VEGOVA
ELEKTROTEHNIŠKO-RAČUNALNIŠKA
STROKOVNA ŠOLA IN GIMNAZIJA
LJUBLJANA

Strokovno poročilo pri predmetu elektrotehnika

# Komunikacijska vezja in naprave

Uporaba matematike v digitalnih komunikacijah

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

Avtor: Jaka Kovač S51JK, G 3. b

Ljubljana, december 2022 – marec 2023

## Povzetek

## Abstract

# Kazalo



# Slike



# Tabele

# 1 Uvod

# 2 Analogna komunikacija

## 2.1 Zgodovina radia

Prav vsi poznamo radio. To je tista majhna naprava v avtu, ki voznikom (in potnikom) olajša 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*. [1]
Leta 1895 [2] je potekal prvi prenos sporočila s pomočjo 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 odločiti najmanjše enote, za katero bi se spremenil. Urni 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 z 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

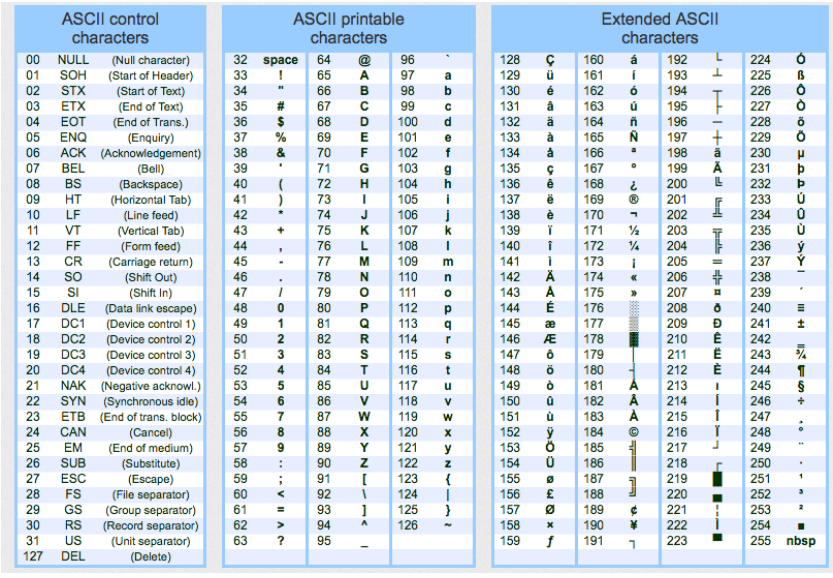
Digitalni signali so načeloma prepoznani kot bolj zanesljivi, vendar pa so še vedno dovzetni za različne motnje.

### 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 [3].

## 3.3 Pretvorba sporočila

Ko so se pričele digitalne komunikacije je bilo potrebno ustvariti standard za prenos sporočil. En izmed takih standardov je tudi ASCII (American Standard Code for Information Interchange). Sedaj pa se večinoma uporablja sistem UTF-8, ki je bolj vsestranski, saj podpira skoraj 300 000 alfanumeričnih, nadzornih ipd. znakov (Slika 1).



**ASCII control characters**

| | | |
|---|---|---|
| 00 | NULL | (Null character) |
| 01 | SOH | (Start of Header) |
| 02 | STX | (Start of Text) |
| 03 | ETX | (End of Text) |
| 04 | EOT | (End of Trans.) |
| 05 | ENQ | (Enquiry) |
| 06 | ACK | (Acknowledgement) |
| 07 | BEL | (Bell) |
| 08 | BS | (Backspace) |
| 09 | HT | (Horizontal Tab) |
| 10 | LF | (Line feed) |
| 11 | VT | (Vertical Tab) |
| 12 | FF | (Form feed) |
| 13 | CR | (Carriage return) |
| 14 | SO | (Shift Out) |
| 15 | SI | (Shift In) |
| 16 | DLE | (Data link escape) |
| 17 | DC1 | (Device control 1) |
| 18 | DC2 | (Device control 2) |
| 19 | DC3 | (Device control 3) |
| 20 | DC4 | (Device control 4) |
| 21 | NAK | (Negative acknowl.) |
| 22 | SYN | (Synchronous idle) |
| 23 | ETB | (End of trans. block) |
| 24 | CAN | (Cancel) |
| 25 | EM | (End of medium) |
| 26 | SUB | (Substitute) |
| 27 | ESC | (Escape) |
| 28 | FS | (File separator) |
| 29 | GS | (Group separator) |
| 30 | RS | (Record separator) |
| 31 | US | (Unit separator) |
| 127 | DEL | (Delete) |

**ASCII printable characters**

| | | | | | |
|---|---|---|---|---|---|
| 32 | space | 64 | @ | 96 | ` |
| 33 | ! | 65 | A | 97 | a |
| 34 | " | 66 | B | 98 | b |
| 35 | # | 67 | C | 99 | c |
| 36 | $ | 68 | D | 100 | d |
| 37 | % | 69 | E | 101 | e |
| 38 | & | 70 | F | 102 | f |
| 39 | ' | 71 | G | 103 | g |
| 40 | ( | 72 | H | 104 | h |
| 41 | ) | 73 | I | 105 | i |
| 42 | * | 74 | J | 106 | j |
| 43 | + | 75 | K | 107 | k |
| 44 | , | 76 | L | 108 | l |
| 45 | - | 77 | M | 109 | m |
| 46 | . | 78 | N | 110 | n |
| 47 | / | 79 | O | 111 | o |
| 48 | 0 | 80 | P | 112 | p |
| 49 | 1 | 81 | Q | 113 | q |
| 50 | 2 | 82 | R | 114 | r |
| 51 | 3 | 83 | S | 115 | s |
| 52 | 4 | 84 | T | 116 | t |
| 53 | 5 | 85 | U | 117 | u |
| 54 | 6 | 86 | V | 118 | v |
| 55 | 7 | 87 | W | 119 | w |
| 56 | 8 | 88 | X | 120 | x |
| 57 | 9 | 89 | Y | 121 | y |
| 58 | : | 90 | Z | 122 | z |
| 59 | ; | 91 | [ | 123 | { |
| 60 | < | 92 | \ | 124 | \| |
| 61 | = | 93 | ] | 125 | } |
| 62 | > | 94 | ^ | 126 | ~ |
| 63 | ? | 95 | _ | | |

**Extended ASCII characters**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 128 | Ç | 160 | á | 192 | └ | 224 | Ó |
| 129 | ü | 161 | í | 193 | ┴ | 225 | ß |
| 130 | é | 162 | ó | 194 | ┬ | 226 | Ô |
| 131 | â | 163 | ú | 195 | ├ | 227 | Ò |
| 132 | ä | 164 | ñ | 196 | ─ | 228 | õ |
| 133 | à | 165 | Ñ | 197 | ┼ | 229 | Õ |
| 134 | å | 166 | ª | 198 | ã | 230 | µ |
| 135 | ç | 167 | º | 199 | Ã | 231 | þ |
| 136 | ê | 168 | ¿ | 200 | ╚ | 232 | Þ |
| 137 | ë | 169 | ® | 201 | ╔ | 233 | Ú |
| 138 | è | 170 | ¬ | 202 | ╩ | 234 | Û |
| 139 | ï | 171 | ½ | 203 | ╦ | 235 | Ù |
| 140 | î | 172 | ¼ | 204 | ╠ | 236 | ý |
| 141 | ì | 173 | ¡ | 205 | ═ | 237 | Ý |
| 142 | Ä | 174 | « | 206 | ╬ | 238 | ¯ |
| 143 | Å | 175 | » | 207 | ¤ | 239 | ´ |
| 144 | É | 176 | ░ | 208 | ð | 240 | ≡ |
| 145 | æ | 177 | ▒ | 209 | Ð | 241 | ± |
| 146 | Æ | 178 | ▓ | 210 | Ê | 242 | ‗ |
| 147 | ô | 179 | │ | 211 | Ë | 243 | ¾ |
| 148 | ö | 180 | ┤ | 212 | È | 244 | ¶ |
| 149 | ò | 181 | Á | 213 | ı | 245 | § |
| 150 | û | 182 | Â | 214 | Í | 246 | ÷ |
| 151 | ù | 183 | À | 215 | Î | 247 | ¸ |
| 152 | ÿ | 184 | © | 216 | Ï | 248 | ° |
| 153 | Ö | 185 | ╣ | 217 | ┘ | 249 | ¨ |
| 154 | Ü | 186 | ║ | 218 | ┌ | 250 | · |
| 155 | ø | 187 | ╗ | 219 | █ | 251 | ¹ |
| 156 | £ | 188 | ╝ | 220 | ▄ | 252 | ³ |
| 157 | Ø | 189 | ¢ | 221 | ¦ | 253 | ² |
| 158 | × | 190 | ¥ | 222 | Ì | 254 | ■ |
| 159 | ƒ | 191 | ┐ | 223 | ▀ | 255 | nbsp |

Slika 1: ASCII znaki

Vir: https://computersciencewiki.org/index.php/File:Ascii_table.png

## 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 morda tudi kompleksna. Moč obeh teh množic je neskončno, kaj pa, če bi uporabili končno 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 seštevan 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 s tabelo na sliki 1.
Naše sporočilo sedaj zgleda:

| 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

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

**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

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 $x^{16}$

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

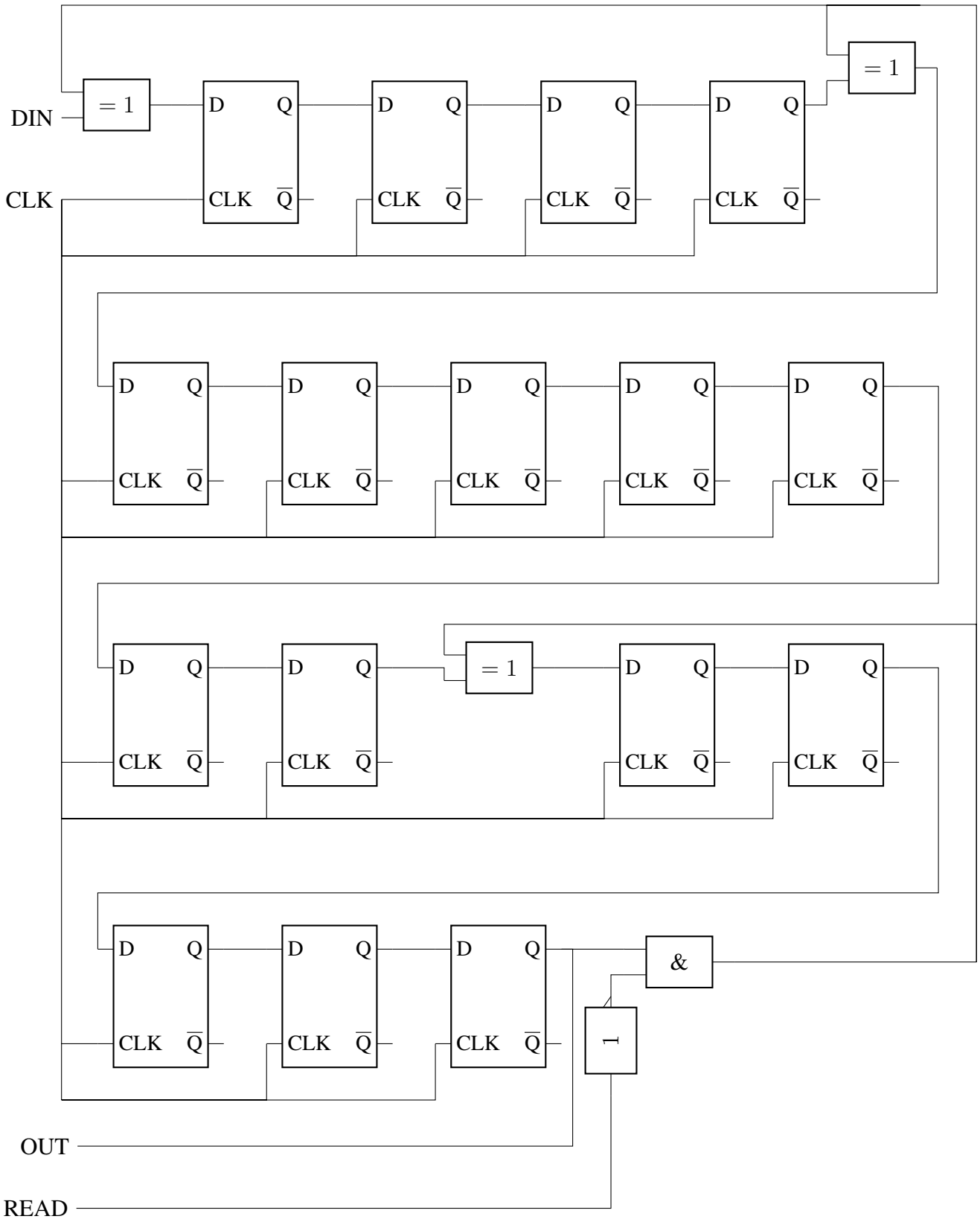
[2] Za vse nadaljne odstavke bom uporabil isti primer, ki ga bom označil z $m(x)$

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.

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

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

# 4 Empirični del – Digitalna vezja




Slika 2: Vezje logičnih enot za računanje 16-bitnega CRC in polinomom $x^{16} + x^{12} + x^5 + 1$

# 5 Viri in literatura


[1] *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).

[2] 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).

[3] *The Universe is Hostile to Computers,* (31. avg. 2021), spletni naslov: https://www.youtube.com/watch?v=AaZ_RSt0KP8 (dostopano: 15. 2. 2023).

[4] *How to send a self-correcting message (Hamming codes)*. (4. sep. 2020), spletni naslov: https://www.yxoutube.com/watch?v=X8jsijhllIA (dostopano: 17. 1. 2023).

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

[6] *How to send a self-correcting message (Hamming codes),* (4. sep. 2020), spletni naslov: https://www.youtube.com/watch?v=AaZ_RSt0KP8 (dostopano: 15. 2. 2023).

[7] *How do CRCs work?* (28. apr. 2019), spletni naslov: https://www.youtube.com/watch?v=izG7qT0EpBw (dostopano: 7. 11. 2022–5. 3. 2023).

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

[9] *Modulacija,* (2019), spletni naslov: https://sl.wikipedia.org/wiki/Modulacija (dostopano: 28. 12. 2022).

[10] *What is Reed-Solomon Code?,* (24. feb. 2022), spletni naslov: https://www.geeksforgeeks.org/what-is-reed-solomon-code/ (dostopano: 26. 12. 2022).

[11] *How Cell Service Actually Works,* (26. jan. 2022), spletni naslov: https://www.youtube.com/watch?v=0faCad2kKeg (dostopano: 29. 12. 2022).