2}, možných

polynomů $Q(x)$ stupně $t-1-k$ je přesně 2^{t-2-k}. Pravděpodobnost, že náhodná shluková chyba délky t nebude odhalena je proto

$$P = \frac{2^{t-2-k}}{2^{t-2}} = 2^{-k} \tag{12}$$

4 Ověření spolehlivosti

Simulaci jsem spustil s rámci délky 35 a generujícím polynomem

```
[1 1 1 0 1 0 1 0 1]
```

pravděpodobnost chyby jsem nastavil na 1%. Celkem bylo odesláno 857 143 framů a z nich bylo 301 139 chybových. CRC kontrola odhalila 301 135 chybných framů, tedy celkem 4 neodhalila, to znamená spolehlivost odhalení chyby kolem 99,999%.

Simulaci jsem opakoval s rámci délky 100, stejným generujícím polynomem a stejnou pravděpodobností chyby. Celkem bylo odesláno 300 001 framů a z nich bylo 198 934 chybových. CRC kontrola odhalila 198 746 chybných framů, tedy celkem 188 neodhalila, v tomto případě byla spolehlivost odhalení chyby kolem 99,905%.

Je vidět, že čím delší je délka rámce v poměru k délce generujícího polynomu jím větší je šance na chybu, která nebude odhalena.