ELEKTROTEHNIŠKO-RAČUNALNIŠKA
STROKOVNA ŠOLA IN GIMNAZIJA
LJUBLJANA

Seminarska naloga pri predmetu elektrotehnika

Komunikacijska vezja in naprave

Mentor: Anton Orehek, uni. dipl. inž., prof.

Avtor: Jaka Kovač S51JK, G 3. b

Ljubljana, december 2022 – marec 2023

Povzetek

Seminarska naloga opisuje matematični vidik delovanja cyclic redundancy check-a, ob tem pa na kratko opiše tudi matematične pojme kot so konča polja in polinomi. Pokaže tudi, kako CRC implementirati z logičnim vezjem.

Ključe besede: CRC, končna polja, polinomi, logična vezja, digitalna komunikacija

Abstract

This paper describes mathematical part of cyclic redundancy check, while at the same time depicts mathematical terms like finite fields and polynomials. The paper shows how to implement CRC with logic circuit.

Keywords: CRC, finite fields, polynomials, logic circuits, digital communication

Kazalo

Slike

1 Uvod

Dandanes se vsak zanaša na digitalno komunikacijo. Pa naj bo pogovor z ljubljeno osebo, kratkočasenje z uporabo interneta ali pa plačevanje z bančno kartico. Potrebno je zagotoviti pravilni prejem sporočila. Motnje so lahko zelo različne. Kot ponavadi si lahko pomagamo z matematiko, saj je bilo iznajdenih že kar nekaj matematičnih algoritmov kot so Hammingov kod in cyclic redundancy check. Matematična kompleksnost prej omenjenega algoritma in preprostost implementacije z diskretnimi logičnimi enotami sta čudovito nasprotujoča. CRC se uporablja pri internetni komunikaciji, WiFi, mobilnih podatkih ipd.

2 Analogna komunikacija

2.1 Zgodovina radia

Prav vsi poznamo radio. To je tista majhna naprava v avtu, ki voznikom (in potnikom) krajša čas, ki so ga prisiljeni preživeti za volanom. Veliko ljudi pa se ne zaveda, da je radio mnogo več. Slovar slovenskega knjižnega jezika s prvim pomenom definira radio kot: "*naprava za oddajanje in sprejemanje električnih impulzov, signalov po radijskih valovih*". [5]
Leta 1895 [6] je potekal prvi prenos sporočila z uporabo radijskih valov, osem let kasneje pa prva uspešna (enosmerna) komunikacija iz ZDA v Združeno kraljestvo. Leta 1920 sta v ZDA in Veliki Britaniji pričeli delovati prvi radiodifuzni[1] postaji, leta 1928 pa je Radio Ljubljana postala prva radiodifuzna postaja v Sloveniji.

2.2 Analogni signali

Analogni signali so tisti signali, ki lahko zavzamejo vse vrednosti na določenem intervalu. Čas je primer analogne vrednosti, ker mu ne moremo dolčiti najmanjše enote, za katero bi se spremenil. Urin kazalec se premika s stalno hitrostjo. To pomeni, da se v neskončno majhnem intervalu časa vseeno spremeni za nek delež stopinje, vendar pa ljudje tega navadno ne opazimo.
Digitalni signali pa so tisti signali, ki lahko zavzamejo samo določene vrednosti. Na primer digitalna ura. "Kazalci"na taki uri (številke) ne morejo zavzeti katerekoli pozicije med dvema številkama, ampak samo celoštevilčne vrednosti med njima.
Če imamo torej dve uri, eno analogno in eno digitalno, ki prikazuje samo ure, lahko na analogni uri vseeno razberemo, kako blizu naslednje ure smo, na digitalni pa tega žal ne bomo mogli doseči.

2.3 Prednosti in slabosti analognih komunikacij

Analogni signali so močno nagnjeni k popačenju. Vsi signali so sicer dovzetni za motnje, vendar lahko digitalne signale rekonstruiramo v prvotno obliko, medtem ko tega pri analognih žal ne moremo. Glavna prednost analognih signalov pa je večja gostota podatkov v primerjavi z digitalnimi signali.

[1]radiodifuzija – oddajanje radijskih signalov namenjenih poslušanju

3 Digitalna komunikacija

3.1 Prednosti in slabosti digitalne komunikacije

Ker lahko digitalni signali zavzamejo le vnaprej določeno število pozicij, so manj dovzetni za motnje, saj lahko predpostavimo, da je prava tista vrednost, ki je najbližja prebrani. Ravno zaradi tega pa se zmanjša količina informacij, ki jih lahko prenesemo s signalom dane frekvence.

3.2 Problemi digitalnih komunikacij

Digitalni signali so načeloma prepoznani kot bolj zanesljivi, vendar pa so še vedno dovzetni za različne motnje.

3.2.1 Bitflips

Bit je najmanjša količina informacij, ki jih lahko signal prenese. Načeloma jih označujemo z nič (logično stanje: nepravilno) in ena (logično stanje: pravilno). Bitflip je dogodek, ko se nič spremeni v ena ali ena v nič. To se lahko zgodi zaradi zunanjih vplivov, na primer inducirane napetosti zaradi bližine drugega vodnika, ki prenaša signal ali kozmičnega sevanja [7].

3.3 Pretvorba sporočila

Ko so se pričele digitalne komunikacije, je bilo potrebno ustvariti standard za prenos sporočil. Enden izmed takih standardov je tudi ASCII (American Standard Code for Information Interchange). Danes pa se večinoma uporablja sistem UTF-8, ki je bolj vsestranski, saj podpira skoraj 300 000 alfanumeričnih, nadzornih ipd. znakov.

3.4 Error correction

Odpravljanje napak (ang.: error correction) je skupek načeloma matematičnih algoritmov, s katerimi lažje opazimo in popravimo napake pri prenosu sporočila. Eden izmed prvih načinov prepoznave in odprave napak je Hammingov kod. Sporočilo je potrebno razdeliti na dele velikosti $2^n - n - 1$, kjer večji n poveča učinkovitost, saj se zmanjša delež paritetnih bitov v oddanem sporočilu, hkrati pa se poveča verjetnost, da bo prišlo do nepopravljive napake.

3.4.1 Matematični uvod

Cyclic redundancy check ali CRC je bolj napredna metoda. Da bi jo lažje razložil, je najprej potrebno vpeljati nekaj matematičnih pojmov.

3.4.1.1 Končna polja

V algebri je polje ali univerzalna množica množica vseh števil, s katerimi operiramo. Navadno so to realna števila, pogosto tudi kompleksna. Moč obeh teh množic je neskončno. Poglejmo si primer končno univerzalne množico.

Definirajmo univerzalno množico tako da vsebuje le dva elementa $U = \{ 0, 1 \}$.
Poskusimo definirati seštevanje in odštevanje:

$$\begin{array}{ll} 0+0=0 & 0-0=0 \\ 0+1=1 & 0-1=1 \\ 1+0=1 & 1-0=1 \\ 1+1=0 & 1-1=0 \end{array}$$

ter množenje in deljenje:

$$\begin{array}{ll} 0*0=0 & \\ 0*1=0 & 0/1=0 \\ 1*0=0 & 1/1=1 \\ 1*1=1 & \end{array}$$

Lahko se je prepričati, da sta tako seštevanje kot množenje asociativna in komutativna. Prav tako veljata identiteti (0 je nevtralni element za seštevanje, 1 za množenje). Še vedno velja zakon o združevanju, prav tako pa lahko določimo nasprotne in obratne vrednosti.

3.4.1.2 Polinomi

Polinom je linearna kombinacija potenčnih funkcij, ki imajo nenegativne cele eksponente.

$$p_n(x) = \sum_{k=0}^{n} a_k x^k \tag{1}$$

Med polinomi lahko izvajamo matematične operacije. Za izračun CRC bomo potrebovali seštevanje in deljenje.

3.4.1.3 Kodiranje sporočila kot polinom

Začnimo s primerom.[2] Predpostavimo, da želimo poslati sporočilo: ”Oj!”. Najprej ga je potrebno pretvoriti v binarni zapis, kar lahko storimo z ASCII tabelo.
Naše sporočilo sedaj izgleda:

O	j	!
01001111	01101010	00100001

Vendar pa še vedno potrebujemo polinom. Za koeficiente uporabimo binarne števke. Polinom $m(x)$ za naše sporočilo bi torej bil:

$$\begin{aligned} m(x) = {} & 0 \cdot x^{23} + 1 \cdot x^{22} + 0 \cdot x^{21} + 0 \cdot x^{20} + 1 \cdot x^{19} + 1 \cdot x^{18} + +1 \cdot x^{17} + 1 \cdot x^{16} + 0 \cdot x^{15} \\ & + 1 \cdot x^{14} + 1 \cdot x^{13} + 0 \cdot x^{12} + 1 \cdot x^{11} + 0 \cdot x^{10} + 1 \cdot x^{9} + 0 \cdot x^{8} + 0 \cdot x^{7} + 0 \cdot x^{6} \\ & + 1 \cdot x^{5} + 0 \cdot x^{4} + 0 \cdot x^{3} + 0 \cdot x^{2} + 0 \cdot x^{1} + 1 \cdot x^{0} \end{aligned} \tag{2}$$

oziroma, če malo uredimo

$$m(x) = x^{22} + x^{19} + x^{18} + x^{17} + x^{16} + x^{14} + x^{13} + x^{11} + x^{9} + x^{5} + x^{0} \tag{3}$$

[2]Za vse nadaljnje odstavke bom uporabil isti primer, ki ga bom označil z $m(x)$

3.4.1.4 Osnovni izrek o deljenju (za polinome)

Osnovni izrek o deljenju naravnih števil lahko zapišemo kot:

$$a = k \cdot b + r; a, b, k, r \in \mathbb{N} \tag{4}$$

Rečemo lahko tudi, da b deli a natanko tedaj, ko je $r = 0$. Tudi pri deljenju polinomov lahko zapišemo podobno:

$$p(x) = k(x) \cdot q(x) + r(x) \tag{5}$$

Polinom $p(x)$ je deljiv s polinomom $q(x)$ samo, če je $r(x) = 0$.

3.4.2 Cyclic redundancy check

3.4.2.1 Generiranje CRC

Za uporabo CRC algoritma moramo najprej določiti generatorski polinom $g(x)$. Za primer vzemimo: $g(x) = x^{16} + x^{12} + x^5 + 1$. Poskusimo naše sporočilo $m(x)$ deliti z $g(x)$, pri tem pa upoštevajmo definicije iz 3.4.1.1. Ker želimo sporočilo na koncu tudi poslati, ga seveda ne želimo uničiti. To zagotovimo tako, da na koncu sporočila dodamo toliko bitov, kolikor bitni CRC uporabljamo. Za primer uporabljamo 16-bitni CRC, saj je stopnja generatorskega polinoma 16 ($st(g) = 16$). Matematično gledano to pomeni, da naše sporočilo pomnožimo z x^{16}

$$\begin{aligned}
&(m(x) \cdot x^{16})/g(x) = \\
&(x^{38} + x^{35} + x^{34} + x^{33} + x^{32} + x^{30} + x^{29} + x^{27} + x^{25} + x^{21} + x^{16}) \\
&/(x^{16} + x^{12} + x^5 + 1) = \\
&x^{22} + x^{19} + x^{17} + x^{16} + x^{15} + x^{14} + x^{12} + x^{11} + x^{10} + x^9 + x^7 + x^6 + x^5 + x^4 + x^3 \\
&+x^2 + x^1 \\
&, ost. : x^{15} + x^{14} + x^{13} + x^8 + x^5 + x^4 + x^3 + x^2 + x^1 \quad (= r(x))
\end{aligned} \tag{6}$$

Ugotovili smo, da $m(x)$ ni deljiv z $g(x)$. Lahko bi rekli, da je naše sporočilo za ostanek ($r(x)$) preveliko, da bi bilo deljivo. Od našega sporočila lahko torej odštejemo ostanek.[3]

$$\begin{aligned}
s(x) =& m(x) - r(x) \\
=& (x^{38} + x^{35} + x^{34} + x^{33} + x^{32} + x^{30} + x^{29} + x^{27} + x^{25} + x^{21} + x^{16}) \\
&+ (x^{15} + x^{14} + x^{13} + x^8 + x^5 + x^4 + x^3 + x^2 + x^1)
\end{aligned} \tag{7}$$

S tem smo zagotovili, da je sporočilo, ki ga bomo oddali $s(x)$ deljivo z $g(x)$.[4]

3.4.2.2 Validacija CRC

Ko prejmemo sporočilo, ki je bilo zavarovano s CRC lahko prejeto sporočilo spet delimo z generatorskim polinomom, ostanek pri deljenju pa mora biti sedaj 0. Če ni tako, smo lahko prepričani, da se je pri prejemu sporočila zgodila napaka. Žal ne moremo ugotoviti, kje se je napaka zgodila.

[3] Zaradi uporabe končnega polja sta seštevanje in oštevanje zamenljivi operaciji in izgleda, kot da sta se polinoma seštela

[4] Za oddajo sporočila polinom seveda pretvorimo nazaj v bite, naše sporočilo pa se glasi 100111101101010001000011100001001111110

4 Empirični del – Digitalno vezje

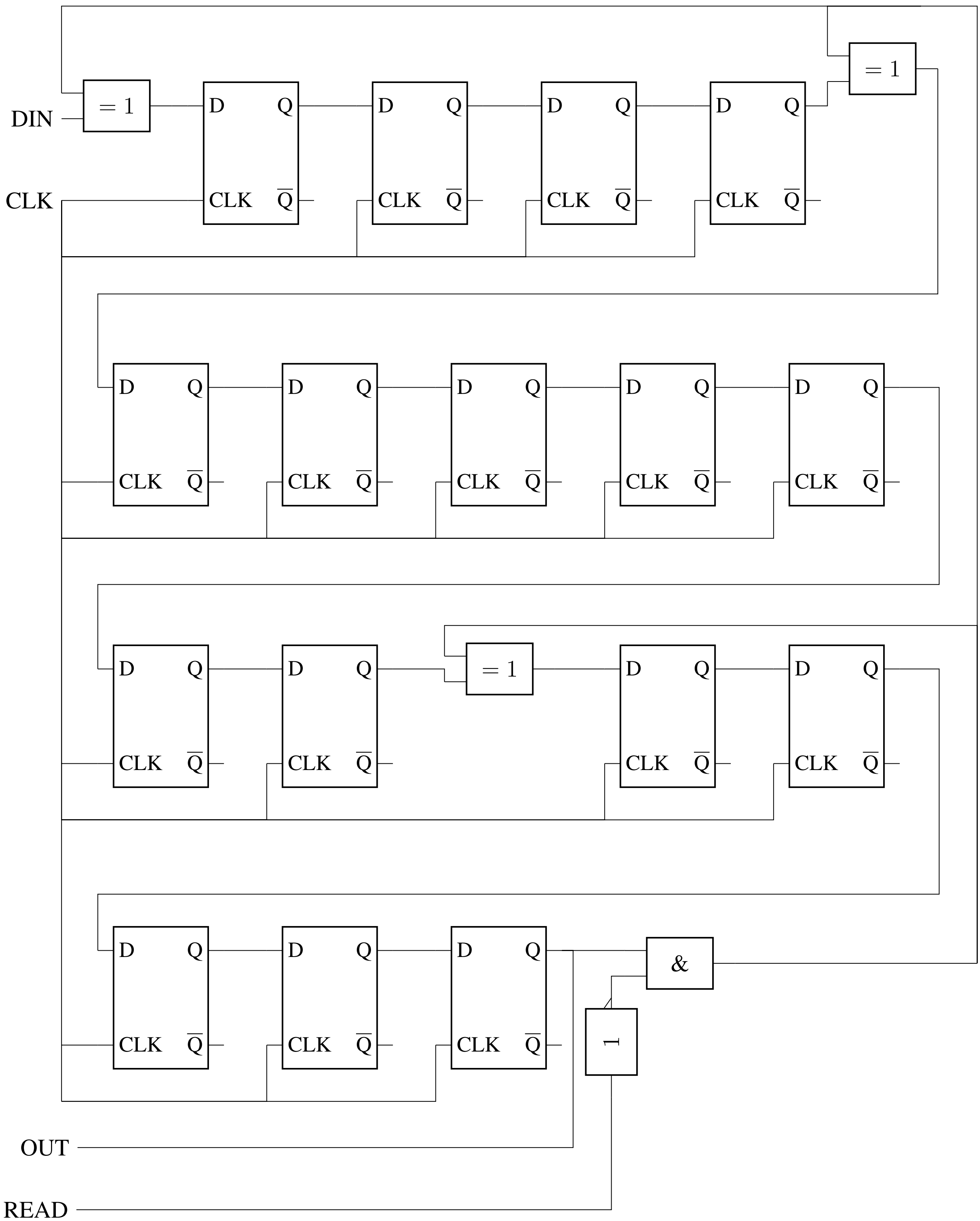
4.1 Delovnje vezja

Najprej potrebujemo naš tok bitov shraniti. To storimo z D polnilnimi celicami. Izhod prve vežemo na vhod druge. Signal tako potuje od prve proti zadnji. Število a lahko delimo s številom b samo če je število a večje od b. To pomeni, da moramo obrniti bite na pravih mestih samo, če je izhod zadnje pomnilne celice 1. Logična vrata, ki nam to omogočajo so vrata XALI. Pravilnostna tabela XALI vrat: Iz pravilnostne tabele lahko vidimo, da je izhod vrat enak vhodu B, če je vhod

A	B	A $\bigoplus$ B
0	0	0
0	1	1
1	0	1
1	1	0

A enak 0 in da je izhod negirana vrednost vhoda B, če je vhod A enak 1. V vhod A priključimo izhodni bit zadnje pomnilne celice in v vhod B izhod pomnilne celice, ki ga želimo nadzirati. Ker je deljenje v izbranem končnem polju enako negiranju bitov so XALI vrata prava izbira. Postavimo jih pred bite, ki jih želimo obrniti. Zadnjega ne potrebujemo, obračati, saj gre z naslednjim ciklom časovnika v pozabo. Ker želimo na koncu ostanek prebrati, pred A vhode XALI vrat postavimo IN vrata, ki nastavijo izhod na 1 samo če sta oba vhoda tudi 1. Če je torej eden izmed vhodov vedno 1, bo vrednost izhoda enaka drugemu vhodu, če pa bo vrednost enega izmed vhodov enaka 0 je izhod tudi 0 neodvisno od drugega vhoda. Če torej v en vhod IN vrat pripeljemo signal s katerim povemo, da želimo samo brati ostanek, lahko s signalom READ preskočimo negiranje bitov v ostanku.

4.2 Shema vezja



Slika 1: Vezje logičnih enot za računanje 16-bitnega CRC in polinomom $x^{16} + x^{12} + x^5 + 1$

5 Zaključek

S seminarsko nalogo sem vam želel podrobno opisati delovanje CRC. Za to je potrebno razložiti tudi nekaj matematike. Žal mi je zmanjkalo časa za poglobitev v delovanje logičnega vezja, sem pa uspešno izdelal oddajnik in sprejemnik sporočila zaščitenega s CRC.

6 Viri in literatura

[1] S. Denby. *How Cell Service Actually Works,* (2022), spletni naslov: https://www.youtube.com/watch?v=0faCad2kKeg (dostopano: 29. 12. 2022).

[2] B. Eater. *Hardware build: CRC calculation,* (2019), spletni naslov: https://www.youtube.com/watch?v=sNkERQlK8j8 (dostopano: 20. 2. 2023–5. 3. 2023).

[3] B. Eater. *How do CRCs work?,* (2019), spletni naslov: https://www.youtube.com/watch?v=izG7qT0EpBw (dostopano: 7. 11. 2022–5. 3. 2023).

[4] B. Eater. *What is error correction? Hamming codes in hardware,* (2020), spletni naslov: https://www.youtube.com/watch?v=h0jloehRKa (dostopano: 15. 2. 2023).

[5] *eSSKJ: radio,* (2016), spletni naslov: https://fran.si/133/sskj2-slovar-slovenskega-knjiznega-jezika-2/4523492/radio?FilteredDictionaryIds=133&View=1&Query=radio (dostopano: 26. 12. 2022).

[6] J. Kordež S52KJ, P. Vovk S54UNC in Ž. Kralj S50ZK. *Radioamaterski tečaj 2022,* (2022/2023), spletni naslov: http://tecaj.jkob.cc/ (dostopano: 26. 12. 2022–5. 1. 2023).

[7] D. A. Muller. *The Universe is Hostile to Computers,* (2021), spletni naslov: https://www.youtube.com/watch?v=AaZ_RSt0KP8 (dostopano: 15. 2. 2023).

[8] G. Sanderson. *How to send a self-correcting message (Hamming codes),* (2020), spletni naslov: https://www.yxoutube.com/watch?v=X8jsijhllIA (dostopano: 17. 1. 2023).

[9] J. Vraničar et. al., *Priročnik za radioamaterje*, 3. dopolnjena izd. Pekre: Zveza radioamaterjev Slovenije, 2019.

[10] *What is Reed-Solomon Code?,* (2022), spletni naslov: https://www.geeksforgeeks.org/what-is-reed-solomon-code/ (dostopano: 26. 12. 2022).

Izjava o avtorstvu

Izjavljam, da je seminarska naloga v celoti moje avtorsko delo, ki sem ga izdelal samostojno s pomoĉjo navedene literature in pod vodstvom mentorja.

7. 3. 2023 Jaka Kovač