Binarna matematika

Stjepanek, Jaruška

Master's thesis / Diplomski rad

2016

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Science / Sveučilište u Zagrebu, Prirodoslovno-matematički fakultet**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:217:927399

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-03-29**



Repository / Repozitorij:

Repository of the Faculty of Science - University of Zagreb







SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Jaruška Stjepanek

BINARNA MATEMATIKA

Diplomski rad

Voditelj rada:
doc. dr. sc. Franka Miriam Brückler

Zagreb, 2016.

Ovaj diplomski rad obranjen je dana _____ pred ispitnim povjerenstvom u sastavu:

1. _____, predsjednik
2. _____, član
3. _____, član

Povjerenstvo je rad ocijenilo ocjenom _____.

Potpisi članova povjerenstva:

1. _____
2. _____
3. _____

Zahvaljujem se svojoj mentorici doc. dr. sc. Franki Miriam Brückler na pomoći pri odabiru teme, strpljivosti i pomoći pri izradi ovog diplomskog rada.
Veliko hvala mojim roditeljima, sestri, djedu, kolegama, prijateljima i svima koji su mi bili podrška tijekom školovanja.

Sadržaj

Sadržaj **iv**

Uvod **3**

1 Matematičke igre i trikovi **4**
1.1 Pogodi zamišljeni broj 4
1.2 Koja kartica je okrenuta? 5
1.3 Matematička igra Nim 7

2 De Bruijnovi nizovi **10**
2.1 Trik s kartama 10
2.2 Primjene de Bruijnovih nizova 15

3 Hammingovi kodovi **17**
3.1 Trik s karticama 17
3.2 Trik iz perspektive matematičara: Hammingovo (de)kodiranje 20

4 Sheme praga u kriptografiji **25**
4.1 Kriptografija 25
4.2 Osnovno o shemama praga 26
4.3 Sheme praga u vizualnoj kriptografiji 27

5 Zaključne napomene **35**

Bibliografija **37**

Uvod

Uz dekadski brojevni sustav, najpoznatiji brojevni sustav primjenjiv u raznim područjima je binarni brojevni sustav. Razvojem moderne tehnologije, robotike, sustava za zaštitu podataka kao i mnogih drugih područja, nizovima binarnih znamenki, tj. nizovima nula i jedinica, koje su osnovica binarnog brojevnog sustava, pridaje se sve veći značaj. Kao primjer spomenimo ovdje korištenje binarnih ASCII kodova za prikaz znakova tastature u računalu.

U ovom radu prikazat ćemo neke primjene binarnog brojevnog sustava u svakodnevnom životu te trikove čije tajne izvođenja leže upravo u primjeni binarnog brojevnog sustava. Neki od navedenih primjera mogu se primijeniti i kao učeničke aktivnosti u nastavi matematike ili njenoj popularizaciji.

Binarni brojevni sustav je pozicijski brojevni sustav s bazom 2, što znači da za zapisivanje brojeva koristimo dvije znamenke: 0 i 1. Pretvorba broja zapisanog u dekadskom brojevnom sustavu u zapis u binarnom brojevnom sustavu provodi se tako da dekadski zapis broja dijelimo bazom 2 te zapisujemo količnik i ostatak pri dijeljenju (0 ili 1). Količnik nastavljamo dijeliti te ponavljamo postupak sve dok je rezultat dijeljenja različit od nule. Ispišemo li ostatke od posljednjeg do prvog, dobivamo broj zapisan u binarnom obliku. Ilustrirajmo taj postupak na primjeru broja $(13)_{10}$:

$$\begin{array}{ll} 13 \div 2 = 6 & 1 \\ 6 \div 2 = 3 & 0 \\ 3 \div 2 = 1 & 1 \\ 1 \div 2 = 0 & \underbrace{1}_{\text{ostatak}} \end{array}$$

Slijedi da je binarni zapis broja $(13)_{10}$ jednak $(1101)_2$. Obrnuti postupak, tj. pretvaranje binarnog zapisa broja u dekadski zapis provodi se tako da se broj zapisan u binarnom obliku rastavi na težinske vrijednosti znamenaka, a težinska vrijednost znamenke dobije se na način da se baza 2 potencira eksponentom čija vrijednost odgovara položaju znamenke. Kao u svim apsolutno pozicijskim sustavima, krajnje desni eksponent ima vrijednost 0, predzadnji vrijednost 1, itd. Provedimo taj postupak na primjeru broja $(10110)_2$:

$$1 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 0 \cdot 2^0 = 1 \cdot 16 + 0 \cdot 8 + 1 \cdot 4 + 1 \cdot 2 + 0 \cdot 1 = 22.$$

Vidimo da je dekadski zapis broja $(10110)_2$ jednak $(22)_{10}$.

Operacija zbrajanja u binarnom brojevnom sustavu provodi se tako da se zbrajaju znamenke iste težinske vrijednosti počevši od znamenaka s najmanjom težinskom vrijednošću pri čemu vrijedi:

$$\begin{aligned} 0 + 0 &= 0 \\ 0 + 1 &= 1 \\ 1 + 0 &= 1 \\ 1 + 1 &= 1\,0 \\ 1 + 1 + 1 &= 1\,1 \end{aligned}$$

Uočimo da je $1 + 1 = 10$, što znači da za zbroj $1 + 1$ pišemo 0, a 1 prenosimo te pribrajamo znamenkama iduće po redu težinske vrijednosti. Analogno, u slučaju $1 + 1 + 1$ pišemo 1 te prenosimo 1.

Primjer 0.0.1. *Izračunajte zbroj brojeva* 101100 *i* 111001 *u binarnom brojevnom sustavu.*

$$\begin{array}{cccccccc} & 1 & 0 & 1 & 1 & 0 & 0 \\ + & 1 & 1 & 1 & 0 & 0 & 1 \\ \hline 1 & 1 & 0 & 0 & 1 & 0 & 1 \end{array}$$

Operacija množenja brojeva u binarnom brojevenom sustavu provodi se analogno kao množenje u dekadskom brojevnom sustavu te vrijedi:

$$\begin{aligned} 0 \cdot 0 &= 0 \\ 0 \cdot 1 &= 0 \\ 1 \cdot 0 &= 0 \\ 1 \cdot 1 &= 1 \end{aligned}$$

Primjer 0.0.2. *Izračunajte umnožak brojeva* 11010 *i* 1011 *u binarnom brojevnom sustavu.*

$$\begin{array}{cccccccccc} & 1 & 1 & 0 & 1 & 0 & \cdot & 1 & 0 & 1 & 1 \\ \hline & 1 & 1 & 0 & 1 & 0 & & & & & \\ & & 0 & 0 & 0 & 0 & 0 & & & & \\ & & & 1 & 1 & 0 & 1 & 0 & & & \\ + & & & & 1 & 1 & 0 & 1 & 0 & & \\ \hline 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & & \end{array}$$

Uz obično zbrajanje u binarnom sustavu često se koristi i tzv. nim-zbrajanje, u oznaci $\oplus$. To je zbrajanje za koje vrijedi:

$$1 \oplus 0 = 0 \oplus 1 = 1$$
$$1 \oplus 1 = 0 \oplus 0 = 0$$

Nim-zbrajanjem binarnih brojki a i b nastaje brojka c na sljedeći način: $(a_m \dots a_0)_2 \oplus (b_m \dots b_0)_2 = (c_m \dots c_0)_2$, gdje je $c_p = (a_p + b_p) \mod 2$, $p = 0, \dots, m$[1].

Primjer 0.0.3. *Izračunajte zbroj, umnožak i nim-zbroj brojeva* 10011 *i* 1010 *u binarnom brojevnom sustavu.*

zbroj:

$$\begin{array}{cccccc} & 1 & 0 & 0 & 1 & 1 \\ + & & 1 & 0 & 1 & 0 \\ \hline & 1 & 1 & 1 & 0 & 1 \end{array}$$

nim-zbroj:

$$\begin{array}{cccccc} & 1 & 0 & 0 & 1 & 1 \\ \oplus & & 1 & 0 & 1 & 0 \\ \hline & 1 & 1 & 0 & 0 & 1 \end{array}$$

umnožak:

$$\begin{array}{cccccccccc} & 1 & 0 & 0 & 1 & 1 & \cdot & 1 & 0 & 1 & 0 \\ \hline & 0 & 0 & 0 & 0 & 0 & & & & & \\ & & 0 & 0 & 0 & 0 & 0 & & & & \\ & & & 1 & 0 & 0 & 1 & 1 & & & \\ + & & & & 0 & 0 & 0 & 0 & 0 & & \\ \hline & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & & \end{array}$$

[1] S $x \mod 2$ označavamo ostatak pri dijeljenju broja x s 2.

Poglavlje 1

Matematičke igre i trikovi

Binarni brojevi koriste se u provođenju različitih trikova te u strategijama matematičkih igara. U ovom poglavlju opisat ćemo neke od njih.

1.1 Pogodi zamišljeni broj

Trik iz perspektive promatrača

1	3	5	7
9	11	13	15
17	19	21	23
25	27	29	31

2	3	6	7
10	11	14	15
18	19	22	23
26	27	30	31

4	5	6	7
12	13	14	15
20	21	22	23
28	29	30	31

8	9	10	11
12	13	14	15
24	25	26	27
28	29	30	31

16	17	18	19
20	21	22	23
24	25	26	27
28	29	30	31

Slika 1.1: Kartice za provođenje trika: Pogodi zamišljeni broj

Izvođač trika daje pet kartica (Slika 1.1) sudioniku trika. Sudionik treba zamisliti prirodan broj između 1 i 31 te izdvojiti kartice na kojima se nalazi zamišljeni broj. Odmah nakon primitka izdvojenih kartica, izvođač pogađa koji je broj zamislio sudionik. Ako su, na primjer, izdvojene prva, treća i četvrta kartica, onda je sudionik trika zamislio broj 13.

Trik iz perspektive matematičara

Na svakoj kartici nalazi se 16 različitih brojeva između 1 i 31 te je prvi broj na svakoj kartici neka od potencija broja 2 (na prvoj kartici prvi broj je $2^0 = 2$, na drugoj $2^1 = 2$, na trećoj $2^2 = 4$, na četvrtoj $2^3 = 8$ i na petoj $2^4 = 16$). Prisjetimo li se pretvorbe brojeva iz binarnog u dekadski brojevni sustav, znamo da mjesta na kojima se nalaze jedinice u binarnom zapisu broja označavaju potencije broja 2 čijim zbrajanjem nastaje dani broj zapisan u dekadskom obliku. Na primjer, $(10110)_2 = 1 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 0 \cdot 2^0 = 16 + 4 + 2 = 22$. Uočimo da se broj 22 nalazi na drugoj, trećoj i četvrtoj kartici. Također, uočimo da prvi brojevi na tim karticama zbrojeni daju broj 22. Tajna trika je u raspodjeli brojeva na karticama, tj. brojevi od 1 do 31 su raspoređeni na kartice tako da se svaki od tih brojeva nalazi na svim karticama na kojima je prvi broj potencija broja 2 čijim zbrajanjem je nastao dani broj pri pretvorbi iz binarnog u dekadski zapis. Tako su, na primjer, na kartici s prvim brojem 4 svi brojevi koji u binarnom zapisu imaju 1 na mjestu druge potencije broja 2. Dakle, pri izvođenju trika, izvođač trika je odgonetnuo o kojem se zamišljenom broju radi tako što je zbrojio brojeve koji se nalaze na prvom mjestu izdvojenih kartica. Ako su izdvojene druga, četvrta i peta kartica, onda je zamišljeni broj $2 + 8 + 16 = 26$.

Ovaj trik je moguće izvesti u različitim varijantama. Trik se može izvesti tako da sudionik mora zamisliti broj manji od bilo koje potencije broja 2. Broj kartica potrebnih za izvođenje trika ovisi o kojoj potenciji broja 2 se radi. Varijanta trika u kojoj sudionik zamišlja broj manji od 8 izvodi se s 3 kartice na kojima se nalaze 4 broja (prva kartica: 1, 3, 5, 7; druga kartica: 2, 3, 6, 7; treća kartica: 4, 5, 6, 7). U varijanti sa zamišljenim brojem manjim od 16 koriste se 4 kartice s po 8 brojeva na svakoj. Uočimo da se povećanjem odabrane potencije broja 2, povećava broj kartica za izvođenje trika kao i količina brojeva na svakoj kartici pa će sudionik trika dulje izdvajati kartice na kojima se nalazi zamišljen broj čime trik postaje zamoran. Također, povećava se vjerojatnost da sudionik pogriješi u izdvajanju kartica u slučaju da previdi zamišljeni broj na kartici zbog velike količine brojeva na karticama.

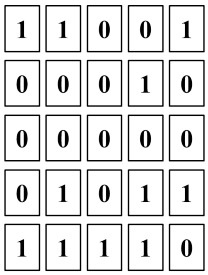
1.2 Koja kartica je okrenuta?

Trik se može izvoditi s karticama s različitim bojama prednje i stražnje strane ili, zbog primjene aktivnosti u popularizaciji binarnog brojevnog sustava, kartice označene s nulom na jednoj i jedinicom na drugoj strani.

Trik iz perspektive promatrača

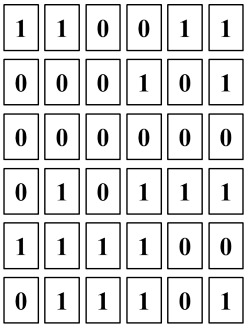
Jedan ili dva sudionika trika poslažu ispred izvođača trika kartice u obliku kvadrata, npr. kartice poslažu u 5 redaka i 5 stupaca odabravši proizvoljno stranu kartice koja će biti vidljiva

(Slika 1.2). Slaganjem većeg broja kartica, povećava se efekt trika. Nakon toga, izvođač



Slika 1.2: Primjer složenih kartica za trik: Koja kartica je okrenuta?

trika dodaje još jedan redak i stupac kartica kako bi se povećao ukupan broj kartica čime se otežava memoriranje položaja svih kartica (Slika 1.3). Dok izvođač ima prekrivene oči,



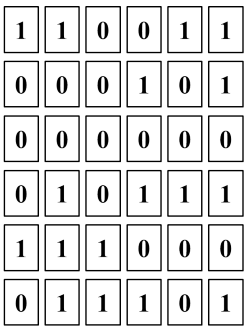
Slika 1.3: Primjer složenih kartica za trik: Koja kartica je okrenuta? s dodanim karticama

netko od sudionika okrene jednu karticu, npr. na Slici 1.4 okrenuta je kartica u 5. retku i 4. stupcu. Pogledavši kartice, izvođač trika pogađa koja kartica je okrenuta.

Trik iz perspektive matematičara

Tajna trika je postupak u kojem izvođač trika dodaje kartice u još jedan redak i stupac k već posloženim karticama. Izvođač dodaje kartice tako da u svakom retku i stupcu, nakon dodavanja, bude paran broj kartica s jedinicom te zbog tako posloženih kartica, izvođač trika nakon okretanja jedne kartice lako otkriva koja kartica je okrenuta jer se u retku i stupcu koji sadrže okrenutu karticu nalazi neparan broj kartica s jedinicom.

Nizovi nula i jedinica na posloženim karticama u pojedinom retku i stupcu predstavljaju kodnu riječ zapisanu u binarnom brojevnom sustavu na koju se dodaje tzv. paritetni



Slika 1.4: Primjer složenih kartica za trik: Koja kartica je okrenuta? nakon okretanja jedne kartice

bit kako bi se zaštitila poruka od pogreške. Takav način zaštite se svakodnevno upotrebljava u ISBN-u, tj. Međunarodnom standardnom knjižnom broju (eng. International Standard Book Number), koji se nalazi na poleđini knjige koju jedinstveno identificira. Od 10 znamenaka ISBN-a, 9 znamenaka identificira knjigu, a deseta znamenka je kontrolna znamenka koja kao paritetni bit u triku otkriva je li došlo do pogreške u zapisu identifikacijskog broja knjige, npr. prilikom naručivanja knjige uz pomoć ISBN-a.

1.3 Matematička igra Nim

Nim je jedna od najstarijih i najpoznatijih matematičkih igara za dva igrača. Matematičar Charles Leonard Bouton je 1902. godine u potpunosti objasnio i analizirao igru te joj dao ime Nim, vjerojatno prema zastarjelom engleskom glagolu *nim* koji znači „uzeti", odnosno „ukrasti" ili prema imperativu njemačkog glagola *nehmen* (*Nimm!*) koji u prijevodu znači „Uzmi!". Igra se može igrati s novčićima, kamenčićima, žetonima, kartama, šibicama i sl.

Pravila i opis igre

Na stolu se rasporede kamenčići u nekoliko hrpica, tj. redova (najčešće tri reda) tako da je broj kamenčića u svakom retku proizvoljan. Igru u kojoj prvi redak sadrži a kamenčića, drugi redak b kamenčića, treći redak c kamenčića, itd. označavamo s (a, b, c,...). Igrači naizmjenično uzimaju jedan ili više kamenčića iz proizvoljno odabranog retka. Igrač koji je na potezu ne smije uzimati kamenčiće iz više od jednog retka u jednom potezu, ali iz jednog retka smije uzeti proizvoljno mnogo kamenčića pa čak i cijeli redak. U standardnoj varijanti igre pobjednik je igrač koji uzme posljednji kamenčić, dok u tzv. mizernoj varijanti gubi igrač koji odigra posljednji potez. Nim igru nazivamo pobjedničkom ako igrač

koji prvi igra može odabrati niz poteza te pobijediti neovisno o tome kako igra drugi igrač, dok gubitničkom igrom nazivamo igru u kojoj drugi igrač, bez obzira što odigra prvi igrač, ispravnim potezom može osigurati sebi pobjedu.

Primjeri mogućih situacija i strategije

Ako se igra samo s jednim retkom kamenčića, ta igra je pobjednička bez obzira na broj kamenčića u retku jer prvi igrač uzima sve kamenčiće i time je pobjednik.

Igra s dva retka s istim brojem kamenčića u retcima je gubitnička jer prvi igrač uzevši proizvoljan broj kamenčića iz odabranog retka ostavlja drugom igraču mogućnost da nizom daljnjih pravilnih poteza svede igru na situaciju (1, 1) te time prvom igraču ne preostaje ništa drugo nego uzeti jedan kamenčić iz jednog retka i drugi igrač uzima posljednji kamenčić čime prvi igrač gubi igru. Igre s različitim brojem kamenčića u dva retka su pobjedničke jer prvi igrač može takvu igru jednim potezom svesti na situaciju s dva jednaka retka čime igra postaje gubitnička za drugog igrača.

Igre s tri retka u kojima je u jednom retku 1 kamenčić, a u drugom i trećem retku se nalazi jednak broj kamenčića su pobjedničke igre jer prvi igrač nizom poteza može svesti igru na situaciju s dva retka s jednakim brojem kamenčića i time osigurati sebi pobjedu. Isto vrijedi i za igru u kojoj se u dva retka nalazi po jedan kamenčić, a u trećem retku je proizvoljan broj kamenčića. Dakle, u takvim situacijama, treba nizom poteza pokušati svesti igru na situaciju s dva jednaka retka. Za otkrivanje opće strategije koristit ćemo binarni brojevni sustav i nim-zbrajanje.

Formula pobjede

Za otkrivanje strategije bitan je teorem L. C. Boutona:

Teorem 1.3.1. *Nim igra* $(x_1, x_2, x_3, \ldots, x_n)$ *je gubitnička ako i samo ako je nim-suma svih redaka jednaka* 0*, tj. ako i samo ako vrijedi:* $x_1 \oplus x_2 \oplus x_3 \oplus \cdots \oplus x_n = 0$.

Skica dokaza. U svakoj krajnjoj poziciji nim-suma svih redaka je nula. Budući da iz svake igre u kojoj nim-suma redaka nije nula, postoji potez koji vodi u poziciju čija je nim-suma svih redaka nula te uzimajući u obzir činjenicu da svaki potez iz igre u kojoj je nim-suma svih redaka jednaka 0 vodi u igru gdje je nim-suma redaka različita od nule, možemo zaključiti da su igre u kojima je nim-suma svih redaka jednaka nuli pobjedničke, odnosno da su pobjedničke igre one pozicije kojima je nim-suma jednaka nuli. Potpuni dokaz ovog teorema može se naći u knjizi [4]. □

Dakle, igrač na potezu treba eliminirati određen broj kamenčića iz pojedinog retka tako da nim-suma postane 0, tj. da igra postane gubitnička za drugog igrača; ukoliko je to moguće, igra je pobjednička, a u suprotnom gubitnička. Primijenimo sada teorem na

primjeru igre (50, 19, 11). Zapišemo li brojeve kamenčića u pojedinom retku u binarnom brojevnom sustavu te ih nim-zbrojimo, dobivamo:

$$\begin{array}{cccccc} 1 & 1 & 0 & 0 & 1 & 0 \\ & 1 & 0 & 0 & 1 & 1 \\ \oplus & & 1 & 0 & 1 & 1 \\ \hline 1 & 0 & 1 & 0 & 1 & 0 \end{array}$$

Vidimo da je nim-suma svih redaka različita od nule, dakle, igra (50, 19, 11) je pobjednička. Igrač odabire hrpu s koje će oduzeti određen broj kamenčića tako da u nim-zbroju odabere 1 s najvećom težinskom vrijednošću. Iznad odabrane 1 postoji barem jedna 1 te igrač odabire jednu od njih ako ih je više (koliko ima 1 iznad odabrane 1 u nim-zbroju, toliko ima mogućnosti odabira hrpe s koje može uzeti kamenčiće) i iz nje će uzeti kamenčiće. Dakle, igrač odabire prvi redak. Na svim mjestima u broju 110010 gdje se se u nim-zbroju pojavile 1 promijenimo 1 u 0 i 0 u 1, tj. promijenimo parnost u tim stupcima čime nim-zbroj postaje 0. Dakle, prvi broj postaje $(11000)_2$=24 što znači da s prve hrpe od 50 kamenčića, igrač mora oduzeti 26 kamenčića. Novonastala igra je (24, 19, 11) te je to gubitnička igra jer je nim-zbroj redaka jednak 0:

$$\begin{array}{cccccc} & 1 & 1 & 0 & 0 & 0 \\ & 1 & 0 & 0 & 1 & 1 \\ \oplus & & 1 & 0 & 1 & 1 \\ \hline & 0 & 0 & 0 & 0 & 0 \end{array}$$

Uzevši 24 kamenčića iz prvog retka, prvi igrač je početnu pobjedničku igru pretvorio u gubitničku igru za drugog igrača. Dakle, igranjem nima, cilj igrača na potezu je svesti igru na situaciju s parnim brojem jedinica u svakom stupcu pri potpisivanju brojeva kamenčića jednog ispod drugog u binarnom zapisu. U nimu iz svake gubitničke igre barem jedno oduzimanje kamenčića vodi u pobjedničku poziciju, a iz pobjedničke igre svako oduzimanje vodi u gubitničku igru.

Poglavlje 2

De Bruijnovi nizovi

De Bruijnovi nizovi su vrsta binarnih nizova sa specijalnim svojstvima i nizom primjena, a mi ćemo ih ovdje uvesti kao osnovu jednog magičnog trika.

2.1 Trik s kartama

Trik iz perspektive promatrača

Trik se izvodi sa špilom karata pred publikom u kojoj je barem petero gledatelja. Izvođač trika šalje špil karata u publiku i zamoli petero gledatelja, koji će biti sudionici trika, da svaki od njih presiječe špil karata tako da razdvoji špil na dva dijela i zamijeni mjesta tim dvama dijelovima. Sudionik koji je peti po redu presjekao špil uzima kartu s vrha špila te vraća špil sudioniku koji je četvrti po redu presjekao špil te on također uzima kartu s vrha špila. Špil se tako prosljeđuje redom sve do sudionika koji je prvi presijecao špil i svaki sudionik trika kod sebe sada ima jednu kartu. Izvođač najavljuje da će svojim telepatskim sposobnostima otkriti koju kartu posjeduje svaki sudionik ako mu oni misaono pošalju informacije o kartama koje posjeduju. Prividno uznemiren, izvođač govori da je previše informacija u zraku te da će mu odgovori na nekoliko pitanja pomoći u otkrivanju. Neka od pitanja koja postavlja su: „Je li netko ručao ćevape?", „Tko je ove godine bio u kazalištu?", „Tko ima crvenu kartu?", „Tko ima kućnog ljubimca?". Nakon postavljenih pitanja, izvođač pogađa boju i vrijednost karte svakog sudionika.

Trik iz perspektive matematičara

Možemo pretpostaviti da su za uspješno provođenje trika bili ključni odgovori sudionika na pitanje „Tko ima crvenu kartu?". Razlikujući moguće slučajeve (samo prvi sudionik ima crvenu kartu, niti jedan sudionik nema crvenu kartu, prva dva sudionika imaju crvenu

kartu i tako dalje), izvođač trika je mogao dobiti 32 različita odgovora jer je svaki od pet sudionika mogao odgovoriti na dva različita načina (da ili ne), iz čega slijedi da postoje $2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 32$ različite mogućnosti odgovora. Napomenimo da se špil karata za izvođenje trika sastoji od 32 karte te da ova povezanost nije slučajna. Ako bi se trik izvodio sa četiri sudionika, onda bi se koristio špil od 16 karata.

Također, bitan je poredak karata na početku, naime 32 karte su poredane tako da je poredak boja u svakom skupu od pet uzastopnih karata jedinstven te se presjecanjem špila ne mijenja taj ciklički poredak. Pogledajmo to na primjeru špila od 8 karata. U tom slučaju, trik bi se provodio s trojicom sudionika te bi se odgovori sudionika, na pitanje „Tko ima crvenu kartu?", mogli pojaviti na 8 različitih načina. Zbog jednostavnosti zapisa, označimo crvene karte s 1, a crne karte s 0. Sada možemo moguće ishode u provođenju trika sa špilom od 8 karata zapisati uz pomoć 0 i 1: 111 (sve tri karte su crvene), 110 (prve dvije karte su crvene, a treća karta je crna), 100, 000, 001, 010, 101 i 011. Nađimo neki niz od 8 nula i jedinica tako da se svaki podniz od tri uzastopna znaka pojavi samo jednom. Jedan takav je 11100010 pa karte u špilu na početku moraju biti poredane tako da su prve tri karte crvene, sljedeće tri karte su crne nakon čega slijedi jedna crvena i jedna crna karta. Uočimo da u špil možemo staviti karte bilo koje vrijednosti.

Želimo li primijeniti analogiju na trik sa špilom od 32 karte, trebamo ispisati sve moguće slučajeve niza od pet karata obzirom na poredak boja, a to je ukupno $2^5 = 32$ i onda osmisliti niz od 32 nule i jedinice u kojem se svaki od ta 32 peteročlana podniza pojavljuje točno po jednom. Takvi se nizovi zovu de Bruijnovi nizovi:

Definicija 2.1.1. *De Bruijnov niz reda k nad alfabetom A od n simbola je n^k-člani ciklički niz u kojem se svaki mogući k-člani podniz simbola iz A pojavljuje točno po jednom.*

U nastavku ćemo pod de Bruijnovim nizovima podrazumijevati binarne de Bruijnove nizove, dakle de Bruijnove nizove nad dvočlanim alfabetom 0, 1.

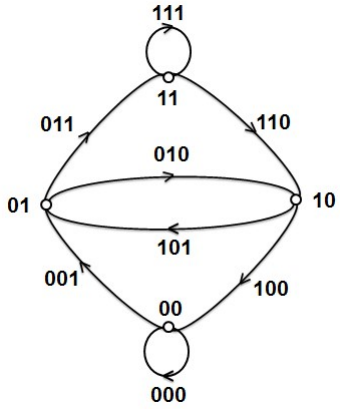
Primjer 2.1.2. *Niz* 11100010 *je de Bruijnov niz reda* 3.

Sada se pitamo postoji li de Bruijnov niz za svaki prirodan broj k? Ako postoji, koliko takvih nizova ima te kako ih pronaći? Da bismo odgovorili na ova pitanja, modelirat ćemo situaciju uz pomoć usmjerenog grafa.

Definicija 2.1.3. *Usmjereni graf ili digraf D sastoji se od nepraznog konačnog skupa V(D), čije elemente zovemo vrhovima (eng. vertex), i konačne familije E(D) uređenih parova elemenata skupa V(D), koje zovemo bridovima ili lukovima (eng. edge).*

Nacrtajmo sada usmjereni graf s 2^{k-1} vrhova koji su označeni svim različitim $(k-1)$-članim nizovima nula i jedinica. Pogledajmo primjer za $k = 3$. Usmjereni graf na slici 2.1 ima $2^2 = 4$ vrha označena s: 00, 01, 10, 11. Brid koji spaja vrh 10 s vrhom 00 označen je s

100, tj. označen je s nizom duljine 3 kojem su prve dvije znamenke 10, a posljednje dvije su 00.



Slika 2.1: De Bruijnov graf za $k = 1$

U tom grafu tražimo Eulerovu turu [1]. Možemo krenuti od bilo kojeg vrha, primjerice iz vrha 00. Ako ispišemo prve znamenke bridova u Eulerovoj turi, redom kojim ih obilazimo, dobit ćemo de Bruijnov niz reda 3: 00011101. Iako je crtanje grafa za $k > 3$ zahtjevnije, de Bruijnov graf možemo promatrati za bilo koji $k \in \mathbb{N}$. Općenito, Eulerovom turom po de Bruijnovom grafu dobivamo de Bruijnov niz s duljinom podniza k, za sve $k \in N$.

Kako je svaki vrh de Bruijnovog grafa označen $(k-1)$-torkom nula i jedinica koje, nakon izlaska iz vrha, postaju k-torke, zaključujemo da iz svakog vrha izlaze točno dva brida. Analogno, zaključujemo da u svaki vrh de Bruijnovog grafa ulaze točno dva brida te time zaključujemo da je svaki vrh grafa paran jer je broj bridova koji ulaze u vrh jednak broju bridova koji izlaze iz tog vrha. Kako vrijedi slijedeći teorem:

Teorem 2.1.4. *Povezani graf je Eulerov (sadrži Eulerovu turu) ako i samo ako mu je svaki vrh parnog stupnja.*

možemo zaključiti da de Bruijnov niz postoji za svaki $k \in \mathbb{N}$. Nizozemski matematičar Nicolaas de Bruijn, osim što je otkrio de Bruijnov niz i graf, otkrio je i da za svaki $k \in \mathbb{N}$ postoji $2^{2^{k-1}-1}$ binarnih de Bruijnovih nizova reda 2 duljine podniza k.

Sad kada smo otkrili kako uz pomoć de Bruijnova grafa možemo naći de Bruijnov niz, vratimo se na trik s kartama. Budući da su u špilu bile 32 karte te da je u triku sudjelovalo 5 sudionika, tražimo de Bruijnov niz reda 5. Nacrtamo li de Bruijnov graf za $k = 5$, pronaći

[1] Eulerova tura na grafu je zatvorena staza koja sadrži svaki brid, tj. zatvorena staza koja prolazi svakim bridom točno jedanput.

ćemo jedan de Bruijnov niz: 00000100101100111110001101110101. Uklonimo iz špila karata sve karte s vrijednošću 9 te kraljeve, dame i dečke svih boja. Posložimo karte u špilu krenuvši od najgornje karte u špilu ovim redoslijedom: 8♣,A♣, 2♣, 4♣,A♠, 2♢, 5♣, 3♠, 6♢, 4♠,A♡, 3♢, 7♣, 7♠, 7♡, 6♡, 4♡, 8♡,A♢, 3♣, 6♣, 5♠, 3♡, 7♢, 6♠, 5♡, 2♡, 5♢, 2♠, 4♢, 8♠, 8♢. Uočimo da pritom boje crveno i crno alterniraju u skladu s odabranim de Bruijnovim nizom i da, naravno, nema duplikata karata. Uloga različitih boja (u standardnom kartaškom smislu boje su četiri: karo, srce, pik i tref) i vrijednosti karata bit će objašnjena niže.

Presijecanjem špila promijenit će se početna karta, no neće se promijeniti ciklički poredak karata u špilu. Izvođaču trika jedino preostaje dekodirati odgovor na pitanje „Tko ima crvenu kartu?" u imena karata koje imaju sudionici trika u čemu će mu pomoći lista (na slici 2.2) svih mogućih slučajeva koje smo ispisali uz pomoć de Bruijnova niza za $k = 5$ pri čemu smo karte crne boje označili nulom, a crvene karte jedinicama. Ako treći i peti sudionik trika imaju crvenu kartu, izvođač to dešifrira u niz nula i jedinica: 00101 te očitava s liste slučajeva da su izvučene karte redom: 5♣, 3♠, 6♢, 4♠,A♡.

00000	8♣ A♣ 2♣ 4♣ A♠	01000	8♠ 8♦ 8♣ A♣ 2♣
00001	A♣ 2♣ 4♣ A♠ 2♦	01001	A♠ 2♦ 5♣ 3♠ 6♦
00010	2♣ 4♣ A♠ 2♦ 5♣	01010	2♠ 4♦ 8♠ 8♦ 8♣
00011	3♣ 6♣ 5♠ 3♥ 7♦	01011	3♠ 6♦ 4♠ A♥ 3♦
00100	4♣ A♠ 2♦ 5♣ 3♠	01100	4♠ A♥ 3♦ 7♣ 7♠
00101	5♣ 3♠ 6♦ 4♠ A♥	01101	5♠ 3♥ 7♦ 6♠ 5♥
00110	6♣ 5♠ 3♥ 7♦ 6♠	01110	6♠ 5♥ 2♥ 5♦ 2♠
00111	7♣ 7♠ 7♥ 6♥ 4♥	01111	7♠ 7♥ 6♥ 4♥ 8♥
10000	8♦ 8♣ A♣ 2♣ 4♣	11000	8♥ A♦ 3♣ 6♣ 5♠
10001	A♦ 3♣ 6♣ 5♠ 3♥	11001	A♥ 3♦ 7♣ 7♠ 7♥
10010	2♦ 5♣ 3♠ 6♦ 4♠	11010	2♥ 5♦ 2♠ 4♦ 8♠
10011	3♦ 7♣ 7♠ 7♥ 6♥	11011	3♥ 7♦ 6♠ 5♥ 2♥
10100	4♦ 8♠ 8♦ 8♣ A♣	11100	4♥ 8♥ A♦ 3♣ 6♣
10101	5♦ 2♠ 4♦ 8♠ 8♦	11101	5♥ 2♥ 5♦ 2♠ 4♦
10110	6♦ 4♠ A♥ 3♦ 7♣	11110	6♥ 4♥ 8♥ A♦ 3♣
10111	7♦ 6♠ 5♥ 2♥ 5♦	11111	7♥ 6♥ 4♥ 8♥ A♦

Slika 2.2: Lista svih mogućih slučajeva

Pravilo za izvođenje trika

Želimo li trik izvesti bez šalabahtera, prikazat ćemo svaku kartu iz špila u obliku $\overbrace{ab}^{\text{boja}}\overbrace{cde}^{\text{vrijednost}}$, pri čemu su $a, b, c, d, e \in \{1, 0\}$. Prve dvije znamenke označavaju boju karte kao na slici 2.3, a posljednje tri znamenke označavaju vrijednost karte i to tako da je vrijednost karte zapisana u binarnom brojevnom sustavu. Karte u špilu imaju vrijednosti: 2, 3, 4, 5, 6,



Slika 2.3: Oznake za boje karata

7, 8 i 1 (as) u dekadskom brojevnom sustavu. Zapišemo sve vrijednosti karata iz špila u binarnom brojevnom sustavu:

dekadski zapis broja	binarni zapis broja
1	001
2	010
3	011
4	100
5	101
6	110
7	111
8	000

Uočimo da u špilu nemamo kartu s vrijednošću 0 pa smo karti s vrijednošću 8 dodijelili oznaku 000 (što je matematički smisleno jer 8 pri dijeljenju s 2 daje ostatak nula). Budući da prva dva znaka predstavljaju boju, a posljednja tri vrijednost karte, slijedi da npr. niz 11010 predstavlja dvojku srce (2♡), niz 01111 sedmicu pik (7♠) itd. Da bismo odredili redoslijed karata u špilu možemo iskoristiti de Bruijnov niz za $k = 5$: 000001001011... Prvih pet znakova 00000 nam govori da je prva karta u špilu osmica tref (8♣), drugi skup od pet znakova, počevši od drugog znaka, je 00001 te zaključujemo da je druga karta u špilu as tref (A♣) i tako dalje.

Provjeravajući tako redom, zaključujemo da se dobiveni niz karata podudara s početnim nizom karata pa bi nam bilo korisno pravilo kojim bismo mogli sami nizati nule i jedinice kako bismo dobili gore navedeni niz. Zbrojimo li prvu i treću znamenku niza 00001, koji

predstavlja as tref (A♣), i ostatak pri dijeljenju dobivenog zbroja s dva dopišemo tom nizu, dobivamo 000010. Uočimo da iz tog niza možemo očitati peteročlani podniz počevši od drugog člana 00010 što predstavlja dvojku tref (2♣). Analognim postupkom na svakom sljedećem peteročlanom podnizu, dobit ćemo de Bruijnov niz iz kojeg lako možemo očitati redoslijed karata.

Pretpostavimo da su karte u špilu posložene gore navedenim redoslijedom. Tada možemo pri izvođenju trika, neprimjetno, nakon što su sudionici trika uzeli karte, pogledati koja karta se nalazi na vrhu špila, prevesti ju u kodni oblik *abcde* te, primjenjujući prikazani postupak, redom otkriti koje karte su izvukli sudionici trika krenuvši od karte koja je posljednja izvučena do karte koja je izvučena prva. Ukoliko karte u špilu koji posjedujemo nisu posložene redoslijedom za provođenje trika, špil možemo složiti tako da uzmemo bilo koju kartu, prevedemo ju u kodni oblik *abcde* te nizanjem znakova prema navedenom pravilu i dešifriranjem slagati redom karte.

2.2 Primjene de Bruijnovih nizova

De Bruijnovi nizovi se primjenjuju, također, u kriptografiji kao ključ pri prijenosu poruke, u biologiji pri spajanju dijelova DNA te pri programiranju kretanja robota.

Koristeći kemijsku olovku s ugrađenom kamerom (primjer takve olovke može se naći na [12]) možemo pisati po papiru te će sve što napišemo ili nacrtamo biti istovremeno prikazano na uparenom računalu, tabletu ili mobitelu. To omogućava kamera ugrađena u olovci koja u svakom trenutku može očitati točan položaj olovke na papiru s ucrtanim točkicama nevidljivim prostom oku. Točkice na papiru su raspoređene tako da je iz svake pozicije, na kojoj se nalazi olovka, vidljiv jedinstven uzorak kamerom. Ako točkice označimo 1, a praznine 0, papir po kojem pišemo olovkom činit će dvodimenzionalni niz brojeva takav da se svaki dvodimenzionalni podniz reda $u \times k$ (red ovisi o kameri na olovci) pojavljuje točno jednom. Takav dvodimenzionalni niz naziva se de Bruijnov dvodimenzionalni niz.

Definicija 2.2.1. *De Bruijnov dvodimenzionalni niz reda* $u \times k$ *je dvodimenzionalni niz* 0 *i* 1 *takav da se svaki dvodimenzionalni podniz* 0 *i* 1 *s u redaka i k stupaca pojavljuje točno jednom.*

Primjer 2.2.2. *De Bruijnov dvodimenzionalni niz reda* 2×2*:*

1	1	0	1
0	0	0	1
1	0	0	0
1	0	1	1

Podniz s dva retka i dva stupca smješten u sredini prikazan je kao: $\begin{array}{|c|c|}\hline 0 & 0 \\ \hline 0 & 0 \\ \hline \end{array}$. *Pomičući okvir s dva retka i dva stupca po danom de Bruijnovom nizu (uključujući rubove i uglove), za svaki položaj naći ćemo jedinstvenu kombinaciju* 0 *i* 1 *unutar rešetke. Još neki primjeri podnizova danog dvodimenzionalnog de Bruijnovog niza su:* $\begin{array}{|c|c|}\hline 1 & 1 \\ \hline 1 & 1 \\ \hline \end{array}$, $\begin{array}{|c|c|}\hline 0 & 1 \\ \hline 1 & 0 \\ \hline \end{array}$.

Nakon što olovka kamerom očita dvodimenzionalni niz brojeva, povezan uređaj će znati njenu točnu lokaciju na papiru jer će za svaku svoju poziciju olovka imati jedinstven vidljiv uzorak te će se tako određena pozicija prikazati na povezanom uređaju, koji ima identičan uzorak podjele papira na točkice.

Poglavlje 3

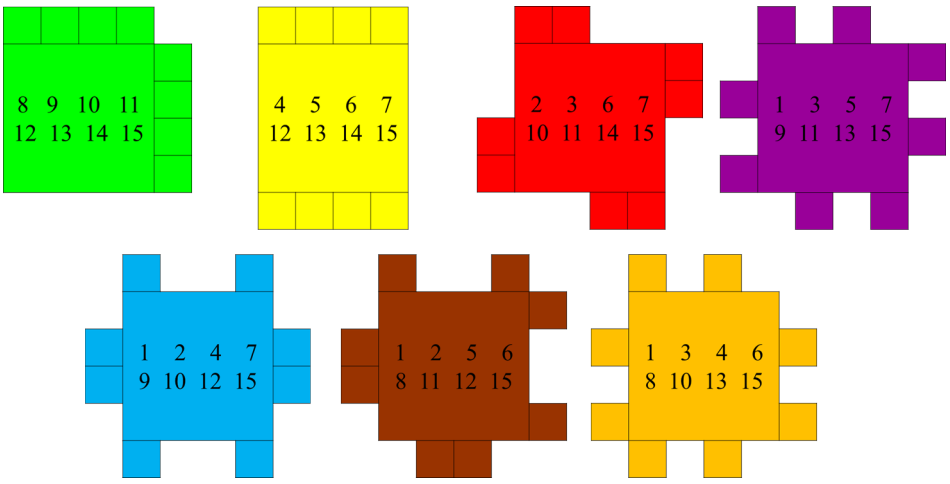
Hammingovi kodovi

U ovom poglavlju opisat ćemo kodove koji se koriste za otkrivanje i ispravljanje grešaka nastalih pri prijenosu poruka, tzv. Hammingove kodove. Pogledajmo prije svega primjer trika čija se tajna krije u upotrebi Hammingovih kodova.

3.1 Trik s karticama

Trik iz perspektive promatrača

Sudionik trika treba zamisliti broj od 1 do 15 te odabrati jednu od ponuđenih boja: zelena, žuta, crvena, ljubičasta, plava, smeđa ili narančasta. Nakon toga izvođač trika pokazuje

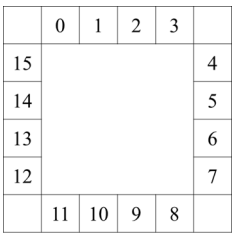


Slika 3.1: Kartice za trik s primjenom Hammingovog koda

sudioniku trika redom kartice (Slika 3.1) te za svaku karticu pita nalazi li se zamišljeni broj na toj kartici, no sudionik je dobio uputu da za karticu u boji koju je odabrao ponudi lažan odgovor, tj. ako se zamišljeni broj nalazi na kartici u boji koju je zamislio, tada treba odgovoriti da se ne nalazi i obrnuto. Nakon što je izvođač dobio odgovore za svaku karticu, on pogađa zamišljeni broj i boju.

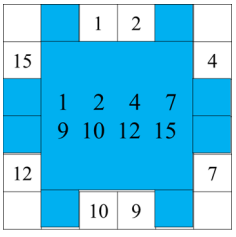
Upute za izvođenje trika

Za uspješno izvođenje trika, izvođač koristi karticu kao na slici 3.2. Brojevi od 0 do 15 na



Slika 3.2: Kartica na koju se slažu ostale kartice u triku s primjenom Hammingovog koda

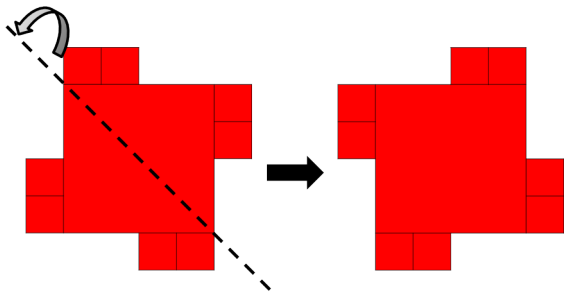
toj tzv. baznoj kartici su poredani po veličini počevši od 0 u lijevom gornjem kutu u smjeru kazaljke na satu. Taj položaj se lako pamti pa se pri izvođenju trika može, radi boljeg efekta, koristiti bazna kartica bez brojeva. Uočimo da se izbočeni kvadratići na karticama nalaze na takvim položajima da kada se kartica položi na baznu karticu, izbočeni kvadratići će prekriti brojeve koji se ne nalaze na kartici, tj. vidljivi će ostati brojevi koji se nalaze na kartici (na slici 3.3 je prikazana situacija u kojoj je sudionik trika odgovorio potvrdno na postavljeno pitanje). Ako sudionik trika odgovori potvrdno na pitanje nalazi li se zamišljen



Slika 3.3: Položena plava kartica na baznoj kartici nakon potvrdnog odgovora

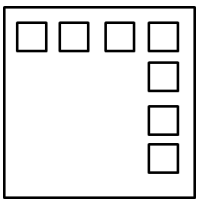
broj na kartici, izvođač polaže tu karticu u uspravnom položaju na baznu karticu, a ako je odgovor niječan, izvođač karticu okreće tako da položena na baznu karticu zauzima položaj

kao da je početna kartica zrcaljena obzirom na dijagonalu koja spaja gornji lijevi kut i donji desni (slika 3.4), tj. izbočeni kvadratići na tako položenoj kartici prekrivaju brojeve bazne kartice koji se ne nalaze na toj kartici. Nakon što su sve kartice položene na baznu karticu,



Slika 3.4: Primjer okretanja kartice u slučaju niječnog odgovora

broj kojeg je sudionik zamislio nalazi se prekriven samo jednom karticom i to karticom u boji koju je sudionik zamislio, dok su ostali brojevi prekriveni s dvije ili više kartica. Kako bi se trik što brže i efektnnije izveo, na bočnim kvadratićima možemo probušiti po jednu rupicu tako da se vidi boja kartice koja se nalazi ispod kartice na vrhu. Položaj rupica na bočnim kvadratićima svih kartica (uočimo da ih na svakoj ima po 8) je jednak za sve kvadratiće određene kartice, ali je različit od položaja rupica na ostalim karticama kako bi se izbjegla situacija u kojoj, nakon svih položenih kartica (uključujući i zrcaljene kartice), dvije kartice dijele istu poziciju rupica. Na slici 3.5 je prikazano sedam položaja na kojima



Slika 3.5: Mogući položaji rupica na karticama

možemo izbušitio rupice, od kojih se za svaku karticu bira jedan. Uz kartice s rupicama, zamišljen broj nalazit će se na mjestu gdje je bijela rupica, a boja koja okružuje tu rupicu odgovara zamišljenoj boji. Primijetimo da se uz zabranu laganja trik mogao izvesti s prve četiri kartice i traženjem jedinog nepokrivenog broja, no tada je trik ekvivalentan triku opisanom u prvom poglavlju ovog rada.

3.2 Trik iz perspektive matematičara: Hammingovo (de)kodiranje

Tajna trika bazirana je na kodu koji služi za otkrivanje i ispravak jedne pogreške (u ovom slučaju lažnog odgovora) tako da se otkrije točna pozicija u kodnoj riječi gdje je nastala greška i to dodavanjem paritetnih bitova. Takav kod naziva se Hammingov kod. Hammingovi kodovi koriste se, osim prilikom prijenosa poruka, i za ispravljanje pogrešaka pri očitavanju ogrebanog CD-a ili DVD-a.

Kao prvo, primijetimo da se radi o prijenosu binarne poruke određene duljine k (u našem slučaju $k = 7$ jer imamo 7 kartica). Svaki odgovor DA ili NE možemo shvatiti kao jednu od binarnih znamenki 0 ili 1 (jedan bit). Dakle, poruku odnosno slijed odgovora, možemo shvatiti kao binarni niz $x = x_1x_2 \dots x_k$ ($x_i \in \{0, 1\}$, $i = 1, \dots, k$). No, poruka je dulja nego je (u slučaju da nema greške odnosno laganja) potrebno da se identificira njen sadržaj (odabrani broj). U opisanom slučaju, želimo identificirati broj između 1 i 15, za što su nam dovoljne $n = 4$ binarne znamenke. Ukratko: Cilj nam je prenijeti binarnu informaciju duljine n,[1] a kako bismo mogli detektirati eventualne greške u prenesenoj informaciji, prenosimo binarnu informaciju duljine $k > n$. Jedan od načina da se to postigne je Hammingov (k, n)-kod. Ovdje ćemo opisati samo najjednostavniji, a to je Hammingov $(7, 4)$-kod, dok za općenitiju verziju čitatelja upućujemo na literaturu [5]. Hammingov kod služi prenošenju jedne od $2^4 = 16$ binarnih poruka duljine 4, uz uvjet da se dozvoljava maksimalno jedan krivo preneseni bit u ukupnoj poruci duljine 7. Dakle, umjesto binarne poruke $m = m_1m_2m_3m_4$, prenosimo binarnu poruku $M = c_1c_2m_1c_3m_2m_3m_4$. Pritom se svaki od triju kontrolnih bitova c_i postavlja na vrijednost 0 ili 1 tako da je nim-zbroj od c_i i triju bitova poruke koje kontrolira jednak 0:

$$c_1 = m_1 \oplus m_2 \oplus m_4,$$

$$c_2 = m_1 \oplus m_3 \oplus m_4,$$

$$c_3 = m_1 \oplus m_2 \oplus m_3.$$

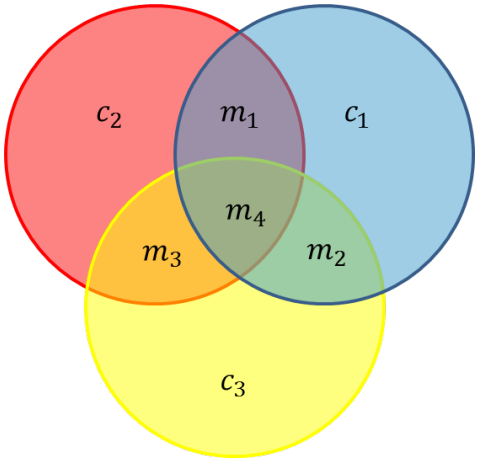
Princip kodiranja se može ilustrirati i Vennovim dijagramom (slika 3.6), iz kojeg se lako očita koji od kontrolnih bitova provjerava koje bitove izvorne poruke.

Primjer 3.2.1. *Kodirat ćemo poruku* 1011 *koristeći Hammingov* $(7, 4)$ *kod.*

pozicija	1	2	3	4	5	6	7
znak	c_1	c_2	1	c_3	0	1	1

.

[1] Uočimo, kako su svih 2^n mogućih nizova jednako vjerojatni, greška ili laž na ikojoj od n pozicija ne može se detektirati bez dodatne informacije.



Slika 3.6: Princip Hammingovog $(7, 4)$-koda.

Budući da c_1 služi za provjeru pariteta na 3., 5. *i* 7., *zaključujemo da je* $c_1 = 1 \oplus 0 \oplus 1 = 0$, *analogno je* $c_2 = 1 \oplus 1 \oplus 1 = 1$ *te* $c_3 = 0 \oplus 1 \oplus 1 = 0$. *Kodirana poruka* 1011 *glasi* 0110011.

Formalnije, postupak kodiranja može se opisati množenjem matrica. Poruka koju kodiramo predstavlja se matricom-stupcem $m^T \in M_{4,1}$. Kodiranje se postiže tako da m^T slijeva pomnožimo matricom

$$E = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Dakle, poruka koja se prenosi bit će sadržana u matrici $M^T = Em^T$.

Primjer 3.2.2. *Kodirat ćemo poruku* $m = 1011$ *množenjem matrica:*

$$Em^T = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \end{pmatrix}$$

Uočimo da smo poruku m kodirali porukom 0110011 *kao u primjeru 3.2.1.*

No, kao i u opisanom triku u kojem izvođač treba otkriti zamišljeni broj, od kodiranja je općenito zanimljivije dekodiranje poruke. Kako otkriti koja od $2^4 = 16$ poruka je „prava", ako znamo da je na najviše jednoj od 7 pozicija „krivi" bit?

Prvo, uočimo da iako prenosimo 7 bitova, imamo samo $16 = 2^4$, a ne $128 = 2^7$, mogućih ispravno prenesenih kodiranih poruka. Ako bismo za svaku od 16 mogućih poruka m odredili odgovarajuću kodiranu poruku M, dobili bismo tablicu iz koje je lako vidjeti koje su poruke M moguće, dakle je li pri prijenosu poruke došlo do greške. Za naš trik to nije bitno, jer znamo (to je bio zahtjev) da će jedna informacija (jedan bit) biti krivi. Dekodiranje je najlakše opisati temeljem dijagrama sa slike 3.6. U dijagram se unesu vrijednosti bitova u skladu s dosadašnjim oznakama te se u svakom krugu nim-zbroje sva četiri bita koji su u njemu. Ukoliko su sve tri nim-sume 0, poruka je prenesena bez greške. Ukoliko je samo jedna od nim-suma 1, onda je greška u odgovarajućem kontrolnom bitu. Ukoliko su dvije nim-sume jednake 1, greška je u bitu izvorne poruke koji odgovara presjeku krugova u kojima je nim-suma bila 1. Ako su sve tri nim-sume 1, greška je u presjeku svih triju krugova, dakle u zadnjem bitu izvorne poruke.

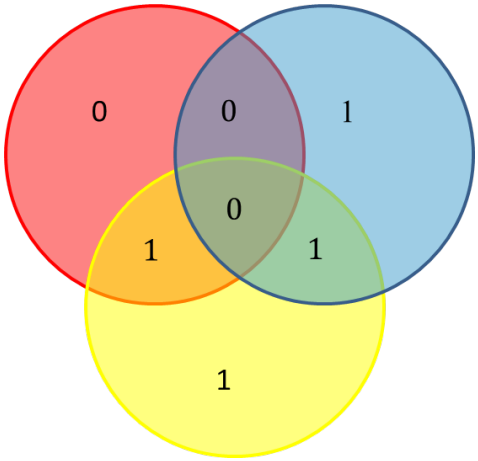
Primjer 3.2.3. *Recimo da ste primili poruku* $M = 1001110$*. Ako nije bilo greške, izvorna je poruka ono što preostaje križanjem kontrolnih bitova koji su na pozicijama* 1*,* 2 *i* 4 *od M, dakle ako nema greške, izvorna bi poruka bila* $m = 0110$*.*

Unesimo sve bitove od M u odgovarajuće dijelove dijagrama sa slike 3.6. Dobit ćemo dijagram poput slike 3.7. Nim-zbrojimo bitove koji se nalaze u svakom od triju krugova pojedinačno: u plavom ćemo dobiti 0*, u crvenom* 1 *i u žutom* 1*. Od zanimanja su krugovi u kojima nim-zbroj nije* 0*, dakle ovdje crveni i žuti krug. U njihovom presjeku se nalazi krivo preneseni bit, dakle ovdje je to* m_3 *(treći bit „izvorne" poruke), koja je stoga umjesto* 0110 *glasila* 0100*.*

Formalni način dekodiranja opet se svodi na množenje matrica: primljena poruka M^T množi se slijeva matricom

$$P = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Dobivena matrica $c^T = PM^T$ sadrži tzv. paritetne bitove (nim-sume iz prethodnog opisa), tj. iz nje se može iščitati je li ikoji bit krivo prenesen i, ako jest, koji. Ako je c^T nulmatrica, poruka M je ispravno prenesena i iz nje samo treba pobrisati kontrolne bitove. Ako c^T sadrži točno jednu jedinicu, krivo je prenesen jedan od kontrolnih bitova, što obično nije bitno, pa isto tako samo iz M pobrišemo kontrolne bitove da bismo dobili ispravnu osnovnu poruku. Ako su svi elementi od X jedinice, posljednji od četiri bita izvorne poruke treba



Slika 3.7: Dekodiranje poruke.

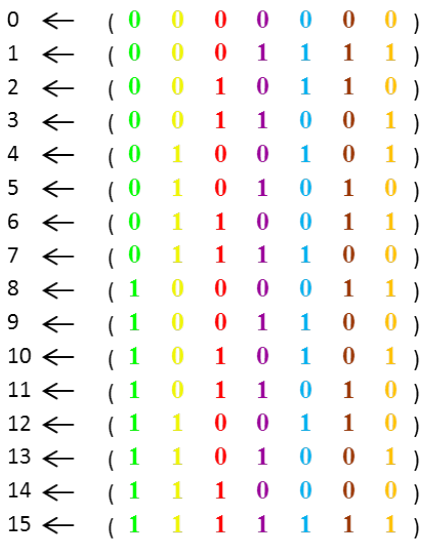
izmijeniti, a ako su dvije jedinice na pozicijama 1 i 2, 1 i 3 ili 2 i 3 onda treba izmijeniti prvi, drugi odnosno treći bit poruke. Za više detalja, čitatelja upućujemo na [5].

Za kraj, primijenimo opisano na trik s karticama. Uočimo da se radi o Hammingovom $(7, 4)$-kodu jer iz prvih četiriju kartica možemo otkriti o kojem se zamišljenom broju radi ako je sudionik trika iskreno odgovorio na pitanje za svaku od te četiri kartice, a posljednje tri kartice su kontrolne za slučaj da je sudionik ponudio lažan odgovor za jednu karticu što je u ovom triku i bio uvjet. Pritom ovom slučaju (u kojem su kontrolni bitovi na kraju poruke) odgovara matrica kodiranja

$$E' = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix}.$$

Množenjem sa svim mogućim porukama od 0 = 0000 do 15 = 1111 vidimo da su moguće kodirane i ispravno prenesene poruke prikazane slikom 3.8 Umjesto da dekodiramo na jedan od dva prije opisana načina, u ovom triku primljenu poruku dekodiramo traženjem najmanje Hammingove udaljenosti [2] između primljene poruke i svih mogućih ispravno prenesenih. Ako je primjerice sudionik trika zamislio broj 13 i zelenu boju, onda će pri

[2]Hammingova udaljenost između dva binarna niza jednake duljine je broj pozicija na kojima se ti nizovi razlikuju



Slika 3.8: 16 kodiranih nizova $(7, 4)$ Hammingovog koda

davanju odgovora lagati za prvu karticu te će niz njegovih odgovora interpretiran kao binarni niz biti $y = 0101001$. Određivanjem Hammingovih udaljenosti između M i svakog od nizova na slici 3.8, uočavamo da je najmanja Hammingova distanca jednaka 1 i to za niz 1101001. Vidimo da se ti nizovi razlikuju samo na prvoj poziciji pa promjenom prve znamenke niza M dobivamo niz 1101001, čije prve četiri znamenke predstavljaju broj 13 zapisan u binarnom brojevnom sustavu, a budući da se radilo o razlici u prvoj znamenci, znači da je zamišljena bila boja prve karte, tj. zelena boja.

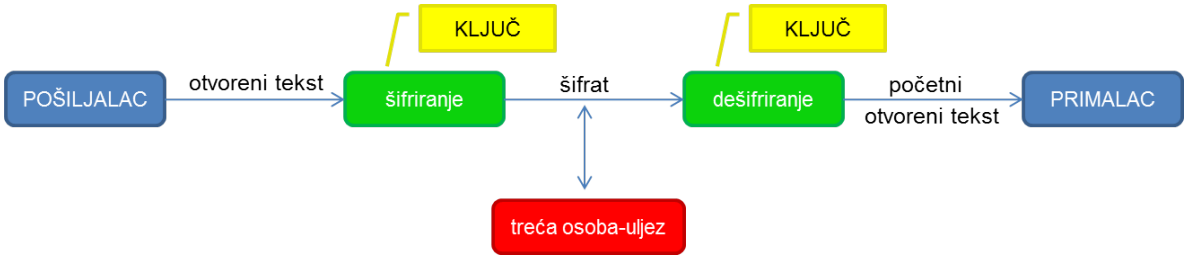
Poglavlje 4

Sheme praga u kriptografiji

U ovom poglavlju prikazat ćemo kako se u kriptografiji koriste binarni zapisi. Kao i u prethodnom poglavlju, krećemo od konkretnog primjera. Prije toga, recimo ukratko nešto o kriptografiji.

4.1 Kriptografija

Ubrzan razvoj informatičke tehnologije omogućava razmjenu velikih količina podataka, a samim time povećan je i rizik od neovlaštenog pristupa podatcima tijekom razmjene. Kako bi se zaštitili podatci tijekom razmjene, potrebno ih je poslati u šifriranom obliku koji će biti razumljiv samo primatelju, a neovlaštenim sudionicima u razmjeni takav oblik neće otkriti nikakve informacije o podatcima koji se šalju. U takvom procesu razmjene podataka važnu ulogu ima kriptografija. Kriptografija je znanstvena disciplina koja se bavi proučavanjem metoda za slanje poruka u obliku takvom da ih samo onaj kome su namijenjene može pročitati. Podatak kojeg pošiljalac šalje primatelju nazivamo otvorenim tekstom. Kako bi se zaštitio podatak tijekom razmjene, pošiljatelj otvoreni tekst šifrira, koristeći unaprijed dogovoreni ključ, u šifrat. Tako dobiveni šifrat je dostupan primatelju, ali i nekoj trećoj osobi, koja, na primjer, nadzire komunikacijski kanal (telefonsku liniju, računalnu mrežu i sl.), no toj osobi šifrat ništa ne govori o otvorenom tekstu za razliku od primatelja poruke koji poznaje ključ te uz pomoć ključa dešifrira šifrat u početni otvoreni tekst (Slika 4.1). Poseban slučaj šifriranja su sheme praga, u kojima ključ ne postoji u klasičnom smislu, ali je potrebno objedinjavanje više dijelova šifrata kako bi se dešifrirala poruka.



Slika 4.1: Proces slanja poruke

4.2 Osnovno o shemama praga

Razmotrimo sad jedan primjer u kojem su sheme praga prikladan način kriptiranja informacije. Za otvaranje trezora u banci potrebno je unijeti odgovarajuću zaporku. Ako je u banci zaposleno šest osoba, zbog sigurnosnih razloga, niti jedan zaposlenik ne dobiva cjelovitu zaporku za otvaranje trezora, već svaki zaposlenik dobiva svoju kombinaciju te je trezor moguće otvoriti samo ako bilo koja tri zaposlenika zajedno unesu kombinaciju koju posjeduju. Dakle, nije dobro da svaki zaposlenik dobije jednu znamenku zaporke jer time zna dio zaporke, što mu može pomoći u dekriptiranju. Prikladan način zaštite provodi se uz pomoć sheme praga.

Definicija 4.2.1. *(t,n)-shema praga je metoda razlaganja tajne na n sudionika tako da bilo koja skupina od t sudionika može otkriti tajnu, ali niti jedna skupina od $t-1$ (ili manje) sudionika ne može otkriti tu tajnu, kao ni bilo kakvu djelomičnu informaciju o njoj.*

Kao primjer (n,n)-sheme praga nam može poslužiti niz binarnih znamenki. Dakle, tajna je niz k binarnih znamenki duljine m koja se razlaže na n dijelova tako da samo svi zajedno omogućavaju otkrivanje početnog niza. Osoba koja razlaže tajni binarni niz na n dijelova, generira $n-1$ slučajnih nizova binarnih brojeva iste duljine m te ih dodjeljuje $n-1$ sudioniku, dok posljednji sudionik dobiva niz nastao tako da se prethodnih $n-1$ nizova nim zbroje s tajnim nizom. Kako su svi osim jednog niza slučajni, a zadnji zbroj slučajnih, očito nijedan sudionik, kao i nikoja 2, 3, ... nemaju nikakvu informaciju o početnom nizu.

Ukoliko su svih n sudionika zajedno prisutni, jednostavna posljedica definicije nim-zbroja je da nim-zbrajanjem svojih nizova mogu rekonstruirati izvorni niz.

Primjer 4.2.2. *Neka su dani nizovi $k_1 = 100101$, $k_2 = 001100$ i $k_3 = 110011$. Nim-zbroj tih nizova je:*

$$\begin{array}{rr} & 100101 \\ & 001100 \\ \oplus & 110011 \\ \hline & 011010 \end{array}$$

Dakle, da se radilo o $(3,3)$*-shemi praga, tajni niz bi bio* $k = 011010$*.*

Zašto ova metoda funkcionira? Prema definiciji nim-zbroja, očito je nim-zbroj isto što i nim-razlika dvaju brojeva. Stoga je zadnji dio dobiven kao $a_n = a_1 \oplus a_2 \oplus \cdots \oplus a_{n-1} \oplus b$, onda je izvorni niz $b = a_1 \oplus \cdots \oplus a_n$.

4.3 Sheme praga u vizualnoj kriptografiji

Tajna, tj. poruka koju prenosimo, može biti bilo kojeg oblika pa tako, na primjer, tajna može biti slika u boji ili crno-bijela rasterska slika. Ovdje ćemo opisati proces kriptiranja crno-bijele slike, dok o metodama prijenosa slika u boji možete pročitati u članku D. Stinsona [11]. Budući da je tajna koju šifriramo slika i da se dešifriranje ne provodi računski, nego se provodi ljudskim osjetilom vida, ova grana kriptografije naziva se vizualnom kriptografijom.

Definicija 4.3.1. *Vizualna (t,n)-shema praga je metoda kojom se tajna slika razlaže na n folija tako da se svaka folija sastoji od crnih i bijelih piksela te se tajna slika dešifrira preklapanjem barem t folija. Preklapanjem bilo kojih* $t-1$ *(ili manje) folija ne otkrivamo tajnu sliku.*

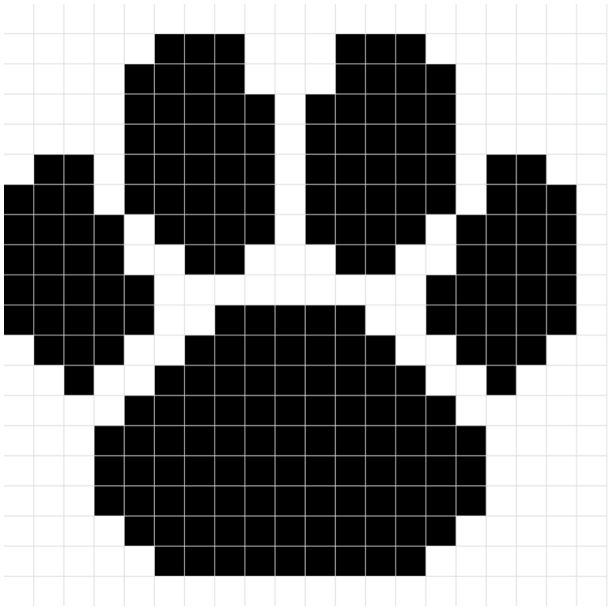
Iz praktičnih razloga, piksele koji bi trebali biti bijeli, na folijama ostavljamo prozirnima.

Vizualna (2,2)-shema praga

Šifriranje vizualnom shemom praga se odvija tako da šifriramo svaki piksel posebno. Pokažimo primjer vizualne (2,2)-sheme praga. Koristeći ovu metodu, početnu sliku (Slika 4.2) razlažemo na dvije folije čijim ćemo preklapanjem dobiti početnu sliku. Osnovna je ideja ove metode svaki piksel izvorne slike razložiti na dva piksela, koji se popunjavaju crnom ili bijelom bojom po određenom pravilu.

Pri razlaganju slike na dvije folije vizualnom (2,2)-shemom praga, na svaki piksel početne slike primijenjujemo algoritam ilustriran slikom 4.3.

Ako je piksel kojeg šifriramo crn, tada slučajnim odabirom (npr. bacanjem novčića) biramo jedan od prva dva retka na slici 4.3 te, sukladno odabranom retku, na svakoj foliji obojimo podpiksele odgovarajućim bojama. Ako je piksel kojeg šifriramo piksel koji je na



Slika 4.2: Crno-bijela rasterska slika

početnoj slici bijel, tada slučajnim odabirom biramo jedan od posljednja dva retka na slici 4.3.

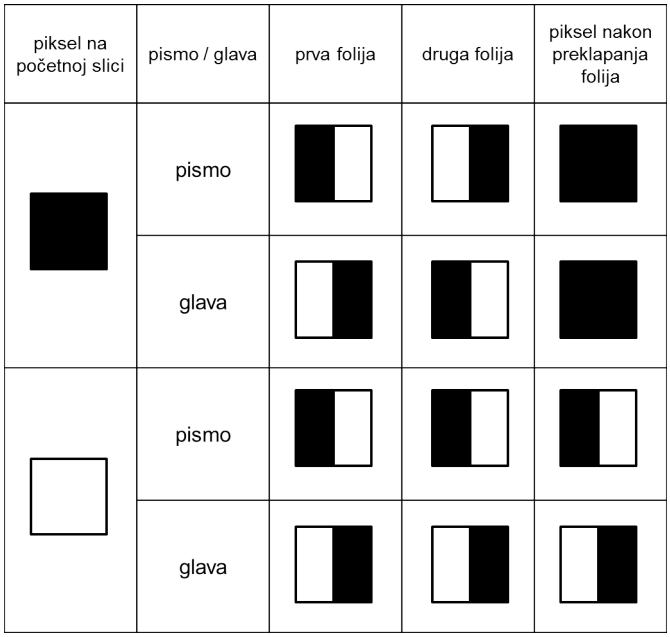
Ako na sliku 4.2 primijenimo opisani algoritam, rezultat može (ali zbog elementa slučajnosti ne mora) izgledati kako je prikazano slikama 4.4 i 4.5.

Svim pikselima na obje folije je jedna polovica zacrnjena, a druga polovica je bijela pa promatranje svake folije zasebno nam ništa ne govori o početnoj slici jer je odabir poretka crnog i bijelog podpiksela u svakom pikselu jednako vjerojatan bez obzira je li izvorni piksel bio bijel ili crn. Dešifriranje vizualnom (2,2)-shemom praga je određeno posljednjim stupcem na slici 4.3, a početnu sliku dobijemo preklapanjem folija (Slika 4.6). Uočimo da, ako je piksel na početnoj slici bio crn, on će i nakon preklapanja također biti crn, no ako je početni piksel bio bijel, nakon preklapanja će se sastojati od bijelog i crnog podpiksela te se time na dešifriranoj slici gubi 50 % kontrasta.

Vizualna (2,n)-shema praga

Već pri preklapanju dviju folija nailazimo na problem preciznog preklapanja pa iz praktičnih razloga[1] nećemo razmatrati slučajeve podjele na više folija te ćemo se ograničiti na raz-

[1]Obzirom da se u praksi preklapanje provodi putem računala, ovo zapravo nije prava smetnja. O općim shemama praga pročitajte u [6]



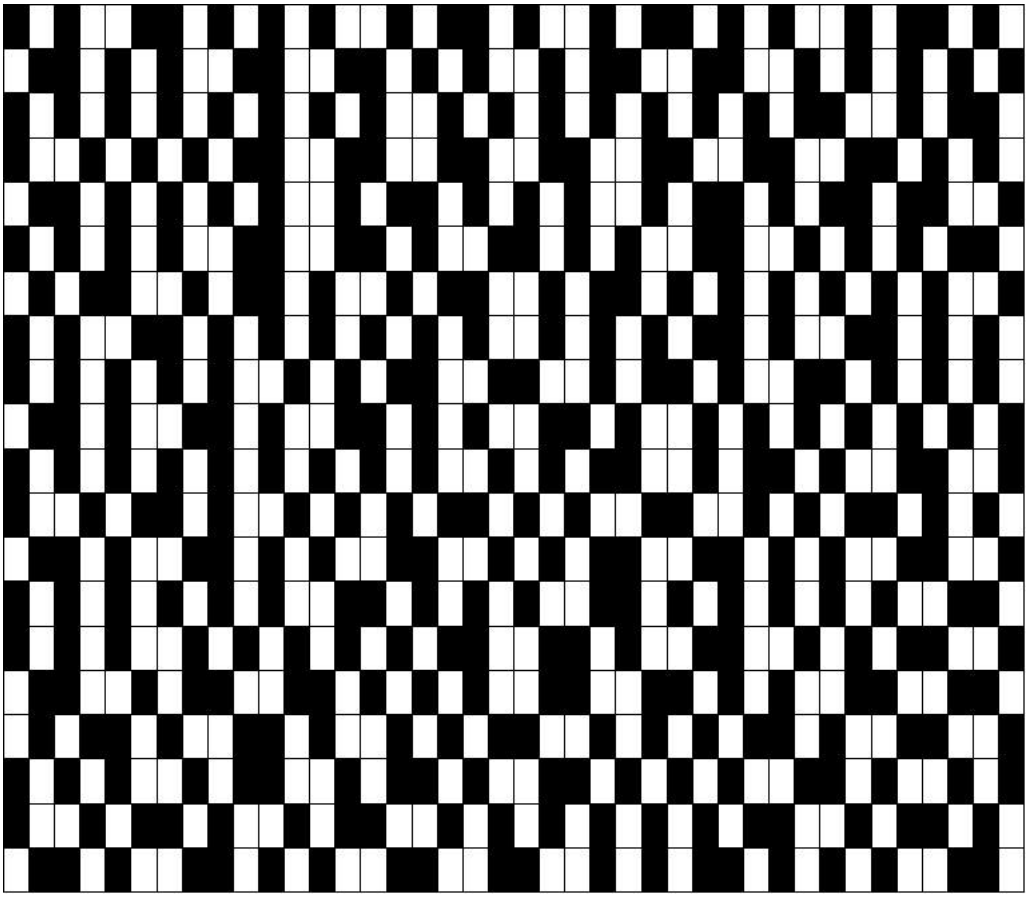
Slika 4.3: Vizualna (2,2)-shema praga

matranje vizualne (2,n)-sheme praga. Svaki piksel na folijama podijeljen je na m podpiksela. Broj m nazivamo ekspanzijom piksela te je za, prethodno opisanu (2,2)-shemu praga, $m = 2$. Označimo li bijele piksele i podpiksele s 0, a crne s 1, tada ćemo svaki piksel, sastavljen od m podpiksela, moći nakon šifriranja prikazati kao m-torku binarnih brojeva. Svaki piksel početne slike šifrirat ćemo koristeći matricu M_1 za šifriranje crnih piksela te matricu M_0 za bijele piksele. Matrice M_0 i M_1 su binarne matrice s n redaka i m stupaca. Matrica M_0 u svakom retku ima w uzastopnih 1 i nakon toga $m - w$ uzastopnih 0, tj. prvih w stupaca matrice sadrže samo 1, dok preostalih $m - w$ sadrže 0. Prirodan broj w, za koji vrijedi $1 \leqslant w \leqslant m$, označava koliko je 1 u svakom retku obiju matrica. Realan broj γ takav da $0 \leq \gamma \leq 1$, opisuje relativni kontrast na dešifriranoj slici nastaloj preklapanjem folija. Nim zbrajanjem bilo koja dva retka matrice M_1 dobivamo niz u kojem se broj 1 pojavi barem $w + \gamma n$ puta.

Primjer 4.3.2. *Za navedenu (2,2)-shemu praga vrijedi:* $m = 2$, $w = 1$, $\gamma = \frac{1}{2}$ *te su matrice oblika:*

$$M_0 = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}, \quad M_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Budući da je $\gamma = \frac{1}{2}$, *znači da je na dešifriranoj slici gubitak kontrasta u odnosu na početnu*



Slika 4.4: Primjer šifriranja Slike 4.2 na prvoj foliji

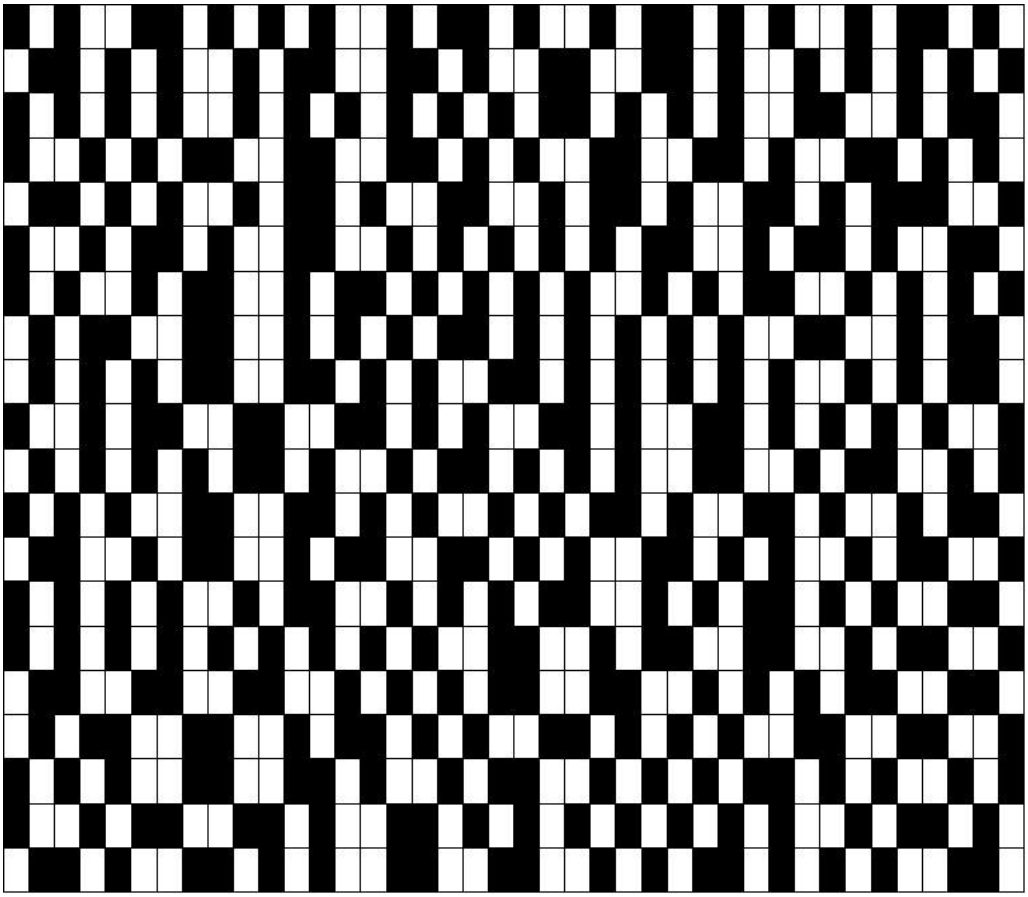
jednak 50%.

Primjer 4.3.3. $(3,4)$-*shema praga s ekspanzijom piksela* $m = 6$

$$M_0 = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 \end{pmatrix}, \; M_1 = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}.$$

Koristeći matrice M_0 i M_1 šifriramo svaki piksel $P \in \{1, 0\}$ početne slike tako da:

1. slučajnim odabirom izaberemo jednu permutaciju σ skupa $\{1, \ldots, m\}$;
2. konstruiramo matricu N_p permutiranjem stupaca od M_p pomoću σ;



Slika 4.5: Primjer šifriranja Slike 4.2 na drugoj foliji

3. očitamo i-ti redak od N_p, što predstavlja poredak boja podpiksela od P na i-toj foliji, za $1 \leq i \leq w$.

Pokažimo opisani postupak na primjeru:

Primjer 4.3.4. $(2, 3)$*-shema praga s ekspanzijom piksela* $m = 3$ *određena je matricama*

$$M_0 = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \; M_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Budući da je $m = 3$*, postoji* $3! = 6$ *mogućih permutacija skupa* $\{1, 2, 3\}$*, tj. permutacija stupaca i to su:* $\sigma_1 = (1, 2, 3)$*,* $\sigma_2 = (1, 3, 2)$*,* $\sigma_3 = (2, 1, 3)$*,* $\sigma_4 = (2, 3, 1)$*,* $\sigma_5 = (3, 1, 2)$



Slika 4.6: Slika 4.2 nakon dešifriranja preklapanjem folija

i $\sigma_6 = (3, 2, 1)$. *Da bismo proveli prvi korak, možemo iskoristiti kockicu s brojevima od* 1 *do* 6 *na svakoj strani za slučajan odabir permutacije. Želimo li šifrirati neki crni piksel* $P = 1$ *i bacanjem kockice dobijemo* 2*, onda je* $\sigma = \sigma_2 = (1, 3, 2)$ *te konstruiramo matricu* N_1 *tako da matrici* M_1 *zamijenimo drugi i treći stupac:*

$$N_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

Iz redaka matrice N_1 *očitamo poredak boja podpiksela na folijama za šifrirani piksel P (Slika* 4.7*).*

U Primjeru 4.3.3 je $m = 6$, $w = 3$, $\gamma = \frac{1}{3}$, a u Primjeru 4.3.4 $m = 3$, $w = 3$, $\gamma = \frac{1}{3}$.

Uočavamo da je za postizanje jednakog kontrasta pri većem broju folija, potrebna veća ekspanzija piksela. Najjači kontrast koji se može postići u opisanoj $(2, n)$-shemi je (prema [11]):

$$\gamma^*(n) = \frac{\left\lfloor \frac{n}{2} \right\rfloor \cdot \left\lceil \frac{n}{2} \right\rceil}{n(n-1)}.$$

Uočimo da je $\gamma^*(n) > \frac{1}{4}$ za svaki $n \geq 2$ te da je $\lim_{n\to\infty} \gamma^*(n) = \frac{1}{4}$. Dakle, najveći gubitak kontrasta je 75% pa bi slika trebala biti vidljiva za relativno jednostavne slike. Pri prijenosu slike, na dešifriranoj slici želimo što veći kontrast (kako bi slika bila što jasnija) te što manju ekspanziju piksela m (zbog tehničkih razloga, tj. što je više podpiksela teže je precizno preklopiti folije).



Slika 4.7: Šifrirani piksel za Primjer 4.3.4

Pogledajmo još jedan primjer kako konstruirati vizualnu $(2, n)$-shemu praga s optimalnim relativnim kontrastom $\gamma^*(n)$ i minimalnom ekspanzijom $m = n$. Pretpostavimo da je $n \equiv 3(mod 4)$ prost te definirajmo $Q(n) = \left\{ i^2 \mod n : 1 \leq i \leq \frac{n-1}{2} \right\}$, skup kvadratnih ostataka modulo n. Nadalje, konstruiramo matricu M_1 dimenzije $n \times n$ pri čemu numeriramo retke i stupce cijelim brojevima iz skupa $\{0, \ldots, n-1\}$. Na poziciji (i, j) matrice M_1 nalazi se 1 ako je $(j - i) \mod n \in Q(n)$, inače na mjestu (i, j) pišemo 0.

Primjer 4.3.5. *Neka je* $n = 11$. *Odredimo elemente skupa* $Q(11)$*:* $1^2 = 1 \equiv 1 \mod 11$, $2^2 = 4 \equiv 4 \mod 11$, $3^2 = 9 \equiv 9 \mod 11$, $4^2 = 16 \equiv 5 \mod 11$ *i* $5^2 = 25 \equiv 3 \mod 11$,

dakle, $Q(11) = \{1, 4, 9, 5, 3\}$ *te možemo odrediti matricu* M_1 *tako da za svaku poziciju* (i, j) *provjerimo vrijedi li* $(j - i) \mod 11 \in Q(11)$*, ako vrijedi, onda na to mjesto zapisujemo* 1*, inače zapisujemo* 0*.*

Uočimo da svaki redak u matrici sadrži pet 1*, tj.* $w = 5$ *i nim zbroj bilo koja dva retka matrice je* 8*. Dakle, konstruirali smo* $(2, 11)$*-shemu s* $m = 11$*,* $w = 5$ *i* $\gamma = \gamma^*(11) = \frac{3}{11}$.

Općenito, ako je $n \equiv 3 mod 4$ prost onda će ovaj postupak rezultirati $(2, n)$-shemom s $m = n$, $w = \frac{n-1}{2}$ i $\gamma = \frac{n+1}{4n}$.

Poglavlje 5

Zaključne napomene

Većina tema navedenih u radu primjenjiva je u nastavi matematike i informatike u osnovnoj i srednjoj školi kao motivacija ili kao oblik vježbe jer se već u petom razredu osnovne škole učenici susreću s pojmom binarnog brojevnog sustava. Tijekom petog razreda učenici savladavaju ispisivanje svih mogućih stanja za nizove od 2, 3 i 4 bita te se upoznaju s težinskom vrijednošću bitova u takvim nizovima pa samim time i otkrivaju binarni zapis broja kao i binarne znamenke. Također, upoznaju se s jednostavnijim oblikom kodiranja teksta u niz bitova koristeći ASCII tablicu. U programu za prvi razred gimnazije, predviđeno je da učenici proširuju znanje pretvaranja zapisa prirodnih brojeva iz binarnog brojevnog sustava u dekadski i obrnuto uz obuhvaćanje pretvorbe zapisa decimalnih brojeva. Također, učenici se upoznaju sa zbrajanjem i množenjem prirodnih brojeva u binarnom brojevnom sustavu. Tijekom upoznavanja s prikazom brojeva i znakova u računalu u nastavi informatike, učenici savladavaju prikazivanje cijelih i realnih brojeva u binarnom brojevnom sustavu.

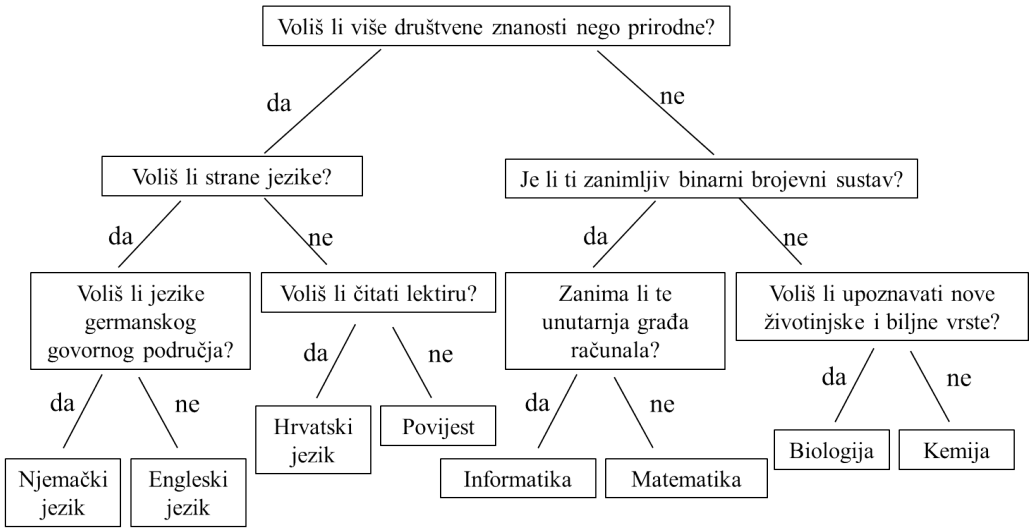
U radu nije spomenuta logička algebra ili Booleova algebra[1], koja čini osnove posebne grane matematike za istraživanje složenih sudova, tzv. matematičke logike, no Booleova algebra je, također, primjer u kojem se pojavljuje binarna matematika jer se provode logičke operacije s logičkim sudovima [2] prikazanim uz pomoć binarnih znamenki (istinitost se zapisuje kao znamenka 1, a laž kao 0). S osnovnim logičkim operacijama (negacija, konjukcija, disjunkcija, složeni) te teoremima Booleove algebre, učenici se upoznaju u prvom razredu gimnazije i to s ciljem otkrivanja izrade raznih logičkih sklopova koji se nalaze u procesoru računala, točnije u aritmetičko-logičkoj jedinici gdje se obavljaju npr. aktivnosti zbrajanja dva broja.

Još jedan zanimljiv primjer primjene binarne matematike je korištenje tzv. binarnog

[1] George Boole (1815.-1864), engleski matematičar i logičar, u svojim je djelima prvi uveo matematičku simboliku za istraživanje logičkih promišljanja

[2] Logički sud je svaka tvrdnja za koju se može reći je li istinita ili lažna

stabla. Binarno stablo je konačan skup elemenata, zvanih čvorovi, takav da za svaki čvor stabla postoje dva podstabla kojima je taj čvor korijenski čvor. Binarna stabla se koriste pri rješavanju zagonetke poznate pod imenom Hanojski tornjevi. Zagonetka se sastoji od 3 tornja, na jednom se nalazi n diskova, poredanih po veličini (na dnu je najveći, a na vrhu najmanji). Cilj je prebaciti sve diskove na neki od preostalih tornjeva, tako da oni zadrže originalni poredak uz pravilo da se prebacuje jedan po jedan disk i da se ne smije staviti veći disk na manji (kako se binarno stablo pojavljuje u rješenju Hanojskih tornjeva možete pročitati u [1]). Vrlo poznata i zanimljiva primjena binarnog stabla je primjena pri postupku donošenja odluke pa se takvo stablo naziva stablo odlučivanja. U stablu odlučivanja čvorovi sadrže pitanja na koja se odgovara s da ili ne, a listovi odluke. Kretanje po stablu započinje u korijenu te se nastavlja odgovaranjem na pitanja i biranjem smjera kretanja ovisno o odgovorima. Dolaskom do lista, završava kretanje i u njemu piše odluka koju trebamo donijeti. Na slici 5.1 prikazan je primjer stabla odlučivanja kojim se otkriva najdraži nastavni predmet u školi.



Slika 5.1: Stablo odlučivanja za odabir najdražeg nastavnog predmeta u školi

Bibliografija

[1] I. Anđelić, *Hanojski tornjevi*, dostupno na: http://mapmf.pmfst.unist.hr/~ani/radovi/zavrsni/Ivan%20An%C4%91eli%C4%87_zavrsni.pdf (listopad 2016.)

[2] A. Beck, M. N. Bleicher, D. W. Crowe, *Magical Mathematics: The Mathematical Ideas That Animate Great Magic Tricks*, A K Peters, 2000.

[3] A. Buljubašić, *Teorija kodiranja i linearni kodovi*, dostupno na: www.mathos.unios.hr/~mdjumic/uploads/diplomski/BUL10.pdf (rujan 2016.)

[4] P. Diaconis, R. Graham, *Excursions into Mathematics*, Princeton University Press, New Jersey, 2011.

[5] K. H. Rosen, *Coding Theory*, dostupno na: http://www.mhhe.com/math/advmath/rosen/r5/instructor/applications/ch05.pdf (svibanj 2016.)

[6] S. Chandramathi, R. Ramesh Kumar, R. Suresh, S. Harish, *An overview of visual cryptography*, International Journal of Computational Intelligence Techniques 1, 32-37, 2010.

[7] D. Veljan, *Kombinatorna i diskretna matematika*, Algoritam, Zagreb, 2001.

[8] F. M. Brückler,*Kako sakriti sliku?*, dostupno na: www.mathos.unios.hr/~middlemath/ppt/vizualna-kriptografija.pdf (srpanj 2016.)

[9] A. M. Goyt, *The Magic of De Bruijn Sequences*, dostupno na: http://web.mnstate.edu/goytadam/talks/DBS.pdf (listopad 2016.)

[10] T.Matter,*A Magic Trick Based on the Hamming Code*, dostupno na: http://www.northeastern.edu/ (rujan 2016.)

[11] D. Stinson, *Visual cryptography*, dostupno na:
http://www.cs.jhu.edu/~fabian/courses/CS600.624/stinson.pdf (lipanj 2016.)

[12] *Livescribe*, dostupno na:
http://www.livescribe.com (rujan 2016.)

Sažetak

U ovom radu opisuje se primjena binarne matematike u različitim područjima te se neki primjeri mogu iskoristiti u popularizaciji matematike, kao i u nastavi matematike i informatike.

Rad je podijeljen na četiri cjeline. Svaka cjelina počinje opisom konkretnog primjera uz pomoć kojeg se u nastavku opisuje tema cjeline. Prva cjelina opisuje neke jednostavne matematičke igre i trikove temeljene na binarnoj aritmetici. U ostatku rada su obuhvaćeni de Bruijnovi nizovi (jednodimenzionalni i dvodimenzionalni), kodovi za otkrivanje i ispravljanje pogrešaka (Hammingovi kodovi) te vizualne sheme praga koje se koriste u kriptografiji za zaštitu prijenosa fotografija.

Summary

In this thesis, the application of binary arithmetic in various fields is described. Therefore, some examples can be used for popularisation of mathematics, as well as in teaching mathematics and computer science.

The thesis is divided in to 4 parts. Each part begins with a description of a certain example which is then used to further describe the part's topic. First, some simple mathematical tricks and games based on binary arithmetic are described. The other topics covered are de Bruijn sequences (both one-dimensional and two-dimensional), error-correcting codes (Hamming codes) and visual threshold schemes that are used in cryptography in order to protect images during transmission.

Životopis

Jaruška Stjepanek rođena je 13. 1. 1993. godine u Zagrebu. Osnovnu školu pohađala je u Međuriću i Banovoj Jaruzi, a 2007. godine upisuje prirodoslovno-matematičku gimnaziju u Srednjoj školi Tina Ujevića u Kutini. Godine 2011. upisala je nastavnički smjer preddiplomskog sveučilišnog studija na Matematičkom odsjeku Prirodoslovno-matematičkog fakulteta u Zagrebu. Akademski naziv sveučilišnog prvostupnika stječe 2014. godine te iste godine upisuje nastavnički smjer diplomskog sveučilišnog studija Matematičkog odsjeka u Zagrebu.