1 Ciklička provera redundansi (CRC)

1.1 Zadaci - slanje poruka

1. Koristeći polinom generator $G(x) = x^4 + x^3 + 1$ odrediti oblik za slanje poruke 11100110.

   polinom generator: $G(x) = x^4 + x^3 + 1$
   stepen polinoma generatora: $n = st\ G(x) = 4$
   binarni ekvivalent: $G(x) = x^4 + x^3 + 1 = 1 \cdot x^4 + 1 \cdot x^3 + 0 \cdot x^2 + 0 \cdot x^1 + 1 \sim 11001$

   dopisujemo $n = 4$ nule na polaznu poruku: 11100110**0000**
   primenom ekskluzivne bitske disjunkcije vršimo deljenje (delilac uvek potpisujemo ispod prve jedinice delimičnog ostatka):

```
111001100000 : 11001
11001
------------
  1011100000
  11001
  ----------
   111000000
   11001
   ---------
     1010000
     11001
     -------
      110100
      11001
      ------
         110
```

   ostatak zapisujemo kao nisku dužine $n = 4$: 0110
   poruka koja se šalje: 11100110**0110**

   Napomene:

   - prilikom deljenja mogu da se spuštaju sve preostale cifre iz zapisa poruke ili samo onoliko koliko je potrebno da delimični ostatak bude dužine $n + 1$
   - primetiti da ostatak pri deljenju može da ima najviše n cifara, računajući od prve jedinice sleva. Kako se delilac (dužine n+1) uvek potpisuje ispod prve jedinice delimičnog ostatka, u ekskluzivnoj disjunkciji će uvek biti dve vodeće jedinice koje u rezultatu daju nulu

2. Koristeći polinom generator $G(x) = x^3 + 1$ odrediti oblik za slanje poruke 101100.

   polinom generator: $G(x) = x^3 + 1$
   stepen polinoma generatora: $n = st\ G(x) = 3$
   binarni ekvivalent: $G(x) = x^3 + 1 = 1 \cdot x^3 + 0 \cdot x^2 + 0 \cdot x^1 + 1 \sim 1001$
   dopisujemo $n = 3$ nule na polaznu poruku: 101100**000**
   primenom ekskluzivne bitske disjunkcije vršimo deljenje:

```
101100000 : 1001
1001
---------
  1000000
  1001
  -------
     1000
     1001
     ----
        1
```

   ostatak zapisujemo kao nisku dužine $n = 3$: 001
   poruka koja se šalje: 101100**001**

3. Koristeći polinom generator $G(x) = x^5 + x^2$ odrediti oblik za slanje poruke 100010111.

   polinom generator: $G(x) = x^5 + x^2$
   stepen polinoma generatora: $n = st\ G(x) = 5$
   binarni ekvivalent: $G(x) = x^5 + x^2 = 1 \cdot x^5 + 0 \cdot x^4 + 0 \cdot x^3 + 1 \cdot x^2 + 0 \cdot x^1 + 0 \sim 100100$
   dopisujemo $n = 5$ nula na polaznu poruku: 100010111**00000**
   primenom ekskluzivne bitske disjunkcije vršimo deljenje:

```
10001011100000 : 100100
100100
---------------
   11011100000
   100100
   ------------
    1001100000
    100100
    -----------
        100000
        100100
        -------
           100
```

   ostatak zapisujemo kao nisku dužine $n = 5$: 00100
   poruka koja se šalje: 100010111**00100**

1.2 Zadaci - prijem poruka

1. Utvrditi da li je poruka 1100101101 uspešno primljena, i ukoliko jeste, odrediti njen polazni oblik. Korišćen je polinom generator $G(x) = x^2 + 1$.

   polinom generator: $G(x) = x^2 + 1$, stepen polinoma generatora: $n = st\ G(x) = 2$
   binarni ekvivalent: $G(x) = x^2 + 1 = 1 \cdot x^2 + 0 \cdot x^1 + 1 \sim 101$
   primenom ekskluzivne bitske disjunkcije vršimo deljenje:

```
1100101101 : 101
101
----------
 110101101
 101
 ---------
  11101101
  101
  --------
   1001101
   101
   -------
     11101
     101
     -----
      1001
      101
      ----
        11
```

   Prilikom deljenja se dobija ostatak, pa poruka nije uspešno primljena. Ne može se odrediti njen polazni oblik, jer CRC algoritam ne daje mogućnost lociranja pogrešnog bita.
   Na osnovu polinoma generatora znamo da je poruka kodirana dopisivanjem $n = 2$ bita zdesna, ali kako ne znamo da li je greška u dopisanim bitovima ili bitovima poruke, polazni oblik ostaje nepoznat.

2. Utvrditi da li je poruka 100111010111011 uspešno primljena, i ukoliko jeste, odrediti njen polazni oblik. Korišćen je polinom generator $G(x) = x^3 + x + 1$.

   polinom generator: $G(x) = x^3 + x + 1$, stepen polinoma generatora: $n = st\ G(x) = 3$
   binarni ekvivalent: $G(x) = x^3 + x + 1 = 1 \cdot x^3 + 0 \cdot x^2 + 1 \cdot x^1 + 1 \sim 1011$
   prikazana su dva načina deljenja, oba su ispravna, samo se razlikuje broj koraka do rezultata (postupak je kraći ukoliko se delilac uvek potpisuje ispod prve jedinice delimičnog ostatka):

```
100111010111011 : 1011            100111010111011 : 1011
1011                              1011
---------------                   ---------------
  1011                              1011010111011
  1011                              1011
  ----                              -------------
      010111011                         010111011
       1011      <- preskace se         1011        <- ne preskace se 0
       ----         sledeca 0 iz        ---------
           1011     zapisa poruke       111011011
           1011     i potpisuje         1011
           ----     ispod prve          ---------
              0     jedinice             10111011
                                         1011
                                         ----
                                             1011
                                             1011
                                             ----
                                                0
```

Prilikom deljenja nema ostatka pa je poruka uspešno primljena. Polazni oblik poruke se dobija odbacivanjem $n = 3$ bita zdesna: 100111010111.

3. Utvrditi da li je poruka 1011001011 uspešno primljena, i ukoliko jeste, odrediti njen polazni oblik. Korišćen je polinom generator $G(x) = x^3 + 1$.

polinom generator: $G(x) = x^3 + 1$, stepen polinoma generatora: $n = st\ G(x) = 3$
binarni ekvivalent: $G(x) = x^3 + 1 = 1 \cdot x^3 + 0 \cdot x^2 + 0 \cdot x^1 + 1 \sim 1001$

```
1011001011 : 1001
1001
----------
  10001011
  1001
  --------
     11011
     1001
     -----
      1001
      1001
      ----
         0
```

Prilikom deljenja nema ostatka pa je poruka uspešno primljena. Polazni oblik poruke se dobija odbacivanjem $n = 3$ bitova zdesna: 1011001

4. Utvrditi da li je poruka 1100110101101 uspešno primljena, i ukoliko jeste, odrediti njen polazni oblik. Korišćen je polinom generator $G(x) = x^4 + x^2$.

polinom generator: $G(x) = x^4 + x^2$, stepen polinoma generatora: $n = st\ G(x) = 4$
binarni ekvivalent: $G(x) = x^4 + x^2 = 1 \cdot x^4 + 0 \cdot x^3 + 1 \cdot x^2 + 0 \cdot x^1 + 0 \sim 10100$

```
1100110101101 : 10100
10100
-------------
 11011
 10100
 -----
  11110
  10100
  -----
   10101
   10100
   -----
       10110
       10100
       -----
          101 <- poruka nije uspesno primeljena i ne moze se odrediti njen polazni oblik
```

2 Hamming SEC kodovi

Hamming SEC (single error corection) kodovi omogućavaju uočavanje i korekciju jedne greške u binarnim podacima (poruci).
Porukama dužine n bitova pridružuje se $log_2 n + 1$ kontrolnih bitova. Za $n = 8$ broj kontrolnih bitova je $log_2 8 + 1 = 4$. Po dogovoru, bitove takve poruke obeležavamo sa $m_8 m_7 m_6 m_5 m_4 m_3 m_2 m_1$ sleva udesno, a kontolne bitove sa $c_4 c_3 c_2 c_1$ takodje sleva udesno.

Tablica Hamming kodova:

12	1100		m_8
11	1011		m_7
10	1010		m_6
9	1001		m_5
8	1000	c_4	
7	0111		m_4
6	0110		m_3
5	0101		m_2
4	0100	c_3	
3	0011		m_1
2	0010	c_2	
1	0001	c_1	

Računanje vrednosti kontrolnih bitova:
$c_1 = m_1 \oplus m_2 \oplus m_4 \oplus m_5 \oplus m_7$
$c_2 = m_1 \oplus m_3 \oplus m_4 \oplus m_6 \oplus m_7$
$c_3 = m_2 \oplus m_3 \oplus m_4 \oplus m_8$
$c_4 = m_5 \oplus m_6 \oplus m_7 \oplus m_8$

Ukoliko je potrebno proveriti ispravnost pročitane (primljene) poruke, postupak je sledeći:

Računanje vrednosti novih kontrolnih bitova:
$c'_1 = m_1 \oplus m_2 \oplus m_4 \oplus m_5 \oplus m_7$
$c'_2 = m_1 \oplus m_3 \oplus m_4 \oplus m_6 \oplus m_7$
$c'_3 = m_2 \oplus m_3 \oplus m_4 \oplus m_8$
$c'_4 = m_5 \oplus m_6 \oplus m_7 \oplus m_8$

Poredjenje izračunatih kontrolnih bitova sa onima koji su pročitani (pristigli) zajedno sa porukom primenom ekskluzivne bitske disjunkcije po pravilu:

$$c_4 c_3 c_2 c_2 \oplus c'_4 c'_3 c'_2 c'_1$$

Rezultat poredjenja (sindrom reč) je neoznačen ceo binarni broj koji ima sledeća svojstva:

- ako ima dekadnu vrednost 0 nije došlo do greške i nema korekcije
- ako u binarnom zapisu ima barem jednu jedinicu, njegova dekadna vrednost je pozicija reda u tablici gde se nalazi bit sa greskom
- ako ima dekadnu vrednost 1, 2, 4 ili 8 (u binarnom zapisu ima samo jednu jedninicu) greška se javlja u jednom od kontrolnih bitova, dok je poruka u redu i ne zahteva nikakvu korekciju
- ako uzima vrednosti iz skupa $\{3, 5, 6, 7, 9, 10, 11, 12\}$, greška se javlja u jednom od bitova poruke; korekcija se sastoji u komplementiranju vrednosti odgovarajućeg bita

2.1 Zadaci

1. Koristeći Hamming SEC kodove kodirati poruku, tj. odrediti kontrolne bitove:

m_8	m_7	m_6	m_5	m_4	m_3	m_2	m_1
0	1	1	0	0	1	0	1

Rešenje:
$c_1 = m_1 \oplus m_2 \oplus m_4 \oplus m_5 \oplus m_7 = 1 \oplus 0 \oplus 0 \oplus 0 \oplus 1 = 0$
$c_2 = m_1 \oplus m_3 \oplus m_4 \oplus m_6 \oplus m_7 = 1 \oplus 1 \oplus 0 \oplus 1 \oplus 1 = 0$
$c_3 = m_2 \oplus m_3 \oplus m_4 \oplus m_8 = 0 \oplus 1 \oplus 0 \oplus 0 = 1$
$c_4 = m_5 \oplus m_6 \oplus m_7 \oplus m_8 = 0 \oplus 1 \oplus 1 \oplus 0 = 0$

Kontrolni bitovi su: $c_4 c_3 c_2 c_1 = 0100$. Kodirana poruka je: 01100101 0100.

2. Koristeći Hamming SEC kodove izvršiti korekciju greške ukoliko postoji u poruci:

m_8	m_7	m_6	m_5	m_4	m_3	m_2	m_1	c_4	c_3	c_2	c_1
1	0	1	0	0	1	1	0	0	1	1	0

Rešenje:
$c_1' = m_1 \oplus m_2 \oplus m_4 \oplus m_5 \oplus m_7 = 0 \oplus 1 \oplus 0 \oplus 0 \oplus 0 = 1$
$c_2' = m_1 \oplus m_3 \oplus m_4 \oplus m_6 \oplus m_7 = 0 \oplus 1 \oplus 0 \oplus 1 \oplus 0 = 0$
$c_3' = m_2 \oplus m_3 \oplus m_4 \oplus m_8 = 1 \oplus 1 \oplus 0 \oplus 1 = 1$
$c_4' = m_5 \oplus m_6 \oplus m_7 \oplus m_8 = 0 \oplus 1 \oplus 0 \oplus 1 = 0$

sindrom reč: $c_4c_3c_2c_1 \oplus c_4'c_3'c_2'c_1' = 0110 \oplus 0101 = 0011$
$\Rightarrow$ greška je na poziciji $(0011)_2 = 3$ tj. u bitu m_1

korektna poruka je: 1010011**1**

3. Koristeći Hamming SEC kodove izvršiti korekciju greške ukoliko postoji u poruci:

m_8	m_7	m_6	m_5	m_4	m_3	m_2	m_1	c_4	c_3	c_2	c_1
0	1	0	1	0	1	0	1	0	0	0	0

Rešenje:
$c_1' = m_1 \oplus m_2 \oplus m_4 \oplus m_5 \oplus m_7 = 1 \oplus 0 \oplus 0 \oplus 1 \oplus 1 = 1$
$c_2' = m_1 \oplus m_3 \oplus m_4 \oplus m_6 \oplus m_7 = 1 \oplus 1 \oplus 0 \oplus 0 \oplus 1 = 1$
$c_3' = m_2 \oplus m_3 \oplus m_4 \oplus m_8 = 0 \oplus 1 \oplus 0 \oplus 0 = 1$
$c_4' = m_5 \oplus m_6 \oplus m_7 \oplus m_8 = 1 \oplus 0 \oplus 1 \oplus 0 = 0$

sindrom reč: $c_4c_3c_2c_1 \oplus c_4'c_3'c_2'c_1' = 0000 \oplus 0111 = 0111$
$\Rightarrow$ greška je na poziciji $(0111)_2 = 7$ tj. u bitu m_4

korektna poruka je: 0101**1**101

4. Koristeći Hamming SEC kodove izvršiti korekciju greške ukoliko postoji u poruci:

m_8	m_7	m_6	m_5	m_4	m_3	m_2	m_1	c_4	c_3	c_2	c_1
0	1	1	0	0	1	0	1	0	1	1	0

Rešenje:
$c_1' = m_1 \oplus m_2 \oplus m_4 \oplus m_5 \oplus m_7 = 1 \oplus 0 \oplus 0 \oplus 0 \oplus 1 = 0$
$c_2' = m_1 \oplus m_3 \oplus m_4 \oplus m_6 \oplus m_7 = 1 \oplus 1 \oplus 0 \oplus 1 \oplus 1 = 0$
$c_3' = m_2 \oplus m_3 \oplus m_4 \oplus m_8 = 0 \oplus 1 \oplus 0 \oplus 0 = 1$
$c_4' = m_5 \oplus m_6 \oplus m_7 \oplus m_8 = 0 \oplus 1 \oplus 1 \oplus 0 = 0$

sindrom reč: $c_4c_3c_2c_1 \oplus c_4'c_3'c_2'c_1' = 0110 \oplus 0100 = 0010$
$\Rightarrow$ greška je na poziciji $(0010)_2 = 2$, pa je došlo do greške u kontrolnom bitu c_2

sama poruka je korektna i glasi: 01100101