UNIVERZITET U BEOGRADU

MATEMATIČKI FAKULTET — BEOGRAD

Miodrag V. Živković

PRILOG ANALIZI LINEARNIH REKURENTNIH NIZOVA U POLJU GF(2)

Doktorska disertacija

BEOGRAD
1990

Mentor: **Žarko Mijajlović**
Univerzitet u Beogradu
Beograd

Članovi komisije: **Zoran Ivković**
Univerzitet u Beogradu
Beograd

Dragan Banjević
Univerzitet u Beogradu
Beograd

Datum odbrane

Datum promocije

Doktorat nauka

PRILOG ANALIZI LINEARNIH REKURENTNIH NIZOVA U POLJU GF(2)

Apstrakt

Analiziran je problem određivanja linearnog rekurentnog niza elemenata polja GF(2) kad je poznat jedan njegov odsečak u kome su neki članovi promenjeni dejstvom slučajnih nezavisnih jednako verovatnih grešaka. Problem je vrlo sličan složenom problemu dekodiranja linearnih kodova, koji je široko razmatran u literaturi a ima odredjeni značaj u kriptologiji. Polazeći od dva poznata efikasna algoritma za njegovo rešavanje, probabilističkog i algoritama zasnovanog na korišćenju informacionih skupova, u disertaciji je predložen novi algoritam za rešavanje ovog problema, nastao njihovim objedinjavanjem, razradom i usavršavanjem. Prvi od tih algoritama je probabilistički, a drugi je sličan algoritmima dekodiranja pomoću informacionih skupova. Data je analiza pojedinih elemenata probabilističke faze algoritma. Predložen je efikasan postupak za formiranje (poznatih) sistema kontrola parnosti za probabilističku fazu, kao i heuristički algoritam za formiranje pogodnih podskupova ovih sistema. Dokazano da su korišćeni sistemi kontrola parnosti linearno nezavisni ako je karakteristični polinom linearne rekurentne relacije nesvodljiv. Dati su postupci za efikasnije i tačnije izračunavanje aposteriornih verovatnoća grešaka, koji se mogu primeniti kad sistemi kontrola parnosti nisu ortogonalni. Polazeći od uopštenja nejednakosti Salivena formulisan je dovoljan uslov za konvergenciju niza vektora verovatnoća u probabilističkoj fazi algoritma. Opisan je postupak za eksperimentalno ocenjivanje verovatnoće da je ispunjen taj dovoljan uslov. Novi algoritam upoređen je sa polaznim algoritmima u jednom specijalnom slučaju.

Ključne reči

linearni rekurentni niz, pomerački registar, linearni kod, dekodiranje

AN ANALISYS OF LINEAR RECURRENT SEQUENCES OVER THE FIELD GF(2)

Abstract

The problem of determining the linear recurrent sequence over the field GF(2) starting from its part in which some members are changed by random independent equiprobable errors is considered. The problem is similar to the complex problem of decoding linear codes, which is widely considered in literature. It has some importance for cryptology. New algorithm for the solution of this problem is proposed, obtained by cupling, developing and improoving the two known efficient algorithms. One of them is probabilistic, and the second is information set decoding method. Some parts of the probabilistic phase of the algorithm are analized. An efficient method for the construction of the (known) parity check sets is proposed, and also a heuristical algorithm for finding appropriate subsets of these sets. It is prooved that these parity check sets are linearly independent if the characteristic polynomial of the linear recurrent relation is irreducible. The methods for efficient and precise calculation of the *a posteriori* probabilities of error are proposed, which are usefull when the parity check sets are not orthogonal. Starting from a generalization of the Sullivan's inequality a sufficient condition is given for the convergence of the probability vectors in the probabilistic phase. An experimental method is given for estimating the probability that the sufficient condition is satisfied. The algorithm is compared with the two known algorithms in a particular case.

Key words:

linear recurrent sequence, shift–register, linear code, decoding

Sadržaj

Spisak tabela

Spisak slika

Uvod

Linearni rekurentni nizovi elemenata polja GF(2), odnosno nizova koji se mogu dobiti pomoću pomeračkog registra sa linearnom povratnom spregom, razmatrani su u ovom radu iz jednog posebnog ugla. Analiziran je problem određivanja ovakvog niza kad je poznat jedan njegov odsečak u kome su neki članovi promenjeni dejstvom slučajnih nezavisnih jednako verovatnih grešaka. Ovaj problem je vrlo sličan složenom problemu dekodiranja linearnih kodova, koji je široko razmatran u literaturi. U radu [Meie89] istaknut je značaj ovog problema u kriptologiji, a data su i dva vrlo efikasna algoritma za njegovo rešavanje. Predmet disertacije je novi algoritam za rešavanje izloženog problema, nastao pogodnim objedinjavanjem, razradom i izvesnim usavršavanjem algoritama iz citiranog rada. Pored toga, data je analiza pojedinih elemenata probabilističke faze algoritma.

Rad se sastoji od pet poglavlja. U poglavlju 1 dat pregled osnovnih pojmova i stavova iz teorije kodova za ispravljanje grešaka (1.1), a zatim je dat osvrt na vezu između linearnih rekurentnih nizova u polju GF(2), izlaznih nizova iz pomeračkih registara sa linearnom povratnom spregom i odgovarajuće klase linearnih kodova (R–kodova). U tački 1.3 detaljno su prikazani rezultati rada [Meie89], s obzirom na njihov značaj. Radi se o Algoritmu A (sličnom algoritmima za dekodiranje linearnih kodova zasnovanim na korišćenju informacionih skupova) i Algoritmu B (probabilističkom algoritmu za dekodiranje koji ima određene sličnosti sa algoritmom iz rada [Gall62]. Pored toga dat je i osvrt na neke srodne algoritme za dekodiranje linearnih kodova.

Novi algoritam za dekodiranje R–kodova (kombinovani algoritam) izložen je ukratko u poglavlju 2. Prikazana je njegova veza sa algoritmima iz [Meie89]. Algoritam sa sastoji od određenog broja ciklusa

probabilističkog algoritma (Algoritma B, [Meie89]), pri čemu je u svaki ciklus na pogodan način ugrađen algoritam pretrage (Algoritam A iz istog rada, odnosno algoritam iz rada [LeeB88]).

U poglavlju 3, koje je najveće po obimu, analizirana je probabilistička faza kombinovanog algoritma. Predložen je efikasan postupak za formiranje sistema kontrola parnosti koji se koriste u Algoritmu B, kao i heuristički algoritam za formiranje pogodnih podskupova ovih sistema u slučaju kad je neprihvatljivo velika složenost rada se kompletnim sistemima kontrola parnosti. Pored toga, u tački 3.1 je dokazano da su korišćeni sistemi kontrola parnosti linearno nezavisni ako je karakteristični polinom linearne rekurentne relacije nesvodljiv. Problem efikasnosti i tačnosti izračunavanja aposteriornih verovatnoća greške (AVG, na kojima se zasniva probabilistička faza algoritma) razmatran je u tački 3.2. Dat je postupak za efikasnije izračunavanje AVG, koji se može primeniti kad sistemi kontrola parnosti nisu ortogonalni, ali matrice formirane od njih imaju grupe jednakih kolona. Pored toga prikazan je i postupak za tačnije izračunavanje AVG, kad su apriorne verovatnoće greške bliske nuli, odnosno jedinici. U tački 3.3 analizirana je verovatnoća pogrešne ocene bita greške na osnovu AVG (verovatnoća zaostale greške), a posebno njeno ponašanje kad je apriorna verovatnoća greške bliska jednoj polovini. Dokazano je da je i u opštem slučaju uslovno matematičko očekivanje AVG veće ako je odgovarajući bit primljene poruke pogrešan, nego ako je tačan. Dat je efikasan postupak za izračunavanje verovatnoće zaostale greške i verovatnoće da je AVG veća od 1/2, koji se može primeniti pod istim uslovima kao i navedeni postupak za izračunavanje AVG. Polazeći od uopštenja nejednakosti Salivena [Sull67] za odnos verovatnoća linearnog koda i njegovog proizvoljnog koseta u tački 3.4 je formulisan dovoljan uslov za konvergenciju niza vektora verovatnoća na kojima se zasniva Algoritam B (i kombinovani algoritam). Ukazano je na postupak za eksperimentalno ocenjivanje verovatnoće da je ispunjen taj dovoljan uslov. Analiza konvergencije jednog sličnog probabilističkog algoritma dekodiranja izvedena je i u radu [Gall62], ali ne dovoljno egzaktno, jer se odnosi na prosečnu verovatnoću greške.

U poglavlju 4 razmatrana je faza pretrage kombinovanog algoritma koja je ustvari algoritam dekodiranja korišćenjem slučajno izabranih informacionih skupova (videti na primer [Clar82, str. 102–131]. Postu-

pak formiranja slučajnih informacionih skupova opisan je u tački 4.1. Donošenje odluke da li je zadata kodna reč najbliža primljenoj poruci razmotreno je u tački 4.2 na osnovu [Sieg85]. Algoritam pretrage skupa kodnih reči koje se od primljene poruke na informacionom skupu razlikuju na ne više od zadatog broja mesta, sličan algoritmu iz [LeeB88], izložen je u tački 4.3. Pri tome je nešto detaljnije razmatrano određivanje optimalne dubine pretrage.

Rezultati sprovedenih eksperimenata sa kombinovanim algoritmom dati su u poglavlju 5. Ovaj algoritam je upoređen sa algoritmima iz rada [Meie89], a navedena su i neka zapažanja koja se odnose na dobijene rezultate.

Dobijeni rezultati proizašli su iz nastavka istraživanja koja je autor sproveo oko 1985. godine sa B. Mrđenovićem. Autor se zahvaljuje na podršci, korisnim primedbama i sugestijama Ž. Mijajloviću, J. Goliću i D. Jociću.

Poglavlje 1

Formulacija problema i pregled poznatih rezultata

U ovom poglavlju najpre će biti izloženi osnovni pojmovi o kodovima za ispravljanje grešaka (tačka 1.1) i kratak pregled osnovnih algoritama za dekodiranje linearnih kodova (tačka 1.3). Pojam R–kodova (linearnih kodova koji se mogu formirati pomoću pomeračkog registra sa linearnom povratnom spregom) i pregled poznatih algoritama za njihovo dekodiranje biće dat u tački 1.2. Ovaj materijal poslužio je kao polazna osnova za formulisanje i analizu kombinovanog algoritma za dekodiranje R–kodova koji je predmet ovog rada.

1.1 Osnovni pojmovi o kodovima za ispravljanje grešaka

U ovoj tački biće uvedene oznake i osnovni pojmovi o kodovima za ispravljanje grešaka (videti na primer knjige [Berl68,Pete72,MacW77, Clar82,LinC83]).

Neka je $B_n = \{0,1\}^n$, $n \geq 1$ i $B = B_1 = \{0,1\}$. Elementi skupa B_n su n–dimenzionalni binarni vektori, odnosno matrice dimenzija $n \times 1$. Vektori i matrice označavaju se masnim slovom, a njihove koordinate odgovarajućim običnim slovom sa indeksom, odnosno indeksima. Ako je $\mathbf{M}$ matrica, a $\mathbf{j} = (j_1, j_2, \ldots)$ uređeni skup indeksa, onda $\mathbf{M_j}$ označava matricu formiranu od kolona matrice $\mathbf{M}$ sa indeksima redom

$j_1, j_2, \ldots$. Vektor $\mathbf{M}_{(j)}$ označava se jednostavnije sa $\mathbf{M}_j$. Izuzetno, ako je $\mathbf{M}$ vektor–kolona, onda je M_j oznaka za njegovu j–tu koordinatu, u skladu sa uvedenim načinom pisanja vektora.

Slučajne promenljive biće označavane velikim štampanim slovom, a njihove realizacije odgovarajućim malim slovom. Pri prenosu poruka kroz kanal veze dolazi do njihovog izobličenja. Ako se na ulaz kanala dovede binarni vektor $\mathbf{x} \in B_n$, pod dejstvom šuma se na drugom kraju kanala dobija slučajni binarni n–dimenzionalni vektor $\mathbf{Y}$. Realizacija $\mathbf{y}$ slučajne promenljive $\mathbf{Y}$ u opštem slučaju nije jednaka vektoru $\mathbf{x}$. Pod pretpostavkom da su greške pojedinih koordinata nezavisne i jednako verovatne, sa verovatnoćom p, kaže se da je vektor $\mathbf{Y}$ nastao propuštanjem vektora $\mathbf{x}$ kroz binarni simetrični kanal (BSK) sa verovatnoćom prelaza p.

Definicija 1.1 *Neka je* $\mathbf{E}$ *slučajna n–dimenzionalna vektorska promenljiva sa raspodelom verovatnoća*

$$P\{\mathbf{E} = \mathbf{e}\} = p^{w(\mathbf{e})}(1-p)^{n-w(\mathbf{e})}, \qquad \mathbf{e} \in B_n, \tag{1.1}$$

pri čemu je $0 \leq p \leq 1$, *a sa* $w(\mathbf{e})$ *za* $\mathbf{e} \in B_n$ *je označena težina vektora* $\mathbf{e}$, *odnosno broj njegovih koordinata različitih od nule. Propuštanjem vektora* $\mathbf{x} \in B_n$ *kroz* binarni simetrični kanal *(BSK) sa* verovatnoćom prelaza p *dobija se vektorska slučajna promenljiva* $\mathbf{Y} = \mathbf{x} \oplus \mathbf{E}$, *primljena poruka, gde je sa* $\oplus$ *označeno pokoordinatno sabiranje vektora po modulu dva.*

Na skupu B_n definiše se metrika relacijom

$$\operatorname{dist}(\mathbf{u}, \mathbf{v}) = w(\mathbf{u} \oplus \mathbf{v})$$

(*Hemingovo rastojanje* vektora $\mathbf{u}, \mathbf{v} \in B_n$). U daljem tekstu se pod kanalom podrazumeva BSK. Da bi se mogle ispravljati greške u primljenoj poruci, na ulaz kanala se dovode vektori iz nekog podskupa skupa B_n. Jedna klasa ovakvih podskupova su *linearni kodovi.*

Definicija 1.2 *Neka su* n, k *prirodni brojevi,* $0 \leq k \leq n$, *i neka je* $\mathbf{G}$ *matrica dimenzija* $k \times n$ *čiji je rang jednak* k. *Skup vektora*

$$C = \left\{\mathbf{x} \mid \mathbf{x} = \mathbf{u}^T\mathbf{G},\ \mathbf{u} \in B_k\right\}$$

je linearni (n, k) kod. *Ovde je sa* T *označena operacija transponovanja matrice. Elemenat koda* $\mathbf{x} \in C$ *je* kodna reč. *Parametar* n *je dužina kodnih reči. Matrica* $\mathbf{G}$ *je* generišuća matrica *koda* C. *Linearni kod* C *je* sistematski *ako ima generišuću matricu* $\mathbf{G}$ *takvu da je* $G_{i,j} = \delta_{i,j}$, $1 \leq i, j \leq k$, *gde je sa* $\delta_{i,j}$ *označen Kronekerov simbol*

$$\delta_{i,j} = \begin{cases} 1, & i = j \\ 0, & i \neq j \end{cases} .$$

Linearni kod C je linearni k–dimenzionalni potprostor linearnog prostora koji čini skup B_n nad poljem GF(2). Baza ovog potprostora je skup vektora–vrsta matrice $\mathbf{G}$. Parametar k je *dimenzija linearnog koda* C. Kod sistematskog linearnog koda sve koordinate kodne reči mogu se očigledno izraziti kao linearne kombinacije prvih k koordinata kodne reči. Ova činjenica može se uopštiti uvođenjem pojma *informacionog skupa.*

Definicija 1.3 *Uređeni skup indeksa* $\mathbf{j} = (j_1, j_2, \ldots, j_k)$ *je* informacioni skup *linearnog koda* C *sa generišućom matricom* $\mathbf{G}$ *ako je matrica* $\mathbf{G_j}$ *nesingularna.*

Elementarnim transformacijama vrsta od matrice $\mathbf{G}$ može se formirati proizvoljna generišuća matrica $\mathbf{G}'$ linearnog koda C. Ove transformacije prevode podmatricu $\mathbf{G_j}$ u nesingularnu podmatricu $\mathbf{G'_j}$ matrice $\mathbf{G}'$, pa se zaključuje da je $\mathbf{j}$ informacioni skup linearnog koda C nezavisno od izbora generišuće matrice.

Definicija 1.4 *Neka je* C *linearni* (n, k) *kod sa generišućom matricom* $\mathbf{G}$. Dualni kod *linearnog koda* C *je linearni* $(n, n-k)$ *kod jednak ortogonalnom komplementu linearnog potprostora* C. *Dimenzija dualnog koda* $n-k$ *obično se označava sa* r. *Matrica* $\mathbf{H}$ *je kontrolna matrica linearnog koda* C *ako je za dualni kod* C' *generišuća matrica. Elementi dualnog koda* $\mathbf{a} \in C'$, *odnosno linearne forme* $\mathbf{a}^T\mathbf{x}$, $\mathbf{x} \in B_n$, *su* kontrole parnosti *linearnog koda* C, *s obzirom da je* $\mathbf{a}^T\mathbf{x} = \mathbf{0}$ *za svako* $\mathbf{x} \in C$. *Ovde je sa* $\mathbf{0}$ *označen nula vektor.*

Jasno je da se linearni kod može ekvivalentno definisati jednakošću

$$C = \{\mathbf{x} \in B_n \mid \mathbf{Hx} = \mathbf{0}\} .$$

Ako je $\mathbf{j}'$ komplement informacionog skupa $\mathbf{j}$ linearnog koda C, odnosno $\mathbf{j}' = \{1, 2, \ldots, n\} \setminus \mathbf{j}$, onda je $\mathbf{j}'$ informacioni skup dualnog koda C'. Zaista, ako se koordinate kodne reči sa indeksima iz skupa $\mathbf{j}'$ napišu kao linearne kombinacije koordinata sa indeksima iz skupa $\mathbf{j}$, dobija se kontrolna matrica $\mathbf{H}$ koda C (generišuća matrica koda C') takva da matrica $\mathbf{H}_{\mathbf{j}'}$ ima u svakoj koloni tačno jednu jedinicu, što znači da je nesingularna.

Isti bit x_i kodne reči, $1 \leq i \leq n$, može da bude obuhvaćen sa više kontrola parnosti $\mathbf{a}^{(j)T}\mathbf{x} = \mathbf{0}$, pri čemu su $\mathbf{a}^{(j)}$ neke kodne reči dualnog koda, $1 \leq j \leq l$. Ovakav sistem kontrola parnosti je *ortogonalan* u odnosu na bit x_i ako u svakoj koloni matrice čije su vrste vektori $\mathbf{a}^{(j)T}$ (sem i–te) postoji najviše jedna jedinica. Naravno, svi elementi i–te kolone ove matrice su jedinice.

Na Slici 1.1 prikazan je model sistema za prenos poruka kroz kanal sa greškama. Kodiranjem poruke $\mathbf{u} \in B_k$ dobija se kodna reč $\mathbf{x} = \mathbf{u}^T\mathbf{G}$, koja se dovodi na ulaz BSK sa verovatnoćom prelaza p. Na izlazu kanala dobija se vektor $\mathbf{y} = \mathbf{x} \oplus \mathbf{e}$, primljena poruka, gde je $\mathbf{e} \in B_n$ realizacija slučajne promenljive $\mathbf{E}$.

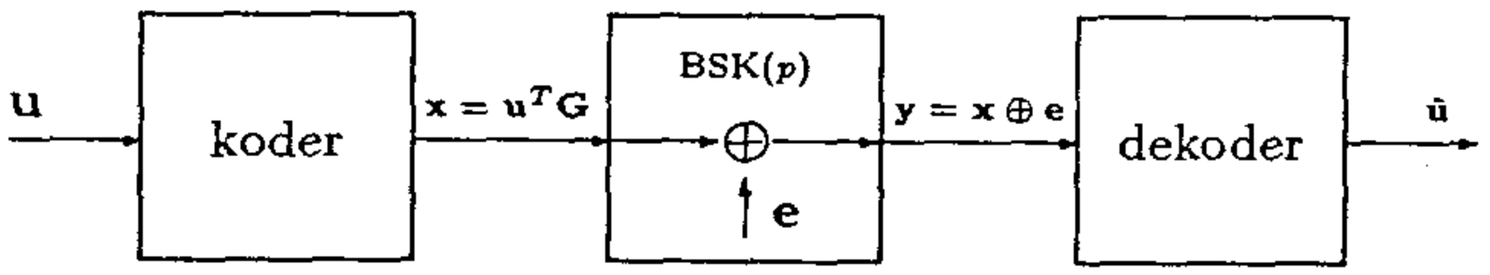
Slučajna promenljiva $\mathbf{S} = \mathbf{HY} = \mathbf{HE}$ je *sindrom* koji odgovara primljenoj poruci. Realizaciji $\mathbf{e}$ slučajne promenljive $\mathbf{E}$ odgovara realizacija $\mathbf{s} = \mathbf{He}$ slučajne promenljive $\mathbf{S}$. U daljem tekstu će se, kad nema opasnosti od zabune, pod primljenom porukom, vektorom greške i sindromom podrazumevati i realizacije slučajnih promenljivih $\mathbf{Y}, \mathbf{E}$ i $\mathbf{S}$. Za fiksiranu primljenu poruku $\mathbf{y}$, sindrom $\mathbf{s}$ *jednoznačno* određuje *koset*

$$C_{\mathbf{s}} = \{\mathbf{v} \mid \mathbf{v} \in B_n,\ \mathbf{Hv} = \mathbf{s}\} \tag{1.2}$$

koda C (kao podgrupe grupe $(B_n, \oplus)$) u kome leži vektor greške $\mathbf{e}$. Poznavanje vektora $\mathbf{y}$ (ili ekvivalentno, $\mathbf{s}$) na prijemnoj strani određuje samo koset u kome leži vektor greške $\mathbf{e}$. Bilo koji član koseta $C_{\mathbf{s}}$ može se usvojiti za vektor greške. Zbog toga je optimalno za ocenu $\hat{\mathbf{e}}$ vektora greške izabrati član koseta $C_{\mathbf{s}}$ sa najvećom verovatnoćom

$$P(\hat{\mathbf{e}}) = \max_{\mathbf{v} \in C_{\mathbf{s}}} P(\mathbf{v}) = \max \{P(\mathbf{v}) \mid \mathbf{v} \in B_n,\ \mathbf{Hv} = \mathbf{s}\}$$

(*dekodiranje po principu maksimuma verodostojnosti*). Odavde je ocena $\hat{\mathbf{x}}$ kodne reči $\mathbf{x}$ data sa $\hat{\mathbf{x}} = \hat{\mathbf{e}} \oplus \mathbf{y}$, a jednakost $\hat{\mathbf{x}} = \hat{\mathbf{u}}^T\mathbf{G}$ jednoznačno određuje ocenu poruke $\hat{\mathbf{u}}$, zbog toga što je $\operatorname{rang} \mathbf{G} = k$. Pri tome je



u – poruka, $\mathbf{u} \in B_k$
x – predata kodna reč, $\mathbf{x} \in C$
e – vektor greške, $\mathbf{e} \in B_n$
y – primljena poruka, $\mathbf{y} \in B_n$
û – ocena poruke u dekoderu

Slika 1.1: Model sistema za prenos poruka kroz kanal sa greškama

rang M oznaka za rang matrice M. *Koset–lider* koseta C_s je neki od njegovih članova najmanje težine. Zbog (1.1) se dekodiranje po principu maksimuma verodostojnosti svodi se na dekodiranje po principu minimuma rastojanja: za ocenu $\hat{\mathbf{e}}$ vektora greške usvaja se neki od koset–lidera koseta C_s, a za ocenu $\hat{\mathbf{x}}$ kodne reči $\mathbf{x}$ usvaja se neka od kodnih reči na najmanjem rastojanju od primljene poruke $\mathbf{y}$.

Postoje dva osnovna algoritma za dekodiranje linearnih kodova po principu minimuma rastojanja: dekodiranje pomoću spiska i dekodiranje pomoću sindroma, videti na primer [Levi85].

Algoritam 1.1 Dekodiranje linearnog (n, k) koda C pomoću spiska.
Ulaz: generišuća matrica G koda C, primljena poruka $\mathbf{y} \in B_n$.
Izlaz: kodna reč $\hat{\mathbf{x}}$ najbliža vektoru $\mathbf{y}$.

1^0 [Inicijalizacija minimalnog Hemingovog rastojanja d.] Staviti $d \leftarrow n + 1$.

2^0 [Prolazak kroz skup C.] Za svako $\mathbf{x} \in C$, ako je $\text{dist}(\mathbf{x}, \mathbf{y}) < d$, onda staviti $d \leftarrow \text{dist}(\mathbf{x}, \mathbf{y})$ i $\hat{\mathbf{x}} \leftarrow \mathbf{x}$.

3^0 [Kraj.] Rezultat dekodiranja je kodna reč $\hat{\mathbf{x}}$; kraj. □

Algoritam 1.2 Dekodiranje linearnog (n, k) koda C pomoću sindroma.
Ulaz: Kontrolna matrica $\mathbf{H}$ koda C, primljena poruka $\mathbf{y} \in B_n$ i tablica T u kojoj je za svaki od 2^{n-k} mogućih sindroma naveden odgovarajući koset–lider.
Izlaz: kodna reč $\hat{\mathbf{x}}$ najbliža vektoru $\mathbf{y}$.

1^0 [Izračunavanje sindroma.] Staviti $\mathbf{s} \leftarrow \mathbf{Hy}$.

2^0 [Očitavanje koset–lidera.] U tabeli T pronaći sindrom $\mathbf{s}$; neka je $\hat{\mathbf{e}}$ koset–lider koji odgovara ovom sindromu.

3^0 [Kraj.] Kodna reč $\hat{\mathbf{x}} = \mathbf{y} \oplus \hat{\mathbf{e}}$ je rezultat dekodiranja primljene poruke $\mathbf{y}$; kraj. □

Pod *numeričkom složenošću* algoritma podrazumeva se broj elementarnih operacija (na primer binarnih operacija sa realnim brojevima ili u polju GF(2), zavisno od konkretnog algoritma) koje treba izvršiti u toku njegovog izvođenja. *Memorijska složenost* algoritma jednaka je broju memorijskih lokacija koje su neophodne za izvršavanje algoritma.

Numerička složenost Algoritma 1.1 je $O(n2^k)$, dok je njegova memorijska složenost mala (određena je veličinom nk, brojem elemenata generišuće matrice koda).Numerička složenost Algoritma 1.2 je $O(n)$, jer se sindrom koristi kao adresa sa koje se iz tablice T očitava odgovarajući koset–lider. Međutim, memorijska složenost ovog algoritma je znatno veća, $O(n2^{n-k})$. Za oba algoritma proizvod numeričke i memorijske složenosti raste eksponencijalno sa dimenzijom problema, sa eksponentom k kod prvog, odnosno $n - k$ kod drugog algoritma.

1.2 Linearni rekurentni nizovi i R–kodovi

U ovoj tački date su definicije i poznati stavovi o vezi izlaznih nizova PRLPS, linearnih rekurentnih nizova u polju GF(2) i R–kodova. Izložene su poznàte činjenice o značaju problema dekodiranja R–kodova u kriptologiji.

Linearni rekurentni niz $\{u_i\}_{i\geq 1}$ reda k elemenata polja GF(2) može se zadati sa prvih k članova $x_1, x_2, \ldots, x_k$ i linearnom rekurantnom relacijom (LRR)

$$x_i = \bigoplus_{j=0}^{k-1} h_j x_{i-k+j}, \qquad i > k, \tag{1.3}$$

gde je $h_0 = 1, h_1, \ldots, h_{k-1} \in B$. Polinom $h(z) = \sum_{i=0}^{k} h_i z^i$ (pri čemu je $h_k = 1$) je *karakteristični polinom* ove rekurentne relacije.

Linearni rekurentni niz moze se definisati i kao izlazni niz pomeračkog registra sa linearnom povratnom spregom (PRLPS), konačnog automata datog sledećom definicijom.

Definicija 1.5 *Pomerački registar sa linearnom povratnom spregom (PRLPS)* $\mathcal{R}_h$ *dužine* $k \geq 1$ *sa polinomom povratne sprege*

$$h(z) = \sum_{i=0}^{k} h_i z^i \in \mathrm{GF}(2)[z]$$

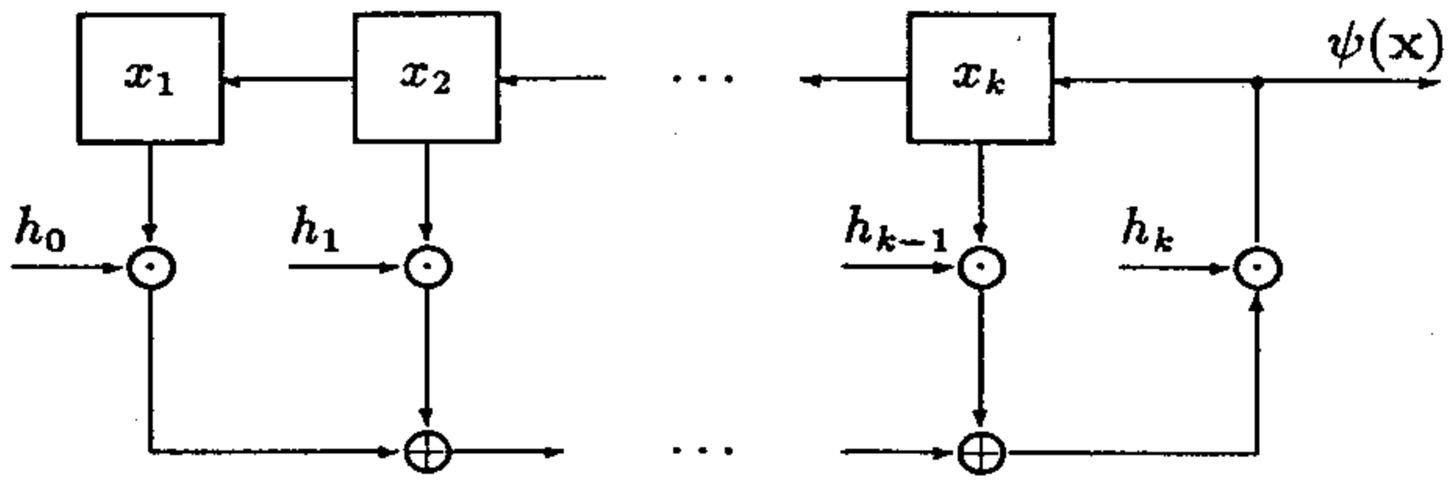
(pri čemu je $h_0 = h_k = 1$*) je konačni automat sa skupom stanja* B_k*, funkcijom prelaza* $\varphi_h : B_k \to B_k$

$$\varphi_h(\mathbf{u}) = \left[u_2 \; u_3 \; \ldots \bigoplus_{j=0}^{k} h_{k-j} u_{k+1-j} \right]^T, \qquad \mathbf{u} \in B_k,$$

i funkcijom izlaza $\psi_h : B_k \to B$,

$$\psi_h(\mathbf{u}) = \bigoplus_{j=0}^{k-1} h_j u_{j+1}, \qquad \mathbf{u} \in B_k.$$

Uobičajeno je da se PRLPS $\mathcal{R}_h$ predstavlja šemom kao na Slici 1.2. Na ovoj slici kvadrati označavaju memorijske elemente, a simboli $\oplus$ i $\otimes$ označavaju sabiranje i množenje u polju GF(2). Stanje PRLPS menja se u trenucima označenim sa $1, 2, \ldots$ tako što stanje svakog memorijskog elementa postaje jednako veličini koja je do tog trenutka bila prisutna na njegovom ulazu. Lako se proverava da ako je vektor stanja PRLPS pre trenutka 1 jednak $\mathbf{u} = [u_1, u_2, \ldots, u_k]^T$, tada se na izlazu PRLPS u trenucima $1, 2, \ldots$ dobija niz $x_{k+1}, x_{k+2}, \ldots$.



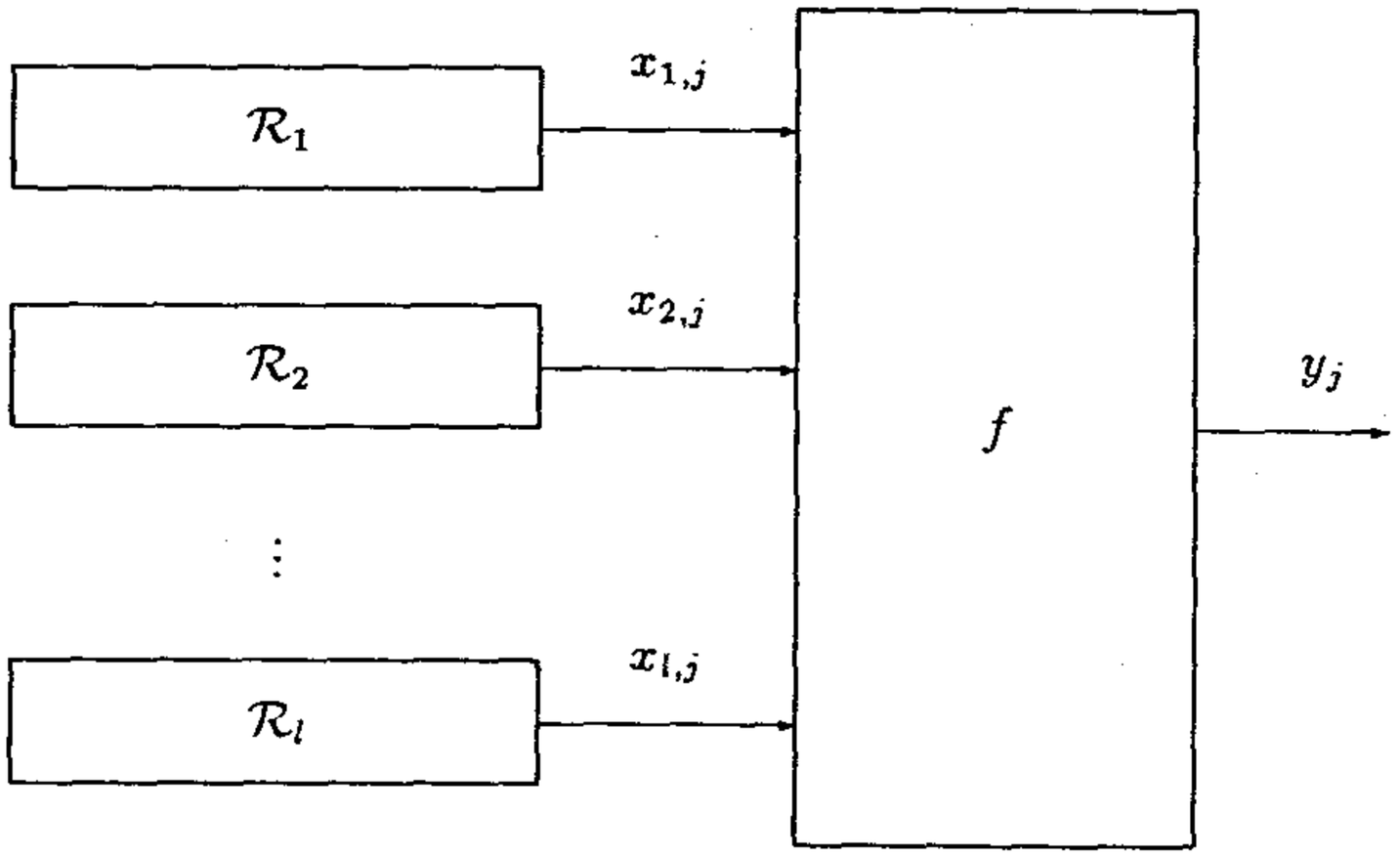
Slika 1.2: Pomerački registar sa linearnom povratnom spregom

Skup svih n–dimenzionalnih vektora $\mathbf{x} = [x_1\ x_2\ \ldots\ x_n]^T$ čije koordinate zadovoljavaju LRR (1.3) za $k < i \leq n$, sa karakterističnim polinomom $h(z)$, očigledno je linearni prostor. Odgovarajući linearni kod biće označavan sa $R_{h,n}$ (kod $R_{h,n}$, ili jednostavnije R–kod). Kontrolna matrica koda $R_{h,n}$ je na primer

$$\mathbf{H} = \begin{bmatrix} h_0 & h_1 & h_2 & \ldots & h_k & 0 & \ldots & 0 & 0 \\ 0 & h_0 & h_1 & \ldots & h_{k-1} & h_k & \ldots & 0 & 0 \\ \vdots & & & & \ddots & & & & \\ 0 & 0 & 0 & & \ldots & & & h_{k-1} & h_k \end{bmatrix}, \tag{1.4}$$

videti LRR (1.3). Polinom $h(z)$ je *karakteristični polinom* koda $R_{h,n}$.

Poznato je (videti [Golo67]) da ako je polinom povratne sprege primitivan (odnosno ako je $\min\{t : h(z) \mid z^t + 1\} = 2^k - 1$), a početno stanje PRLPS nije vektor $\mathbf{0}$, onda izlazni niz PRLPS ima maksimalno moguću periodu $(2^k - 1)$ i dobre statističke osobine. Zbog ove činjenice se nizovi maksimalne periode često koriste kao realizacije niza nezavisnih binarnih slučajnih promenljivih sa ravnomernom raspodelom verovatnoća. Međutim, ovakav *generator pseudoslučajnog niza* (GPSN) za neke primene, posebno u kriptologiji, nije pogodan zbog svoje jed-



Slika 1.3: GPSN dobijen sprezanjem nekoliko PRLPS pomoću Bulove funkcije

nostavne algebarske strukture, što omogućuje da se niz jednostavno rekonstruiše na osnovu svog proizvoljnog odsečka od k članova. Drugim rečima, postoji potreba za algebarski složenijim GPSN.

Klasa GPSN dobijenih sprezanjem izlaza nekoliko PRLPS pomoću Bulove funkcije (Slika 1.3) analizirana je u radu [Sieg85]. Na slici su izlazni nizovi $l \geq 1$ PRLPS označeni sa $\{x_{i,j}\}_{j\geq 1}$, $1 \leq i \leq l$, a izlazni niz GPSN $\{y_j\}$ definisan je jednakošću

$$y_j = f(x_{1,j}, x_{2,j}, \ldots, x_{l,j}), \qquad j \geq 1,$$

pri čemu je $f : B_l \to B$ Bulova funkcija od l promenljivih.

Neka je $\{x_j\}_{j\geq 1}$ bilo koji od nizova $\{x_{i,j}\}_{j\geq 1}$, $1 \leq i \leq l$. U [Sieg85] je pokazano da se pod određenim uslovima (koji se svode na to da se niz vektora na koje se primenjuje funkcija f približno ravnomerno prolazi kroz skup B_l)`može smatrati da je niz $\{y_j\}$ dobijen propuštanjem niza $\{x_j\}$ kroz BSK sa verovatnoćom prelaza p, $0 \leq p \leq 1$, pri čemu

verovatnoća p zavisi samo od funkcije f i rednog broja i niza $\{x_{i,j}\}_{j\geq 1}$. Prema tome, ako je $p \neq 1/2$ i raspolaže se odsečkom $\{y_j\}_{1\leq j\leq n}$ izlaznog niza iz GPSN, problem određivanja niza $\{x_j\}$ ekvivalentan je problemu dekodiranja koda $R_{h,n}$, gde je $h(z)$ karakteristični polinom linearnog rekurentnog niza $\{x_j\}$. Činjenica da se pojedini ulazni nizovi mogu rekonstruisati na osnovu izlaznog niza GPSN nezavisno od ostalih, predstavlja ozbiljnu slabost ovog GPSN. Izborom funkcije f koja je *korelaciono imuna* određenog reda (videti [Sieg84]) može se značajno otežati (videti [Meie89]) rekonstrukcija pojedinih ulaznih nizova. Međutim, ta problematika neće ovde biti razmatrana, već će naglasak biti na algoritmima za dekodiranje R–kodova.

1.3 Pregled poznatih algoritama za dekodiranje R–kodova

Prvi put je problem dekodiranja R–kodova razmatran u radu [Sieg85], gde je u suštini rešavan algoritmom dekodiranja po spisku (Algoritam 1.1). Posto je kombinovani algoritam za dekodiranje R–kodova iz narednog poglavlja nastao sprezanjem dva algoritma iz [Meie89], rezultati iz ovog rada biće detaljnije prikazani (komentari koji se odnose na ovaj rad biće dati u narednom poglavlju). Zatim će biti dat osvrt na druge algoritme za dekodiranje linearnih kodova značajne u ovom kontekstu.

Neka je $\mathbf{x}$ kodna reč koda $R_{h,n}$ i neka je $\mathbf{Y}$ primljena poruka, slučajna promenljiva dobijena propuštanjem vektora $\mathbf{x}$ kroz BSK sa verovatnoćom prelaza p, $0 \leq p < 1/2$. U radu [Sieg85] utvrđeno je da za dovoljno veliko n postoji prag rastojanja d_0 takav da je sa verovatnoćom bliskom jedinici $\mathrm{dist}\,(\mathbf{x}, Y) \leq d_0$, a da je za proizvoljno $\mathbf{x}' \in R_{h,n}$, $\mathbf{x}' \neq \mathbf{x}$, sa verovatnoćom bliskom jedinici $\mathrm{dist}\,(\mathbf{x}', Y) > d_0$. Ova činjenica omogućuje da se za proizvoljno $\mathbf{x}' \in R_{h,n}$ i proizvoljnu realizaciju $\mathbf{y} \in B_n$ slučajne promenljive $\mathbf{Y} = \mathbf{x} \oplus \mathbf{E}$ lako se može ustanoviti (sa određenom verovatnoćom greške) da li kodna reč $\mathbf{x}'$ jeste ili nije rezultat dekodiranja vektora $\mathbf{y}$ po principu maksimuma verodostojnosti: dovoljno je proveriti da li je $\mathrm{dist}\,(\mathbf{x}, Y) \leq d_0$ (tada je $\mathbf{x}' = \mathbf{x}$) ili $\mathrm{dist}\,(\mathbf{x}', Y) > d_0$ (iz čega se zaključuje da je $\mathbf{x}' \neq \mathbf{x}$).

Pri izlaganju rezultata iz [Meie89] neke oznake su promenjene, a terminologija je prilagođena onoj koja se koristi u teoriji kodova za ispravljanje grešaka.

Vektor $\mathbf{x} \in B_n$ jednak odsečku od prvih n članova niza $\{x_i\}$, koji zadovoljava LRR (1.3) sa karakterističnim polinomom $h(z) \in \mathrm{GF}(2)[z]$, je kodna reč koda $R_{h,n}$. Pored LRR (1.3) niz $\{x_i\}$ zadovoljava i LRR sa karakterističnim polinomom $h(z)g(z)$, gde je $g(z) \in \mathrm{GF}(2)[z]$ proizvoljni polinom. Specijalno, niz $\{x_i\}$ zadovoljava LRR sa karakterističnim polinomom

$$(h(z))^{2^j} = h\left(z^{2^j}\right),$$

za proizvoljno j, $j \geq 0$. Dakle, koordinate vektora $\mathbf{x}$ zadovoljavaju rekurentne relacije oblika

$$\bigoplus_{l=0}^{k} h_l x_{i+2^j l} = 0, \qquad j \geq 0,\ 1 - 2^j l \leq i \leq n - 2^j l, \tag{1.5}$$

koje su ustvari kontrole parnosti za kod $R_{h,n}$. Sve ove kontrole parnosti sadrže po $m+1$ sabiraka, gde je sa m označen broj nekonstantnih članova polinoma $h(z)$. U daljem tekstu pretpostavlja se da je m paran broj, jer ako je m neparno, onda polinom $h(z)$ nije nesvodljiv, a tim pre nije ni primitivan.

Neka je sa x označena fiksirana koordinata x_i vektora $\mathbf{x}$, $1 \leq i \leq n$. Bit x zadovoljava kontrole parnosti ekvivalentne nekim od LRR (1.5),

$$x \oplus b_j = 0, \qquad 1 \leq j \leq r. \tag{1.6}$$

Ovde je r broj kontrola parnosti u kojima učestvuje bit x, a b_j je suma tačno m različitih koordinata vektora $\mathbf{x}$. U daljim izvođenjima se u [Meie89] pretpostavlja da je ovaj sistem kontrola parnosti ortogonalan u odnosu na bit x. Broj r zavisi od indeksa bita x u kodnoj reči, pa je izračunata njegova srednja vrednost

$$r = \left[\log \frac{n}{2k}\right](m+1), \tag{1.7}$$

gde se logaritam uzima sa osnovom dva, a $[z]$ označava celi deo realnog broja z, odnosno takav celi broj d da je $d \leq z < d+1$.

Korišćenjem kontrola parnosti (1.6) može se preko primljene poruke, slučajnog vektora $\mathbf{Y} \in B_n$, izraziti aposteriorna verovatnoća greške

(AVG) bita $Y = Y_i$. Neka je zadovoljeno tačno t od ukupno r kontrola parnosti

$$L_j = Y \oplus C_j = 0, \qquad 1 \leq j \leq r, \tag{1.8}$$

gde je sa C_j označena suma po modulu dva koordinata vektora $\mathbf{Y}$ koje odgovaraju koordinatama vektora $\mathbf{x}$ obuhvaćenim sumom b_j u (1.6), $1 \leq j \leq r$. Verovatnoća $\tilde{p} = P\{C_j \neq b_j\}$ ne zavisi od j i jednaka je

$$\tilde{p} = \frac{1 - (1-2p)^m}{2} \tag{1.9}$$

jer je $C_j \neq b_j$ ako i samo ako je neparna suma m nezavisnih jednako raspodeljenih slučajnih $0-1$ promenljivih sa verovatnoćom jedinice p. Na osnovu toga dobija se uslovna verovatnoća da je bit x pogrešno primljen (odnosno $Y \neq x$) pod uslovom da je nekih t fiksiranih kontrola parnosti (1.8) jednako nuli

$$\begin{aligned} \hat{P} &= P\left(\{Y \neq x\} \mid \{L_1 = L_2 = \cdots = L_t = 0\}\right) \\ &= \frac{p\tilde{p}^t(1-\tilde{p})^{r-t}}{p\tilde{p}^t(1-\tilde{p})^{r-t} + (1-p)(1-\tilde{p})^t\tilde{p}^{r-t}} \end{aligned} \tag{1.10}$$

Ova verovatnoća je slučajna promenljiva, čija realizacija $\hat{p}$ omogućuje da se sa većom pouzdanošću oceni da li je bit y primljene poruke (realizacija slučajne promenljive Y) jednak ili različit od odgovarajućeg bita x kodne reči (odnosno da li je *tačan* ili *pogrešan*). Na jednom primeru je pokazano da uslovna matematička očekivanja slučajne promenljive $\hat{P}$ zadovoljavaju nejednakost

$$M\left(\hat{P} \mid \{Y = x\}\right) < M\left(\hat{P} \mid \{Y \neq x\}\right).$$

Zatim je dokazano (na primeru homogenog sistema ortogonalih kontrola parnosti) da za matematičko očekivanje ove slučajne promenljive važi jednakost $M(\hat{P}) = p$, što je inače očigledno.

Ova činjenica omogućuje da se efikasnije izvrši dekodiranje koda $R_{h,n}$ po principu minimuma rastojanja. Potrebno je izabrati k koordinata vektora $\mathbf{y}$ sa najmanjim AVG, odnosno sa najvećim brojem t zadovoljenih kontrola parnosti oblika (1.8). Postoji kodna reč takva da joj se odgovarajućih k koordinata poklapa sa vektorom $\mathbf{y}$ (ako takva

kodna reč nije jedinstvena, onda se može odabrati još nekoliko novih koordinata vektora $\mathbf{y}$). Izračunavanjem rastojanja od vektora $\mathbf{y}$ utvrđuje se da li se ova kodna reč može usvojiti za rezultat dekodiranja. Ako to nije slučaj, ispituju se zatim na isti način kodne reči koje se od ove na izabranom skupu koordinata razlikuju na jednoj, dve, ... pozicije, dok se ne dođe do rešenja. Prag za broj t zadovoljenih kontrola parnosti bira se tako da očekivani broj koordinata kodne reči sa bar t zadovoljenih kontrola parnosti bude bar k: $nT(p,r,t) \geq k$. Ovde je $T(p,r,t)$ uslovna verovatnoća da je $Y = x$, pod uslovom da je zadovoljeno bar t od r kontrola parnosti oblika (1.8),

$$T(p,r,t) = \left(\sum_{i=t}^{r} \binom{r}{i} (1-p)(1-\tilde{p})^i \tilde{p}^{r-i} \right) / Q(p,r,t),$$

gde je

$$Q(p,r,t) = \sum_{i=t}^{r} \binom{r}{i} \left((1-p)(1-\tilde{p})^i \tilde{p}^{r-i} + p\tilde{p}^i (1-\tilde{p})^{r-i} \right)$$

verovatnoća da je zadovoljeno bar t od r kontrola parnosti (1.8). Na osnovu ovih činjenica je formulisan sledeći algoritam za dekodiranje R–kodova [Meie89, Algoritam A].

Algoritam 1.3 *(Algoritam A)* Dekodiranje koda $R_{h,n}$.
Ulaz: prirodni brojevi n, k, polinom $h(z) \in \mathrm{GF}(2)[z]$ stepena k, primljena poruka $\mathbf{y} \in B_n$, verovatnoća prelaza BSK p.
Izlaz: kodna reč $\mathbf{x} \in R_{h,n}$ koja se nalazi na najmanjem Hemingovom rastojanju od vektora y.

1^0 Odrediti srednji broj kontrola parnosti r na osnovu (1.7).

2^0 Odrediti najveći broj t takav da je $nQ(p,r,t) \geq k$. Tada je među k koordinata primljene poruke koje od r zadovoljavaju bar t kontrola parnosti (1.8) očekivani broj grešaka jednak

$$\bar{N}_g = k\,(1 - T(p,r,t))\,.$$

3^0 Odrediti skup koordinata $\mathbf{j}$ vektora $\mathbf{y}$ koje zadovoljavaju bar t od r kontrola parnosti (1.8). Odrediti kodnu reč čije su koordinate sa indeksima iz skupa $\mathbf{j}$ jednake odgovarajućim koordinatama vektora $\mathbf{y}$.

4^0 Odrediti kodnu rec **x** pretragom po skupovima kodnih reči koje se od vektora **y** na skupu indeksa **j** razlikuju redom na $0, 1, \ldots$ koordinata (ispituje se da li su ove kodne reči na Hemingovom rastojanju manjem od zadate granice od vektora **y**, videti [Sieg85]). □

U slučaju kad n nije dovoljno veliko, dobijena kodna reč ne mora biti jednaka onoj od koje je propuštanjem kroz BSK dobijen vektor **y**, [Meie89]. Pored ovog, data su i sledeća dva komentara.

- Pojedine koordinate kodne reči zadovoljavaju različit broj kontrola parnosti oblika (1.8), pa je bolje u koraku 3^0 algoritma formirati skup **j** kao skup indeksa koordinata za koje su najmanje AVG (verovatnoće $\hat{p}$).

- U skup **j** mogu se uključivati i koordinate za koje je AVG $\hat{p}$ bliska jedinici, pošto se odgovarajuće koordinate vektora **y** komplementiraju. Međutim, ocenjuje se da ovakvo poboljšanje algoritma nije previše značajno.

Neka je slučajna promenljiva N_g jednaka broju grešaka u vektoru **Y** među koordinatama iz skupa **j** i neka je n_g realizacija ove slučajne promenljive kad je realizacija slučajne promenljive **Y** jednaka vektoru **y**. Ukoliko se za elementarnu operaciju proglasi formiranje i provera jedne kodne reči u tački 4^0 algoritma (što se može izvesti sa $O(n)$ operacija u polju GF(2), odnosno sabiranja celih brojeva), tada je numerička složenost Algoritma A ograničena sa

$$A(k, n_g) = \sum_{i=0}^{n_g} \binom{k}{i}.$$

Ovaj izraz može se ograničiti odozgo na poznati način [Lint82, str. 20]

$$A(k, n_g) \leq 2^{kH(n_g/k)},$$

gde je $H(z) = -z\mathrm{ld}\, z - (1-z)\mathrm{ld}\,(1-z)$, a ld je oznaka za logaritam sa osnovom dva. Međutim, poznata je samo očekivana vrednost slučajne promenljive N_g. Zbog toga se numerička složenost algoritma može proceniti sa 2^{ck}, gde je $c = c(p, m, n/k) = H\,(1 - T(p, r, t'))$, a t' je najveći broj t za koji je $Q(p, r, t) \geq k/n$. U radu je zatim data

tablica vrednosti veličine c kad je $p = 0.25(0.02)0.49$ i $m = 2(2)16$, za $n/k \in \{10^2, 10^6\}$. Ovi podaci dati su u Tabeli 1.1 za $m = 2(2)8$, pri čemu se navode i vrednosti parametara r i t'. Analizom tabele zaključeno je da je numerička složenost ovog algoritma znatno manja od složenosti potpune pretrage, odnosno dekodiranja pomoću spiska (Algoritam 1.1). Na primer, za $n = 25000$, $k = 500$, $m = 2$ dobija se $r = 12$, $t' = 11$ i $c = 0.0195$.

Iz eksperimenata sa algoritmom proistekla su sledeća zapažanja.

- Sa rastom m (odnosno broja članova polinoma $h(z)$) vrednost $c(p, m, n/k)$ teži graničnoj vrednosti $H(p)$, jer je tada $\tilde{p} \simeq 1/2$ i $T(p, r, t) \simeq 1 - p$. Navedeno je da se ova ocena može primeniti na algoritam iz rada [Sieg85], ako se na isti način, po broju grešaka na informacionom skupu, organizuje pretraga 2^k kodnih reči koda $R_{h,n}$.

- za $m = 2$ i $p \leq 0.4$ algoritam je znatno efikasniji od potpune pretrage, što omogućuje dekodiranje čak i kad je $k \geq 1000$.

- Upoređenjem slučajeva $n/k = 10^2$ i $n/k = 10^6$ u Tabeli 1.1 zapaža se da se sa rastom odnosa n/k efikasnost algoritma drastično popravlja samo za $m \leq 8$.

- Za $m \geq 10$ i $p \geq 0.25$ ovaj algoritam ne daje nikakvo poboljšanje u odnosu na uređenu totalnu pretragu.

Drugi algoritam za dekodiranje R–kodova [Meie89, Algoritam B] ima prema tvrđenju autora polinomijalnu složenost. Najpre se nekoliko puta apriorne verovatnoće greške zamenjuju (na osnovu njih) izračunatim AVG, a zatim se komplementiraju biti primljene poruke kojima je AVG iznad određenog praga. Dekodiranje se sastoji od nekoliko ovakvih ciklusa pri čemu se posle svakog ciklusa verovatnoće greške izjednačavaju sa verovatnoćom prelaza p BSK.

Neka je $U(p, r, t)$ verovatnoća da je zadovoljeno najviše t od r kontrola parnosti (1.8) i neka je $V(p, r, t)$, odnosno $W(p, r, t)$, verovatnoća da je zadovoljeno najviše t od r kontrola parnosti pri čemu je istovremeno $Y = x$, odnosno $Y \neq x$. Tada je

$$U(p, r, t) = \sum_{i=0}^{t} \binom{r}{i} \left((1-p)(1-\tilde{p})^i \tilde{p}^{r-i} + p\tilde{p}^i (1-\tilde{p})^{r-i} \right),$$

Vrednosti $c = c(p, m, n/k)$ za $n/k = 100$								
	$m = 2$,	$r = 15$	$m = 4$,	$r = 25$	$m = 6$,	$r = 35$	$m = 8$,	$r = 45$
p	c	t'	c	t'	c	t'	c	t'
0.25	0.012	13	0.314	19	0.671	24	0.772	30
0.27	0.028	13	0.462	19	0.761	24	0.822	30
0.29	0.062	13	0.641	18	0.825	24	0.860	30
0.31	0.122	13	0.750	18	0.871	24	0.890	30
0.33	0.293	12	0.832	18	0.905	24	0.914	30
0.35	0.432	12	0.890	18	0.930	24	0.934	30
0.37	0.584	12	0.930	18	0.949	24	0.951	30
0.39	0.729	12	0.956	18	0.964	24	0.965	30
0.41	0.846	12	0.973	18	0.976	24	0.976	30
0.43	0.927	12	0.985	18	0.986	24	0.986	30
0.45	0.973	12	0.993	18	0.993	24	0.993	30
0.47	0.994	12	0.997	18	0.997	24	0.997	30
0.49	1.000	12	1.000	18	1.000	24	1.000	30
Vrednosti $c = c(p, m, n/k)$ za $n/k = 1000000$								
	$m = 2$,	$r = 54$	$m = 4$,	$r = 90$	$m = 6$,	$r = 126$	$m = 8$,	$r = 162$
p	c	t'	c	t'	c	t'	c	t'
0.25	0.000	49	0.009	69	0.311	90	0.660	111
0.27	0.000	48	0.043	69	0.515	90	0.768	111
0.29	0.000	47	0.150	68	0.692	89	0.836	111
0.31	0.000	47	0.327	68	0.805	89	0.880	111
0.33	0.001	46	0.555	67	0.875	89	0.910	111
0.35	0.007	46	0.734	67	0.917	89	0.932	111
0.37	0.039	45	0.856	67	0.945	89	0.950	111
0.39	0.132	45	0.926	67	0.963	89	0.965	111
0.41	0.362	44	0.963	67	0.976	89	0.976	111
0.43	0.642	44	0.982	67	0.986	89	0.986	111
0.45	0.870	44	0.992	67	0.993	89	0.993	111
0.47	0.976	44	0.997	67	0.997	89	0.997	111
0.49	0.999	44	1.000	67	1.000	89	1.000	111

Tabela 1.1: Vrednosti $c(p, m, n/k)$ za $n/k \in \{100, 1000000\}$ sa odgovarajućim vrednostima r i t_{min}

$$V(p,r,t) = \sum_{i=0}^{t} \binom{r}{i} (1-p)(1-\tilde{p})^i \tilde{p}^{r-i}$$

i

$$W(p,r,t) = \sum_{i=0}^{t} \binom{r}{i} p\tilde{p}^i (1-\tilde{p})^{r-i}.$$

Ukoliko se posle izračunavanja AVG komplementiraju oni biti primljene poruke koji zadovoljavaju najviše t kontrola parnosti, tada je $nU(p,r,t)$ – matematičko očekivanje broja komplementiranih bita, $nV(p,r,t)$ – matematičko očekivanje broja pogrešno komplementiranih bita, dok je $nW(p,r,t)$ – matematičko očekivanje broja ispravno komplementiranih bita (bita koji posle komplementiranja postaju tačni, odnosno jednaki odgovarajućim koordinatama vektora x). Matematičko očekivanje priraštaja broja tačnih bita u vektoru y posle komplementiranja je $nI(p,r,t)$, gde je

$$I(p,r,t) = W(p,r,t) - V(p,r,t) \tag{1.11}$$

smanjenje verovatnoće greške. Za parametar t usvaja se vrednost t_{max} takva da izraz $I(p,r,t)$ ima maksimalnu vrednost za $t = t_{max}$. Ovakva optimizacija demonstrirana je na jednom primeru.

Napomenuto je da stoji slično zapažanje kao i za Algoritam A: mogu se komplementirati oni biti primljene poruke kojima je AVG veća od nekog praga. Kao prag se koristi veličina

$$p_{thr} = \frac{1}{2}\left(\hat{p}(p,r,t_{max}) + \hat{p}(p,r,t_{max}+1)\right), \tag{1.12}$$

gde je verovatnoća $\hat{p}$ definisana jednakostima (1.9) i (1.10). Posle prvog ciklusa očekivani broj bita kojima je $\hat{p}$ veće od p_{thr} je $nU(p,r,t_{max}$.

Da bi se mogle izračunavati AVG opisan je (iterativni) postupak nala

vzenja verovatnoće da je neparna suma m nezavisnih bita sa različitim verovatnoćama jedinice $p_1, p_2, \ldots, p_m$. U zatvorenom obliku je ova verovatnoća (umesto (1.9)) jednaka (videti [Gall62])

$$\tilde{p}(p_1, p_2, \ldots, p_m; m) = \frac{1}{2}\left(1 - \prod_{i=1}^{m}(1-2p_i)\right),$$

što menja i druge izraze u kojima figuriše verovatnoća $\tilde{p}$ ((1.10) i izraze za verovatnoće $U(p,r,t)$, $V(p,r,t)$ i $W(p,r,t)$). Na osnovu sprovedenih eksperimenata zaključeno je da nema potrebe da broj α iteracija (izračunavanja novih AVG za sve bite) bude veliki; predlaže se vrednost $\alpha = 5$).

Algoritam 1.4 *(Algoritam B)* Dekodiranje koda $R_{h,n}$.
Ulaz: prirodni brojevi n, k, polinom $h(z) \in \mathrm{GF}(2)[z]$ stepena k, primljena poruka $\mathbf{y} \in B_n$, verovatnoća greške p.
Izlaz: kodna reč $\mathbf{x} \in R_{h,n}$ koja se nalazi na najmanjem Hemingovom rastojanju od vektora y.

1^0 Odrediti srednji broj kontrola parnosti r na osnovu (1.7).

2^0 Odrediti vrednost $t = t_{max}$ takvu da maksimizira funkciju $I(p,r,t)$.
Ako je $I(p,r,t) \leq 0$, dekodiranje je neizvodljivo ovim algoritmom; kraj. U protivnom izračunati prag verovatnoće p_{thr} (1.12) i očekivani broj $n_{thr} = nU(p,r,t_{max})$ bita sa AVG većom od p_{thr}.

3^0 Inicijalizovati brojač iteracija $i \leftarrow 0$.

4^0 Za svaku koordinatu y vektora $\mathbf{y}$ izračunati AVG $\hat{p}$ (1.10) na osnovu broja kontrola parnosti (1.8) koje ova koordinata zadovoljava. Odrediti broj n_w bita za koje je $\hat{p} > p_{thr}$.

5^0 Ako je $n_w < n_{thr}$ i $i < \alpha$, onda staviti $i \leftarrow i + 1$, skok na 4^0.

6^0 Komplementirati koordinate y vektora $\mathbf{y}$ kojima odgovara verovatnoća $\hat{p} > p_{thr}$ i vratiti verovatnoće greške pridružene koordinatama na polaznu vrednost p.

7^0 Ako postoje koordinate vektora $\mathbf{y}$ koje ne zadovoljavaju sve kontrole parnosti (1.8), odnosno ako nije $\mathbf{y} \in R_{h,n}$, onda skok na 3^0.

8^0 Rezultat dekodiranja je vektor $\mathbf{y} = \mathbf{x}$. □

Pod iteracijom se podrazumeva unutrašnja petlja algoritma (koraci $4^0 - 5^0$), a pod ciklusom - spoljašnja petlja (koraci $3^0 - 7^0$). Iz eksperimenata sa ovim algoritmom proistekla su sledeća zapažanja.

- U prvom ciklusu je $n_w \simeq n_{thr}$, što je i očekivano, pa je dovoljno u prvom ciklusu izvršiti jednu iteraciju.

- U narednim ciklusima biti greške $Y_i \oplus x_i$ nisu više nezavisni, što znači da, striktno govoreći, ovaj statistički model (BSK) nije više primeljiv. Zbog toga je u eksperimentima obično $n_w < n_{thr}$ i potrebno je izvršavati nekoliko iteracija. Posle malog broja iteracija sve AVG se grupišu u okolini nule ili jedinice, pri čemu je grupisanje relativno stabilno. Time se opravdava ograničavanje broja iteracija u ciklusu. Ipak, broj grešaka konstantno opada iz ciklusa u ciklus i na kraju vektor **y** dobija vrednost **x**. Ovu pojavu je veoma teško teorijski analizirati.

- Verovatnoće se u koraku 6^0 mogu resetovati i na vrednost manju od p, u skladu sa očekivanim smanjenjem broja grešaka. Ovo međutim nije dovelo do uočljivog poboljšanja eksperimentalnih rezultata.

Kao i kod Algoritma A ukoliko dužina n kodnih reči nije dovoljno velika, rezultat dekodiranja može da bude kodna reč različita od one koja je dovedena na ulaz BSK.

Ocena granice primenljivosti algoritma izvedena je tako što je analizirana funkcija $I_{max} = I(p, r, t_{max})$. Pošto je r funkcija od m i $d = n/k$, a t_{max} je funkcija od p i r, veličina I_{max} zavisi od p, m i d, tj. $I_{max} = I_{max}(p, m, d)$. Očekivani broj ispravljenih bita posle prve iteracije je

$$nI_{max}(p, m, d) = k \times F(p, m, d),$$

gde je

$$F(p, m, d) = d \times I_{max}(p, m, d)$$

faktor korekcije koji ne zavisi od k. Ako je $F(p, m, d) \leq 0$, ne može se očekivati ispravljanje grešaka. Ako je $F(p, m, d) \geq 0.5$, tvrdi se da je Algoritam B davao dobre rezultate u većini eksperimenata a da je u nekim slučajevima dekodiranje bilo uspešno i za $F(p, m, d) = 0.1$. Zbog toga su date tablice vrednosti veličina p' i p'' u zavisnosti od d i t, gde je $F(p', m, d) = 0.5$, i $F(p, m, d) > 0.5$ za $p < p'$, odnosno $F(p'', m, d) = 0$, i $F(p, m, d) \leq 0$ za $p > p''$. U Tabeli 1.2 su za $m \in \{2, 4, 6, 8\}$ pored p', odnosno p'', navedene i odgovarajuće vrednosti r, t_{max}. Na osnovu

	Vrednosti p'' za koje je $F(p'', m, n/k) = 0.0$											
	$m = 2$			$m = 4$			$m = 6$			$m = 8$		
n/k	p''	r	t_{max}	p''	r	t_{max}	p''	r	t_{max}	p''	r	t_{max}
10^1	0.416	6	-1	0.261	10	-1	0.196	14	-1	0.160	18	-1
10^2	0.467	15	-1	0.327	25	-1	0.250	35	-1	0.204	45	-1
10^3	0.479	24	-1	0.352	40	-1	0.269	56	-1	0.217	72	-1
10^4	0.486	36	-1	0.367	60	-1	0.281	84	-1	0.227	108	-1
10^5	0.488	45	-1	0.373	75	-1	0.287	105	-1	0.232	135	-1
10^6	0.490	54	-1	0.377	90	-1	0.291	126	-1	0.236	162	-1
10^7	0.491	66	-1	0.382	110	-1	0.296	154	-1	0.240	198	-1
10^8	0.492	75	-1	0.384	125	-1	0.298	175	-1	0.243	225	-1
10^9	0.492	84	-1	0.387	140	-1	0.301	196	-1	0.245	252	-1
10^{10}	0.493	96	-1	0.389	160	-1	0.304	224	-1	0.247	288	-1
	Vrednosti p' za koje je $F(p', m, n/k) = 0.5$											
	$m = 2$			$m = 4$			$m = 6$			$m = 8$		
n/k	p'	r	t_{max}	p'	r	t_{max}	p'	r	t_{max}	p'	r	t_{max}
10^1	0.239	6	1	0.120	10	3	0.065	14	5	0.050	18	7
10^2	0.405	15	4	0.247	25	8	0.176	35	12	0.137	45	16
10^3	0.447	24	7	0.293	40	12	0.212	56	18	0.167	72	25
10^4	0.467	36	10	0.321	60	18	0.237	84	28	0.188	108	38
10^5	0.475	45	12	0.337	75	22	0.252	105	34	0.201	135	46
10^6	0.481	54	14	0.349	90	26	0.263	126	40	0.210	162	54
10^7	0.484	66	17	0.359	110	31	0.273	154	49	0.219	198	67
10^8	0.487	75	18	0.367	125	35	0.280	175	54	0.225	225	75
10^9	0.489	84	20	0.372	140	39	0.286	196	60	0.231	252	83
10^{10}	0.490	96	22	0.378	160	44	0.292	224	69	0.236	288	95

Tabela 1.2: Vrednosti p za koje je $F(p, t, n/k) \in \{0, 0.5\}$ sa odgovarajućim vrednostima r i t_{max}

ovih podataka zaključeno je da je za $m < 8$ dekodiranje izvodljivo u situacijama koje se mogu pojaviti u praksi, a za $m = 2$ veličine p' i p'' postaju veoma bliske jednoj polovini. S druge strane, za $m \geq 10$ je dekodiranje praktično neizvodljivo.

Na jednom primeru ($n = 10000$, $k = 100$, $m = 4$, $p = 0.25$) demonstrirana je efikasnost algoritma. U toku ukupno 12 iteracija (5 ciklusa) ispravljene su sve greške u vektoru $\mathbf{y}$.

Numerička složenost Algoritma B ocenjena je (u [Meie89]; i zaključivanje koje sledi je iz ovog rada) polazeći od pretpostavke da potreban broj iteracija zavisi samo od p, m i d, ali ne i od dimenzije k koda (pošto faktor korekcije $F(p, m, d)$ ne zavisi direktno od k). Numerička složenost izračunavanja jedne AVG takođe zavisi samo od d. Dakle, za fiksirano d numerička složenost algoritma zavisi linearno od n, a time i od k.

U radu [BerM78] pokazano je da je problem dekodiranja linearnih kodova NP–kompletan. Srednja složenost dekodiranja za familije kodova razmatrana je u nekim radovima autora iz SSSR [Bass77,Kruk89,Zyab75]. Jedan algoritam dekodiranja pomoću informacionih skupova predložen je u radu [Evse83]. Dekodiranje simbol–po–simbol, korišćenjem AVG (složenost izračunavanja reda 2^r) razmatrana je u radovima [Hart76, Wolf78]. Postoji posebna klasa algoritama za dekodiranje kod kojih se koriste dopunske informacije o pouzdanosti pojedinih bita (*soft decision decoding*), videti [Baum78,Dors74]. Ovi algoritmi se mogu primeniti kao dopuna algoritma iz rada [LeeB88], ako se AVG interpretiraju kao mere nepouzdanosti bita. Usavršena verzija Algoritma B iz [Meie89] data je u [Miha90]; predloženo je uvođenje novih kontrola parnosti sa malim brojem članova. Neki algoritmi za dekodiranje eksponencijalne složenosti razmatrani su i u radu [Be'e86]. U nekoliko radova se razmatraju algoritmi za iterirano ispravljanje grešaka na osnovu težine sindroma [Gall60,Boss86,Zolo86].

Poglavlje 2

Kombinovani algoritam za dekodiranje kodova $R_{h,n}$

U ovom poglavlju biće izložen i analiziran algoritam za dekodiranje kodova $R_{h,n}$ dobijen usavršavanjem, razradom i objedinjavanjem Algoritma A i Algoritma B iz [Meie89]. Razrada i analiza probabilističke faze algoritma, koja sadrži uglavnom rezultate iz radova [Živk90,Živl90], biće izložene u poglavlju 3. Faza pretrage (dekodiranja pomoću informacionih skupova) algoritma izložena je u poglavlju 4. Primeri dekodiranja pomoću ovog algoritma dati su u poglavlju 5.

Uključivanje dekodiranja pomoću informacionih skupova (Algoritam A iz [Meie89], odnosno algoritam za dekodiranje linearnih kodova iz [LeeB88]) u svaki ciklus Algoritma B [Meie89], može se izvršiti kao u narednom algoritmu za dekodiranje kodova $R_{h,n}$. Pri tome su polazni algoritmi pretrpeli još neke izmene, koje će naknadno biti komentarisane.

Algoritam 2.1 *(Kombinovani algoritam)* Dekodiranje koda $R_{h,n}$.
Ulaz: prirodni brojevi n, k, polinom $h(z) \in \mathrm{GF}(2)[z]$ stepena k, primljena poruka $\mathbf{y} \in B_n$, verovatnoća prelaza BSK p.
Izlaz: kodna reč $\mathbf{x} \in R_{h,n}$ koja se nalazi na najmanjem Hemingovom rastojanju od vektora y.
Kao tipične vrednosti parametara algoritma mogu se usvojiti $\alpha = 5$ (gornja granica za broj iteracija u jednom ciklusu), $w = 1$ (dubina pretrage okoline informacionog skupa, videti tačku 3.2), $\alpha_1 = 10$ (gornja

granica za broj slučajno izabranih informacionih skupova), $\alpha_c = 20$ (gornja granica za broj ciklusa). Postupak izbora vrednosti parametra k' izložen je u tački 4.1.

1^0 [Formiranje lokalnih kontrolnih matrica (LKM).] Korišćenjem Algoritma 3.1 i Algoritma 3.2 formirati matrice $\mathbf{H}^{(i)}$, $1 \leq i \leq n$.

2^0 [Matematičko očekivanje broja koordinata primljene poruke sa AVG većom od 1/2.] Izračunati sumu n_{thr} verovatnoća promene bita primljene poruke (videti tačku 3.3).

3^0 [Inicijalizacija brojača ciklusa.] $i_c \leftarrow 0$.

4^0 [Početak novog ciklusa, inicijalizacija brojača iteracija.] Staviti $i_c \leftarrow i_c + 1$, $j \leftarrow 0$ i za $1 \leq i \leq n$ staviti $p_j^{(0)} = p$.

5^0 [Naredna iteracija u okviru probabilističke faze ciklusa.] Polazeći od vektora $\mathbf{p}^{(j)}$ kao vektora apriornih verovatnoća greške, izračunati vektor $\mathbf{p}^{(j+1)}$ aposteriornih verovatnoća greške (korišćenjem vektora $\mathbf{y}$ i svih LKM, videti tačku 3.2). Izračunati broj n_w koordinata vektora $\mathbf{p}^{(j+1)}$ većih od 1/2.

6^0 [Poslednja iteracija ciklusa?] Ako je $n_w < n_{thr}$ i $j < \alpha$ (sem ako je $j = 1$) onda $j \leftarrow j + 1$, skok na 5^0.

7^0 [Komplementiranje bita primljene poruke sa AVG većom od 1/2.] Ako za svako i, $1 \leq i \leq n$, važi nejednakost $\mathbf{p}_i^{(j)} \leq 1/2$, onda je dekodiranje završeno neuspehom. U protivnom za $1 \leq i \leq n$ ako je $\mathbf{p}_i^{(j)} > 1/2$, staviti $y_i \leftarrow 1 \oplus y_i$ i $\mathbf{p}_i^{(j)} \leftarrow 1 - \mathbf{p}_i^{(j)}$.

8^0 [Početak faze pretrage: formiranje skupa koordinata sa malom AVG; inicijalizacija brojača informacionih skupova.] Formirati uređeni skup $\mathbf{l}' = (l'_1, l'_2, \ldots, l'_{k'})$ od $k' > k$ indeksa najmanjih koordinata vektora $\mathbf{p}^{(j)}$ tako da je rang $\mathbf{G}_{\mathbf{l}'} = k$; $i_1 \leftarrow 0$.

9^0 [Formiranje slučajnog informacionog skupa.] Formirati slučajni podskup $\mathbf{l} = (l_1, l_2, \ldots, l_k) \in \mathbf{l}'$ takav da je rang $\mathbf{G}_{\mathbf{l}'} = k$ i izračunati matricu $\mathbf{G}_{\mathbf{l}'}^{-1}$ (Algoritam 4.1); $i_c \leftarrow i_c + 1$.

10^0 [Pokušaj ispravke najviše w grešaka među koordinatama vektora $\mathbf{y}$ sa indeksima iz informacionog skupa $\mathbf{I}$, videti tačku 4.3, odnosno Algoritam 4.2.] Ako neka kodna reč $\mathbf{x}^*$ iz skupa

$$\{\mathbf{x} \in R_{h,n} \mid \mathrm{dist}\,(\mathbf{x}_\mathbf{I}, \mathbf{y}_\mathbf{I}) \leq w\}$$

zadovoljava uslov

$$\mathrm{dist}\,(\mathbf{x}^*, \mathbf{y}) < d_0 = np + 3\sqrt{np(1-p)}$$

(videti (4.3)), tada je $\hat{\mathbf{x}} = \mathbf{x}^*$, kraj; u protivnom, ako je $i_1 < \alpha_1$, skok na 9^0.

11^0 [Neuspeh u fazi pretrage; naredni ciklus algoritma.] Ako je $i_c < \alpha_c$, skok na 4^0; u protivnom — kraj, neuspešno dekodiranje. □

Kao i u algoritmima iz [Meie89] i ovde se mora pretpostaviti da je n dovljno veliko (videti tačku 4.2), jer se u protivnom može desiti da algoritam prihvati kao rešenje kodnu reč različitu od one koja je dovedena na ulaz BSK.

Opisani algoritam sastoji se od pripremnog dela (koraci 1^0–3^0) i određenog broja α_c ciklusa (koraci 4^0–11^0). Parametar α_c može imati proizvoljnu vrednost, a ograničen je samo vremenom izvršavanja algoritma. Svaki ciklus algoritma sastoji se od probabilističke faze, (koraci 5^0–7^0) koja odgovara Algoritmu B, i faze pretrage (dekodiranje pomoću informacionih skupova, koraci 8^0–10^0), koja odgovara Algoritmu A.

Za formiranje LKM $\mathbf{H}^{(i)}$, $1 \leq i \leq n$, koristi se Algoritam 3.1, koji koristi činjenicu da postoje intervali za indeks i unutar kojih su LKM identične do na translaciju. Pored toga, u slučaju kad sistem kontrola parnosti sadržan u LKM nije ortogonalan, pomoću Algoritma 3.2 formiraju se LKM maksimalnih dimenzija tako da numerička složenost izračunavanja AVG u koraku 5^0 (primenom Teoreme 3.2) bude manja od zadate granice. Slučaj kad sistem kontrola parnosti obuhvaćenih LKM nije ortogonalan nije razmatran u radu [Meie89], iako je jasno da ovi sistemi kontrola parnosti mogu da budu ortogonalni samo za male vrednosti m.

Umesto praga p_{thr} (1.12) za izračunavanje očekivanog broja koordinata kojima je AVG veća od praga, koristi se prag 1/2 (koraci

2^0 i 7^0). Ovo se može obrazložiti time što je, posle komplementiranja bita sa AVG većom od nekog praga, matematičko očekivanje broja pogrešnih bita najveće ako je prag jednak 1/2. Zbog toga što se prag p_{thr} u [Meie89] računa približno, u Algoritmu B se pojavljuje mogućnost da se komplementiranjem bita kojima je AVG veća od praga poveća matematičko očekivanje broja pogrešnih bita. Nasuprot tome, u tački 3.3 se jednostavno pokazuje da se matematičko očekivanje broja pogrešnih bita na ovaj način ne može povećati ukoliko se koristi prag 1/2.

Sva izračunavanja u algoritmu izvode se sa algebarskim vrednostima $\ln((1-p)/p)$ umesto sa samim verovatnoćama p. Time je povećana tačnost izračunavanja u slučajevima kad su verovatnoće bliske nuli ili jedinici (videti Teoremu 3.4), što ima za posledicu efikasnije odvajanje bita manje *nepouzdanosti* (videti tačku 4.1).

Faza pretrage je nešto složenija od Algoritma A, jer su primenjene neke ideje iz drugih radova, posebno [LeeB88,Dors74]. Slučajno se bira više informacionih skupova, čiji indeksi su iz skupa indeksa koordinata sa malom nepouzdanošću. Pri tome se koristi činjenica da se bez posledica mogu istovremeno komplementirati bilo koja AVG i odgovarajući bit primljene poruke, videti tačku 3.2.

Granica za broj ispravki na informacionom skupu, *dubinu pretrage*, bira se tako da se (slično kao u radu [LeeB88]) optimizira verovatnoća uspešnog dekodiranja (videti tačku 4.3).

Poglavlje 3

Kombinovani algoritam: probabilistička faza

Aposteriorne verovatnoće greške bita primljene poruke izračunavaju se na osnovu određenog broja kontrola parnosti, koje u opštem slučaju ne predstavljaju bazu koda dualnog kodu $R_{h,n}$. Izračunavanje AVG na osnovu kompletne kontrolne matrice koda $R_{h,n}$ gotovo uvek ima neprihvatljivo veliku numeričku složenost.

Definicija 3.1 *Neka je i proizvoljni fiksirani indeks,* $1 \leq i \leq n$. *Lokalna kontrolna matrica (LKM) za koordinatu sa indeksom i linearnog* (n, k) *koda* C *je proizvoljna matrica* $\mathbf{H}^{(i)}$ *čije su vrste jednake nekim (linearno nezavisnim) kodnim rečima koda dualnog kodu* C, *pri čemu su svi elementi u i–toj vrsti ove matrice jednaki jedinici.*

Ovako definisane LKM korišćene su na primer u [Batt79] za izračunavanje AVG. Sa aspekta numeričke složenosti izračunavanja AVG posebno je interesantan slučaj kad su LKM $\mathbf{H}^{(i)}$ formirane od kontrola parnosti ortogonalnih u odnosu na i–tu koordinatu kodne reči, $1 \leq i \leq n$. Kontrole parnosti sa malim brojem članova su korisne, jer omogućuju postizanje pouzdanije ocene tačnosti pojedinih bita primljene poruke [Gall62].

U ovom poglavlju se najpre razmatra postupak za formiranje svih LKM za kod $R_{h,n}$ (tačka 3.1), a zatim problemi efikasnosti i tačnosti izračunavanja AVG (tačka 3.2). Verovatnoća pogrešnog odlučivanja o

bitu greške na osnovu AVG, *verovatnoća zaostale greške*, analizirana je u tački 3.3. Formulacija i dokaz dovoljnog uslova za konvergenciju niza vektora koji određuju raspodelu verovatnoća na skupu B_n (korak 5^0 Algoritma 2.1) dati su u tački 3.4. Ovaj rezultat omogućuje eksperimentalnu analizu probabilističke faze kao zasebnog algoritma za dekodiranje.

3.1 Formiranje lokalnih kontrolnih matrica

AVG bita primljene poruke izračunavaju se kao i u [Meie89] samo na osnovu kontrola parnosti oblika (1.5), izvedenih iz osnovne LRR koda $R_{h,n}$. U ovoj tački biće detaljnije izložen algoritam za formiranje lokalnih kontrolnih matrica (LKM) za svaku koordinatu primljene poruke. Predloženi algoritam je pogodan u slučaju kad je veliki odnos n/k, jer se koristi činjenica da su tada LKM za neke grupe koordinata kodne reči sličnog oblika. Dokazano je da LKM formirane na ovaj način imaju linearno nezavisne vrste ako je polinom $h(z)$ nesvodljiv (Teorema 3.1). Na kraju je dat heuristički algoritam za nalaženje LKM kao podmatrice (maksimalne LKM) sa najvećim brojem vrsta, takve da je numerička složenost izračunavanja AVG pomoću nje (ako se koristi Teorema 3.2 iz naredne tačke) manja od zadate gornje granice.

Ako se sa I_h označi skup eksponenata članova polinoma $h(z) \in \mathrm{GF}(2)[z]$, tj.

$$I_h = \{i \mid 0 \le i \le k,\ h_i \neq 0\},$$

tada se jednakost (1.5) može napisati u obliku

$$\bigoplus_{\lambda \in I_h} x_{j+\lambda 2^\nu} = 0, \qquad \nu \ge 0,\ 1 \le j \le n - k2^\nu. \tag{3.1}$$

Sve kontrole parnosti ovog oblika imaju isti broj $m+1$ članova, jednak broju članova polinoma $h(z)$.

Neka je za $1 \le i \le n$ sa $\mathcal{H}_i$ označen skup parova celih brojeva

$$\mathcal{H}_i = \{(\nu, \lambda) \mid \nu \ge 0,\ \lambda \in I_h,\ (\forall l \in I_h)(1 \le i + (l-\lambda)2^\nu \le n)\},$$

i neka je

$$\nu_{max} = \left[\mathrm{ld}\,\frac{n-1}{k}\right],$$

gde je sa ld označen logaritam za osnovu dva. Lako se pokazuje da je

$$\max\left\{\nu \mid (\nu,\lambda) \in \bigcup_{i=1}^{n} \mathcal{H}_i\right\} = \nu_{max}.$$

Zaista, očigledno je $(\nu_{max}, 0) \in \mathcal{H}_i$ za $i = 1$, jer je $1 + k2^{\nu_{max}} \leq n$. S druge strane, za $\nu > \nu_{max}$ i proizvoljno $\lambda \in I_h$ zbog

$$(i + (k-\lambda)2^{\nu}) - (i + (0-\lambda)2^{\nu}) = k2^{\nu} \geq$$

$$\geq k2^{\nu_{max}+1} = 2k2^{[\mathrm{ld}\,((n-1)/k)]} > 2k2^{\mathrm{ld}\,((n-1)/k)-1} = n-1$$

dobija se da je

$$(\nu,\lambda) \notin \bigcup_{i=1}^{n} \mathcal{H}_i.$$

Neka je fiksiran indeks i, $1 \leq i \leq n$. Svakom paru $(\nu,\lambda) \in \mathcal{H}_i$ odgovara tačno jedna kontrola parnosti

$$\bigoplus_{l \in I_h} x_{i+(l-\lambda)2^{\nu}} = 0 \tag{3.2}$$

oblika (3.1) koja sadrži koordinatu x_i kodne reči. Prema tome, LKM $\mathbf{H}^{(i)}$ je jednoznačno određena skupom $\mathcal{H}_i$.

Uslovi koje zadovoljavaju parovi $(\nu,\lambda) \in \mathcal{H}_i$ mogu se transformisati u jednostavniji oblik. Uslov $(\forall l \in I_h)\,(1 \leq i + (l-\lambda)2^{\nu} \leq n)$ je zadovoljen ako i samo ako je

$$i + (k-\lambda)2^{\nu} \leq n, \quad i + (0-\lambda)2^{\nu} \geq 1, \tag{3.3}$$

odnosno

$$k - \frac{n-i}{2^{\nu}} \leq \lambda \leq \frac{i-1}{2^{\nu}}, \qquad \lambda \in I_h.$$

Zbog toga se skup $\mathcal{H}_i$ može ekvivalentno definisati jednakošću

$$\mathcal{H}_i = \left\{(\nu,\lambda) \mid 0 \leq \nu \leq \nu_{max},\ \lambda \in I_h,\ k - \frac{n-i}{2^{\nu}} \leq \lambda \leq \frac{i-1}{2^{\nu}}\right\}.$$

Skup $\mathcal{H}_i$ je očigledno podskup skupa

$$\mathcal{H}' = \{(\nu, \lambda) \mid 0 \leq \nu \leq \nu_{max},\ \lambda \in I_h\}.$$

koji ima

$$\rho = (m+1)(\nu_{max}+1), \tag{3.4}$$

elemenata. Broj vrsta u matrici $\mathbf{H}^{(i)}$ jednak je broju elemenata skupa $\mathcal{H}_i$ i nije veći od ρ.

Postupak formiranja LKM biće ilustrovan jednim primerom.

Primer 3.1 Neka je $h(z) = 1 + z^3 + z^7$ i $n = 16$. Dimenzija koda $R_{h,n}$ je $k = 7$. Da bi se formirala matrica $\mathbf{H}^{(8)}$ od kontrola parnosti oblika (3.2) koje obuhvataju koordinatu x_8 kodne reči $\mathbf{x}$, treba formirati skup $\mathcal{H}_8$ parova (ν, λ) koji zadovoljavaju uslove

$$0 \leq \nu \leq \nu_{max} = \left[\mathrm{ld}\,\frac{16-1}{7}\right] = 1$$

i

$$7 - \frac{16-8}{2^\nu} \leq \lambda \leq \frac{8-1}{2^\nu}, \qquad \lambda \in I_h = \{0,3,7\}.$$

Za $\nu = 0$ moguće vrednosti za λ su $0, 3$ i 7, a za $\nu = 1$ ovi uslovi zadovoljeni su samo za vrednost $\lambda = 3$. Skupu $\mathcal{H}_8 = \{(0,0),(0,3),(0,7),(1,3)\}$ odgovara skup kontrola parnosti

$$\begin{aligned} x_8 \oplus x_{11} \oplus x_{15} &= 0 \\ x_5 \oplus x_8 \oplus x_{12} &= 0 \\ x_1 \oplus x_4 \oplus x_8 &= 0 \\ x_2 \oplus x_8 \oplus x_{16} &= 0 \end{aligned}$$

Od ovih kontrola parnosti direktno se formira LKM $\mathbf{H}^{(8)}$,

$$\mathbf{H}^{(8)} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Dobijeni skup kontrola parnosti je u ovom slučaju ortogonalan u odnosu na koordinatu x_8. □

U navedenom primeru LKM ima dosta veliki broj kolona koje su nula–vektori. U opštem slučaju broj koordinata kodne reči obuhvaćenih kontrolama parnosti iz LKM $\mathbf{H}^{(i)}$, odnosno broj kolona LKM različitih od nula–vektora, nije veći od

$$1 + \rho m = 1 + m(m+1)\left[\mathrm{ld}\,\frac{n-1}{k}\right].$$

Zbog toga, ako je

$$m \ll \sqrt{n/\mathrm{ld}\,(n/k)}$$

onda je veliki deo kolona LKM jednak nula–vektoru. Tada se dimenzije LKM efektivno smanjuju, jer koordinate primljene poruke kojima u LKM odgovaraju nula–vektori ne utiču na izračunavanje AVG.

Postupak formiranja LKM $\mathbf{H}^{(i)}$ sličan je za neke vrednosti indeksa i, jer su jednaki odgovarajući skupovi $\mathcal{H}_i$. Ova činjenica se može iskoristiti za uprošćenje postupka formiranja svih LKM. Fiksirani par $(\nu, \lambda) \in \mathcal{H}'$ pripada skupu $\mathcal{H}_i$ ako i samo ako je zadovoljen sistem nejednakosti (3.3), odnosno

$$1 + \lambda 2^{\nu} \leq i \leq n - (k - \lambda)2^{\nu}.$$

Za ovaj par (ν, λ) i za svaku vrednost indeksa i iz ovog intervala dobija se tačno jedna kontrola parnosti (3.2). Nanošenjem ovakvih ρ intervala na interval $[1, n]$, dobija se njegova podela na podintervale u kojima je skup $\mathcal{H}_i$ konstantan. Ako je za neko i, $1 \leq i \leq n$, $\mathcal{H}_i = \mathcal{H}_{i+1}$, tada je $\mathbf{H}_n^{(i+1)} = \mathbf{0}$ i $\mathbf{H}_j^{(i+1)} = \mathbf{H}_{j-1}^{i}$ za $2 \leq j \leq n$. Drugim rečima, matrica $\mathbf{H}^{(i+1)}$ dobija se od matrice $\mathbf{H}^{(i)}$ translacijom kolona udesno, odnosno, može se reći da su ove dve matrice identične do na translaciju. Dakle, dovoljno je formirati samo po jednu LKM u svakom od podintervala.

Broj podintervala intervala $[1, n]$ nije veći od $2\rho + 1$. Preciznija gornja granica za broj podintervala je $1 + 2m(\nu_{max} + 1)$, jer je donja granica intervala $1 + \lambda 2^{\nu}$ jednaka 1 za sve parove $(\nu, 0)$, $0 \leq \nu \leq \nu_{max}$, a gornja granica $n - (k - \lambda)2^{\nu}$ jednaka je n za sve parove (ν, k), $0 \leq \nu \leq \nu_{max}$. Postupak podele intervala $[1, n]$ na podintervale biće ilustrovan jednim primerom.

Primer 3.2 *(nastavak primera 3.1)* Skup

$$\mathcal{H}' = \{(0,0), (0,3), (0,7), (1,0), (1,3), (1,7)\}$$

Kontrola parnosti	Vrednosti indeksa i															
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$x_i \oplus x_{i+3} \oplus x_{i+7} = 0$	•	•	•	•	•	•	•	•	•							
$x_{i-3} \oplus x_i \oplus x_{i+4} = 0$				•	•	•	•	•	•	•	•	•				
$x_{i-7} \oplus x_{i-4} \oplus x_i = 0$								•	•	•	•	•	•	•	•	•
$x_i \oplus x_{i+6} \oplus x_{i+14} = 0$	•	•														
$x_{i-6} \oplus x_i \oplus x_{i+8} = 0$							•	•								
$x_{i-14} \oplus x_{i-8} \oplus x_i = 0$															•	•

Tabela 3.1: Primer formiranja intervala sa konstantnim skupovima kontrola parnosti

ima na osnovu (3.4) $\rho = (1+1)(1+2) = 6$ elemenata. Elementu $(0,0) \in \mathcal{H}'$ odgovaraju kontrole parnosti $x_i \oplus x_{i+3} \oplus x_{i+7} = 0$ oblika (3.2), pri čemu i leži u intervalu $[1+0\times 2^0, 16-(7-0)\times 2^0] = [1,9]$. Na sličan način, elementu $(0,3) \in \mathcal{H}'$ odgovaraju kontrole parnosti $x_{i-3} \oplus x_i \oplus x_{i+4} = 0$, pri čemu je $i \in [4,12]$. Intervali koji odgovaraju elementima skupa $\mathcal{H}'$ pregledno su prikazani u Tabeli 3.1. Interval $[1,16]$ je tako podeljen na devet podintervala, $[1,2]$, $[3,3]$, $[4,6]$, $[7,7]$, $[8,8]$, $[9,9]$, $[10,12]$, $[13,14]$ i $[15,16]$, takvih da su u svakome od njih skupovi $\mathcal{H}_i$ konstantni. Na primer, za $i \in [10,12]$ je $\mathcal{H}_i = \{(0,3),(0,7)\}$, što znači da se matrica $\mathbf{H}^{(i)}$ formira od kontrola parnosti $x_{i-3} \oplus x_i \oplus x_{i+4} = 0$ i $x_{i-7} \oplus x_{i-4} \oplus x_i = 0$. Broj podintervala upravo je jednak gornjoj granici $1 + 2m(\nu_{max}+1) = 9$. □

U opštem slučaju se podela intervala $[1,n]$ na podintervale sa konstantnim skupovima $\mathcal{H}_i$, kao i formiranje ovih skupova, može izvršiti korišćenjem sledećeg algoritma.

Algoritam 3.1 Podela intervala $[1,n]$ na podintervale sa konstantnim skupovima $\mathcal{H}_i$ i formiranje ovih skupova.
Ulaz: prirodni brojevi n, k, $n \geq k$ i polinom $h(z) \in \mathrm{GF}(2)[z]$ stepena k.
Izlaz: donje i gornje granice podintervala za indeks i, $1 \leq i \leq n$, u kojima su konstantni skupovi $\mathcal{H}_i$, i skup $\mathcal{H}_i$ za svaki podinterval.

1^0 [Izračunavanje granica podintervala koji odgovaraju pojedninim parovima $(\nu,\lambda) \in \mathcal{H}'$. Skup $\mathcal{H}'$ parova (ν,λ) uređen je prema rastućim vrednostima ν, a u grupama sa istom vrednošću ν prema

rastućim vrednostima λ. Niz $\{g_j\}$ sadrži granice podintervala, niz $\{t_j\}$ sadrži podatke o tome da li su odgovarajući elementi niza $\{g_j\}$ donje ili gornje granice, a j je redni broj para (ν, λ) u skupu $\mathcal{H}'$, $1 \le j \le \rho$ (3.4).] Za svako $(\nu, \lambda) \in \mathcal{H}'$ staviti $j \leftarrow \nu(m+1) + \mathrm{ord}(\lambda, I_h)$, $g_{2j-1} \leftarrow 1 + \lambda 2^\nu$, $t_{2j-1} \leftarrow 1$, $\nu_{2j-1} \leftarrow \nu$, $\lambda_{2j-1} \leftarrow \lambda$, $g_{2j} \leftarrow n - (k-\lambda)2^\nu + 1$, $t_{2j} \leftarrow -1$, $\nu_{2j} \leftarrow \nu$, $\lambda_{2j} \leftarrow \lambda$. Ovde $\mathrm{ord}(\lambda, I_h)$ označava rang (redni broj) elementa λ u rastuće uređenom skupu I_h.

2^0 [Sortiranje granica.] Urediti niz brojeva $g_1, g_2, \ldots, g_{2\rho}$ po veličini. Neka je dobijen niz $1 = g'_1 \le g'_2 \le \ldots \le g'_{2\rho} = n$. Neka su dalje nizovi $t'_1, t'_2, \ldots, t'_{2\rho}$, $\nu'_1, \nu'_2, \ldots, \nu'_{2\rho}$ i $\lambda'_1, \lambda'_2, \ldots, \lambda'_{2\rho}$ dobijeni od nizova $t_1, t_2, \ldots, t_{2\rho}$, $\nu_1, \nu_2, \ldots, \nu_{2\rho}$ i $\lambda_1, \lambda_2, \ldots, \lambda_{2\rho}$ primenom iste permutacije koja niz $g_1, g_2, \ldots, g_{2\rho}$ prevodi u niz $g'_1, g'_2, \ldots, g'_{2\rho}$.

3^0 [Formiranje skupova $\mathcal{H}_i$, $0 \le i \le n$, odnosno skupova kontrola parnosti za pojedine podintervale.] Staviti $\mathcal{H}'_0 \leftarrow \emptyset$, a zatim za $j = 1(1)2\rho$ staviti

$$\mathcal{H}'_j = \begin{cases} \mathcal{H}'_{j-1} \cup \{(\nu'_j, \lambda'_j)\}, & t_j = 1 \\ \mathcal{H}'_{j-1} \setminus \{(\nu'_j, \lambda'_j)\}, & t_j = -1 \end{cases}.$$

Neka je $g'_{2\rho+1} = n + 1$. Tada je

$$\mathcal{H}_i = \mathcal{H}'_j, \qquad g'_j \le i \le g'_{j+1} - 1,\ 1 \le j \le 2\rho. \qquad \square$$

Desne granice podintervala povećane su za jedan, tako da oni ne sadrže svoje desne granice. Lako se proverava da je u koraku 1^0 algoritma $g_1 = 1$ i $g_{2\rho} = n + 1$. Zbog toga je i $g'_1 = 1$ i $g'_{2\rho} = n + 1$, pa je unija nepraznih intervala $[g'_j, g'_{j+1} - 1]$, $1 \le j \le 2\rho$, jednaka intervalu $[1, n]$. Sledeći primer ilustruje primenu algoritma.

Primer 3.3 *(Nastavak primera 3.2)* U koraku 1^0 algoritma formiraju se nizovi $\{g_j\}$, $\{t_j\}$, $\{\nu_j\}$ i $\{\lambda_j\}$:

j	1	2	3	4	5	6	7	8	9	10	11	12
g_j	1	10	4	13	8	17	1	3	7	9	15	17
t_j	1	−1	1	−1	1	−1	1	−1	1	−1	1	−1
ν_j	0	0	0	0	0	0	1	1	1	1	1	1
λ_j	0	0	3	3	7	7	0	0	3	3	7	7

Sortiranjem kolona ove tablice prema rastućim vrednostima elemenata g_j, u koraku 2^0 algoritma dobijaju se nizovi $\{g'_j\}$, $\{t'_j\}$, $\{\nu'_j\}$ i $\{\lambda'_j\}$:

j	1	2	3	4	5	6	7	8	9	10	11	12
g'_j	1	1	3	4	7	8	9	10	13	15	17	17
t'_j	1	1	−1	1	1	1	−1	−1	−1	1	−1	−1
ν'_j	0	1	1	0	1	0	1	0	0	1	0	1
λ'_j	0	0	0	3	3	7	3	0	3	7	7	7

Konačno, u koraku 3^0 algoritma dobijaju se skupovi $\mathcal{H}_i$ za pojedine podintervale na koje se razbija interval $[1, 16]$:

j	interval	t_j	$\mathcal{H}'_j = \mathcal{H}_i$
1	$[1,0]$	1	$\{(0,0)\}$
2	$[1,2]$	1	$\{(0,0),(1,0)\}$
3	$[3,3]$	−1	$\{(0,0)\}$
4	$[4,6]$	1	$\{(0,0),(0,3)\}$
5	$[7,7]$	1	$\{(0,0),(0,3),(1,3)\}$
6	$[8,8]$	1	$\{(0,0),(0,3),(1,3),(0,7)\}$
7	$[9,9]$	−1	$\{(0,0),(0,3),(0,7)\}$
8	$[10,12]$	−1	$\{(0,3),(0,7)\}$
9	$[13,14]$	−1	$\{(0,7)\}$
10	$[15,16]$	1	$\{(0,7),(1,7)\}$
11	$[17,16]$	−1	$\{(1,7)\}$
12	$[17,16]$	−1	$\emptyset$

Kao što se moglo i očekivati, dobijen je isti rezultat kao i u prethodnom primeru. □

U koraku 1^0 algoritma izračunava se najviše 2ρ granica intervala, što zahteva izvršavanje $O(\rho)$ operacija (celobrojnih sabiranja, oduzimanja i množenja). Sortiranje vektora u koraku 2^0 može se najjednostavnijim algoritmom izvršiti pomoću $O(\rho^2)$ operacija. Formiranje jednog skupa $\mathcal{H}'_j$ u koraku 3^0 zahteva najviše $O(\rho)$ operacija. Konačno, najviše $1 + 2m(\nu_{max} + 1) < 2\rho$ matrica $\mathbf{H}^{(i)}$ (po jedna u svakom podintervalu intervala $[1, n]$) može se formirati pomoću najviše $O(2\rho \times \rho n)$ operacija. Ukupno je dakle za formiranje svih LKM potrebno izvršiti ne više od $O(m^2 n \log^2 \frac{n}{k})$ operacija. Numerička složenost ovog algoritma, kao što

se vidi, nije velika. Prednost korišćenja ovog algoritma ispoljava se i prilikom izračunavanja AVG na osnovu uprošćene (na osnovu Teoreme 3.2) LKM: dovoljno je izvršiti transformaciju samo jedne LKM iz svakog podintervala formiranog u Algoritmu 3.1.

Polinom $h(z)$ stepena k je *simetričan* ako je $h(z) = z^k h(1/z)$. U vezi sa LKM formiranom na opisani način, postavlja se pitanje može li se dogoditi da neke njene vrste budu linearno zavisne. Odgovor na ovo pitanje daje sledeća teorema.

Teorema 3.1 *Pretpostavimo da je stepen k karakterističnog polinoma $h(z)$ koda $R_{h,n}$ neparan, ili, ako je k parno, da polinom $h(z)$ nije simetričan. Tada su vrste LKM formirane od kontrola parnosti oblika (3.2) linearno nezavisne.*

DOKAZ. Pokazaćemo da su kontrole parnosti (3.2) koje odgovaraju parovima $(\nu, \lambda) \in \mathcal{H}'$ linearno nezavisne, iz čega sledi da su one linearno nezavisne i ako je $(\nu, \lambda) \in \mathcal{H}_i \subset \mathcal{H}'$ za proizvoljno i, $1 \leq i \leq n$. Kontrole parnosti (3.2) koje odgovaraju parovima $(\nu, \lambda) \in \mathcal{H}'$ linearno su nezavisne ako i samo ako su linearno nezavisni polinomi

$$\bigoplus_{l=0}^{k} h_l z^{(l-\lambda)2^\nu} = z^{-\lambda 2^\nu} h(z^{2^\nu}), \qquad 0 \leq \nu \leq \nu_{max},\ \lambda \in I_h.$$

Ovi polinomi su linearno nezavisni ako i samo ako ne postoje koeficijenti $\alpha_{\nu,\lambda}$, $(\nu, \lambda) \in \mathcal{H}'$, od kojih je bar jedan različit od nule, takvi da je

$$\bigoplus_{\nu=0}^{\nu_{max}} h(z^{2^\nu}) \bigoplus_{\lambda \in I_h} \alpha_{\nu,\lambda} z^{-\lambda 2^\nu} \equiv 0,$$

odnosno

$$\bigoplus_{\nu=0}^{\nu_{max}} h(z^{2^\nu}) \bigoplus_{l=0}^{k} \alpha_{\nu,l} z^{-l 2^\nu} \equiv 0,$$

gde je $\alpha_{\nu,l} = 0$ za $l \notin I_h$, $0 \leq \nu \leq \nu_{max}$. Ako sa g_ν označimo polinom $\bigoplus_{l=0}^{k} \alpha^{\nu,l} z^l$ stepena k, onda se poslednji identitet može napisati u obliku

$$\bigoplus_{\nu=0}^{\nu_{max}} h(z^{2^\nu}) g_\nu(z^{-2^\nu}) \equiv 0. \tag{3.5}$$

Pretpostavimo da je bar jedan koeficijenat polinoma $g_{\nu_{max}}(z)$ različit od nule (ako to nije tačno, onda se sa ν_{max} može označiti najveći broj ν takav da je bar jedan koeficijenat polinoma $g_\nu(z)$ različit od nule). Polinom

$$\bigoplus_{\nu=0}^{\nu_{max}-1} h(z^{2^\nu}) g_\nu(z^{-2^\nu})$$

ima članove stepena između $-k2^{\nu_{max}-1}$ i $k2^{\nu_{max}-1}$. Neka su sa l_{min} i l_{max} označeni najmanji i najveći stepen nekog člana polinoma $g_{\nu_{max}}(z)$. Proizvod

$$h(z^{2^{\nu_{max}}}) g_{\nu_{max}}(z^{-2^{\nu_{max}}})$$

ima članove stepena između $-l^{max}2^{\nu_{max}}$ i $(k - l_{min})2^{\nu_{max}}$, jer se pretpostavlja da polinom $h(z)$ ima članove stepena 0 i k. Zbog identiteta (3.5) mora da bude $-l^{max}2^{\nu_{max}} \geq -k2^{\nu_{max}-1}$ i $(k - l_{min})2^{\nu_{max}} \leq k2^{\nu_{max}-1}$, odnosno $2l_{max} \leq k$ i $2l_{min} \geq k$, i konačno $l_{min} = l_{max} = k/2$. Za neparno k ovo je nemoguće, što znači da je za neparno k tvrđenje teoreme dokazano. Lako se proverava da je identitet (3.5) nemoguć i ako je $\nu_{max} = 0$.

Razmotrimo sada slučaj kad je k parno, $k = 2k_1$, i $\nu_{max} \geq 1$. Tada je $g_{\nu_{max}}(z) = z^{k_1}$, a identitet (3.5) postaje

$$z^{-k_1 2^{\nu_{max}}} h(z^{2^{\nu_{max}}}) \oplus \bigoplus_{\nu=0}^{\nu_{max}-1} h(z^{2^\nu}) g_\nu(z^{-2^\nu}) \equiv 0. \qquad (3.6)$$

Za $\nu_{max} = 1$ ovaj identitet svodi se na

$$z^{-2k_1} h(z^2) \oplus h(z) g_0(z^{-1}) \equiv 0,$$

odnosno zbog $h(z^2) = (h(z))^2$,

$$h(z) \left(z^{-k} h(z) \oplus g_0(z^{-1}) \right) \equiv 0.$$

Odavde se dobija da je $g_0(z) = z^k h(z^{-1})$. Polinom $h(z)$ po pretpostavci nije simetričan, pa postoji bar jedno l', $0 < l' < k$ takvo da je $h_{l'} = 0$, $h_{k-l'} = 1$ i $l' \notin I_h$. Međutim, tada je $\alpha_{0,l'} = 1$, suprotno pretpostavci o koeficijentima polinoma $g_0(z)$ ($\alpha_{0,l} = 0$ za svako l, $l \notin I_h$).

Preostalo je da se razmotri slučaj $\nu_{max} \geq 2$. Smenom

$$g_{\nu_{max}-1}(z) = z^k h(z^{-1}) \oplus \varphi(z),$$

gde je $\varphi(z)$ polinom stepena ne većeg od k, identitet (3.6) postaje

$$\varphi(z^{-2^{\nu_{max}-1}}h(z^{2^{\nu_{max}-1}}) \oplus \bigoplus_{\nu=0}^{\nu_{max}-2} h(z^{2^\nu})g_\nu(z^{-2^\nu}) \equiv 0.$$

Sličnim rezonovanjem kao kod identiteta (3.5) odavde se dobija da je $\varphi(z) = uz^{k_1}$, $u \in B$, i $g_{\nu_{max}-1}(z) = z^k h(z^{-1}) \oplus uz^{k_1}$. Međutim, ovo vodi kontradikciji, jer je $\alpha_{\nu_{max}-1,l'} = 1$, iako $l' \notin I_h$. Time je tvrđenje teoreme dokazano. □

Poznato je da simetrični polinom iz GF(2)[z] stepena većeg od dva ne može da bude nesvodljiv. Zbog toga važi sledeća posledica dokazane teoreme.

Posledica 3.1 *Ako je karakteristični polinom $h(z)$ koda $R_{h,n}$ nesvodljiv, onda su vrste LKM formirane od kontrola parnosti oblika (3.2) linearno nezavisne.* □

Iz razmatranja složenosti izračunavanja AVG korišćenjem LKM u narednoj tački sledi da je često potrebno kao LKM koristiti ne matrice dobijene pomoću Algoritma 3.1 (odnosno pomoću svih kontrola parnosti oblika (3.2)), nego matrice koje se od njih dobijaju izbacivanjem nekih vrsta. Numerička složenost izračunavanja AVG na osnovu LKM, videti (3.24), treba da bude ispod zadate granice, dok istovremeno broj kontrola parnosti treba da bude što je moguće veći. Ovaj kriterijum (što veći broj kontrola parnosti) je praktična zamena za pravi kriterijum, minimalnu *verovatnoću zaostale greške* (videti narednu tačku), odnosno maksimalno *smanjenje verovatnoće greške* (videti tačku 1.3). Uslov koji nameće ograničenje na numeričku složenost svodi se na uslov da veličina

$$\min(r+1, n-r-l)$$

bude manja od zadate gornje granice (na primer 10). Ovde je l jednako broju kolona u polaznoj (maksimalnoj) LKM koje se mogu izbaciti na osnovu Teoreme 3.2, jer su jednake nekoj drugoj koloni LKM. Formulisani optimizacioni problem vrlo je složen i može se rešavati jedino metodom heurističke pretrage, jer je u tipičnim slučajevima veliki broj podskupova skupa vrsta LKM.

Pre nego što bude izložen algoritam, potrebno je najpre definisati nekoliko pojmova (videti na primer [Nils71]). Skup koji se pretražuje,

prostor stanja, je familija podskupova skupa vrsta razmatrane LKM. Elementi prostora stanja su *čvorovi*. *Sledbenik čvora* je čvor čiji je podskup dobijen proširenjem polaznog čvora (kao podskupa) nekom novom kontrolom parnosti (vrstom maksimalne LKM). Od čvorova dostignutih u toku pretrage može se, vezivanjem čvorova za sledbenike, formirati stablo, tzv. *stablo pretrage*. Za svaki čvor definišu se njegova *vrednost*, jednaka broju elemenata odgovarajućeg podskupa i *složenost* $\min(r+1, n-r-l)$, gde su r i n dimenzije LKM formirane od izabranih vrsta, a l je broj kolona ove LKM koje su izbačene jer su jednake nekoj drugoj njenoj koloni.

Prilikom izvršenja algoritma pretrage koriste se dve liste, OPEN i CLOSED. Na listu OPEN zapisuju se dostignuti čvorovi. Čvorovi sa liste OPEN se posle *razvijanja* (stavljanja na listu OPEN svih sledbenika razvijanog čvora, koji već nisu na listi OPEN ili CLOSED) prebacuju na listu CLOSED. Cilj pretrage je naći čvor čija složenost nije veća od zadate granice, a čija vrednost je što je moguće veća.

Pre izvršenja algoritma treba fiksirati vrednosti nekih parametara (granica n_c za broj razvijanih čvorova, granica n_s za složenost čvorova). Sam algoritam je tipičan algoritam heurističke pretrage, videti [Nils71].

Algoritam 3.2 Nalaženje podmatrice date maksimalne LKM formirane od što većeg broja njenih vrsta, tako da numerička složenost izračunavanja AVG na osnovu nje bude manja od zadate granice n_s.
Ulaz: maksimalna LKM, granica n_s složenosti LKM.
Izlaz: podmatrica maksimalne LKM složenosti ne veće od n_s sa što je moguće većom cenom.
Parametri: granica n_c za broj razvijanih čvorova, granica n_s za složenost čvorova.

1^0 [Inicijalizacija lista OPEN i CLOSED.] Staviti prazan skup na listu OPEN, isprazniti listu CLOSED.

2^0 [Izbor čvora za razvijanje.] Izabrati sa liste OPEN neki od čvorova sa najvećom vrednošću (prvog na listi među njima) i prebaciti ga na listu CLOSED. Ukoliko je lista OPEN prazna ili je dostignuta granica n_c broja razvijenih čvorova, kraj, pri čemu je rešenje čvor najveće vrednosti sa liste OPEN ili CLOSED.

3^0 [Razvijanje izabranog čvora.] Sledbenike izabranog čvora koji nisu na listi OPEN ili CLOSED, a složenost im ne prelazi vrednost n_s, zapisati na listu OPEN (ukoliko na njoj ima još prostora), skok na 2^0; ako na listi OPEN nema više prostora, kraj, pri čemu je rešenje čvor najveće vrednosti sa liste OPEN ili CLOSED. □

3.2 Izračunavanje aposteriornih verovatnoća greške

Osnovni korak probabilističke faze Algoritma 2.1 je izračunavanje AVG svih koordinata primljene poruke korišćenjem odgovarajućih LKM. Numerička složenost izračunavanja AVG raste eksponencijalno sa dimenzijama LKM, pa je od interesa pronaći efikasnije algoritme za rešavanje ovog problema. Jedan takav algoritam biće izložen u ovoj tački. Pored toga, biće razmatran problem tačnog izračunavanja (izračunavanja sa malom greškom) u slučaju kad su apriorne verovatnoće greške bliske jedinici ili nuli.

Zbog jednostavnosti će u ovoj i narednoj tački sa **H** biti označavana LKM, pošto su iz nje prethodno izbačene kolone jednake nuli (nula-vektoru). Time su iz kodne reči, primljene poruke, kao i svakog vektora iz B_n isključene su koordinate koje ne učestvuju u bar jednoj kontroli parnosti sa izabranom (prvom, zbog jednostavnosti) koordinatom. Broj koordinata vektora posle skraćivanja biće u ovoj i narednoj tački označavan sa n. Dimenzija dobijenog linearnog koda biće označavana sa k. Pretpostavlja se da su vrste LKM **H** linearno nezavisne, videti Teoremu 3.1. Broj vrsta matrice **H** je $r = n - k$. Bez gubitka opštosti može se razmatrati izračunavanje AVG $\hat{p}_1$ prve koordinate primljene poruke, jer se izračunavanje AVG neke druge koordinate svodi na ovaj problem odgovarajućom permutacijom koordinata kodnih reči.

Neka je vektor greške slučajna promenljiva sa raspodelom verovatnoća

$$P\{\mathbf{E} = \mathbf{e}\} = \prod_{i=1}^{n} p_i^{e_i}(1-p_i)^{1-e_i}, \qquad \mathbf{e} \in B_n \tag{3.7}$$

određenom vektorom $\mathbf{p}$ apriornih verovatnoća greške (videti (1.1); ovde su verovatnoće jedinice za pojedine koordinate vektora $\mathbf{E}$ različite). U ovom izrazu sa koordinatama vektora $\mathbf{e}$ računa se kao sa odgovarajućim realnim brojevima. Neka je vektor $\mathbf{y}$ realizacija slučajne promenljive $\mathbf{Y} = \mathbf{x} \oplus \mathbf{E}$, gde je $\mathbf{x} \in R_{h,n}$ fiksirana kodna reč, koja je dovedena na ulaz kanala sa greškom. Prilikom izračunavanja AVG

$$\hat{p}_1 = P\left(\{E_1 = 1\} \mid \{\mathbf{HE} = \mathbf{Hy}\}\right) = \hat{p}_1(\mathbf{H}, \mathbf{y}, \mathbf{p})$$

na osnovu primljene poruke $\mathbf{y} \in B_n$, bez smanjenja opštosti može se pretpostaviti da koordinate vektora $\mathbf{p}$ zadovoljavaju uslov

$$0 \leq p_i \leq 1/2, \qquad 1 \leq i \leq n.$$

Pretpostavimo da vektor $\mathbf{p}$ ne zadovoljava ovaj uslov. Neka je vektor $\mathbf{d} \in B_n$ određen jednakostima

$$d_i = \begin{cases} 0, & p_i \leq 1/2 \\ 1, & p_i > 1/2 \end{cases}, \qquad 1 \leq i \leq n.$$

Definišimo slučajne promenljive $\mathbf{E}', \mathbf{Y}'$ i vektor $\mathbf{y}'$ jednakostima $\mathbf{E}' = \mathbf{E} \oplus \mathbf{d}$, $\mathbf{Y}' = \mathbf{Y} \oplus \mathbf{d}$ i $\mathbf{y}' = \mathbf{y} \oplus \mathbf{d}$. Tada je vektor $\mathbf{y}'$ realizacija slučajne promenljive $\mathbf{Y}' = \mathbf{x} \oplus \mathbf{E} \oplus \mathbf{d} = \mathbf{x} \oplus \mathbf{E}'$. Koordinate vektora $\mathbf{p}'$ koji određuje raspodelu verovatnoća slučajne promenljive $\mathbf{E}'$

$$P\{\mathbf{E}' = \mathbf{e}\} = \prod_{i=1}^{n} p_i'^{e_i}(1 - p_i')^{1-e_i}, \qquad \mathbf{e} \in B_n$$

zadovoljavaju očigledno uslov $0 \leq p_i' \leq 1/2,\ 1 \leq i \leq n$, jer je

$$p_i' = \begin{cases} p_i, & p_i \leq 1/2 \\ p_i', & p_i > 1/2 \end{cases}, \qquad 1 \leq i \leq n.$$

Izračunavanjem AVG

$$\hat{p}_1' = P\left(\{E_1' = 1\} \mid \{\mathbf{HE}' = \mathbf{Hy}'\}\right) = \hat{p}_1(\mathbf{H}, \mathbf{y}', \mathbf{p}')$$

direktno se dobija i AVG $\hat{p}_1'$, jer je

$$\begin{aligned} \hat{p}_1' &= P\left(\{E_1' = 1\} \mid \{\mathbf{HE}' = \mathbf{Hy}'\}\right) \\ &= P\left(\{E_1 \oplus d_1 = 1\} \mid \{\mathbf{HE} = \mathbf{Hy}\}\right) \\ &= \begin{cases} \hat{p}_1, & d_1 = 0 \\ 1 - \hat{p}_1, & d_1 \neq 0 \end{cases}. \end{aligned}$$

Iz ovog izraza sledi da ako se istovremeno komplementiraju neke koordinate vektora verovatnoća $\mathbf{p}$ i odgovarajuće koordinate vektora $\mathbf{y}$, tada se novi vektor AVG dobija od starog komplementiranjem istog skupa koordinata. Pod komplementiranjem realnog broja z ovde se podrazumeva njegova zamena brojem $1 - z$.

Neka je za dati vektor $\mathbf{s} \in B_r$ i $u \in B$ sa $C_{\mathbf{s},u}$ označen skup

$$C_{\mathbf{s},u} = \{\mathbf{e} \in B_n \mid \mathbf{He} = \mathbf{s},\ e_1 = u\}. \tag{3.8}$$

Uzimajući u obzir (1.2), očigledno je $C_{\mathbf{s},0} \cup C_{\mathbf{s},1} = C_{\mathbf{s}}$, odnosno skupovi $C_{\mathbf{s},0}$ i $C_{\mathbf{s},1}$ predstavljaju razlaganje koseta $C_{\mathbf{s}}$. Ako je $\mathbf{y} \in B_n$ primljena poruka, a $\mathbf{s} = \mathbf{Hy}$ odgovarajući sindrom, onda se AVG $\hat{p}_1$ može izračunati na osnovu jednakosti

$$\begin{aligned} \frac{1-\hat{p}_1}{\hat{p}_1} &= \frac{P\{E_1 = 0, \mathbf{HE} = \mathbf{s}\}}{P\{E_1 = 1, \mathbf{HE} = \mathbf{s}\}} = \frac{P\{\mathbf{E} \in C_{\mathbf{s},0}\}}{P\{\mathbf{E} \in C_{\mathbf{s},1}\}} \\ &= \frac{\sum_{\mathbf{e} \in C_{\mathbf{s},0}} P\{\mathbf{E} = \mathbf{e}\}}{\sum_{\mathbf{e} \in C_{\mathbf{s},1}} P\{\mathbf{E} = \mathbf{e}\}}. \end{aligned} \tag{3.9}$$

Pod pretpostavkom da je r vrsta matrice $\mathbf{H}$ linearno nezavisno, skup $C_{\mathbf{s},u}$ za proizvoljno $\mathbf{s} \in B_r$ ima $2^{n-r-1} = 2^{k-1}$ elemanata, pa je numerička složenost izračunavanja AVG na osnovu ovog izraza $O(n2^k)$ (oko $n2^k$ množenja, 2^k sabiranja i dva deljenja).

Za izračunavanje AVG postoji i drugi algoritam, čija je numerička složenost $O(n2^r)$. Najpre će biti definisana generatrisa koseta linearnog koda (videti na primer [Batt79]). Ako je $\mathbf{z} = (z_1, z_2, \ldots, z_r)$ vektorska promenljiva i $\mathbf{a} \in B_r$ vektor, neka je sa $\mathbf{z}^{\mathbf{a}}$ označen izraz

$$\mathbf{z}^{\mathbf{a}} = z_1^{a_1} z_2^{a_2} \ldots z_r^{a_r}.$$

Ovde je $z_i^{a_i}$ jednako z_i ako je $a_i = 1$, odnosno 1 ako je $a_i = 0$, $1 \leq i \leq r$. Neka je dalje sa $\otimes$ označena operacija množenja ovakvih izraza, distributivna u odnosu na sabiranje, takva da je za svako $\mathbf{a}, \mathbf{b} \in B_r$

$$\mathbf{z}^{\mathbf{a}} \otimes \mathbf{z}^{\mathbf{b}} = \mathbf{z}^{\mathbf{a} \oplus \mathbf{b}}.$$

Ako je $\mathbf{H}$ kontrolna matrica linearnog (n, k) koda, lako se pokazuje da je u izrazu

$$\bigotimes_{i=1}^{n} \left((1 - p_i) + p_i \mathbf{z}^{\mathbf{H}_i}\right) \tag{3.10}$$

koeficijenat uz $\mathbf{z}^{\mathbf{s}}$ jednak verovatnoći $P\{\mathbf{HE} = \mathbf{s}\}$ (videti [Batt79]). Na sličan način, verovatnoće $P\{\mathbf{HE} = \mathbf{s}, E_1 = 0\}$, odnosno $P\{\mathbf{HE} = \mathbf{s}, E_1 = 1\}$ jednake su koeficijentu uz $\mathbf{z}^{\mathbf{s}}$ u izrazu

$$(1 - p_1) \bigotimes_{i=2}^{n} \left((1 - p_i) + p_i \mathbf{z}^{\mathbf{H}_i} \right),$$

odnosno u izrazu

$$p_1 \mathbf{z}^{\mathbf{H}_1} \otimes \bigotimes_{i=2}^{n} \left((1 - p_i) + p_i \mathbf{z}^{\mathbf{H}_i} \right).$$

Razvijanje ovih izraza može se izvršiti množenjem član po član pomoću $O(n2^r)$ operacija (od čega oko $2n2^r$ realnih množenja), što znači da numerička složenost izračunavanja AVG ovim metodom nije veća od $O(n2^r)$.

Sledeća teorema [Živk90] pokazuje kako se može uprostiti izračunavanje AVG u slučaju kad LKM $\mathbf{H}$ ima nekoliko jednakih (nenultih) kolona.

Teorema 3.2 *Pretpostavimo da su kolone kontrolne matrice* $\mathbf{H}$ *linearnog* (n, k) *koda* C *sa indeksima iz skupa* $\mathbf{i} = \{i_1, i_2, \ldots, i_l\}$, $1 \notin \mathbf{i}$ *jednake. Neka je vektor* $\mathbf{y} \in B_n$ *primljena poruka, i neka je* $\mathbf{p}$ *vektor koji određuje raspodelu verovatnoća na skupu* B_n *(3.7). Neka su matrica* $\mathbf{H}'$ *i vektori* $\mathbf{y}'$, $\mathbf{p}'$ *dobijeni redom od* $\mathbf{H}$, $\mathbf{y}$, *i* $\mathbf{p}$ *izbacivanjem kolona, odnosno koordinata sa indeksima* $i_2, i_3, \ldots, i_l$, *pri čemu se koordinata sa indeksom* i_1 *vektora* $\mathbf{y}$ *zamenjuje u vektoru* $\mathbf{y}'$ *sa* $\bigoplus_{i=1}^{l} y_i$, *a odgovarajuća koordinata vektora* $\mathbf{p}$ *zamenjuje se u vektoru* $\mathbf{p}'$ *vrednošću izraza*

$$\frac{1}{2}\left(1 - \prod_{j=1}^{l}(1 - 2p_{i_j})\right). \tag{3.11}$$

Tada su AVG izračunate na osnovu $\mathbf{H}, \mathbf{y}$ *i* $\mathbf{p}$, *odnosno* $\mathbf{H}', \mathbf{y}'$ *i* $\mathbf{p}'$ *jednake:*

$$\hat{p}_1(\mathbf{H}, \mathbf{y}, \mathbf{p}) = \hat{p}_1(\mathbf{H}', \mathbf{y}', \mathbf{p}'). \qquad \square$$

Dokaz. Neka je sa $\mathbf{E}'$ označena vektorska slučajna promenljiva koja se od slučajne promenljive $\mathbf{E}$ dobija izbacivanjem koordinata sa

indeksima $i_2, i_3, \ldots, i_l$, pri čemu se koordinata sa indeksom i_1 vektora $\mathbf{E}$ zamenjuje u vektoru $\mathbf{E}'$ slučajnom promenljivom $\bigoplus_{i=1}^{l} E_i$. Tada je zbog

$$P\left\{\bigoplus_{i=1}^{l} E_i = 1\right\} = \frac{1}{2}\left(1 - \prod(1 - 2p_{i_j})\right)$$

(videti [Gall62, Teorema 1]) raspodela verovatnoće slučajne promenljive $\mathbf{E}'$ određena vektorom $\mathbf{p}'$. Međutim, slučajne promenljive $E_{i_1}, E_{i_2}, \ldots, E_{i_l}$ u kontrolama parnosti $\mathbf{HE} = \mathbf{0}$ figurišu samo u okviru zbira $\bigoplus_{j=1}^{l} E_{i_j}$. Kako je $\mathbf{HE} = \mathbf{H}'\mathbf{E}'$ i $\mathbf{Hy} = \mathbf{H}'\mathbf{y}'$, biće

$$\begin{aligned}\hat{p}_1(\mathbf{H}', \mathbf{y}', \mathbf{p}') &= P(\{E_1' = 1\} \mid \{\mathbf{H}'\mathbf{E}' = \mathbf{H}'\mathbf{Y}'\}) \\ &= P(\{E_1' = 1\} \mid \{\mathbf{HE} = \mathbf{HY}\}) \\ &= P(\{E_1 = 1\} \mid \{\mathbf{HE} = \mathbf{HY}\}) = \hat{p}_1(\mathbf{H}, \mathbf{y}, \mathbf{p}),\end{aligned}$$

čime je teorema dokazana. □

Primenom ove teoreme AVG se može izračunati pomoću približno 2^{l-1} puta manje operacija nego direktnim postupkom ako LKM $\mathbf{H}$ ima l identičnih kolona. Pri ovoj proceni može se zanemariti mali broj operacija koje treba izvršiti prilikom izračunavanja verovatnoće $P\left\{\bigoplus_{i=1}^{l} E_i = 1\right\}$ (l množenja i $2l + 1$ sabiranja).

Razmotrimo sada LKM $\mathbf{H}$ formiranu od homogenog sistema od r ortogonalnih $m+1$–članih kontrola parnosti bita y_1. Pomoću ove teoreme ili na drugi način dobija se da je [Gall62]

$$\hat{p}_1 = \frac{1}{1 + \frac{1-p}{p}\left(\frac{1+(1-2p)^m}{1-(1-2p)^m}\right)^{r-2\zeta}}, \tag{3.12}$$

gde je sa $\zeta = w(\mathbf{s})$ označena težina sindroma $\mathbf{s} = \mathbf{Hy}$. Zapaža se da ovaj izraz zavisi od veličine $r - 2\zeta = (r - \zeta) - \zeta$ jednake razlici broja nula i jedinica među koordinatama sindroma, a ne zavisi od ukupnog broja r kontrola parnosti. Vrednosti izraza za $p \in \{0.15, 0.3, 0.35, 0.4, 0.45\}$, $\mid r - 2\zeta \mid \in \{1, 2, 3, 4, 6, 8, 10, 15, 20, 30, 40, 50, 100\}$ i $m \in \{2, 4, 6\}$ date su u Tabeli 3.2. Za proizvoljne m, p je očigledno

$$\lim_{r-2\zeta \to +\infty} \hat{p}_1 = 0$$

i

$$\lim_{r-2\zeta \to -\infty} \hat{p}_1 = 1.$$

Brzina konvergencije u ovim izrazima opada kad se p približava jednoj polovini sa donje strane ili kad m raste.

Teorema 3.2 može se dovesti u vezu sa sledećim tvrđenjem, nešto opštijim od tvrđenja iz rada [Gall62] (u izvornom obliku matrica $\mathbf{H}$ ima speifičnu strukturu).

Teorema 3.3 *(videti [Gall62]) Neka je* $\mathbf{y} \in B_n$ *i neka je* $\mathbf{p}$ *vektor koji određuje preko (3.7) raspodelu verovatnoća na skupu* B_n. *Pretpostavimo da je LKM* $\mathbf{H}$ *takva da je* $H_{i,j} = 0$ *za* $i = r,\ 1 \leq j \leq n-l$ *i* $1 \leq i < r,\ n-l+2 \leq j \leq n$, *odnosno* $H_{i,j} = 1$ *za* $i = r,\ n-l+1 \leq j \leq n$, *gde je* $l \geq 2$ *(činjenica da su indeksi kolona težine jedan redom* $n-l+2, n-l+3, \ldots, n$ *ne smanjuje opštost, jer se koordinate kodnih reči mogu ispermutovati). Označimo sa* $\mathbf{H}'$ *matricu jednaku podmatrici matrice* $\mathbf{H}$ *formiranoj od njenih prvih* $r-1$ *vrsta i prvih* $n-l+1$ *kolona. Neka je* $\mathbf{y}' = \mathbf{y}_{\{1,2,\ldots,n-l+1\}}$. *Neka se prvih* $n-l$ *koordinata* $(n-l+1)$*-dimenzionalnog vektora* $\mathbf{p}'$ *podudara se sa odgovarajućim koordinatama vektora* $\mathbf{p}$ *i neka je*

$$\begin{aligned} p'_{n-l+1} &= \hat{p}_1\left([11\ldots1]_{1\times l}, [y_{n-l+1}y_{n-l+2}\cdots y_n]^T, (p_{n-l+1}, p_{n-l+2}, \ldots, p_n)\right) \\ &= \frac{1}{1+\frac{1-p_{n-l+1}}{p_{n-l+1}}\left(\frac{1+\prod_{i=n-l+2}^{n}(1-2p_i)}{1-\prod_{i=n-l+2}^{n}(1-2p_i)}\right)^{1-2s_r}}, \end{aligned}$$

gde je

$$s_r = \bigoplus_{i=n-l+1}^{n} y_i.$$

Tada je

$$\hat{p}_1(\mathbf{H}, \mathbf{y}, \mathbf{p}) = \hat{p}_1(\mathbf{H}', \mathbf{y}', \mathbf{p}'). \qquad \square$$

Zapaža se da je poslednjih $l-1$ kolona matrice $\mathbf{H}$ identično, i da se AVG primenom ove teoreme može izračunati sa približno istim brojem operacija kao i na osnovu Teoreme 3.2. Razlika je u tome što se pomoću Teoreme 3.2 mogu "izbacivati" iz LKM suvišne kolone težine veće od jedan.

Prilikom primene Teoreme 3.2 u slučaju kad su koordinate vektora $\mathbf{p}$ bliske nuli, pojavljuje se problem tačnosti izračunavanja na osnovu

$r-2\zeta$ \ p	0.15	0.3	0.35	0.4	0.45
100.	0.00000	0.00000	0.00000	0.00022	0.09968
50.	0.00000	0.00000	0.00006	0.01204	0.23135
40.	0.00000	0.00000	0.00039	0.02641	0.26880
30.	0.00000	0.00003	0.00239	0.05696	0.30988
20.	0.00000	0.00067	0.01436	0.11854	0.35419
15.	0.00000	0.00337	0.03468	0.16713	0.37738
10.	0.00000	0.01671	0.08137	0.23043	0.40115
8.	0.00003	0.03139	0.11275	0.26003	0.41080
6.	0.00028	0.05820	0.15421	0.29199	0.42051
4.	0.00242	0.10542	0.20735	0.32615	0.43029
3.	0.00703	0.13996	0.23858	0.34398	0.43520
2.	0.02026	0.18350	0.27289	0.36226	0.44012
1.	0.05696	0.23684	0.31013	0.38095	0.44505
0.	0.15000	0.30000	0.35000	0.40000	0.45000
-1.	0.34018	0.37179	0.39209	0.41935	0.45495
-2.	0.60100	0.44973	0.43584	0.43896	0.45992
-3.	0.81484	0.53022	0.48062	0.45876	0.46489
-4.	0.92783	0.60916	0.52571	0.47869	0.46987
-6.	0.99097	0.74826	0.61394	0.51869	0.47984
-8.	0.99893	0.85004	0.69527	0.55845	0.48984
-10.	0.99987	0.91532	0.76600	0.59748	0.49983
-15.	1.00000	0.98191	0.88976	0.68894	0.52481
-20.	1.00000	0.99635	0.95215	0.76770	0.54967
-30.	1.00000	0.99985	0.99180	0.88036	0.59853
-40.	1.00000	0.99999	0.99864	0.94247	0.64551
-50.	1.00000	1.00000	0.99978	0.97332	0.68984
-100.	1.00000	1.00000	1.00000	0.99950	0.85808

Tabela 3.2: Vrednosti AVG za homogeni sistem ortogonalnih kontrola parnosti, $m = 2$

$r-2\zeta$ \ p	0.15	0.3	0.35	0.4	0.45
100.	0.00000	0.00255	0.09630	0.32619	0.44506
50.	0.00000	0.03205	0.19324	0.36228	0.44753
40.	0.00000	0.05236	0.21976	0.36971	0.44802
30.	0.00000	0.08443	0.24879	0.37720	0.44852
20.	0.00001	0.13337	0.28028	0.38474	0.44901
15.	0.00011	0.16583	0.29691	0.38854	0.44926
10.	0.00132	0.20434	0.31409	0.39235	0.44951
8.	0.00350	0.22149	0.32112	0.39387	0.44960
6.	0.00926	0.23966	0.32822	0.39540	0.44970
4.	0.02428	0.25881	0.33540	0.39693	0.44980
3.	0.03902	0.26876	0.33903	0.39770	0.44985
2.	0.06215	0.27894	0.34267	0.39846	0.44990
1.	0.09758	0.28936	0.34632	0.39923	0.44995
0.	0.15000	0.30000	0.35000	0.40000	0.45000
-1.	0.22359	0.31086	0.35369	0.40077	0.45005
-2.	0.31972	0.32194	0.35741	0.40154	0.45010
-3.	0.43406	0.33322	0.36114	0.40231	0.45015
-4.	0.55588	0.34469	0.36488	0.40308	0.45020
-6.	0.76923	0.36818	0.37242	0.40462	0.45030
-8.	0.89876	0.39231	0.38003	0.40616	0.45040
-10.	0.95942	0.41698	0.38769	0.40770	0.45050
-15.	0.99636	0.48023	0.40708	0.41157	0.45074
-20.	0.99968	0.54412	0.42677	0.41545	0.45099
-30.	1.00000	0.66575	0.46679	0.42325	0.45149
-40.	1.00000	0.76873	0.50724	0.43108	0.45198
-50.	1.00000	0.84726	0.54760	0.43894	0.45248
-100.	1.00000	0.98626	0.73126	0.47865	0.45495

Tabela 3.2: (nastavak) Vrednosti AVG za homogeni sistem ortogonalnih kontrola parnosti, $m = 4$

p $r-2\zeta$	0.15	0.3	0.35	0.4	0.45
100.	0.00000	0.15889	0.31760	0.39693	0.44995
50.	0.00000	0.22151	0.33360	0.39847	0.44997
40.	0.00001	0.23596	0.33685	0.39877	0.44998
30.	0.00015	0.25104	0.34012	0.39908	0.44998
20.	0.00156	0.26676	0.34340	0.39939	0.44999
15.	0.00506	0.27484	0.34504	0.39954	0.44999
10.	0.01633	0.28308	0.34669	0.39969	0.44999
8.	0.02594	0.28642	0.34735	0.39975	0.45000
6.	0.04097	0.28978	0.34801	0.39982	0.45000
4.	0.06415	0.29316	0.34867	0.39988	0.45000
3.	0.07989	0.29486	0.34901	0.39991	0.45000
2.	0.09909	0.29657	0.34934	0.39994	0.45000
1.	0.12228	0.29828	0.34967	0.39997	0.45000
0.	0.15000	0.30000	0.35000	0.40000	0.45000
-1.	0.18269	0.30172	0.35033	0.40003	0.45000
-2.	0.22066	0.30345	0.35066	0.40006	0.45000
-3.	0.26397	0.30519	0.35100	0.40009	0.45000
-4.	0.31238	0.30693	0.35133	0.40012	0.45000
-6.	0.42159	0.31042	0.35199	0.40018	0.45000
-8.	0.53906	0.31394	0.35266	0.40025	0.45000
-10.	0.65234	0.31748	0.35332	0.40031	0.45001
-15.	0.85952	0.32642	0.35499	0.40046	0.45001
-20.	0.95227	0.33549	0.35666	0.40061	0.45001
-30.	0.99531	0.35399	0.36001	0.40092	0.45002
-40.	0.99956	0.37294	0.36338	0.40123	0.45002
-50.	0.99996	0.39229	0.36676	0.40154	0.45003
-100.	1.00000	0.49298	0.38385	0.40308	0.45005

Tabela 3.2: (nastavak) Vrednosti AVG za homogeni sistem ortogonalnih kontrola parnosti, $m = 6$

izraza (3.11). Zbog toga će sada biti razmotreno izračunavanje na osnovu izraza oblika

$$p^* = \frac{1 - \prod_{j=1}^{l}(1 - 2p_j)}{2} \tag{3.13}$$

Oduzimanje od jedinice proizvoda bliskog jedinici u značajnoj meri povećava relativnu grešku rezultata. Da bi se ovaj problem rešio, pogodno je gornji izraz napisati u obliku (videti [Gall62])

$$a^* = f\left(\sum_{j=1}^{l} f(a_j)\right), \tag{3.14}$$

gde je $a^* = \ln \frac{1-p^*}{p^*}$, $a_j = \ln \frac{1-p_j}{p_j}$, $1 \leq j \leq l$, a funkcija $f(z)$ definisana je izrazom

$$f(z) = \ln \frac{e^z + 1}{e^z - 1}, \qquad z > 0$$

(izraz $\ln \frac{1-p}{p}$, gde je p verovatnoća, $0 < p < 1$, je *algebarska vrednost* te verovatnoće).

Kao što je već rečeno, bez gubitka opštosti može se pretpostaviti da je $0 \leq p_j < 1/2$, $1 \leq j \leq l$. Ova pretpostavka može se opravdati i na drugi način: ako je $p_j > 1/2$, tada se smenom $p'_j = 1 - p_j$ dobija $p'_j < 1/2$, a oblik izraza (3.13) zbog $1 - 2p'_j = -(1 - 2p_j)$ ostaje isti. Ako je $p_j = 1/2$ za bilo koje j, $1 \leq j \leq l$, onda je $p^* = 1/2$. Kako je tada $a_j = 0$ i $\lim_{z \to 0} f(z) = +\infty$, biće

$$\lim_{p_j \to 1/2} a^* = \lim_{a_j \to 0} a^* = +\infty,$$

što odgovara ponašanju izraza (3.13) za $p_j = 1/2$.

Preslikavanje $p_j \to a_j$ je monotono. Vrednostima p_j bliskim nuli odgovaraju velike vrednosti a_j, jer je $\lim_{p_j \to 0} a_j = +\infty$. Zbog toga se problem tačnog izračunavanja vrednosti izraza (3.13) kad su brojevi p_j bliski nuli svodi na problem tačnog izračunavanja vrednosti izraza (3.14) kad su argumenti a_j, $1 \leq j \leq l$, veliki. Funkcija $f(z)$ je monotono opadajuća, pri čemu je $\lim_{z \to 0} f(z) = +\infty$ i $\lim_{z \to +\infty} f(z) = 0$. Pod navedenim pretpostavkama argument $\sum_{i=1}^{l} f(a_j)$ funkcije f u izrazu (3.14) ima malu vrednost. Dakle, da bi se vrednost izraza (3.14) mogla tačno izračunavati, potrebno je omogućiti tačno izračunavanje

vrednosti funkcije f za velike argumente i argumente bliske nuli. Neka je sa γ označena relativna greška zaokruživanja realnih brojeva proizrokovana ograničenim prostorom za njihovo smeštanje u računaru. Tipična vrednost ovog parametra je $\gamma = 2^{-56} = 1.39 \times 10^{-17}$. Rešenje postavljenog problema daje naredna teorema [Živk90].

Teorema 3.4 *Neka relativna greška zaokruživanja γ zadovoljava uslov $\gamma \leq 2^{-56}$. Neka je funkcija $\hat{f}(z)$, $z > 0$ definisana jednakošću*

$$\hat{f}(z) = \begin{cases} 2e^{-z}, & z_0 \leq z < +\infty \\ 2e^{-z} + \frac{2}{3}e^{-3z}, & z_1 \leq z < z_0 \\ f(z), & z_2 \leq z < z_1 \\ \ln\frac{2}{z} + \frac{1}{12}z^2, & z_3 \leq z < z_2 \\ \ln\frac{2}{z}, & 0 < z < z_3 \end{cases}, \tag{3.15}$$

gde je $z_0 = \frac{1}{3}\ln\frac{c}{10\gamma}$, $z_1 = \frac{1}{5}\ln\frac{3c}{25\gamma}$, $z_2 = (48\gamma)^{1/3}$, $z_3 = 6\gamma$ *i* $c = \frac{2}{3(1-e^{-2})} \simeq 0.771$. *Tada je za* $z > 0$

$$\frac{1}{z} \mid f(z) - \hat{f}(z) \mid < \gamma. \qquad \square \tag{3.16}$$

DOKAZ. Razmotrimo najpre slučaj $z > z_0 = \frac{1}{3}\ln\frac{c}{10\gamma} > 12.1$. Korišćenjem Tejlorovog razvoja

$$\ln\frac{1+w}{1-w} = 2\sum_{k=1}^{\infty}\frac{1}{2k-1}w^{2k-1}, \qquad w < 1, \tag{3.17}$$

dobijaju se nejednakosti

$$\begin{aligned} 2w \leq \ln\frac{1+w}{1-w} &< 2w + \frac{2}{3}\sum_{k=2}^{\infty}w^{2k-1} = 2w + \frac{2}{3}\frac{w^3}{1-w^2} \\ &< 2w + \frac{2}{3\,(1-e^{-2})}w^3 = 2w + cw^3. \end{aligned}$$

Zamenom w u ovom izrazu sa $e^{-z} < 1$, dobija se

$$\frac{1}{z} \mid \ln \frac{e^z + 1}{e^z - 1} - 2e^{-z} \mid < \frac{c}{z} e^{-3z} < \frac{c}{10} e^{-3z} < \gamma, \qquad z > z_0,$$

čime je (3.16) dokazano u slučaju $z > z_0$. Na sličan način, uzimajući u obzir dva prva člana razvoja (3.17), dobijaju se nejednakosti

$$2w + \frac{2}{3}w^3 \leq \ln \frac{1+w}{1-w} \leq 2w + \frac{2}{3}w^3 + \frac{3}{5}cw^5,$$

pa je za $z > z_1$

$$\frac{1}{z} \mid \ln \frac{e^z + 1}{e^z - 1} - 2e^{-z} - \frac{2}{3}e^{-3z} \mid < \frac{3}{5}\frac{c}{z}e^{-5z} < \frac{3c}{25}e^{-5z} < \gamma.$$

Time je (3.16) dokazano u slučaju $z_1 \leq z < z_0$.

Slučaj kad je z malo, $z < z_2$, je komplikovaniji. Razmotrimo Tejlorov razvoj funkcije $\varphi(z) = f(z) - \ln\left(\frac{2}{z}\right)$,

$$\varphi(z) = \ln\left(\frac{e^z + 1}{e^z - 1}\frac{z}{2}\right) = \frac{z^2}{12} + \frac{\varphi^{IV}(\theta z)}{4!}z^4, \qquad 0 < \theta < 1. \qquad (3.18)$$

Potrebno je naći donju i gornju granicu izvoda $\varphi^{IV}(z)$ kad je na primer $0 < z < 0.01$, a time i granice izraza $\varphi^{IV}(\theta z)$. Izraz za $f(z)$ može se napisati u obliku

$$\varphi(z) = \varphi_1(z) + \varphi_2(z), \qquad (3.19)$$

gde je

$$\varphi_1(z) = \ln \frac{e^z + 1}{2},$$

i

$$\varphi_2(z) = \ln \frac{z}{e^z - 1},$$

Četvrti izvod funkcije $\varphi_1(z)$ je

$$\varphi_1^{IV}(z) = \frac{1}{1+e^{-z}} - \frac{7}{(1+e^{-z})^2} + \frac{12}{(1+e^{-z})^3} - \frac{6}{(1+e^{-z})^4}.$$

Polazeći od nejednakosti

$$\frac{1}{2} \leq \frac{1}{1+e^{-z}} < \frac{1}{1+e^{-0.01}} = c' \simeq 0.5025$$

lako se dobijaju sledeće granice za $\varphi_1(z)$

$$-0.150 \simeq 2 - 7c'^2 - 6c'^4 < \varphi_1^{IV}(z) < c' + 12c'^3 - \frac{17}{8} \simeq -0.0999,$$

a time i

$$| \varphi_1^{IV}(z) | < 0.2, \qquad 0 < z < 0.01. \tag{3.20}$$

Četvrti izvod $\varphi_2^{IV}(z)$ može se napisati u obliku

$$\varphi_2^{IV}(z) = \varphi_3(t) \left(\frac{t}{z}\right)^4, \tag{3.21}$$

gde je $t = 1 - e^{-z}$ i

$$\varphi_3(t) = \frac{(\ln(1-t))^4 (6 - 12t + 7t^2 - t^3) - 6t^4}{t^8}. \tag{3.22}$$

Promenljiva t za $0 < z \leq z_2$ očigledno zadovoljava nejednakosti $0 \leq t < 1 - e^{-0.01} < 0.01$. Da bi se ocenio moduo izvoda $| \varphi_3(t) |$, može se poći od Tejlorovog razvoja

$$-\ln(1-t) = t + \frac{t^2}{2} + \frac{t^3}{3} + \frac{t^4}{4} + \frac{U}{5}t^5,$$

gde je $U = (1 - \theta_1 t)^{-5}$, $0 < \theta_1 < 1$, i zbog toga $1 \leq U < (1-t)^{-5} = e^{5z} < e^{0.05} \simeq 1.0513$. Zamenom ovog razvoja u (3.22), dobija se izraz za $\varphi_3(t)$ u kome figurišu t i U,

$$\begin{aligned}
\varphi_3(t) = & - \frac{115}{24} + \frac{24}{5}U \\
& + t\left(-\frac{19}{12} - \frac{12}{5}U\right) \\
& + t^2\left(-\frac{145}{144} - \frac{2}{5}U\right) \\
& + t^3\left(-\frac{35}{48} - \frac{1}{5}U\right) \\
& + t^4\left(\frac{125}{144} - 3U + \frac{36}{25}U^2\right) \\
& + t^5\left(\frac{35}{72} + \frac{2}{5}U - \frac{36}{25}U^2\right)
\end{aligned}$$

$$
\begin{aligned}
&+ \quad t^6\left(\frac{959}{2592}+\frac{2}{45}U+\frac{3}{25}U^2\right)\\
&+ \quad t^7\left(\frac{775}{2592}+\frac{1}{90}U\right)\\
&+ \quad t^8\left(\frac{205}{3456}+\frac{31}{54}U-\frac{29}{50}U^2+\frac{24}{125}U^3\right)\\
&+ \quad t^9\left(\frac{5}{192}+\frac{47}{540}U+\frac{19}{50}U^2-\frac{36}{125}U^3\right)\\
&+ \quad t^{10}\left(\frac{5}{768}+\frac{7}{120}U+\frac{1}{60}U^2+\frac{12}{125}U^3\right)\\
&+ \quad t^{11}\left(-\frac{1}{256}+\frac{3}{80}U+\frac{1}{75}U^2\right)\\
&+ \quad t^{12}\left(-\frac{1}{80}U+\frac{13}{200}U^2-\frac{14}{375}U^3+\frac{6}{625}U^4\right)\\
&+ \quad t^{13}\left(-\frac{3}{200}U^2+\frac{17}{375}U^3-\frac{12}{625}U^4\right)\\
&+ \quad t^{14}\left(-\frac{1}{125}U^3-\frac{7}{625}U^4\right)\\
&+ \quad t^{15}\left(-\frac{1}{625}U^4\right)
\end{aligned}
$$

Apsolutne vrednosti koeficijenata uz $t^2, t^3, \ldots, t^{15}$ u ovom izrazu su manje od 15 za $0 < z < 0.01$, što se direktno proverava. Ova činjenica omogućuje nalaženje gornje granice modula $\mid \varphi_3(t) \mid$ za $0 \leq t < 0.01$,

$$
\begin{aligned}
\mid \varphi_3(t) \mid \quad &\leq \quad \mid -\frac{115}{24}+\frac{24}{5}e^{0.05} \mid + t\left(\frac{19}{12}+\frac{12}{5}e^{0.05}\right)+15\left(t^2+\cdots+t^{15}\right)\\
&\leq \quad 0.255+4.16t+15t^2\frac{1-t^{14}}{1-t}\\
&\leq \quad 0.255+0.0416+30t^2<0.3
\end{aligned}
$$

Zbog $t < z$, zamenom u (3.21) zaključuje se da je $\mid \varphi_2^{IV}(z) \mid < 0.3$ za $0 < z < 0.01$, i konačno, na osnovu (3.19) i (3.20),

$$\mid \varphi^{IV}(z) \mid < 0.5, \qquad 0 < z < 0.01.$$

Razmotrimo sada slučaj $0 < z < z_2 = (48\gamma)^{1/3}$. Na osnovu (3.18) i ocene $\mid \varphi^{IV}(z) \mid$ za $0 < z < z_2 < 0.01$ je

$$\frac{1}{z} \mid \ln\frac{e^z+1}{e^z-1}-\ln\frac{2}{z}-\frac{z^2}{12} \mid = \mid \varphi^{IV}(\theta z)\frac{z^3}{24} \mid < \frac{z^3}{48} < \gamma.$$

Konačno, za $0 < z < z_3$, lako se izvodi nejednakost

$$\frac{1}{z} \mid \ln \frac{e^z + 1}{e^z - 1} - \ln \frac{2}{z} \mid = \mid \frac{z}{12} + \varphi^{IV}(\theta z)\frac{z^3}{24} \mid \leq \frac{z}{12} + \frac{z^3}{48} < \frac{z}{6} < \gamma.$$

Time je završen dokaz teoreme. □

Prilikom određivanja razvoja $\varphi_3(z)$ korišćen je program za simboličku matematiku "MUSIMP". Za $\gamma = 2^{-56}$ parametri u (3.15) imaju sledeće vrednosti: $z_0 \simeq 12.1$, $z_1 \simeq 7.29$, $z_2 \simeq 8.733 \times 10^{-6}$ i $z_3 \simeq 8.33 \times 10^{-17}$.

Razmotrimo sada izračunavanje AVG na osnovu izraza (3.9). Zbog ograničenog broja mesta za eksponent realnih brojeva (prilikom njihovog smeštanja u računaru), ovaj izraz nije pogodan za izračunavanje AVG, jer se brojevi manji od na primer 10^{-39} ne mogu razlikovati od nule. Pokazuje se da je i u ovoj situaciji pogodno umesto sa verovatnoćama p_i, $1 \leq i \leq n$, računati sa njihovim algebarskim vrednostima $a_i = \ln \frac{1-p_i}{p_i}$, $1 \leq i \leq n$. Izraz (3.7) posle ove smene postaje

$$\begin{aligned} P\{\mathbf{E} = \mathbf{e}\} &= \prod_{i=1}^{n}(1 - p_i) \times \prod_{i=1}^{n}\left(\frac{p_i}{1 - p_i}\right)^{e_i} \\ &= \exp\left(\sum_{i=1}^{n} e^{-a_i e_i}\right) \times \prod_{i=1}^{n}(1 - p_i). \end{aligned}$$

Ako se sa $\hat{a}_1$ označi aposteriorna algebarska vrednost $\hat{a}_1 = \ln \frac{1-\hat{p}_1}{\hat{p}_1}$, izraz (3.9) postaje

$$\hat{a}_1 = \ln \frac{\sum_{\mathbf{e} \in C_{\mathbf{s},0}} \exp\left(-\sum_{i=1}^{n} a_i e_i\right)}{\sum_{\mathbf{e} \in C_{\mathbf{s},1}} \exp\left(-\sum_{i=1}^{n} a_i e_i\right)}. \tag{3.23}$$

Zanimljivo je da se vrednost ovog izraza može izračunati pomoću $O(2^k)$ umesto $O(n2^k)$ množenja, sa konstantom proporcionalnosti određenom složenošću izračunavanja eksponencijalne funkcije.

Mogućnost primene Teoreme 3.2 i Teoreme 3.4 na izračunavanje AVG u okviru Algoritma 2.1 (odnosno Algoritma B, [Meie89]) biće ilustrovana jednim primerom.

Primer 3.4 Posmatrajmo kod $R_{h,n}$, gde je $h(z) = 1+z^2+z^8+z^{12}+z^{26}$, $n = 192$. Verovatnoća greške je $p = 6/32$. Podela intervala $[1, 196]$ na 17

	Granica za i		r_i	n_i	k_i	n'_i	k'_i
	donja	gornja					
1	1	1	2	9	7	3	1
2	2	2	3	12	9	5	2
3	3	4	4	15	11	7	3
4	5	6	5	18	13	9	4
5	7	8	6	21	15	11	5
6	9	12	7	23	16	14	7
7	13	13	8	26	18	16	8
9	14	26	9	29	20	18	9
9	27	166	10	33	23	19	9
10	167	168	9	31	22	16	7
11	169	174	8	29	21	13	5
12	175	178	7	27	20	10	3
13	179	179	6	25	19	7	1
14	180	180	5	21	16	6	1
15	181	183	4	17	13	5	1
16	184	185	3	13	10	4	1
17	186	192	2	9	7	3	1

Tabela 3.3: Dimenzije LKM pre, odnosno posle izbacivanja ponovljenih kolona

podintervala sa sličnim LKM prikazana je u Tabeli 3.3. U ovoj tabeli su navedene dimenzije LKM $\mathrm{H}^{(i)}$ r_i, n_i (odnosno r_i, n'_i) pre (odnosno posle) primene Teoreme 3.2, $1 \leq i \leq n$, kao i dimenzije $k_i = n_i - r_i$, $k'_i = n'_i - r_i$ odgovarajućih linarnih kodova. Zapaža se značajno smanjenje složenosti izračunavanja AVG na osnovu (3.9): na intervalu $27 \leq i \leq 166$ čak za faktor $2^{23-9} = 65536$! Međutim, ako se upoređenje izvrši sa algoritmom zasnovanim na generatrisi koseta [Batt79], ušteda je manja (približno za faktor četiri na intervalu $27 \leq i \leq 166$).

Na ovom primeru može se uočiti i prednost korišćenja aposteriornih algebarskih vrednosti umesto AVG. Izvršeno je 100 eksperimenata sa pojednostavljenom verzijom Algoritma 2.1 (broj ciklusa ograničen je na jedan). Za fiksirani broj iteracija j, $1 \leq j \leq 10$, po 10 puta je izvršavan ovaj algoritam. Informacioni skupovi formirani su slučajnim izborom

iz skupa od 40 koordinata sa najmanjom nepouzdanošću (odnosno sa najmanjim AVG posle j iteracija). Za dubinu pretrage usvojena je vrednost 1 (videti tačku 4.3). Broj uspešnih dekodiranja od ukupno 10 za $j = 1, 2, \ldots, 10$ bio je redom 4, 6, 0, 0, 1, 2, 4, 10, 10, 10 kad je korišćena Teorema 3.4, odnosno 4, 6, 0, 0, 0, 0, 0, 0, 0, 0 prilikom direktnog izračunavanja. Ovi rezultati se mogu objasniti činjenicom da se zbog akumuliranja grešaka prilikom direktnog izračunavanja posle pete iteracije nisu mogle efikasno izdvojiti koordinate primljene poruke sa manjom nepouzdanošću. □

Iako se LKM formiraju od relativno malog broja kontrola parnosti, ipak se dešava (naročito za veće vrednosti m) da se AVG praktično ne mogu izračunavati zbog prevelikih dimenzija LKM. Broj množenja koja treba izvršiti prilikom izračunavanja AVG (pomoću opisanih algoritama) na osnovu LKM dimenzija $r \times n$ dat je približno izrazom

$$n2^{\min\{r+1, n-r-l\}} \tag{3.24}$$

gde je sa l označen broj kolona LKM izbačenih na osnovu Teoreme 3.2 (iz svake grupe jednakih kolona u LKM se zadržava samo jedan predstavnik). Na osnovu toga se mogu isključivanjem nekih kontrola parnosti tražiti pogodne LKM – takve koje omogućuju izračunavanje AVG sa numeričkom složenošću manjom od zadate, videti Algoritam 3.2.

3.3 Verovatnoća zaostale greške

U ovoj tački koristi se uprošćeno označavanje LKM uvedeno u prethodnoj tački. Opštije nego u [Meie89] razmatra se AVG kao slučajna promenljiva. Dokazuje se da je i u opštem slučaju uslovno matematičko očekivanje AVG veće ako je odgovarajući bit primljene poruke pogrešan, nego ako je tačan. Prilikom odlučivanja po principu maksimuma verodostojnosti značajan parametar je verovatnoća pogrešne odluke, (Bajesova greška, videti na primer [Dels78]) odnosno *verovatnoća zaostale greške*. Pod verovatnoćom zaostale greške (VZG) podrazumeva se verovatnoća da je o grešci bita doneta pogrešna odluka: da je bit tačan i AVG veća od 1/2, ili da je bit pogrešan i da AVG nije veća od 1/2.

Ova veličina je u literaturi detaljnije razmatrana za postupke dekodiranja kojima se ispravlja ograničeni broj grešaka u kodnoj reči, videti na primer [Cohe76]. Pokazuje se da je VZG jednaka razlici apriorne verovatnoće greške i *smanjenja verovatnoće greške* [Meie89]. U Algoritmu 2.1, slično kao i u Algoritmu B, od značaja je i verovatnoća da je AVG veća od 1/2 (u daljem tekstu *verovatnoća promene*) jer se na osnovu nje izračunava matematičko očekivanje broja bita primljene poruke koje treba komplementirati u koraku 7^0 Algoritma 2.1. Slučaj kad LKM obuhvata homogeni sistem ortogonalnih kontrola parnosti detaljnije je razmotren. U opštem slučaju nađen je potreban i dovoljan uslov da VZG bude jednaka p kad je p u nekoj okolini jedne polovine. Na kraju je pokazano da se VZG i verovatnoća promene mogu izračunavati na osnovu uprošćene LKM, slično kao AVG na osnovu Teoreme 3.2.

Aposteriorna verovatnoća greške data je jednakošću

$$\hat{p}_1 = \frac{P(C_{\mathbf{s},1})}{P(C_{\mathbf{s}})},$$

videti (3.9). Ova veličina je realizacija slučajne promenljive

$$\hat{P}_1 = \frac{P(C_{\mathbf{S},1})}{P(C_{\mathbf{S}})}, \tag{3.25}$$

gde je $\mathbf{S} = \mathbf{HE} = \mathbf{HY}$ slučajni *sindrom*. Za razliku od [Meie89], ovde se ne pretpostavlja da su kontrole parnosti sadržane u LKM $\mathbf{H}$ ortogonalne. Činjenica da je matematičko očekivanje slučajne promenljive $\hat{P}_1$ jednako p trivijalna je,

$$\begin{aligned} M(\hat{P}_1) &= \sum_{\mathbf{s}\in B_r} P\{\mathbf{S}=\mathbf{s}\}\hat{P}_1 = \sum_{\mathbf{s}\in B_r} P(C_{\mathbf{s}})\frac{P(C_{\mathbf{s},1})}{P(C_{\mathbf{s}})} = \\ &= \sum_{\mathbf{s}\in B_r} P\{\mathbf{HE}=\mathbf{s}, E_1=1\} = p. \end{aligned}$$

Pokazaćemo da nejednakost uslovnih matematičkih očekivanja

$$M(\hat{P}_1 \mid E_1 = 1) \geq M(\hat{P}_1 \mid E_1 = 0)$$

važi i u opštem slučaju. Za nenegativne realne brojeva $a, b,\ a+b>0$ i $0<p<1$ očigledno važi nejednakost

$$\frac{a}{a+b}\left(\frac{a}{p}-\frac{b}{1-p}\right) = p\left(\frac{a}{p}-\frac{b}{1-p}\right)+\frac{p(1-p)}{a+b}\left(\frac{a}{p}-\frac{b}{1-p}\right)^2$$

$$\geq \quad p\left(\frac{a}{p} - \frac{b}{1-p}\right).$$

Zamenom a, b u ovoj nejednakosti redom sa $P(C_{\mathbf{s},1}), P(C_{\mathbf{s},0})$ i sumiranjem po $\mathbf{s} \in B_r$, dobija se nejednakost

$$\begin{aligned} M(\hat{P}_1 \mid \{E_1 = 1\}) \; - \; & M(\hat{P}_1 \mid \{E_1 = 0\}) \\ = \; & \sum_{\mathbf{s}\in B_r} \frac{P(C_{\mathbf{s},1})}{P(C_{\mathbf{s},1}) + P(C_{\mathbf{s},0})} \left(\frac{P(C_{\mathbf{s},1})}{p} - \frac{P(C_{\mathbf{s},0})}{1-p}\right) \\ \geq \; & \sum_{\mathbf{s}\in B_r} p\left(\frac{P(C_{\mathbf{s},1})}{p} - \frac{P(C_{\mathbf{s},0})}{1-p}\right) = 0, \end{aligned}$$

čime je dokazana nejednakost između uslovnih matematičkih očekivanja slučajne promenljive $\hat{P}_1$. Pri tome jednakost važi ako i samo ako je za svako $\mathbf{s} \in B_r$

$$\frac{P(C_{\mathbf{s},1})}{p} = \frac{P(C_{\mathbf{s},0})}{1-p}.$$

Posmatrajmo slučajnu promenljivu E_1^* (*zaostala greška*) definisanu jednakošću

$$E_1^* = I\left(E_1 = 1, \hat{P}_1 \leq \frac{1}{2}\right) + I\left(E_1 = 0, \hat{P}_1 > \frac{1}{2}\right). \tag{3.26}$$

Ovde je sa $I(izraz)$ označen indikator izraza $izraz$, jednak 1 ako je izraz tačan, odnosno 0 u protivnom. Pošto se o bitu greške E_1 odlučuje na osnovu AVG $\hat{p}_1$ (da je $E_1 = 1$ ocenjuje se ako i samo ako je $\hat{p}_1 > 1/2$), gornji izraz jednak je jedninici ako i samo ako je o bitu greške E_1 pogrešno odlučeno. Drugim rečima, E_1^* je Bajesova greška odlučivanja. Uzimajući u obzir (3.25), dobija se da je

$$E_1^* = I\left(E_1 = 1, P(C_{\mathbf{S},0}) \geq P(C_{\mathbf{S},1})\right) + I\left(E_1 = 0, P(C_{\mathbf{S},0}) < P(C_{\mathbf{S},1})\right).$$

Uslovna verovatnoća $P\left(\{E_1^* = 1\} \mid \{\mathbf{HE} = \mathbf{s}\}\right)$ za proizvoljno $\mathbf{s} \in B_r$ jednaka je zbog toga

$$P\left(\{E_1^* = 1\} \mid \{\mathbf{HE} = \mathbf{s}\}\right) = \min\left\{P(C_{\mathbf{s},0}), P(C_{\mathbf{s},1})\right\} / P(C_{\mathbf{s}}),$$

pa je VZG data izrazom

$$P\{E_1^* = 1\} = \sum_{\mathbf{s}\in B_r} \min\left\{P(C_{\mathbf{s},0}), P(C_{\mathbf{s},1})\right\}. \tag{3.27}$$

Jasno je da VZG zavisi samo od linearnog prostora kome je baza skup vektora–vrsta matrice **H**.

Verovatnoća promene definše se jednakošću

$$P\left\{\hat{P}_1 > \frac{1}{2}\right\} = \sum_{\mathbf{s}\in B_r} I\left(P(C_{\mathbf{s},0}) < P(C_{\mathbf{s},1})\right) P(C_{\mathbf{s}}). \tag{3.28}$$

Lako se pokazuje da je VZG uvek manja od apriorne verovatnoće greške p. Zaista,

$$P\{E_1^* = 1\} \leq \sum_{\mathbf{s}\in B_r} P(C_{\mathbf{s},1}) = p. \tag{3.29}$$

Razmotrimo sada detaljnije slučaj kad je LKM **H** formirana od r ortogonalnih $(m+1)$–članih kontrola parnosti bita x_1. Neka je, kao i u izrazu (3.2) za AVG, sa $\zeta = w(\mathbf{s})$ označena težina sindroma $\mathbf{s} \in B_r$. Podskupovi $C_{\mathbf{s},0}$ i $C_{\mathbf{s},1}$, koji čine particiju koseta $C_{\mathbf{s}}$, imaju verovatnoće

$$P(C_{\mathbf{s},0}) = (1-p)\tilde{p}^{\zeta}(1-\tilde{p})^{r-\zeta}$$

i

$$P(C_{\mathbf{s},1}) = p(1-\tilde{p})^{\zeta}\tilde{p}^{r-\zeta},$$

gde je $\tilde{p} = \left(1-(1-2p)^m\right)/2$ verovatnoća da bude neparna suma m nezavisnih jednako raspodeljenih slučajnih $0-1$ promenljivih sa verovatnoćom jedinice jednakom p, videti (1.9). Neka je

$$\zeta_g = \left[\frac{1}{2}\left(r + \frac{\ln\frac{1-p}{p}}{\ln\frac{1-\tilde{p}}{\tilde{p}}}\right)\right]. \tag{3.30}$$

Neposredno se proverava da je nejednakost $P(C_{\mathbf{s},0}) < P(C_{\mathbf{s},1})$ ekvivalentna sa nejednakošću $\zeta = w(\mathbf{s}) > \zeta_g$. Verovatnoća promene je na osnovu (3.28) jednaka

$$P\left\{\hat{P}_1 > \frac{1}{2}\right\} = \sum_{\zeta>\zeta_g}\binom{r}{\zeta}\left((1-p)\tilde{p}^{\zeta}(1-\tilde{p})^{r-\zeta} + p(1-\tilde{p})^{\zeta}\tilde{p}^{r-\zeta}\right). \tag{3.31}$$

Ovaj izraz odgovara verovatnoći $U(p,r,t)$ iz [Meie89], ako se za prag broja zadovoljenih kontrola parnosti t usvoji $r-\zeta_g-1$. Na osnovu (3.27) dobija se da je VZG jednaka

$$\begin{aligned} P\{E_1^*=1\} &= \sum_{\zeta\le\zeta_g}\binom{r}{\zeta}P(C_{s,1}) + \sum_{\zeta>\zeta_g}\binom{r}{\zeta}P(C_{s,0}) \\ &= \sum_{\zeta=0}^{r}\binom{r}{\zeta}P(C_{s,1}) - \sum_{\zeta>\zeta_g}\binom{r}{\zeta}\left(P(C_{s,1})-P(C_{s,0})\right) \\ &= p - \sum_{\zeta>\zeta_g}\binom{r}{\zeta}\left(p(1-\tilde{p})^{\zeta}\tilde{p}^{r-\zeta} - (1-p)\tilde{p}^{\zeta}(1-\tilde{p})^{r-\zeta}\right). \quad (3.32) \end{aligned}$$

Razlika $p - P\{E_1^*=1\}$ iz ovog izraza odgovara *smanjenju verovatnoće greške* $I(\cdot,\cdot,\cdot)$ iz [Meie89], videti (1.11), ako se za parametar t (gornja granica za broj zadovoljenih kontrola parnosti) usvoji vrednost $r-\zeta_g-1$. U citiranom radu je ova granica određivana numeričkim metodima, iako se ona u ovom slučaju bez poteškoća može direktno odrediti. Iz nejednakosti (3.29) sledi da je uvek $I(p,r,t)\ge 0$, a time i $F(p,m,d)\ge 0$, videti tačku 1.3. Veličina $I(p,r,t)$ očigledno zavisi i od m.

Iz poslednjeg izraza i (3.30) vidi se da VZG zavisi od p, r i m. Vrednosti VZG i verovatnoće promene (3.31) za $p\in\{0.15, 0.3, 0.35, 0.4, 0.45\}$, $r\in\{1,2,3,4,6,8,10,15,20,30,40,50,100\}$ i $m\in\{2,4\}$ navedene su Tabeli 3.4.

Zapaža se da je za p dovoljno blisko 1/2 uvek $P(E_1^*=1)=p$. Ova činjenica može se objasniti na sledeći način. Na osnovu (3.30) za $m>2$ je $\lim_{p\to 1/2-}=+\infty$, što znači da je za p dovoljno blisko 1/2 $\zeta_g\ge r$. Odatle na osnovu (3.32) sledi da je $P(E_1^*=1)=p$. U Tabeli 3.5 data je za $r\in\{1,2,3,4,6,8,10,15,20,30,40,50,100\}$ i $m\in\{2,4,6\}$ granična verovatnoća p iznad koje je $P(E_1^*=1)=p$.

U opštem slučaju se VZG ne ponaša uvek na ovaj način u okolini 1/2, što se može ilustrovati sledećim jednostavnim primerom.

Primer 3.5 Neka je LKM **H** data jednakošću

$$\mathbf{H}=\begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}$$

Ovde je $r=2$ i $m=1$, pa je na osnovu (3.30) $\zeta_g=[(r+1)/2]=1$. U ovom slučaju (kao i za $m=1$ i proizvoljno $r\ge 2$) granica ζ_g ne zavisi od verovatnoće p, i manja je od broja kontrola parnosti r. Za VZG se na osnovu (3.32) dobija

$$P(E_1^*=1)=p-\left(p(1-p)^2-p^2(1-p)\right)=p-p(1-p)(1-2p)<p$$

VZG, $m = 2$										
p / r	0.15		0.30		0.35		0.40		0.45	
1	0.1500	1	0.3000	1	0.3500	2	0.4000	3	0.4500	5
2	0.1220	1	0.3000	2	0.3500	2	0.4000	3	0.4500	6
3	0.1021	2	0.2933	2	0.3500	3	0.4000	4	0.4500	6
4	0.0861	2	0.2878	3	0.3470	3	0.4000	4	0.4500	7
6	0.0609	3	0.2746	4	0.3421	4	0.3994	5	0.4500	8
8	0.0434	4	0.2619	5	0.3365	5	0.3984	6	0.4500	9
10	0.0311	5	0.2498	6	0.3307	6	0.3971	7	0.4500	10
15	0.0135	8	0.2237	8	0.3170	9	0.3939	10	0.4500	12
20	0.0063	10	0.1998	11	0.3026	11	0.3886	12	0.4499	15
30	0.0014	15	0.1628	16	0.2781	16	0.3794	17	0.4494	20
40	0.0003	20	0.1342	21	0.2569	21	0.3705	22	0.4486	25
50	0.0001	25	0.1116	26	0.2383	26	0.3620	27	0.4476	30
100	0.0000	50	0.0478	51	0.1698	51	0.3260	52	0.4419	55
Verovatnoća promene, $m = 2$										
1	0.0000	1	0.0000	1	0.0000	2	0.0000	3	0.0000	5
2	0.1385	1	0.0000	2	0.0000	2	0.0000	3	0.0000	6
3	0.0761	2	0.1104	2	0.0000	3	0.0000	4	0.0000	6
4	0.1551	2	0.0557	3	0.0587	3	0.0000	4	0.0000	7
6	0.1576	3	0.0967	4	0.1023	4	0.0152	5	0.0000	8
8	0.1571	4	0.1269	5	0.1347	5	0.0343	6	0.0000	9
10	0.1559	5	0.1499	6	0.1596	6	0.0533	7	0.0000	10
15	0.1448	8	0.2519	8	0.1407	9	0.0577	10	0.0037	12
20	0.1516	10	0.2136	11	0.2303	11	0.1277	12	0.0059	15
30	0.1504	15	0.2428	16	0.2644	16	0.1750	17	0.0213	20
40	0.1501	20	0.2595	21	0.2847	21	0.2073	22	0.0401	25
50	0.1500	25	0.2701	26	0.2983	26	0.2311	27	0.0591	30
100	0.1500	50	0.2911	51	0.3288	51	0.2946	52	0.1346	55

Tabela 3.4: VZG i verovatnoća promene za homogeni sistem ortogonalnih kontrola parnosti, $m = 2$.

VZG, $m = 4$									
p / r	0.15		0.30		0.35		0.40		0.45	
1	0.1500	2	0.3000	8	0.3500	19	0.4000	63	0.4500	502
2	0.1500	2	0.3000	9	0.3500	20	0.4000	64	0.4500	502
3	0.1500	3	0.3000	9	0.3500	20	0.4000	64	0.4500	503
4	0.1455	3	0.3000	10	0.3500	21	0.4000	65	0.4500	503
6	0.1377	4	0.3000	11	0.3500	22	0.4000	66	0.4500	504
8	0.1289	5	0.3000	12	0.3500	23	0.4000	67	0.4500	505
10	0.1200	6	0.3000	13	0.3500	24	0.4000	68	0.4500	506
15	0.0997	9	0.3000	15	0.3500	26	0.4000	70	0.4500	509
20	0.0824	11	0.3000	18	0.3500	29	0.4000	73	0.4500	511
30	0.0567	16	0.3000	23	0.3500	34	0.4000	78	0.4500	516
40	0.0394	21	0.2998	28	0.3500	39	0.4000	83	0.4500	521
50	0.0276	26	0.2995	33	0.3500	44	0.4000	88	0.4500	526
100	0.0050	51	0.2953	58	0.3500	69	0.4000	113	0.4500	551
Verovatnoća promene, $m = 4$										
1	0.0000	2	0.0000	8	0.0000	19	0.0000	63	0.0000	502
2	0.0000	2	0.0000	9	0.0000	20	0.0000	64	0.0000	502
3	0.0000	3	0.0000	9	0.0000	20	0.0000	64	0.0000	503
4	0.0399	3	0.0000	10	0.0000	21	0.0000	65	0.0000	503
6	0.0675	4	0.0000	11	0.0000	22	0.0000	66	0.0000	504
8	0.0865	5	0.0000	12	0.0000	23	0.0000	67	0.0000	505
10	0.1002	6	0.0000	13	0.0000	24	0.0000	68	0.0000	506
15	0.0897	9	0.0000	15	0.0000	26	0.0000	70	0.0000	509
20	0.1323	11	0.0000	18	0.0000	29	0.0000	73	0.0000	511
30	0.1428	16	0.0007	23	0.0000	34	0.0000	78	0.0000	516
40	0.1470	21	0.0029	28	0.0000	39	0.0000	83	0.0000	521
50	0.1488	26	0.0069	33	0.0000	44	0.0000	88	0.0000	526
100	0.1502	51	0.0397	58	0.0000	69	0.0000	113	0.0000	551

Tabela 3.4: (nastavak) VZG i verovatnoća promene za homogeni sistem ortogonalnih kontrola parnosti, $m = 4$.

r	$m=2$		$m=4$		$m=6$	
	p	ζ_g	p	ζ_g	p	ζ_g
1	0.02001	1	0.02001	1	0.02001	1
2	0.22816	2	0.06118	1	0.02752	2
3	0.32699	3	0.12652	3	0.06952	2
4	0.37236	4	0.16602	4	0.09783	3
6	0.41590	6	0.21307	6	0.13377	5
8	0.43718	8	0.24156	8	0.15668	8
10	0.44984	10	0.26134	9	0.17317	10
15	0.46662	15	0.29305	14	0.20067	15
20	0.47497	19	0.31271	19	0.21849	20
30	0.48332	29	0.33709	30	0.24156	29
40	0.48748	39	0.35231	39	0.25664	39
50	0.48930	48	0.36113	48	0.26568	48
100	0.49284	84	0.37960	86	0.28550	86

Tabela 3.5: Granična verovatnoća p iznad koje je VZG za homogeni sistem ortogonalnih kontrola parnosti jednaka p

za proizvoljno p, $0 < p < 1/2$. □

Za zadatu LKM **H** VZG zavisi samo od verovatnoće greške p. Oblik ove funkcije je u opštem slučaju vrlo komplikovan, pa se najjednostavnije može analizirati numerički.

Primer 3.6 Za sledeće tri LKM

$$\mathbf{H}' = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{bmatrix},$$

$$\mathbf{H}'' = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}$$

i

$$\mathbf{H}''' = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix},$$

data je u Tabeli 3.6 vrednost VZG kad je $p = 0.0(0.01)0.36$. Za sve ove vrednosti p najmanja je vrednost VZG za $\mathbf{H}'$, a najveća za LKM $\mathbf{H}''$. S obzirom da su dimenzije odgovarajućih linearnih kodova redom $2, 3, 4$, ovaj odnos se ne može objasniti na jednostavan način. U sva tri slučaja postoji granica za verovatnoću p (manja od 0.36) iznad koje je VZG jednaka p. □

Činjenica da za neke LKM postoji granica za verovatnoću p iznad koje je VZG identički jednaka p, može se objasniti na osnovu sledeće teoreme.

Teorema 3.5 *Posmatrajmo linearni (n, k) kod određen lokalnom kontrolnom matricom $\mathbf{H}$ dimenzija $r \times n$, $r = n - k$. Neka je sa l označen broj kodnih reči težine dva u dualnom kodu, takvih da im je prva koordinata jednaka jedinici. Ako je $l \geq 2$ onda postoji broj p_0, $0 < p_0 < 1/2$, takav da je za proizvoljnu verovatnoću greške p, $p_0 < p < 1/2$, VZG strogo manja od p. Ako je pak $l = 0$, onda postoji broj p_0, $0 < p_0 < 1/2$, takav da je za svako p, $p_0 < p < 1/2$, VZG jednaka p.* □

DOKAZ. Neka je $\mathbf{s}$ proizvoljni fiksirani sindrom. Koset koji odgovara sindromu $\mathbf{s}$ je skup vektora koji zadovoljavaju sistem jednačina $\mathbf{He} = \mathbf{s}$. Ovaj sistem jednačina može se rešiti tako da se neke koordinate vektora $\mathbf{e}$ izraze kao linearne kombinacije ostalih koordinata (nezavisnih promenljivih) i koordinata sindroma. Pri tome se zbog oblika matrice $\mathbf{H}$ (svi elementi njene prve kolone su jedinice) koordinata e_1 uvek može svrstati u grupu nezavisnih promenljivih. Neka su (za $l > 0$) sa e_{i_j}, $1 \leq j \leq l$, označene promenljive za koje dualni kod sadrži vektor težine dva, sa jedinicama na pozicijama jedan i i_j, $1 \leq j \leq l$. Ove promenljive nisu među nezavisnim promenljivim, jer im je vrednost jednoznačno određena vrednošću nezavisne promenljive e_1. Ostale zavisne promenljive su očigledno linearne kombinacije nezavisnih promenljivih, od kojih je bar jedna različita od e_1.

Posmatrajmo razliku $\Delta_{\mathbf{s}}$ broja jedinica u skupovima vektora $C_{\mathbf{s},0}$ i $C_{\mathbf{s},1}$ (3.8), odnosno razliku suma težina njihovih članova. Elementi skupova $C_{\mathbf{s},0}$ i $C_{\mathbf{s},1}$ mogu se napisati u obliku tablica koje u svakoj vrsti sadrže po jedan vektor. Koordinate vektora se mogu tako ispermutovati da se najpre napišu koordinate koje odgovaraju nezavisnim, a zatim

p	LKM		
	H'	H''	H'''
0.01	0.000588	0.000683	0.000590
0.02	0.002306	0.002667	0.002320
0.03	0.005084	0.005855	0.005130
0.04	0.008857	0.010157	0.008961
0.05	0.013561	0.015485	0.013754
0.06	0.019134	0.021755	0.019449
0.07	0.025517	0.028888	0.025989
0.08	0.032652	0.036807	0.033317
0.09	0.040484	0.045441	0.041377
0.10	0.048960	0.054720	0.050112
0.11	0.058028	0.064580	0.059469
0.12	0.067638	0.074957	0.069395
0.13	0.077744	0.085795	0.079837
0.14	0.088298	0.097037	0.090745
0.15	0.099259	0.108630	0.102070
0.16	0.110582	0.120526	0.113764
0.17	0.122228	0.132677	0.125781
0.18	0.134158	0.145040	0.138075
0.19	0.146334	0.157574	0.150605
0.20	0.158720	0.170240	0.163328
0.21	0.171282	0.183002	0.176205
0.22	0.183988	0.195827	0.189197
0.23	0.196806	0.208683	0.202269
0.24	0.209705	0.221541	0.215386
0.25	0.222656	0.234376	0.228516
0.26	0.235633	0.247159	0.241626
0.27	0.248609	0.259869	0.254689
0.28	0.261557	0.272486	0.267677
0.29	0.274456	0.284989	0.280565
0.30	0.287280	0.297360	0.293328
0.31	0.300008	0.309583	0.305945
0.32	0.312620	0.320000	0.318395
0.33	0.325094	0.330000	0.330000
0.34	0.337411	0.340000	0.340000
0.35	0.349554	0.350000	0.350000
0.36	0.360000	0.360000	0.360000

Tabela 3.6: Zavisnost VZG od verovatnoće greške za tri LKM

zavisnim promenljivim. Bez gubitka opštosti može se pretpostaviti da promenljivoj e_1 odgovara prva kolona u obe tablice. U prvoj koloni tablice koja odgovara skupu $C_{\mathbf{s},1}$ ima 2^{r-1} jedinica, a u prvoj koloni tablice koja odgovara skupu $C_{\mathbf{s},0}$ ima 2^{r-1} nula.

Pretpostavimo najpre da je $l = 0$. U svakoj koloni sem prve, u oba skupa, broj jedinica jednak je broju nula. Zbog toga je zbir težina elemenata skupa $C_{\mathbf{s},1}$ veći od zbira težina elemenata skupa $C_{\mathbf{s},0}$ za 2^{r-1}, što znači da je u ovom slučaju $\Delta_{\mathbf{s}} = -2^{r-1}$, za svaki sindrom $\mathbf{s} \in B_r$.

Neka je sada $l \geq 2$. Kad sindrom $\mathbf{s}$ prolazi kroz skup B_r tada i vektor slobodnih koeficijenata (u r jednakosti kojima se zavisne promenljive izražavaju kao linearne kombinacije nezavisnih promenljivih i koordinata sindroma) prolazi kroz skup B_r. Zbog toga postoji takav sindrom $\mathbf{s}'$ da se zavisne promenljive e_{i_j} izražavaju jednakostima $e_{i_j} = e_1 \oplus 1$, $1 \leq j \leq l$. Tada je $\Delta_{\mathbf{s}'} = (l-1)2^{r-1} > 0$, jer l kolona tablice vektora skupa $C_{\mathbf{s}',0}$ ($C_{\mathbf{s}',1}$) koje odgovaraju promenljivim e_{i_j} sadrže 2^{r-1} nula (jedinica), $1 \leq j \leq l$.

Označimo sa $\alpha_{\mathbf{s},i}$, odnosno $\beta_{\mathbf{s},i}$ broj vektora težine i, $0 \leq i \leq n$, u skupu $C_{\mathbf{s},0}$, odnosno $C_{\mathbf{s},1}$. Za proizvoljno $\mathbf{s} \in B_r$ označimo sa $\psi_{\mathbf{s}}(p)$ razliku verovatnoća $P(C_{\mathbf{s},0}) - P(C_{\mathbf{s},1})$. Tada je

$$\psi_{\mathbf{s}}(p) = \sum_{i=0}^{n} (\alpha_{\mathbf{s},i} - \beta_{\mathbf{s},i})\, p^i (1-p)^{n-i},$$

odnosno posle smene $p = \frac{1}{2} - \frac{\epsilon}{2}$

$$\psi_{\mathbf{s}}(p) = 2^{-n} \sum_{i=0}^{n} (\alpha_{\mathbf{s},i} - \beta_{\mathbf{s},i})\, (1-\epsilon)^i (1+\epsilon)^{n-i}.$$

Razvojem ove funkcije u Tejlorov red u okolini $\epsilon = 0$ dobija se da je

$$\psi_{\mathbf{s}}(p) = 2^{-n}(1+n\epsilon) \sum_{i=0}^{n} (\alpha_{\mathbf{s},i} - \beta_{\mathbf{s},i}) - 2^{1-n}\epsilon \sum_{i=0}^{n} (i\alpha_{\mathbf{s},i} - i\beta_{\mathbf{s},i}) + O(\epsilon^2).$$

U ovoj jednakosti je $\sum_{i=0}^{n} (\alpha_{\mathbf{s},i} - \beta_{\mathbf{s},i}) = 0$ (skupovi $C_{\mathbf{s},0}$ i $C_{\mathbf{s},1}$ imaju isti broj elemenata) i $\sum_{i=0}^{n} (i\alpha_{\mathbf{s},i} - i\beta_{\mathbf{s},i}) = \Delta_{\mathbf{s}}$ (jer je na primer proizvod $i\alpha_{\mathbf{s},i}$ jednak broju jedinica u u vektorima težine i skupa $C_{\mathbf{s},0}$), pa je

$$\psi_{\mathbf{s}}(p) = -2^{1-n}\epsilon\Delta_{\mathbf{s}} + O(\epsilon^2).$$

Prema tome, ako je $l = 0$, onda je $\Delta_{\mathbf{s}} < 0$ za svaki sindrom $\mathbf{s} \in B_r$, pa postoji takvo p_0, $0 < p_0 < 1/2$, da za svako $\mathbf{s} \in B_r$ važi nejednakost $\psi_{\mathbf{s}}(p) > 0$, odnosno $P(C_{\mathbf{s},0}) > P(C_{\mathbf{s},1})$. Za $p_0 < p < 1/2$ se tada na osnovu (3.27) dobija

$$P\{E_1^* = 1\} = \sum_{\mathbf{s} \in B_r} P(C_{\mathbf{s},1}) = p.$$

U drugom slučaju, kad je $l \geq 2$, postoji takav sindrom $\mathbf{s}'$ da je $\Delta_{\mathbf{s}'} > 0$. Zbog toga postoji broj p_0, $0 < p_0 < 1/2$, takav da je

$$\psi_{\mathbf{s}'}(p) = P\left(C_{\mathbf{s}',0}\right) - P\left(C_{\mathbf{s}',1}\right) < 0$$

za svako p, $p_0 < p < 1/2$, pa je

$$\begin{aligned} P\{E_1^* = 1\} &= P(C_{\mathbf{s}',0}) + \sum_{\mathbf{s} \in B_r, \mathbf{s} \neq \mathbf{s}'} \min\left\{P(C_{\mathbf{s},0}), P(C_{\mathbf{s},1})\right\} \\ &\leq P(C_{\mathbf{s}',0}) + \sum_{\mathbf{s} \in B_r, \mathbf{s} \neq \mathbf{s}'} P(C_{\mathbf{s},1}) \\ &< \sum_{\mathbf{s} \in B_r} P(C_{\mathbf{s},1}) = p. \end{aligned}$$

Time je završen dokaz teoreme. □

Ako se pretpostavi da su LKM koje se koriste za dekodiranje kodova $R_{h,n}$ takve da u odgovarajućim dualnim kodovima nema kodnih reči težine manje od tri, tada one zadovoljavaju uslove dokazane teoreme, pa za njih postoji granica p_0, $0 < p_0 < 1/2$, takva da je za $p_0 < p < 1/2$ VZG jednaka p.

Izračunavanje VZG i verovatnoće promene u opštem slučaju je težak problem, jer je na primer numerička složenost izračunavanja VZG prema izrazu (3.27) $O(n2^n)$. Izvesna ušteda može se postići izračunavanjem VZG na osnovu jednostavnije "ekvivalentne" LKM i na odgovarajući način transformisanog vektora verovatnoća $\mathbf{p}$, na osnovu sledeće teoreme, analogne Teoremi 3.2.

Teorema 3.6 *Neka su kolone LKM* $\mathbf{H}$ *sa indeksima iz skupa* $\mathbf{i} = \{i_1, i_2, \ldots, i_l\}$ *jednake,* $1 \notin \mathbf{i}$, *i neka je raspodela verovatnoća na skupu* B_n *određena jednakošću (3.7) i vektorom* $\mathbf{p}$. *Pretpostavimo da su matrica* $\mathbf{H}'$ *i vektor* $\mathbf{p}'$ *formirani na način opisan u Teoremi 3.2. Tada su*

VZG i verovatnoća promene za LKM $\mathbf{H}$, *sa vektorom verovatnoća* $\mathbf{p}$, *jednake VZG i verovatnoći promene za LKM* $\mathbf{H}'$, *sa vektorom verovatnoća* $\mathbf{p}'$. □

DOKAZ. Neka je $\mathbf{e} \in B_n$, $\mathbf{E}$ – slučajni vektor greške, i neka su vektor $\mathbf{e}' \in B_{n-l+1}$ i slučajna vektorska promenljiva $\mathbf{E}'$ formirani od vektora $\mathbf{e}$ i slučajne promenljive $\mathbf{E}$ na isti način kao vektor $\mathbf{y}'$ od vektora $\mathbf{y}$ u iskazu Teoreme 3.2. Realizacija slučajne promenljive $\mathbf{E}$ jednoznačno određuje realizaciju slučajne promenljive $\mathbf{E}'$. Ako se u oba koda fiksiraju nulti vektori kao kodne reči, realizacije vektora $\mathbf{E}$ i $\mathbf{E}'$ su primljene poruke. Na osnovu Teoreme 3.2 za svaku realizaciju $\mathbf{e} \in B_n$ slučajne promenljive $\mathbf{E}$, realizacije AVG $\hat{p}_1 = \hat{p}_1(\mathbf{H}, \mathbf{e}, \mathbf{p})$ i $\hat{p}'_1 = \hat{p}_1(\mathbf{H}', \mathbf{e}', \mathbf{p}')$ su jednake. Iz (3.26) sledi da su realizacije slučajne promenljive E_1^* (zaostale greške) i slučajne promenljive

$$E_1^{*\prime} = I\left(E'_1 = 1, \hat{P}'_1 \leq \frac{1}{2}\right) + I\left(E'_1 = 0, \hat{P}'_1 > \frac{1}{2}\right)$$

jednake za svaku realizaciju slučajne promenljive $\mathbf{E}$, pa su i odgovarajuće VZG jednake. Slično se pokazuje da su i verovatnoće promene izračunate na ova dva načina jednake. □

Napomenimo da se VZG i verovatnoća promene pomoću ove teoreme mogu izračunavati na osnovu LKM sa manjim brojem kolona, ali da je zato raspodela verovatnoća na skupu B_{n-l+1} određena vektorom $\mathbf{p}'$ kome nisu jednake sve koordinate.

3.4 Analiza probabilističke faze kombinovanog algoritma

Polazeći od uopštenja nejednakosti Sullivana za odnos verovatnoća linearnog koda i njegovog proizvoljnog koseta u ovoj tački je formulisan dovoljan uslov za konvergenciju niza vektora verovatnoća $\left\{\mathbf{p}^{(j)}\right\}_{j\geq 0}$ u koracima 4^0 i 5^0 Algoritma 2.1. Za konkretni kod $R_{h,n}$ i verovatnoću greške p teško je tačno izračunati verovatnoću da ovaj dovoljan uslov bude ispunjen. Međutim, ta verovatnoća se može eksperimentalno

ocenjivati, što je demonstrirano na jednom primeru. Analiza konvergencije jednog sličnog probabilističkog algoritma dekodiranja izvedena je i u radu [Gall62], ali ne dovoljno egzaktno, jer se odnosi na prosečnu verovatnoću greške. Materijal izložen u ovoj tački zasniva se na radu [Živl90].

Pre nego što bude formulisano uopštenje nejednakosti Salivena (Teorema 3.7), najpre će biti uvedene neophodne oznake. Neka je q stepen prostog broja, a B_n aditivna grupa polja GF(q^n). Elementi B_n su vektori $\mathbf{v} = [v_1\ v_2\ \ldots\ v_n]^T$, gde je $v_i \in B_1$ za $1 \leq i \leq n$. Prilikom dokaza Teoreme 3.7 biće korišćena sledeća lema, direktno uopštenje leme J. L. Massey-a iz [Sull67] (u kojoj je tretiran slučaj $q = 2$). Elemenat $\mathbf{v}$ koseta C podgrupe G aditivne podgrupe GF(q^n) je koset–lider tog koseta ako u C nema elemenata manje težine (odnosno elemenata sa manje nenultih koordinata).

Lema 3.1 *Neka je G podgrupa grupe B_n, i neka je C pravi koset podgrupe G. Pretpostavimo da je $\mathbf{v}$ koset–lider koseta C, i $w(\mathbf{v}) = m < n$. Neka je G' podgrupa čiji se elementi dobijaju od elemenata podgrupe G zamenom nulama onih koordinata koje odgovaraju koordinatama $\mathbf{v}$ različitim od nule. Tada je red podgrupe G' jednak redu podgrupe G.* □.

DOKAZ. Pretpostavimo da lema nije tačna, tj. da postoje elementi $\mathbf{a}, \mathbf{b} \in G$, $\mathbf{a} \neq \mathbf{b}$ od kojih se zamenom nulama koordinata odgovarajućih nenultim koordinatama vektora $\mathbf{v}$ dobija isti elemenat $\mathbf{c} \in G'$. Tada je $\mathbf{a} - \mathbf{b} \in G$, a sve koordinate elementa $\mathbf{a} - \mathbf{b}$ koje odgovaraju nultim koordinatama vektora $\mathbf{v}$ jednake su nuli. Zbog toga, suprotno pretpostavci o elementu $\mathbf{v}$, važi nejednakost $w(\mathbf{a} - \mathbf{b} + \mathbf{v}) < w(\mathbf{v})$, iako je $\mathbf{a} - \mathbf{b} + \mathbf{v} \in C$. Time je lema dokazana. □.

Podgrupa G je linearni potprostor linarnog prostora $(B_n, \oplus)$, odnosno linearni kod. Neka je $\mathbf{H}$ kontrolna matrica koda G. Dokazana lema ima sledeću očiglednu posledicu.

Posledica 3.2 *Ako je $\mathbf{v}$ koset–lider koseta C linearnog koda G, onda postoji informacioni skup koda G koji je podskup skupa indeksa nultih koordinata vektora $\mathbf{v}$.* □

Na skupu B_n definiše se raspodela verovatnoća $P(\cdot)$ tako da je za svako $A \subset B_n$

$$P(A) = \sum_{\mathbf{v} \in A} \prod_{i=1}^{n} p_{i,v_i}. \tag{3.33}$$

Ovde su $p_{i,j}$, $1 \leq i \leq n$, $0 \leq j < q$, realni nenegativni brojevi koji zadovoljavaju uslove

$$\begin{cases} \sum_{j=0}^{q-1} p_{i,j} = 1 \\ p_{i,0} \geq p_{i,j}, \quad 1 \leq j < q \end{cases}, \qquad 1 \leq i \leq n. \tag{3.34}$$

Neka je G proizvoljna podgrupa reda q^k grupe B_n, $1 \leq k < n$ (q–arni linearni kod), a C neki njegov koset. Problem nalaženja donje granice za odnos $P(G)/P(C)$ postavljen je i rešen u [Sull67] za slučaj kad je $q = 2$ i

$$p_{i,1} = p, \; p_{i,0} = 1 - p, \qquad 1 \leq i \leq n, \; 0 < p < 1/2. \tag{3.35}$$

Tada je

$$\frac{P(G)}{P(C)} \geq \frac{1 + (1-2p)^{k+1}}{1 - (1-2p)^{k+1}} > 1. \tag{3.36}$$

U radu [Redi73] je ova nejednakost dokazana na drugi način, a navedene su i njene moguće primene.

Neka je $\mathbf{j} = (j_1, j_2, \ldots, j_n)$ proizvoljna permutacija skupa indeksa $\{1, 2, \ldots, n\}$, k — celi broj, $0 \leq k < n$, i $u \in B_1$. Sa $C_{\mathbf{j},k,u}$ biće označen skup vektora

$$C_{\mathbf{j},k,u} = \left\{ \mathbf{v} \in B_n \mid v_{j_1} + \cdots + v_{j_{k+1}} = u, \; v_{j_{k+2}} = \cdots = v_{j_n} = 0 \right\}. \tag{3.37}$$

Skup $C_{\mathbf{j},k,0}$ je podgrupa reda 2^k, a skupovi $C_{\mathbf{j},k,u}$ su koseti ove podgrupe za $u \neq 0$.

Lako se pokazuje da je za $q = 2$ donja granica odnosa $P(G)/P(C)$ u (3.36) jednaka odnosu $P(C_{\mathbf{j},k,0})/P(C_{\mathbf{j},k,1})$. Donja granica za odnos verovatnoća $P(G)/P(C)$ u opštem slučaju, kad raspodela verovatnoća $P(\cdot)$ na skupu B_n zadovoljava samo uslov (3.34) teže je odrediti. Šta više, za fiksirano $u \in B_1$, $u \neq 0$, ako je G neka podgrupa $C_{\mathbf{j},k,0}$ oblika (3.37), a C odgovarajući koset $C_{\mathbf{j},k,u}$, teško je odrediti permutaciju indeksa $\mathbf{j}$ za koju odnos verovatnoća $P(G)/P(C)$ dostiže najmanju vrednost.

Zbog toga će biti razmatran manje opšti slučaj kad raspodela verovatnoća $P(\cdot)$ zadovoljava pored uslova (3.34) i uslov

$$p_{i,j} = p_i, \qquad 1 \leq j < q,\ 1 \leq i \leq n, \tag{3.38}$$

a time i uslov

$$p_{i,0} = 1 - (q-1)p_i,\ p_i < 1/q, \qquad 1 \leq i \leq n. \tag{3.39}$$

Naravno, sistem uslova (3.38) i (3.39) važi ako i samo ako važi sistem uslova (3.34) i (3.38). Odnos verovatnoća $P(C_{\mathbf{j},k,0})/P(C_{\mathbf{j},k,u})$ za $u \neq 0$ može se tada izraziti jednakošću

$$\begin{aligned}\frac{P(C_{\mathbf{j},k,0})}{P(C_{\mathbf{j},k,u})} &= \frac{1+(q-1)\prod_{i=1}^{k+1}(1-qp_{j_i})}{1-\prod_{i=1}^{k+1}(1-qp_{j_i})} \\ &= 1-q+\frac{q}{1-\prod_{i=1}^{k+1}(1-qp_{j_i})}\,.\end{aligned}$$

Ako je permutacija $\mathbf{j}$ takva da je

$$p_{j_1} \geq p_{j_2} \geq \cdots \geq p_{j_n}, \tag{3.40}$$

a pored toga je i $p_{j_1} < 1/q$, tada je na osnovu prethodnog izraza za svako k, $1 \leq k < n$,

$$\frac{P(C_{\mathbf{j},k,0})}{P(C_{\mathbf{j},k,u})} \geq F_k(\mathbf{p}).$$

Ovde je funkcija $F_k(\mathbf{p})$ definisana posredstvom permutacije $\mathbf{j}$ (3.40)

$$F_k(\mathbf{p}) = \frac{1+(q-1)\prod_{i=1}^{k+1}(1-qp_{j_i})}{1-\prod_{i=1}^{k+1}(1-qp_{j_i})}\,. \tag{3.41}$$

U izrazu za $F_k(\mathbf{p})$ figuriše dakle $k+1$ najvećih koordinata vektora $\mathbf{p} = (p_1, p_2, \ldots, p_n)$. Ako je $p_{j_1} < 1/q$ tada funkcija $F_k(\mathbf{p})$ ima za svako k, $0 \leq k < n$, sledeće osobine (što se može neposredno proveriti).

OSOBINA 1. $F_k(\mathbf{p}) > 1$.

OSOBINA 2. $F_{k+1}(\mathbf{p}) \leq F_k(\mathbf{p})$.

OSOBINA 3. $F_k(\mathbf{p})$ je nerastuća funkcija po svakoj od koordinata vektora $\mathbf{p}$.

Pokazuje se da je donja granica odnosa $P(C_{\mathbf{j},k,0})/P(C_{\mathbf{j},k,u})$, $u \neq 0$, istovremeno i donja granica odnosa verovatnoća $P(G)/P(C)$, kad je G proizvoljna podgrupa reda q^k grupe B_n, C njen proizvoljan koset, a raspodela verovatnoća $P(\cdot)$ zadovoljava ograničenja (3.34) i (3.38). Sledeća teorema sadrži uopštenje nejednakosti (3.36) iz [Sull67].

Teorema 3.7 *Neka je raspodela verovatnoća na grupi B_n, data jednakošću (3.33), pri čemu parametri $p_{i,j}$, $1 \leq i \leq n$, $0 \leq j < q$, zadovoljavaju uslove (3.38) i (3.39). Ako je G proizvoljna podgrupa grupe B_n reda q^k, $0 \leq k < n$, a C proizvoljan (pravi) koset podgrupe G, onda važi nejednakost*

$$\frac{P(G)}{P(C)} \geq F_k(\mathbf{p}) > 1, \tag{3.42}$$

gde je $\mathbf{p} = (p_1, p_2, \ldots, p_n)$, permutacija $\mathbf{j}$ skupa indeksa $\{1, 2, \ldots, n\}$ je takva da važe nejednakosti (3.40), a funkcija $F_k(\mathbf{p})$ je definisana jednakošću (3.41). Odnos $P(G)/P(C)$ dostiže donju granicu u ovoj nejednakosti ako je $G = C_{\mathbf{j},k,0}$ i $C = C_{\mathbf{j},k,u}$, $u \neq 0$, videti (3.37), pri čemu je $\mathbf{j}$ opisana permutacija indeksa. □

DOKAZ. Tvrđenje teoreme biće dokazano indukcijom po k, $0 \leq k < n$, gde je q^k red podgrupe G. Za $k = 0$ je $G = \{\mathbf{0}\}$ i $C = \{\mathbf{v}\}$, pri čemu je sa $\mathbf{0}$ označen vektor čije su sve koordinate jednake nuli. Bez gubitka opštosti može se pretpostaviti da su koordinate elemenata linearnog prostora B_n tako permutovane da je $v_i = 0$ za $1 \leq i \leq n-m$, i $v_i = 1$ za $i > n-m$, gde je $m = w(\mathbf{v})$. Prema tome,

$$\begin{aligned}
\frac{P(G)}{P(C)} &= \frac{\prod_{i=1}^{n}(1-(q-1)p_i)}{\prod_{i=1}^{n-m}(1-(q-1)p_i)\prod_{i=n-m+1}^{n}p_i} \\
&= \prod_{i=n-m+1}^{n}\frac{1-(q-1)p_i}{p_i} > \frac{1-(q-1)p_n}{p_n} \\
&\geq \frac{1-(q-1)p_{j_1}}{p_{j_1}} = F_0(\mathbf{p}).
\end{aligned}$$

Pretpostavimo da je tvrđenje teoreme dokazano za sve podgrupe reda ne većeg od q^{k-1}. Neka je G podgrupa reda q^k, a C neka je njen

proizvoljni koset, pri čemu je elemenat $\mathbf{v}$ jedan od koset–lidera koseta C i $w(\mathbf{v}) = m$. Da je nejednakost (3.42) tačna za podgrupe reda q^k biće dokazano indukcijom po težini m koset–lidera.

Razmotrimo najpre slučaj $m = 1$. Bez gubitka opštosti može se pretpostaviti da prvih k pozicija u kodnim rečima predstavlja informacioni skup i da je $v_i = 0$ za $i \neq k+1$, $1 \leq i \leq n$ (odnosno da je indeks jedine koordinate koset–lidera različite od nule jednak $k+1$; ovo se može postići odgovarajućom permutacijom koordinata svih vektora).

Neka je sa $\mathbf{x}'$ označen vektor $[x_1\ x_2\ \ldots\ x_k]^T$, a sa $g(\mathbf{x}')$, odnosno $c(\mathbf{x}')$ vektori

$$g(\mathbf{x}') = [x_1\ x_2\ \ldots\ x_k\ L_{k+1}\ \ldots\ L_n]^T, \tag{3.43}$$

odnosno

$$c(\mathbf{x}') = g(\mathbf{x}') + \mathbf{v} = [x_1\ x_2\ \ldots\ x_k\ L_{k+1} + v_{k+1}\ \ldots\ L_n]^T. \tag{3.44}$$

Ovde su sa $L_i = L_i(\mathbf{x}')$, $1 \leq i \leq n$, označene odgovarajuće linearne kombinacije nezavisnih promenljivih $x_1, x_2, \ldots, x_k$. Jasno je da je

$$G = \{g(\mathbf{x}') \mid \mathbf{x}' \in B_k\}, \tag{3.45}$$

i

$$C = \{c(\mathbf{x}') \mid \mathbf{x}' \in B_k\}. \tag{3.46}$$

Skup B_k može se podeliti na q disjunktnih podskupova $\mathcal{D}_u$, $0 \leq u < q$, prema vrednosti linearne kombinacije $L_{k+1}(\mathbf{x}')$, $\mathbf{x}' \in B_k$,

$$\mathcal{D}_u = \{\mathbf{x}' \in B_k \mid L_{k+1}(\mathbf{x}') = u\},\ 0 \leq u < q.$$

Neka je sa T_u, $0 \leq u < q$, označena sledeća suma

$$T_u = \sum_{\mathbf{x}' \in \mathcal{D}_u} \left(\prod_{i=1}^{k} p_{i,x_i} \right) \left(\prod_{i=k+2}^{n} p_{i,L_i} \right).$$

Vrednosti parametara $p_{i,j}$, $1 \leq i \leq n$, $0 \leq j < q$, date su sa (3.38), odnosno (3.39). Verovatnoće $p_{i,0}$ biće označavane sa q_i, $1 \leq i \leq n$.

Skup $G_0 = \{g(\mathbf{x}') \mid \mathbf{x}' \in \mathcal{D}_0\}$ je podgrupa grupe G. Pretpostavimo najpre da je $G_0 = G$, odnosno da je $L_{k+1}(\mathbf{x}') \equiv 0$, $\mathbf{x}' \in B_k$. Tada je (videti Osobinu 2 funkcije F)

$$\frac{P(C)}{P(G)} = \frac{p_{k+1}}{q_{k+1}} \leq \frac{p_{j_1}}{q_{j_1}} = \phi_1(\mathbf{p}) \leq \phi_k(\mathbf{p}),$$

odnosno nejednakost (3.42) je u ovom slučaju tačna. Ovde je korišćena oznaka

$$\phi_k(\mathbf{p}) = 1/F_k(\mathbf{p}).$$

Neka je sada $L_{k+1}(\mathbf{x}') \neq 0$ za neko $\mathbf{x}' \in B_k$. Red podgrupe G_0 je tada q^{k-1}, a skupovi $G_u = \{g(\mathbf{x}') \mid \mathbf{x}' \in \mathcal{D}_u\}$, $1 \leq u < q$, su koseti podgrupe G_0. Neka je sa G'_u označen skup koji se od skupa G_u dobija brisanjem koordinate sa indeksom $k+1$ iz svih elemenata, $0 \leq u < q$, i neka je $\mathbf{p}' = (p_1, \ldots, p_k, p_{k+2}, \ldots, p_n)$. Skup G'_0 je na osnovu Leme podgrupa reda q^{k-1}, a skupovi G'_u su koseti ove podgrupe za $1 \leq u < q$. Kako je $P(G'_u) = T_u$, prema induktivnoj pretpostavci je

$$\frac{T_u}{T_0} \leq \phi_{k-1}(\mathbf{p}'), \qquad 1 \leq u < q. \tag{3.47}$$

Korišćenjem uvedenih oznaka, verovatnoće $P(G)$ i $P(C)$ mogu se izraziti jednakostima

$$P(G) = q_{k+1}T_0 + p_{k+1}T$$

i

$$P(C) = q_{k+1}T_{-v_{k+1}} + p_{k+1}\left(T + T_0 - T_{-v_{k+1}}\right),$$

gde je sa T označena suma $T = \sum_{u=1}^{q-1} T_u$. Indeksi se ovde smatraju elementima polja GF(q). Odnos verovatnoća $P(C)/P(G)$ je odavde

$$\frac{P(C)}{P(G)} = 1 - (q_{k+1} - p_{k+1}) \frac{1 - \frac{T_{-v_{k+1}}}{T_0}}{q_{k+1} + p_{k+1}\frac{T}{T_0}}.$$

Desna strana ove nejednakosti raste sa $T_{-v_{k+1}}/T_0$ i T/T_0, pa se korišćenjem nejednakosti (3.47) odavde dobija da je

$$\begin{aligned} \frac{P(C)}{P(G)} &\leq 1 - (q_{k+1} - p_{k+1}) \frac{1 - \phi_{k-1}(\mathbf{p}')}{q_{k+1} + p_{k+1}(q-1)\phi_{k-1}(\mathbf{p}')} \qquad (3.48) \\ &= \frac{1 - (1 - p_{k+1})(1 - \phi_{k-1}(\mathbf{p}'))}{1 - p_{k+1}(q-1)(1 - \phi_{k-1}(\mathbf{p}'))}. \end{aligned}$$

Neka su $j'_1, j'_2, \ldots, j'_k$ indeksi u vektoru $\mathbf{p}$ najvećih k koordinata vektora $\mathbf{p}'$. Tada je

$$\phi_{k-1}(\mathbf{p}') = \frac{1-\Pi}{1+(q-1)\Pi},$$

gde je sa Π označen proizvod $\Pi = \prod_{i=1}^{k}\left(1 - qp'_{j_i}\right)$. Zamenom u desnu stranu nejednakosti (3.48) dobija se

$$\frac{P(C)}{P(G)} \leq \frac{1-(1-qp_{k+1})\Pi}{1+(1-qp_{k+1})(q-1)\Pi}.$$

Neka je desna strana ove nejednakosti označena sa A. Zbog načina formiranja vektora $\mathbf{p}'$ je $j'_i \neq k+1$ za $1 \leq i \leq k$. Ukoliko je p_{k+1} jedna od $k+1$ najvećih koordinata vektora $\mathbf{p}$, tada je $A = \phi_k(\mathbf{p})$. U protivnom, zbog toga što je izraz A neopadajuća funkcija od p_{k+1}, polazeći od $p_{k+1} \leq p_{j_{k+1}}$, dobija se da je $A \leq \phi_k(\mathbf{p})$. Dakle, ako koset–lider $\mathbf{v}$ ima težinu jedan onda u oba slučaja važi nejednakost (3.42), tvrđenje Teoreme 3.7.

Pretpostavimo da je nejednakost dokazana za podgrupe reda ne većeg od q^{k-1}, kao i za podgrupe reda q^k sa kosetom za koji je težina koset–lidera manja od m, $m \geq 1$. Neka je G proizvoljna podgrupa reda q^k i neka je C bilo koja njena podgrupa. Neka je $\mathbf{v}$ jedan od koset–lidera podgrupe C, pri čemu je $w(\mathbf{v}) = m$. Slično kao u slučaju $m = 1$, bez gubitka opštosti se može pretpostaviti da je $\{1, 2, \ldots, k\}$ informacioni skup koda (grupe) G, a da su indeksi različitih od nule koordinata vektora $\mathbf{v}$ upravo $k+1, k+2, \ldots, k+m$. Elementi grupe G mogu se predstaviti u obliku (3.43), a elementi koseta C u obliku

$$c(\mathbf{x}') = g(\mathbf{x}') + \mathbf{v} =$$
$$= [x_1 \ \ldots \ x_k \ L_{k+1} + v_{k+1} \ \ldots \ L_{k+m} + v_{k+m} \ \ldots \ L_n]^T, \ \mathbf{x}' \in B_k,$$

tj. važe jednakosti (3.45) i (3.46). Skup B_k može se podeliti na q disjunktnih podskupova $\mathcal{D}_u$, $0 \leq u < q$, prema vrednosti linearne kombinacije $L_{k+m}(\mathbf{x}')$ na sledeći, način

$$\mathcal{D}_u = \{\mathbf{x}' \in B_k \mid L_{k+m}(\mathbf{x}') = u\}, \ 0 \leq u < q.$$

Neka je sa T_u, odnosno R_u, $0 \leq u < q$, označena suma

$$T_u = \sum_{\mathbf{x}' \in \mathcal{D}_u} \left(\prod_{i=1}^{k} p_{i,x_i}\right)\left(\prod_{i=k+1}^{k+m-1} p_{i,L_i}\right)\left(\prod_{i=k+m+1}^{n} p_{i,L_i}\right),$$

odnosno

$$R_u = \sum_{\mathbf{x}' \in \mathcal{D}_u} \left(\prod_{i=1}^{k} p_{i,x_i} \right) \left(\prod_{i=k+1}^{k+m-1} p_{i,L_i+v_i} \right) \left(\prod_{i=k+m+1}^{n} p_{i,L_i} \right).$$

Vrednosti parametara $p_{i,s}$, $1 \leq i \leq n$, $0 \leq s < q$, date su sa (3.38), i (3.39). Verovatnoće $P(G)$, odnosno $P(C)$, mogu se izraziti jednakostima

$$P(G) = q_{k+m} T_0 + p_{k+m} T \tag{3.49}$$

odnosno

$$P(C) = q_{k+m} R_{-v_{k+m}} + p_{k+m} \left(R - R_{-v_{k+m}} + R_0 \right), \tag{3.50}$$

pri čemu su sa T, odnosno R, označene sume $T = \sum_{u=1}^{q-1} T_u$, odnosno $R = \sum_{u=1}^{q-1} R_u$. Neka je G' podgrupa koja se od grupe G dobija tako što se u svim njenim elementima koordinata sa indeksom $k+m$ zameni nulom. Slično, neka je C' skup vektora koji se od skupa C dobija tako što se u svim njegovim elementima koordinata sa indeksom $k+m$ zameni nulom. Na osnovu Leme 1 red podgrupe G' je q^k. Skup C' je koset podgrupe G', a elemenat $\mathbf{v}' = [0 \ \ldots \ 0 \ v_{k+1} \ \ldots \ v_{k+m-1} \ 0 \ \ldots \ 0]^T$ je jedan od koset–lidera koseta C' (videti na primer [Pete72, Teorema 3.9]). Pošto je $w(\mathbf{v}') = m - 1$, na osnovu induktivne pretpostavke je

$$\frac{P(C')}{P(G')} \leq \phi_k(\mathbf{p}') < 1, \tag{3.51}$$

gde je $\mathbf{p}'$ vektor koji se od vektora $\mathbf{p}$ dobija brisanjem koordinate sa indeksom $k+m$. Zamenom $P(G') = q_{k+m}(T_0+T)$ i $P(C') = q_{k+m}(R_0+R)$ u prethodnu nejednakost, dobija se da je

$$\phi_k(\mathbf{p})(T_0 + T) \geq R_0 + R, \tag{3.52}$$

jer je $\phi_k(\mathbf{p}') \leq \phi_k(\mathbf{p})$.

Razmotrimo najpre slučaj $L_{k+m}(\mathbf{x}') \equiv 0$, $\mathbf{x}' \in B_k$. Zbog toga što je $\mathcal{D}_0 = B_k$, biće $G_0 = \{g(\mathbf{x}') \mid \mathbf{x}' \in \mathcal{D}_0\} = G$ i $T_u = R_u = 0$ za $1 \leq u < q$. Zamenom $P(G)$ sa $P(G')$, i $P(C)$ sa $(p_{k+m}/q_{k+m})\, P(C')$, na osnovu(3.51) dobija se da je

$$\frac{P(C)}{P(G)} = \frac{p_{k+m}}{q_{k+m}} \, \frac{P(C')}{P(G')} < \frac{p_{k+m}}{q_{k+m}} \leq \frac{p_{j_1}}{q_{j_1}} = \phi_0(\mathbf{p}) \leq \phi_k(\mathbf{p}).$$

Neka je sada $L_{k+m}(\mathbf{x}') \neq 0$ za neko $\mathbf{x}' \in B_k$. Skup G_0 je podgrupa reda q^{k-1} grupe G, a za proizvoljno u, $1 \leq u < q$, skup $C_u = \{c(\mathbf{x}') \mid \mathbf{x}' \in \mathcal{D}_u\}$ je koset podgrupe G_0. Na osnovu induktivne pretpostavke je za $u = -v_{k+m}$

$$\frac{P\left\{C_{-v_{k+m}}\right\}}{P(G_0)} = \frac{R_{-v_{k+m}}}{T_0} \leq \phi_{k-1}(\mathbf{p}),$$

odnosno

$$T_0\phi_k(\mathbf{p}) - R_{-v_{k+m}} > 0.$$

Polazeći od (3.52) i ove nejednakosti dobija se nejednakost

$$\begin{aligned} p_{k+m}\left(-\phi_k(\mathbf{p}')T + R_0 + R - R_{-v_{k+m}}\right) &\leq p_{k+m}\left(\phi_k(\mathbf{p})T_0 - R_{-v_{k+m}}\right) \\ &< q_{k+m}\left(\phi_k(\mathbf{p})T_0 - R_{-v_{k+m}}\right), \end{aligned}$$

odnosno, zbog (3.49) i (3.50), nejednakost $\phi_k(\mathbf{p})P(G) > P(C)$. Time je dokazano da nejednakost (3.42) važi za svako m, $m \geq 1$, za podgrupe reda q^k. Dakle, indukcijom je dokazano da nejednakost (3.42) važi za podgrupe proizvoljnog reda q^k, $0 \leq k < n$, čime je završen dokaz teoreme. □

U opštem slučaju kad raspodela verovatnoća $P(\cdot)$ na skupu B_n zadovoljava samo opšte uslove (3.34), neka je

$$p_i = \max\{p_{i,j} \mid 1 \leq j < q\} < 1/q, \qquad 1 \leq i \leq n,$$

i $\mathbf{p} = (p_1, p_2, \ldots, p_n)$. Interesantno bi bilo pod ovim pretpostavkama dokazati ili opovrgnuti nejednakost (3.42). Ovaj rezultat predstavljao bi dalje uopštenje Teoreme 3.7, a time i nejednakosti (3.36) iz rada [Sull67].

Neka je $\mathbf{x}$ kodna reč koja se propušta kroz kanal sa greškom. Vektor greške, slučajna promenljiva $\mathbf{E}$, ima raspodelu verovatnoća

$$P_{\mathbf{p}}\{\mathbf{E} = \mathbf{e}\} = \prod_{i=1}^{n} p_i^{e_i}(1-p_i)^{1-e_i}, \qquad \mathbf{e} \in B_n. \tag{3.53}$$

Primljena poruka je slučajna promenljiva $\mathbf{Y} = \mathbf{x} \oplus \mathbf{E}$. Za proizvoljan vektor $\mathbf{y} \in B_n$ funkcija $\mathcal{F}_{\mathbf{y}} : [0,1]^n \to [0,1]^n$ definiše se kao preslikavanje koje prevodi vektor $\mathbf{p}$ (koji na osnovu (3.53) određuje raspodelu

verovatnoća na skupu B_n) u vektor $\hat{\mathbf{p}}$ aposteriornih verovatnoća greške, sa koordinatama

$$\begin{aligned}\hat{p}_i &= P_{\mathbf{p}}\left(\{E_i = 1\} \mid \left\{\mathbf{H}^{(i)}\mathbf{E} = \mathbf{H}^{(i)}\mathbf{y}\right\}\right) \\ &= \frac{P_{\mathbf{p}}\left\{\mathbf{H}^{(i)}\mathbf{E} = \mathbf{H}^{(i)}\mathbf{y}, E_i = 1\right\}}{P_{\mathbf{p}}\left\{\mathbf{H}^{(i)}\mathbf{E} = \mathbf{H}^{(i)}\mathbf{y}\right\}}, \qquad 1 \le i \le n. \end{aligned} \tag{3.54}$$

Neka je niz vektora $\left\{\mathbf{p}^{(j)}\right\}_{j\ge 0}$ zadat uslovom

$$\mathbf{p}^{(0)} = (p, p, \ldots, p), \tag{3.55}$$

(gde je p verovatnoća greške u BSK, $0 < p < 1/2$) i rekurentnom relacijom

$$\mathbf{p}^{(j+1)} = \mathcal{F}_{\mathbf{y}}\left(\mathbf{p}^{(j)}\right), \qquad j \ge 0. \tag{3.56}$$

U koracima 4^0 i 5^0 Algoritma 2.1 izračunavaju se članovi upravo ovog rekurentnog niza vektora. Realizacija vektora greške $\mathbf{E}$ može se oceniti vektorom $\bar{\mathbf{e}}$ dobijenim od vektora $\mathbf{p}^{(d)}$ za neki fiksirani prirodni broj d zaokruživanjem na jednu binarnu cifru, tj.

$$\bar{e}_i = \begin{cases} 0, & p_i^{(d)} \le 1/2 \\ 1, & p_i^{(d)} > 1/2 \end{cases}. \tag{3.57}$$

Razmotrimo pojednostavljeni algoritam dekodiranja (u daljem tekstu Algoritam P) kod koga se predata kodna reč ocenjuje vektorom $\bar{\mathbf{e}} \oplus \mathbf{y}$. Ako je vektor $\bar{\mathbf{e}} \oplus \mathbf{y}$ kodna reč, onda se on usvaja za rezultat dekodiranja, a u protivnom se dekodiranje smatra neuspešnim. Dekodiranje je neuspešno i ako kodna reč $\bar{\mathbf{e}} \oplus \mathbf{y}$ nije jednaka kodnoj reči $\mathbf{x}$ dovedenoj na ulaz BSK.

Za $d = 1$ Algoritam P je ustvari poznati algoritam dekodiranja simbol–po–simbol, videti na primer [Hart76]. Ponavljanje izračunavanja aposteriornih verovatnoća grešaka ima heurističku motivaciju, a omogućuje da na odluku o svakom bitu greške utiče veći deo primljene poruke (videti [Gall62] i [Meie89]).

Od interesa je ustanoviti pod kojim uslovima konvergira niz vektora $\left\{\mathbf{p}^{(j)}\right\}_{j\ge 0}$, zadat sa (3.55) i (3.56). Zaista, ako ovaj niz vektora konvergira, onda za dovoljno veliko $d' > 0$ vektori $\bar{\mathbf{e}}$ formirani zaokruživanjem (3.57) koordinata vektora $\mathbf{p}^{(d)}$, $d > d'$, ne zavise od d. Naredna teorema daje dovoljan uslov konvergencije ovog niza vektora.

Teorema 3.8 *Neka je C linearni (n,k) kod sa kontrolnom matricom* $\mathbf{H}$. *Za $1 \leq i \leq n$ neka su vrste matrice $\mathbf{H}^{(i)}$ neki linearno nezavisni vektori iz dualnog koda. Neka je $\mathbf{y} \in B_n$ i neka je niz vektora $\left\{\mathbf{p}^{(j)}\right\}_{j\geq 0}$ definisan uslovom (3.55) i rekurentnom relacijom (3.56), pri čemu je p, $0 < p < 1/2$, proizvoljno. Ako za neko $\mathbf{x} \in C$ i za neko $d > 0$ koordinate vektora $\mathbf{p}^{(d)}$ zadovoljavaju uslov*

$$p_i^{(d)} \begin{cases} < 1/2, & y_i = x_i \\ > 1/2, & y_i \neq x_i \end{cases}, \qquad 1 \leq i \leq n, \tag{3.58}$$

onda je

$$\lim_{j\to\infty} p_i^{(j)} = \begin{cases} 0, & y_i = x_i \\ 1, & y_i \neq x_i \end{cases}, \qquad 1 \leq i \leq n. \qquad \square$$

DOKAZ. Neka je slučajna promenljiva $\mathbf{E}'$ data sa $\mathbf{E}' = \mathbf{E} \oplus \mathbf{x} \oplus \mathbf{y}$ i neka su članovi niza vektora $\left\{\bar{\mathbf{p}}^{(j)}\right\}_{j\geq 0}$ definisani jednakostima

$$\bar{p}_i^{(j)} = \begin{cases} \mathbf{p}_i^{(j)}, & y_i = x_i \\ 1 - \mathbf{p}_i^{(j)}, & y_i \neq x_i \end{cases}, \qquad 1 \leq i \leq n,\ j \geq 0. \tag{3.59}$$

Slučajna promenljiva $\mathbf{E}$ ima raspodelu verovatnoća određenu vektorom $\mathbf{p}^{(j)}$ ako i samo ako slučajna promenljiva $\mathbf{E}'$ ima raspodelu verovatnoća određenu vektorom $\bar{\mathbf{p}}^{(j)}$, $j \geq 0$. Niz $\left\{\bar{\mathbf{p}}^{(j)}\right\}_{j\geq 0}$ zadovoljava rekurentnu relaciju

$$\bar{\mathbf{p}}^{(j+1)} = \mathcal{F}_0\left(\bar{\mathbf{p}}^{(j)}\right), \qquad j \geq 0.$$

Zaista, neka je $j \geq 0$ i neka je $\mathcal{F}_0\left(\bar{\mathbf{p}}^{(j)}\right) = \hat{\mathbf{p}}$. Tada su prema definiciji funkcije $\mathcal{F}$ koordinate vektora $\hat{\mathbf{p}}$ date sa

$$\begin{aligned}
\hat{p}_i &= P_{\bar{\mathbf{p}}^{(j)}}\left(\{E_i = 1\} \mid \left\{\mathbf{H}^{(i)}\mathbf{E} = \mathbf{0}\right\}\right) \\
&= P_{\mathbf{p}^{(j)}}\left(\{E_i' = 1\} \mid \left\{\mathbf{H}^{(i)}\mathbf{E}' = \mathbf{0}\right\}\right) \\
&= P_{\mathbf{p}^{(j)}}\left(\{E_i = 1 \oplus x_i \oplus y_i\} \mid \left\{\mathbf{H}^{(i)}\mathbf{E} = \mathbf{H}^{(i)}\mathbf{y}\right\}\right) \\
&= \begin{cases} \mathbf{p}_i^{(j+1)}, & x_i = y_i \\ 1 - \mathbf{p}_i^{(j+1)}, & x_i \neq y_i \end{cases} = \bar{p}_i^{(j+1)}, \qquad 1 \leq i \leq n,
\end{aligned}$$

tj. $\mathcal{F}_{\mathbf{y}}(\bar{\mathbf{p}}^{(j)} = \bar{\mathbf{p}}^{(j+1)}$. Koordinate vektora $\bar{\mathbf{p}}^{(d)}$ zbog (3.59) i uslova teoreme (3.58) zadovoljavaju nejednakosti

$$\bar{p}_i^{(d)} < 1/2, \qquad 1 \leq i \leq n. \tag{3.60}$$

Označimo sa C_i^u skup vektora koji se od skupa

$$\left\{\mathbf{e} \in B_n \mid \mathbf{H}^{(i)}\mathbf{e} = \mathbf{0},\ e_i = u\right\}$$

dobija brisanjem i–te koordinate u svakom elementu, $u \in \{0,1\}$, $1 \leq i \leq n$. Skup C_i^0 je podgrupa reda 2^{k_i} ($k_i \geq k$) grupe B_{n-1}, a skup C_i^1 je njen koset, $1 \leq i \leq n$. Neka je

$$a_i^{(j)} = \frac{1 - \bar{p}_i^{(j)}}{\bar{p}_i^{(j)}} = \frac{1}{\bar{p}_i^{(j)}} - 1, \qquad 1 \leq i \leq n,\ j \geq 0. \tag{3.61}$$

Neka je dalje $\bar{\mathbf{p}}^{(j,i)}$ vektor koji se od vektora $\bar{\mathbf{p}}^{(j)}$ dobija brisanjem i–te koordinate, $j \geq d$, $1 \leq i \leq n$, i neka je za $1 \leq i \leq n$ sa δ_i označena veličina

$$\delta_i = F_{k_i}\left(\bar{\mathbf{p}}^{(d,i)}\right).$$

Zbog (3.60) i Teoreme 3.7 je $\delta_i > 1$ za svako i, $1 \leq i \leq n$. Na osnovu (3.60) i (3.61) zaključuje se da je $a_i^{(d)} > 1$, $1 \leq i \leq n$. Polazeći od ovih nejednakosti može se indukcijom pokazati da za proizvoljno j, $j \geq d$, važe nejednakosti $a_i^{(j)} > 1$, $1 \leq i \leq n$, a za $j > d$ i nejednakost

$$a_i^{(j)} > a_i^{(j-1)}\delta_i > 1, \qquad 1 \leq i \leq n. \tag{3.62}$$

Ovo tvrđenje je za $j = d$ očigledno tačno. Pretpostavimo da je tvrđenje tačno za $d, d+1, \ldots, j$. Na osnovu Teoreme 3.7 za $j > d$ je

$$\frac{P_{\bar{\mathbf{p}}^{(j,i)}}(C_i^0)}{P_{\bar{\mathbf{p}}^{(j,i)}}(C_i^1)} \geq F_{k_i}\left(\bar{\mathbf{p}}^{(j,i)}\right), \qquad 1 \leq i \leq n.$$

Prema induktivnoj pretpostavci zbog (3.61) koordinate vektora $\bar{\mathbf{p}}^{(j,i)}$ veće su od odgovarajućih koordinata vektora $\bar{\mathbf{p}}^{(d,i)}$, pa na osnovu Osobine 3 funkcije F

$$F_{k_i}\left(\bar{\mathbf{p}}^{(j,i)}\right) \geq F_{k_i}\left(\bar{\mathbf{p}}^{(d,i)}\right) = \delta_i, \qquad 1 \leq i \leq n.$$

Ova nejednakost je naravno tačna i za $j = d$. Polazeći od jednakosti (videti (3.54))

$$a_i^{(j+1)} = a_i^{(j)} \frac{P_{\bar{\mathbf{p}}^{(j,i)}}(C_i^0)}{P_{\bar{\mathbf{p}}^{(j,i)}}(C_i^1)},$$

i poslednje dve nejednakosti, pokazuje se da je $a_i^{(j+1)} > a_i^{(j)}\delta_i$, $1 \leq i \leq n$, pa je indukcijom dokazano da nejednakosti (3.62) važe za svako $j > d$. Neposredna posledica dokazanih nejednakosti je

$$\lim_{j\to\infty} a_i^{(j)} = +\infty, \qquad 1 \leq i \leq n,$$

i dalje, zbog (3.61)

$$\lim_{j\to\infty} \bar{p}_i^{(j)} = 0, \qquad 1 \leq i \leq n.$$

Iz ove jednakosti i (3.59) direktno sledi tvrđenje teoreme. □

Parametar p u ovoj teoremi ima proizvoljnu vrednost. Međutim, jasno je da je za uspešnu primenu Algoritma P neophodno da p bude upravo jednako verovatnoći greške u BSK na čijem je izlazu dobijena poruka $\mathbf{y}$.

Koordinate vektora $\mathbf{p}^{(1)}$ imaju jasnu interpretaciju, jer predstavljaju aposteriorne verovatnoće greške bita primljene poruke. Koordinate ostalih vektora $\mathbf{p}^{(2)}, \ldots$ ne mogu se interpretirati kao verovatnoće, što se može shvatiti kao izvestan nedostatak Algoritma P. Precizniji u ovom pogledu je algoritam za dekodiranje "kodova sa kontrolama parnosti male gustine" [Gall62]. Prilikom izračunavanja AVG nekog bita koriste se druge AVG, u čijem izračunavanju nisu korišćene kontrole parnosti koje sadrže polazni bit. Međutim, ovakav postupak izračunavanja AVG je nešto komplikovaniji, a ipak nije potpuno egzaktan, jer se posle malog broja iteracija obuhvataju (i više puta) sve koordinate kodne reči.

Razmotrimo sada praktični značaj Teoreme 3.8. Za $d = 1$ ona se može preformulisati na sledeći način: ako se može izvršiti simbol–po–simbol dekodiranje primljene poruke $\mathbf{y}$ korišćenjem LKM $\mathbf{H}^{(i)}$, $1 \leq i \leq n$, tada primena Algoritma P na poruku $\mathbf{y}$ vodi uspešnom dekodiranju. Značaj Teoreme 3.8 proističe iz činjenice da se Algoritam P završava uspešnim dekodiranjem i u drugim slučajevima, kad je uslov (3.58) zadovoljen za proizvoljno d, $d \geq 1$. Egzaktno izračunavanje verovatnoće

uspešnog dekodiranja za Algoritam P je vrlo komplikovano čak i za relativno jednostavne kodove. Međutim, postoji mogućnost da se ova verovatnoća oceni eksperimentalno.

Neka je $\mathbf{x}$ kodna reč koja se dovodi ulaz BSK. Pretpostavimo da vektor greške, slučajna promenljiva $\mathbf{E}$, ima raspodelu verovatnoća (3.53), pri čemu su sve koordinate vektora $\mathbf{p}$ jednake p, verovatnoći prelaza BSK. Neka je za $d \geq 1$ sa A_d označen skup vektora greške $\mathbf{e} \in B_n$ takvih da ako se Algoritam P primeni na vektor $\mathbf{y} = \mathbf{x} \oplus \mathbf{e}$, vektor $\mathbf{p}^{(d)}$ zadovoljava uslov (3.58). Iz dokaza Teoreme 3.8 sledi da je $A_1 \subseteq A_2 \subseteq \cdots$. Neka je za $d \geq 1$ slučajna promenljiva U_d definisana kao funkcija od slučajne promenljive $\mathbf{E}$,

$$U_d = I(\mathbf{E} \in A_d), \qquad d \geq 1.$$

Veličina $\alpha_d = P\{U_d = 1\} = P\{\mathbf{E}_d \in A_d\}$ je ustvari verovatnoća da vektor $\mathbf{p}^{(d)}$, $d \geq 1$, zadovolji uslov (3.58), pa prema tome i verovatnoća uspešnog dekodiranja ako se za dekodiranje koristi vektor $\mathbf{p}^{(d)}$. Prema tome, veličina α_d može se eksperimentalno određivati uobičajenim postupkom. Nezavisnim slučajnim promenljivim $\mathbf{E}^{(s)}$ sa istom raspodelom verovatnoća (3.53), $1 \leq s \leq n_e$, $n_e > 1$, odgovaraju nezavisne slučajne promenljive $U_d^{(s)}$, sa istom $0-1$ raspodelom verovatnoća. Slučajna promenljiva $n_e \bar{U}_d$, gde je

$$\bar{U}_d = \frac{1}{n_e} \sum_{s=1}^{n_e} U_d^{(s)},$$

ima binomnu raspodelu verovatnoće sa parametrima α_d i n_e. Zbog toga se parametar α_d ove binomne raspodele može oceniti sa $\alpha_d \simeq \bar{u}_d$, gde je $\bar{u}_d$ realizacija slučajne promenljive $\bar{U}_d$. Preciznije, sa verovatnoćom od oko 95% veličina α_d je u intervalu $[\bar{u}_d - 2\sigma_d, \bar{u}_d + 2\sigma_d]$, gde je

$$\sigma_d \simeq \sqrt{\bar{u}_d(1 - \bar{u}_d)/n_e}.$$

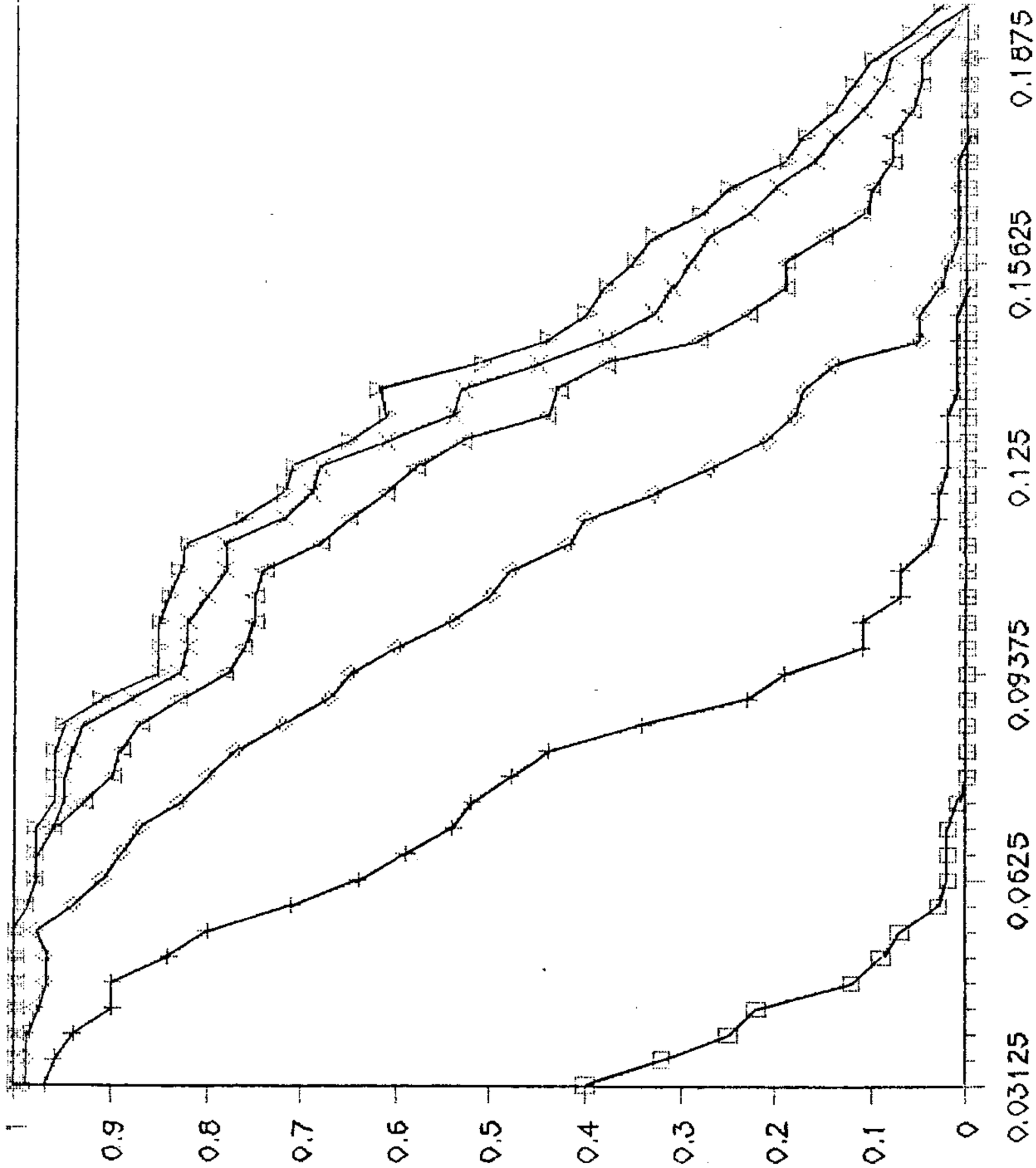
Napomenimo da izbor kodne reči $\mathbf{x}$ ne utiče na ishod eksperimenta, pa se može uzeti da je $\mathbf{x} = \mathbf{0}$. Opisana procedura može se ilustrovati sledećim primerom.

Primer 3.7 Neka je C linearni kod $R_{h,n}$, gde je $h(z) = 1 + z^{37} + z^{100}$, i $n = 512$. Sistemi kontrola parnosti koji odgovaraju LKM $\mathbf{H}^{(i)}$, formiranim pomoću Algoritma 3.1, $1 \leq i \leq n$, su ortogonalni.

Neka je fiksirana kodna reč $\mathbf{x} \in R_{h,n}$, verovatnoća p greške u BSK i parametar d, broj iteracija u Algoritmu P. Korišćenjem generatora slučajnih brojeva formirane su realizacije $\mathbf{e}^{(s)} \in B_{512}$, $1 \leq s \leq n_e = 100$, vektorskih slučajnih promenljivih $\mathbf{E}^{(s)}$, $1 \leq s \leq n_e$, sa raspodelom verovatnoća zadatom jednakošću (1.1). Na svaku od primljenih poruka $\mathbf{y}^{(s)} = \mathbf{x} \oplus \mathbf{e}^{(s)}$, $1 \leq s \leq n_e$, primenjen je Algoritam P, posle čega je registrovan broj uspešnih dekodiranja. Dobijeni rezultati za $p = 8/256(1/256)50/256$ i $d = 1(1)10$ prikazani su u Tabeli 3.7. Zavisnost ocene verovatnoće uspešnog dekodiranja od verovatnoće greške p prikazana je i na Slici 3.1, za $d = 1, 2, 3, 5, 7, 10$. Zapaža se da je za $p < 1/16$ verovatnoća uspešnog dekodiranja vrlo bliska jedinici, posle čega relativno brzo opada. □

Verovatnoća greške	Broj iteracija									
	1	2	3	4	5	6	7	8	9	10
0.031250	40	97	99	100	100	100	100	100	100	100
0.035156	32	96	99	100	100	100	100	100	100	100
0.039062	25	94	99	100	100	100	100	100	100	100
0.042968	22	90	98	99	100	100	100	100	100	100
0.046875	12	90	97	99	100	100	100	100	100	100
0.050781	9	84	97	99	100	100	100	100	100	100
0.054687	7	80	98	99	100	100	100	100	100	100
0.058593	3	71	94	96	99	99	99	99	99	99
0.062500	2	64	91	94	98	98	98	98	98	98
0.066406	2	59	89	92	98	98	98	98	98	98
0.070312	2	54	87	91	96	96	96	97	98	98
0.074218	1	52	83	89	93	93	95	95	96	96
0.078125	0	48	80	85	90	93	95	95	96	96
0.082031	0	44	77	84	89	92	94	94	95	96
0.085937	0	34	72	82	87	90	93	93	94	95
0.089843	0	23	67	79	83	87	88	88	90	91
0.093750	0	19	65	73	78	82	83	83	85	85
0.097656	0	11	60	71	76	81	82	84	85	85
0.101562	0	11	54	70	75	81	82	83	85	85
0.105468	0	7	50	67	75	80	80	82	83	84
0.109375	0	7	48	62	74	78	78	81	82	83
0.113281	0	4	42	58	68	74	78	80	81	82
0.117187	0	3	40	56	65	69	72	73	74	76
0.121093	0	3	33	50	61	67	69	69	70	72
0.125000	0	2	27	44	58	64	68	68	69	71
0.128906	0	2	21	40	53	59	61	62	63	65
0.132812	0	2	18	33	44	50	54	58	59	61
0.136718	0	1	17	32	43	49	53	56	59	62
0.140625	0	1	14	29	38	41	45	47	49	51
0.144531	0	1	5	19	28	34	38	40	42	44
0.148437	0	1	5	13	23	28	33	38	40	40
0.152343	0	0	3	11	19	25	31	35	37	38
0.156250	0	0	2	10	19	24	29	31	33	35
0.160156	0	0	1	9	15	22	27	29	31	33
0.164062	0	0	1	7	11	19	23	24	26	28
0.167968	0	0	1	7	10	17	20	21	23	25
0.171875	0	0	1	6	8	12	16	16	18	19
0.175781	0	0	0	4	8	12	14	15	16	17
0.179687	0	0	0	3	6	9	11	12	13	14
0.183593	0	0	0	3	5	7	9	11	11	12
0.187500	0	0	0	2	5	7	8	9	9	10
0.191406	0	0	0	1	2	3	4	4	5	6
0.195312	0	0	0	0	0	0	0	0	2	3

Tabela 3.7: Zavisnost broja uspešnih dekodiranja (od 100) od verovatnoće greške p



Slika 3.1: Zavisnost verovatnoće uspešnog dekodiranja od verovatnoće greške u primeru

Poglavlje 4

Kombinovani algoritam: faza pretrage

Svaki ciklus kombinovanog algoritma za dekodiranje kodova $R_{h,n}$ sastoji se, kao što je rečeno u poglavlju 2, od probabilističke faze i faze pretrage. Faza pretrage (koraci 8^0, 9^0 i 10^0 Algoritma 2.1) je ustvari algoritam dekodiranja korišćenjem slučajno izabranih informacionih skupova (videti na primer [Clar82, str. 102–131]. Postupak formiranja informacionih skupova opisan je u tački 4.1. Donošenje odluke da li je zadata kodna reč najbliža primljenoj poruci razmotreno je u tački 4.2, a algoritam pretrage po skupu kodnih reči koje se od primljene poruke na informacionom skupu razlikuju na ne više od zadatog broja mesta izložen je u tački 4.3.

4.1 Formiranje slučajnih informacionih skupova

Osnovna ideja *dekodiranja pomoću informacionog skupa* je pronalaženje informacionog skupa na kome u primljenoj poruci nema grešaka. Zbog toga je potrebno da se informacioni skup formira najpouzdanijih bita primljene poruke. U ovoj tački je detaljnije razrađen postupak slučajnog izbora informacionog skupa (Algoritam 4.1). Ocenjeno je matematičko očekivanje broja indeksa koji se uzimaju u obzir za formiranje informacionog skupa, kao i numerička složenost ovog algoritma.

Pod *nepouzdanošću* bita y_i primljene poruke u koraku 8^0 Algoritma 2.1 podrazumeva se veličina $p_i^{(j)}$, $1 \leq i \leq n$. Dakle, informacioni skupovi se formiraju od indeksa najmanjih koordinata vektora $\mathbf{p}^{(j)}$, slično kao i u [Meie89, Algoritam A] (izuzev što se u tom radu koristi samo vektor $\mathbf{p}^{(1)}$). Da bi se pak omogućilo formiranje više slučajnih informacionih skupova, izbori se vrše iz skupa $\mathbf{I}'$ indeksa k' najmanjih koordinata vektora $\mathbf{p}^{(j)}$, $k < k' < n$. Skup $\mathbf{I}'$ mora da sadrži bar jedan informacioni skup. Drugim rečima, ako je $\mathbf{G}$ proizvoljna generišuća matrica koda $R_{h,n}$, potrebno je da bude rang $\mathbf{G}_{\mathbf{I}'} = k$. S druge strane, broj k' ne sme da bude previše veliki da se informacioni skupovi ne bi formirali od nepouzdanih koordinata primljene poruke. Pogodna vrednost parametra k' bira se na osnovu ova dva uslova, u zavisnosti od parametara koda i verovatnoće greške p.

Procenićemo sada matematičko očekivanje broja razmatranih elemenata skupa $\mathbf{I}'$ prilikom formiranja slučajnog informacionog skupa. Pri tome se zbog jednostavnosti smatra da su elementi skupa $\mathbf{I}'$ jednako verovatni, kao i da su izabrani nezavisno i sa ravnomernom raspodelom verovatnoće iz skupa B_k. Neka je $\mathbf{L}$ slučajno izabrani informacioni skup, pri čemu su $L_1, L_2, \ldots, L_k$ njegovi elementi, onim redom kojim su izvlačeni iz skupa $\mathbf{I}'$. Neka je dalje $\mathbf{L}^{(0)} = \emptyset$ i $\mathbf{L}^{(j)} = \{L_1, L_2, \ldots, L_j\}$ za $1 \leq j \leq k$. Skup $\mathbf{L}^{(j)}$ formira se od skupa $\mathbf{L}^{(j-1)}$ dodavanjem slučajno izabranog indeksa $L_j \in \mathbf{I}' \backslash \mathbf{L}^{(j-1)}$. Ovaj izbor ponavlja se dotle dok se ne dobije indeks L_j takav da je vektor $\mathbf{G}_{L_j}$ linearno nezavisan od vektora–kolona matrice $\mathbf{G}_{\mathbf{L}^{(j-1)}}$. Zbog jednostavnosti modela smatra se da je ovo izvlačenje sa vraćanjem, iako je to za algoritam beskorisno,jer se time povećava matematičko očekivanje broja izvlačenih elemenata skupa $\mathbf{I}'$. Verovatnoća da je vektor $\mathbf{G}_{L_j}$ linearno nezavisan od vektora–kolona matrice $\mathbf{G}_{\mathbf{L}^{(j-1)}}$ je na osnovu pretpostavke o skupu $\mathbf{I}'$ približno jednaka verovatnoći izbora iz $B_k \setminus \emptyset$, slučajnog vektora linearno nezavisnog od zadatih $j-1$ (linearno nezavisnih) vektora

$$p_j^* = \frac{2^k - 2^{j-1}}{2^k - j}, \qquad 1 \leq j < k.$$

Drugim rečima, pretpostavlja se da su za $1 \leq j < k$ "gustine" vektora linearno nezavisnih od vektora–kolona matrice $\mathbf{G}_{\mathbf{L}^{(j-1)}}$ približno iste u skupovima $\mathbf{I}' \setminus \mathbf{L}^{(j-1)}$ i $B^k \setminus \left(\{\mathbf{0}\} \cup \mathbf{L}^{(j-1)}\right)$.

S obzirom na sistem linearnih veza između kolona matrice $\mathbf{G}$ može se reći da skup $\mathbf{I}' \setminus \mathbf{L}^{(j-1)}$ nije dovoljno reprezentativan uzorak elemenata skupa $B^k \setminus \left(\{\mathbf{0}\} \cup \mathbf{L}^{(j-1)}\right)$, odnosno da iskorišćena aproksimacija nije potpuno opravdana. Međutim, ovde joj se ipak pribegava zbog složenosti egzaktnog izračunavanja očekivanog broja izabranih elemenata skupa $\mathbf{I}'$ prilikom formiranja slučajnog informacionog skupa.

Verovatnoća da se posle $\nu - 1$ neuspešnih u ν–tom pokušaju, $\nu \geq 1$, izabere pogodan elemenat $L_j \in \mathbf{I}' \setminus \mathbf{L}^{(j-1)}$ je $\left(1 - p_j^*\right)^{\nu-1} p_j^*$, pa je matematičko očekivanje broja razmatranih kandidata za L_j

$$\sum_{\nu=1}^{\infty} \nu \left(1 - p_j^*\right)^{\nu-1} p_j^* = \frac{1}{p_j^*} = \frac{2^k - j}{2^k - 2^{j-1}}.$$

Matematičko očekivanje ukupnog broja razmatranih elemenata skupa $\mathbf{I}'$ može se proceniti sa

$$\begin{aligned} \sum_{j=1}^{k} \frac{2^k - j}{2^k - 2^{j-1}} &< \sum_{j=1}^{k} \frac{2^k}{2^k - 2^{j-1}} \\ &= k + \sum_{j=1}^{k} \frac{1}{2^j - 1} < k + 2, \end{aligned}$$

jer je

$$\begin{aligned} \sum_{j=1}^{k} \frac{1}{2^j - 1} &= \frac{1}{1} + \sum_{j=2}^{k} \frac{1}{2^j - 1} < 1 + \sum_{j=2}^{k} \frac{1}{2^{j-1}} \\ &< 1 + \sum_{j=1}^{\infty} \frac{1}{2^j} = 2 \end{aligned} \tag{4.1}$$

Na sličan način može se oceniti da je disperzija broja razmatranih elemenata skupa $\mathbf{I}'$ manja od $k + 7$. Eksperimentalni rezultati pokazuju da je aproksimacija pri izvođenju ove procene vrlo gruba. Najčešće je dovoljno uzeti $k' = 3k$, iako ponekad čak i za tako veliku vrednost k' nije zadovljen uslov $\operatorname{rang} \mathbf{G}_{\mathbf{I}'} = k$. Zaključuje se da je u skupu vektora $\left\{\mathbf{G}_{l_j} \mid L_j \in \mathbf{I}' \setminus \mathbf{L}^{(j-1)}\right\}$ gustina vektora linearno zavisnih od vektora–kolona u matrici $\mathbf{G}_{\mathbf{L}^{(j-1)}}, 1 \leq j < k$, najčešće znatno veća nego u skupu vektora $B^k \setminus \left(\{\mathbf{0}\} \cup \mathbf{L}^{(j-1)}\right)$.

Slučajni informacioni skup može se formirati korišćenjem sledećeg algoritma, sličnog Gausovom postupku rešavanja sistema linearnih jednačina.

Algoritam 4.1 Formiranje slučajnog informacionog skupa $\mathbf{l} \subset \mathbf{l}'$ linearnog (n, k) koda sa generišućom matricom $\mathbf{G}$, pri čemu je $\mathbf{l}'$ zadati podskup skupa $\{1, 2, \ldots, n\}$.
Ulaz: generišuća matrica koda $\mathbf{G}$ i skup $\mathbf{l}' \subset \{1, 2, \ldots, n\}$ takav da je matrica $\mathbf{G}_{\mathbf{l}'}$ nesingularna.
Izlaz: slučajni informacioni skup $\mathbf{l} \subset \mathbf{l}'$ i matrica $\mathbf{u} = \mathbf{G}_{\mathbf{l}'}{}^{-1}$.

1^0 [Inicijalizacija, izbor prvog slučajnog indeksa.] $j \leftarrow 1$; izabrati slučajni elemenat $l_1 \in \mathbf{l}'$; staviti $\mathbf{l}^{(1)} = \{l_1\}$; staviti $\mathbf{v}^{(1)} \leftarrow \mathbf{G}_{l_1}$; neka je γ_1 indeks prve koordinate vektora $\mathbf{v}^{(1)}$ različite od nule; staviti $\mathbf{u} \leftarrow I^{(k)}$, gde je $\mathbf{I}^{(k)}$ jedinična matrica reda k; inicijalizovati matricu $\mathbf{v} \leftarrow \mathbf{v}^{(1)}$.

2^0 [Priprema za slučajni izbor narednog člana informacionog skupa.] $j \leftarrow j + 1$; izabrati slučajni elemenat $l_j \in \mathbf{l}' \setminus \mathbf{l}^{(j-1)}$; staviti $\mathbf{v}^{(j)} \leftarrow \mathbf{G}_{l_j}$; za $i = 1, 2, \ldots, j-1$ ako je $\mathbf{v}^{(j)}_{\gamma_i} \neq 0$, onda staviti $\mathbf{v}^{(j)} \leftarrow \mathbf{v}^{(j)} \oplus \mathbf{v}^{(i)}$.

3^0 [Rang podmatrice od izabranih kolona nije povećan?] Ako je $\mathbf{v}^{(j)} = \mathbf{0}$, skok na 2^0; u protivnom, neka je γ_j indeks prve koordinate vektora $\mathbf{v}^{(j)}$ različite od nule, staviti $\mathbf{l}^{(j)} = \mathbf{l}^{(j-1)} \cup \{l_j\}$, matrici $\mathbf{v}$ dodati vektor $\mathbf{v}^{(j)}$ kao poslednju kolonu, a sa kolonama matrice $\mathbf{u}$ izvršiti iste operacije koje su u koraku 2^0 izvršene sa kolonama matrice $\mathbf{v}$.

4^0 [Kraj?] Ako je $j < k$, skok na 2^0; u protivnom $\mathbf{l} \leftarrow \mathbf{l}^{(k)}$.

5^0 [Formiranje matrice $\mathbf{G}_{\mathbf{l}}^{-1}$.] Za $i = k, k-1, \ldots, 2$ Izvršiti sledeće operacije sa kolonama matrica $\mathbf{v}$ i $\mathbf{u}$: za $j = 1, 2, \ldots, i-1$ ako je $(\mathbf{v}_j)_{\gamma_i} = 1$, onda $\mathbf{u}_j \leftarrow \mathbf{u}_j \oplus \mathbf{u}_i$. Zatim ispermutovati kolone matrica $\mathbf{u}$ i $\mathbf{v}$ istim skupom permutacija tako da se od matrice $\mathbf{v}$ dobije jedinična matrica. Tada je $\mathbf{u} = \mathbf{G}_{\mathbf{l}}^{-1}$. □

Pomoćni vektor $\mathbf{v}^{(j)}$ se za $1 \leq j \leq k$ formira u koraku 2^0 kao linearna kombinacija vektora $\mathbf{G}_{l_1}, \mathbf{G}_{l_2}, \ldots, \mathbf{G}_{l_j}$ tako

- da bude linearno nezavisan od vektora $\mathbf{G}_{l_1}, \mathbf{G}_{l_2}, \ldots, \mathbf{G}_{l_{j-1}}$, ili, što je ekvivalentno, od vektora $\mathbf{v}^{(1)}, \mathbf{v}^{(2)}, \ldots, \mathbf{v}^{(j-1)}$;

- da je linearni potprostor sa bazom $\mathbf{v}^{(1)}, \mathbf{v}^{(2)}, \ldots, \mathbf{v}^{(j)}$ jednak linearnom potprostoru sa bazom $\mathbf{G}_{l_1}, \mathbf{G}_{l_2}, \ldots, \mathbf{G}_{l_j}$;

- da mu koordinate sa indeksima $\gamma_1, \gamma_2, \ldots, \gamma_{j-1}$ budu jednake nuli; za vrednost γ_j uzima se indeks prve koordinate ovog vektora različite od nule.

Koordinata vektora $\mathbf{v}^{(j)}$ sa indeksom γ_j koristi se za dobijanje nula na koordinatama sa tim indeksom u vektorima $\mathbf{v}^{(j+1)}, \mathbf{v}^{(j+2)}, \ldots, \mathbf{v}^{(k)}$, $1 \leq j < k$. Da bi se formirao vektor $\mathbf{v}^{(j)}$ potrebno je izvršiti najviše $k(j-1)$ sabiranja po modulu dva, $1 \leq j \leq k$, pa je zbog (4.1) matematičko očekivanje numeričke složenosti operacija sa vektorima $\mathbf{v}^{(j)}$, $1 \leq j \leq k$, u koraku 2^0 algoritma ograničeno odozgo veličinom

$$\begin{aligned}
\sum_{j=1}^{k}(j-1)k\frac{2^k-j}{2^k-2^{j-1}} &< k\sum_{j=1}^{k-1}\frac{j\left(2^k-2^j+2^j\right)}{2^k-2^j} \\
&= k\left(\sum_{j=1}^{k-1}j\right)+k\sum_{j=1}^{k-1}\frac{j}{2^{k-j}-1} \\
&= \frac{1}{2}k^2(k-1)+k\sum_{j=1}^{k-1}\frac{k-j}{2^j-1} \\
&< \frac{1}{2}k^2(k-1)+k\sum_{j=1}^{k-1}\frac{k-1}{2^j-1} \\
&< \frac{1}{2}k^2(k-1)+2k(k-1)\simeq\frac{1}{2}k^3
\end{aligned}$$

Numerička složenost operacija sa matricom u u koraku 2^0 je najviše

$$\sum_{j=1}^{k}(j-1)k = k^2(k-1)/2.$$

U koraku 5^0 je potrebno izvršiti još

$$2\sum_{j=1}^{k}(j-1) = k(k-1)$$

operacija u prvom delu i oko $2k^2$ operacija za preuređenje kolona. Dakle, numerička složenost Algoritma 4.1 je oko k^3.

4.2 Kriterijum za diskriminaciju kodnih reči

Prilikom dekodiranja po principu minimuma rastojanja u opštem slučaju se za fiksiranu kodnu reč ne može tvrditi da je najbliža primljenoj poruci pre nego što se provere rastojanja primljene poruke od svih kodnih reči. Međutim, u slučaju kodova $R_{h,n}$ za n dovoljno veliko kodna reč $\mathbf{x}$ je (sa određenom pouzdanošću) najbliža primljenoj poruci $\mathbf{y} \in B_n$ ako i samo ako je rastojanje $\mathrm{dist}\,(\mathbf{x},\mathbf{y})$ manje od određene granice (videti na primer u radu [Sieg85]). Ova činjenica je značajna u slučaju kad se unapred zna da neki podskup koda sadrži traženu kodnu reč. U ovoj tački će na osnovu [Sieg85] biti izložen odgovarajući statistički model, kao i način određivanja praga odlučivanja (diskriminacije) o kodnoj reči $\mathbf{x}$ na osnovu rastojanja $\mathrm{dist}\,(\mathbf{x},\mathbf{y})$.

Neka je $\mathbf{x}$ kodna reč, $\mathbf{E}$ – vektor greške sa raspodelom verovatnoća 1.1, i $\mathbf{Y} = \mathbf{x} \oplus \mathbf{E}$ – primljena poruka. Statistički model koji omogućuje diskriminaciju kodnih reči koda $R_{h,n}$ prema rastojanju od primljene poruke $\mathbf{y}$ (realizacije slučajne promenljive $\mathbf{Y}$) je sledeći: rastojanje kodne reči $\mathbf{x}' \in R_{h,n}$ od primljene poruke $\mathbf{Y}$ ima binomnu (odnosno približno normalnu) raspodelu verovatnoća, sa srednjom vrednošću koja zavisi od toga da li je $\mathbf{x}' = \mathbf{x}$ ili $\mathbf{x}' \neq \mathbf{x}$. Neka je sa

$$U = \mathrm{dist}\,(\mathbf{x}', \mathbf{Y}) = \mathrm{dist}\,(\mathbf{x}', \mathbf{x} \oplus \mathbf{E}) = \mathrm{dist}\,(\mathbf{x}' \oplus \mathbf{x}, \mathbf{E})$$

označena slučajna promenljiva jednaka rastojanju fiksirane kodne reči $\mathbf{x}'$ od primljene poruke. U slučaju kad je $\mathbf{x}' = \mathbf{x}$, slučajna promenljiva U ima binomnu $\mathcal{B}(n,p)$ raspodelu verovatnoća sa matematičkim očekivanjem np i disperzijom npq, gde je $q = 1 - p$. U slučaju kad je $\mathbf{x}' \neq \mathbf{x}$, slučajna promenljiva U jednaka je zbiru slučajnih promenljivih U_0 i U_1 zadatih jednakošću

$$U_\eta = \mid \{i \mid 1 \leq i \leq n,\ x_i \oplus x'_i = 1 \oplus \eta,\ E_i = \eta\} \mid, \qquad \eta \in B.$$

Ovde je $|\cdot|$ oznaka za kardinalni broj skupa. Slučajne promenljive U_0 i U_1 su nezavisne i imaju redom binomnu raspodelu $\mathcal{B}(w_x, q)$, odnosno

$\mathcal{B}(n-w_x, p)$, gde je $w_x = w(\mathbf{x}' \oplus \mathbf{x})$. Zbog toga je raspodela verovatnoća slučajne promenljive U jednaka konvoluciji ovih dveju raspodela (videti na primer [El-A84])

$$P\{U = u\} = \sum_{u_0+u_1=u} P\{U_0 = u_0\} P\{U_1 = u_1\}, \tag{4.2}$$

i u opštem slučaju nije binomna. Njeno matematičko očekivanje je $np + w_x(q-p)$, a disperzija npq. Poznato je da je u kodnim rečima koda $R_{h,n}$ broj nula približno jednak broju jedinica, videti na primer [Golo67]. Zbog toga je $w_x \simeq n/2$, pa je matematičko očekivanje slučajne promenljive U približno jednako matematičkom očekivanju slučajne promenljive sa binomnom raspodelom $\mathcal{B}(n, p)$.

Razmotrimo sada složeniji model u kome je kodna reč $\mathbf{x}'$ realizacija slučajne promenljive $\mathbf{X}'$ sa ravnomernom raspodelom verovatnoća na skupu $R_{h,n}$. Ovaj model više odgovara realnoj situaciji, zbog toga što se kodna reč $\mathbf{x}$ ne zna. Veličina $w_x = w(\mathbf{x}' \oplus \mathbf{x})$ je tada realizacija slučajne promenljive $W_x = w(\mathbf{X}' \oplus \mathbf{x})$. Nezavisne slučajne promenljive U_0 i U_1 definisane jednakošću

$$U_\eta = \mid \{i \mid 1 \le i \le n,\ x_i \oplus X'_i = 1 \oplus \eta,\ E_i = \eta\} \mid, \qquad \eta \in B,$$

zavise i od $\mathbf{X}'$ i $\mathbf{E}$, a njihov zbir je slučajna promenljiva

$$U = \operatorname{dist}(\mathbf{X}', \mathbf{Y}) = w(\mathbf{X}' \oplus \mathbf{x} \oplus \mathbf{E}).$$

Slučajna promenljiva U_0, odnosno U_1, ima pri uslovu $W_x = w_x$, $0 \le w_x \le n$, binomnu uslovnu raspodelu verovatnoća $\mathcal{B}(w_x, q)$, odnosno $\mathcal{B}(w_x, p)$. Uslovna raspodela verovatnoća slučajne promenljive U pod istim uslovom $W_x = w_x$ je konvolucija ovih dveju uslovnih raspodela (videti (4.2)). Pretpostavimo da slučajna promenljiva W_x ima binomnu raspodelu $\mathcal{B}(n, 1/2)$ (u radu [KasaS5] utvrđeno je da se raspodela težina većine linearnih kodova dobro može aproksimirati binomnom raspodelom). Iz ove pretpostavke sledi da i slučajna promenljiva U ima istu binomnu raspodelu, jer je tada za $0 \le u \le n$

$$\begin{aligned} & P\{U = u\} = \\ = & \sum_{w_x=0}^{n} P\{W_x = w_x\} P(\{U(\mathbf{X}', \mathbf{Y}) = u\} \mid \{W_x = w_x\}) \end{aligned}$$

$$= \sum_{w_x=0}^{n} \binom{n}{w_x} 2^{-n} \sum_{w'=0}^{\min(w_x,u)} \binom{w_x}{w'} \binom{n-w_x}{u-w'} p^{u+w_x-2w'} q^{n-w_x-u+2w'}$$

$$= \left(\frac{q}{2}\right)^n \sum_{w'=0}^{u} \sum_{w_x=w'}^{n} \binom{n}{w_x} \binom{w_x}{w'} \binom{n-w_x}{u-w'} \left(\frac{p}{q}\right)^{w_x+u-2w'}$$

$$= \left(\frac{q}{2}\right)^n \sum_{w'=0}^{u} \sum_{w_x=w'}^{n} \binom{n}{u} \binom{u}{w'} \binom{n-u}{w_x-w'} \left(\frac{p}{q}\right)^{w_x+u-2w'}$$

$$= \left(\frac{q}{2}\right)^n \binom{n}{u} \left(\frac{p}{q}\right)^u \left(\sum_{w'=0}^{u} \binom{u}{w'} \left(\frac{p}{q}\right)^{-w'} \right) \left(\sum_{\nu=0}^{n-w'} \binom{n-u}{\nu} \left(\frac{p}{q}\right)^{\nu} \right)$$

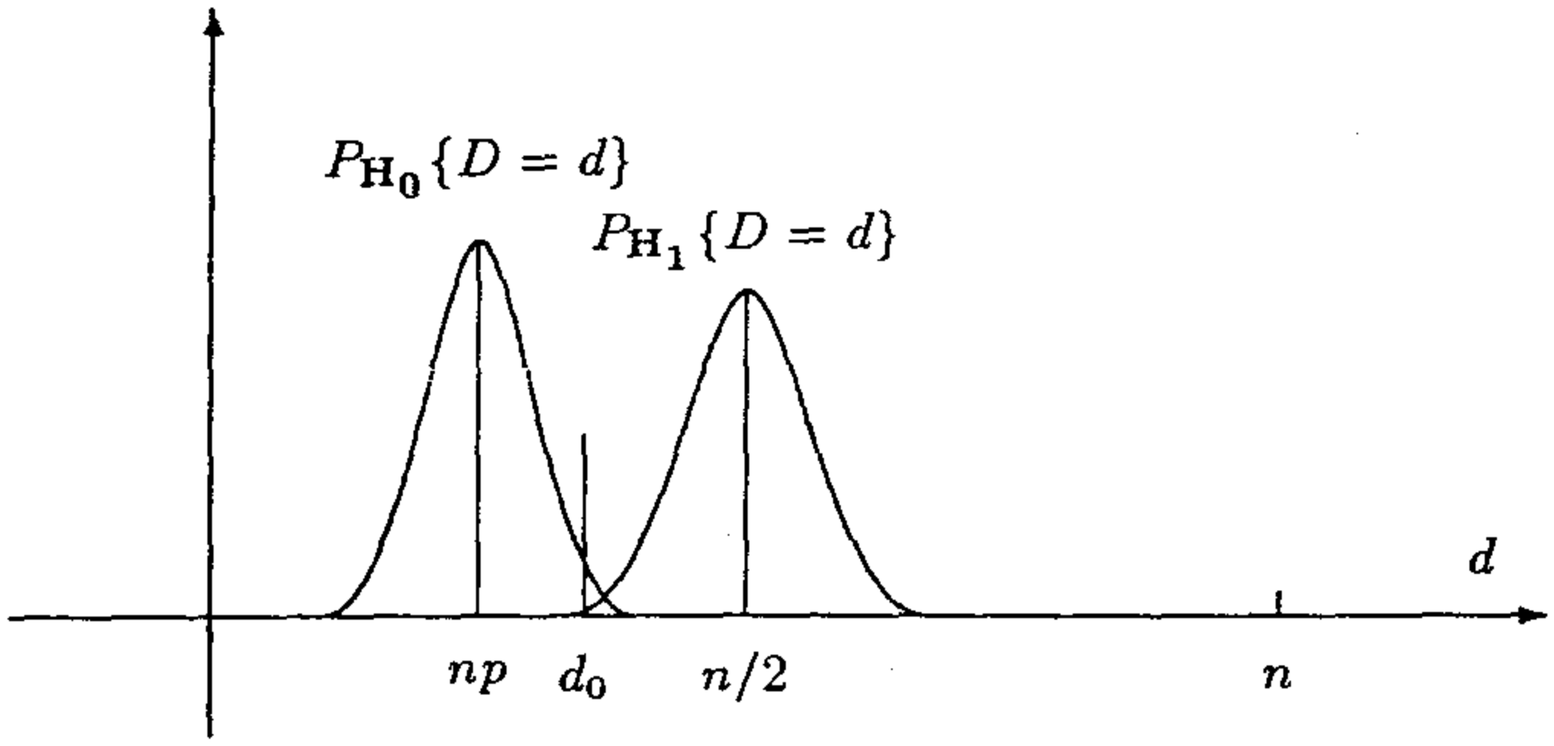
$$= \left(\frac{q}{2}\right)^n \binom{n}{u} \left(\frac{p}{q}\right)^u \left(1+\frac{q}{p}\right)^u \left(1+\frac{p}{q}\right)^{n-u}$$

$$= \binom{n}{u} 2^{-n}$$

Odlučivanje o tome da li je slučajno izabrana kodna reč $\mathbf{x}'$ linearnog koda $R_{h,n}$ jednaka kodnoj reči $\mathbf{x}$ čijim je propuštanjem kroz BSK (odnosno sabiranjem po modulu dva sa vektorom $\mathbf{E}$ slučajnih grešaka) dobijen vektor $\mathbf{y}$, može se formulisati kao testiranje hipoteze $\mathbf{H_0} : \mathbf{x}' = \mathbf{x}$ protiv alternativne hipoteze $\mathbf{H_1} : \mathbf{x}' \in R_{h,n},\ \mathbf{x}' \neq \mathbf{x}$. Statistika na osnovu koje se vrši odlučivanje je Hemingovo rastojanje $d = \mathrm{dist}\,(\mathbf{x}', \mathbf{y})$ Uslovna raspodela verovatnoća slučajne promenljive $U = \mathrm{dist}\,(\mathbf{X}', \mathbf{Y})$ (čija je realizacija statistika u) kad je tačna hipoteza $\mathbf{H_0}$, odnosno hipoteza $\mathbf{H_1}$, je binomna $\mathcal{B}(n,p)$, odnosno $\mathcal{B}\,(n,1/2)$ raspodela, videti Sliku 4.1. Za dovoljno veliko n (na primer $n > 20$) ove raspodele mogu se aproksimirati normalnim raspodelama $\mathcal{N}\left(np, \sqrt{npq}\right)$, odnosno $\mathcal{N}\,(n/2, \sqrt{n}/2)$. Kritična oblast testa je oblika $\{u \mid u \leq d_0\}$, pa se smatra da je hipoteza $\mathbf{H_0}$ tačna ako je rastojanje d manje od praga d_0.

Prilikom odlučivanja da li je tačna hipoteza $\mathbf{H_0}$ ili hipoteza $\mathbf{H_1}$ moguće je napraviti dve vrste grešaka: proglasiti za rešenje kodnu reč koja to nije (proglasiti tačnom hipotezu $\mathbf{H_0}$ iako je tačna hipoteza $\mathbf{H_1}$), ili prevideti tačno rešenje (proglasiti tačnom hipotezu $\mathbf{H_1}$ iako je tačna hipoteza $\mathbf{H_0}$). Verovatnoće ovih grešaka, koje će biti označene redom sa $P_{0|1}$, $P_{1|0}$, date su za dovoljno veliko n približnim izrazima

$$P_{0|1} = P_{\mathbf{H_1}}\{U \leq d_0\}$$



Slika 4.1: Uslovne raspodele verovatnoća rastojanja slučajno izabrane kodne reči od primljene poruke

$$= \sqrt{\frac{2}{n\pi}} \int_{-\infty}^{d_0} e^{-\frac{2}{n}(z-n/2)^2}\, dz$$
$$= Q\left(\frac{n/2 - d_0}{\sqrt{n}/2}\right),$$

odnosno

$$P_{1|0} = P_{\mathbf{H_0}}\{U > d_0\}$$
$$= \frac{1}{\sqrt{2\pi npq}} \int_{d_0}^{+\infty} e^{-\frac{(z-np)^2}{2npq}}\, dz$$
$$= Q\left(\frac{d_0 - np}{\sqrt{npq}}\right).$$

Ovde je sa $Q(z)$ označena funkcija

$$Q(z) = \frac{1}{\sqrt{2\pi}} \int_z^{+\infty} e^{-\frac{t^2}{2}}\, dt.$$

Da bi se odlučivanjem na ovaj način uspešno izvršilo dekodiranje, treba obezbediti da verovatnoća $P_{1|0}$ bude dovoljno mala, na primer

$P_{1|0} < 0.001$. Neka je $\alpha_0 = Q^{-1}(0.001) \simeq 3$. Uslov $P_{1|0} < 0.001$ ekvivalentan je sa

$$d_0 \geq np + \alpha_0\sqrt{npq}.$$

Zbog toga se za *prag odlučivanja* (diskriminacije) može usvojiti veličina

$$d_0 = np + \alpha_0\sqrt{npq}. \tag{4.3}$$

Verovatnoća $P_{0|1}$ treba da bude manja od 2^{-k} da bi se u proseku jednom na 2^k testiranja proglašavala tačnom hipoteza $\mathbf{H_0}$ kad je tačna hipoteza $\mathbf{H_1}$. Ako se uvede oznaka $\beta_0 = Q^{-1}\left(2^{-k}\right)$, ovaj uslov ekvivalentan je uslovu

$$d_0 \leq n/2 - \frac{\beta_0}{2}\sqrt{n}. \tag{4.4}$$

Prag d_0 koji zadovoljava oba navedena uslova može se izabrati ako i samo ako je

$$n/2 - \frac{\beta_0}{2}\sqrt{n} \geq np + \alpha_0\sqrt{npq},$$

odnosno

$$n \geq \frac{\left(\alpha_0\sqrt{pq} + \frac{\beta_0}{2}\right)^2}{(1/2 - p)^2}. \tag{4.5}$$

U ovom izrazu brojilac je relativno mala konstanta, pa na dužinu kodne reči n najviše utiče parametar p, verovatnoća greške u BSK.

4.3 Pretraga okoline informacionog skupa

U ovom odeljku će detaljnije biti opisano generisanje i provera kodnih reči iz neke okoline izabranog informacionog skupa. Pored toga biće pokazano (slično kao u radu [LeeB88]) kako se može odrediti optimalna dubina pretrage okoline informacionog skupa. Algoritam za dekodiranje druge klase linearnih kodova iz [LeeB88] (nešto opštiji od Algoritma A) bez većih promena može se primeniti i na kodove $R_{h,n}$. Taj algoritam je ugrađen u Algoritam 2.1 kao faza pretrage u okviru svakog ciklusa.

Neka je (videti poglavlje 5) $\mathbf{I}$ izabrani informacioni skup. Pre izlaganja samog algoritma, uvešćemo pojam *okoline informacionog skupa* u odnosu na primljenu poruku.

Definicija 4.1 *Za fiksirani vektor* $\mathbf{y}$, $\mathbf{y} \in B_n$, *pod* okolinom dubine w *informacionog skupa* $\mathbf{I}$ *linearnog koda* $R_{h,n}$ *u odnosu na primljenu poruku* $\mathbf{y}$ *podrazumeva se skup kodnih reči* $\mathbf{O}_{\mathbf{y},\mathbf{I},w}$ *koje se na skupu pozicija* $\mathbf{I}$ *od vektora* $\mathbf{y}$ *razlikuju na najviše* w *mesta, odnosno*

$$\mathbf{O}_{\mathbf{y},\mathbf{I},w} = \{\mathbf{x}' \in R_{h,n} \mid \mathrm{dist}\,(\mathbf{x}'_\mathbf{I}, \mathbf{y}_\mathbf{I}) \leq w\}\,.$$

Neka je $\mathbf{u} \in B_n$ proizvoljni vektor. Kodna reč koja se na informacionom skupu $\mathbf{I}$ poklapa sa vektorom $\mathbf{u}$ može se napisati u obliku

$$\left(\mathbf{u}_\mathbf{I}^T \mathbf{G}_\mathbf{I}^{-1} \mathbf{G}\right)^T$$

jer je

$$\left(\mathbf{u}_\mathbf{I}^T \mathbf{G}_\mathbf{I}^{-1} \mathbf{G}\right)_\mathbf{I} = \left(\mathbf{u}_\mathbf{I}^T \mathbf{G}_\mathbf{I}^{-1}\right) \mathbf{G}_\mathbf{I} = \mathbf{u}_\mathbf{I}^T.$$

Označimo sa $\mathbf{e}^{(j)}$ vektor kojme je koordinata sa indeksom l_j i samo ona jednaka jedinici, $1 \leq j \leq k$. Neka je $\mathbf{x}^{(0)}$ kodna reč koja se na informacionom skupu $\mathbf{I}$ poklapa sa vektorom $\mathbf{y}$, i neka je za $1 \leq j \leq k$ sa $\mathbf{x}^{(j)}$ označena kodna reč koja se na informacionom skupu $\mathbf{I}$ poklapa sa vektorom $\mathbf{e}^{(j)}$. Tada je

$$\mathbf{x}^{(0)} = \left(\mathbf{y}_\mathbf{I}^T \mathbf{G}_\mathbf{I}^{-1} \mathbf{G}\right)^T \tag{4.6}$$

i

$$\mathbf{x}^{(j)} = \left(\left(\mathbf{e}_\mathbf{I}^{(j)}\right)^T \mathbf{G}_\mathbf{I}^{-1} \mathbf{G}\right)^T = \left(\left(\mathbf{G}_\mathbf{I}^{-1} \mathbf{G}\right)^T\right)_j, \qquad 1 \leq j \leq k. \tag{4.7}$$

Vektor $\mathbf{x}^{(0)}$ je *koren stabla pretrage*, jer u narednom algoritmu pretraga okoline $O_{\mathbf{y},\mathbf{I},w}$ započinje upravo sa njim (preciznije, koren stabla pretrage je vektor $\mathbf{x}^{(0)} \oplus \mathbf{y}$). Sistem vektora $\mathbf{x}^{(j)}, 1 \leq j \leq k$ je očigledno baza linearnog koda $R_{h,n}$.

Neka je w celi broj, $0 \leq w \leq k$. Svakom vektoru $\mathbf{e}$ takvom da je $w(\mathbf{e}) = w(\mathbf{e}_\mathbf{I})$ (što znači da su mu koordinate van informacionog skupa jednake nuli) i $w(\mathbf{e}) \leq w$ jednoznačno se može pridružiti kodna reč

$$\mathbf{x}' = \mathbf{x}^{(0)} \oplus \bigoplus_{i=1}^{k} e_{l_j} \mathbf{x}^{(j)}$$

iz okoline $O_{\mathbf{y},\mathbf{l},w}$. Naredni algoritam zbog ove činjenice omogućuje formiranje svih kodnih reči iz okoline $O_{\mathbf{y},\mathbf{l},w}$ zajedno sa svim vektorima $\mathbf{e} \in B_n$ takvim da je $w(\mathbf{e}) = w(\mathbf{e}_\mathbf{l}) \leq w$. Prilikom izlaganja koriste se slični termini kao za Algoritam 3.2, iako ovaj algoritam nije heuristički (radi se o potpunoj pretrazi okoline $O_{\mathbf{y},\mathbf{l},w}$).

Algoritam 4.2 Pretraga okoline $O_{\mathbf{y},\mathbf{l},w}$ informacionog skupa $\mathbf{l}$ koda $R_{h,n}$ u odnosu na primljenu poruku $\mathbf{y}$, sa ciljem da se (ako postoji) odredi kodna reč $\mathbf{x}'$ iz te okoline takva da je $\mathrm{dist}\,(\mathbf{x}', \mathbf{y}) < d_0$ (4.3).
Ulaz: prirodni brojevi $n, k,\ n \geq k$, polinom $h(x) \in \mathrm{GF}(2)[z]$ stepena k, primljena poruka $\mathbf{y} \in B_n$, informacioni skup $\mathbf{l}$ koda $R_{h,n}$, prirodni broj $w,\ 1 \leq w \leq k$, i prag diskriminacije d_0 (4.3).
Izlaz: kodna reč $\mathbf{x}' \in O_{\mathbf{y},\mathbf{l},w}$ takva da je $\mathrm{dist}\,(\mathbf{x}', \mathbf{y}) < d_0$ (4.3) (ako postoji).

1^0 [Izračunavanje vektora $\mathbf{x}^{(0)}$ i baze $\mathbf{x}^{(1)}, \mathbf{x}^{(2)}, \ldots, \mathbf{x}^{(k)}$ koda $R_{h,n}$.] Izračunati na osnovu (4.6) i (4.7) vektore $\mathbf{x}^{(0)}$ i $\mathbf{x}^{(j)},\ 1 \leq j \leq k$.

2^0 [Inicijalizacija stabla pretrage: korena $\mathbf{v}^{(0)}$, rednog broja generacije g i vektora $\mathbf{e}$ grešaka na informacionom skupu $\mathbf{l}$.] $\mathbf{v}^{(0)} \leftarrow \mathbf{x}^{(0)} \oplus \mathbf{y}$, $g \leftarrow 0$, i $\mathbf{e} \leftarrow \mathbf{0}$.

3^0 [Korak u dubinu stabla.] Ako je $g < k$, onda $\mathbf{v}^{(g+1)} \leftarrow \mathbf{v}^{(g)}$, $g \leftarrow g + 1$, i $e_{l_g} \leftarrow 0$; ako je pak $g = k$, onda skok na 5^0.

4^0 [Naredni korak u dubinu.] Skok na 3^0.

5^0 [Povratak nazad na prvu nulu vektora $\mathbf{e}$ na informacionom skupu.] Ako je $e_{l_g} = 0$, skok na 7^0.

6^0 [Smanjenje tekuće dubine g.] Staviti $g \leftarrow g - 1$; ako je $g > 0$, skok na 5^0, a u protivnom – kraj, bez rešenja.

7^0 [Promena nađenog bita greške u jedinicu.] $e_{l_g} \leftarrow 1$, $\mathbf{v}^{(g)} \leftarrow \mathbf{v}^{(g-1)} \oplus \mathbf{x}^{(g)}$.

8^0 [Test da li je pronađeno rešenje.] Ako je $w(\mathbf{v}^{(g)}) \leq d_0$, onda $\mathbf{x}' \leftarrow \mathbf{v}^{(g)} \oplus \mathbf{y}$, kraj.

9^0 [Dostignuta je granica w dubine pretrage, odnosno broja ispravki na informacionom skupu?] Ako je $w(\mathbf{e}) \geq w$, skok na 5^0.

10^0 [Obrađivana je poslednja koordinata informacionog skupa?] Ako je $g \geq k$, skok na 5^0; u protivnom, skok na 3^0. □

Vektori $\mathbf{v}^{(g)}$ formirani u koraku 7^0 algoritma jednaki su zbiru po modulu dva kodnih reči iz okoline $O_{\mathbf{y},\mathbf{I},w}$ i primljene poruke $\mathbf{y}$. Svaki od njih dobija se pomoću n sabiranja po modulu dva. Opisani algoritam sličan je algoritmu iz [LeeB88], s tim što je preciziran način formiranja vektora iz okoline $O_{\mathbf{y},\mathbf{I},w}$. Taj deo algoritma odgovara poznatom algoritmu pretrage stabla u dubinu, videti na primer [Nije71].

Algoritam 4.2 sastoji se od dve jasno odvojene faze, pripreme za pretragu (korak 1^0) i samog izvođenja pretrage (koraci $2^0 - 10^0$). Formiranje informacionog skupa I i izračunavanje matrice $\mathbf{G}_\mathbf{I}^{-1}$ pomoću Algoritma 4.1 zahteva izvršavanje oko k^3 operacija. Proizvod $\mathbf{G}_\mathbf{I}^{-1}\mathbf{G}$ može se izračunati pomoću $2k^2n$ operacija običnim množenjem matrica. Efikasniji način izračunavanja ove matrice je da se najpre izračuna njenih privih k kolona (oko $2k^3$ operacija), pa da se zatim primenom rekurentne relacije (1.3) izračunaju elementi ostalih vrsta (jer elementi svake vrste zadovoljavaju navedenu rekurentnu relaciju). Na ovaj način je potrebno izvršiti samo $k^3 + mk(n-k)$ operacija, gde je m broj članova polinoma $h(z)$ različitih od konstante. Dakle, zbir numeričkih složenosti Algoritma 4.1 i prve faze Algoritma 4.2 je oko $mkn + 2k^3$. U tipičnim situacijama je veličina m mala u odnosu na k, pa se numerička složenost pripreme za pretragu može, kao i u [LeeB88] oceniti sa αk^3. S druge strane, za proveru udaljenosti jedne kodne reči iz okoline $O_{\mathbf{y},\mathbf{I},w}$ od vektora $\mathbf{y}$ potrebno je, kao i u [LeeB88] izvršiti samo βn operacija (n celobrojnih sabiranja i n sabiranja po modulu dva). Ovde su α i β odgovarajuće konstante. Dakle, zbir numeričkih složenosti Algoritama 4.1 i 4.2 je

$$\alpha k^3 + \beta n \sum_{\nu=0}^{w} \binom{k}{\nu}$$

Zbog ovakvog odnosa složenosti pripreme za pretragu i njenog izvođenja, efikasnost algoritma može se optimizirati pogodnim izborom parametra w, dubine pretrage [LeeB88]. Vektor $\mathbf{y}_\mathbf{I}$ je realizacija slučajne

promenljive $\mathbf{x_l} \oplus \mathbf{E_l}$, dobijene propuštanjem vektora $\mathbf{x_l}$ kroz BSK sa verovatnoćom greške p. Pri tome parametar p ima drugačiju vrednost od one sa kojom se ulazi u Algoritam 2.1, jer se pretpostavlja da je rezultat probabilističke faze tog algoritma efektivno smanjenje verovatnoće greške, posebno za koordinate primljene poruke sa indeksima iz informacionog skupa. S druge strane, koordinate vektora $\mathbf{E_l}$ zbog toga nisu nezavisne. Ipak će zbog jednostavnosti biti pretpostavljeno da su koordinate ovog vektora nezavisne. Verovatnoća da se kodna reč $\mathbf{x}$ nađe u okolini $O_{\mathbf{Y},\mathbf{l},w}$slučajnog vektora $\mathbf{Y}$ jednaka je

$$P\left\{\mathrm{dist}\left(\mathbf{Y_l}, \mathbf{x_l}\right) \leq w\right\} = P\left\{w(\mathbf{E_l}) \leq w\right\} = \sum_{\nu=0}^{w} \binom{k}{\nu} p^{\nu}(1-p)^{k-\nu}$$

U radu [LeeB88] je za ovu verovatnoću korišćen drugi izraz,

$$\binom{n}{k}^{-1} \sum_{\nu=0}^{w} \binom{[np]}{\nu} \binom{n-[np]}{k-\nu},$$

ali se lako pokazuje da su za veliko n vrednosti ova dva izraza približno jednake. Pretpostavimo da je fiksiran broj n_t operacija koje se mogu izvršiti u toku dekodiranja korišćenjem Algoritama 4.1 i 4.2. Tada je broj slučajno izabranih informacionih skupova koji se mogu obraditi manji od

$$\frac{n_t}{\alpha k^3 + \beta n \sum_{\nu=0}^{w} \binom{k}{\nu}},$$

a verovatnoća da se kodna reč $\mathbf{x}$ nađe u bar jednoj od na ovaj način dobijenih okolina nije veća od

$$\frac{n_t}{\beta n} \mathcal{R}_{k,p,\gamma}(w),$$

gde je

$$\mathcal{R}_{k,p,\gamma}(w) = \frac{\sum_{\nu=0}^{w} \binom{k}{\nu} p^{\nu} q^{k-\nu}}{\gamma k^2 + \sum_{\nu=0}^{w} \binom{k}{\nu}}, \tag{4.8}$$

i

$$\gamma = \frac{\alpha}{\beta} \frac{k}{n}.$$

Na primer, za $\alpha = 4$, $\beta = 2$ je $\gamma = 2k/n$. Maksimizacija uspešnog dekodiranja primenom Algoritama 4.1 i 4.2 svodi se dakle na maksimizaciju izraza $\mathcal{R}_{k,p,\gamma}$. U Tabeli 4.1 date su vrednosti funkcije $\mathcal{R}_{k,p,\gamma}(w)$ za $k = 50$, $1 \leq w \leq 4$ i $p = 0(0.01)0.5$, $\gamma = 0.02$. Zapaža se da je optimalna vrednost w u ovom slučaju jednaka $w = 0$ za $p = 0.01$, $w = 1$ za $0.02 \leq p \leq 0.33$, odnosno $w = 2$ za $0.34 \leq p \leq 0.49$,

Da bi se pronašla optimalna vrednost w, potrebno je ustanoviti pod kojim uslovima važe nejednakosti

$$\mathcal{R}_{k,p,\gamma}(w) \leq \mathcal{R}_{k,p,\gamma}(w+1), \qquad w \geq 0, \tag{4.9}$$

odnosno

$$\frac{\sum_{\nu=0}^{w} \binom{k}{\nu} p^\nu q^{k-\nu}}{\gamma k^2 + \sum_{\nu=0}^{w} \binom{k}{\nu}} \leq \frac{\binom{k}{w+1} p^{w+1} q^{k-w-1} + \sum_{\nu=0}^{w} \binom{k}{\nu} p^\nu q^{k-\nu}}{\binom{k}{w+1} + \gamma k^2 + \sum_{\nu=0}^{w} \binom{k}{\nu}},$$

ili

$$\sum_{\nu=0}^{w} \binom{k}{\nu} p^\nu q^{k-\nu} \leq \left(\gamma k^2 + \sum_{\nu=0}^{w} \binom{k}{\nu}\right) p^{w+1} q^{k-w-1}.$$

Smenom $z = q/p$, $z > 1$, dobija se nejednakost

$$\gamma k^2 - \sum_{\nu=0}^{w} \binom{k}{\nu} \left(z^{w+1-\nu} - 1\right) \geq 0. \tag{4.10}$$

Izraz sa leve strane ove nejednakosti opada sa w. Pošto je $z > 1$ (zbog $p < 1/2$) skup vrednosti w za koje nejednakost važi je interval $(1, w_0]$, gde je $w_0 = w_0(k, p, \gamma)$ takav broj da je

$$\gamma k^2 - \sum_{\nu=0}^{w_0} \binom{k}{\nu} \left(z^{w_0+1-\nu} - 1\right) \geq 0 > \gamma k^2 - \sum_{\nu=0}^{w_0+1} \binom{k}{\nu} \left(z^{w_0+2-\nu} - 1\right).$$

Broj w_0 je upravo tražena optimalna vrednost dubine pretrage, jer za $w \neq w_0$ važi nejednakost $\mathcal{R}_{k,p,\gamma}(w) \leq \mathcal{R}_{k,p,\gamma}(w_0)$. Za fiksirane vrednosti k i γ optimalna dubina pretrage w_0 zavisi od verovatnoće greške p. Na osnovu činjenice da leva strana nejednakosti (4.10) opada sa $z = (1-p)/p = 1/p - 1$, odnosno raste sa p, zaključuje se da ako je ta nejednakost zadovoljena za neko p, onda je ona zadovoljena i za svaku vrednost $p' > p$. Dakle, za $p' > p$ je

$$w_0(k, p', \gamma) \geq w_0(k, p, \gamma).$$

w / p	0	1	2	3	4
0.01	0.119E-01	0.902E-02	0.744E-03	0.477E-04	0.398E-05
0.02	0.714E-02	0.728E-02	0.695E-03	0.469E-04	0.397E-05
0.03	0.428E-02	0.550E-02	0.611E-03	0.448E-04	0.391E-05
0.04	0.255E-02	0.397E-02	0.510E-03	0.411E-04	0.379E-05
0.05	0.151E-02	0.277E-02	0.408E-03	0.363E-04	0.357E-05
0.06	0.889E-03	0.188E-02	0.314E-03	0.309E-04	0.327E-05
0.07	0.521E-03	0.125E-02	0.234E-03	0.255E-04	0.290E-05
0.08	0.303E-03	0.819E-03	0.170E-03	0.203E-04	0.250E-05
0.09	0.176E-03	0.527E-03	0.121E-03	0.158E-04	0.210E-05
0.10	0.101E-03	0.335E-03	0.843E-04	0.120E-04	0.172E-05
0.11	0.578E-04	0.210E-03	0.576E-04	0.886E-05	0.137E-05
0.12	0.329E-04	0.130E-03	0.387E-04	0.643E-05	0.107E-05
0.13	0.186E-04	0.794E-04	0.256E-04	0.458E-05	0.814E-06
0.14	0.104E-04	0.480E-04	0.167E-04	0.320E-05	0.608E-06
0.15	0.580E-05	0.288E-04	0.107E-04	0.220E-05	0.446E-06
0.16	0.321E-05	0.171E-04	0.678E-05	0.149E-05	0.322E-06
0.17	0.176E-05	0.100E-04	0.425E-05	0.993E-06	0.228E-06
0.18	0.962E-06	0.582E-05	0.263E-05	0.652E-06	0.159E-06
0.19	0.521E-06	0.335E-05	0.161E-05	0.423E-06	0.109E-06
0.20	0.280E-06	0.191E-05	0.969E-06	0.270E-06	0.736E-07
0.21	0.149E-06	0.108E-05	0.579E-06	0.171E-06	0.490E-07
0.22	0.789E-07	0.602E-06	0.342E-06	0.106E-06	0.322E-07
0.23	0.414E-07	0.333E-06	0.199E-06	0.653E-07	0.208E-07
0.24	0.215E-07	0.183E-06	0.115E-06	0.397E-07	0.133E-07
0.25	0.111E-07	0.991E-07	0.657E-07	0.238E-07	0.839E-08
0.26	0.568E-08	0.532E-07	0.371E-07	0.141E-07	0.522E-08
0.27	0.287E-08	0.283E-07	0.207E-07	0.826E-08	0.320E-08
0.28	0.144E-08	0.149E-07	0.114E-07	0.478E-08	0.194E-08
0.29	0.717E-09	0.775E-08	0.622E-08	0.273E-08	0.116E-08
0.30	0.353E-09	0.399E-08	0.336E-08	0.154E-08	0.684E-09
0.31	0.172E-09	0.203E-08	0.179E-08	0.857E-09	0.399E-09
0.32	0.828E-10	0.103E-08	0.942E-09	0.472E-09	0.229E-09
0.33	0.395E-10	0.511E-09	0.490E-09	0.256E-09	0.130E-09
0.34	0.186E-10	0.251E-09	0.252E-09	0.137E-09	0.727E-10
0.35	0.867E-11	0.122E-09	0.128E-09	0.728E-10	0.401E-10
0.36	0.399E-11	0.587E-10	0.640E-10	0.380E-10	0.219E-10
0.37	0.182E-11	0.279E-10	0.317E-10	0.196E-10	0.117E-10
0.38	0.817E-12	0.130E-10	0.154E-10	0.996E-11	0.622E-11
0.39	0.362E-12	0.603E-11	0.743E-11	0.499E-11	0.325E-11
0.40	0.158E-12	0.275E-11	0.353E-11	0.247E-11	0.167E-11
0.41	0.684E-13	0.123E-11	0.165E-11	0.120E-11	0.846E-12
0.42	0.291E-13	0.547E-12	0.760E-12	0.576E-12	0.422E-12
0.43	0.122E-13	0.238E-12	0.345E-12	0.272E-12	0.207E-12
0.44	0.503E-14	0.102E-12	0.154E-12	0.126E-12	0.100E-12
0.45	0.204E-14	0.433E-13	0.678E-13	0.578E-13	0.476E-13
0.46	0.817E-15	0.180E-13	0.293E-13	0.260E-13	0.223E-13
0.47	0.321E-15	0.734E-14	0.124E-13	0.115E-13	0.102E-13
0.48	0.124E-15	0.295E-14	0.519E-14	0.498E-14	0.462E-14
0.49	0.469E-16	0.116E-14	0.213E-14	0.212E-14	0.204E-14

Tabela 4.1: Vrednosti funkcije $\mathcal{R}_{k,p,\gamma}(w)$ za $k = 50$ i $\gamma = 0.02$

Razmotrimo sada specijalne slučajeve nejednakosti (4.10) kad je $w \in \{0, 1, 2\}$. Za $w = 0$ dobija se nejednakost $z \leq \gamma k^2 + 1$, ili $p \geq 1/(\gamma k^2 + 2)$, pa je

$$w_0(k, p, \gamma) = 0 \text{ za } p \leq \frac{1}{\gamma k^2 + 2} .$$

Dalje, za $w = 1$ nejednakost (4.10) postaje

$$z^2 + kz - \gamma k^2 - 1 - k \leq 0.$$

Njeno rešenje je $z \geq z_1$, gde je

$$z_1 = \sqrt{(\frac{1}{4} + \gamma)k^2 + k + 1} - \frac{k}{2},$$

odnosno $p < 1/(1 + z_1)$. Dakle, $w_0 = 1$ je optimalna dubina pretrage ako je p iz intervala

$$\frac{1}{\gamma k^2 + 2} < p < \frac{1}{1 + z_1} .$$

Nejednakost $\mathcal{R}_{k,p,\gamma}(2) < \mathcal{R}_{k,p,\gamma}(3)$ je za $z = 1 + 2\gamma$ ekvivalentna sa $-k(3\gamma + 4\gamma^2) + 1 - (1 + 2\gamma)^3 \geq 0$, pa nije zadovoljena ni za jedno $k \geq 1$. Zbog toga suprotna nejednakost važi za svako z, $z \geq 1 + 2\gamma$, i za svako k, $k \geq 1$. Dakle,

$$w_0(k, p, \gamma) = 2 \text{ za } \frac{1}{1 + z_1} < p < \frac{1}{2(1 + \gamma)} .$$

Time je nalaženje optimalne dubine pretrage praktično rešeno. U specijalnom slučaju kad je $k = 50$ i $\gamma = 0.02$, dobija se da je optimalna dubina w jednaka $w = 0$ za $0 < p = 0.0192$, $w = 1$ za $0.0192 < p < 0.3396$, odnosno $w = 2$ za $0.3396 < p < 0.4901$, što je u skladu sa podacima navedenim u Tabeli 4.1

Na osnovu izloženog može se zaključiti da je u sklopu Algoritma 2.1 za dekodiranje kodova $R_{h,n}$ optimalna dubina pretrage najčešće jednaka jedan ili dva, tj. optimalno je za izabrani informacioni skup izračunavati rastojanje od primljene poruke onih kodnih reči koje se od nje na informacionom skupu razlikuju na najviše jednoj ili dve pozicije.

Poglavlje 5

Eksperimentalni rezultati

S obzirom da se Algoritam 2.1 zbog složenosti ne može do kraja teorijski analizirati, sproveden je izvestan broj eksperimenata sa ciljem da se ovaj algoritam uporedi sa Algoritmima A i B iz [Meie89]. Da bi se stekla bolja predstava o ponašanju algoritma, njegovo izvršavanje nije prekidano u trenutku nalaženja rešenja. Eksperimenti su sprovedeni sa jednim fiksiranim kodom $R_{h,n}$, pri čemu je varirana verovatnoća greške. Za kontrolu ponašanja algoritma korišćeno je rešenje, odnosno kodna reč koja je dovedena na ulaz BSK. Praćeno je kretanje broja grešaka posle pojedinih ciklusa, odnosno iteracija, i to u celoj primljenoj poruci, kao i na pozicijama iz izabranih informacionih skupova.

Eksperimenti su vršeni sa kodom $R_{h,n}$, gde je $h(z) = 1 + z^{25} + z^{73}$ i $n = 800$. Broj članova polinoma $h(z)$ različitih od konstante je $m = 2$. Razmotrimo najpre na osnovu [Meie89] kako bi se na ovom kodu ponašali Algoritmi A i B iz ovog rada kad verovatnoća p uzima vrednosti 220/1024, 230/1024, ..., 280/1024. Numerička složenost Algoritma A ocenjuje se sa 2^{ck} (videti [Meie89], odnosno tačku 1.3). Vrednosti parametra c i ocene složenosti 2^{ck} date su u sledećoj tabeli.

p	$c(p,m,n/k)$	2^{ck}	$F(p,m,n/k)$
220/1024	0.111	275	0.687
230/1024	0.137	1020	0.619
240/1024	0.167	4680	0.567
250/1024	0.201	26100	0.525
260/1024	0.238	170000	0.482
270/1024	0.280	1420000	0.439
280/1024	0.325	13900000	0.395

Na osnovu toga može se zaključiti da je dekodiranje ovog koda pomoću Algoritma A praktično izvodljivo za sve ove verovatnoće. Ipak, za $p = 280/1024$ složenost dekodiranja je blizu gornje granice prihvatljivosti, naročito ako se uzme u obzir da se pod elementarnom operacijom ovde podrazumeva sabiranje dva vektora iz B_{800} i nalaženje težine njihovog zbira.

U istoj tabeli navedene su i odgovarajuće vrednosti faktora korekcije $F(p,m,n/k)$ za Algoritam B (videti takođe [Meie89], odnosno tačku 1.3). Na osnovu zaključka iz citiranog rada, vrednosti faktora korekcije veće od 0.5 garantuju uspešno dekodiranje primenom Algoritma B sa velikom verovatnoćom. S druge strane, ako je faktor korekcije mali (manji od 0.5), onda se značajno smanjuje verovatnoća uspešnog dekodiranja. Sprovedeni eksperimenti (iako ne opsežni) sa probabilističkom fazom Algoritma 2.1, koja je slična Algoritmu B, potvrđuju ove zaključke. Za $p = 220/1024$ dekodiranje je završeno u drugom ciklusu, odnosno posle ukupno šest iteracija, a za $p = 230/1024$ – u trećem ciklusu, posle ukupno sedam iteracija. Za veće vrednosti verovatnoće, $p \geq 230/1024$ dekodiranje nije bilo uspešno. Broj grešaka se posle prvih nekoliko iteracija značajno smanjuje, a zatim se blago povećava i zaustavlja. Dekodiranje se u ovim slučajevima uvek završavalo tako što na kraju nekog ciklusa ni jedna AVG ne bi bila veća od 1/2.

U naredne tri tabele prikazano je ponašanje Algoritma 2.1 u tri eksperimenta sa verovatnoćom greške $p = 280/1024$. Broj iteracija u jednom ciklusu ograničen je na pet, kao i u [Meie89]. Očekivani broj bita sa AVG većom od 1/2 posle prve iteracije je $n_{thr} = 121$. Za svaku iteraciju prikazan je broj bita sa AVG većom od 1/2, kao i trenutni broj grešaka (zbir broja tačnih bita sa AVG većom od 1/2 i broja pogrešnih bita sa AVG manjom od 1/2). U fazi pretrage svakog ciklusa birano je

Redni broj	Ciklus	Iteracija	n_w	Broj grešaka	k'		Inform. skupova sa				
					min.	izabrano	0	1	2	3	bar 4
							grešaka				
				230							
1	1	1	128	188	157	172	0	0	0	0	10
2	2	1	34	166							
3	2	2	79	127							
4	2	3	111	107							
5	2	4	138	96	493	542	0	0	2	4	4
6	3	1	9	95							
7	3	2	28	86							
8	3	3	39	81							
9	3	4	43	77							
10	3	5	50	68	674	741	0	0	0	0	10
11	4	1	2	66							
12	4	2	9	61							
13	4	3	10	60							
14	4	4	17	55							
15	4	5	25	57	454	499	0	0	1	1	8
16	5	1	0	57							
17	5	2	3	60							
18	5	3	6	63							
19	5	4	6	63							
20	5	5	6	63	277	304	0	0	0	0	10
21	6	1	0	63							
22	6	2	0	63							
23	6	3	0	63							
24	6	4	0	63							
25	6	5	0	63	114	125	0	0	0	0	10

Tabela 5.1: Prikaz rezultata prvog eksperimenta

na slučajan način po 10 informacionih skupova. Broj koordinata k' u podskupu I' iz koga se bira informacioni skup biran je tako da bude za 10% veći od donje granice (najmanjeg broja za koji je rang odgovarajuće podmatrice generišuće matrice koda jednak k, videti tačku 4.1) U tabeli je za svaki ciklus dat broj informacionih skupova sa 0, 1, 2, 3, odnosno bar 4 grešaka. Jasno je da ako se za dubinu pretrage w usvoji vrednost $w = 2$, onda se dekodiranje uspešno završava onog trenutka kad se naiđe na informacioni skup sa najviše dve greške.

U sva tri eksperimenta se za $w = 2$ dekodiranje uspešno završava već posle drugog ciklusa. Nasuprot tome, dekodiranje primenom samo probabilističke faze (odnosno Algoritma B) nije bilo uspešno ni u jednom slučaju! Zapaža se da se dekodiranje obično završava posle drugog ciklusa, kada je najmanji srednji broj grešaka u informacionim skupovima. Ovu pojavu je teško objasniti, jer se ne vidi način da

Redni broj	Ciklus	Iteracija	n_w	Broj grešaka	k'		Inform. skupova sa				
					min.	izabrano	0	1	2	3	bar 4
							grešaka				
				222							
1	1	1	96	170	169	185	0	0	0	1	9
2	2	1	39	139							
3	2	2	90	98							
4	2	3	129	73	472	519	0	4	4	1	1
5	3	1	4	69							
6	3	2	14	59							
7	3	3	32	53							
8	3	4	44	47							
9	3	5	51	44	641	705	0	0	1	4	5
10	4	1	0	44							
11	4	2	0	44							
12	4	3	0	44							
13	4	4	0	44							
14	4	5	0	44	114	125	0	0	1	5	4

Tabela 5.2: Prikaz rezultata drugog eksperimenta

Redni broj	Ciklus	Iteracija	n_w	Broj grešaka	k'		Inform. skupova sa				
					min.	izabrano	0	1	2	3	bar 4
							grešaka				
				215							
1	1	1	109	168	183	201	0	0	0	0	10
2	2	1	34	142							
3	2	2	79	107							
4	2	3	117	75							
5	2	4	132	60	593	652	0	2	3	4	1
6	3	1	6	54							
7	3	2	17	47							
8	3	3	26	38							
9	3	4	31	31							
10	3	5	31	31	530	583	0	7	3	0	0
11	4	1	0	31							
12	4	2	0	31							
13	4	3	0	31							
14	4	4	0	31							
15	4	5	0	31	560	616	0	9	1	0	0

Tabela 5.3: Prikaz rezultata trećeg eksperimenta

se postavi dovoljno precizan model ove situacije koji bi se zatim mogao egzaktno analizirati.

Zapaža se za parametar k' posle druge i kasnijih iteracija uzima znatno veću vrednost nego što bi se to očekivalo na osnovu analize iz tačke 4.1. Odstupanje je tako veliko da bi se ovakvim postupkom mogle formirati velike podmatrice generišuće matrice koda sa rangom manjim od k.

Bibliografija

[Bass77] Л. А. Бассалиго, В. В. Зяблов, М. С. Пинскер, Проблемы сложности в теории корректирующих кодов, Проблемы Передачи Информации XIII/3, 5–17, 1977.

[Batt79] G. Battail, M. C. Decouvelaere, P. Godlewski, "Replication Decoding", *IEEE Trans. Inform. Theory*, IT–25, 332–345, maj 1979.

[Baum78] L. D. Baumert, R. J. McEliece, Soft Decision Decoding of Block Codes, *DSN Progres Report* 42–47, JPL, California Institute of Technology, Pasadena, California, jul i avg. 1978.

[Be'e86] Y. Be'ery, J. Snyders, Optimal Soft Decision Block Decoders Based on Fast Hadamard Transform, *IEEE Trans. Inform. Theory*, IT–32/3, 355–364, 1986.

[BerM78] E. R. Berlecamp, R. J. McEliece, H. C. A. van Tilborg, On the Inherent Intractability of Certain Coding Problems, *IEEE Trans. Inform. Theory*, IT–24/3, 384–386, maj 1978.

[Berl68] E. R. Berlekamp, *Algebraic Coding Theory*, McGraw–Hill, New York, 1968.

[Boss86] M. Bossert, F. Hergert, Hard– and Soft–Decision Decoding Beyond the Half Minimum Distance – An Algorithm for Linear Codes, *IEEE Trans. Inform. Theory*, IT–32/5, 709–714, sep. 1986.

[Clar82] G. C. Clark, Jr., J. B. Cain, *Error–Correction Coding for Digital Communications*, Plenum Press, New York, 1982.

[Cohe76] G. Cohen, P. J. Godlewski, Rezidual Error Rate of Linear Block Codes, *IEEE Trans. Inform. Theory*, IT–22/4, 483–485, jul 1976.

[Dels78] P. Delsarte, Partial–Optimal Piecewise Decoding of Linear Codes, IEEE Trans. Inform. Theory IT–24/1, 70–75, jan. 1978.

[Dors74] B. G. Dorsch, A Decoding Algorithm for Binary Block Codes and J–ary Output Channels, *IEEE Trans. Inform. Theory*, IT–20/5, 391–394, maj 1974.

[El–A84] M. A. El–Agamy, E. Munday, Probabilistic Hard–Decision Table Look–up Decoding for Bynary Block Codes, *Electronics Letters*, 20/22, 922–923, okt. 1984.

[Evse83] Г. С. Евсеев, О сложности декодирования линейних кодов, Проблемы Передачи Информации XIX/1, 3–8, 1983.

[Gall62] R. G. Gallager, Low–Density Parity–Check Codes, IEEE Transactions on Information Theory IT–8, 21–28, jan. 1962.

[Gall60] R. G. Gallager, *Low–Density Parity–Check Codes*, disertacija, MIT, Cambridge, 1960.

[Golo67] S. W. Golomb, *Shift Register Sequences*, Holden–Day, San Francisko, 1967.

[Hart76] C. R. P. Hartmann, L. D. Rudolph, An Optimum Symbol–by–Symbol Decoding Rule for Linear Codes, *IEEE Trans. Inform. Theory*, IT–22/5, 514–517, sep. 1976.

[Kasa85] T. Kasami, T. Fujiwara, S. Lin, An Approximation to the Weight Distribution of Binary Linear Codes, *IEEE Trans. Inform. Theory*, IT–31/6, 769–780, nov. 1985.

[Kruk89] Е. А. Крук, Граница сложности декодирования линейных блоковых кодов, Проблемы Передачи Информации XXV/2, 103–107, 1989.

[LeeB88] P. J. Lee, E. F. Brickell, An Observation on the Security of McEliece's Public–Key Cryptosystem, Eurocrypt'88

[Levi85] L. B. Levitin, C. R. P. Hartmann, A New Approach to the General Minimum Distance Decoding Problem: The Zero–Neighbors Algorithm, *IEEE Trans. Inform. Theory*, IT–31/3, 378–384, maj 1985.

[LinC83] S. Lin, D. J. Costello, *Error–Control Coding – Fundamentals and Applications*, Prentice–Hall, 1983.

[Lint82] J. H. van Lint, *Introduction to Coding Theory*, Graduate texts in Mathematics 86, Springer, New York, 1982.

[MacW77] F. J. MacWilliams, N. J. A. Sloane, *The Theory of Error Correcting Codes*, North–Holland, 1977.

[Meie88] W. Meier, O. Staffelbach, Fast Correlation Attacks on Stream Ciphers, u knj. C. G. Günter, ed., *Advances in Cryptology — EUROCRYPT'88*, Springer, Berlin, 1988. (ser. Lecture Notes in Computer Sciences, 330)

[Meie89] W. Meier, O. Staffelbach, Fast Correlation Attacks on Certain Stream Ciphers, *Journal of Cryptology*, 1, 159–176, 1989.

[Miha90] M. Mihaljević, J. Dj. Golić, A Fast Iterative Algorithm for a Shift Register Initial State Reconstruction Given the Noisy Output Sequence, Proc. Auscrypt'90, Sidnej, jan. 1990.

[Nije71] A. Nijenhuis, H. S. Wilf, *Combinatorial Algorithms for Computers and Calculators*, Academic Press, New York, 1978.

[Nils71] N. J. Nilsson, *Problem–Solving Methods in Artificial Inteligence*, McGraw–Hill, New York, 1971.

[Pete72] W. W. Peterson, E. J. Weldon, *Error–Correcting Codes*, 2nd Edition, MIT Press, 1972.

[Redi73] G. R. Redinbo, Inequalities Between the Probability of a Subspace and the Probabilities of its Cosets, *IEEE Trans. Inform. Theory*, IT–19, 533–536, jul 1973.

[Sieg84] T. Siegenthaler, Correlation–Immunity of Nonlinear Combining Functions for Cryptographic Applications, *IEEE Trans. Inform. Theory*, IT–30/5, 776–780, sep 1984.

[Sieg85] T. Siegenthaler, Decrypting a Class of Stream Ciphers Using Ciphertext Only, *IEEE Trans. Comput.*, C–34/1, 81–85, jan. 1985.

[Sull67] D. D. Sullivan, A Fundamental Inequality Between the Probabilities of Binary Subgroups and Cosets, *IEEE Trans. Inform. Theory*, IT–13/1, 91–94, jan. 1967.

[Wolf78] J. K. Wolf, Efficient Maximum Likelihood Decoding of Linear Block Codes Usinng a Trellis, *IEEE Trans. Inform. Theory*, IT–24/1, 76–80, jan. 1978.

[Zolo86] В. В. Золотарев, Многопороговое декодирование, Проблемы Передачи Информации, XXII/1, 104–109, 1986.

[Zyab75] В. В. Зяблов, М. С. Пинскер, Оценка сложности исправления осхибок низкоплотностными кодами Галлагера, Проблемы Передачи Информации, XI/1, 23–36, 1975.

[Živk90] M. Živković, On Two Probabilistic Decoding Algorithms for Binary Linear Codes, rad u pripremi

[Živl90] M. Živković, Some Improooovements of a Decoding Algorithm for Linear Codes, rad u pripremi

INDEX

Index