

**O‘ZBEKISTON RESPUBLIKASI AXBOROT TEXNOLOGIYALARI
VA KOMMUNIKATSIYALARINI RIVOJLANTIRISH VAZIRLIGI**

**MUHAMMAD AL-XORAZMIY NOMIDAGI
TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI**

Ganiev Salim Karimovich

G‘ulomov Sherzod Rajaboevich

Axborot nazariyasi va kodlash

O‘quv qo‘llanma

prof. S.K. Ganiev tahriri ostida

Toshkent 2017

Axborot nazariyasi va kodlash: O‘quv qo‘llanma / S.K. Ganiev, SH.R. G‘ulomov. Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti. –Toshkent: 2017, 99 b.

S.K. Ganiev, SH.R. G‘ulomov

“Axborot nazariyasi va kodlash” fani bo‘yicha o‘quv qo‘llanma tayanch oliy o‘quv yurti Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universitetining “Axborot xavfsizligini ta’minlash” kafedrasida professor-o‘qituvchilari tomonidan tayyorlangan bo‘lib, unda informatsiya, informatsion jarayonlar, sistemalar, texnologiyalar; informatsiyaning miqdoriy o‘lchovlari, entropiya; shartli entropiya va birlashma entropiya; nisbiy entropiya va xabarlarining ortiqchaligi; informatsiyani uzatish tezligi va aloqa kanalining o‘tkazish qobiliyati; kodlar, kodlash va dekodlash, kodlash nazariyasining asosiy tushunchalari; xalalsiz kanallar uchun SHennon teoremasi; samarali kodlarni qurish algoritmlari; xalalli kanallar uchun SHennon teoremasi, xalallarga bardosh kodlash; kodning tuzatish qobiliyati bilan kod masofasi orasidagi bog‘liqlik; berilgan tuzatish qobiliyatli kodlarni qurish; chiziqli blok kodlar; uzluksiz, rekurrent va zanjir rekurrent kodlar xususida ma’lumotlar keltirilgan. O‘quv qo‘llanmada analog signallarni raqamli shaklga keltirish, avtomatlar nazariyasi, kod o‘zgartgichlari hamda kodlash yordamida informatsiyani himoyalash xususidagi materiallar ham o‘rin olgan.

O‘quv qo‘llanma 5330500-Kompyuter injiniringi (“Kompyuter tizimlarini loyihalash”, “Amaliy dasturiy vositalarni loyihalash”, “Axborot va multimedia texnologiyalari”, “Axborot xavfsizligi, kriptografiya va kriptozanaliz”) magistratura mutaxassisligining “Axborot xavfsizligi, kriptografiya va kriptozanaliz” ixtisosligi bo‘yicha ta’lim oluvchi talabalarga mo‘ljallangan.

Taqrizchilar:

TATU, Telekommunikatsiyada boshqaruv tizimlarining apparat va dasturiy ta’minoti kafedrasida mudiri, t.f.n., dotsent **Abduraxmonov R.P.**

Axborot xavfsizligini ta’minlash markazining “Axborot xavfsizligini ta’minlash vositalarini joriy qilishning istiqbolli tadqiqotlari” bo‘limi boshlig‘i, t.f.n. **Nigmanov A.A.**

Mundarija

Muqaddima	4
1 BOB Informatsiya, informatsion jarayonlar, sistemalar va texnologiyalar	5
1.1. “Informatsiya” tushunchasi.....	5
1.2. Informatsion jarayonlar.....	5
1.3. Informatsion sistemalar.....	6
1.4. Informatsion texnologiyalar.....	7
2 BOB Informatsiyani miqdoriy baholash	9
2.1. Informatsiyaning struktura o‘lchovi.....	9
2.2. Informatsiyaning statistik o‘lchovi. Entropiya.....	11
2.2.1. Shartli entropiya va birlashma entropiya.....	14
2.2.2. Nisbiy entropiya va xabarlarining ortiqchaligi.....	16
2.2.3. Informatsiyani uzatish tezligi va aloqa kanalining o‘tkazish qobiliyati.....	19
2.3. Informatsiyaning semantik o‘lchovi.....	22
2.4. Informatsiyani o‘zgartirish.....	23
3 BOB Kodlash va dekodlash	25
3.1. Kodlar, kodlash va dekodlash.....	25
3.2. Samarali kodlarni qurishning Shannon-Fano algoritmi.....	29
3.3. Samarali kodlarni qurishning Xaffmen algoritmi.....	32
4 BOB Xalallarga bardosh kodlash	34
4.1. Xalallarga bardosh kodlar.....	34
4.2. Kodning tuzatish qobiliyati bilan kod masofasi orasidagi bog‘liqlik.....	37
4.3. Berilgan tuzatish qobiliyatli kodlarni qurish.....	41
5 BOB Chiziqli blok kodlar	43
5.1. Xemming kodi.....	43
5.2. Siklik kodlar.....	47
6 BOB Uzlaksiz kodlar. Rekurrent kodlar	51
6.1. Avtomatlar nazariyasi.....	51
6.2. Rekurrent kodlar.....	56
6.3. Zanjir rekurrent kodlar.....	60
7 BOB Kod o‘zgartgichlari	66
7.1. To‘g‘ri koddan teskari va qo‘shimcha kodlarni hosil qilish.....	66
7.2. O‘nli kodni ikkilik-o‘nli kodda va ikkilik-o‘nli kodni o‘nli kodda ifodalovchi o‘zgartgichlar.....	68
7.3. Grey kodi.....	71
7.4. Kodlash yordamida informatsiyani himoyalash.....	74
Adabiyotlar	76
Ilovalar	77

MUQADDIMA

Ehtimollik nazariyasi va matematik statistikaga asoslanuvchi axborot nazariyasi hozirda jiddiy va yetarlicha universal fanga aylandi. Ushbu nazariya o'lchash, nazoratlash va boshqarish jarayonlarini tahlillashda keng qo'llaniladi. Ushbu nazariyaning qoidalarini fikrlash, anglash, psixologiya jarayonlarini hamda ijtimoiy hodisalarni tadqiqlashda yanada kengroq ishlatiladi.

Axborot nazariyasi rivojining avji 1947-1948 yillarga amerika matematigi va injeneri K. Shennon tomonidan ilmiy ishlar chop etilganidan keyingi vaqtlarga to'g'ri keladi. Ushbu ilmiy ishlarda axborotni miqdoriy baholashga doir asosiy qoidalar ta'riflangan.

Axborot nazariyasining rivoji aloqa texnikasining rivoji bilan uzviy bog'langan. Yigirmanchi asrning birinchi yarmida chop etilgan ilmiy ishlar aloqa tizimining asosiy xarakteristikalarini va axborotni uzatish sifatini miqdoriy baholashni ilmiy asoslashga bag'ishlangan. Ushbu ilmiy ishlarda axborot miqdorini baholashning logarifmik o'lchovi, signallarni diskretlash xususidagi teorema hamda aloqa kanalining o'tkazish qobiliyatini baholash bo'yicha qator amaliy tavsiyalar taklif etilgan.

Axborot nazariyasi va kodlash fanining masalalari quyidagilar:

- axborotni saqlashga mo'ljallangan xotira qurilmasining hajmini aniqlash;
- berilgan axborot simvollarining minimal soni orqali uzatishga imkon beruvchi kodlashning eng tejamli usullarini qidirish;
- uzatilayotgan axborotning kechikishsiz va buzilishsiz uzatishini ta'minlovchi kanalning o'tkazish qobiliyatini aniqlash;
- kodlashdan axborotni kriptografik berkitish vositasi sifatida foydalanish.

Ushbu o'quv qo'llanma talabalarga yuqorida keltirilgan masalalar bo'yicha ko'nikmalar hosil qilishlarida ko'makchi vazifasini o'taydi.

1 BOB. INFORMATSIYA, INFORMATSION JARAYONLAR, SISTEMALAR VA TEXNOLOGIYALAR

1.1. “Informatsiya” tushunchasi

Informatsiya atamasi, lotincha *information* soʻzidan kelib chiqib, bildirish, ish mazmunini bayon etish tushunchalarini beradi. Kibernetika fanining asoschisi Norbert Viner oʻzining asarida *informatsiya materiya emas, energiya emas, bu - informatsiya* deb yozadi. Aytib oʻtish joizki, informatsiya doimo moddiy – energetika shaklida signal koʻrinishida namoyon boʻladi.

Texnika vositalari yordamida qidirish, qabul qilish, saqlash, ishlov berish, uzatish mumkin boʻlgan shaklga keltirilgan har qanday informatsiya *maʼlumot* deb ataladi.

Informatsiya va *maʼlumot* *Informatika* fanining asosiy tushunchalari hisoblanadi. *Ushbu tushunchalar orasida farq bormi?* degan savol tugʻilishi tabiiy. Savolga javob berish uchun quyidagi misolni koʻraylik: Doʻstingiz bir varaq qogʻozga oʻnta telefon tartib raqamini yozib sizga koʻrsatdi, deylik. Siz koʻrsatilgan raqamlarni *maʼlumot* sifatida qabul qilasiz. Chunki siz bu raqamlardan foydalana olmaysiz. Agar doʻstingiz telefon tartib raqamining toʻgʻrisiga firmaning nomi va faoliyat turini yozsa, unda siz uchun bu *maʼlumotlar* informatsiyaga aylanadi, chunki kelgusida undan foydalanish mumkin.

Informatsiya tushunchasiga umumiy falsafiy taʼrifdan (voqeʼ dunyoning inʼikosi) tor praktik taʼrifgacha (saqlash, uzatish va ishlov berish obʼekti hisoblanuvchi barcha *maʼlumotlar*) koʻpgina taʼrif berilgan.

Fikrimizcha, quyidagi taʼrif informatsiya mohiyatini toʻlaroq aks ettiradi.

Informatsiya – muayyan obʼekt xususidagi bilimlarimiz noaniqlik darajasini pasaytirishga imkon beruvchi har qanday axborot (*maʼlumot*).

1.2. Informatsion jarayonlar

Informatsiya oʻz – oʻzidan paydo boʻlmaydi, u informatsion jarayonlarda paydo boʻladi. Informatsiyani qidirish, toʻplash, saqlash, uzatish, ishlov berish va

foydalanish bilan bog‘liq jarayonlar *informatsion jarayonlar* deyiladi.

Informatsiyani *qidirishning* quyidagi usullarini ko‘rsatish mumkin:

- bevosita kuzatish;
- qiziqtiradigan masala bo‘yicha mutaxassislar bilan muloqot;
- kerakli adabiyotlarni o‘qish;
- video, teleprogrammalarini ko‘rish;
- audio kasseta, radio eshittirishlarni eshitish;
- axborot – resurs markazlarida, arxivlarda ishlash;
- informatsion sistemalarga, kompyuter ma’lumotlarining baza va banklariga

murojaat;

- boshqa usullar.

Informatsiyani *saqlash* usullari uning to‘plagichlariga bog‘liq. Jamoat uchun informatsiya axborot – resurs markazlarida, videotekalarda, fonotekalarda, arxivlarda, patent byurolarida, muzeylarda, rasm galereyalarida saqlansa, kompyuterda saqlashda esa ma’lumot bazalari va banklaridan, informatsion qidirish sistemalaridan, elektron ensiklopediyalaridan, mediatekalardan foydalaniladi.

Informatsiyani *uzatish* jarayonida informatsiya manbai va qabul qiluvchisi qatnashadi: birinchisi informatsiyani uzatadi, ikkinchisi uni qabul qiladi. Ularning orasida informatsiyani uzatish kanali – aloqa kanali ishlaydi. Uzatish jarayonida informatsiya yo‘qolishi yoki buzilishi mumkin. Shu sababli aloqa kanalini himoya qilish qurilmalari ishlatilishi lozim.

1.3. Informatsion sistemalar

Sistema – atrof-muhit shart – sharoitlarini hisobga olgan holda ma’lum (yagona) maqsadga yo‘naltirilgan, o‘zaro bog‘langan ob’ektlar majmui. Sistemalar o‘zining tarkibi va maqsadi bilan bir – biridan farq qiladi.

Informatsion sistema – berilgan maqsadga erishishda informatsiyani saqlash, unga ishlov berish va uzatish jarayonlarida foydalaniladigan vositalar, usullar va xodimlarning o‘zaro bog‘langan majmui.

Umuman, informatsion sistemani murakkab sistemalar safiga kiritish mumkin va uning tarkibi informatsion, texnik, matematik, dasturiy, tashkiliy va huquqiy ta'minotlardan iborat ekanligini tasavvur etish mumkin.

Informatsion ta'minotga informatsiyani tasniflash va kodlashning yagona sistemasi, unifikatsiyalangan xujjatlar sistemasi, tashkilotda ishlatiluvchi informatsion oqim sxemalari hamda ma'lumotlar bazasini qurish metodologiyasi kiradi.

Texnik ta'minotga informatsion sistemaning ishlashini ta'minlovchi texnik vositalar kompleksi hamda bu vositalarga va texnologik jarayonlarga taalluqli xujjatlar kiradi.

Matematik va dasturiy ta'minotga informatsion sistema maqsadi va vazifalarini amalga oshiruvchi hamda texnik vositalar majmuini bir me'yorda ishlashini ta'minlovchi matematik modellar, metodlar, algoritmlar va dasturlar kiradi.

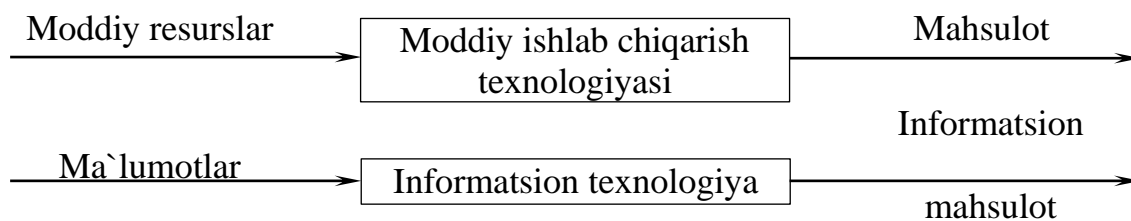
Tashkiliy ta'minotga informatsion sistemani yaratish va ishlatish jarayonida xodimlarning texnik vositalar bilan o'zaro munosabati tartibini belgilovchi usullar va vositalar kiradi.

Huquqiy ta'minotga informatsion sistemani yaratish, yuridik maqomini va ishlashini aniqlovchi, informatsiyani olish, o'zgartirish va undan foydalanish tartibini belgilovchi huquqiy me'yorlar kiradi.

1.4. Informatsion texnologiyalar

Informatsiya jamiyat uchun elektroenergiya, neft, gaz, foydali qazilmalar va h. singari muhim resurslardan hisoblanadi.

Moddiy ishlab chiqarish texnologiyasining maqsadi - inson yoki sistemaning ehtiyojini qondirish, maxsulot chiqarish bo'lsa, informatsion texnologiyaning maqsadi – inson taxlili asosida aniq amal bajarishga qaror qabul qilish uchun informatsiyani shakllantirish. Moddiy ishlab chiqarish va informatsion texnologiyalarning struktura jihatidan bir – biriga o'xshashligini quyidagi rasmdan ko'rish mumkin.



1.1-rasm. Informatsion texnologiyaning moddiy resurslarni ishlash texnologiyasiga o‘xshashligi

Demak, informatsion texnologiya tushunchasiga quyidagicha ta’rif berish mumkin.

Informatsion texnologiya-ob’ekt, jarayon yoki xodisa holati xususidagi yangi sifatli informatsiyani (informatsion mahsulotni) olish maqsadida ma’lumotlarni (birlamchi informatsiyani) to‘plash, ishlash va uzatish vositalari majmuasidan foydalanish jarayoni. Berilgan moddiy resursga turli texnologiyani qo‘llab, turli mahsulot, buyum olishimiz mumkin. Bu informatsiyani ishlash texnologiyasiga ham taalluqlidir.

Misol:

“Oliy matematika” fanidan nazorat ishini bajarish uchun talaba dastlabki informatsiyani (masala qo‘yilishini) ishlashda o‘zining texnologiyasini qo‘llaydi. Informatsion mahsulot (masala yechimi) talaba tanlagan yechish texnologiyasiga bog‘liq. Odatda masala qo‘lda yechiladi. Agar informatsion texnologiyadan foydalanilsa informatsion mahsulot boshqacha sifat kasb etadi. Informatsion texnologiyaning vazifalari bo‘yicha quyidagi turlarini ko‘rsatish mumkin:

- boshqarish;
- ofisni avtomatlashtirish;
- qaror qabul qilishni qo‘llash;
- ekspert sistemalar.

Nazorat savollari:

1. “Informatsiya” nima?
2. Informatsiyaning axborotdan farqi.

3. Informatsion jarayonga ta'rif bering.
4. Informatsion sistemaga ta'rif bering.
5. Informatsion sistemaning strukturasi.
6. Informatsion texnologiyaga ta'rif bering.

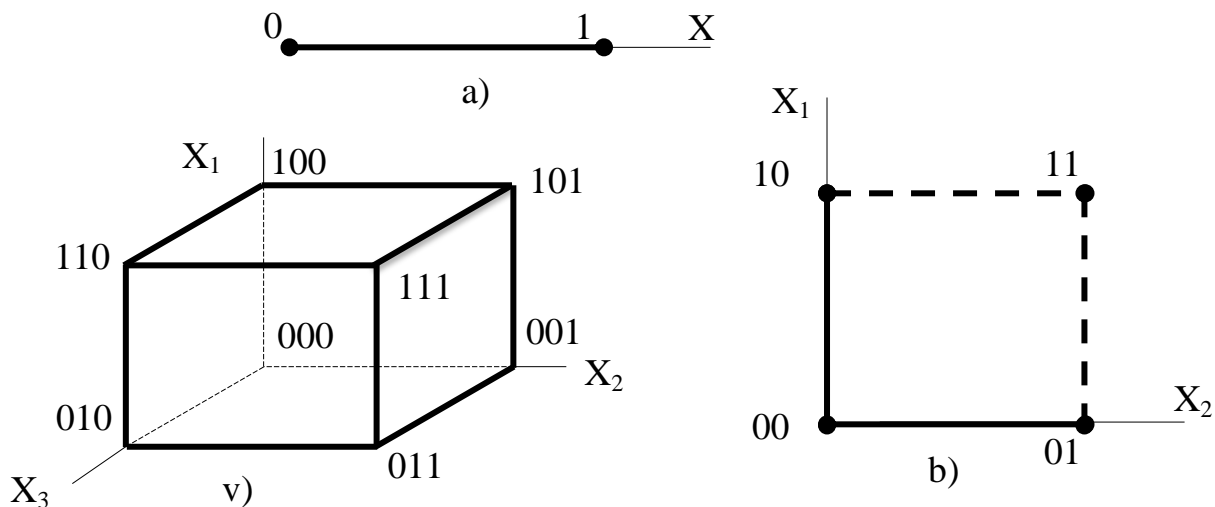
2 BOB. INFORMATSIYANI MIQDORIY BAHOLASH

2.1. Informatsiyaning struktura o'lchovi

Informatsiyaning struktura o'lchovidan foydalanilganda faqat xabarning diskret tuzilishini, undagi mavjud informatsion elementlar va ular orasidagi bog'lanishlar hisobga olinadi. Strukturaviy yondashishda informatsiyaning geometrik, kombinatorik va additiv o'lchovlari farqlanadi.

Geometrik o'lchov informatsion xabarning geometrik modelining parametrini (uzunligini, yuzasini, hajmini) diskret birliklarda o'lchashni faraz qiladi.

Masalan, informatsiyaning geometrik modeli sifatida birlik uzunlikdagi chiziqni (2.1-rasm a – "0" yoki "1" qiymatni oluvchi bir xonali so'z), kvadratni (2.1-rasm b – ikki xonali so'z) yoki kubni (2.1-rasm v – uch xonali so'z) ko'rsatish mumkin.



2.1-rasm. Informatsiyaning geometrik modeli

Ushbu strukturalarda informatsiyaning mumkin bo‘lgan maksimal qiymati modelning informatsion hajmini belgilaydi. Informatsion hajm barcha koordinatalar bo‘yicha diskret qiymatlarning yig‘indisi sifatida aniqlanadi.

Kombinatorik o‘lchovda informatsiya miqdori elementlar (simvollar) kombinatsiyalari soni sifatida aniqlanadi. Informatsiyaning mumkin bo‘lgan miqdori elementlarning mumkin bo‘lgan biriktirishlar, o‘rin almashtirishlar va joylashtirishlar soniga mos keladi. Faqat “0” va “1” lardan tarkib topgan so‘zlardagi simvollarni kombinatsiyalash so‘z qiymatini o‘zgartiradi.

Additiv o‘lchoviga (Xartli o‘lchoviga) muvofiq informatsiya miqdori ikkilik birliklarda – bitlarda o‘lchanadi. Bunda sonning teranligi (glubina) q va uzunligi n tushunchalari kiritiladi.

Sonning teranligi q – informatsiyani ifodalash uchun qabul qilingan elementlar (simvollar) soni. Sonning uzunligi n – berilgan kattalikdagi sonni ifodalash uchun zaruriy va yetarli pozitsiyalar (o‘rinlar) soni.

Sonning berilgan teranligi va uzunligida ifodalanish mumkin bo‘lgan sonlar soni $N = q^n$ ga teng. N kattalik informatsiya hajmini baholashda qulay hisoblanmaydi. Chunki, masalan, $N = 1$ bo‘lganida xabar nulli informatsiyani eltadi. Oldindan xarakteri ma’lum bo‘lgan xabarni olish esa hech nima bermaydi. Shu sababli, informatsiya miqdorini(bitlarni) hisoblashga imkon beruvchi logarifmik o‘lchov kiritilgan(Xartli tomonidan).

$$I(q) = \log_2 N = n \cdot \log_2 q$$

Demak, informatsiyaning 1 biti sodir bo‘luvchi yoki sodir bo‘lmaydigan bitta elementar hodisaga mos keladi. Informatsiya miqdorining bunday o‘lchovi qulay hisoblanadi, chunki u o‘lchovni son orqali ifodalashga imkon beradi. Bunda informatsiya miqdori “1” yoki “0” ikkilik simvollarning soniga ekvivalent hisoblanadi.

Ta’kidlash lozimki, ba’zida sonning teranligi tushunchasi *sanoq sistemasining asosi* tushunchasi bilan almashtiriladi.

Misol:

Alfavit simvollari ikkita sifat alomatlariga ega.

a) Xabar elementlarini 3,4,5 va 6 tadan kombinatsiyalab xabarlarining qanday miqdorini olish mumkin?

b) Bunday xabarlarining bitta elementiga informatsiyaning qanday miqdori to'g'ri keladi?

Yechish:

$$q = 2.$$

$$a) N_1=2^3=8; N_2=2^4=16; N_3=2^5=32; N_4=2^6=64.$$

$$b) I_1=\log_2 8=3 \text{ bit}; I_2=\log_2 16=4 \text{ bit}; I_3=\log_2 32=5 \text{ bit};$$

$$I_4=\log_2 64=6 \text{ bit}.$$

Nazorat savollari:

1. Strukturaviy yondashishda informatsiyaning qanday o'lchovlari farqlanadi?
2. Xartli o'lchovi nima?
3. Son teranligi nima?
4. Son uzunligi nima?

2.2. Informatsiyaning statistik o'lchovi. Entropiya

Informatsiyaning statistik nazariyasi K.Shennon tomonidan batafsil o'rganilgan. Yuz berish ehtimolligi birga yaqin bo'lgan tez-tez uchraydigan hodisa xususida xabar paydo bo'lsa, bunday xabarning qabul qiluvchi uchun informativligi kam bo'ladi. Xuddi shunday, yuz berish ehtimolligi nolga yaqin bo'lgan xabarning ham informativligi kam bo'ladi.

Hodisalarga qandaydir tajribaning natijasi sifatida qarash mumkinki, bunday tajribaning barcha natijalari *ansamblni*, ya'ni hodisalarning to'liq guruhini tashkil etadi. K.Shennon tajriba jarayonida paydo bo'luvchi hodisaning noaniqligi tushunchasini kiritdi va uni *entropiya* deb atadi.

Ansambl entropiyasi uning noaniqligining va demak informativligining miqdoriy o'lchovi bo'lib, tajribaning har bir mumkin bo'lgan natijalari ehtimolligi

to'plamining o'rtacha funksiyasi sifatida ifodalanadi.

Faraz qilaylik, q turli xilli N tajriba natijalari mavjud bo'lsin. i – natija n_i marta qaytariladi va miqdori I_i sifatida baholanuvchi informatsiyaga ega. U vaqtda bitta tajriba natijasida hosil bo'luvchi o'rtacha informatsiya quyidagicha aniqlanadi:

$$I_{o'rt} = \frac{n_1 I_1 + n_2 I_2 + \dots + n_q I_q}{N}$$

Agar har bir natijadagi informatsiya miqdorining uning ehtimolligi p_i bilan bog'liqligini hamda ikkilik birliklarda (bitlarda)

$$I_i = \log_2 \frac{1}{p} = -\log_2 p_i$$

kabi ifodalanishini hisobga olsak, quyidagini yozish mumkin.

$$I_{o'rt} = \frac{n_1(-\log_2 p_1) + \dots + n_i(-\log_2 p_i) + \dots + n_q(-\log_2 p_q)}{N}$$

$$\text{yoki } I_{o'rt} = \frac{n_1}{N}(-\log_2 p_1) + \dots + \frac{n_i}{N}(-\log_2 p_i) + \dots + \frac{n_q}{N}(-\log_2 p_q)$$

$\frac{n_1}{N}$ nisbatlar – natijalarning qaytarilish chastotalari, demak, ularni ehtimolliklari bilan almashtirish mumkin ($\frac{n_i}{N} = p_i$).

Unda bitlarda ifodalangan o'rtacha informatsiya miqdori quyidagiga teng bo'ladi:

$$I_{o'rt} = p_1(-\log_2 p_1) + \dots + p_i(-\log_2 p_i) + \dots + p_q(-\log_2 p_q)$$

$$\text{yoki } I_{o'rt} = -\sum_{i=1}^q p_i (\log_2 p_i) = H \text{ (Shenon formulasi)}$$

Hosil bo'lgan kattalik *entropiya* deb ataladi va H harfi bilan belgilanadi.

Entropiya quyidagi xususiyatlarga ega:

1. Entropiya haqiqiy va manfiy bo'lmagan kattalik. Chunki, har qanday i ($1 \leq i \leq N$) uchun p_i 0 dan 1 gacha oraliqda o'zgaradi, ya'ni $\log_2 p_i$ manfiy va, demak, $-p_i \log_2 p_i$ musbat.

2. p_i lardan biri birga teng, qolganlari nolga teng bo'lganida entropiya nolga teng. Bu vaziyat manbaning holati to'la aniqlanganiga mos keladi.

3. Barcha ehtimolliklar bir-biriga teng bo'lganida entropiya eng katta qiymatga ega bo'ladi, ya'ni

$$4. \quad H_{max} = -\log_2 1/q = \log_2 q$$

5. Bir necha statistik bog‘lanmagan informatsiya manbalarining birlashma entropiyasi dastlabki manbalar entropiyalarining yig‘indisiga teng.

Umumiy holda, axborot miqdorini tajriba natijasida entropiyaning kamayishi deb hisoblash mumkin. Agar noaniqlik butunlay bartaraf etilsa, informatsiya miqdori entropiyaga teng bo‘ladi, ya’ni:

$$I = H$$

Agar noaniqlik qisman bartaraf etilsa, informatsiya miqdori boshlang‘ich va oxirgi entropiyalarning farqiga teng, ya’ni:

$$I = H_1 - H_2.$$

Ta’kidlash lozimki, agar barcha hodisalar teng ehtimollikka ega va statistik bog‘lanmagan bo‘lsa, Xartli va Shannon bo‘yicha informatsiya miqdori bir xil bo‘ladi.

Misol:

Alfavit A, B, C, D harflardan tashkil topgan. Harflarning paydo bo‘lish ehtimolliklari quyidagicha:

$$p_A = p_B = 0.25;$$

$$p_C = 0,34; p_D = 0.16$$

Ushbu alfavitdan tuzilgan xabar simvoliga to‘g‘ri keladigan informatsiya miqdori aniqlansin.

Yechish:

Alfavit simvollarining ehtimolliklari teng bo‘lmaganligi sababli entropiya quyidagicha aniqlanadi:

$$H = -\sum_{i=1}^q p_i (\log_2 p_i) = (2 \cdot 0,25 \log_2 0,25 + 0,34 \log_2 0,34 + 0,16 \log_2 0,16) = 2 \cdot 0,5 + 0,529174 + 0,423017 = 1,952191 \text{ bit/simvol.}$$

Nazorat savollari:

1. Ansambl nima?
2. Shannon formulasi bilan Xartli formulasining farqi nimada?
3. Entropiya xususiyatlarini sanab o‘ting.

2.2.1. Shartli entropiya va birlashma entropiya

Shartli entropiya informatsiya nazariyasida kodlanuvchi alfavit simvollarini orasidagi o'zaro bog'liqlikni aniqlashda, aloqa kanallari bo'yicha informatsiya uzatishdagi yo'qotishlarni aniqlashda va birlashma entropiyani hisoblashda ishlatiladi. Entropiyalarni jamlash qoidasiga muvofiq ikkita mazmun jihatidan turli (mustaqil) kitoblardagi informatsiya miqdori – alohida kitoblardagi informatsiya miqdorlarining yig'indisiga teng. Agar bir kitob ikkinchi kitobning qismini o'z ichiga olsa, ushbu ikki kitobdagi informatsiya miqdori alohida kitoblardagi informatsiya miqdorlarining yig'indisiga teng bo'lmaydi, balki undan kam bo'ladi. Bu holda informatsiya miqdorini o'lchashda *shartli entropiya* tushunchasidan foydalaniladi. Shartli entropiyani hisoblashda *shartli ehtimolliklar* u yoki bu ko'rinishda ishlatiladi.

Agar n ta xabar uzatilganida A simvoli m marta, B simvoli l marta, A simvoli B simvoli bilan birgalikda k marta paydo bo'lgan bo'lsa, A simvolning paydo bo'lish ehtimolligi:

$$P(A) = \frac{m}{n}$$

B simvolning paydo bo'lish ehtimolligi:

$$P(B) = \frac{l}{n}$$

A va B simvollarning birgalikda paydo bo'lish ehtimolligi:

$$P(AB) = \frac{k}{n}$$

B simvolga nisbatan A simvolning paydo bo'lishining shartli ehtimolligi:

$$P(A/B) = \frac{P(AB)}{P(B)} = \frac{k}{n} \cdot \frac{n}{l} = \frac{k}{l}$$

A simvolga nisbatan B simvolning paydo bo'lishining shartli ehtimolligi:

$$P(B/A) = \frac{P(AB)}{P(A)} = \frac{k}{n} \cdot \frac{n}{m} = \frac{k}{m}$$

Ushbu ifodalardan foydalanib A va B simvollarning birgalikda paydo bo'lish ehtimolligini aniqlash mumkin.

$$P(AB) = P(B)P(A/B) = P(A)P(B/A)$$

Ehtimolliklar shartli bo'lgani sababli, *shartli entropiya* quyidagicha yoziladi:

$$H(b_j/a_i) = - \sum_j p(b_j/a_i) \log_2 p(b_j/a_i)$$

$$H(a_i/b_j) = - \sum_i p(a_i/b_j) \log_2 p(a_i/b_j)$$

Bu yerda i indeks A xabar manbaining ixtiyoriy holatini tavsiflash uchun, j indeksi B adresatning ixtiyoriy holatini tavsiflash uchun tanlangan.

Birlashma entropiya. Birlashma entropiya statistik bog'langan xabarlarining birgalikda paydo bo'lish entropiyasini hisoblashda ishlatiladi.

Masalan, xalalli aloqa kanali bo'yicha 5 raqamini yuz marta uzatish natijasida 5 raqami 90 marta, 6 raqami 8 marta, 4 raqami 2 marta qabul qilindi. 5 raqami uzatilganida 5-4, 5-5, 5-6 kombinatsiyalarning paydo bo'lishining noaniqligini birlashma entropiya yordamida tavsiflash mumkin.

$H(A, B)$ – A simvol uzatilganida B simvol qabul qilinishining noaniqligi.

Uzatilgan A xabarlarining va qabul qilingan B xabarlarining ansambllari uchun birlashma entropiya quyidagi yig'indi ko'rinishiga ega:

$$H(A, B) = - \sum_i \sum_j p(a_i, b_j) \log_2 p(a_i, b_j) \text{ bit/ikkita simvol};$$

Birlashma entropiya va shartli entropiya o'zaro quyidagi munosabat orqali bog'langan.

$$H(A, B) = H(A) + H(B/A) = H(B) + H(A/B),$$

$$H(B/A) = H(A, B) - H(A); \quad H(A/B) = H(A, B) - H(B).$$

Misol:

Tajribadan ma'lum bo'ldiki, uzunligi 5 ta simvoldan iborat har bir 100 ta xabar uzatilganida A simvol 50 marta, B simvol 30 marta, B simvoli A simvoli bilan birgalikda 10 marta uchraydi. $H(A/B)$ va $H(B/A)$ shartli entropiyalar aniqlansin.

Yechish:

Uzatilgan simvollarning umumiy soni:

$$n = 100 \cdot 5 = 500.$$

A simvolning paydo bo'lish ehtimolligi:

$$P(A) = \frac{50}{500} = 0,1$$

B simvolning paydo bo'lish ehtimolligi:

$$P(B) = \frac{30}{500} = 0,06$$

A va B simvollarning birgalikda paydo bo'lish ehtimolligi:

$$P(AB) = \frac{10}{500} = 0.02$$

B simvolga nisbatan A simvolning paydo bo'lishining shartli ehtimolligi:

$$P(A/B) = \frac{P(AB)}{P(B)} = \frac{0.02}{0.06} = 0.33$$

A simvolga nisbatan B simvolning paydo bo'lishining shartli ehtimolligi:

$$P(B/A) = \frac{P(AB)}{P(A)} = \frac{0.02}{0.1} = 0.2$$

B simvolga nisbatan A simvolning shartli entropiyasi:

$$H(A, B) = - \sum_j p(b_j/a_j) \log_2 p(b_j/a_j) = -\{p(A/B) \log_2 p(A/B) + [1 - p(A/B)] \log_2 [1 - p(A/B)]\} = -(0.33 \log_2 0.33 + 0.67 \log_2 0.67) = 0.9149 \text{ bit/simvol};$$

A simvolga nisbatan B simvolning shartli entropiyasi:

$$H(B/A) = -(0.2 \log_2 0.2 + 0.8 \log_2 0.8) = 0.7219 \text{ bit/simvol}$$

Nazorat savollari:

1. Shartli ehtimollikning ehtimollikdan qanday farqi bor?
2. Shartli entropiya nima?
3. Birlashma entropiya qachon ishlatiladi?

2.2.2. Nisbiy entropiya va xabarlarning ortiqchaligi

Tatbiq nuqtai nazaridan informatsiya miqdorini baholash, asosan, tejamli kodlarni qurish, aloqa kanallari xususiyatlarini va ularning o'tkazish qobiliyatini baholash, kodlarning ortiqchaligini va ularning xalallarga bardoshligini aniqlash

uchun zarur hisoblanadi.

Masalan, aloqa kanallarini tahlilashda holatlari to'plami ma'lum elementlar yordamida uzatilishi mumkin bo'lgan informatsiyaning maksimal miqdorini aniqlashni bilish zarur. Xabar elementiga to'g'ri keluvchi informatsiyaning maksimal miqdorini faqat holatlarning teng ehtimolligi va mustaqilligida olish mumkin.

Entropiyasi maksimal qiymatga ($H_{max} = \log_2 q$) teng bo'lgan xabarlar uzatiladigan informatsiyaning maksimal miqdori jihatidan optimal xabarlar hisoblanadi. Real xabarlar kamdan – kam bu shartni qanoatlantiradi. Shu sababli, real xabarlarning har bir elementiga ular uzatishi mumkin bo'lganidan kam informatsiya yuklamasi to'g'ri keladi. Bunday xabarlarning entropiyasi maksimaldan kam bo'ladi.

Agar xabar elementi *to'la yuklanmagan* bo'lsa, xabarning o'zi informatsiya ortiqchaligi xususiyatiga ega hisoblanadi.

Informatsiya nazariyasida ortiqchalik *ortiqcha* informatsiya miqdorini ko'rsatadi. Bu informatsiya miqdori elementlar holati to'plamining strukturasi orqali aniqlanadi va odatda, statistik ma'lumotlardan oldindan ma'lum bo'ladi. Xabarlar manbaining entropiyasi sifat alomatlarining berilgan soniga ega bo'lgan alfavit uchun maksimal entropiyaga teng bo'lmasligi ushbu manbaa xabarlarning ko'p sonli informatsiyani eltishi mumkinligini anglatadi.

Bunday manba xabarlarning simvoliga to'g'ri keluvchi absolyut yuklanmaganlik:

$$\Delta D = (H_{max} - H) \text{ bit/simvol}$$

Informatsion ortiqchalik. Alfavit strukturasiidagi *ortiqcha* informatsiya miqdorini aniqlash uchun *ortiqchalik* tushunchasi kiritilgan. *Informatsion ortiqchalik* o'lchamsiz kattalik bo'lib, alfavit simvoliga to'g'ri keladigan *nisbiy* ortiqchalikni ifodalaydi.

$$\Delta = \frac{H_{max} - H}{H_{max}} = 1 - \frac{H}{H_{max}}$$

bu yerda $\frac{H}{H_{max}} = \mu$ – zichlash koeffitsienti (nisbiy entropiya).

Xabardagi simvollar paydo bo'lish ehtimolliklari teng bo'lmagan holda, ortiqchalik:

$$\Delta_p = 1 - \left(\frac{-\sum_i p_i \log_2 p_i}{\log_2 q} \right)$$

Xabar simvollar orasidagi statistik bog'lanish tug'diruvchi ortiqchalik:

$$\Delta_s = 1 - \left(\frac{\sum_i \sum_j p(a_i) p(b_j/a_i) \log_2 p(b_j/a_i)}{-\sum_i p_i \log_2 p_i} \right)$$

To'liq informatsion ortiqchalik:

$$\Delta = \Delta_s + \Delta_p - \Delta_s \Delta_p$$

Ortiqchalik har doim ham nomaqbul hisoblanmaydi. Kodlarning xalallarga bardoshligini oshirish uchun ortiqchalik zarur va u sun'iy ravishda qo'shimcha simvollar ko'rinishida kiritiladi.

Informatsion ortiqchalik – odatda tabiiy hodisa bo'lib, birlamchi alfavitning aslida mavjud. Tuzatuvchi ortiqchalik sun'iy hodisa bo'lib, ikkilamchi alfavitdagi kodda mavjud. Ortiqchalikni kamaytirishning eng samarali usuli samarali kodlarni qurish.

Misol:

Xabarlar a, b, c, d alfavit vositasida tuzilgan. Matnlarda alfavit harflarining paydo bo'lishi ehtimolliklari quyidagicha:

$p_a = 0.2, p_b = 0.3, p_c = 0.4, p_d = 0.1$. Ushbu alfavit asosida tuzilgan xabarlar ortiqchaligi aniqlansin.

Yechish:

Ortiqchalik, $\Delta = 1 - \frac{H}{H_{max}}$

To'rtta harfli alfavit uchun maksimal entropiya:

$$H_{max} = \log_2 q = \log_2 4 = 2 \text{ bit/simvol}$$

Xabar simvoliga to'g'ri keladigan o'rtacha entropiya

$$H = -\sum_i p_i \log_2 p_i = -(0.2 \log_2 0.2 + 0.3 \log_2 0.3 + 0.4 \log_2 0.4 + 0.1 \log_2 0.1) = 0.4644 + 0.5211 + 0.5288 + 0.3322 = 1.8465 \text{ bit/simvol}$$

Ortiqchalik

$$\Delta = 1 - \frac{1.8465 \text{ bit/simvol}}{2 \text{ bit/simvol}} = 1 - 0.9232 = 0.0768$$

Nazorat savollari:

1. Informatsiyaning maksimal miqdorini qachon olish mumkin?
2. Ortiqchalik iborasini tushuntiring.
3. Informatsion ortiqchalik nima?
4. Ortiqchalik doimo nomaqbulmi?

2.2.3. Informatsiyani uzatish tezligi va aloqa kanalining o'tkazish qobiliyati

Xalallar yo'qligi sharoitida *informatsiyani uzatish tezligi* vaqt birligida xabar simvoli eltadigan informatsiya miqdori orqali aniqlanadi.

$$C = n \cdot H,$$

bu yerda n – vaqt birligida xabarlar manbaida shakllanuvchi simvollar soni;

H – ushbu manbaada shakllangan xabarlarining bitta simvoli olinganida bartaraf etiluvchi entropiya(noaniqlik).

Ikkilik simvollar uchun informatsiyani uzatish tezligini quyidagicha ifodalash mumkin.

$$C = \frac{H}{\tau} \text{ bit/sek},$$

bu yerda τ – bitta ikkilik simvolni uzatish vaqti.

Informatsiyani uzatish tezligi doimo birlamchi alfavitga nisbatan aniqlanadi va faqat uning entropiyasiga bog'liq, signalni uzatish tezligi esa ikkilamchi alfavitga nisbatan aniqlanadi.

Demak, informatsiyani uzatish tezligi xabarlar manbaining informatsion xarakteristikalariga bog'liq, signallarni uzatish tezligi esa apparaturaning tezkorligiga bog'liq. Signallarni uzatish tezligi quyidagi ifoda bo'yicha hisoblanadi:

$$V = \frac{1}{\tau} \text{ simvol/sek},$$

bu yerda τ – ikkilamchi alfavitning bitta simvolini uzatish vaqti.

Ehtimolliklari teng, o'zaro bog'lanmagan davomlilik teng simvollardan

tuzilgan xabarlar uchun informatsiyani uzatish tezligi:

$$C = \frac{1}{\tau} \log_2 q \text{ bit/sek}$$

Ehtimolliklari teng bo'lmagan, davomlilikgi teng simvollar uchun informatsiyani uzatish tezligi:

$$C = -\frac{1}{\tau} \sum_{i=1}^q p_i \log_2 p_i \text{ bit/sek}$$

Ehtimolliklari teng bo'lmagan va o'zaro bog'langan davomlilikgi turli simvollar uchun informatsiyani uzatish tezligi:

$$C = \frac{\sum_i \sum_j p(a_i) p(b_j/a_i) \log_2 p(b_j/a_i)}{\sum_i \tau p_i}$$

Aloqa kanalining o'tkazish qobiliyati. Aloqa kanalining o'tkazish qobiliyati ushbu aloqa kanali bo'yicha informatsiyani uzatishning maksimal tezligi orqali aniqlanadi:

$$C_{max} = \frac{H_{max}}{\tau} \text{ bit/sek}$$

Ikkilik kod uchun

$$C_{max} = \frac{\log_2 2}{\tau} = \frac{1}{\tau} \text{ bit/sek}$$

Xalallar mavjudligida aloqa kanalining o'tkazish qobiliyati bir sekunda qabul qilingan simvollar sonini xabarlar manbai entropiyasidan xabarlar manbaining qabul qilingan signallarga nisbatan shartli entropiyasini ayirmasiga ko'paytirish sifatida hisoblanadi.

$$C_x = n[H(A) - H(A/B)] \text{ bit/sek}$$

yoki,

$$C_x = -n[\sum_i p_i \log_2 p_i + \sum_i \sum_j p(a_i) p(b_j/a_i) \log_2 p(b_j/a_i)] \text{ bit/sek}$$

Umumiy holda:

$$C_x = n[H(A) - H(A/B)] = n[H(B) - H(B/A)] = n[H(A) + H(B) - H(B,A)] \text{ bit/sek}$$

Misollar:

1). Xabar 5ta sifat alomatlaridan ($q = 5$) tuzilgan. Simvol davomlilikgi

$\tau = 20$ msek. Signallarni uzatish tezligi hamda informatsiyani uzatish tezligi aniqlansin.

Yechish:

Signallarni uzatish tezligi:

$$V = \frac{1}{\tau} = \frac{1}{0.02} = 50 \text{ simvol/sek}$$

Informatsiyani uzatish tezligi:

$$C = \frac{H}{\tau} = \frac{\log_2 q}{\tau} = \frac{\log_2 5}{0.02} = \frac{2.32}{0.02} = 116 \text{ simvol/sek}$$

2). Aloqa kanallari bo'yicha xabarlarini uzatishda to'rtta turli simvolli alfavitdan foydalanilgan. Barcha simvollarning davomligi $\tau = 1$ sek. Aloqa kanalining o'tkazish qobiliyati aniqlansin.

Yechish:

Aloqa kanalining o'tkazish qobiliyatini aniqlash uchun quyidagi formuladan foydalanamiz:

$$C = \frac{H_{max}}{\tau} \text{ bit/sek}$$

yoki,

$$S^* = \frac{\log_2 q}{\tau} \text{ bit/sek}$$

bu erda q –xabarlarning umumiy soni; τ – signalning o'rtacha davomligi.

Xabarlarini uzatish uchun to'rtta simvolli alfavit ishlatilganligi sababli,

$$q = 4^4$$

Barcha signallarning davomligi:

$$4\tau = 4 \text{ mc}$$

Demak,

$$C^* = 250 \log_2 4^4 = 250 \log_2 2^8 = 2 * 10^3 \text{ bit/sek}$$

Nazorat savollari:

1. Signalni uzatish tezligi nimaga bog'liq?
2. Informatsiyani uzatish tezligi nimaga bog'liq?
3. Xalallar yo'qligida aloqa kanalining o'tkazish qobiliyati qanday

aniqlanadi?

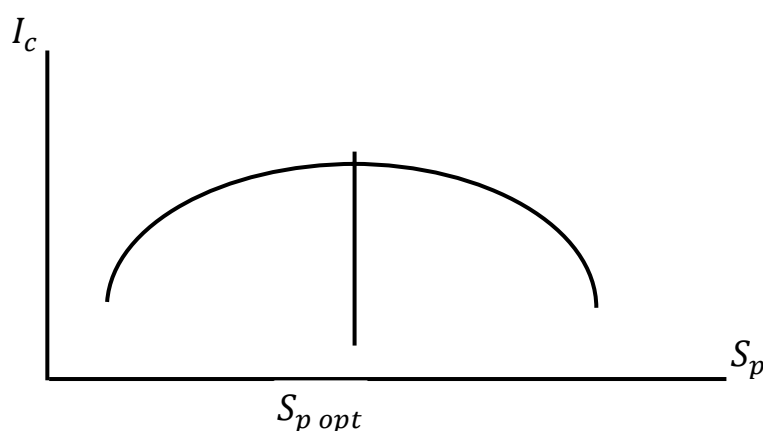
4. Xalallar mavjudligida aloqa kanalining o'tkazish qobiliyati qanday aniqlanadi?

2.3. Informatsiyaning semantik o'lchovi

Informatsiyaning ma'noli mazmunini, ya'ni uning semantik bosqichidagi miqdorini o'lchashda tezaurusli o'lchov keng tarqalgan. Bu o'lchov informatsiyaning semantik xususiyatlarini informatsiya olinishidagi foydalanuvchining qobiliyati bilan bog'laydi. Buning uchun *foydalanuvchining tezaurusi* tushunchasi ishlatiladi. *Tezaurus* – foydalanuvchi yoki sistema ixtiyoridagi ma'lumotlar majmui.

Foydalanuvchi qabul qiladigan va kelgusida o'zining tezaurusiga kiritadigan informatsiya miqdori I_c informatsiyaning ma'noli mazmuni S va foydalanuvchi tezaurusi S_p orasidagi o'zaro nisbatda o'zgaradi. Bu bog'liqlik tabiatini 2.2-rasmdagi egri chiziq yordamida ko'rsatish mumkin.

Foydalanuvchi semantik informatsiyaning maksimal miqdoriga informatsiyaning ma'noli mazmunini o'zining tezaurusi bilan muvofiqlashtirgan xolda ($S_p = S_{p\ opt}$) ega bo'ladi. Unda qabul qilingan informatsiya foydalanuvchiga tushunarli bo'ladi va unda oldin noma'lum bo'lgan (uning tezaurusida bo'lmagan) ma'lumotlarni beradi.



2.2-rasm. Foydalanuvchi qabul qiladigan semantik informatsiya miqdori bilan uning tezaurusi orasidagi bog'liqlik $I_c = f(S_p)$

Shunday qilib, foydalanuvchi qabul qiladigan ma'lumotlardagi semantik informatsiyaning miqdori, yangi bilimlar miqdori nisbiy kattalikdir. Bir xil ma'lumotlar bilimdon foydalanuvchi uchun ma'noli mazmunga ega bo'lsa, xabarsiz foydalanuvchi uchun ma'noga ega bo'lmaydi(semantik shovqin).

Semantik informatsiya miqdorining nisbiy o'lchovi sifatida semantik informatsiya miqdorining uning hajmiga nisbati orqali aniqlanuvchi mazmunli koeffitsienti C xizmat qilishi mumkin:

$$C = I_c/V_m$$

Ta'kidlash lozimki, informatsiyani semantik o'lchash muammolari uzatiluvchi informatsiya mazmunini formallashtirish bilan bog'liq. Ushbu muammolar juda murakkab, chunki informatsiyaning mazmuni qabul qiluvchiga, xabar semantikasiga nisbatan, ko'proq bog'liq.

Nazorat savollari:

1. Foydalanuvchining tezaurusi nima?
2. Semantik informatsiya miqdori.

2.4. Informatsiyani o'zgartirish

Har qanday sistemaga informatsiya signal ko'rinishida beriladi. Fizik jarayonlarning turli parametrlari datchiklar yordamida elektrik signallarga aylantiriladi. Odatda ushbu signallar uzluksiz o'zgaruvchi tok yoki kuchlanish bo'lishi mumkin.

Beriluvchi informatsiyani uzluksiz (analog) yoki diskret (raqamli) signallar ko'rinishida saqlash, uzatish va ishlash mumkin bo'lsada, hozirgi informatsion texnologiyaning rivojlanishi bosqichida diskret (raqamli) signallar afzal hisoblanadi. Shu sababli, analog signallar raqamli (diskret) shaklga keltiriladi.

Analog shakldagi signallarni raqamli shaklga keltirishda quyidagi uchta jarayonni ko'rsatish mumkin: diskretlash, kvantlash, kodlash. Ushbu jarayonlar mohiyatini ko'rib chiqamiz. Keyingi bayonlarda aniqlikni ta'minlash maqsadida

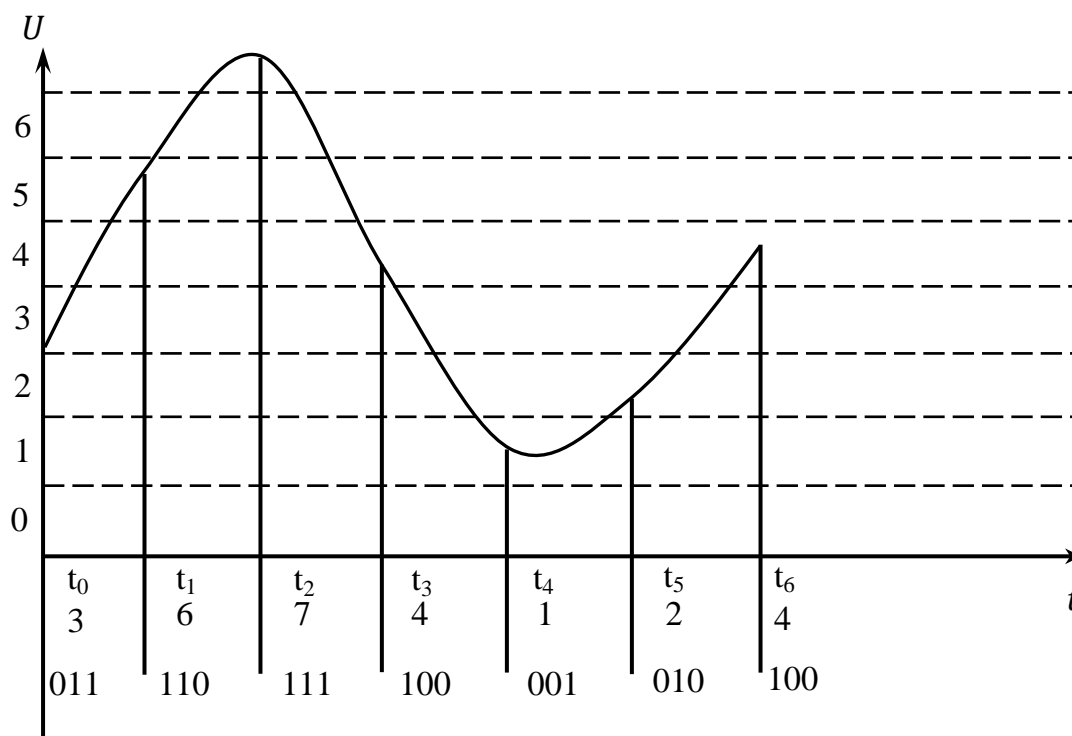
o'zgartirish qiymati bo'yicha uzluksiz o'zgaruvchi kuchlanish shaklida ifodalangan signallar ustida amalga oshiriladi deb hisoblaymiz.

Diskretlash. Diskretlash jarayoniga muvofiq vaqt bo'yicha uzluksiz signaldan uning alohida qiymatlari ma'lum vaqt intervali t oralab tanlab olinadi. (2.3-rasmda t_0, t_1, \dots, t_n onlar).

Interval t vaqt intervali, sanaladigan, onlar vaqtning takt onlari deb yuritiladi. Ravshanki, sanaladigan onlar qanchalik ko'p bo'lsa (diskretlash chastotasi yuqori bo'lsa) signal raqam ko'rinishida shunchalik aniq ifodalanadi.

Sanaladigan onlar kam bo'lsa (diskretlash chastotasi past bo'lsa) signal hususidagi axborot yo'qolishi mumkin.

Bu holat mashhur Naykvist – Kotelnikov mezonidan bevosita kelib chiqadi. Ushbu mezoniga muvofiq diskretlash chastotasi bo'lmaganda signal chastotasidan ikki marta katta bo'lishi lozim. Aks xolda signal xususidagi axborot yo'qoladi va signalni berilgan aniqlikda analog shakliga tiklab bo'lmaydi.



2.3-rasm. Diskretlash, kvantlash va kodlash jarayoni

Kvantlash. Kvantlashning mohiyati quyidagicha. Bir – biridan kvantlash qadami deb ataluvchi Δ kattalikka siljigan kvantlar to'ri hosil qilinadi (2.3-rasm).

Kvantlashning har bir sathiga tartib raqami (0, 1, 2, 3, 4 va h) berilishi mumkin. So'ngra diskretlash natijasida olingan dastlabki analog kuchlanish qiymatlari ularga yaqin kvantlash sathi bilan almashtiriladi.

Masalan, 2.3 – rasmdagi diagrammada t_0 onidagi kuchlanish qiymati unga yaqin 3 nomerli kvantlash sathi bilan almashtiriladi, t_1 onidagi kuchlanish qiymati 6-chi sathga yaqin va ushbu sath bilan almashtiriladi va h. Har qanday yaxlitlash kabi kvantlash jarayoni kuchlanishning diskret qiymatlarini ifodalashda xatolikka olib keladi, ya'ni kvantlash shovquni hosil bo'ladi. Analog-raqam o'zgartgichlarini loyihalashda kvantlash shovqinini pasaytirishga harakat qilinadi.

Kodlash. *Kodlashning* mohiyati quyidagicha: Kvantlash amali kuchlanish qiymatlarini sonlar – mos kvantlash sathlari nomerlari orqali ifodalashga imkon beradi. 2.3- rasmdagi diagramma uchun 3, 6, 7, 4, 1, 2,4 va h. sonlarning ketma-ketligi ikkilik kod orqali ifodalanadi.

Nazorat savollari:

1. Analog shakldagi signallarni raqamli shaklga keltirish qanday mezonga asoslanadi?
2. Diskretlash mohiyatini tushuntiring.
3. Kvantlash mohiyatini tushuntiring.
4. Kodlash mohiyatini tushuntiring.

3 BOB. KODLASH VA DEKODLASH

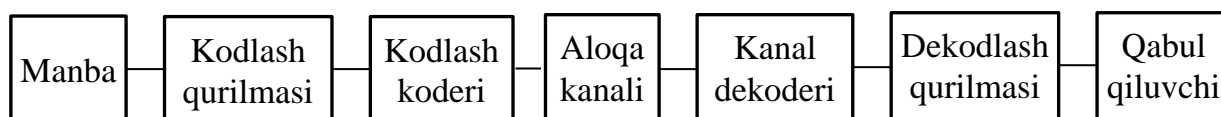
3.1. Kodlar, kodlash va dekodlash

Informatsiyani kodlash zaruriyati kompyuterlar paydo bo'lmasdan anchagina oldin vujudga kelgan. Texnikada kodlashga ehtiyoj telegraf paydo bo'lishi bilan vujudga kelgan bo'lsada, kompyuter ixtiro qilinganidan so'ng bunday ehtiyoj yanada ortdi.

Kodlash nazariyasining ta'sir sohasi real (yoki xalalli) kanallar bo'yicha ma'lumotlarni qamrab olsa, predmeti uzatilgan informatsiyaning korrektligini ta'minlash hisoblanadi. Boshqacha aytganda, kodlash nazariyasi signal uzatilganidan so'ng ma'lumotlardan ishonchli va osongina foydali informatsiyani ajratib olishga imkon beruvchi ma'lumotlarni qanday joylashtirish lozimligini o'rganadi. Ba'zida kodlash nazariyasini shifrlash bilan almashtirishadi, ammo bu noto'g'ri. Chunki kriptografiya teskari masalani yechadi. Uning maqsadi – ma'lumotlardan informatsiyani ajratib olishni qiyinlashtirish.

Kodlash – xabarni berilgan kanal bo'yicha uzatish uchun qulay holga keltirish. Oddiy misol tariqasida xabarni *telegramma* ko'rinishida uzatishni ko'rsatish mumkin. Bunda barcha simvollar telegraf kodida kodlanadi.

Dekodlash – qabul qilingan xabarni tiklash amali. Aloqa sistemasida kodlash va dekodlash uchun qurilmalar ko'zda tutilishi lozim (3.1-rasm).



3.1-rasm. Xalalli aloqa kanalining informatsion modeli

Bunday sistemalarni nazariy asoslash K.Shennon tomonidan amalga oshirilgan. U qator teoremlar orqali kodlash va dekodlash qurilmalarining kiritilishi lozimligini asosladi. Kodlash va dekodlash qurilmalarining vazifalari informatsiya manbai xususiyatlarini aloqa kanallari xususiyatlari bilan muvofiqlashtirishdir. Ularning biri (kodlash qurilmasi yoki koder) shunday kodlashni amalga oshirishi lozimki, natijada informatsiya ortiqchaligini bartaraf etish yo'li bilan xabar birligida simvollarning o'rtacha soni jiddiy kamaysin.

Bu esa o'z navbatida xalallar yo'qligida uzatishning vaqti yoki xotira qurilmasining hajmi bo'yicha yutuqqa ega bo'lishga imkon beradi. Bunday kodlash *samarali* deb ataladi, chunki u sistema samaradorligini oshiradi. Uzatish kanalida xalallar mavjudligida bunday kodlash kirish yo'li informatsiyasini uning keyinchalik ishlanishi masalasiga maqbul javob beruvchi ketma-ketlikka o'zgartirishga imkon beradi. Boshqa kodlash qurilmasi (kanal koderi) qo'shimcha

informatsiya ortiqchaligini kiritish yoʻli bilan informatsiyani uzatishda yoki saqlashda berilgan haqiqiylikni taʼminlaydi. Bunday kodlash *ortiqchali* yoki *xalallarga bardosh* kodlash deb yuritiladi.

Kodlar va kodlash nazariyasining asosiy tushunchalari. Kodlar maxfiy yozuv vositasi sifatida qadimdan maʼlum. Yunon tarixchisi Gerodot eramizdan avval V – asrda faqat adresatga tushunarli xatlarga misol keltirgan. Maxfiy *alfavit* Yuliy Sezar tomonidan ishlatilgan. Turli maxfiy shifrlarni yaratish ustida oʻrta asr olimlari F.Bekon, D.Kardano va boshqalar ishlashgan. Juda antiqa shifrlar va kodlar paydo boʻldi. Ammo vaqt oʻtishi bilan ular rasshifrovka qilindi va ularning maxfiyligi yoʻqoldi.

Aloqa kanallari boʻyicha xabarlarni uzatishga moʻljallangan birinchi kod S.Morze kodi hisoblanadi. Bu kodda harf va sonlarni kodlashga moʻljallangan simvollarining turli soni mavjud. Keyin telegrafiyada ishlatiluvchi N.Bodo kodi paydo boʻldiki, unda har bir harf va son simvollarining bir xil soniga ega. Simvollar sifatida berilgan onda elektr zanjiridagi impulsning borligi yoki yoʻqligini koʻrsatish mumkin.

Ikkita turli elementar signallarni ishlatuvchi kodlar *ikkilik kodlar* deb ataladi. Ushbu signallarni 0 va 1 simvollarini yordamida belgilash qulay hisoblanadi. Unda kod soʻzi nollar va birlar ketma-ketligidan iborat boʻladi. Informatsiyani kodlash masalasiga raqamli maʼlumotlarni qandaydir oʻzgartirish sifatida qarash mumkin. Xususiyl holda ushbu amal simvollarini guruhlash (triadalar yoki tetradalar koʻrinishida ifodalash) yoki pozitsion sanoq sistemasidagi simvollar (raqamlar) koʻrinishida ifodalashga keltirilishi mumkin. Har qanday pozitsion sistemada ortiqcha informatsiya boʻlmaganligi va barcha kombinatsiyalari ruxsat etilganligi sababli, bunday sistemalardan nazoratlashda foydalanish mumkin emas.

Sistematik kod – informatsion xonalaridan tashqari nazorat xonalari ega boʻlgan kod. Nazorat xonalari dastlabki son xususida qandaydir informatsiya yoziladi. Shu sababli sistematik kod ortiqchalikka ega. Bunday absolyut ortiqchalik nazorat xonalari soni m orqali, nisbiy ortiqchalik esa m/n nisbat orqali ifodalanadi. Bu yerda $n = m + k$ – kod soʻzidagi xonalarning umumiy soni,

k – informatsion xonalar soni.

Kodning tuzatish (korrektlash) qobiliyati tushunchasini odatda xatolarni aniqlash va tuzatish imkoniyati bilan bog‘lashadi. Miqdoran kodning tuzatish qobiliyati xatolikni aniqlash va tuzatish ehtimolligi orqali aniqlanadi. Ta’kidlash lozimki, asosiy e’tiborni yakka xatoliklarni aniqlash va tuzatishga qaratilishi lozimligi isbot qilingan. Kodning tuzatish qobiliyati kod masofasi tushunchasi bilan ham bog‘liq.

Kod kombinatsiyasining salmog‘i $V(A)$ – kod kombinatsiyasidagi birlar soni. A va B kod kombinatsiyalari uchun *kod masofasi* $d(A, B)$ dastlabki kombinatsiyalarni 2ning moduli asosida xonalar bo‘yicha jamlash orqali aniqlanuvchi uchinchi kombinatsiyaning salmog‘i sifatida aniqlanadi. Ushbu masofa ba’zida Xemming masofasi deb ham yuritiladi.

Misol:

$A = 011011100$ va $B = 100111001$ kombinatsiyalari uchun salmoq va kod masofasi aniqlansin.

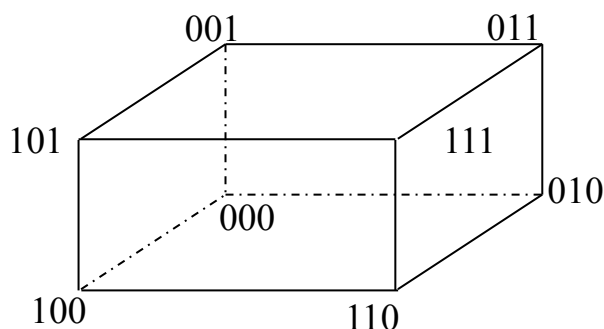
Yechish:

$$V(A) = 5; V(B) = 5.$$

$$\text{Uchinchi kod kombinatsiyasi } C = A \oplus B = 111100101.$$

$$\text{Demak } d(A, B) = 6.$$

Kodlarni qandaydir geometrik shakllar sifatida ko‘rish mumkin. Masalan, triadani ikkilik simvollarga mos keluvchi koordinata o‘qlariga ega bo‘lgan quyidagi birlik kub ko‘rinishida ifodalash mumkin.



3.1-rasm. Triadaning ikkili simvollarga mos keluvchi koordinata o‘qlariga ega bo‘lgan birlik kub ko‘rinishi

Bunda kod masofasi kubning mos uchlar orasidagi yoylar uzunligi yig'indisi orqali aniqlanadi (bitta yoy uzunligi 1 ga teng deb qabul qilingan). Ma'lum bo'lishicha, har qanday pozitsion sistemada minimal kod masofasi 1 ga teng.

Kodlash nazariyasiga muvofiq sistematik kod xatoliklarni faqat undagi minimal kod masofasi $2t$ dan katta yoki unga teng bo'lgandagina aniqlash imkoniyatiga ega, ya'ni: $d_{min} \geq 2t$,

bu yerda t – aniqlanuvchi xatolikning karraligi (yakka xatoliklar holida $t = 1$ va h). Demak, qo'shni ruxsat etilgan kod so'zlari orasida bo'lmaganida bitta kod so'zi mavjud.

Nafaqat xatoliklarni aniqlash balki uni tuzatish (ya'ni xatolik joyini ko'rsatish) zaruriyati hollarida minimal kod oralig'i $d_{min} \geq 2t + 1$ ga teng bo'lishi lozim.

Nazorat savollari:

1. Xalalli aloqa kanalining informatsion modelini keltiring.
2. Sistematik kod nima?
3. Kod masofasi qanday aniqlanadi?
4. Kod salmog'i qanday aniqlanadi?
5. Xatoliklarni aniqlashga imkon beruvchi kod masofasi.
6. Xatoliklarni nafaqat aniqlash, balki tuzatishga imkon beruvchi kod masofasi.

3.2. Samarali kodlarni qurishning Shannon-Fano algoritmi

Xalalsiz kanallar uchun *Shannon teoremasiga* binoan qandaydir alfavitning harflaridan tuzilgan xabarlarni shunday kodlash mumkinki, bitta harfga to'g'ri keladigan ikkilik simvollarning o'rtacha soni ushbu xabarlar manbai entropiyasiga yaqin bo'ladi, ammo undan kam bo'lmaydi.

Bunday kodlar quyidagi shartni qanoatlantirsa maksimal samarali

hisoblanadi.

$$N_{o'rt.} = H,$$

ikkilik kodlar uchun

$$\sum_i p_i(A_i) \cdot n = - \sum_i p_i \log_2 p_i$$

Teorema kodlashning muayyan usuliga ishora qilmaydi, ammo kod kombinatsiyasining har bir simvolini tanlaganda uning maksimal informatsiyani eltishini ta'minlashga harakat qilishi zarur. Demak, har bir simvol iloji boricha teng ehtimollik bilan 0 va 1 qiymatlarni olishi va har bir tanlov oldingi simvollar qiymatlariga bog'liq bo'lmasligi lozim.

O'zaro statistik bog'lanmagan xabarlar alfaviti harflari uchun samarali kodlarni qurish usullari ilk bor amerika olimlari Shennon va Fano tomonidan taklif etilgan. Ularning usullari, jiddiy farqlanmaganligi tufayli, mos kod *Shennon-Fano kodi* nomini olgan.

Shennon-Fano algoritmgiga binoan samarali kodni qurish quyidagicha amalga oshiriladi:

- xabar alfavitining harflari ehtimolliklarining pasayishi tartibida joylashtiriladi;
- barcha kodlanuvchi xabar harflari ikkita guruhga shunday ajratiladiki, ikkala guruhdagi harflar ehtimolliklarining yig'indilari iloji boricha teng bo'lsin. Agar tenglikka erishib bo'lmasa, yig'indi orasidagi tafovut minimal bo'lsin;
- yuqori guruhga 0 simvoli, pastki guruhga 1 simvoli beriladi;
- hosil bo'lgan qism guruhlar o'z navbatida ikki qismga shunday ajratiladiki, yangidan hosil bo'lgan qism guruhlardagi harflar ehtimolliklarining yig'indilari iloji boricha teng bo'lsin va h.;
- jarayon har bir qism guruhda bitta harf qolgunicha takrorlanadi.

Misol:

Alfavitdagi harflarning paydo bo'lish ehtimolliklari:

$p(A_1)=0,25;$	$p(A_2)=0,25;$	$p(A_3)=0,125;$	$p(A_4)=0,125;$
$p(A_5)=0,0625;$	$p(A_6)=0,0625;$	$p(A_7)=0,0625;$	$p(A_8)=0,0625$

bo‘lgan xabarning samarali notekis kodi qurilsin.

Yechish:

Kod qurilishining natijasi quyidagi jadvalda aks ettirilgan.

Harflar	Ehtimolliklar	Harflarni guruhlariga ketma-ket ajratish				Kod so‘zlar	$p_i(A_i) \cdot n$	
		1	2	3	4			
A ₁	0.25	}	}			00	0.5	
A ₂	0.25		}			01	0.5	
A ₃	0.125	}	}			100	0.375	
A ₄	0.125					101	0.375	
A ₅	0.0625		}	}	}	}	1100	0.25
A ₆	0.0625							
A ₇	0.0625	}		}	}	}	1110	0.25
A ₈	0.0625							

Shunday qilib, quyidagi kodlar hosil qilindi:

A ₁ =00;	A ₂ =01;	A ₃ =100;	A ₄ =101;
A ₅ =1100;	A ₆ =1101;	A ₇ =1110;	A ₈ =1111

Harflar ehtimolliklari ikkining butun sonli manfiy darajasi bo‘lganligi sababli kodlashda ortiqchalik to‘laligicha bartaraf etiladi. Undan tashqari ushbu kodlar maksimal samarali notekis kodlardir. Bunga ishonch hosil qilish uchun entropiyani va kod kombinatsiyalarining o‘rtacha uzunligini hisoblaymiz.

$$H = - \sum_{i=1}^8 p_i \log_2 p_i = 2 \cdot 0.25 \log_2 0.25 + 2 \cdot 0.125 \log_2 0.125 + 4 \cdot 0.0625 \log_2 0.0625 = 1 + 2 \cdot 0.375 + 4 \cdot 0.25 = 2.75 \text{ bit/simvol}$$

$$N_{o'rt.} = \sum_i p_i(A_i) \cdot n = 2 \cdot 0.5 + 2 \cdot 0.375 + 4 \cdot 0.25 = 2.75$$

Sakkizta simvollarni uzunligi o‘zgarmas kod orqali kodlashda uchta ikkilik xona kerakligi hisobga olinsa, bitta simvolga o‘rtacha 0,25 ikkilik xona tejalganligini ko‘rish mumkin.

Nazorat savollari:

1. Shannon-Fano algoritmini so‘zlab bering.
2. Qanday kodlarga samarali notekis kodlar deyiladi?
3. Samarali notekis kodlarning maksimal samarali bo‘lishi shartini keltiring.

3.3. Samarali kodlarni qurishning Xaffmen algoritmi

Shannon Fano usuli doimo bir ma’noli kod qurishga imkon bermaydi, chunki qismguruxlarga ajratishda ehtimolligi bo‘yicha yuqoridagi yoki pastki qismguruxni katta deb hisoblash mumkin. Bunday kamchilik Xaffmen usulida yo‘q.

Xaffmen algoritmi bo‘yicha samarali notekis kodni qurish quyidagicha amalga oshiriladi:

- xabarlar alfavitining harflari asosiy ustunga ehtimolliklarining pasayishi tartibida joylashtiriladi;
- ikkita oxirgi harf bitta yordamchi harfga birlashtirilib, unga yig‘indi ehtimollik yoziladi;
- birlashtirishda ishtirok etmagan harflar ehtimolliklari hosil qilingan yig‘indi ehtimolligi bilan birga ehtimolliklarining pasayishi tartibida yordamchi ustunga yoziladi va ohirgi ikkitasi birlashtiriladi va h;
- jarayon yig‘indi ehtimolligi 1 ga teng bo‘lgan yagona yordamchi harf hosil qilinmaguncha davom etadi.

Misol:

Alfavitdagi harflarning paydo bo‘lish ehtimolliklari:

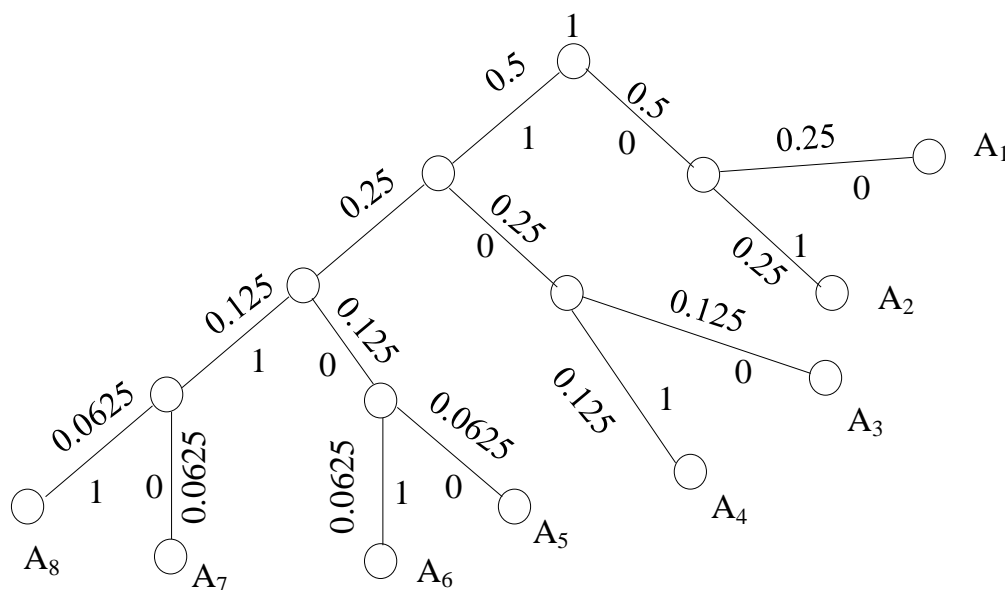
$p(A_1)=0,25;$	$p(A_2)=0,25;$	$p(A_3)=0,125;$	$p(A_4)=0,125;$
$p(A_5)=0,0625;$	$p(A_6)=0,0625;$	$p(A_7)=0,0625;$	$p(A_8)=0,0625$

bo‘lgan xabarning samarali notekis kodi qurilsin.

Yechish: Kodlash jarayonini quyidagi jadval yordamida tushuntirish mumkin.

Harflar	Ehtimolliklar	Yordamchi ustunlar						
		1	2	3	4	5	6	7
A ₁	0.25	0.25	0.25	0.25	0.25	0.5	0.5	1
A ₂	0.25	0.25	0.25	0.25	0.25	0.25	0.5	
A ₃	0.125	0.125	0.125	0.25	0.25	0.25		
A ₄	0.125	0.125	0.125	0.125	0.25			
A ₅	0.0625	0.125	0.125	0.125				
A ₆	0.0625	0.0625	0.125					
A ₇	0.0625	0.0625						
A ₈	0.0625							

Berilgan xabarga mos kod kombinatsiyasini aniqlash uchun harfning jadval qatori va ustuni bo'yicha o'tish yo'lini kuzatish zarur.



Ko'zga tashlanuvchanlikni ta'minlash maqsadida kod daraxti quriladi. Ehtimolligi birga mos nuqtadan ikkita shox yo'naltirilib, ehtimolligi katta shoxga 1 simvoli, ehtimolligi kichik shoxga 0 simvoli beriladi. Bunday ketma – ket shoxlash har bir harf ehtimollikiga yetguncha davom ettiriladi.

Kod daraxti bo'yicha yuqoridan pastga qarab harakatlanib, har bir harf uchun unga mos kod kombinatsiyasini yozish mumkin.

A_1	A_2	A_3	A_4	A_5	A_6	A_7	A_8
00	01	100	101	1100	1101	1110	1111

Hosil qilingan kodlardan ko‘rinib turibdiki, ular Shennon-Fano usuli bo‘yicha shakllangan kodlarga mos. Demak, Shennon-Fano va Xaffmen usullari bil xil samaradorlikka ega.

Nazorat savollari:

1. Xaffmen algoritmini so‘zlab bering.
2. Xaffmen algoritmining Shennon-Fano algoritmidan farqi nimada?
3. Kod daraxti qanday quriladi?

4 BOB. XALALLARGA BARDOSH KODLASH

4.1. Xalallarga bardosh kodlar

Xalalli kanallar uchun *Shennon teoremasiga* binoan simvollarni kodlashning mos usullarini tanlash yo‘li bilan kanaldagi xalallar ta’siridagi xatoliklar ehtimolligini pasaytirish mumkin. Teoremadan kanaldagi xalallarning informatsiyani uzatish aniqligiga emas, balki uzatish tezligiga cheklovlar qo‘yilishi xulosasi kelib chiqadi.

Ammo, Shennon teoremasida xalallarga bardosh kodlarning qanday qurilishi lozimligi aytilmaydi. Bu savolga xalallarga bardosh kodlash nazariyasi javob beradi. Xalallarga bardosh yoki tuzatuvchi (korrektlovchi) kodlar deganda uzatish jarayonida xalallar ta’sirida paydo bo‘luvchi xatoliklarni aniqlovchi va tuzatuvchi kodlar tushuniladi.

Bunda kodlash shunday amalga oshirilishi zarurki, qabul qilingan simvollar ketma-ketligiga mos signal (unga kanalda bo‘lishi mumkin bo‘lgan xalallar ta’siridan so‘ng) uzatilgan simvollar ketma-ketligiga mos signalga yaqin bo‘lishi shart. Bunga kodlashda ortiqchalikni kiritish evaziga erishiladi. Ortiqchalik

uzatiluvchi simvollar ketma-ketligini shunday tanlashga imkon beradiki, qabul qiluvchi tarafda xatoliklarni aniqlashga va tuzatishga imkon beruvchi qo‘shimcha shartlar qanoatlantiriladi.

Hozirda mavjud xalallarga bardosh kodlarning aksariyatida qo‘shimcha shartlar ularning algebraik strukturalarining natijasi hisoblanadi. Shu sababli ular *algebraik kodlar* deb yuritiladi.

Ajraluvchi va ajralmaydigan blok kodlar farqlanadi.

Ajraluvchi kodlar yordamida kodlashda chiqish yo‘li ketma-ketligi vazifalari aniq chegaralangan simvollardan tashkil topadi. Bu kanal koderi kirish yo‘liga beriluvchi simvollar ketma-ketligi bilan bir xil bo‘lgan informatsion simvollar hamda xatoliklarni aniqlashga va tuzatishga xizmat qiluvchi dastlabki ketma-ketlikka kiritiluvchi ortiqcha (tekshiruvchi) simvollar.

Ajralmaydigan kodlar yordamida kodlashda chiqish yo‘li ketma-ketligining simvollarini informatsion va tekshiruvchilarga ajratish mumkin emas.

Ajraluvchi blok kodlarning eng katta sinfini sistematik yoki chiziqli blok kodlar tashkil etadi. Bunday kodlarda tekshiruvchi simvollar ma’lum informatsion simvollar ustida chiziqli amallar bajarilishi natijasida aniqlanadi. Ikkilik kod uchun har bir tekshiruvchi simvol shunday tanlanadiki, uning ma’lum informatsion simvollar bilan 2ning moduli bo‘yicha yig‘indisi nolga teng bo‘lsin.

Dekodlash simvollarining ma’lum guruhini juftlikka tekshirishga keltiriladi. Shu sababli bunday kodlar *juftlikka tekshirishli kodlar* nomini olgan.

Uzluksiz(rekurrent, o‘raluvchi) kodlarda kodlanuvchi informatsion simvollar ketma-ketligiga ortiqcha simvollarini kiritish uzluksiz ravishda, uni bloklarga ajratmasdan amalga oshiriladi. Uzluksiz kodlar ham ajraluvchi va ajralmaydigan bo‘lishi mumkin. Ushbu kodlar texnik amalga oshirilishi nuqtai nazaridan eng sodda hisoblanadi.

Asosiy tushunchalar. Ma’lumki, ikkilik kod-asosi $q = 2$ bo‘lgan kod. Kod kombinatsiyasidagi xonalar soni n kod uzunligi deb yuritiladi. Ixtiyoriy ikkita kod kombinatsiyasining bir-biridan farqi d kodlar orasidagi masofa orqali xarakterlanadi va ushbu kod kombinatsiyalarini 2ning moduli bo‘yicha

yig'indisining salmog'i sifatida aniqlanadi.

Xalallar ta'sirida xatolik kod kombinatsiyasining faqat bitta xonasida sodir bo'lsa, bunday xatolik *bir karrali* deb ataladi. Ikki, uch va h. xonalarda xatolik bo'lsa, bunday xatolik mos holda *ikki karrali*, *uch karrali* va h. deb ataladi.

Kod kombinatsiyasidagi buzilgan simvollar joyini ko'rsatishda *xatolik vektori* tushunchasidan foydalaniladi. n xonali kodning xatolik vektori – n xonali kombinatsiya bo'lib, undagi birlar kod kombinatsiyasidagi buzilgan simvollar o'rnini ko'rsatadi.

Xatolik vektorining salmog'i xatolik karraligini xarakterlaydi. Buzilgan kod kombinatsiyasi va xatolik vektorining 2ning moduli bo'yicha yig'indisi dastlabki buzilmagan kod kombinatsiyasini beradi.

Yuqorida aytib o'tilganidek, ikkita ixtiyoriy kod kombinatsiyalarining farqini aniqlashda kodlar orasidagi masofa xarakteristikasidan foydalaniladi.

Ikkita ruxsat etilgan kod kombinatsiyalari orasidagi eng kichik masofa minimal kod masofasi deb ataladi va kodning bu xarakteristikasi uning tuzatish qobiliyatini belgilaydi.

Kodlash nazariyasida sistematik kodlar(informatsion xonalardan tashqari nazorat xonalari ega kodlar) minimal kod masofasi $2t$ ga teng yoki undan katta bo'lgandagina xatoliklarni aniqlay olishi isbot qilingan, ya'ni

$$d_{min} \geq t + 1$$

bu yerda t – aniqlanuvchi xatoliklarning karraligi (yakka xatoliklarda $t = 1$ va h.).

Nafaqat xatoliklarni aniqlash, balki uni tuzatish (xatolik o'rnini ko'rsatish) talab qilinganida minimal kod masofasi quyidagicha bo'lishi shart.

$$d_{min} \geq 2t + 1$$

Misol:

1100 kod kombinatsiyasi uzatilgan, xatolik vektorining salmog'i $V_{\bar{e}} = 2$.

– buzilgan kod kombinatsiyalarining bo'lishi mumkin bo'lgan variantlari aniqlansin;

- barcha xatoliklarni aniqlashga zarur kod masofasi aniqlansin.

Yechish:

1) Buzilgan kombinatsiyalar dastlabki kombinatsiyani xatolik vektoriga 2ning moduli bo'yicha jamlash orqali aniqlanadi.

$V_{\bar{e}} = 2$ da xatolik vektorining quyidagi variantlari bo'lishi mumkin:

$\bar{e} = 0011; 0101; 1001; 0110; 1010; 1100.$

Demak, buzilgan kombinatsiya variantlari quyidagicha:

1111; 1001; 0101; 1010; 0110; 0000.

2) $V_{\bar{e}} = 2$ da xatolik karraligi $t = 2$. Bunday xatoliklarni aniqlash uchun zarur minimal kod masofasi $d_{min} \geq t + 1 = 2 + 1 = 3$.

Nazorat savollari:

1. Qanday kodlar xalallarga bardosh kodlar deb ataladi?
2. Algebraik kodlar, blok kodlar, uzluksiz kodlar.
3. Juftlikka tekshirishli kodlar.
4. Ajraluvchi va ajralmaydigan blok kodlar.
5. Uzluksiz (rekurrent, o'raluvchi) kodlar.
6. Qanday kodlar texnik nuqtai nazaridan sodda hisoblanadi?
7. Kod uzunligi, kod kombinatsiyasining salmog'i, kodlar orasidagi masofa, xatolik vektori va uning salmog'i, xatolik karraligi, minimal kod masofasi tushunchalariga izoh bering.

4.2. Kodning tuzatish qobiliyati bilan kod masofasi orasidagi bog'liqlik

Aytaylik karraligi t va undan kichik barcha xatoliklarni aniqlovchi kodni qurish kerak bo'lsin.

Bunday kodni qurish uchun mumkin bo'lgan $N_0 = 2^n$ kombinatsiyalar to'plamidan ruxsat etilgan $N = 2^k$ kombinatsiyalarni shunday tanlab olish kerakki, ulardan ixtiyoriysining salmog'i $V_e < t$ bo'lgan ixtiyoriy xatoliklar vektori bilan 2ning moduli bo'yicha jamlanganda tanlangan ruxsat etilgan kombinatsiya olinsin.

Buning uchun qo‘yidagi shart qanoatlantirilishi lozim:

$$d_{min} \geq t + 1$$

Kod kombinatsiyasining tuzatuvchi sifatida ishlatilishi uchun taqiqlangan kod kombinatsiyalari bir-birini kesib o‘tmaydigan qismto‘plamlarga ajratiladi.

Qism to‘plamlarning har biriga ruxsat etilgan kombinatsiyalarining biri moslashtiriladi. Agar qabul qilingan taqiqlangan kombinatsiya qandaydir qismto‘plamga taalluqli bo‘lsa ushbu to‘plamga moslashtirilgan ruxsat etilgan kombinatsiya uzatilgan deb hisoblanadi va xatolik tuzatiladi.

Misol tariqasida uzunligi $n = 3$ bo‘lgan kodni ko‘raylik.

Bunday kodning bo‘lishi mumkin bo‘lgan kombinatsiyalari 4.1 jadvalda keltirilgan.

4.1-jadval

A_1	A_2	A_3	A_4	A_5	A_6	A_7	A_8
000	001	010	011	100	101	110	111

Kod kombinatsiyalari orasidagi masofa matritsasi 4.2-jadvalda keltirilgan.

4.2-jadval

	A_1	A_2	A_3	A_4	A_5	A_6	A_7	A_8
A_1	0	1	1	2	1	2	2	3
A_2		0	2	1	2	1	3	2
A_3			0	1	2	3	1	2
A_4				0	3	2	2	1
A_5					0	1	1	2
A_6						0	2	1
A_7							0	1
A_8								0

Kodning bir karrali xatoliklarni aniqlanishini ta'minlashi uchun bo'lishi mumkin bo'lgan kombinatsiyalar to'plami $N_0 = 8$ dan ruxsat etilganlari sifatida shundaylarini tanlab olish kerakki, ular orasidagi masofa $d = 2$ dan kam bo'lmasin. Masofalar matritsasidan ko'rinib turibdiki, ruxsat etilgan kombinatsiyalar sifatida quyidagilarni tanlash mumkin:

$$A_1 = 000; \quad A_4 = 011; \quad A_6 = 101; \quad A_7 = 110.$$

Ikki karrali xatoliklarni aniqlash uchun kod masofasi $d_{min} = 3$ bo'lishi lozim. Bunda ruxsat etilgan kombinatsiyalar sifatida quyidagilarni tanlash mumkin:

$$A_1 = 000; \quad A_8 = 111.$$

Quyidagi shartning to'g'riligi shubhasiz.

$$d \leq n$$

Demak, ushbu holda ikki karrali xatoliklar aniqlanishi mumkin emas, chunki bunday xatoliklar natijasida ruxsat etilgan kombinatsiyalarning o'zi bir-biriga $n = 3$ qiymatda o'tadi.

Aytaylik, bir karrali xatoliklarni bartaraf etuvchi kodni qurish kerak bo'lsin. Birinchi ruxsat etilgan kombinatsiya sifatida $A_1=000$ ni tanlaymiz. Bir karrali xatoliklar mavjudligida A_1 kombinatsiyasi $A_2=001$; $A_3=010$ va $A_5=100$ ruxsat etilmagan kombinatsiyalarining biriga o'tishi mumkin. A_2 , A_3 va A_5 kombinatsiyalarni A_1 kombinatsiyasining ruxsat etilmagan(taqiqlangan) qismto'plami sifatida qabul qilish mumkin. Yani, ushbu qismto'planning biror bir kombinatsiyasi qabul qilinsa, A_1 kombinatsiyasi uzatilgan deb xulosa qilinadi.

Ikkinchi ruxsat etilgan kombinatsiya sifatida birinchisidan $d = 2$ masofadagi $A_4=011$ kombinatsiyani tanlaymiz. Unga $A_2=001$ $A_3=010$ va $A_8=111$ kombinatsiyalar qismto'plami mos kelishi lozim. Ammo taqiqlangan qismto'plamlarining kesishishi sodir bo'ldiki, A_2 yoki A_3 taqiqlangan kombinatsiyalar qabul qilinganida A_1 signal uzatilganligini yoki A_4 signal uzatilganligini bir ma'noda aniqlash mumkin emas.

Agar ikkinchi ruxsat etilgan kombinatsiya sifatida birinchisidan $d = 3$ masofadagi $A_8=111$ tanlansa, bu kombinatsiyaga $A_4=011$; $A_6=101$ va $A_7=110$

taqiqlangan kombinatsiyalari qismto‘plami mos keladi. Bunda taqiqlangan qismto‘plamlari kesishmaydi. Demak, $d = 3$ da barcha bir karrali xatoliklar bartaraf etilishi ta’minlanadi.

Umumiy holda, σ karrali xatoliklarni bartaraf etish uchun kod masofasi quyidagi shartni qanoatlantirishi lozim:

$$d_{min} \geq 2\sigma + 1$$

Mulohazalar natijasida aniqlash mumkinki, karraligi σ dan katta bo‘lmagan barcha xatoliklarni tuzatish va bir vaqtda t dan ($t \geq \sigma$) katta bo‘lmagan barcha xatoliklarni aniqlash uchun kod masofasi quyidagi shartni qanoatlantirishi lozim:

$$d_{min} \geq t + \sigma + 1$$

Ta’kidlash lozimki, kod yordamida aniqlangan xatolik $t > \sigma$ karralikka ega bo‘lsa, bunday xatolik bartaraf etilishi mumkin emas, ya’ni bu holda kod xatolikni faqat aniqlaydi.

Misol:

Ruxsat etilgan kombinatsiyalari:

00000; 01110; 10101; 11011;

bo‘lgan kodning tuzatish qobiliyatini aniqlash talab etilsin.

Yechish:

Kodning tuzatish qobiliyati kod masofasi yordamida aniqlanadi. Kod kombinatsiyalari orasidagi masofalar matritsasini tuzamiz.

	00000	01110	10101	11011
00000	0	3	3	4
01110		0	4	3
10101			0	3
11011				0

Matritsadan ko‘rinib turibdiki, kod masofasi $d_{min} = 3$. Demak, berilgan kod quyidagilarga qodir:

1. Ikki karrali xatolikni aniqlash.

2. Bir karrali xatoliklarni bartaraf etish.
3. Bir karrali xatoliklarni aniqlash va bartaraf etish.

Nazorat savollari:

1. Kod kombinatsiyalari orasidagi masofa qanday aniqlanadi?
2. Masofa matritsasi qanday tuziladi?
3. Kodning tuzatish qobiliyati bilan kod masofasi orasida qanday bog‘liqlik mavjud?

4.3. Berilgan tuzatish qobiliyatli kodlarni qurish

Hozirgacha tuzatuvchi qobiliyatli kodlarni qurganda kod uzunligi n berilgan deb faraz qilgan edik. Kodning tuzatish qobiliyatiga n saqlangan holda ruxsat etilgan kombinatsiyalar to‘plami N ni (yoki informatsion simvollar k ni) kamaytirish evaziga erishilgan edi. Odatda esa kodni qurish teskari tartibda amalga oshiriladi: avval manbaa alfaviti hajmiga muvofiq informatsion simvollar soni k aniqlanadi, so‘ngra ortiqcha simvollarini qo‘shish evaziga kodning kerakli tuzatish qobiliyati ta’minlanadi.

Aytaylik, manbaa alfavitining hajmi N ma’lum. Informatsion simvollarining kerakli soni quyidagicha aniqlanadi:

$$k = \log_2 N;$$

Tuzatilishi lozim bo‘lgan xatolik vektorlarining soni E ham ma’lum bo‘lsin. Masala shundan iboratki, berilgan N va E da istalgan tuzatish qobiliyatiga ega kod uzunligi n aniqlansin.

Tuzatilishi lozim bo‘lgan xatolik kombinatsiyalarining to‘liq soni:

$$E \cdot 2^k = E \cdot N.$$

Xatolik kombinatsiyalarining soni $N_0 - N$ bo‘lganligi sababli, kod $N_0 - N$ dan katta bo‘lmagan kombinatsiyalarni tuzatishni ta’minlaydi.

$$NE \leq N_1 - N_0$$

yoki,

$$N_0 \geq (1 + E)N$$

yoki,

$$N \leq \frac{2^n}{1 + E}$$

Ushbu formula kod uzunligi n ni tanlash shartini ifodalaydi.

Xususiyl hollarni ko'raylik. Turli karrali xatoliklar mavjudligida avvalo paydo bo'lish ehtimolliklari eng katta bo'lgan bir karrali xatoliklarning bartaraf etilishini ta'minlash lozim. Bir karrali xatolik vektorlarining bo'lishi mumkin bo'lgan soni:

$$E = C_n^1 = n$$

Bu holda quyidagini yozish mumkin:

$$2^k = N \leq \frac{2^n}{1 + n}$$

Kodni qurishda 4.3-jadvaldan foydalanish maqsadga muvofiq hisoblanadi.

4.3-jadval

n	2	3	4	5	6	7	8	9
$\frac{2^n}{1+n}$	1.33	2	3.2	5.33	9.1	16	28.4	51.2

Ta'kidlash lozimki, kod quyidagi shartni qanoatlantirishi lozim.

$$d_{min} \geq 3$$

Karraligi 1 dan l gacha bo'lgan barcha xatoliklarning bartaraf etilishi kerak bo'lsa, quyidagilarni hisobga olish zarur:

- bo'lishi mumkin bo'lgan bir karrali xatoliklar soni $E_1 = C_n^1$
- bo'lishi mumkin bo'lgan ikki karrali xatoliklar soni $E_2 = C_n^2$

.....

- bo'lishi mumkin bo'lgan l karrali xatoliklar soni $E_l = C_n^l$

Xatoliklarning umumiy soni:

$$E = \sum_{i=1}^l C_n^i$$

Unda quyidagini yozish mumkin:

$$N = \frac{2^n}{1 + \sum_{i=1}^l C_n^i}$$

Misol:

Ruxsat etilgan kod kombinatsiyalari soni $N = 8$ bo'lganida barcha yakka xatoliklarni tuzatishni ta'minlovchi kod uzunligi n aniqlansin.

Yechish:

Hisoblash quyidagi formula yordamida amalga oshirilishi mumkin.

$$N \leq \frac{2^n}{1 + n}$$

Yuqorida keltirilgan jadvalga binoan

$$N = \frac{2^6}{1 + 6} = \frac{64}{7} \approx 9,1$$

Demak, kod uzunligi $n = 6$.

Nazorat sovellari:

1. Informatsion simvollarning kerakli soni qanday aniqlanadi?
2. Xatolikni tuzatish imkoniyati sharti qanday ifodalanadi?
3. Kod uzunligi n ni tanlash shartini keltiring.

5 BOB. CHIZIQLI BLOK KODLAR

5.1. Xemming kodi

Xemming kodi oddiy chiziqli blok kod bo'lib, minimal kod masofasi 3 ga teng, ya'ni bu kod bitta xatolikni tuzata oladi. Xemming kodi boshqa kodlarga o'xshab k informatsion va $(n - k)$ ortiqcha simvollarga ega. Kodning ortiqchalik qismi shunday quriladiki, dekodlash natijasida nafaqat qabul qilingan kombinatsiyadagi xatolik mavjudligini, balki xatolik sodir bo'lgan o'rin nomerini aniqlash mumkin bo'ladi. Bunga qabul qilingan kombinatsiyani ko'p marta juftlikka tekshirish evaziga erishiladi. Tekshirishlar soni ortiqcha simvollar soniga,

ya'ni $(n - k)$ ga teng. Har bir tekshirishda informatsion simvollarining bir qismi va ortiqcha simvoldan biri qatnashadi. Har bir tekshirishdan so'ng ikkilik nazorat simvoli olinadi. Tekshirish natijasi juft sonni bersa nazorat simvoliga 0 qiymati, toq sonni bersa 1 qiymati beriladi. Barcha tekshirishlar natijasida buzilgan simvollar o'rnining nomerini ko'rsatuvchi $(n - k)$ xonali ikkilik son olinadi.

Xatolikni tuzatish uchun faqat ushbu simvol qiymatini teskarisiga o'zgartirish kifoya.

Xemming kodining uzunligi:

$$2^k = \frac{2^n}{1 + n}$$

formula yordamida aniqlanadi.

Xemming usuliga binoan tekshiruvchi simvollar qiymati va o'rinlarining nomeri kod kombinatsiyasining tekshiruvchi guruhlarini tanlash bilan bir vaqtda belgilanadi. Bunda quydagilarga asoslanmoq lozim. Birinchi tekshirish natijasida buzilgan simvol o'rnini nomerini ko'rsatuvchi nazorat kodining kichik xonasi raqami olinadi. Agar birinchi tekshirish natijasi 1 ni bersa, demak tekshirilgan guruxning bitta simvoli buzilgan hisoblanadi. Simvoldan qaysi birining buzilganligini aniqlash uchun 5.1-jadvalga murojaat etamiz.

5.1-jadval

№ k/ k	Nazorat son simvollarining xonalari			
	4	3	2	1
0	0	0	0	0
1	0	0	0	1
2	0	0	1	0
3	0	0	1	1
4	0	1	0	0
5	0	1	0	1
6	0	1	1	0
7	0	1	1	1
8	1	0	0	0
9	1	0	0	1
10	1	0	1	0

Jadvalda to'rt xonali nazorat sonlarining natural qatori ikkilik sanoq sistemasida keltirilgan.

5.1-jadvaldan ko'rinib turibdiki, agar nazorat sonining kichik xonasida 1 bo'lsa, buzilish kod kombinatsiyasining toq o'rinlarida bo'ladi. Demak, birinchi tekshirish o'z ichiga toq nomerli simvollarni, ya'ni 1, 3, 5, 7, 9, . . . larni oladi.

Agar ikkinchi tekshirish natijasi 1 ni bersa, nazorat sonining ikkinchi xonasida 1 ni olamiz. Demak ikkinchi tekshirish o'z ichiga ikkinchi xonasida 1 bo'lgan simvollarni, ya'ni 2, 3, 6, 7, 10 . . . larni oladi.

Xuddi shunday, uchinchi tekshirish o'z ichiga uchinchi xonasida 1 bo'lgan simvollarni, ya'ni 4, 5, 6, 7, 12 . . . larni oladi va h.

Bu kabi mushohadalar tekshirish jadvalini shakllantirishga imkon beradi (5.2-jadval).

5.2-jadval

Tekshirish nomeri	Tekshiriluvchi o'rinlar nomeri	Nazorat simvollari o'rinlarining nomeri
1	1, 3, 5, 7, 9, 11, 13 . . .	1
2	2, 3, 6, 7, 10 . . .	2
3	4, 5, 6, 7, 12 . . .	4
4	8, 9, 10, 11, 12 . . .	8
.
.

Agar tekshiriluvchi kod kombinatsiyasining simvollarini a_i orqali, tekshiruvchi amallarni S_i orqali belgilasak, quyidagini yozish mumkin.

$$S_1 = a_1 \oplus a_3 \oplus a_5 \oplus a_7 \oplus a_9 \oplus \dots$$

$$S_2 = a_2 \oplus a_3 \oplus a_6 \oplus a_7 \oplus a_{10} \oplus \dots$$

$$S_3 = a_4 \oplus a_5 \oplus a_6 \oplus a_7 \oplus a_{12} \oplus \dots$$

$$S_4 = a_8 \oplus a_9 \oplus a_{10} \oplus a_{11} \oplus a_{12} \oplus \dots$$

Nazorat simvollarini tekshiriluvchi guruxlarning faqat bittasida uchraydigan nomerli o'rinlarda joylashtirish qulay hisoblanadi (5.2-jadvalga qaralsin). Jadvalga muvofiq bu o'rinlar nomeri 1, 2, 4, 8, . . . Demak, kod kombinatsiyasida $a_1, a_2, a_4, a_8 . . .$ simvollar tekshiruvchi, $a_3, a_5, a_6, a_7, a_9 . . .$ simvollar informatsion

hisoblanishlari lozim.

Informatsion simvollar qiymati oldindan ma'lum bo'lganligi sababli, tekshiruvchi simvollarning qiymati shunday bo'lishi lozimki, har bir tekshiruvchi guruxdagi birlarning yig'indisi juft son bo'lsin.

Misol:

10011 ikkili kombinatsiyaning Xemming kodini topish so'ralsin.

Yechish:

Informatsion simvollar soni $k = 5$.

$2^k \leq \frac{2^n}{1+n}$ formulaga binoan $32 \leq \frac{2^n}{1+n}$. Demak, Xemming kodining uzunligi $n = 9$. Informatsion simvol a_3, a_5, a_7, a_9 bo'lganligi sababli, ko'rilayotgan kod uchun quyidagini yozish mumkin.

$$a_3 = 1; a_5 = 0; a_6 = 0; a_7 = 1; a_9 = 1.$$

Tekshiruvchi simvollar qiymati yig'indilar juftligini ta'minlash shartiga binoan quyidagicha aniqlanadi.

$$S_1 = a_1 \oplus 1 \oplus 0 \oplus 1 \oplus 1 \quad a_1 = 1.$$

$$S_2 = a_2 \oplus 1 \oplus 0 \oplus 1 \quad a_2 = 0.$$

$$S_3 = a_4 \oplus 0 \oplus 0 \oplus 1 \quad a_4 = 1.$$

$$S_4 = a_8 \oplus 1 \quad a_8 = 1.$$

Demak, oddiy besh xonali kod 10011 ga quyidagi to'qqiz xonali Xemming kodi mos keladi.

1 0 1 1 0 0 1 1 1

Faraz qilaylik, uzatishda beshinchi simvolda xatolik ro'y berdi, ya'ni kod quyidagi ko'rinishni oldi.

1 0 1 1 1 0 1 1 1

Tekshirish quyidagicha amalga oshiriladi.

Birinchi tekshirish:

$$S_1 = 1 \oplus 1 \oplus 1 \oplus 1 \oplus 1; \quad 1.$$

Ikkinchi tekshirish:

$$S_2 = 0 \oplus 1 \oplus 0 \oplus 1; \quad 0.$$

Uchinchi tekshirish:

$$S_3 = 1 \oplus 1 \oplus 0 \oplus 1; \quad 1.$$

To'rtinchi tekshirish:

$$S_4 = 1 \oplus 1; \quad 0.$$

Shunday qilib, tekshirish natijasida 0101 ikkili son olindi. Demak, xatolik beshinchi simvolda sodir bo'lganligi isbotlandi.

Nazorat savollari:

1. Xemming kodi xalallarga bardosh kodlarning qaysi turiga mansub?
2. Xemming kodini qurish muolajasini so'zlab bering.
3. Xemming kodining minimal kod masofasi nimaga teng?

5.2. Siklik kodlar

Siklik kodlar ma'lum tuzatuvchi kodlar ichida eng sodda va samarador hisoblanadi. Ushbu kodlarning kodlovchi va dekodlovchi qurilmalari sifatida oddiy siljituvchi registrlar ishlatiladi. Siklik kodlarning asosiy xususiyati – har bir kod kombinatsiyasini ushbu kodga taalluqli kombinatsiya simvollari o'rnini siklik o'zgartirish yo'li bilan olish mumkinligi.

Boshqacha aytganda agar kod vektori $V = (a_0, a_1, a_2, \dots, a_{n-1})$ siklik kod V ga tegishli bo'lsa, kod vektoriga taalluqli kombinatsiya simvollari o'rnini siklik o'zgartirish yo'li bilan olingan vektor $V' = (a_{n-1}, a_0, a_1, a_2, \dots, a_{n-2})$ ham kod V ga tegishli bo'ladi.

Siklik kodlarni qandaydir darajali ko'phad ko'rinishida ifodalash qulay hisoblanadi, ya'ni:

$$G(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \dots + a_1x + a_0,$$

bu erda x – o'zgaruvchi; a_i – berilgan sanoq sistemasidagi raqamlar (ikkilik sistemada “0” va “1”).

Masalan, yetti xonali ikkilik kod 1010101 x o'zgaruvchining ko'phadi ko'rinishida quyidagicha yozilishi mumkin:

$$1010101 = G(x) = 1 \cdot x^6 + 0 \cdot x^5 + 1 \cdot x^4 + 0 \cdot x^3 + 1 \cdot x^2 + 0 \cdot x^1 + 1 \cdot x^0 \\ = x^6 + x^4 + x^2 + 1.$$

Kod kombinatsiyasining bunday ifodalanishi kombinatsiyalar ustida bajariladigan amallarni ko'phadlar ustida bajariladigan amallarga keltirish imkonini beradi. Bunday ikkilik ko'phadni qo'shish o'zgaruvchi x ning darajalari teng bo'lganida koeffitsientlarni 2ning moduli bo'yicha jamlashga keltiriladi. Ko'paytirish darajali funksiyalarni odatdagi ko'paytirish qoidalari bo'yicha amalga oshiriladi, ammo hosil qilingan koeffitsientlar 2ning moduli bo'yicha jamlanadi; bo'lish darajali funksiyalarni odatdagi bo'lish qoidalari bo'yicha amalga oshiriladi, ammo ayirish amallari 2ning moduli bo'yicha jamlash amallari bilan almashtiriladi.

Kombinatsiyalarni yuqorida keltirilgan shakllarda ifodalash yana shunisi bilan qulayki, siklik o'rin almashtirish berilgan ko'pxadni x ga oddiy ko'paytirish natijasi hisoblanadi.

Haqiqattan, agar kod kombinatsiyalarining biri ko'pxad $V(x) = a_0 + a_1x + a_2x^2 + \dots + a_{n-1}x^{n-1}$ orqali ifodalansa, yangi kombinatsiya siklik siljitish hisobiga

$$x \cdot V(x) = a_0x + a_1x^2 + a_2x^3 + \dots + a_{n-2}x^{n-1} + a_{n-1}x^n \text{ ko'rinish oladi.}$$

Oxirgi xadda x^n ni 1 bilan almashtirish zarur. Demak, yangi kombinatsiya

$$V'(x) = a_{n-1} + a_0x + a_1x^2 + \dots + a_{n-2}x^{n-1}$$

Yuqorida keltirilganlardan foydalanib siklik kodlarga quyidagicha ta'rif berish mumkin.

Siklik kod– $k - 1$ darajali $Q(x)$ ko'phad ko'rinishida ifodalangan oddiy k xonali kodni qandaydir $(n - k)$ darajali yasovchi ko'pxad $P(x)$ ga ko'paytirish yo'li bilan hosil bo'luvchi $(n - k)$ kod.

Oddiy $k - xonali$ kodning barcha kod kombinatsiyalarini yasovchi ko'phad $R(x)$ ga ko'paytirish natijasida ruxsat etilgan kombinatsiyalar soni o'zgarmaydi va 2^k ga tenglicha qoladi, taqiqlangan kod kombinatsiyalarining umumiy soni $2^n - 2^k$ ga teng bo'ladi. Taqiqlangan kod kombinatsiyasiga mos birorta ham

ko'phad yasovchi ko'phadga qoldiqsiz bo'linmaydi. Ushbu xususiyat xatolikni aniqlashga imkon beradi. Qoldik ko'rinishi bo'yicha xatolik vektorini ham aniqlash mumkin.

Siklik kodni qurish muolajasi. Siklik kodni qurish muolajasi quyidagicha. Oddiy k –xonali kod $G(x)$ ning kod kombinatsiyasi birhad x^{n-k} ga ko'paytiriladi, so'ngra darajasi $(n - k)$ bo'lgan yasovchi ko'phad $P(x)$ ga bo'linadi. Ko'paytirish natijasida $G(x)$ tarkibidagi har bir hadning darajasi $(n - k)$ ga ortadi. $x^{n-k} \cdot G(x)$ ko'paytmani yasovchi ko'phad $P(x)$ ga bo'lish natijasida darajasi $G(x)$ darajasiga teng bo'linma $Q(x)$ olinadi.

Ko'paytirish va bo'lish natijasini quyidagicha ifodalash mumkin:

$$\frac{x^{n-k} \cdot G(x)}{P(x)} = Q(x) + \frac{R(x)}{P(x)},$$

bu yerda $R(x)$ – bo'lish natijasidagi qoldiq.

Bo'linma $Q(x)$ ning darajasi oddiy kod kombinatsiyasi $G(x)$ ning darajasiga teng bo'lganligi sababli $Q(x)$ oddiy k –xonali kodning kod kombinatsiyasi hisoblanadi.

Yuqoridagi tenglikning ikki tarafini $P(x)$ ga ko'paytirib ba'zi o'rin almashtirishlarni bajarish natijasida quyidagini yozish mumkin.

$$F(x) = Q(x)P(x) = x^{n-k}G(x) + R(x)$$

Ushbu ifodaning o'ng tarafidagi $R(x)$ manfiy ishorasi musbat ishora bilan almashtirilgan, chunki 2 ning moduli bo'yicha ayirish jamlashga keltiriladi.

Aytaylik, informatsion simvollar soni $k = 4$ ga bo'lgan (0011), bir karrali xatoliklarni bartaraf etuvchi yoki ikki karrali xatoliklarni aniqlovchi siklik kodni qurish so'ralsin.

$N = 2^k \leq \frac{2^n}{1+n}$ munosabatdan foydalanib berilgan informatsion simvollar soni $k = 4$ bo'yicha kod uzunligini aniqlaymiz. Demak, $n = 7$ va tekshiruvchi simvollar soni $7 - 4 = 3$ ga teng.

Demak, darajasi 3 ga teng bo'lga yasovchi ko'phadni tanlash zarur.

3-ilovadagi jadvalga binoan $P(x) = x^3 + x^2 + 1$ ni yasovchi ko'phad sifatida olish mumkin. Ushbu yasovchi ko'phad ikkilik sanoq sistemasida $P(x) = 1101$. Ikkilik kodni qurish uchun berilgan to'rt simvolli kodni yasovchi ko'phadga ko'paytirish lozim. Ko'paytirish amali quyidagicha yoziladi.

$$\begin{array}{r} 0011 \\ \underline{1101} \\ 0011 \\ 0011 \\ \underline{0011} \\ 0010111 \end{array}$$

Shunday qilib, oddiy to'rt simvolli kombinatsiya $Q(x) = 0011$ yetti simvolli siklik kod $F(x) = 0010111$ orqali ifodalanadi.

Misollar:

a) $F(x) = x^6 + x^4 + x^3 + x^2$ siklik kod bilan kodlangan kombinatsiya olingan. Agar yasovchi ko'phad $P(x) = x^3 + x^2 + 1$ bo'lsa, dekodlash orqali olingan kombinatsiyada xatolik mavjudligini tekshirish lozim.

Yechish:

Dekodlash olingan kombinatsiyani yasovchi ko'phadga bo'lish orqali amalga oshiriladi.

$$\begin{array}{r|l} x^6 + x^4 + x^3 + x^2 & x^3 + x^2 + 1 \\ \underline{x^6 + x^5 + x^3} & x^3 + x^2 \\ x^4 + x^5 + x^2 & \\ \underline{x^4 + x^5 + x^2} & \\ 0 & \end{array}$$

Bo'lish natijasidagi qoldiq $R(x) = 0$. Demak, kombinatsiya buzilmasdan qabul qilingan.

b) $F(x) = x^6 + x^4 + x^2 + 1$ siklik kod bilan kodlangan kombinatsiya olinigan. Agar so'z yasovchi ko'phad $P(x) = x^3 + x^2 + 1$ bo'lsa, dekodlash orqali olingan kombinatsiyada xatolik mavjudligini tekshirish lozim.

Yechish:

Dekodlash olingan kombinatsiyani yasovchi ko'phadga bo'lish orqali amalga oshiriladi.

$x^6 + x^4 + x^2 + 1$	$x^3 + x^2 + 1$
$x^6 + x^5 + x^3$	$x^3 + x^2 + 1$
$x^5 + x^4 + x^3 + x^2 + 1$	
$x^4 + x^5 + x^2$	
$x^3 + 1$	
$x^3 + x^2 + 1$	
x^2	

Bo'lish natijasidagi qoldiq $R(x) = x^2 \neq 0$. Demak, kombinatsiya xatolik bilan qabul qilingan.

Nazorat savollari:

1. Siklik kodga ta'rif bering.
2. Siklik kodni qurish muolajasini so'zlab bering.
3. Qanday hususiyat xatolikni aniqlashga imkon beradi?

6 BOB. UZLUKSIZ KODLAR. REKURRENT KODLAR

6.1. Avtomatlar nazariyasi

Avtomat atamasining ikkita jihatini ko'rish mumkin. Bir tomondan, avtomat – inson ishtirokisiz qandaydir funksiyalarni bajaruvchi qurilma. Bu ma'noda kompyuter avtomat hisoblanadi, chunki u dastlabki ma'lumotlar va dasturlar kiritilganidan so'ng berilgan masalani insonning ishtirokisiz yechadi. Ikkinchi tomondan *avtomat* atamasi matematik tushuncha sifatida real texnik avtomatlarning matematik modelini anglatadi.

Avtomat chekli hisoblanadi, agar uning ichki holatlari to'plami va kirish yo'li signallari to'plami cheklangan to'plamlar bo'lsa.

Amalda ko'pincha *raqamli avtomat* tushunchasi ishlatiladi. Raqamli avtomat deganda raqamli informatsiyani o'zgartirishga mo'ljallangan qurilma tushuniladi. Raqamli avtomat ishlashini tavsiflash uchun quyidagi to'plamlar berilishi zarur:

- kirish yo'li signallari to'plami

$$(A = (a_1, a_2, \dots, a_n));$$

avtomat ichki holatlari to'plami

$$S = (s_1, s_2, \dots, s_n);$$

- ⊙ chiqish yo'li signallari to'plami

$$Z = (z_1, z_2, \dots, z_n);$$

- ⊙ o'tish funksiyasi $f: (a_k s_k) \rightarrow (s_m)$. Bu funksiya olingan signal qiymati a_k va avtomatning joriy xolati s_k ga bog'liq holda s_k avtomat xolatini s_m ga almashtiradi;

- ⊙ chiqish yo'li funksiyasi $g: (a_k s_k) \rightarrow (z_k)$. Bu funksiya kirish yo'li signali s_k asosida avtomatning joriy xolatini hisobga olgan holda chiqish yo'li signali qiymatini yaratadi.

Avtomat Mur avtomati

$$S(t + 1) = f[S(t), a_1(t), a_2(t), \dots, a_k(t)];$$

$$z_1(t) = g_1[S(t)];$$

$$z_2(t) = g_2[S(t)];$$

⋮

⋮

⋮

$$z_n(t) = g_n[S(t)];$$

yoki Mili avtomati

$$S(t + 1) = f[S(t), a_1(t), a_2(t), \dots, a_k(t)]$$

$$z_1(t) = g_1[S(t), a_1(t), a_2(t), \dots, a_k(t)];$$

$$z_2(t) = g_2[S(t), a_1(t), a_2(t), \dots, a_k(t)];$$

⋮

⋮

⋮

$$z_n(t) = g_n[S(t), a_1(t), a_2(t), \dots, a_k(t)];$$

sifatida berilishi mumkin.

Ushbu tenglamalar sistemasidan ko'rinib turibdiki, Mur avtomatida chiqish yo'li signallari avtomat joriy holatiga bog'liq bo'lsa, Mili avtomatida esa chiqish yo'li signallari nafaqat avtomat joriy holatiga, balki kirish yo'li signallari qiymatiga ham bog'liq.

Misol:

Barcha qiymatlar raqamli bo'lganligi sababli f va g funksiyalar odatda jadval ko'rinishida beriladi.

Avtomat kirish yo'liga $A = 0011101010$ signali berilgan. O'tish funksiyasi f va chiqish yo'li funksiyasi g 6.1-jadval ko'rinishida berilgan bo'lsa, chiqish yo'li signali aniqlansin.

6.1-jadval

	f		g	
	0	1	0	1
s_0	s_1	s_0	0	1
s_1	s_1	s_2	1	1
s_2	s_0	s_1	1	0

Yechish:

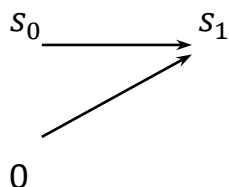
Avtomat ishlashining tadqiqini ikki bosqichda o'tkazish qulay hisoblanadi. Birinchi bosqichda kirish yo'li signali ta'sirida avtomat holatining o'zgarishini, ya'ni f funksiyani ko'ramiz.

Kirish yo'li signalini qator ko'rinishida yozamiz

$$A = 0011101010$$

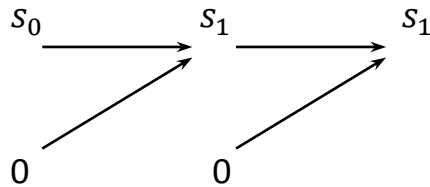
Avtomatning boshlang'ich holatini (s_0) birinchi qiymat ustiga yozamiz. Kirish yo'li signalining birinchi qiymati $a_1 = 0$.

Jadvaldan f uchun s_0 va 0 kesishgan joydan avtomatning yangi holati s_1 ni topamiz va uni ikkinchi qiymat ustiga yozamiz:

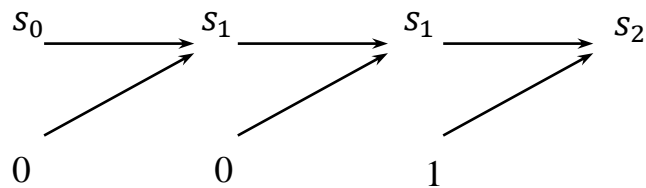


Kirish yo'li signalining ikkinchi qiymati $a_2 = 0$.

Jadvaldan f uchun s_1 va 0 kesishgan joydan avtomatning yangi holati s_1 ni topamiz va uni uchinchi qiymat ustiga yozamiz:

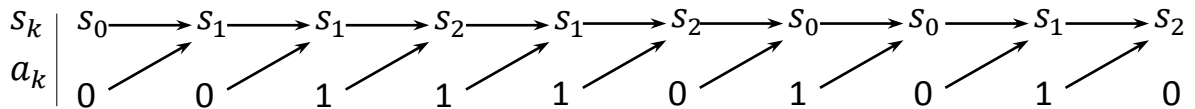


Kirish yo‘li signalining uchinchi qiymati $a_3 = 1$. Jadvaldan f uchun s_1 va 1 kesishgan joydan avtomatning yangi holati s_2 ni topamiz va uni uchinchi qiymat ustiga yozamiz:



va.h.

Kirish yo‘li signali ta‘sirida avtomat oladigan holatlarning to‘liq ketma – ketligi quyidagicha:



Ikkinchi bosqichda avtomatning barcha holatlarini bilgan holda jadvaldagi g funksiyadan foydalanib chiqish yo‘li signalini topamiz.

Kirish yo‘li signalining birinchi qiymati $a_1 = 0$ va s_0 holat uchun chiqish yo‘li signali qiymati 0 ni topamiz.

s_0
 0
 0

Kirish yo‘li signalining ikkinchi qiymati $a_2 = 0$ va s_1 holat uchun chiqish yo‘li signali qiymati 1 ni topamiz.

$s_0 \ s_1$
 $0 \ 0$
 $0 \ 1$

Kirish yo‘li signalining uchinchi qiymati $a_3 = 1$ va s_1 holat uchun chiqish

yo‘li signali qiymati 1 ni topamiz.

s_0	s_1	s_1
0	0	1
0	1	1

va h.

Kirish yo‘li signali ta’sirida avtomat oladigan holatlarning hamda chiqish yo‘li signallarining to‘liq ketma – ketligi quyidagicha:

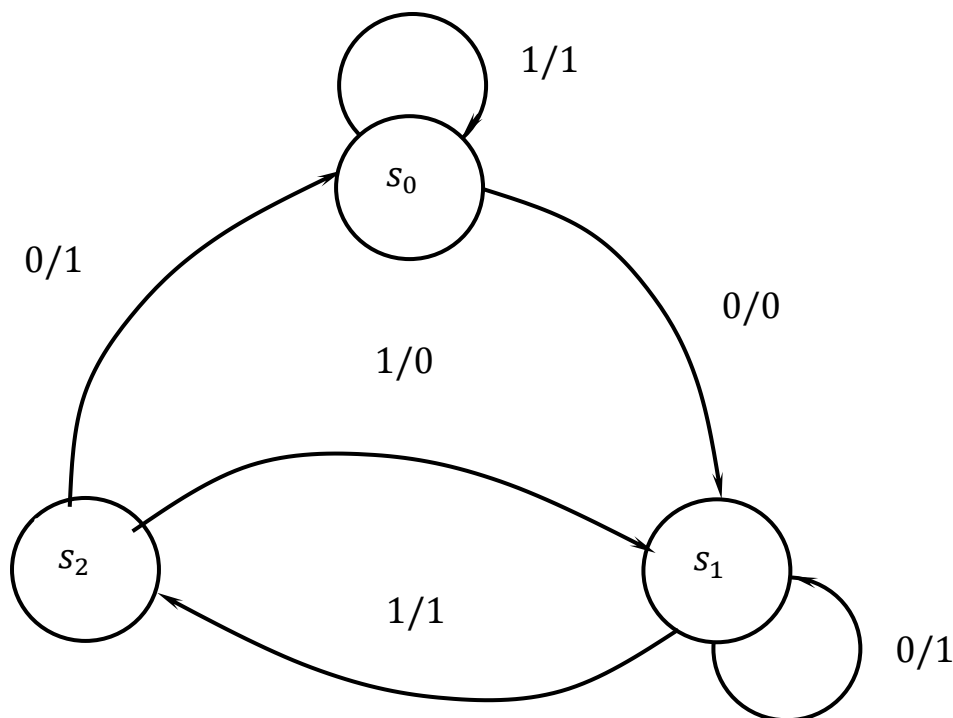
s_k	s_0	→	s_1	→	s_1	→	s_2	→	s_1	→	s_2	→	s_0	→	s_0	→	s_1	→	s_2
a_k	0	↗	0	↗	1	↗	1	↗	1	↗	0	↗	1	↗	0	↗	1	↗	0
z_k	0	↘	1	↘	1	↘	0	↘	1	↘	1	↘	1	↘	0	↘	1	↘	1

Shunday qilib, avtomat ishlashining chiqish yo‘li ketma – ketligi quyidagi ko‘rinishga ega.

$$Z = 0110111011$$

Har bir avtomatga yo‘naltirilgan graf moslashtirilishi mumkin. Bunda graf uchi sifatida avtomat xolatlari olinsa, graf yoylari salmog‘i sifatida a_k/z_k qiymati olinadi.

Ko‘rilgan misol uchun graf quyidagi ko‘rinishga ega.



Nazorat savollari:

1. Qanday avtomat chekli hisoblanadi?
2. Raqamli avtomat tushunchasiga izoh bering.
3. Mur avtomatining Mili avtomatidan farqi nimada?
4. Avtomat grafi qanday quriladi?

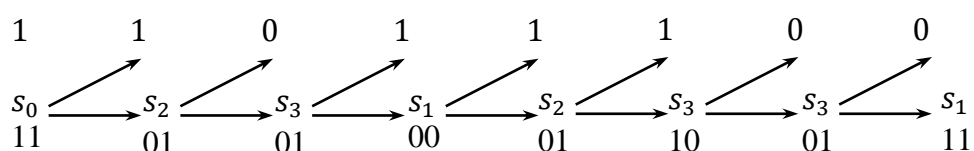
6.2. Rekurrent kodlar

Rekurrent kodlar (Сверхточные коды) uzluksiz kodlarga mansub bo'lib, bloklarga ajralmaydi. Bunda kod simvollarini kodlash va dekodlash amallari uzluksiz bajariladi. Bunday kodlar xalallarga bardosh kodlashning keng tarqalgan xili hisoblanadi. Ular simsiz aloqa protokollarida, raqamli yer usti va yer yo'ldoshi aloqa sistemalarida, kosmos bilan aloqa sistemalarida qo'llaniladi. Ushbu kodlarning ishlash prinsipining avtomatlar nazariyasiga asoslanganini 4 holatli va ikkilik ketma-ketlikni ishlovchi avtomat misolida ko'ramiz.

6.2-jadvalga binoan $A = 1, 1, 0, 1, 1, 1, 0, 0$ kirish yo'li ketma – ketligiga mos avtomat chiqish yo'li signalini aniqlaymiz.

6.2-jadval

	f		g	
	0	1	0	1
s_0	s_0	s_2	00	11
s_1	s_0	s_3	11	00
s_2	s_1	s_3	10	01
s_3	s_1	s_3	01	10



Demak, avtomat chiqish yo'lidagi signal shakllanadi:

11, 01, 01, 00, 01, 10, 01, 11

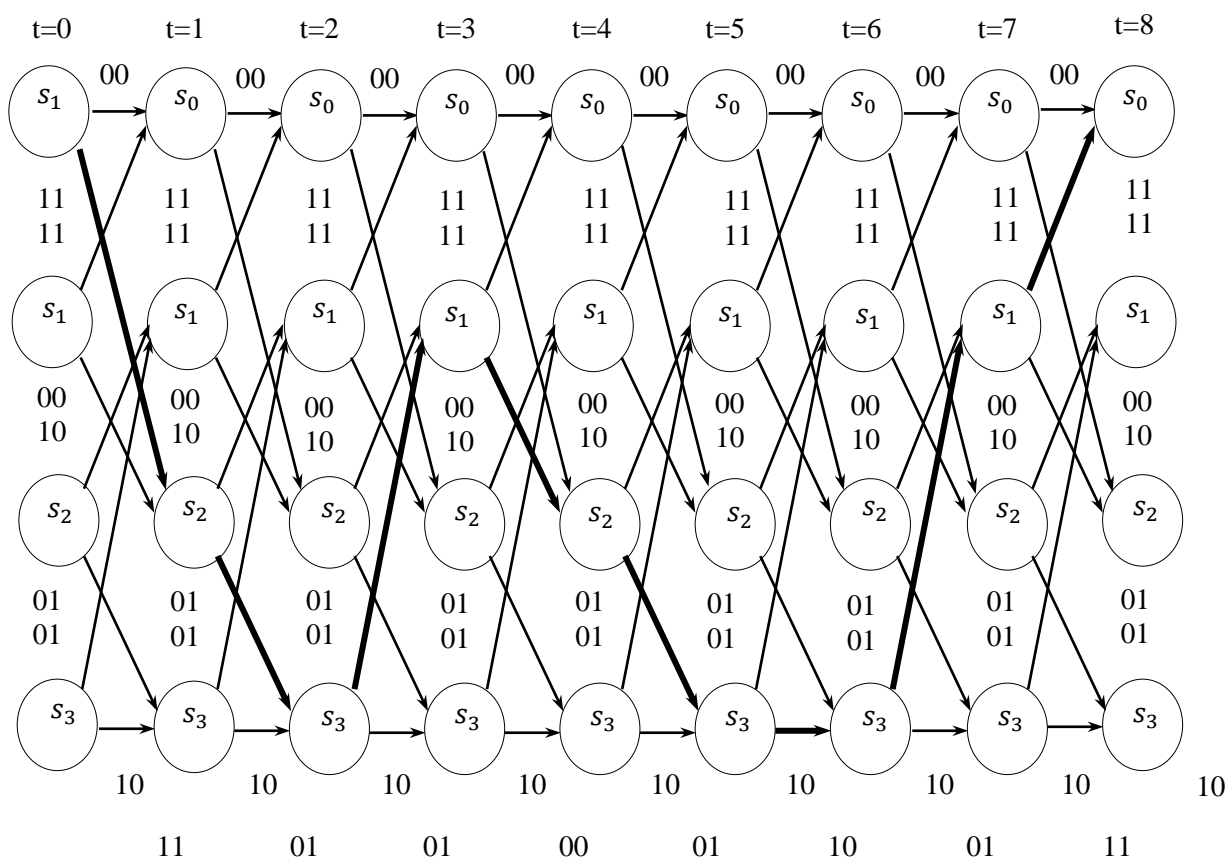
Avtomat ishlashini yoyilgan panjara diagramma – (Trellis diagram)

yordamida tavsiflash qulay hisoblanadi. Dastlabki avtomat s_0 holatida deb faraz qilinganligi sababli har qanday yo‘l trellisning chapki yuqori burchagidan boshlanadi. Har bir qadamda diagramma bo‘yicha yo‘l ikki yo‘nalishni qabul qilishi mumkin. Agar informatsion ketma – ketlikning navbattagi simvoli 0 qiymatini olsa, avtomat yuqori yo‘lni tanlaydi. Agar simvol 1 ga teng bo‘lsa avtomat pastki yo‘lni tanlaydi. Avtomatning chiqish yo‘li kodi ketma – ketligi tanlangan yo‘l yoyi salmog‘iga teng. Olingan kod ketma – ketligini dekodlash teskari tartibda amalga oshiriladi.

Trellisning har bir uzeli ikkita – yuqori va pastki yoylarga ega. Agar berilgan uzul uchun ajratilgan yo‘l yuqori yoy orqali o‘tsa informatsion signal 0 qiymatini oladi. Agar berilgan uzul uchun ajratilgan yo‘l pastki yoy orqali o‘tsa informatsion signal 1 qiymatini oladi. Bizning misolimizda dastlabki informatsion ketma – ketlik

$$A = 1, 1, 0, 1, 1, 1, 0, 0.$$

Yuqoridagi avtomat chiqish yo‘lida shakllangan kod ketma – ketligi uchun trellis quyidacha:



Rekurrent kodlar yordamida xatoliklarni tuzatish. Olingan har qanday kod ketma – ketligi uchun trellisda yo‘lni chizish mumkin emas. Masalan, 11, 11, 11 yoki 01, 01, 01 kombinatsiyalar uchun yo‘llar mavjud emas. Xuddi shunday 01 yoki 10 dan boshlanuvchi kod kombinatsiyalari ham mavjud emas. Bunday juftliklar xatolik borligini ko‘rsatadi.

Ikkilik kod kombinatsiyasi xalalli kanallar orqali uzatilganida biror bir bitning teskarisiga o‘zgarishi kod kombinatsiyasining buzilishiga olib keladi. Ma’lumki, xabarlar orasidagi masofa farqlanuvchi xonalar soni sifatida aniqlanadi. Shuning uchun uzatiladigan kod kombinatsiyasidagi har bir xatolik uning dastlabki qiymatidan masofasini orttiradi.

Buzilgan kod kombinatsiyasi, mos holda, trellisdagi yo‘lning buzilishiga olib keladi. Ba’zi hollarda, yo‘lning bo‘lmasligi ham mumkin. Xatolikni tuzatish masalasi – olingan kod kombinatsiyasi uchun bo‘lishi mumkin bo‘lgan yo‘llar to‘plamini olish va ular orasidagi shunday yo‘lni tanlash kerakki, bu yo‘l olingan kod kombinatsiyasidan minimal masofaga ega bo‘lsin.

Misol:

Uzatiladigan informatsion xabar quyidagi ko‘rinishga ega $A = (1010)$

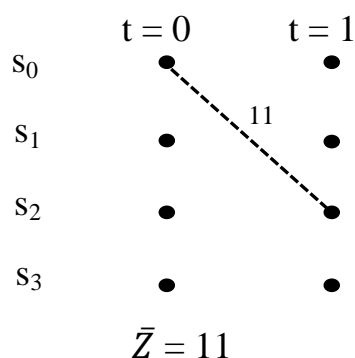
Bu xabarga quyidagi kod kombinatsiyasi mos keladi. $Z = (11, 10, 00, 10)$

Aytaylik, uzatiladigan kombinatsiyada xatolik sodir bo‘ldi.

$Z = (11, 11, 00, 10)$

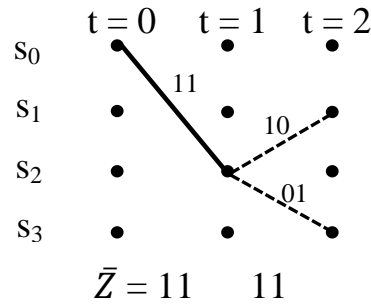
Informatsion ketma – ketlikni tiklash lozim.

Yechish:



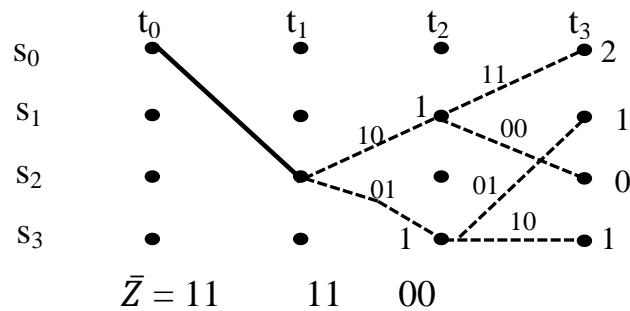
Trellisning $s_0(t = 0)$ uzeli dan boshlab olingan kod kombinatsiyasiga mos yoyni tanlaymiz. Birinchi juft simvol 11. Trellisda bu s_0 dan chiquvchi pastki

yoyga mos keladi. Demak, s_2 uzalga keldik.

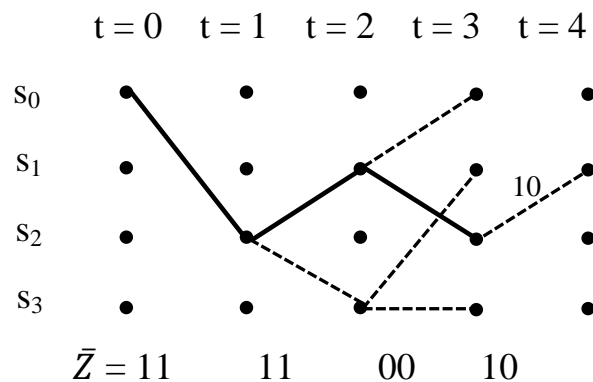


Ikkinchi qadamda trellisning $s_2(t = 1)$ uzalidan \bar{Z} ning ikkinchi juftiga mos keluvchi 11 salmoqli yoyni tanlashimiz lozim. Bunday salmoqli yoy bo‘lmaganligi sababli, ikkita variantni ko‘ramiz.

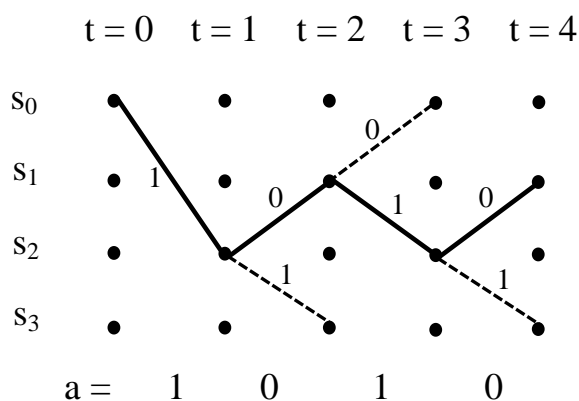
Yuqori yoy uchun 10 salmoq mos keladi. 10 va 11 orasidagi masofani $s_1(t = 2)$ uzalga yozamiz. Pastki yoy uchun 01 salmoq mos keladi. 01 va 11 orasidagi masofani $s_3(t = 2)$ uzalga yozamiz.



Qabul qilingan kombinatsiyaning uchinchi jufti 00. Uchinchi qadamda ikkita marshrut mavjud. $s_1(t = 2)$ uzeldan 11 va 00 salmoqlarga ega bo‘lgan ikkita yoy chiqadi. Ular va qabul qilingan qiymatlar orasidagi masofalarni mos uzellarga yozamiz. $s_3(t = 2)$ uzeldan ham 01 va 10 salmoqlarga ega bo‘lgan ikkita yoy chiqadi. Ular va qabul qilingan qiymatlar orasidagi masofani s_1 va s_0 uzellarga yozamiz.



To‘rtinchi qadamda maksimal salmoqqa ega bo‘lgan uzellarni tashlab yuborish lozim. Chunki ular uzatiladigan ketma – ketlikdan ko‘proq farqlanuvchi ketma – ketlikka mos keladi. Keyingi yo‘l uchun faqat s_2 uzeli qoldiramiz. Qabul qilingan kombinatsiyaning to‘rtinchi jufti 10. Trellisning $s_2(t = 3)$ uzeliidan 10 salmoqli yuqori yoy chiqadi va ushbu yoy orqali s_1 uzelga o‘tamiz.



Oxirida masofalar yig‘indisi minimal bo‘lgan uzellardan o‘tuvchi yo‘lni aniqlash lozim. Har bir qadamda yuqori yoyga 0 qiymati, pastki yoyga 1 qiymati beriladi. Dekodlangan informatsiyaning ketma-ketligi quyidagi ko‘rinishga ega.

$$A = (1010).$$

Nazorat savollari:

1. Rekurrent kodlar qanday kodlarga mansub?
2. Rekurrent kodlar qayerlarda qo‘llaniladi?
3. “Trellis” nima?
4. Kodlash va dekodlash muolajalarini tushuntiring.

6.3. Zanjir rekurrent kodlar

Xatoliklar guruhini aniqlash va tuzatishga imkon beruvchi zanjir rekurrent kod keng qo‘llaniladi. Rekurrent kodlar (m/n) kabi shartli belgilanadi. Har bir informatsion simvoldan so‘ng nazorat (tekshiruvchi) simvol keluvchi kod eng sodda rekurrent kod hisoblanadi. Bunday kod $(1/2)$ kabi belgilanadi.

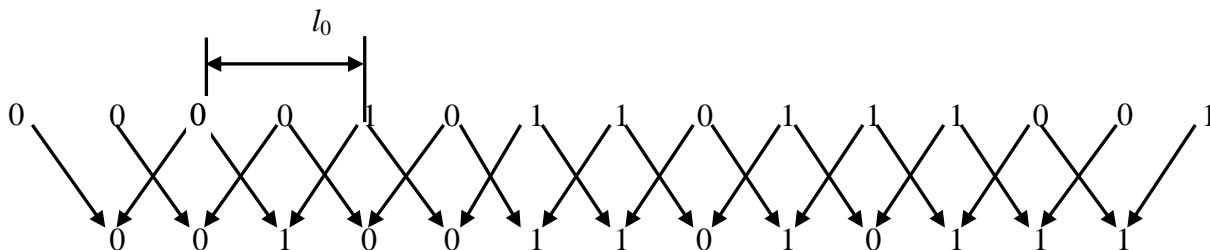
Bunda nazorat simvollarining uzunligi informatsion simvollar uzunligiga

teng, ya'ni: $m = k = n/2$.

Demak, ortiqchalik

$$D = (n - m) \cdot 100/n = (n - 0,5n) \cdot 100/n = 50\%.$$

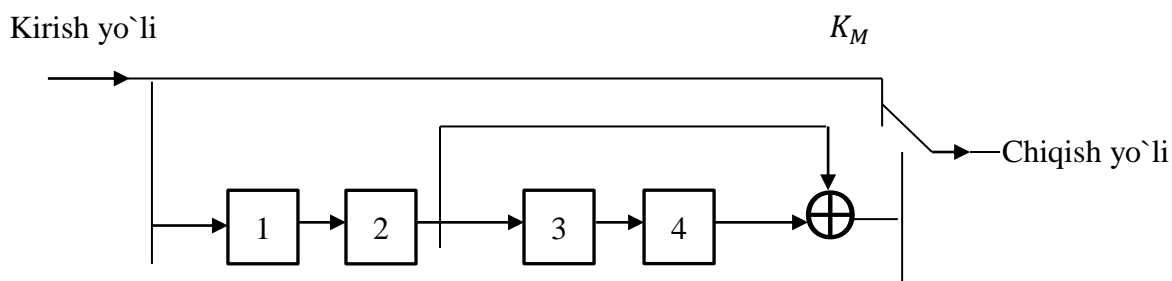
Rekurrent kodni qurish prinsipi 6.1 – rasmda keltirilgan.



6.1-rasm. Rekurrent kodni qurish prinsipiga

Nazorat simvollarining ketma – ketligi (6.1-rasmdagi pastki qator) informatsion simvollar ketma – ketligidan (6.1 – rasmdagi yuqori qator) bir – biridan l_0 masofadagi informatsion simvollarni 2 ning moduli bo‘yicha jamlash yo‘li bilan hosil qilinadi.

To‘rt xonali siljitivchi registr asosidagi kodlash sxemasi (koder) 6.2– rasmda keltirilgan.



6.2-rasm. Koder sxemasi

Agar koderning kirish yo‘liga quyidagi simvollar ketma – ketligi

$$1\ 0\ 1\ 1\ 0\ 1\ 1\ 1\ 0\ 0\ 1 \quad (1)$$

berilsa, siljitivchi registrning chiqish yo‘lida quyidagi simvollar ketma – ketligi shakllanadi.

$$0\ 0\ 1\ 0\ 0\ 1\ 1\ 0\ 1\ 0\ 1 \quad (2)$$

(2) ketma – ketlikning hosil qilinishini 6.3–jadval yordamida tushunish mumkin.

Diskret vaqt	Registr xonalari holati				Jamlag'ich chiqish yo'lida
	1-chi	2-chi	3-chi	4-chi	
t_1	1	0	0	0	0
t_2	0	1	0	0	0
t_3	1	0	1	0	1
t_4	1	1	0	1	0
t_5	0	1	1	0	0
t_6	1	0	1	1	1
t_7	1	1	0	1	1
t_8	1	1	1	0	0
t_9	0	1	1	1	1
t_{10}	0	0	1	1	0
t_{11}	1	0	0	1	1

Informatsion ketma – ketlik (1) diskret on t_i dagi registrning 1–xonasi holatiga mos kelsa, nazorat (tekshiruvchi) simvollar ketma – ketligi (2) 2ning moduli bo'yicha jamlag'ichning chiqish yo'lidagi simvollarga mos keladi.

(2) ketma – ketlik siljituvchi registrning oldingi taktdagi ikkinchi va to'rtinchi xonalarining chiqish yo'lidagi signallarni jamlash yo'li bilan olinadi. Bu 6.3 – jadvalning oldingi qatoridagi registrning ikkinchi va to'rtinchi xonasidagi simvollarni jamlashga mos keladi.

Uzatuvchi tarafdagi kommutator (K_M) chiqish yo'liga birinchi informatsion simvoldan, so'ngra birinchi nazorat simvolidan, so'ngra ikkinchi informatsion simvoldan va h. tarkib topgan ketma – ketlikni uzatadi, ya'ni:

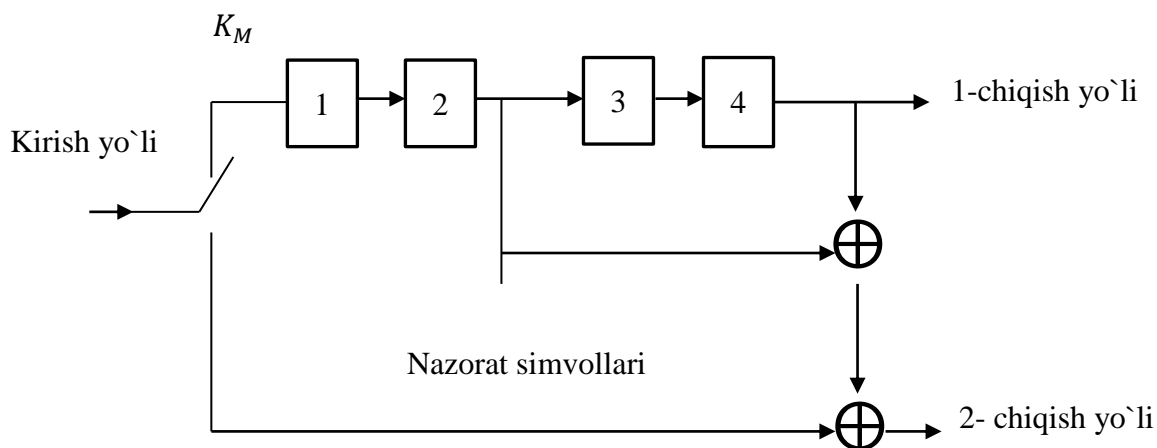
$$1\ 0\ 0\ 0\ 1\ 1\ 1\ 0\ 0\ 0\ 1\ 1\ 1\ 1\ 1\ 0\ 0\ 1\ 0\ 0\ 1\ 1 \quad (3)$$

(3) ketma – ketlik (1/2) rekurrent kodning kodlangan simvollarining ketma – ketligidir.

Dekoder sxemasi. Dekoder ikki qismli sxemadan iborat:

Birinchi qism sxemada tuzatuvchi ketma – ketlik shakllansa, ikkinchi qism sxemada kod tuzatiladi.

Birinchi qism sxemada (6.3-rasm) kommutator K_M (dekoder kommutatori) koder kommutatori bilan (6.2-rasm) sinxron va sinfaz ishlaydi.



6.3-rasm. Tuzatuvchi ketma-ketlikni shakllantirish sxemasi

Dekoder siljituvchi registri ham to‘rt xonali. Dekoder kirish yo‘liga simvollarning ketma – ketligi (3) beriladi va bu ketma – ketlik kommutator yordamida siljituvchi registr kirish yo‘liga beriluvchi informatsion ketma – ketlik (1)ga va chiqish yo‘li jamlagichining pastki kirish yo‘liga beriluvchi nazorat simvollarini ketma – ketligi (2)ga ajratiladi.

Dekoderdagi to‘rt xonali siljituvchi registr koderdagi siljituvchi registr sxemasidek sxemaga ega. Shu sababli, agar xatolik bo‘lmasa, yuqoridagi jamlagichning chiqish yo‘lidagi simvollar ketma – ketligi pastki jamlagich kirish yo‘liga beriluvchi nazorat simvollarini ketma – ketligiga mos keladi. Bu holda jamlagichning 2 – chiqish yo‘lida simvollarning ketma – ketligi faqat nollardan iborat bo‘ladi, jamlagichning 1 – chiqish yo‘lida esa buzilmagan simvollarning ketma – ketligi (1) shakllanadi.

Agar aloqa kanalida, koder va dekodeer orasida xatolik paydo bo‘lsa jamlagichning 2-chiqish yo‘lidagi simvollar ketma – ketligi tarkibida xatolikni tuzatishga imkon beruvchi ma’lum kombinatsiyadagi birlar paydo bo‘ladi. Demak, ushbu ketma – ketlik tuzatuvchi ketma – ketlik hisoblanadi.

Misol:

$2l_0=4$ uzunlikdagi seriya holidagi xatoliklar paydo bo‘lishi misolini ko‘raylik. Bunday xatoliklar paketi faqat uzunligi $l_0=2$ bo‘lgan informatsion simvollarning yarmini va uzunligi $l_0=2$ bo‘lgan nazorat simvollarining yarmini shikastlaydi.

Aytaylik, quyidagi xatoliklar ketma – ketligi sodir bo‘ldi:

$$00000\underline{1011}00000000000000 \quad (4)$$

(3) va (4) simvollar ketma – ketligini jamlab, dekoderga beriluvchi qabul qilingan ketma – ketlikni hosil qilamiz.

$$1000101110111110010011 \quad (5)$$

6.3 – rasmdagi kommutator K_m (5) ketma – ketlikni informatsion simvollarga

$$1011\underline{1}111001 \quad (6)$$

va nazorat simvollariga

$$00\underline{0}10110101 \quad (7)$$

ajratadi.

(6) va (7) simvollar ketma – ketligida xatoliklar mavjud (xato simvollarning tagiga chizilgan).

Siljitivchi registrning (6.3-rasm) chiqish yo‘lida quyidagi simvollar ketma – ketligi shakllanadi.

$$00100100001 \quad (8)$$

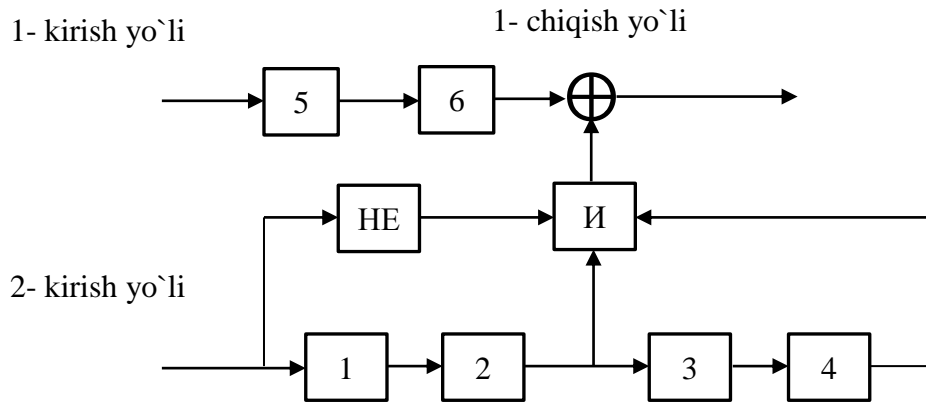
(8) ketma – ketlikni (7) ketma – ketlik bilan jamlash natijasida tuzatuvchi ketma – ketlik hosil bo‘ladi:

$$00110010100 \quad (9)$$

6.4 – rasmda xatoliklarni tuzatish sxemasi keltirilgan. Ushbu sxema dekoderning 1 – chiqish yo‘lida paydo bo‘lgan (6) ketma – ketlikni tuzatuvchi (9) ketma – ketlik yordamida avtomatik tarzda tuzatishni amalga oshirishga mo‘ljallangan.

Ushbu sxema 6.3 – rasmda keltirilgan sxemaning davomi hisoblanadi. (1 – chiqish yo‘li 1 – kirish yo‘li bilan, 2 – chiqish yo‘li 2–kirish yo‘li bilan ulanadi). Tuzatuvchi ketma – ketlik (9) bevosita inverslovchi mantiqiy element HE ning kirish yo‘liga beriladi.

Ushbu elementning chiqish yo‘lida shakllangan ketma – ketlik (10) mantiqiy element H ning chapdagi kirish yo‘liga beriladi.



6.4-rasm. Xatoliklarni tuzatuvchi dekodeer sxemasi

6.4 – rasmdagi pastki siljituvchi registr sxemasi 6.3 – rasmdagidek. Ushbu siljituvchi registrning 2 –xonasining chiqish yo‘lidan tuzatuvchi ketma – ketlik (9) $l_0=2$ qadam bilan siljigan holda mantiqiy element И ning pastki kirish yo‘liga (11) ketma – ketlik beriladi, 4 –xonasining chiqish yo‘lidan $2l_0=4$ qadam bilan siljigan holda mantiqiy element И ning o‘ngdagi kirish yo‘liga (12) ketma – ketlik beriladi. Natijada mantiqiy element И ning chiqish yo‘lida (13) ketma-ketlik hosil bo‘ladi.

$$1 \ 1 \ 0 \ 0 \ 1 \ 1 \ 0 \ 1 \ 0 \ 1 \ 1 \quad (10)$$

$$\dots \ 0 \ 0 \ 1 \ 1 \ 0 \ 0 \ 1 \ 0 \ 1 \quad (11)$$

$$\dots \dots \ 0 \ 0 \ 1 \ 1 \ 0 \ 0 \ 1 \quad (12)$$

$$\dots \dots \dots \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 1 \quad (13)$$

Ketma – ketliklarning chap tarafidagi nuqtalar simvollar siljishini belgilaydi. И mantiqiy element chiqish yo‘lidagi bir faqat uning uchchala kirish yo‘liga bir berilganidagina paydo bo‘ladi. Ushbu bir xatoliklarni tuzatishga buyruq (komanda) sifatida ishlatiladi. Ushbu komandaning berilishi dekodeerining 1 – kirish yo‘liga beriluvchi (xatolik) informatsion simvollar ketma – ketligi bilan vaqt bo‘yicha mos bo‘lishi lozim. Bu maqsadga $l_0=2$ ni ta’minlovchi 1- kirish yo‘lidagi siljituvchi registrning 5 - va 6 – xonalari xizmat qiladi. Tuzatilgan ketma – ketlik sxemaning chiqish yo‘lida (14) va (15) simvollar ketma – ketliklarining yig‘indisi ko‘rinishida shakllanadi. (14) va (15) ketma – ketliklar mos holda $2l_0=4$ va $3l_0=6$ qadamlar bilan siljigan (13) va (6) ketma – ketliklardir. Qadamlar soni ketma – ket ulangan siljituvchi registr xonalari soni orqali aniqlanadi.

$$\begin{array}{r}
 \dots 0000001000000 \quad (14) \\
 \oplus \dots 10111111001 \quad (15) \\
 \hline
 10110111001 \quad (16)
 \end{array}$$

Tuzatilgan ketma – ketlik (16) dastlabki ketma – ketlik (1) bilan mos.

Rekurrent kod uchun apparaturaning murakkabligi siljitivchi registr xonalari soni orqali baholanadi.

Nazorat savollari:

1. Zanjir rekurrent kodlarni qurish prinsipini so‘zlab bering.
2. Kodlash sxemasini keltiring.
3. Dekodlash sxemasi nechta qismdan iborat? Ularning vazifalarini va sxemalarini keltiring.
4. Zanjir rekurrent kodlar qanday xatoliklarni tuzatadi?

7 BOB. KOD O‘ZGARTGICHLARI

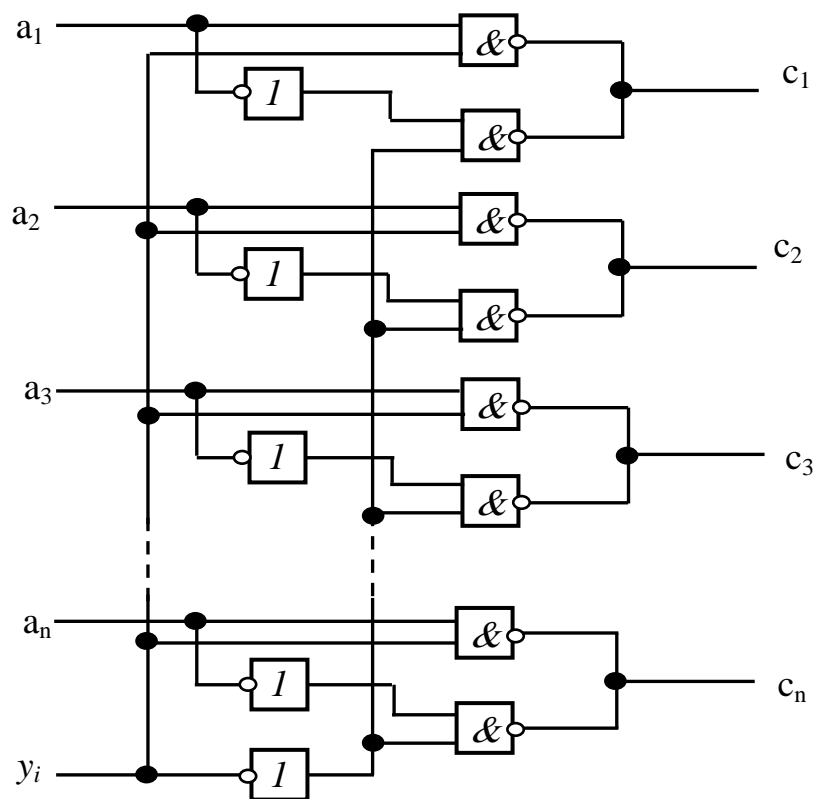
7.1. To‘g‘ri koddan teskari va qo‘shimcha kodlarni hosil qilish

Ma’lumki, *teskari kod* to‘g‘ri kod xonalari qiymatini invertirlab hosil qilinadi. 7.1-rasmda kirish yo‘lining ikkilik kodi $(a_1, a_2, a_3, \dots, a_n)$ ni boshqarish signali (y_i) ga bog‘liq holda, to‘g‘ri yoki teskari kodda uzatilishini ta’minlovchi sxema keltirilgan.

Haqiqatan, $(y_i) = 0$ bo‘lganida $c_i = a_i$ ya’ni chiqish yo‘liga to‘g‘ri kod uzatiladi. $(y_i) = 1$ bo‘lganida $c_i = \bar{a}_i$ ya’ni chiqish yo‘liga teskari kod uzatiladi. Umumiy ko‘rinishda $c_i = a_i \bar{y}_i + \bar{a}_i y_i$

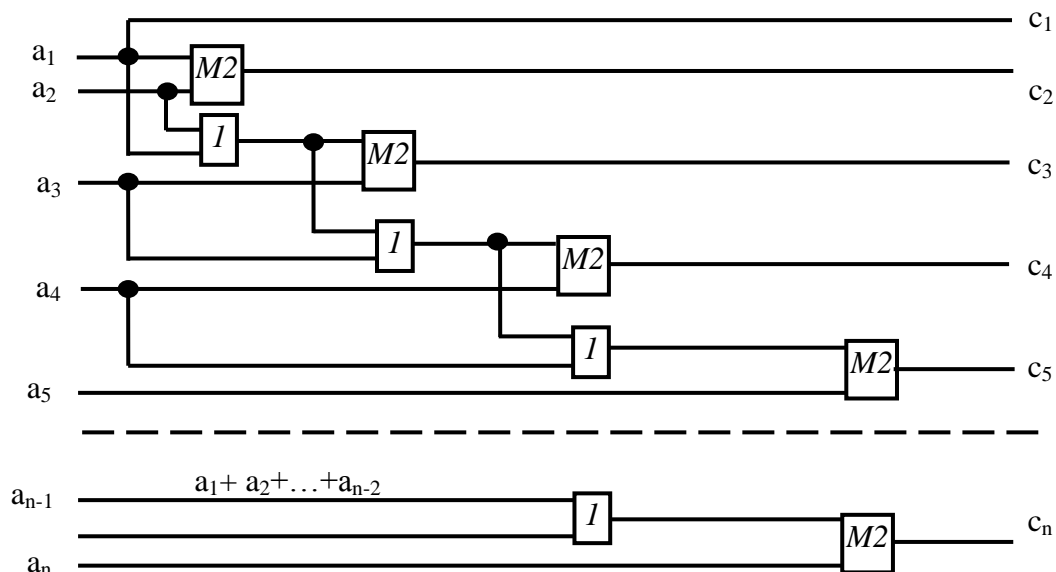
To‘g‘ri koddan *qo‘shimcha kodni* hosil qilish qoidasini umumiy ko‘rinishda quyidagicha yozish mumkin:

$$c_i = (a_1 + a_2 + \dots + a_{i-1}) \oplus a_i$$



7.1-rasm.

Ushbu ifodadan ko‘rinib turibdiki, $s_1 = a_1$, ya‘ni sonlarning to‘g‘ri va qo‘shimcha kodlaridagi kichik xonalarining qiymati bir xil. Haqiqatan, qo‘shimcha kodni hisoblaganda kichik xonasi (1 yoki 0) invertirlanadi va unga 1 qo‘shiladi, ya‘ni doimo a_1 xonaning qiymati tiklanadi. To‘g‘ri kodni qo‘shimcha kodga o‘zgartiruvchi sxema 7.2-rasmida keltirilgan.



7.2-rasm

7.2. O‘nli kodni ikkilik – o‘nli kodda va ikkilik – o‘nli kodni o‘nli kodda ifodalovchi o‘zgartgichlar

O‘nlik kodni ikkilik-o‘nli shaklda (8421 kodida) ifodalovchi o‘zgartgich sxemasi 7.3-rasmda keltirilgan. Ushbu o‘zgartgichning kirish yo‘lida 10 ta signal shinasi bo‘lib, faqat bittasida signal 1 qiymatga ega bo‘ladi. O‘zgartgichning chiqish yo‘lida esa ikkilik-o‘nlik kodning to‘rtta xonasiga mos c_1, c_2, c_3, c_4 shinalari mavjud (c_1 –kichik xona). Ushbu to‘rtta chiqish yo‘lida ikkilik raqamlarning 16 ta kombinatsiyasi mumkin bo‘lsada, faqat 10 tasi ishlatiladi (7.1-jadvalga qaralsin). Jadvaldan ko‘rinib turibdiki, c_1, c_2, c_3, c_4 xonalarning ikkilik funksiyasining $a_0, a_1, a_2, \dots, a_9$ o‘nli xonalar qiymatlari funksiyalarining mantiqiy qo‘shilishi ko‘rinishida ifodalash mumkin.

7.1-jadval

8	4	2	1
c_4	c_3	c_2	c_1
0	0	0	0
0	0	0	1
0	0	1	0
0	0	1	1
0	1	0	0
0	1	0	1
0	1	1	0
0	1	1	1
1	0	0	0
1	0	0	1

Masalan, o‘nli son 1,3,5,7,9 ga teng bo‘lgandagina ikkilik-o‘nli kodning kichik xonasi (c_1) birlik qiymatiga ega bo‘ladi.

$$c_1 = a_1 \vee a_3 \vee a_5 \vee a_7 \vee a_9$$

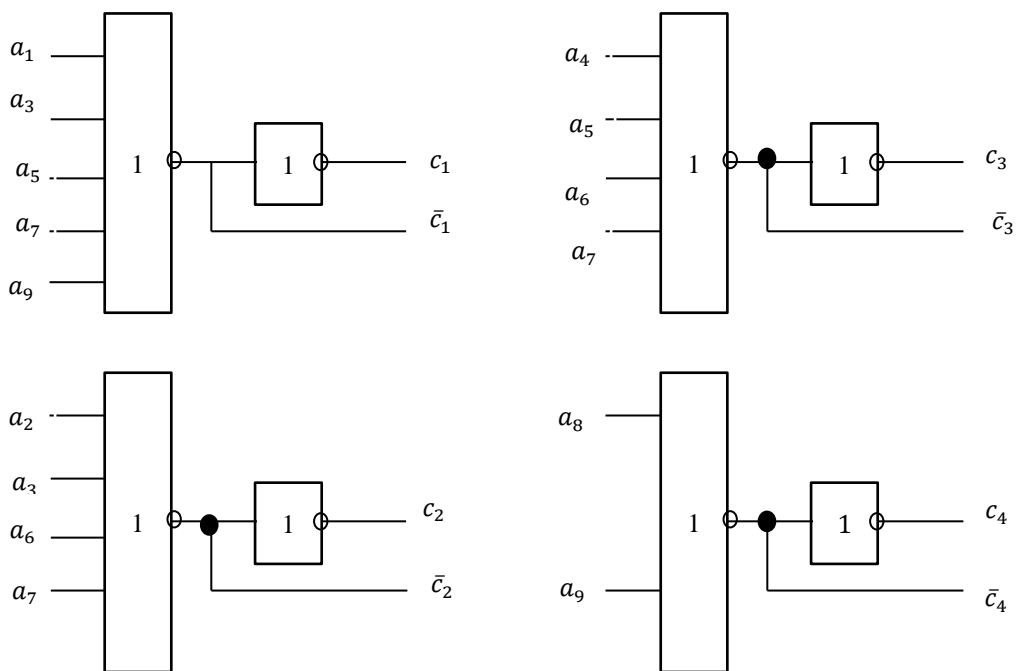
Shunga o‘xshash c_2, c_3, c_4 funksiyalari uchun quyidagilarni yoza olamiz:

$$c_2 = a_2 \vee a_3 \vee a_6 \vee a_7$$

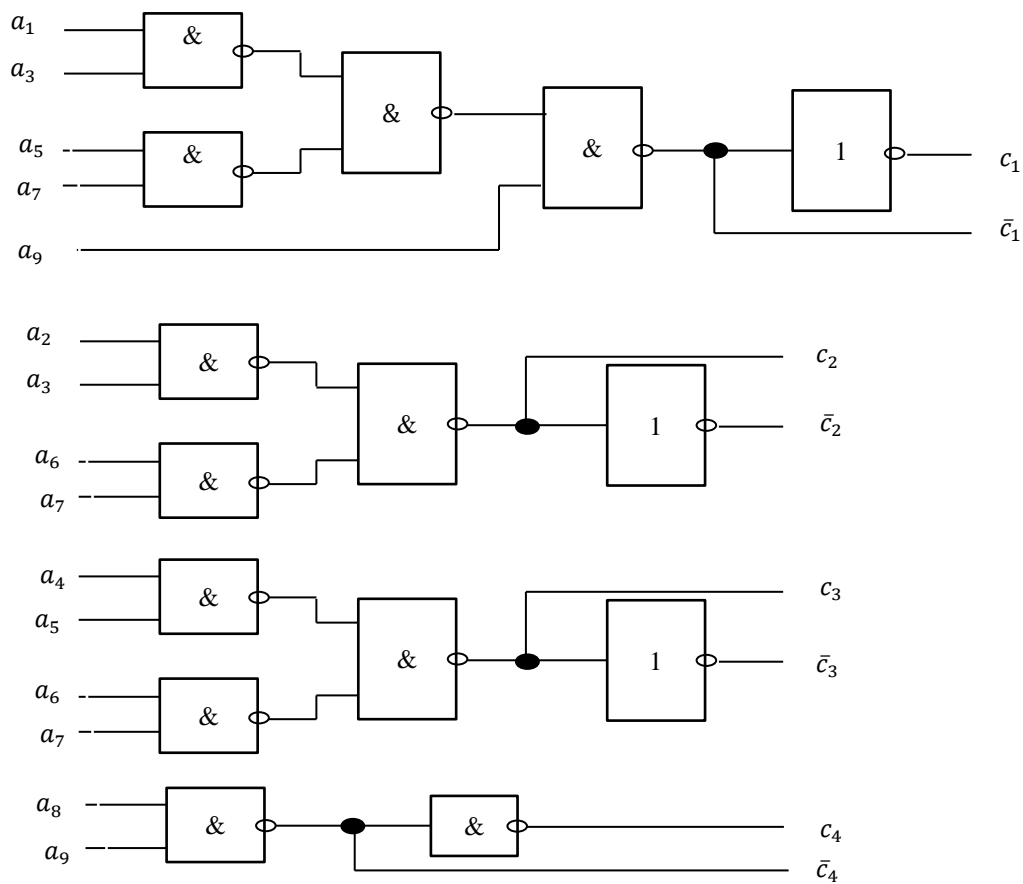
$$c_3 = a_4 \vee a_5 \vee a_6 \vee a_7$$

$$c_4 = a_8 \vee a_9$$

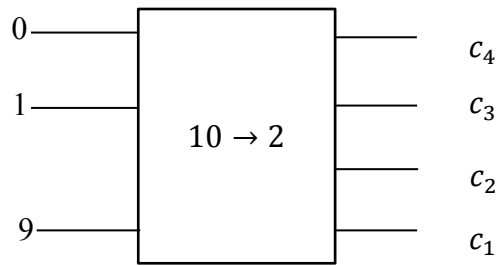
Ushbu funksiyalarni amalga oshiruvchi sxema 7.3-rasm “a” da, o‘nli kodni ikkilik-o‘nli kodda ifodalovchi sxema va uning shartli belgilanishi esa mos holda 7.3-rasm “b” va “v” da keltirilgan.



7.3-rasm (a)



7.3-rasm (b)

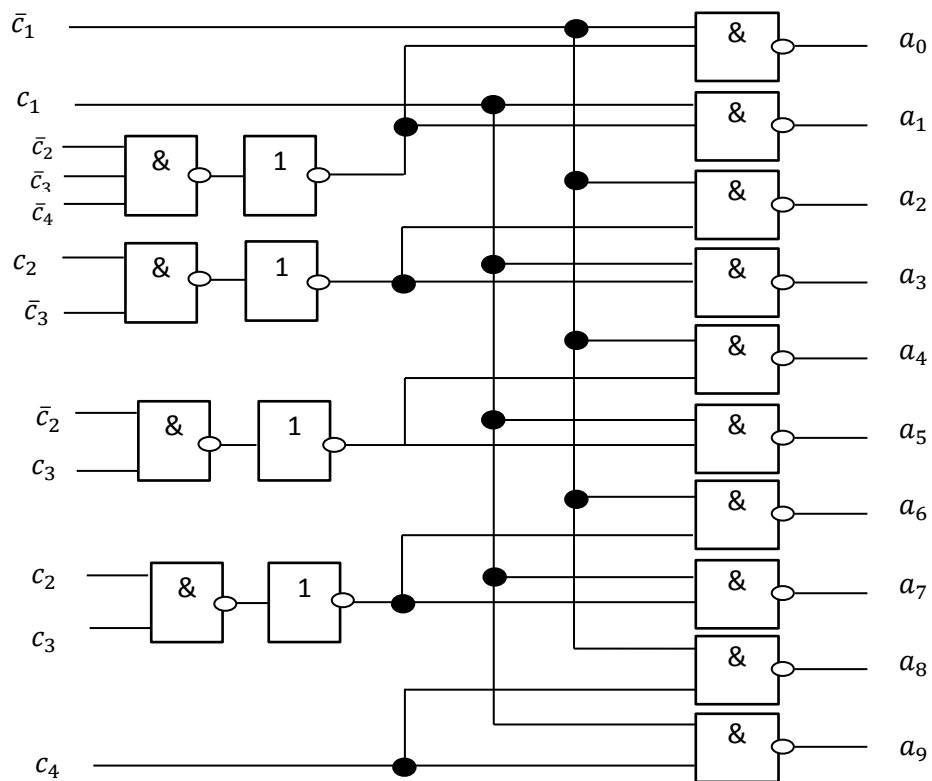


7.3-rasm (v)

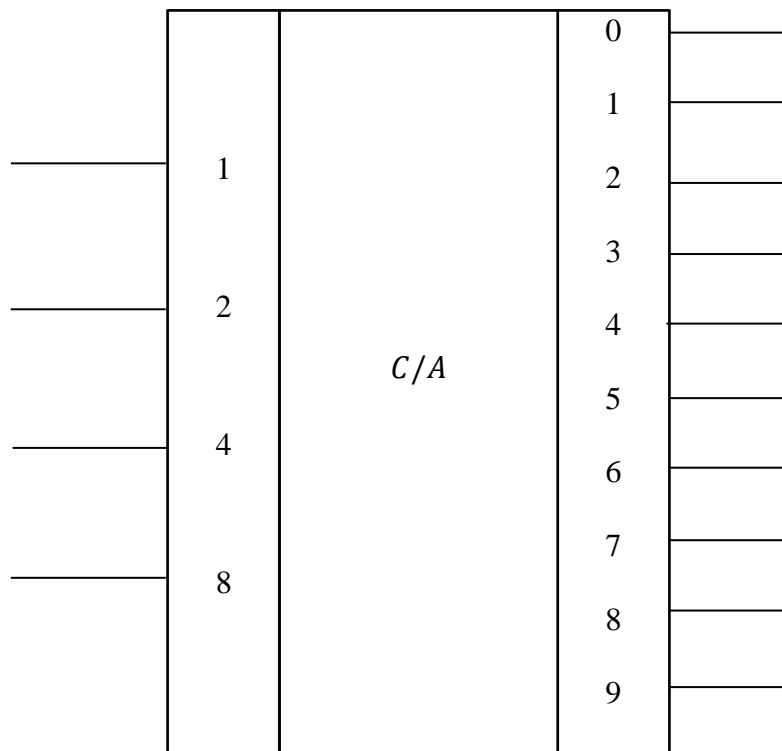
Ikkilik-oʻnli kodni oʻnli kodda ifodalash uchun a_i funksiyasini c_1, c_2, c_3, c_4 oʻzgaruvchilar orqali quyidagicha yozish kerak:

$$\begin{aligned}
 a_0 &= \bar{c}_1, \bar{c}_2, \bar{c}_3, \bar{c}_4 = \bar{c}_1, \bar{c}_2, \bar{c}_3, \bar{c}_4; & a_5 &= c_1, \bar{c}_2, c_3, \bar{c}_4 = c_1, \bar{c}_2, c_3; \\
 a_1 &= c_1, \bar{c}_2, \bar{c}_3, \bar{c}_4 = c_1, \bar{c}_2, \bar{c}_3, \bar{c}_4; & a_6 &= \bar{c}_1, c_2, c_3, \bar{c}_4 = \bar{c}_1, c_2, c_3; \\
 a_2 &= \bar{c}_1, c_2, \bar{c}_3, \bar{c}_4 = \bar{c}_1, c_2, \bar{c}_3; & a_7 &= c_1, c_2, c_3, \bar{c}_4 = c_1, c_2, c_3; \\
 a_3 &= c_1, c_2, \bar{c}_3, \bar{c}_4 = c_1, c_2, \bar{c}_3; & a_8 &= \bar{c}_1, \bar{c}_2, \bar{c}_3, c_4 = \bar{c}_1, c_4; \\
 a_4 &= \bar{c}_1, \bar{c}_2, c_3, \bar{c}_4 = \bar{c}_1, \bar{c}_2, c_3; & a_9 &= c_1, \bar{c}_2, \bar{c}_3, c_4 = c_1, c_4;
 \end{aligned}$$

Ushbu ifodalarni amalga oshiruvchi, yaʼni ikkilik-oʻnlik kodni oʻnli kodda ifodalovchi oʻzgartgichning sxemasi va uning shartli belgilanishi, mos holda 7.4-rasm “a” va “b” da berilgan.



7.4-rasm (a)



7.4-rasm (b)

Nazorat savollari:

1. To'g'ri, teskari va qo'shimcha kodlar qanday kodlar?
2. O'nli kodni ikkilik-o'nli va ikkilik-o'nli kodni o'nli kodga qanday o'zgartiriladi?

7.3. Grey kodi

Ma'lumki, ikkilik va ikkilik-o'nli kodlar uchun ikkita ketma-ket kodlardagi birlar sonining har xilligi xarakterlanadi. Masalan, $3_{10}=0011_2$ soni $4_{10}=0100_2$ sonidan bitta birga farq qilsa, $7_{10}=0111_2$ soni $8_{10}=1000_2$ sonidan to'rtta birga farq qiladi. Boshqacha aytganda, " n " xonali son uchun kod masofasi "1"dan " n " gacha o'zgarsa, *Grey kodida(davriy kodda)* qo'shni sonlar uchun kod masofasi birga teng bo'ladi. Grey kodi pozitsion bo'lmagan kodlar sinfiga mansub (7.2-jadvalga qaralsin). Grey kodi analog signallarni raqamli signallarga o'zgartirish sxemalarini qurishda qo'llaniladi va o'qishdagi bir ma'noga ega bo'lmagan xatolikni kichik xonaning birligiga keltirishga imkon beradi. $a_1, a_2, a_3, \dots, a_n$ ikkili soni

$c_1, c_2, c_3, \dots, c_n$ davriy kodga quyidagi qoida bo'yicha keltiriladi:

$$c_n = a_n,$$

$$c_{n-1} = a_{n-1} \oplus a_n,$$

.....

$$c_3 = a_3 \oplus a_4,$$

$$c_2 = a_2 \oplus a_3,$$

$$c_1 = a_1 \oplus a_2.$$

7.2-jadval

Ikkilik kod			
a_4	a_3	a_2	a_1
0	0	0	0
0	0	0	1
0	0	1	0
0	0	1	1
0	1	0	0
0	1	0	1
0	1	1	0
0	1	1	1
1	0	0	0
1	0	0	1
1	0	1	0
1	0	1	1
1	1	0	0
1	1	0	1
1	1	1	0
1	1	1	1

Grey kodi			
c_4	c_3	c_2	c_1
0	0	0	0
0	0	0	1
0	0	1	1
0	0	1	0
0	1	1	0
0	1	1	1
0	1	0	1
0	1	0	0
1	1	0	0
1	1	0	1
1	1	1	1
1	1	1	0
1	0	1	0
1	0	1	1
1	0	0	1
1	0	0	0

Sonning davriy kodidan ikkilik kodiga o'tish esa quyidagi qoida bo'yicha bajariladi:

$$a_n = c_n,$$

$$a_{n-1} = a_n \oplus c_{n-1},$$

.....

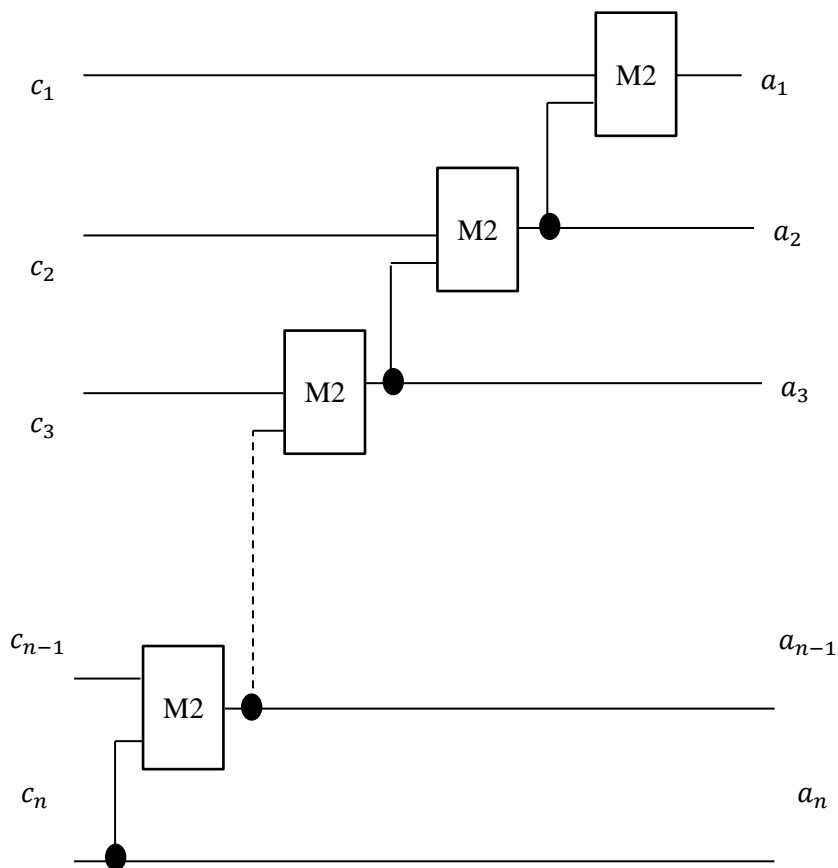
$$a_3 = a_4 \oplus c_3,$$

$$a_2 = a_3 \oplus c_2,$$

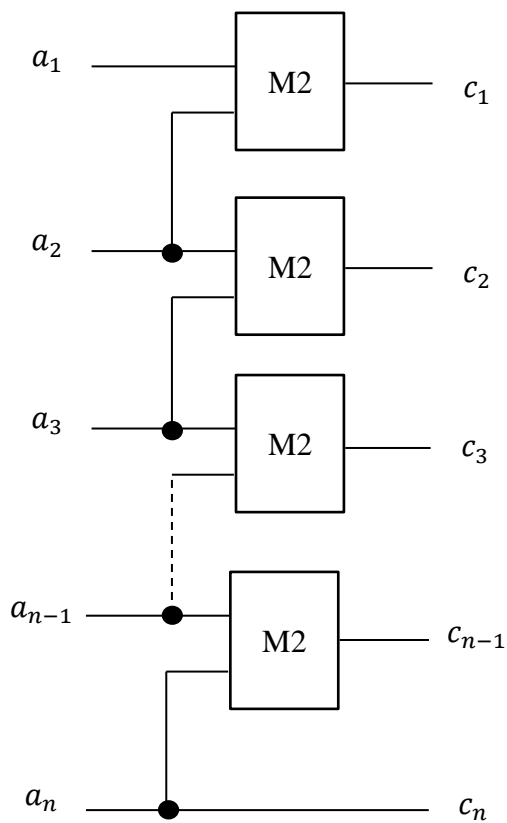
$$a_1 = a_2 \oplus c_1.$$

"n" xonali ikkilik sonni davriy kodga va davriy kodni ikkilik kodga

o'zgartiruvchi sxemalar mos holda 7.5-rasm "a" va "b" da keltirilgan.



7.5-rasm (a)



7.5-rasm (b)

Nazorat savollari:

1. Grey kodi qanday kod? Uning asosiy xususiyati nimada?
2. Ikkilik kod Grey kodiga, Grey kodi ikkilik kodga qanday o'zgartiriladi?

7.4. Kodlash yordamida informatsiyani himoyalash

Ko'pgina hollarda saqlanuvchi va uzatiluvchi informatsiya undan g'arazli maqsadlarda foydalanuvchi shaxslar uchun qiziqish uyg'otishi tabiiy. Informatsiyadan bunday ruxsatsiz foydalanish oqibati jiddiy zararlarga olib kelishi mumkin. Shu sababli, hozirda informatsiyani ruxsatsiz foydalanishdan himoyalash muammosi dolzarb hisoblanadi.

Hududni va binoni qo'riqlash, binodan foydalanishni tartibga soluvchi, foydalanishni identifikatsiyalovchi qurilmalar va hokazolarni o'z ichiga oluvchi himoyalashning texnik vositalar kompleksi mavjud. Ushbu ma'ruzada informatsiyani, uni aloqa kanali bo'yicha uzatilganida ruxsatsiz foydalanishdan himoyalash usullaridan birini ko'rish bilan chegaralanamiz. Himoyalashning ushbu usuli xabarlarini (ma'lumotlarni) shunday o'zgartirishini ta'minlaydiki, ularning dastlabki mazmunidan spetsifik informatsiyaga (kalitga) ega foydalanuvchi foydalanishi va kalit yordamida teskari o'zgartirishni amalga oshirishi mumkin. Bunday usullar *informatsiyani kriptografik berkitish usullari* deb yuritiladi.

Informatsiyani kriptografik berkitish usullaridan foydalanuvchi sistemalarda bajariladigan o'zgartirishlarni kodlash va dekodlash jarayonlarining bir turi deb hisoblash mumkin. Ushbu jarayon *shifrlash va rasshifrovka qilish* nomlarini olgan.

Informatsiyani shifrlash deganda ochiq informatsiyani (dastlabki matnni) shifrlangan informatsiyaga o'zgartirish (shifrlash) va aksincha (rasshifrovka qilish) jarayoni tushuniladi. Shifrlangan matn *shifrmtn* deb yuritiladi. Shifrlashning ko'pgina turli usullari mavjud. Quyida keng tarqalgan shifrlardan biri – *Vijiner shifri* ustida so'z boradi. Bunda shifrlashning ishonchlilik darajasi alfavit xarflarining paydo bo'lish statistik qonuniyatlarining buzilishi evaziga ortadi.

Vijiner shifriga binoan alfavitning har biriga nomer beriladi. Masalan, o'zbek alfaviti harflariga 0 (A = 0) dan to 34 (X = 34) gacha raqam moslashtiriladi.

А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18

Т	У	Ф	Х	Ц	Ч	Ш	Ъ	Ь	Э	Ю	Я	Ў	Қ	Ғ	Ҳ
19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34

Kalit xabar tagiga qaytarilib yoziladigan qandaydir soʻz yoki oddiy harflar ketma – ketligi sifatida ifodalanadi. Shifrmatning har bir harfiga raqamli ekvivalent xabar harfi raqamli ekvivalentini uning tagidagi kalit harfi raqamli ekvivalentiga 35 ning moduli boʻyicha jamlash orqali aniqlanadi.

Misol:

“FŸ3A” kaliti yordamida “ПAХТАКОР” dastlabki matnni shifrlash va rasshifrovka qilish talab etilsin.

Yechish.

Shifrlash va rasshifrovka qilish natijasi quyida keltirilgan.

Dastlabki matn	П	А	Х	Т	А	К	О	Р
Kalit	Ғ	Ў	3	А	Ғ	Ў	3	А
Shifrmatn	Н	Ў	Я	Т	Р	Ж	Ц	Р
Kalit	Ғ	Ў	3	А	Ғ	Ў	3	А
Dastlabki matn	П	А	Х	Т	А	К	О	Р

Vijiner shifri faqat juda uzun kalitlardan foydalanilganda yetarlicha yuqori kriptobardoshlikka ega boʻladi.

Bitta harfdan iborat kalitli Vijiner shifri Sezar shifri, chegaralanmaydigan qaytarilmaydigan kalitli Vijiner shifri Vernam shifri sifatida maʼlum.

Nazorat savollari:

1. Vijiner shifri yordamida matnni shifrlash va rasshifrovka qilish muolajasini tushuntiring.
2. Sezar va Vernam shifrlarining Vijiner shifridan farqi nimada?

Adabiyotlar

1. Вентцель Елена Сергеевна. Теория вероятности. Учебник. ISBN: 978-5-4060-0476-0, издательство: Кнорус, 2016 г. 664 с.
2. А.С. Гуменюк, Н.Н. Поздниченко. Теория информации и кодирования: Учебное пособие / Минобрнауки России, ОмГТУ. – Омск: Изд-во ОмГТУ, ISBN 978-5-8149-2111-6, 2015 г.
3. С.К. Ганиев. “Ахборот назарияси ва кодлаш” фанидан маърузалар матни. ТАТУ илмий услубий кенгаши мажлисида кўрилган ва чоп этишга тавсия этилган. Қайднома №7/68. 13.04.2014 й.
4. Ганиев С.К., Абдуллаев Д.Ф. “Ахборот назарияси ва кодлаш” фани бўйича амалий машғулотларга услубий кўрсатма. ТАТУ. Тошкент 2012.
5. Думачев В.Н. Теория информации и кодирования-Воронеж: Воронежский институт МВД России, 2012.-200 с.
6. Richard E. Algebraic Codes for Data Transmission. Blahut Paperback. ISBN-13:9780521556590 Subject: Communications and Signal processing. Publication date January 2012.
7. Теория информации: учеб. / В.А. Фурсов. - Самара: Изд-во Самар, гос. аэрокосм, ун-та, 2011. - 128 с.: ил.
8. Березкин Е.Ф. Основы теории информации и кодирования: Учебное пособие. – М.: НИЯУ МИФИ, 2010. – 312 с.
9. Крушной В.В. Основы теории информации и кодирования. Снежинск-СГФТА-2005.
10. Ганиев С.К., Каримов М.М., Мамбетов Н.М. Ҳисоблаш системаларининг информация асослари. Олий ўқув юрти талабалари учун дарслик. – Тошкент, ТДТУ, 2002.
11. Савельев А.Я. Основы информатики. Учебник для вузов. М: Издательство МГТУ им. Н.Э. Баумана. 2001.
12. Димитриев В.И. Прикладная теория информации. Учеб. для студ. вузов. М.: высш.шк. 1989.

Ilovalar

1-ilova

Butun sonlarning ikkilik logarifmlari

<i>A</i>	<i>log₂A</i>	<i>A</i>	<i>log₂A</i>	<i>A</i>	<i>log₂A</i>
1	0,00000	38	5,24793	75	6,22882
2	1,00000	39	5,28540	76	6,24793
3	1,58496	40	5,32193	77	6,26679
4	2,00000	41	5,35755	78	6,28540
5	2,32193	42	5,39232	79	6,30378
6	2,58496	43	5,42626	80	6,32193
7	2,80735	44	5,45943	81	6,33985
8	3,00000	45	5,49185	82	6,35755
9	3,16993	46	5,52356	83	6,37504
10	3,32193	47	5,55459	84	6,39232
11	3,45943	48	5,58496	85	6,40939
12	3,58496	49	5,61471	86	6,42626
13	3,70044	50	5,64386	87	6,44294
14	3,80735	51	5,67242	88	6,45943
15	3,90689	52	5,70044	89	6,47573
16	4,00000	53	5,72792	90	6,49185
17	4,08746	54	5,75489	91	6,50779
18	4,16993	55	5,78136	92	6,52356
19	4,24793	56	5,80735	93	6,53916
20	4,32193	57	5,83289	94	6,55459
21	4,39232	58	5,85798	95	6,56986
22	4,45943	59	5,88264	96	6,58496
23	4,52356	60	5,90689	97	6,59991
24	4,58496	61	5,93074	98	6,61471
25	4,64386	62	5,95420	99	6,62936
26	4,70044	63	5,97728	100	6,64386
27	4,75489	64	6,00000	200	7,644
28	4,80735	65	6,02237	300	8,229
29	4,85798	66	6,04439	400	8,614
30	4,90689	67	6,06609	500	8,966
31	4,95420	68	6,08746	600	9,229
32	5,00000	69	6,10852	700	9,451
33	5,04439	70	6,12928	800	9,644
34	5,08746	71	6,14975	900	9,814
35	5,12928	72	6,16992	1000	9,965
36	5,16993	73	6,18982	10000	13,288
37	5,20945	74	6,20945		

- $p \log_2 p$ kattaliklarning qiymatlari

p	$-p \log_2 p$	p	$-p \log_2 p$	p	$-p \log_2 p$	p	$-p \log_2 p$
0.00	0.0000	0.26	0.5053	0.52	0.4906	0.78	0.2796
0.01	0.0664	0.27	0.5100	0.53	0.4854	0.79	0.2678
0.02	0.1129	0.28	0.5142	0.54	0.4800	0.80	0.2575
0.03	0.1517	0.29	0.5179	0.55	0.4744	0.81	0.2462
0.04	0.1857	0.30	0.5211	0.56	0.4684	0.82	0.2348
0.05	0.2161	0.31	0.5238	0.57	0.4623	0.83	0.2231
0.06	0.2435	0.32	0.5260	0.58	0.4558	0.84	0.2113
0.07	0.2686	0.33	0.5278	0.59	0.4491	0.85	0.1993
0.08	0.2915	0.34	0.5292	0.60	0.4422	0.86	0.1871
0.09	0.3127	0.35	0.5301	0.61	0.4350	0.87	0.1748
0.10	0.3322	0.36	0.5306	0.62	0.4276	0.88	0.1623
0.11	0.3503	0.37	0.5307	0.63	0.4199	0.89	0.1496
0.12	0.3671	0.38	0.5304	0.64	0.4121	0.90	0.1368
0.13	0.3826	0.39	0.5298	0.65	0.4040	0.91	0.1238
0.14	0.3971	0.40	0.5288	0.66	0.3957	0.92	0.1107
0.15	0.4105	0.41	0.5274	0.67	0.3871	0.93	0.0978
0.16	0.4230	0.42	0.5856	0.68	0.3784	0.94	0.0839
0.17	0.4346	0.43	0.5236	0.69	0.3694	0.95	0.0703
0.18	0.4453	0.44	0.5211	0.70	0.3602	0.06	0.0565
0.19	0.4552	0.45	0.5181	0.71	0.3508	0.97	0.0426
0.20	0.4644	0.46	0.5153	0.72	0.3412	0.98	0.0286
0.21	0.4728	0.47	0.5120	0.73	0.3314	0.99	0.0140
0.22	0.4806	0.48	0.5083	0.74	0.3215	1.00	0.0000
0.23	0.4877	0.49	0.5043	0.75	0.3113		
0.24	0.4941	0.50	0.5000	0.76	0.3009		
0.25	0.500	0.51	0.4954	0.77	0.2903		

Yasovchi polinomlar jadvali

№	Daraja	Polinom	Ikkilik ketma-ketlik
1	1	$x + 1$	11
2	2	$x^2 + x + 1$	111
3	3	$x^3 + x + 1$	1011
4		$x^3 + x^2 + 1$	1101
5	4	$x^4 + x + 1$	10011
6		$x^4 + x^3 + 1$	11001
7		$x^4 + x^3 + x^2 + x + 1$	11111
8	5	$x^5 + x^2 + 1$	100101
9		$x^5 + x^3 + 1$	101001
10		$x^5 + x^3 + x^2 + x + 1$	101111
11		$x^5 + x^4 + x^2 + x + 1$	110111
12		$x^5 + x^4 + x^3 + x + 1$	111011
13		$x^5 + x^4 + x^3 + x^2 + 1$	111101
14	6	$x^6 + x + 1$	1000011
15		$x^6 + x^3 + 1$	1001001
16		$x^6 + x^4 + x^2 + x + 1$	1010111
17		$x^6 + x^4 + x^3 + x + 1$	1011011
18		$x^6 + x^5 + 1$	1100001
19		$x^6 + x^5 + x^2 + x + 1$	1100111
20		$x^6 + x^5 + x^3 + x^2 + 1$	1101101
21		$x^6 + x^5 + x^4 + x + 1$	1110011
22		$x^6 + x^5 + x^4 + x^2 + 1$	1110101
23	7	$x^7 + x + 1$	10000011
24		$x^7 + x^3 + 1$	10001001
25		$x^7 + x^3 + x^2 + x + 1$	10001111
26		$x^7 + x^4 + 1$	10010001
27		$x^7 + x^4 + x^3 + x^2 + 1$	10011101
28		$x^7 + x^5 + x^2 + x + 1$	10100111
29		$x^7 + x^5 + x^3 + x + 1$	10101011
30		$x^7 + x^5 + x^4 + x^3 + 1$	10111001
31		$x^7 + x^5 + x^4 + x^3 + x^2 + x + 1$	10111111
32		$x^7 + x^6 + 1$	11000001
33		$x^7 + x^6 + x^3 + x + 1$	11001011
34		$x^7 + x^6 + x^4 + x + 1$	11010011
35		$x^7 + x^6 + x^4 + x^2 + 1$	11010101
36		$x^7 + x^6 + x^5 + x^2 + 1$	11100101
37		$x^7 + x^6 + x^5 + x^3 + x^2 + x + 1$	11101111

Atamalarning rus, o'zbek va ingliz tillaridagi izohli lug'ati

Atama	Sharhi
<p>Абстрактное представление данных Ma'lumotlarni abstrakt ifodalash Abstract representation of data</p>	<p>Принцип определения типа данных через операции, которые могут выполняться над объектами данного типа. При этом вводятся следующие ограничения: значения объектов могут модифицироваться и наблюдаться только путем использования этих операций.</p> <p>Ob'ektlarning berilgan turi ustida bajarilishi mumkin bo'lgan amallar orqali ma'lumotlar xilini aniqlash prinsipi. Bunda quyidagi cheklashlar kiritiladi: ob'ektlar mavqei faqat ushbu amallar yordamida modifikatsiyalanishi va kuzatilishi mumkin.</p> <p>The principle of determining the type of data through the operations that may be performed on given objects type. In this case the following restrictions can be considered: the values of objects can be modified and observed only by using these operations.</p>
<p>Бит (двоичный код) Bit (ikkili kod) Bit (binary)</p>	<p>Минимальная единица количества информации в компьютере, равная одному двоичному разряду.</p> <p>Kompyuterdagi bitta ikkili xonaga teng axborot miqdorining minimal birligi.</p> <p>The minimum unit amount of information into a computer, which is equal to one binary digit.</p>
<p>Бит достоверности Haqiqiylik biti Validity bit</p>	<p>Разряд, добавляемый к слову в памяти компьютера для указания достоверности информации.</p> <p>Axborot haqiqiyligini ko'rsatish maqsadida kompyuter хотirasidagi so'zga qo'shiladigan bit.</p> <p>Bit that is added to a word in the computer memory for indicating the reliability of the information.</p>

<p>Бит защиты Himoya biti Protection bit</p>	<p>Двоичный разряд в ключе памяти, устанавливающий защиту соответствующего блока памяти от записи либо от выборки и записи</p> <p>Xotiraning mos blokiga yozish yoki undan tanlash va unga yozishdan himoyalash uchun o'rnatiladigan хотира kalitidagi ikkili хона.</p> <p>Bit in the key memory, setting protection according memory block from record or chose and record.</p>
<p>Бит контроля на четность Juftlikka tekshirish biti Parity bit</p>	<p>Контрольный бит, добавляемый к данным для контроля их верности таким образом, чтобы сумма двоичных единиц, составляющих данное, включая и единицу контрольного бита, всегда была четной (либо всегда нечетной).</p> <p>Ma'lumotlardagi ikkili birliklar yig'indisi doimo juft (yoki doimo toq) bo'lishligini ta'minlash maqsadida ularga qo'shiladigan nazorat biti.</p> <p>To provide the binary digits sum of the information which is always an even (or always odd) the additional control bits</p>
<p>Бит маски Niqob biti Mask bit</p>	<p>Сочетание битов, устанавливаемых в нулевое или единичное значение для разрешения или запрета определенных операций либо для проверки или изменения содержимого поля.</p> <p>Ma'lum amallar bajarilishiga ruxsat berish yoki rad etish yoki hoshiya tarkibini tekshirish yoki o'zgartirish uchun nul yoki bir qiymatiga o'rnatiluvchi bitlar birikmasi.</p> <p>A combination of bits set to zero or single value to enable or disable certain operations or to inspect or modify the contents of the field.</p>
<p>Бит управления доступом Foydalanishni boshqarish biti Access control bit</p>	<p>Один из нескольких битов ключа памяти, сопоставляемых с ключом защиты при обращении к соответствующему блоку памяти с целью организации ее защиты.</p>

	<p>Xotirani himoyalashni tashkil etish maqsadida xotiraning mos blokiga murojaat vaqtida himoya kaliti bilan taqqoslanuvchi xotira kalitining bitta yoki bir necha biti.</p>
	<p>One of several key bits of memory mapped to the key protection when accessing the corresponding memory which are blocked in order to organize its defense.</p>
<p>Блок данных Ma'lumotlar bloki Data block</p>	<p>Последовательность битов, имеющая фиксированную длину и используемая для представления данных в памяти или для их пересылки.</p>
	<p>O'zgarimas uzunlikka ega va xotirada ma'lumotlarni ifodalanishda yoki ularni jo'natishda ishlatiluvchi bitlar ketma-ketligi.</p>
	<p>Bit sequence having a unchangeable length and its use to represent data in memory or for shipment.</p>
<p>Блок доступа к записи YOzishda foydalanuvchi blok Record access block</p>	<p>В «серия малых» компьютере структура данных в системе управления данными (СУД), содержащая запрос на доступ к записи файла СУД.</p>
	<p>“Kichik seriyali” kompyuterdagi tarkibida faylni yozish so'rovi bo'lgan ma'lumotlarni boshqarish tizimidagi ma'lumotlar strukturasi.</p>
	<p>The “small series” computer data structure data management system (DMS), containing a request for writing access to the DMS's file.</p>
<p>Блок текста Matn bloki Text Block</p>	<p>Мультиграмма текста (текста открытого, текста шифрованного или промежуточного), составленная из подряд идущих знаков. Обычно текст разбивается на блоки одинаковой длины.</p>
	<p>Ketma-ket keluvchi belgilardan tuzilgan matn mul'tigrammasi (ochiq matn, shifrlangan matn, oraliq matn). Odatda matn uzunligi bir xil bloklarga ajratiladi.</p>

	Multigramma text (text open, encrypted text or intermediate), composed of contiguous characters. Usually the text is divided into blocks of equal length.
Блокировка записи в память Xotiraga yozishni blokirovka qilish Memory write lock	<p>Ситуация при обмене данными, характеризующаяся тем, что запись, читаемая с внешнего носителя, в основную память не переводится.</p> <p>Ma'lumotlar almashinuvidagi vaziyat bo'lib, tashqi eltuvchidan o'qiladigan yozuv asosiy xotiraga o'tkazilmaydi.</p> <p>Situation at information transfer, characterized in that the record read from the external media to the main memory is not translated.</p>
Взвешенный код Salmoqlangan kod Weighted code	<p>Блочный код, в котором каждой позиции символа в закодированном слове присваивается определенный вес.</p> <p>Blokli kod bo'lib, unda kodlangan so'zdagi har bir o'ringa ma'lum salmoq beriladi.</p> <p>Block code in which each character position in the encoded word is assigned a specific weight.</p>
Граница кодирования Kodlash chegarasi Coding bound	<p>Предел производительности кода, зависящий от таких параметров, как мощность кода, минимальное расстояние Хемминга, длина кодовой комбинации.</p> <p>Kod salmog'i, minimal Xemming masofasi, kod kombinatsiyasining uzunligi kabi parametrlarga bog'liq kod unumdorligining chegarasi.</p> <p>Limit of code performance, depending on such parameters as the output code, the minimum Hamming distance, the length of the codeword.</p>
Данные	Информация, представленная в формализованном виде, пригодном для передачи, интерпретации или обработки с участием человека либо автоматическими средствами.

<p>Ma'lumotlar Data</p>	<p>Odam ishtiroki bilan yoki avtomatik tarzda uzatishga, izohlashga yoki ishlashga yaroqli, formallashgan ko'rinishda ifodalangan axborot.</p>
<p>Двоичный код с исправлением ошибок Xatoliklarni tuzatuvchi ikkilik kod Vinary error correction code</p>	<p>Information presented in a formalized manner suitable for communication, interpretation or processing involving human or automated means.</p> <p>Двоичный код, избыточность которого обеспечивает автоматическое обнаружение и исправление ошибок некоторых типов в передаваемых данных.</p> <p>Ortiqchaligi uzatiluvchi ma'lumotlardagi ba'zi xatoliklarni avtomatik tarzda aniqlashni va to'g'rilashni ta'minlovchi ikkili kod.</p> <p>Binary code whose redundancy provides automatic detection and correction of errors in certain types of data transmitted.</p>
<p>Декодирование Dekodlash Decoding</p>	<p>Преобразование данных в исходную форму, которую они имели до кодирования; операция, обратная кодированию.</p> <p>Ma'lumotlarni, ular kodlanishidan avvalgi dastlabki shakliga o'zgartirish; kodlash amaliga teskari amal.</p> <p>Converting the data into its original shape that they had prior to encoding; inverse operation of coding.</p>
<p>Дескриптор Deskriptor Descriptor</p>	<p>Описатель, элемент информационной структуры объекта, указывающий, в каком виде запоминается та или иная информация (например, в массиве записи или файле). Обратившись к дескриптору, программа получает возможность интерпретировать характеризующие им данные.</p> <p>U yoki bu axborot qanday ko'rinishda (masalan, yozuv massivida yoki faylda) xotirlanishini ko'rsatuvchi ob'ekt axborot strukturasiining elementi, tavsiflovchi. Dastur deskriptorga murojaat etib u harakterlovchi ma'lumotlarni sharxlash</p>

	<p>imkoniyatiga ega bo'лади.</p> <p>Descriptor information element structure of the object, indicating the form in which is stored this or any other information (eg, in an array of records or file). Turning to the handle, the program is able to interpret the data they are characterized.</p>
<p>Дешифратор (декодер) Deshifrator (dekoder) Decoder</p>	<p>Логическая схема, преобразующая n разрядное входное двоичное слово (код, шифр) в единичный сигнал на одном из $2k$ выходов этой схемы. Обратную функцию выполняет шифратор.</p> <p>Kirish yo'llariga beriladigan n xonali ikkili so'zni (kod, shifr) $2k$ chiqish yo'llarining bittasida birlik signaliga o'zgartiruvchi sxema. Teskari funksiyani shifrator bajaradi.</p> <p>Logic circuit that converts an input binary word n bit (code, cipher) in a single signal on one of $2k$ outputs of the circuit. Encoder performs the inverse function.</p>
<p>Дешифратор адреса Adres deshifratori Address decoder</p>	<p>Преобразователь адреса в управляющие сигналы, направляемые запоминающему устройству.</p> <p>Adresni хотирловчи qurilmaga yuboriluvchi boshqarish signaliga o'zgartirgich.</p> <p>Address converter control signals directed to the memory device.</p>
<p>Дополнительный бит Qo'shimcha bit Additional bit</p>	<p>Бит, добавляемый к слову данных с определенной целью (например, контроль на четность).</p> <p>Ma'lumotlar so'ziga ma'lum maqsad bilan qo'shiladigan bit (masalan, juftlikka tekshirish).</p> <p>Bit added to a data word with a specific purpose (e.g for framing or even parity).</p>
<p>Защита от ошибок Xatolardan himoyalash Error protection</p>	<p>Применение кодов с обнаружением и исправлением ошибок. Действия по проверке правильности выполнения предыдущих операций. Контроль</p>

	<p>допустимости значений аргументов при входе в процедуру.</p>
	<p>Xatolarni aniqlovchi va tuzatuvchi kodlardan foydalanish. Oldingi amallarni bajarilishining to'g'riligini tekshirish bo'yicha harakatlar. Muolajaga kirishda argumentlar qiymatlarining joizligini nazoratlash.</p>
	<p>Application of codes with detection and correction of mistakes. Actions on check of correctness of performance of the previous operations. Control of an admissibility of values of arguments at an entrance to procedure.</p>
<p>Избыточная система Ortiqchalik tizim Redundant system</p>	<p>Система, обладающая избыточностью некоторого типа аппаратной, алгоритмической, информационной, обеспечивающей повышение надежности ее функционирования.</p>
	<p>Ishlash ishonchliligini oshirilishini ta'minlovchi qandaydir xil apparat, algoritm, axborot ortiqchaligiga ega tizim.</p>
	<p>The system possessing redundancy of some type of an equipment room, algorithmic, information reliability of its functioning providing increase.</p>
<p>Избыточность Ortiqchali Redudancu</p>	<p>Введение в систему дополнительных компонентов сверх минимально необходимого их числа с целью повышения надежности системы. Различают избыточность аппаратную, информационную, алгоритмическую.</p>
	<p>Tizim ishonchliligini oshirish maqsadida unga keragidan ortiq qo'shimcha komponentlarning kiritilishi. Apparat, algoritm, axborot ortiqchaliklar farqlanadi.</p>
	<p>Introduction in system of additional components over minimum their necessary number for the purpose of increase of reliability of system. Distinguish redundancy hardware, information, algorithmic.</p>

<p>Избыточность кода (кодовая избыточность) Kod ortiqchaligi Sode redudansu</p>	<p>Разность между средним числом битов, используемых для кодирования одного сообщения источника и минимально возможным числом битов, полученным из теоремы Шеннона.</p>
	<p>Manbaning bitta xabarini kodlash uchun ishlatiladigan bitlarning o'rtacha soni bilan SHennon teoremasidan olingan bitlarning minimal soni orasidagi tafovut.</p>
	<p>Difference between average of the bits used for coding of one message of a source and minimum possible number of bits, received from Shannon's theorem.</p>
<p>Информационная система Axborot tizimi Information system</p>	<p>Организационно упорядоченная совокупность документов (массивов документов) и информационных технологий, в том числе с использованием средств вычислительной техники и связи, реализующих информационные процессы.</p>
	<p>Hujjatlarning (hujjatlar massivining) va axborot texnologiyalarining, xususan axborot jarayonlarini amalga oshiruvchi, hisoblash texnikasi va aloqa vositalaridan foydalanib, tashkiliy tartibga solingan majmui.</p>
	<p>Organizationally ordered set of documents (document files) and information technologies, including with use of computer aids and the communications, realizing information processes.</p>
<p>Информационная технология Axborot texnologiyasi Information technology</p>	<p>Система технических средств и способов обработки информации.</p>
	<p>Axborotni ishlash usullari va texnik vositalari tizimi.</p>
	<p>System of technical means and ways of information processing.</p>
<p>Информационные процессы Axborot jarayonlari Information processes</p>	<p>Процессы сбора, обработки, накопления, хранения, поиска и распространения информации.</p>

	<p>Axborotni qidirish, to'plash, saqlash, uzatish, ishlash va undan foydalanish jarayonlari.</p> <p>Processes of collecting, processing, accumulation, storage, search and information distribution.</p>
<p>Информация Axborot Information</p>	<p>Сведения, которые уменьшают степень неопределенности нашего знания о конкретном объекте.</p> <p>Ma'yuuan ob'ekt xususidagi bilimlarimizning noaniqlik darajasini pasaytirishga imkon beruvchi har qanday ma'lumot.</p> <p>Data that reduces the uncertainty degree of knowledge about certain object.</p>
<p>Канальное кодирование Kanal kodlash Channel coding</p>	<p>Использование кодов с обнаружением ошибок или кодов с исправлением ошибок для обеспечения надежной передачи по каналу связи. При канальном кодировании код выбирается в соответствии с каналом (главным образом, с его шумовыми характеристиками), а не с источником информации.</p> <p>Aloqa kanali bo'yicha ishonchli uzatishni ta'minlash uchun xatoliklarni aniqlash kodlaridan yoki xatoliklarni tuzatuvchi kodlardan foydalanish. Kanal kodlashda kod, axborot manbaiga emas, balki kanalga (asosan uning shovqunlash xarakteristikalariga) mos holda tanlanadi.</p> <p>Use of codes with detection of mistakes or codes with correction of mistakes for ensuring reliable transfer on a communication channel. At channel coding the code gets out according to the channel (mainly, with its noise characteristics), instead of with information source.</p>
<p>Каскадный код Kaskad kod Concatenated code</p>	<p>Код с исправлением ошибок, который можно рассматривать как результат последовательного применения нескольких других кодов.</p>

	<p>Bir necha boshqa kodlarning ketma-ket ishlatilishi natijasi sifatida ko‘rish mumkin bo‘lgan xatolikni tuzatuvchi kod.</p> <p>Code with correction of mistakes which can be considered as result of consecutive application of several other codes.</p>
<p>Код с контролем на четность Juftlikga nazoratlovchi kod Rarity chek sode</p>	<p>Двоичный код, в котором к каждой кодовой комбинации присоединяется дополнительный контрольный разряд, что позволяет сохранить принятую в системе одну и ту же четность двоичных блоков.</p> <p>Tizimda qabul qilingan ikkili bloklarning juftligini saqlashga imkon beruvchi, har bir kod kombinatsiyasiga nazorat xonasi sifatida qo‘shiladigan qo‘shimcha ikkili kod.</p> <p>Binary code in which the additional control category joins each code combination that allows to keep the same parity of binary blocks accepted in system.</p>
<p>Код с минимальной избыточностью Minimal ortiqchalik kod Minimum redundancy code</p>	<p>Как правило, под этим подразумевается код, построенный по процедуре Хаффмена.</p> <p>Odatda, bunday kod Xaffmen muolajasi bo‘yicha quriladi.</p> <p>As a rule, it is meant as the code constructed on procedure of Huffman.</p>
<p>Код с минимальным расстоянием Minimal oraliqli kod Minimum distance code</p>	<p>Избыточный код, в котором переход от одного допустимого значения к следующему сопровождается минимальным изменением в кодовой комбинации. Позволяет обнаруживать в передаваемых данных только одиночные ошибки.</p> <p>Bir joiz qiymatdan keyingisiga o‘tishda kod kombinatsiyasida minimal o‘zgarish yuz beradigan ortiqchalik kod. Uzatiluvchi ma’lumotlarda faqat yakka xatoliklarni aniqlashga imkon beradi.</p> <p>Excess code in which transition from one admissible value to the following is</p>

	<p>accompanied by the minimum change in a code combination. Allows to find in transmitted data only single mistakes.</p>
<p>Код с переменной скоростью Tezligi o'zgaruvchi kod Code with variable velocity</p>	<p>Как правило, используется при описании сверточных кодов, у которых длина кодовых подблоков изменяется во времени, а длина информационных подблоков остается постоянной.</p> <p>Odatda o'raluvchi kodlarni tavsiflashda ishlatiladi. Bunday kodlarda kod qismlarining uzunligi vaqt bo'yicha o'zgaradi, axborot qismlarining uzunligi esa o'zgarmaydi.</p> <p>As a rule, it is used at the description the svertochnykh of codes at which length of code subblocks changes in time, and length of information subblocks remains to a constant.</p>
<p>Код Хаффмена Xaffmen kodi Huffman code</p>	<p>Префиксный код, в котором длина кодовой комбинации обратно пропорциональна частоте появления кодируемого элемента (чем чаще встречается элемент, тем короче кодовая комбинация).</p> <p>Kod kombinatsiyasining uzunligi kodlanuvchi elementning paydo bo'lishi chastotasiga teskari proporsional (element qanchalik tez-tez uchrasa, kod kombinatsiyasi shunchalik qisqa bo'ladi) bo'lgan prefiks kod.</p> <p>Prefix code in which length of a code combination is inversely proportional to the frequency of emergence of a coded element (the more often the element meets, the code combination is shorter).</p>
<p>Код Хемминга Xemming kodi Hamming sode</p>	<p>Код с минимальной избыточностью, обеспечивающий исправление одиночных ошибок.</p> <p>Yakka xatoliklarni tuzatishni ta'minlovchi minimal ortiqchalikka ega kod.</p> <p>Code with the minimum redundancy, providing correction of single mistakes.</p>

<p>Кодирование Kodlash Coding</p>	<p>Отождествление данных с их кодовыми комбинациями; установление соответствия между элементом данных и совокупностью символов, называемой кодовой комбинацией, словом кода.</p>
	<p>Ma'lumotlarning ularning kod kombinatsiyalari bilan tenglashtirish; ma'lumot elementlari va kod kombinatsiyasi, kod so'zi deb ataluvchi simvollar majmuasi orasida moslikni o'rnatish.</p>
	<p>Identification of data with their code combinations; compliance establishment between an element of data and the set of symbols called by a code combination, the code word.</p>
<p>Кодирование источника Manbani kodlash Source coding</p>	<p>Использование в рамках заданного алфавита кодов переменной длины с целью уменьшения числа символов в сообщении до минимума, необходимого для представления всей информации сообщения или по крайней мере для обеспечения условий такого сокращения.</p>
	<p>Xabarning barcha axborotini ifodalash uchun zarur bo'lgan xabardagi simvollar sonini minimalgacha kamaytirish yoki, bo'lmaganida bunday qisqartirish shartini ta'minlash maqsadida, berilgan alfavit doirasida uzunligi o'zgaruvchi kodlardan foydalanish.</p>
	<p>Use within the set alphabet of codes of variable length for the purpose of reduction of number of symbols in the message to the minimum necessary for submission of all information of the message or at least for providing conditions of such reduction.</p>
<p>Кодирование с критерием верности Haqiqiylik mezonini bo'yicha kodlash Coding with fidelity criterion</p>	<p>Преобразование сообщения источника в кодовое слово, такое, что обратное преобразование приводит к некоторому другому сообщению, близкому к исходному в смысле</p>

	<p>заданного критерия верности.</p> <p>Manba xabari kod soʻziga shunday oʻzgartiriladiki, teskar oʻzgartirish berilgan haqiqiylik mezoni nuqtai nazaridan, dastlabki xabarga yaqin qandaydir boshqa xabarni beradi.</p> <p>Transformation of the message of a source to the code word, such that leads the return transformation to some other message close to initial that is set criterion of fidelity.</p>
<p>Кодирование, использующее флаг Bayroqdan foydalanib kodlash Flag based encoding</p>	<p>К коду добавляется некоторая последовательность символов, которая не является кодовым словом и в процессе работы может быть использована как разделитель между словами.</p> <p>Kodga kod soʻzi boʻlmagan qandaydir simvollar ketma-ketligi qoʻshiladi va u ish jarayonida soʻzlar orasidagi ajratuvchi sifatida ishlatiladi.</p> <p>To a code some sequence of symbols which isn't the code word is added and in the course of work can be used as a divider between words.</p>
<p>Кодирующее устройство Kodlash qurilmasi Coder</p>	<p>Автоматическое или автоматизированное устройство для кодирования программ и данных на носителе информации с целью последующего их ввода в компьютер.</p> <p>Kompyuterga kiritish maqsadida dasturlarni va maʼlumotlarni axborot eltuvchisida avtomatik yoki avtomatlashtirilgan tarzda kodlash qurilmasi.</p> <p>The automatic or automated device for coding of programs and data on a data carrier for the purpose of the subsequent their input in the computer.</p>
<p>Кодовая решетка Kod panjara Code trellis</p>	<p>Направленный граф, в который превращается дерево сверточного кода с конечной длиной ограничения.</p> <p>Uzunligi cheklangan oʻraluvchi kod daraxti aylanadigan yoʻnaltirilgan graf.</p>

	The directed count into which the tree of a convolutional code with a final length of restriction turns.
<p>Коды Боуза Чоудхури Хокенгема (коды БЧХ) Bouz CHoudhuri Хокенгем kodlari (BCHX kodlar) Bose Chaudhuri Носсвенгем codes (BCH codes)</p>	<p>Семейство двоичных линейных блочковых кодов с исправлением ошибок. Эти коды весьма эффективны, но главное их преимущество состоит в простоте кодирования/ декодирования (с использованием сдвиговых регистров). Их можно рассматривать и как обобщение кодов Хэмминга, и как специальный случай кодов РидаСоломона. Коды БЧХ используются и в качествециклических кодов.</p>
	<p>Xatoliklarni tuzatuvchi ikkili chiziqli blokli kodlar oilasi. Ushbu kodlar juda effektiv, ammo ularning eng muhim afzalligi kodlashning / dekodlashning (siljitivchi registlar yordamida) soddaligi hisoblanadi. Ularni Xemming kodining umumlashtirilgani kabi va Rid Solomon kodining maxsus xoli sifatida ko'rish mumkin. BCHX kodlar siklik kodlar sifatida ham ishlatiladi.</p>
	<p>Family of binary linear block codes with correction of mistakes. These codes are very effective, but their main advantage consists in simplicity of coding / decoding (with use of shift registers).</p>
<p>Коды Голя Goley kodlari Golay codes</p>	<p>Семейство совершенных линейных блочковых кодов с исправлением ошибок. Наиболее полезным является двоичный код Голя. Известен также троичный код Голя. Коды Голя можно рассматривать как циклические коды.</p>
	<p>Xatoliklarni tuzatuvchi mukammal chiziqli blokli kodlar oilasi. Goleyning ikkili kodi eng foydali hisoblanadi. Goleyning uchli kodi ham ma'lum. Goley kodlarini siklik kodlar sifatida ko'rish mumkin.</p>

	Family of the made linear block codes with correction of mistakes. The most useful is Goley's binary code. Goley's also ternary code is known. Goley's codes can be considered as cyclic codes.
Коды Рида Мюллера Rid Myuller kodlari Reed Muller codes	Семейство двоичных циклических блочных кодов с исправлением ошибок.
	Xatoliklarni tuzatuvchi ikkili siklik blokli kodlar oilasi.
	Family of binary cyclic block codes with correction of mistakes.
Коды Рида Соломона Rid Solomon kodlari Reed - Solomon codes	Важное семейство линейных блочных кодов с исправлением ошибок, особенно удобных для исправления пакетов ошибок. Они могут рассматриваться и как обобщение кодов Боуза Чоудхури Хокенгема, и как особый случай кодов Гоппы, могут быть отнесены к циклическим кодам.
	Xatoliklarni tuzatuvchi, ayniqsa, xatoliklar paketini tuzatishga qulay chiziqli blokli kodlarning muhim oilasi. Ushbu kodlarni Bouz CHoudxuri Hokengem kodlarining umumlashtirilgani sifatida va Goppa kodlarining maxsus xoli sifatida, siklik kodlar sifatida ko‘rish mumkin.
	Important family of linear block codes with correction of the mistakes which are especially convenient for correction of packages of mistakes. They can be considered and as generalization of codes of Bose Chaudhuri Hocquenghem and as a special case of codes of Goppy, which can be carried to cyclic codes.
Коды с повторением Takrorlanuvchi kodlar Repetition codes	Семейство совершенных циклических блочных кодов с исправлением ошибок, в котором ключевые слова формируются просто r -кратным повторением слов сообщения. Если данные коды рассматривать как коды с параметрами (n, k) , то для любого k у них $n=rk$.

	<p>Kalit soʻzlari xabar soʻzlarining oddiy “r”- karrali takrorlanishi orqali shakllanuvchi, xatolikni tuzatuvchi mukammal siklik blokli kodlar oilasi. Agar berilgan kodlarda (n,k) parametrlilik kodlar sifatida qaralsa, ixtiyoriy “k” uchun ularda “n = rk” boʻladi.</p>
	<p>Family of the made cyclic block codes with correction of mistakes in which keywords are formed by simply r-fold repetition of words of the message. If to consider these codes as codes with parameters (n, k) for any k of n=rk at them.</p>
<p>Компилятор Kompilyator Compiler</p>	<p>Транслятор, предназначенный для выполнения компиляции. Kompilyasiyani amalga oshirishga moʻljallangan translyator. The translator intended for performance of compilation.</p>
<p>Контроль по избыточности Ortiqchalik boʻyicha nazorat Redundacy check</p>	<p>Контроль, выполняемый или с помощью резервированных технических средств, или на основе избыточной информации и обеспечивающий выдачу сведений о наличии определенных ошибок. Muayyan xatoliklar mavjudligi xususida xabar berilishini taʼminlovchi rezervlangan texnik vositalar yordamida yoki ortiqchalik axborot asosida bajariluvchi nazorat. The control which is carried out or by means of redundant technical means, or on the basis of surplus information and providing issue of data on existence of certain mistakes.</p>
<p>Контрольный код Nazorat kodi Check code</p>	<p>Код, позволяющий автоматически обнаруживать, локализовать и устранять ошибки в передаваемых данных. Uzatilayotgan maʼumotlardagi xatoliklarni avtomatik tarzda aniqlash, lokalizatsiya va bartaraf etishga imkon beruvchi kod.</p>

	The code allowing automatically to find, localize and eliminate errors in transmitted data.
Коэффициент сжатия в источнике сообщений Xabarlar manbaida zichlash koefitsienti Source compressing factor	Отношение длин сообщения до и после его сжатого кодирования. Xabarning dastlabki uzunligini, zichlab kodlanganidan keyingi uzunligiga nisbati. The relation of lengths of the message before its squeezed coding.
Машинный код Mashina kodi Computer sode	Двоичный код, используемый для кодирования машинных команд по правилам, предусмотренным в данном типе компьютера. Kompyuterning muayyan turida ko'zda tutilgan qoidalar bo'yicha mashina komandalarini kodlash uchun ishlatiladigan ikkili kod. The binary code used for coding of machine teams by rules, provided in the computer this type.
Нарушение кода передачи Uzatish kodining buzilishi Transmission code violation	Использование цифр, не принадлежащих коду передачи данных по линиям связи. Aloqa liniyalari bo'yicha ma'lumotlarni uzatish kodiga taalluqli bo'lmagan raqamlardan foydalanish. Use numbers do not belong to the code data on the communication lines.
Некорректируемая ошибка Tuzatilmaydigan xatolik Uncorrectable error	Ошибка в сообщении, которая не может быть исправлена средствами корректирующего кода. Tuzatuvchi kod vositalari yordamida tuzatib bo'lmaydigan xabardagi xatolik. Error messages that can not be corrected by means of correcting code.
Обнаружение и исправление ошибок Xatoliklarni aniqlash va tuzatish Error detection and correction	Для обнаружения ошибок либо в данные вводится определенная избыточность, позволяющая их контролировать, либо процесс вычислений дублируется. Некоторые ошибки, связанные с передачей данных, могут быть исправлены путем повторной пересылки этих данных. В других случаях приходится применять

	<p>системы с прямым исправлением ошибок.</p> <p>Xatoliklarni aniqlash uchun ma'lumotlarga ularni nazoratlashga imkon beruvchi ortiqchalik kiritiladi yoki hisoblash jarayoni takrorlanadi. Ma'lumotlarni uzatish bilan bog'liq ba'zi xatoliklar ushbu ma'lumotlarni qayta uzatish yo'li bilan tuzatish mumkin. Boshqa hollarda to'g'ridan – to'g'ri tuzatish tizimlarini qo'llashga to'g'ri keladi.</p> <p>To detect errors in data or entering certain redundancy, allowing them to control, or the calculation process is duplicated. Some of the errors associated with data transmission, can be corrected by re-sending the data. In other cases it is necessary to use systems with forward error correction.</p>
<p>Однозначно декодируемый код Bir ma'noli dekodlanuvchi kod Uniquely decodable code</p>	<p>Код, слова которого образуют однозначно дешифрируемое множество.</p> <p>So'zlari bir ma'noli deshifrlanuvchi to'plamni hosil qiluvchi kod.</p> <p>Code words which form a uniquely decrypted set.</p>
<p>Помехи Xalallar Noise</p>	<p>Возмущения в канале связи, искажающие передаваемое сообщение.</p> <p>Uzatiluvchi xabarni buzuvchi aloqa kanalidagi g'alayon.</p> <p>Disturbance in the communication channel, which distort the transmitted message.</p>
<p>Помехоустойчивое кодирование Xalallarga bardoshli kodlash Noiseless coding</p>	<p>Использование кода, повышающего эффективность системы связи, в которой помехи отсутствуют вообще или незначительны. Помехоустойчивое кодирование в общем виде идентично кодированию источника.</p> <p>Xalallar umuman bo'lmagan yoki juda kam bo'lgan aloqa tizimi samaradorligini oshiruvchi kodlardan foydalanish.</p>

	Umumiy holda xalallarga bardosh kodlash manbani kodlash bilan bir xil.
	Using code efficacy enhancing communication system in which interference or absent altogether negligible. Noiseless coding generally identical source coding.
Скремблер Skrembler Scrambler	Кодирующее устройство, используемое в цифровом канале, которое выдает случайную последовательность бит.
	Raqamli kanalda ishlatiluvchi, bitlarning ketma-ketligini shakllantiruvchi kodlovchi qurilma.
	An encoder used in a digital channel which provides a random sequence of bits.

5330500-Kompyuter injiniringi (“Kompyuter tizimlarini loyihalash”, “Amaliy dasturiy vositalarni loyihalash”, “Axborot va multimedia texnologiyalari”, “Axborot xavfsizligi, kriptografiya va kriptozanaliz”) magistratura mutaxassisligining “Axborot xavfsizligi, kriptografiya va kriptozanaliz” ixtisosligi talabalari uchun o‘quv qo‘llanma

AXT kafedrasining 2017 yil “15” mart,
(15 – sonli bayonnoma) majlisida
ko‘rib chiqildi va chop etishga tavsiyalandi

AX fakultetining ilmiy-uslubiy Kengashida
ko‘rib chiqildi va chop etishga tavsiyalandi
2017 yil “17” mart, 7 – sonli bayonnoma

Muxammad al-Xorazmiy nomidagi TATU
ilmiy-uslubiy Kengashida ko‘rib
chiqildi va chop etishga tavsiyalandi
2017 yil “24” mart, 6(97) – sonli bayonnoma

Mualliflar: S.K. Ganiev
SH.R. G‘ulomov

Taqrizchilar: A.A. Nigmanov
R.P. Abduraxmonov

Mas’ul muxarrir:

Korrektor: