

Дәріс 10. Циклдік кодтардың сипаттамасы. Кодтау және декодтау алгоритмдерін іске асыру

Дәріс жоспары.

1. Циклдік кодтардың жалпы анықтамасы
2. Көпмүшелер арқылы кодты сипаттау идеясы
3. Генератор көпмүшесінің рөлі
4. Кодтау процесінің мәні

Циклдік кодтардың жалпы анықтамасы

Циклдік кодтар - ақпараттық хабарламаларды қателерден қорғауға арналған тиімді әдістердің бірі. Бұл кодтардың басты ерекшелігі — егер бір кодтық комбинация кодтың құрамына кірсе, онда оның циклдік түрде ығысқан барлық түрлері де сол кодқа жатады. Мұндай қасиет кодты аппараттық және бағдарламалық түрде оңай жүзеге асыруға мүмкіндік береді.

Циклдік кодтар дискретті сигналдарды немесе деректерді қателерден қорғау мақсатында қолданылады. Байланыс арнасы арқылы ақпарат жіберу кезінде сигналға әртүрлі шу әсер етіп, кейбір биттердің бұзылуына әкелуі мүмкін. Осындай жағдайда циклдік кодтар деректердің тұтастығын қамтамасыз етіп, қателерді анықтау немесе түзетуге мүмкіндік береді.

Бұл кодтардың математикалық негізі екілік өрістегі арифметикаға сүйенеді. Әрбір кодтық комбинация биттер тізбегі түрінде көрсетіліп, оны екілік көпмүше ретінде қарастыруға болады. Мұндай тәсіл циклдік кодтардың қасиеттерін зерттеуді және кодтау операцияларын орындауды жеңілдетеді.

Циклдік кодтың құрылымы арнайы генератор арқылы анықталады. Генератор деп аталатын көпмүше кодтың ережесін белгілейді және барлық кодтық комбинациялардың дұрыс құрылуын қамтамасыз етеді. Генератор көпмүшесі негізінде әрбір ақпараттық хабарламаға сәйкес бақылау биттері есептеледі. Бұл бақылау биттері хабарламаның соңына қосылып, кодтық комбинация құрайды.

Циклдік кодтарда кодтау мен декодтау процестері логикалық операциялар арқылы жүзеге асырылады. Мұндай операциялар көбінесе екілік қосу, яғни XOR логикалық функциясы түрінде орындалады. Сондықтан циклдік кодтарды микроконтроллерлерде, сандық схемаларда және бағдарламалық жүйелерде оңай іске асыруға болады.

Циклдік кодтардың басты артықшылығы – олардың қарапайымдылығы мен сенімділігі. Олар аз есептеу ресурстарын талап етеді, жылдам жұмыс істейді және аппараттық деңгейде оңай бейімделеді. Осы себепті циклдік кодтар байланыс жүйелерінде, компьютерлік желілерде, деректерді сақтау құрылғыларында және басқа да ақпараттық жүйелерде кеңінен қолданылады.

Сонымен, циклдік кодтардың жалпы анықтамасы бойынша, бұл – ақпараттық хабарламаларды қателерден қорғау үшін қолданылатын, кодтық комбинациялардың циклдік ығысу қасиетіне негізделген сызықтық кодтардың бір түрі. Олардың негізгі мақсаты – ақпараттың тұтастығын сақтау және деректерді дұрыс жеткізуді қамтамасыз ету.

Циклдік кодтар сызықтық блоктық кодтардың түріне жатады. Әрбір кодтық комбинация белгілі бір ұзындықтағы биттер тізбегінен тұрады. Циклдік кодтарда бұл биттер тізбегі арнайы ережелерге сәйкес құралады және циклдік ығыстыру кезінде де кодтың құрылымы бұзылмайды.

Циклдік кодты анықтау үшін арнайы генератор деп аталатын кодтық сипаттама қолданылады. Генератор белгілі бір заңдылық бойынша биттерді тексеруге және қосымша бақылау биттерін есептеуге арналған. Осы бақылау биттері арқылы қабылданған хабарламаның дұрыстығы тексеріледі.

Кодтау процесі ақпараттық биттерден тұратын хабарламаны генератор ережесіне сай толықтыру арқылы жүргізіледі. Хабарлама соңына бақылау биттері қосылады. Бұл бақылау биттері деректердің дұрыс немесе бұзылған күйде жеткізілгенін анықтауға көмектеседі.

Мысалы, егер бастапқы хабарлама төрт биттен тұрса, ал код ұзындығы жеті бит болуы керек болса, онда үш бақылау биті есептеледі. Нәтижесінде жеті биттік кодтық комбинация алынады. Бұл комбинация қабылдау кезінде тексеріледі және қажет болған жағдайда қате анықталады.

Көпмүшелер арқылы кодты сипаттау идеясы

Циклдік кодтарды аппараттық түрде жүзеге асыру үшін ығысу регистрі қолданылады. Мұндай құрылғы биттерді бір-бірімен байланыстырып, қажетті бақылау биттерін автоматты түрде есептейді. Регистр ішіндегі логикалық байланыстар генератор сипаттамасына сәйкес орнатылады.

Декодтау процесі қабылданған кодтық комбинацияның дұрыстығын тексеру мақсатында жүргізіледі. Қабылданған хабарлама генератор ережесіне сай қайта өңделеді. Егер нәтиже дұрыс болса, яғни бақылау биттері сәйкес келсе, хабарламада қате жоқ деп есептеледі.

Қабылданған хабарлама дұрыс болмаса, яғни есептелген бақылау мәндері сәйкес келмесе, онда жүйе қате туралы хабар береді. Мұндай жағдайларда кодтық жүйе қателердің бар екенін ғана емес, олардың орналасқан орнын да анықтай алады.

Кейбір циклдік кодтар, мысалы CRC кодтары, тек қателерді анықтауға арналған. Олар ақпаратты түзетпейді, бірақ деректердің тұтастығын тексеруде жоғары дәлдік береді. CRC кодтары желілік протоколдарда, файл алмасу жүйелерінде және электрондық құрылғыларда кеңінен қолданылады.

Қателерді түзету үшін циклдік кодтардың кеңейтілген түрлері қолданылады. Мұндай кодтар бірнеше биттің бұзылуын да анықтап, оларды бастапқы қалпына келтіре алады. Бұл тәсіл спутниктік байланыс пен деректерді сақтау жүйелерінде кеңінен пайдаланылады.

Бағдарламалық іске асыруда циклдік кодтар биттік операциялар арқылы орындалады. Көптеген микроконтроллерлер мен ендірілген жүйелерде мұндай операциялар тез және тиімді жұмыс істейді. Сондықтан циклдік кодтар ресурсы шектеулі құрылғыларда жиі қолданылады.

Генератор көпмүшесінің рөлі

Циклдік кодтардың басты артықшылығы - олардың қарапайым құрылымы және аппараттық іске асырудың жеңілдігі. Олар деректерді

қорғаудың сенімді және тиімді әдісін қамтамасыз етеді. Сонымен қатар, кодтың жұмыс жылдамдығы жоғары, бұл нақты уақыттағы жүйелер үшін маңызды.

Қазіргі уақытта циклдік кодтар телекоммуникация, компьютерлік желілер, радиобайланыс, өнеркәсіптік автоматтандыру және көліктік жүйелер сияқты көптеген салаларда қолданылады. Әсіресе, CRC түріндегі циклдік кодтар деректердің тұтастығын бақылауда негізгі стандартқа айналған.

Қорытындылай келе, циклдік кодтар – ақпараттың сенімділігін арттыруға арналған маңызды құрал. Олар байланыс жүйелерінде қателердің әсерін азайтады және деректердің дұрыстығын қамтамасыз етеді. Мұндай кодтарды дұрыс қолдану ақпараттық қауіпсіздіктің маңызды бөлігі болып табылады.

Циклдік кодтардың теориясы мен тәжірибелік іске асырылуын білу болашақ инженерлер мен бағдарламашылар үшін маңызды. Бұл білім арқылы қателерді анықтайтын және түзететін сенімді байланыс жүйелерін құруға болады.

Кодтау процесінің мәні

1. Кодтау алгоритмі:

Алгоритм Encode(бастапқы_хабарлама, генератор):

1. Хабарламаны бірнеше нөлдік бит қосу арқылы кеңейт
2. Генератор ережесі бойынша бақылау биттерін есепте
3. Бақылау биттерін хабарламаның соңына қос
4. Нәтижесінде кодталған хабарлама алынады
5. Кодталған хабарламаны қайтар

2. Декодтау алгоритмі:

Алгоритм Decode(қабылданған_код, генератор):

1. Қабылданған кодты генератор ережесі бойынша тексер
2. Егер тексеру нәтижесі дұрыс болса:
"Қате жоқ" деп хабарла
Әйтпесе:
"Қате анықталды" деп хабарла
3. Нәтижені қайтар

3. CRC қолдану мысалы:

Хабарлама = "11010011101100"

Генератор = "1011"

Кодталған = Encode(Хабарлама, Генератор)

Нәтиже = Decode(Кодталған, Генератор)

Экранға шығару: Нәтиже

1. Кодтау алгоритмі (Encoding)

Алгоритм Encode(message_bits, generator_bits, n, k):

1. $m \leftarrow \text{message_bits}$
2. $g \leftarrow \text{generator_bits}$
3. $\text{message_shifted} \leftarrow m \ll (n - k) \quad // m(x) \cdot x^{(n-k)}$
4. $\text{remainder} \leftarrow \text{DivideModulo}(\text{message_shifted}, g)$

5. codeword $\leftarrow$ message_shifted XOR remainder
6. Қайтар: codeword

Функция DivideModulo(dividend, divisor):

- while ұзындығы(dividend) $\geq$ ұзындығы(divisor):
 - shift $\leftarrow$ позиция айырмасы
 - dividend $\leftarrow$ dividend XOR (divisor $\ll$ shift)
- Қайтар: dividend (қалдық)

2. Декодтау алгоритмі (Decoding)

Алгоритм Decode(received_bits, generator_bits):

1. r $\leftarrow$ received_bits
2. g $\leftarrow$ generator_bits
3. syndrome $\leftarrow$ DivideModulo(r, g)
4. Егер syndrome == 0 болса:
 - Шығару: "Қате жоқ"
- Әйтпесе:
 - Шығару: "Қате анықталды"

3. CRC қолдану мысалы

message = 11010011101100

generator = 1011

n = ұзындығы(message) + ұзындығы(generator) - 1

codeword = Encode(message, generator, n, ұзындығы(message))

print("Кодталған хабарлама:", codeword)

ҚОРЫТЫНДЫ

Циклдік кодтар – ақпаратты қателерден қорғаудың ең тиімді және кеңінен қолданылатын әдістерінің бірі. Олар сызықтық блоктық кодтардың ерекше түрі болып саналады және өздерінің циклдік қасиеттері арқылы кодтау мен декодтау операцияларын қарапайым әрі тез орындауға мүмкіндік береді. Циклдік кодтардың басты ерекшелігі – кодтық комбинацияның кез келген циклдік ығысуы да сол кодтың құрамына енуі. Бұл қасиет аппараттық және бағдарламалық іске асыруды едәуір жеңілдетеді.

Кодтау процесінде ақпараттық хабарлама генератордың ережесіне сәйкес өңделіп, соңына бақылау биттері қосылады. Бұл бақылау биттері хабарламаның дұрыстығын тексеру үшін қажет. Декодтау кезінде қабылданған кодтық комбинация генератор сипаттамасына сай тексеріліп, хабарламада қате бар-жоғы анықталады. Егер бақылау мәндері сәйкес келсе – хабарлама дұрыс жеткізілді, ал сәйкес келмесе – қате анықталғанын білдіреді.

Циклдік кодтар тек қателерді анықтап қана қоймай, кейбір жағдайларда оларды түзете де алады. Мұндай кодтардың жетілдірілген түрлеріне БЧХ және Рида–Соломон кодтары жатады. Бұл кодтар бірнеше биттік қателерді де анықтап, ақпаратты бастапқы қалпына келтіруге мүмкіндік береді. Осы қасиеттерінің арқасында циклдік кодтар телекоммуникациялық жүйелерде,

желілік байланыстарда, ақпарат сақтау құрылғыларында және өнеркәсіптік автоматтандыруда кеңінен қолданылады.

Бағдарламалық және аппараттық іске асыру тұрғысынан алғанда, циклдік кодтар өте тиімді. Олар аз есептеу ресурстарын талап етеді және биттік деңгейде жұмыс істейтіндіктен, микроконтроллерлер мен ендірілген жүйелер үшін оңтайлы шешім болып табылады. Мысалы, CRC кодтары нақты уақыт режимінде қателерді анықтап, деректердің тұтастығын қамтамасыз етуге мүмкіндік береді.

Қазіргі ақпараттық қоғамда деректердің сенімді берілуі мен сақталуы – басты міндеттердің бірі. Сол себепті циклдік кодтар ақпараттық қауіпсіздік саласында маңызды рөл атқарады. Олар деректердің бұзылуын, жоғалуын немесе өзгертілуін ерте анықтап, жүйенің жалпы сенімділігін арттырады.

Қорыта айтқанда, циклдік кодтар – ақпаратты қорғаудың математикалық негізделген және практикалық тұрғыда дәлелденген әдісі. Бұл кодтарды меңгеру болашақ инженерлер мен бағдарламашыларға деректердің дұрыстығын қамтамасыз ететін заманауи байланыс жүйелерін, криптографиялық және IoT құрылғыларын сенімді жобалауға мүмкіндік береді. Циклдік кодтар бүгінгі цифрлық әлемнің тұрақтылығын қамтамасыз ететін маңызды технологиялардың бірі болып қала береді.

Пайдаланылған әдебиеттер тізімі

1. Шеннон, К. Э. *Математикалық коммуникация теориясы*. — М.: Наука, 1963.
2. Хаффман, Д. А. *A Method for the Construction of Minimum-Redundancy Codes*. — Proceedings of the IRE, 1952.
3. Фано, Р. М. *The Transmission of Information: A Statistical Theory of Communications*. — Cambridge, MIT Press, 1961.
4. Коберн, Д., Трембле, Г. *Теория кодирования и ее приложения*. — М.: Мир, 1982.
5. Мауо Венбо. *Прикладная криптография. Протоколы, алгоритмы и исходные тексты на языке С*. — М.: Триумф, 2004.