

“SIKLIK KODLAR VA ULARNING BCH HAMDA REED–SOLOMON KODLARI BILAN BOG‘LIQLIGI”

Halilov.M.M

Raxmatxonov Boboxo'ja Shukurulloxon o'g'li
Farg'ona Davlat Texnika Universiteti talabasi

Annotatsiya: Ushbu maqolada siklik kodlarning matematik asoslari, ularning xatolarni aniqlash va tuzatishdagi roli hamda BCH va Reed–Solomon (RS) kodlari bilan o‘zaro bog‘liqligi tahlil qilinadi. Avvalo siklik kodlarning polinomial tuzilishi, generator polinomini tanlash jarayoni va kodlash-dekodlash mexanizmlari yoritiladi. Shundan so‘ng BCH va Reed–Solomon kodlarining siklik kodlar asosida qurilishi, ularning farqlari va afzalliklari ilmiy jihatdan izohlanadi. Tadqiqot natijalari ushbu kodlarning zamonaviy raqamli aloqa tizimlarida yuqori ishonchlilikni ta’minlashdagi o‘rnini ko‘rsatadi.

Kalit so‘zlar: Siklik kodlar, BCH kodlari, Reed–Solomon, polinomlar, generator polinomi, xatolarni tuzatish, kodlash, dekodlash.

Аннотация: В данной статье рассматриваются математические основы циклических кодов, их роль в обнаружении и исправлении ошибок, а также взаимосвязь с кодами BCH и Рида–Соломона. Описывается полиномиальная структура циклических кодов, выбор порождающего полинома и механизмы кодирования и декодирования. Далее анализируется построение BCH и RS-кодов на основе циклических кодов, их различия и преимущества. Результаты исследования демонстрируют важность данных кодов в современных цифровых коммуникационных системах.

Ключевые слова: Циклические коды, BCH-коды, коды Рида–Соломона, полиномы, порождающий полином, исправление ошибок, кодирование, декодирование.

Annotation: This article explores the mathematical foundations of cyclic codes, their role in error detection and correction, and their relationship with BCH and Reed–Solomon (RS) codes. The polynomial structure of cyclic codes, generator polynomial selection, and encoding–decoding mechanisms are discussed. Furthermore, the construction of BCH and RS codes based on cyclic code principles, their differences, and advantages are analyzed. The findings highlight the importance of these codes in ensuring high reliability in modern digital communication systems.

Keywords: Cyclic codes, BCH codes, Reed–Solomon codes, polynomials, generator polynomial, error correction, encoding, decoding.

KIRISH



Raqamli aloqa tizimlarida ma'lumotlarni ishonchli uzatish bugungi kunda eng muhim masalalardan biridir. Uzatilayotgan signal turli shovqinlar, interferensiyalar yoki fizik muhitning xususiyatlari sababli buzilishi, ya'ni bitlar noto'g'ri qabul qilinishi mumkin. Shu sababli xatolarni aniqlash va ularni avtomatik tuzatish imkonini beruvchi maxsus kodlash usullari ishlab chiqilgan. Ular orasida siklik kodlar, BCH kodlari va Reed–Solomon (RS) kodlari eng ko'p qo'llaniladigan, ishonchliligi yuqori bo'lgan kodlar sirasiga kiradi.

Siklik kodlar polinomial algebra tamoyillariga asoslangan bo'lib, ularning asosiy afzalligi — kod so'zlarini siklik siljitish xususiyatining saqlanishidadir. Bu xususiyat kodlarni apparat darajasida sodda, tez va samarali tarzda amalga oshirishga imkon beradi. Aynan shu jihatlar siklik kodlar oilasidan kelib chiqqan BCH va Reed–Solomon kodlarining yaratilishiga asos bo'lgan.

BCH kodlari siklik kodlarning umumlashtirilgan shakli bo'lib, katta miqdordagi xatolarni aniq matematik asoslar bilan tuzatish imkoniyatiga ega. Reed–Solomon kodlari esa BCH kodlarining kengaytirilgan ko'rinishi bo'lib, blokli raqamli tizimlarda, ayniqsa, ommaviy axborot saqlash vositalari (CD, DVD), fazoviy aloqa, Wi-Fi va mobil aloqa texnologiyalarida keng qo'llaniladi. Ushbu kodlar turli xildagi xatolar, jumladan, ketma-ket bitlar buzilishi (burst error) uchun juda samarali hisoblanadi.

Mazkur ishda siklik kodlarning nazariy asoslari, ularning BCH va RS kodlari bilan bog'liqligi, bu kodlarning matematik modeli hamda qo'llanilish sohalari tahlil qilinadi. Shuningdek, har uchala kodning afzallik va kamchiliklari solishtirilib, zamonaviy aloqa tizimlarida qaysi sharoitda qaysi kod samaraliroq bo'lishi ilmiy asoslarda yoritiladi.

KIRISH

Siklik kodlar xatolarni aniqlash va tuzatish imkoniyatiga ega bo'lgan chiziqli blokli kodlar sinfiga kiradi. Ularning asosiy farqlovchi xususiyati shundaki, har qanday haqiqiy kod so'zi siklik ravishda bir bitga siljirilganda ham yana kod so'zi hosil bo'ladi. Bu xususiyat generator polinomiga asoslangan bo'lib, kodlash jarayonini sodda va apparat jihatdan qulay qiladi. Siklik kodlar ko'pincha Galois maydoni $GF(2)$ yoki umumiy holatda $GF(q)$ ustida quriladi. Kodning asosiy elementlari — generator polinomi, tekshiruv polinomi va sindrom hisoblash mexanizmlaridir. Ma'lumotlar polinom ko'rinishida ifodalanib, generator polinomiga bo'linadi va natijada xatolarga sezgir bo'lmagan kod so'zi hosil qilinadi.

Siklik kodlarning ahamiyatli jihat shundaki, ular ko'plab xatolarni, ayniqsa ketma-ket ravishda yuzaga kelgan xatolarni aniqlashda yuqori samaradorlikka ega. Kodlash jarayoni polinomial bo'lishi sababli, apparat darajasidagi realizatsiyalar – registrlar, ko'paytirgichlar, bo'luvchilar yordamida juda tez amalga oshiriladi. Shu sababli siklik

kodlar kompyuter tarmoqlari, simsiz aloqa, ma'lumot uzatish protokollari va disk tizimlarida keng qo'llaniladi.

BCH kodlari siklik kodlarning kengaytirilgan matematik modeli bo'lib, chastotalar maydonidagi aniq belgilar to'plamiga asoslanadi. BCH kodlarining asosiy afzalligi — istalgan oldindan belgilangan miqdordagi xatolarni tuzatish imkoniyatidir. Ya'ni, BCH kodlari ko'p xatoliklarni matematik jihatdan kafolatlangan darajada tuzatadi. Ularning generator polinomi Galois maydonidagi ildizlar orqali aniqlanadi. BCH kodlari odatda 2 va undan ortiq xatolar mavjud bo'lgan bloklarda ishlatiladi. Bu ularni ayniqsa telekommunikatsiya kanallarida, shovqin darajasi yuqori bo'lgan uzatish muhitlarida juda foydali qiladi.

Reed–Solomon kodlari esa BCH kodlarining yanada umumlashtirilgan ko'rinishi bo'lib, ko'pliklar ustida emas, balki yaxlitar maydon $GF(2^m)$ ustida quriladi. Bu esa RS kodlariga bittadan ortiq ketma-ket buzilgan simvollarni tuzatish imkonini beradi. Bunda bitta simvol odatda bir nechta bitdan tashkil topadi. RS kodlari ayniqsa “burst error” deb ataluvchi uzluksiz buzilishlarga qarshi nihoyatda samarali bo'ladi. Shu sababli RS kodlari multimedia fayllar, optik disklar (CD, DVD), raqamli televideniye, WiMAX, LTE kabi tizimlarda asosiy kodlash usuli sifatida qo'llaniladi.[1]

Siklik kodlar, BCH va Reed–Solomon kodlarining bog'liqligi ularning umumiy polinomial strukturasida namoyon bo'ladi. Har uchala kod ham generator polinomi yordamida quriladi, sindrom orqali xatoni aniqlaydi va Galois maydonlaridagi arifmetikaga asoslanadi. Farqi shundaki, siklik kodlar oddiyroq va bir nechta xatoni aniqlashda samarali, BCH kodlari ko'p xatoliklarni matematik kafolat bilan tuzatadi, RS kodlari esa simvol darajasidagi uzluksiz buzilishlarni bartaraf etishda eng optimal hisoblanadi.

Shu bilan birga, ushbu kodlar orasidagi yana bir muhim farq — dekodlash algoritmlarining murakkabligida namoyon bo'ladi. Siklik kodlarni dekodlash nisbatan sodda bo'lsa, BCH va RS kodlari Berlekamp–Massey, Forney yoki Euclid algoritmlaridan foydalanadi. Bu kodlarni amaliyotda qo'llash uchun maxsus apparat yoki dasturiy realizatsiyalar talab qilinadi. Biroq, ularning yuqori ishonchliligi telekommunikatsiya va ma'lumotlarni uzatishda bu murakkablikni oqlaydi.

METODOLOGIYA

Ushbu tadqiqotda siklik kodlar, BCH kodlari va Reed–Solomon kodlarining matematik modeli, ularning ishlash prinsiplari hamda o'zaro bog'liqligi tizimli yondashuv orqali o'rganildi. Metodologiya polinomial algebra, Galois maydonlari va blokli kodlash nazariyasiga tayangan holda qurildi. Tadqiqotning asosiy bosqichlari quyidagilardan iborat bo'ldi:

Birinchi bosqichda siklik kodlarning generator polinomi, tekshiruv polinomi va sindrom hisoblash mexanizmlari tahlil qilindi. Kodlash jarayoni $GF(2)$ maydonidagi polinomial ko'paytirish va bo'lish amallari orqali modellashtirildi. Siklik kodlarning xatolarni aniqlashdagi samaradorligi turli uzunlikdagi kod so'zlari yordamida nazariy jihatdan baholandi.

Ikkinchi bosqichda BCH kodlarining strukturasini tashkil etuvchi Galois maydoni elementlari, ularning minimal polinomi va ildizlarga asoslangan generator polinomini qurish usullari o'rganildi. Tadqiqotda BCH kodlarining aniqlangan xatolar soniga nisbatan tuzatish imkoniyati matematik yondashuv orqali asoslab berildi. Dekodlash jarayonini modellashtirish davomida Berlekamp–Massey va Euclid algoritmlarining ishlash tamoyillari tahlil qilindi.

Uchinchi bosqichda Reed–Solomon kodlarining $GF(2^m)$ maydoni ustida qurilish tamoyillari o'rganildi. RS kodlarining simvol darajasidagi xatolarni tuzatish imkoniyatlari, ularning BCH kodlari bilan bog'liq umumiy polinomial modeli va farqlari chuqur tahlil qilindi. Praktik misollar asosida RS kodlarining ketma-ket buzilishlarni tuzatishdagi samaradorligi matematik jihatdan modellashtirildi.

To'rtinchi bosqichda uchala kodning amaliy qo'llanilish samaradorligini solishtirish uchun nazariy tahlil, formulalar asosida baholash, bit xatolik ehtimoli (BER) bo'yicha taqqoslash kabi metodlardan foydalanildi. Bu jarayonda kanal shovqini, kod uzunligi, xatolar chastotasi va tuzatish darajasi kabi mezonlar tahlil

Kod turi	Ta'rifi	Ishlash printsiplari
Siklik kodlar	Kod so'zidagi bitlar aylantirilganda (shift) yana kod so'zi hosil bo'ladigan chiziqli kodlar.	Polinomlar ustida mod 2 bo'yicha amallar bajariladi.
BCH kodlari	Berilgan minimal distance (d) ga ega bo'lishi kafolatlangan maxsus siklik kodlar.	$GF(2^m)$ maydonidagi ildizlardan foydalaniladi.
Reed–Solomon kodlari	Simvol uzunligi bitta bittan emas, balki bitta blokdan iborat bo'lgan kuchli tahrirlovchi kodlar.	$GF(2^m)$ maydonidagi polinomlarni baholashga asoslanadi.

qilindi.[2]

O'tkazilgan tahlillar asosida siklik kodlar, BCH va Reed–Solomon kodlarining o'zaro bog'liqligi, afzalliklari hamda qo'llanilish sohasi ilmiy asoslangan tarzda belgilandi. Natijalar keyingi bo'limlarda umumlashtirildi.

1-jadval

2-jadval

Xususiyat	Siklik kodlar	BCH kodlari	Reed–Solomon kodlari
Tuziqlishi	Oddiy	Murakkabroq	Eng murakkab
Asosi	Polinomlar	Polinom ildizlari	Polinom baholash
O'zgarish	Bitlar aylanishiga invariant	Aniqlangan masofa bilan	Simvolga asoslangan
Minimal masofa	Har doim yuqori emas	Kafolatlangan	juda yuqori ($d = n - k + 1$)

3-jadval

Kod turi	Xato turlari	Tuzatish imkoniyati
Siklik kodlar	Bitta va ketma-ket bit xatosi	Cheklangan
BCH kodlari	Bir nechta tarqoq bit xatolari	t ta xatoni tuzatadi
Reed–Solomon kodlari	Butun blok (symbol) xatolari	$t = (n - k) / 2$ simvol tuzatadi

TAHLIL

O'tkazilgan tadqiqot va tahlillar shuni ko'rsatdiki, siklik kodlar, BCH va Reed–Solomon (RS) kodlari ma'lumotlarni uzatishda xatolarni aniqlash va tuzatishda samarali mexanizmlarni ta'minlaydi. Jadval ma'lumotlaridan ko'rinib turibdiki, ularning afzalliklari va cheklovlari turlicha, va ular qo'llaniladigan tizim shartlariga bog'liq.

Siklik kodlar apparat jihatdan eng sodda va tez ishlaydigan kodlar bo'lib, bitlar aylanishi xususiyatiga ega. Bu kodlar bir yoki bir nechta bit xatolarini aniqlashda samarali bo'lib, CRC tekshiruvlari va zaxira xotira tizimlarida keng qo'llaniladi. Biroq, ular ko'p xatoliklarni tuzatishda cheklangan imkoniyatga ega, shu sababli murakkab tizimlarda yetarli samaradorlikni ta'minlamaydi.

BCH kodlari esa siklik kodlarning kengaytirilgan varianti bo'lib, ma'lum sonli xatolarni matematik kafolat bilan tuzatish imkonini beradi. Tadqiqot natijalari ko'rsatdiki, BCH kodlari kanal shovqiniga nisbatan chidamliligi yuqori va bit xatolik ehtimoli (BER) past tizimlarda juda samarali. Dekodlash jarayonlari murakkab bo'lsa-da, Berlekamp–Massey algoritmi va sindrom hisoblash metodlari yordamida tizimlarda keng qo'llaniladi.

Reed–Solomon kodlari esa eng yuqori samaradorlikni ta'minlaydi, ayniqsa ketma-ket simvol xatolari ("burst error") mavjud bo'lgan holatlarda. Tadqiqot natijalari shuni ko'rsatdiki, RS kodlari multimedia fayllar, kosmik aloqa va diskli saqlash tizimlarida yuqori ishonchlilikni ta'minlaydi. RS kodlari simvol darajasidagi xatolarni tuzatish imkoniyatiga ega bo'lgani uchun ular BCH kodlariga nisbatan "burst error"larga nisbatan kuchliroq.[3]

Tahlil shuni ko'rsatadiki, kod tanlashda tizimning talab qilinadigan xato tuzatish qobiliyati, kanal shovqin darajasi, apparat va hisoblash xarajatlari hisobga olinishi lozim. Oddiy tizimlar uchun siklik kodlar yetarli bo'lsa, yuqori sifat va ishonchlilik talab qilinadigan tizimlarda BCH va RS kodlari afzal hisoblanadi. Shu bilan birga, uchala kod turi bir-biri bilan bog'liq matematik asoslarga ega bo'lib, ularning apparat yoki dasturiy realizatsiyalari polinomial algebra va Galois maydonlariga tayangan holda amalga oshiriladi.

NATIJALAR

O'tkazilgan tadqiqotlar va tahlillar asosida quyidagi natijalarga erishildi:

1. **Siklik kodlar** oddiy va tezkor kodlash imkonini beradi. Bit xatolarini aniqlashda samarali bo'lsa-da, ko'p xatolarni tuzatishda cheklangan. Ular CRC tekshiruvlari va apparat jihatdan sodda tizimlarda samarali qo'llaniladi.
2. **BCH kodlari** ma'lum miqdordagi xatolarni matematik kafolat bilan tuzatadi. Bit xatolik ehtimoli (BER) past tizimlarda ishlatilishi ma'qul. Ular telekommunikatsiya tizimlari va zaxira xotira qurilmalarida keng qo'llanadi.
3. **Reed–Solomon kodlari** simvol darajasidagi ketma-ket xatolarni samarali tuzatadi. Multimedia fayllar, optik disklar, kosmik va mobil aloqa tizimlarida afzal kodlash usuli hisoblanadi.

Natijalar shuni ko'rsatdiki, kodlarni tanlash tizimning talablariga bog'liq: sodda tizimlar uchun siklik kodlar, bit darajasida ko'p xatolarni tuzatish zarur bo'lsa BCH kodlari, uzluksiz xatolar bo'lsa RS kodlari samaraliroq.[4]

4-jadval

Kod turi	Xato aniqlash / tuzatish	Ishlash tezligi	Qo'llanilish sohasi	Afzalliklar	Kamchiliklar

Siklik kodlar	Bitta va ketma-ket bit xatolari	Juda tez	CRC, apparat tekshiruvlari	Sodda, apparatga mos	Ko'p xatolarni tuzatolmaydi
BCH kodlari	ta tarqoq bit xatolarin i tuzatadi	O'rtacha	WiFi, CD/DVD, telekommunikatsiya	Kafolatlangan xato tuzatish	Murakkab dekodlash
Reed-Solomon kodlari	ta simvol ketma-ket xatolarin i tuzatadi	Nisbatan sekin	QR-kodlar, multimedia, kosmik aloqa	"Burst error"larga samarali	Murakkab arifmetika, katta hisoblash

XULOSA

Ushbu tadqiqot natijalariga ko'ra, siklik kodlar, BCH kodlari va Reed-Solomon kodlari zamonaviy raqamli aloqa tizimlarida xatolarni aniqlash va tuzatishda muhim ahamiyatga ega ekanligi tasdiqlandi. Siklik kodlar apparat jihatdan sodda va tez ishlash xususiyati bilan ajralib turadi, lekin ko'p xatolarni tuzatishda cheklangan imkoniyatga ega. Shu sababli ular asosan CRC tekshiruvlari, oddiy apparat tizimlar va zaxira xotira qurilmalarida samarali qo'llaniladi. BCH kodlari ko'p bitli xatolarni matematik kafolat bilan tuzatish imkoniyatiga ega. Ular telekommunikatsiya tizimlarida, Wi-Fi va CD/DVD kabi ma'lumot uzatish tizimlarida yuqori ishonchlilikni ta'minlaydi. BCH kodlari murakkabroq bo'lsa-da, apparat va dasturiy realizatsiyasi orqali yuqori samaradorlikka erishish mumkin.

Reed-Solomon kodlari esa simvol darajasidagi ketma-ket xatolarni samarali tuzatadi. Multimedia fayllar, optik disklar, QR-kodlar, kosmik va mobil aloqa tizimlarida qo'llanilishi ularning "burst error"larga nisbatan mukammal samaradorligini ko'rsatadi.

Tahlil va natijalar shuni ko'rsatdiki, kodlarni tanlash tizimning talablariga bog'liq bo'lib, sodda tizimlar uchun siklik kodlar, bit darajasidagi ko'p xatolarni tuzatish zarur bo'lsa BCH kodlari, ketma-ket xatolarni tuzatish zarur bo'lsa Reed-Solomon kodlari eng samarali hisoblanadi.

Shu bilan birga, uchala kod turi matematik jihatdan bir-biri bilan bog'liq bo'lib, polinomial algebra va Galois maydonlari asosida ishlaydi. Bu ularning apparat yoki dasturiy realizatsiyasini ilmiy va amaliy jihatdan asoslash imkonini beradi. Natijada,

raqamli aloqa tizimlarida ishonchlilikni oshirish uchun kodlash algoritmlarini to'g'ri tanlash muhim ahamiyat kasb etadi.

FOYDALANILGAN ADABIYOTLAR

1. Peterson, W. W., & Weldon, E. J. "Error-Correcting Codes." MIT Press, 2nd edition, 1972.(Siklik kodlar, BCH va RS kodlarining nazariy asoslarini eng batafsil yoritgan klassik manba.)
2. Blahut, R. E. "Theory and Practice of Error Control Codes." Addison-Wesley, 1983.(Galois maydonlari, BCH va Reed–Solomon kodlari uchun kodlash va dekodlash algoritmlarining to'liq bayoni.)
3. Lin, S., & Costello, D. J. "Error Control Coding: Fundamentals and Applications." Prentice Hall, 2004.(Siklik kodlar, BCH kodlari va RS kodlarining amaliy qo'llanishlari va apparat implementatsiyasi.)
4. MacWilliams, F. J., & Sloane, N. J. A. "The Theory of Error-Correcting Codes." North-Holland, 1977.(Kodlash nazariyasining fundamental matematik asoslari, ayniqsa Galois maydonlari uchun.)