ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ

Қ.И. Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті

Ақпараттық және телекоммуникациялық технологиялар институты

Электроника, телекоммуникациялар және ғарыштық технологиялар кафедрасы

Темирханов О. А.

Бөгеуілге тұрақты LBC кодының қолданылуының анализі

ДИПЛОМДЫҚ ЖҰМЫС

5В071900 – «Радиотехника, электроника және телекоммуникация» мамандығы

Алматы 2019

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ

Қ.И. Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті

Ақпараттық және телекоммуникациялық технологиялар институты

Электроника, телекоммуникациялар және ғарыштық технологиялар кафедрасы

ҚОРҒАУҒА ЖІБЕРІЛДІ
Кафедра меңгерушісі
техн. ғыл. канд-ы
_____Е. Т. Таштай
«26» 04 2019 ж.

ДИПЛОМДЫҚ ЖҰМЫС

Тақырыбы: «Бөгеуілге тұрақты LBC кодының қолданылуының анализі»

5В071900 – «Радиотехника, электроника және телекоммуникация» мамандығы

Орындаған: Темирханов О. А.

Пікір беруші
ҚазҰАУ, ЭҮжА каф. меңгерушісі
доктор PhD.,
қауымдастырылған профессор
_____Ж. С. Шыныбай
«25» 04 2019 ж.

Ғылыми жетекші
ЭТжҒТ кафедрасының
техн. ғыл. канд-ы
қауымдастырылған профессор
_____Л. Б. Илипбаева
«24» 04 2019 ж.

Алматы 2019

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ

Қ.И. Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті

Ақпараттық және телекоммуникациялық технологиялар институты

Электроника, телекоммуникация және ғарыштық технологиялар кафедрасы

5В071900 – Радиотехника, электроника және телекоммуникация

ҚОРҒАУҒА ЖІБЕРІЛДІ
Кафедра меңгерушісі,
техн.ғыл.канд.
_____Е.Таштай
«_20_» _01_____2019 ж.

Дипломдық жұмыс орындауға
ТАПСЫРМА

Білім алушы *Темирханов Орайбек Абдыхамитулы*
Тақырыбы «Бөгеуілге тұрақты LBC кодының қолданылуының анализы»
Университет ректорының «*16*» *қазан 2018 ж. № 1162-б* бұйрығымен бекітілген.
Аяқталған жұмысты тапсыру мерзімі "25" сәуір 2019 ж.
Дипломдық жұмыстың бастапқы берілістері:
1) GF(2) жиынының (64, 32) екілік коды;
2) (6, 2) сызықты блокты кодының құраушы матрицасы;
3) $GF(2^2)$ өрісіндегі $P(X)=X^3+X+1$ құраушы полиномы;
4) Құрылымдық анализ жүргізу тәсілдері;
Дипломдық жұмыста қарастырылатын мәселелер тізімі:
а) Бөгеуілге тұрақты LBC кодының құрылымына әдебиеттік шолу;
ә) Сызықты блокты кодты құру әдістерін салыстырмалы сараптау;
б) LBC кодының іске асырылуының артықшылығын бағалау әдістеріне шолу;
Сызбалық материалдар тізімі (міндетті сызбалар дәл көрсетілуі тиіс)
LBC кодтарының кодер мен декодерлердің функционалдық схемалары.
Ұсынылатын негізгі әдебиет:

1) Вернер М. Основы кодирования. Москва, Техносфера, 2010.
2) Морелос-Сарагоса Р. Искусство помехоустойчивого кодирования. Москва, Техносфера, 2008.
3) Shu L. Error control coding: fundamental and applications. New Jersey, 2012.

Дипломдық жұмысты (жобаны) дайындау

КЕСТЕСІ

Бөлімдер атауы, қарастырылатын мәселелер тізімі	Ғылыми жетекшіге және кеңесшілерге көрсету мерзімі	Ескерту
Сызықты блокты кодтарға аналитикалық шолу жасау	20.01.2019 - 01.03.2019	
Сызықты блокты кодтарды кодтау және декодтау	02.03.2019-02.04.2019	
БЧХ кодтарының түзету қабілеттерін зерттеу	01.04.2019–15.04.2019	

Дипломдық жұмыс (жоба) бөлімдерінің кеңесшілері мен норма бақылаушының аяқталған жұмысқа(жобаға) қойған

қолтаңбалары

Бөлімдер атауы	Кеңесшілер (аты, әкесінің аты, тегі, ғылыми дәрежесі, атағы)	Қол қойылған күні	Қолы
Норма бақылау	PhD докторы, ЭТжҒТ каф.сениор-лекторы Тайсариева К.Н.	25.04.19	

Ғылыми жетекшісі _____ Л. Б. Илипбаева

(қолы)

Тапсырманы орындауға алған білім алушы _____ О. Темирханов

Күні “25” 04 2019 ж.

АҢДАТПА

Дипломдық жұмыста бөгеуілге тұрақты сызықта блокты кодтарға аналитикалық шолу жасалынған. Бөгеуілге тұрақты қателерді жөндеу коэффициенттері сараптама жасалынды. Сызықты блокты кодтардың артықшылықтары мен параметрлері көрсетіліп сипаттама беріледі. БЧХ коды мен Рид – Соломон кодтарының алгоритмдері және құраушы матрицалары арқылы есептеулер жүргізілген. Функционалды сұлбалары анықталды.

Дипломдық жұмыста БЧХ кодының жұмыс істеу принципі MATLAB бағдарламасында модельдердің жұмысы арқылы көрсетілді.

АННОТАЦИЯ

В дипломной работе были проведены обзор помехоустойчивым линейным блоковым кодам. Сделаны анализы помехоустойчивым корректирующим коэффициентам.Приведены параметры и ряд преимущества, а также свойства линейных блокирующихся кодов. Были проведены расчёты с помощью алгоритма и образующий матрицы кода Ридо-Соломона и кодов БЧХ. А также были определены функциональные схемы.

В дипломной работе принцип работы кода БЧХ были показаны с помощью моделирования в программе MATLAB.

ANNOTATION

In the thesis work, a review of the noise-resistant linear block codes was conducted. Analyzes of noise-correcting correction factors are made. Parameters and a number of advantages, as well as properties of linear blocking codes are given. Calculations were carried out using the algorithm and the generator matrix of the Rido-Solomon code and BCH codes. And also functional schemes were defined.

In the thesis work, the principle of operation of the BCH code was shown using simulation in the MATLAB program

МАЗМҰНЫ

КІРІСПЕ

Ақпаратты бөгеуілге қарсы кодтау телекоммуникация саласында өте маңызды рөл атқарады. Себебі қазіргі цифрлі технологиялар заманында ақпараттың цифрлі түрдегі берілісі, бұрмаланусыз тұтынушыға жеткізілуі үшін заманауи талаптарға сай бөгеуілге тұрақты кодтардың болуын қажет етеді. Мұндай талаптарды қанағаттандыратын сызықты блокты кодтардың артықшылықтары олардың код аралықтарының ұзындығында және құраушы, түзетуші матрицаларының құрылуы мен алгоритмдерінің нақтылығында. Сонымен қатар бөгеуілге тұрақты сызықты блокты кодтардың бағдарламалық деңгейде анализ жасауға үлкен мүмкіншіліктерге ие болуында. Сол себепті бөгеуілге тұрақты сызықты блокты кодтар заманауи жүйелерде кең қолданылады.

Дипломдық жұмыстың мақсаты қарастырылып отырған өзектілікке сәйкес бөгеуілге тұрақты сызықты блокты кодтарға сараптама жасап, жұмыс істеу негіздерін анықтап сипаттама беру болып табылады.

Алғашқы кезеңде, бөгеуілге тұрақты LBC сызықты блокты кодтарға аналитикалық шолу жүргізу арқылы, LBC кодтарының негізгі сипаттайтын параметрлері анықталып және құрылу тәсілдері қарастырылды.

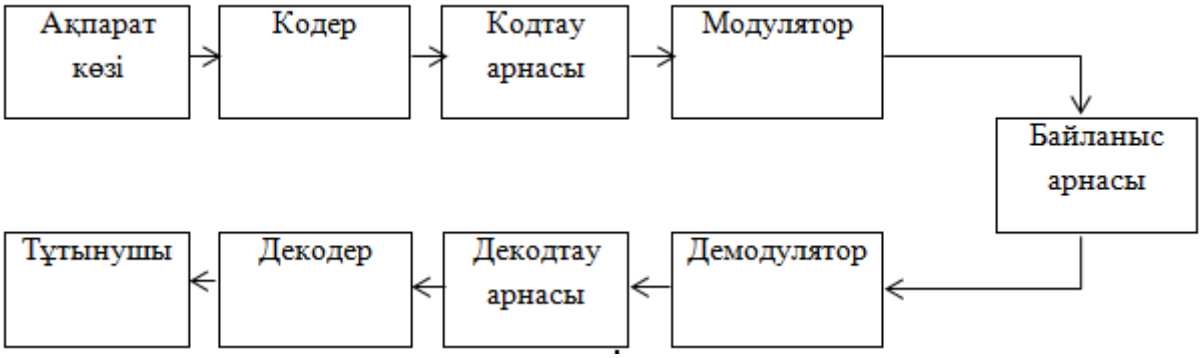
Екінші кезеңде, тұтынушыға ақпараттардың бұрмаланусыз жетуін қамтамассыз ететін кодтардың ішінен Боуз-Чоудхури-Хоквингем (БЧХ) және Рид – Соломон кодтарына қатысты есептеулер жүргізілді. Бөгеуілге тұрақты кодтардың құраушы және тексеруші матрицаларын құру әдістерін көрсетіп, оларға сараптама жүргізілді. Анықталған полиномы бойынша олардың құрылымдық структурасы көрсетіліп сипатталды. Кодтауды іске асыру кезіндегі өз ара айырмашылықтары мен алгоритмдерінің құрылысы қарастырылады.

Үшінші кезеңде, бөгеуілге тұрақты БЧХ кодының MATLAB бағдарламасында моделі қарастырылып, кіріс және шығыс нәтижелері анықталды.

1 Сызықты блокты кодтарға аналитикалық шолу жасау

1.1 Сызықты блокты кодтардың негізгі параметрлері және қасиеттері

Математикалық кодтар теориясының бастамасы клод шеннон бастаған (1948ж.) және Хэмминг кодтарының өнер табыстары бастады. Солайша бөгеуілге және шуылдарға тұрақты кодттар тарихы пайда болды. Ақпараттарды таратқыш және қабалдағыштары келесі схема бойынша бір бірімен цифрлық байланыс жүйесі арқылы байланысады.



Сурет 1.1 – Цифрлі тарату жүйесінің құрылымдық сұлбасы

Кодерде кіріс ақпараттар жазылып цифрлық түрге белгілі бір алгаритм түріне түрлендіреді әдетте биттер түрінде. Кодтау арнасында ақпараттық сөздер кодтталып сол алгаритм түрінде жазылады. Бұл кодттаудың ең маңызды бөлігі болып табылады. Өйткені дискретті символдар физикалық арна арқылы тарай алмағандықтан можулятор қолданылады, өзгерген ақпараттар байланыс арнасына келіп түседі ақпараттарға бұл жерде әр түрлі шуылдар әсер етуі мүмкін содан кейін байланыс арнасынан кейін ақпараттар тұтынушыға қарай кері процесс жүреді. Декодтау арнасында қателерді қалпына келтіру процессі жүреді. 1.1- сурет.

Арнайы түзетуші кодтарды қарастырмас бұрын, кез келген код қателерді табуға және түзетуге қабілетті болатынын ескерте кету керек. Мұны блокті кодтың мысалдарында анық көруге болады, олардың шығыс көзінде символдар тізбегі блоктарға бөлініп кетеді(кодті сөз,кодті комбинациялар), бірдей k символар санынан тұрады. Сонымен қоса, екілік код үшін хабарлама ансамблі $n_p=2^k$ көлеміне ие болады. Кедергіге тұрақты кодтау кезінде n_p көпшілік хабарламалар, $n_p=2^n$ көпшілік мүмкін болатын кодті сөздерде көрініс табады, мұндай шара дискретті хабарламаларлың кедергіге тұрақты кодтауы деп аталады(n-кодтаудан кейінгі кодтағы символар саны, кейде оларды кодті сөздің ұзындығы немесе кодтың мәні деп те атайды).

Жалпы жағдайда біркелкі блокті код үшін, m негізді код $n=m^n$ мүмкін болатын кодтар сөзінен тұрады. Көпшілік жағдайда хабарлама тасымалдау үшін қолданылатын кодті сөздер $n_р < n$ рұқсат етілген деп аталады, өзгелері болса,

$$N_э = (N - N_p) \quad (1.1)$$

Егер

$$p_{об} = \frac{p_{ex}(\geq 1, n) -}{p_{ex}(\geq 1, n) - p_{об}} \quad (1.2)$$

Бұл декодердің кірісіндегі n разрядты кодты сөздегі, $t \geq 1$ еселігінің қате ықтималдылығы, ал $p_{анық}$-декодердегі қателерді анықтау ықтималдылығы, онда анықтау коэффициенті келесідей өрнектеледі:

$$K_{об} = \frac{P_{вх}(\geq 1, n)}{P_{вх}(\geq 1, n) - P_{об}} \quad (1.3)$$

Қателерді түзету коэффициенті келесідей өрнектеледі:

$$K_{ис} = \frac{P_{вх}(\geq 1, n)}{P_{вх}(\geq 1, n) - P_{ис}} \quad (1.4)$$

Мұндағы $p_{түз}$-декодердағы қателерді түзету ықтималдылығы.Соңғысы кодті сөздегі қателер ықтималдылығы санына тең, олардың еселігі кепілді түзетілген қателер көлемінен асып кетпейді $t_{түз,}$ яғни ртүз=рвх($\leq t, n$).

Кодты түзету коэффициенті үнемі анықтау коэффициентінен кем болады, ол кез келген түзетуші кодтар үшін жалпылама шарт болып табылады.

Қателерді түзететін кодтың потенциалды мүмкіндігін жүзеге асыру үшін, нақты байланыс арналарындағы қателердің статистикалық қасиеттерін ескеріп отыру қажет. Рұқсат етілмеген комбинацияларды $n_З^{(i)}$ ішкі жиынтыққа бөлу жүзеге асырылуы тиіс , егер осы байланыс арнасында анағұрлым пайда болуы мүмкін қателер түзетілетін болса. [1]

Жалпы жағдайда, тасымалданатын кодті комбинация кездейсоқ түрде бұрмаланады, байланыс арнасында кедергінің кездейсоқ қасиетімен анықталады. Сондықтан қателерді түзететін декодер құрылымына, байланыс арналарын көрсеткіш қасиеттерін зерттеу алдыңғы орында тұру керек.мысал ретінде, сурет 1.2 екі жағдай үшін қате еселігінің $p_n(t)$ қисық орналасуы келтірілген: кодті символдағы дербес қателері бар екілік арна үшін, р-қисық 1 (биноминалді орналасуы)

$$p_n(t) = C_n^i p^i (1-p)^{n-i} \quad (1.5)$$

Бірдей ықтималдылықпен берілетін кодті сөз ,берілген арнада өзге де кодті сөзге өзгеру мүмкін болатын арна үшін.

$$p_n(\text{t}) = C_n^i / m^n \qquad (1.6)$$

Графиктер ұзындығы n=6 кодті сөзге сәйкес келеді.

$$p_n = p_{\text{вх}}(\geq 1, \text{n}) = 1 - (1 - \text{p})^{\text{n}} = 1 - 0{,}9^6 = 0{,}465$$

Қатені түзету ықтималдылығы(t=1 бұрмалауы бар қате ықтималдылығы):

$$\text{P}_{\text{ис}} = C_n^t * \text{p}^{\text{t}}(1 - \text{p})^{\text{n-t}} = C_6^1 * \text{p}(1 - \text{p})^5 = 6 * 0{,}1 * 0{,}9^5 = 0{,}36$$

Онда

$$K_{ис} = \frac{P_{вх}(\geq 1, n)}{P_{вх}(\geq 1, n) - P_{ис}} = \frac{0{,}465}{0{,}465 - 0{,}36} \approx 4{,}4.$$

$\text{p}_\text{n}(\text{t})$ қате еселігі бар байланыс арнасында , қисық 2 сәйкес қатені түзету ықтималдық тең болады [2]

$$\text{P}_{\text{ис}} = \text{P}_\text{n} * \frac{\sum_{\infty}^{i} C_n^t}{m^n} = \text{P}_\text{n} \frac{C_6^1}{2^6} \qquad (1.7)$$

Мұндағы $\sum_{i=1}^{t} C_n^t$ -қателердің үлесі,олардың мүмкін болатын қателердің жалпы санынан еселігі $\leq$ t тең. Онда түзету коэффициенті тең болады [3]

$$\text{K}_{\text{ис}} = \frac{p_n}{p_n - p_{\text{ис}}} = \frac{p_n}{p_n - \text{Pn}\frac{C_6^1}{2^6}} = \frac{2^6}{2^6 - C_6^1} = \frac{64}{64-6} \approx 1{,}24$$

Осылайша, бірінші жағдайда дәл сол сияқты кодтар қатені төрт есе көп түзетеді, екінші жағдаймен салыстырғанда. Мұндай жағдайды түсіндіретін болса, бірінші жағдайда көптеген қателер саны еселі t=1 болады және осы код арқылы түзетіледі, ал екінші жағдайда қателердің көптеген мөлшері еселігіне t> 1 ие , олар бұл кодпен түзетілмейді.

Анық болғандай,егер байланыс арнасында еселігі үлкен қателер басым болса, рұқсат етілген кодті сөздерге осындай көптеген тыйым салынған сөздерді белгілеу айқын болады.

Сызықты кодтар қайта кодтау(декодерлау) шараларын жеңілдететін , бірқатар қасиеттерге ие. Ең маңыздыларын келтіреміз.

1-ші қасиет. Екі кодты сөздің сызықты комбинациясы кодты сөз болып табылады.

Дәлел: кеңістік аралықgf ^{n} (q) кеңістік аралық ретінде сызықты кодтың анықтамасы, берілген кеңістіктегі екі вектордың сызықты комбинациясы дәл солай кеңістік аралығына тиеслі және тиесінше кодты сөз болатынын білдіреді. Нөлдік емес компонент саны ретінде, хэмминг салмағы w(c)ұғымын еңгізейік.

2-ші қасиет. Сызықты кодтың минималды ара қашықтығы,нөлдік емес кодті сөздің минималды салмағы болып табылады.

Дәлел: кодтың минималды ара қашықтығы анықтамасы бойынша

$$d_{min}= \min_{c1*c2\in C} d(c1,c2) = \min_{c1*c2\in C} w(c1\text{-}c2) \qquad (1.8)$$

Код сызықты болғандықтан, кодты сөздердің комбинациясы c_1-c_2 дәл солай кодті сөз болып табылады. Сәйкесінше,кодтың минималды ара қашықтығы келесідей көрсетілуі мүмкін

$$d_{min} = \min_{c\in C, c\neq 0} w(c) \qquad (1.9)$$

3-ші қасиет. С коді н тексеру матрицасына ие болсын делік.онда с кодтың минималды ара қашықтығы, н матрицасының сызықты тәуелді бағандардың минималды санына тең болады.

Тексеру матрицасы коды анықтамасынан $нс^{т}=0$ теңдігі шығады.егер с кодті сөз w(c) салмаққа ие болса, онда $нс^{т}$ туындысы н матрица бағандарының сызықты комбинациясы болады. Сәйкесінше, w салмақтың кодті сөзі пайда болады,егер де н матрицасы w сызықты тәуелді бағандардан тұратын болса.

Эквивалентті кодтардың түсінігін еңгіземіз. Екі (n,k) код бірдей қашықтық құрылымына ие болса, онда эквивалентті деп аталады.байқайтын болсақ,кодті сөздің символдарын берілу ретінің өзгерісі,кодтың қашықтық қасиеттерін өзегтпейді.

Екі код эквивалентті болады тек ,және тек қана берілген кодтардың тудырушы матрицасы бірінен соң бірі, келесі түрлендіру көмегімен алынатын болса

1. Бағандардың орнын ауыстыру
2. Жолақтардың үстінен қарапайым операциялар

Тудырушы матрицаның жолақтары сызықты кеңістіктің базисі болғандықтын, онда тудырушы матрица жолақтарының сызықты операциялар ,кодті кеңістікті өзгертпейді. Атап айтқанда,қатарлардың сызықты комбинациялар көмегімен ,кез келген кодті жүйелік түрге келтіруге болады.

1.2 Кодтық ара қашықтық, кодтың артықшылығы

Түзетуші кодтардың анықтайтын және түзететін қасиеттері , рұқсат етілген кодті сөздер ара қашықтығымен тығыз байланысты болып келеді. Кез келген көдті сөз a_i және a_j жұптарының арасындағы ара қашықтық , олардың арасындағы айырмашылықтарды көрсетеді:

$$d_{ij} - \sum_{k-1}^{n} |x_{ik} - x_{jk}| \qquad (1.10)$$

Мұндағы x_{ik} ,x_{jk} - n-өлшемді евклид емес l_n кеңістіктегі a_i ,a_j кодті сөздердің координаты .

Егер код екілік болса, онда кодті сөздер жұптар арасындағы ара қашықтық түсінігінде символдар көлемі болып түсінеді. Олар 2 модул бойынша,осы екі сөздің бірігуімен анықталады және осы соммадағы бірлік санына тең болады. Мысалы

$$\begin{array}{l} 101001 \quad -A_i \\ \oplus\ 011011 \quad -A_j \\ \hline 110010 \quad d_{ij}=3 \end{array}$$

Белгі $\oplus$, модул 2 бойынша сомманы білдіреді(екінші модул бойынша қосу ережеге сәйкес орындалады: $0\oplus 0=0,\ 0\oplus 1=1,\ 1\oplus 0=1,\ 1\oplus 1=0$.ескеретін жағдай,n-таңбалы екілік кодтардың геометриялық модулі бірге тең, n-өлшемді куб қабырғасы болып табылады. D_{ij} сөздер арасындағы ара қашықтық ,куб қабырға санына тең, және олар шыңдарды бір бірінен алшақтатады. Берілген кодтағы кез келген рұқсат етілген жұптар арасындағы ара қашықтық , кодті ара қашықтық деп атайды.

$$d = \min d_{ij} \qquad (1.11)$$

Геометриялық түсінік бойынша t қате еселігі, тасымалданған және бұрмаланған комбинация арасындағы ара қашықтық болып табылады, онда қате еселігін t табу үшін кодті ара қашықтық қажет болады.

$$d \geq t_{об} + 1 \qquad (1.12)$$

Қате еселігін $t_{түз}$ түзету үшін , кодті ара қашықтық қажет болады

$$d \geq 2t_{ис} + 1 \qquad (1.13)$$

Бұл қателерді түзету үшін бұрмаланған кодті сөз сәйкес келетін дұрыс сөзге барынша жақын орналасқан абзал екенін білдіреді. Еселік өшіруді $t_{өш}$ түзету үшін кодті ара қашықтық қажет болады

$$d \geq t_{об} + 1 \tag{1.14}$$

Яғни, өшіруді түзету үшін дәл осындай кодті ара қашықтық қажет болады, қатені анықтау үшін солай. Түзетуші кодтардың негізгі қасиеті, ол қателерді анықтау және түзету, сонымен қоса олар байланыс арнасы арқылы қосымша ақпарат тасымалдау негізінде анықталады. Ақпарат теориясына сәйкес,артықшылық коэффициенті белгілі болғандай

$$g = \frac{\log N - \log N_p}{\log N} = \frac{\log m^n - \log m^n}{\log m^n} = \frac{n-k}{n} = \frac{r}{n} \tag{1.15}$$

Тең болады, мұндағы r-сөздегі артық кодті символдар саны(k+r=n). Тәуелсіз қателері бар арналар үшін ,кодті сөздің қабылдау мүмкіндігі келесі өрнек түрінде анықталады . [4]

$$P_{бх}\ (\geq 1, n) = 1 - (1-p)^n. \tag{1.16}$$

Ал декодтау кезінде қателерді анықтау мүмкіндігі тең болады

$$P_{об} = P_{бх}(\leq t_{об}, n) = \sum_{i=1}^{t_{об}} C_n^i p^i (1-p)^{n-i}. \tag{1.17}$$

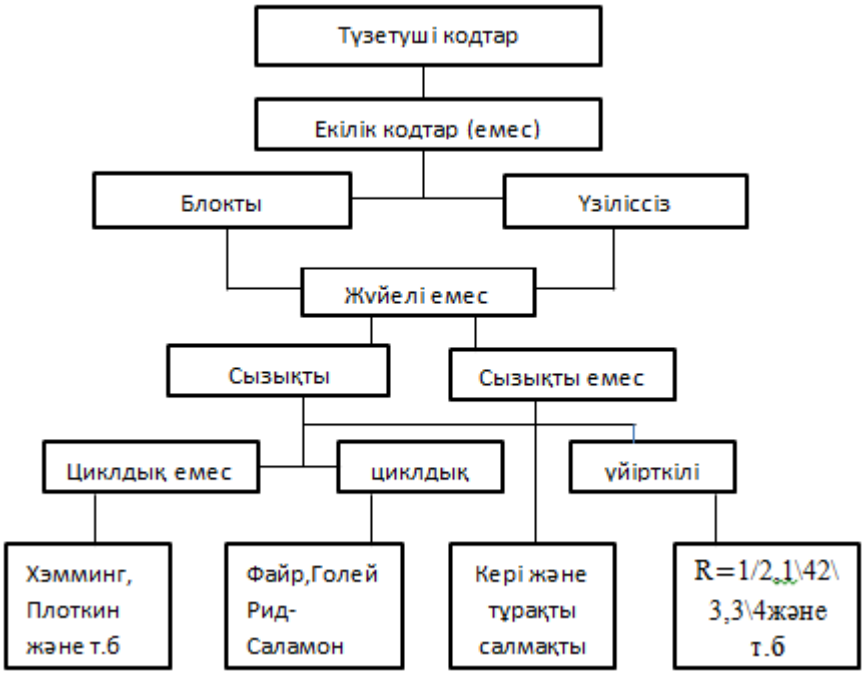
Онда декодтау кезінде қателерді анықтамау мүмкіндігі сәйкесінше тең болады $P_{но} = P_{бх}(> t_{об}, n) = P_{бх}\ (\geq 1, n) - P_{об}$,яғни

$$P_{но} = P_{бх}(> t_{об}, n) = P_{бх}(\geq 1, n) - \sum_{i=1}^{t_{ob}} C_n^i p^i (1-p)^{n-i} \tag{1.18}$$

Онда анықтау коэффициентін келесі түрде анықтауға болады:

$$K_{об} = 2^r \frac{P_{бх}(\geq 1, n)}{P_{бх}(> t_{об}, n)} \tag{1.19}$$

Қазіргі уақытта кедергіге тұрақтылығы және құрылымдық қасиеті бойынша, түзетуші кодтардың үлкен саны белгілі.



Сурет 1.2– Кедергіге тұрақты кодтардың жіктелуі

Түзетуші кодттарды қолдану, байланыс арналарында қателерді түзету үшін күресте ең тиімді тәсіл болып табылады.мұндай кодтар тек қана қателерді анықтау үшін, немесе анықтау және түзету үшін қолданылады.

1.3 Сызықты блокті кодтарды анықтау түсініктері

Біз бұл бөлімде, сызықты блокты кодттардың класстарын қарастырамыз. Сызықты кодтың тізбектілік кодтау элементі соңғы өріске $gf(q)^1$ тиеслі деп есептейміз. Кодтың тізбектілігі ,тиімді кодтарды іздеуді жеңілдетеді, сонымен қоса кодттау және қайта кодттау іс-шараларында маңызды жеңілдіктер алуға мүмкіндік береді.

Сызықты блокті код n ұзындығы , gf^n (q) де кеңістік іші бар. K кодтың өлшемі ,осы кеңістік ішінің өлшемі деп атайтын боламыз. Сызықты блокті кодтың кодтық сөздері -ол gf (q)үстінен ұзындық тізбегі,мұндағы әрбір тізбектілік элементі көптің ішінен элемент gf (q) болып табылады.

$$\mathbf{c} = (c1, c2, \ , cn), ci \in GF(q) \qquad (1.20)$$

Кодты сөздер кеңістік ішінің элементі болғандықтан, онда екі кодты сөздің сызықты үйлесімділігі сондай-ақ кодты сөз болып табылады. [5]

$$\mathbf{c} = \alpha \cdot \mathbf{c}1 + \beta \cdot \mathbf{c}2 = \left(\alpha \cdot c1^{1} + \beta \cdot c1^{2}, \alpha \cdot c^{1}2 + \beta \cdot c2^{2}, \ \ , \alpha \cdot c^{1}n + \beta \cdot cn^{2} \right), ci, \alpha, \beta \in GF(q) \qquad (1.21)$$

Атап айтқанда нөлдік тізбек

$$\mathbf{C_0} = (0,0, \ \ ,0) \qquad (1.22)$$

Сондай-ақ кодты сөз болып табылады. Код с векторлық кеңістік болғандықтан,осы кеңістік құратын базиске ие болады.кеңістік ішінің сызықты блокті кодын құрған базистің ұзындығы k тең. С кодын құрайтын кеніс ішілік базисті $\{g_0, g_{1,....,}g_{k-1}\}$ деп белгілейміз. Онда кез келген с кодті сөз, базисті векторлардың сызықты үйлесім түрінде берілу мүмкін.

$$\mathbf{c} = \sum_{i=0}^{k-1} u_i \cdot \mathbf{g}_i, u_i \in GF(q). \qquad (1.23)$$

U_i элементтерін $u=(u_0,u_1,....,u_{k-1})$ векторлық тізбекке,ал g_i векторын g матрицасына біріктіретін болсақ,онда (2.1.4) өрнегі матрица-векторлық түрде қайта жазылуы мүмкін.

$$c = u \cdot G \qquad (1.24)$$

Вектор u-ді ақпараттық ,ал с векторын кодті деп атаймыз.ендеше, с базиспен анықталатын $\{g_0, g_{1,....,}g_{k-1}\}$ сызықты блокті код (n,k) болсын. Онда k× n матрицасы

$$G = \begin{bmatrix} \mathbf{g}_0 \\ \mathbf{g}_1 \\ \vdots \\ \mathbf{g}_{k-1} \end{bmatrix},$$

С кодын туғызушы матрица деп атайды.

Коді $gf^{m}(q)$ кеңістік аралығы болғандықтан, n-k өлшемді нөлдік (ортогоналді) кеңістікке ие болады. Осы кеңістік аралықты дуалды код деп атаймыз ,және C^{1} деп белгілейміз.анық болғандай, C^{2}кеңістік аралық және n-k× n өлшемді туғызушы н матрицасына ие болып табылады. Нөлдік кеңістік аралық,шығыс кеңістік аралығында әрбір векторға ортагоналді векторлардан құралғандықтан ,онда әрбір кодті векторға келесідей шарт орындалуы тиіс

$$cH^{T} = 0 \qquad (1.25)$$

Мұндағы кішкентай c сызықты кодтің нөлдік кеңістік аралық базисін беріп отыратын, H матрицасы кодтың тексеру матрицасы деп аталады. Өрнегі v тізбекті тексеруі ретінде қолданылуы мүмкін. Егер өрнегі орындалса, онда вектор кодті кеңістікке тиеслі болады, демек кодті тізбек болып табылады. Байқағанымыздай, берілген код үшін g және h матрицалары бірнеше тәсілдермен беріліп отыруы мүмкін.

Кодтың матрица-векторлық анықтамасы ,кодтаудың іс жүзінде орындалуына маңызды артықшылықтар беріп отырады. Мысалы,(64,32) екілік код 64 ұзындықты $2^{32}=4.29*10^9$ кодті сөзге ие. Барлық кодті сөздерді сақтау үшін ~35 гбайт жады қажет болар еді. Алайда,егер (64,32) коді сызықты болса, онда туғызушы матрица кодын сақтау үшін ,барлығы 256 байт жады қажет болады.

Бұдан кейінгі кодтау шарасын жеңілдету, жүйелік кодтарды пайдалану кезінде мүмкін болады,мұнда әрбір кодті сөз ақпаратты тізбектен тұрады. Кодті сөздің қалған символдары тексеру символы деп аталады.сызықты жүйелік код үшін , туғызушы матрица арнайы түрге(формаға) ие .ақпарат тізбегіне ие жүйелік код үшін ,туғызушы матрица коді келесідей түрге ие болады.

$$G = [I \mid P] \tag{1.26}$$

Мұндағы, i- $k \times k$ өлшемді бірлік матрицасы,және p - $k \times n - k$ өлшемді матрица,олар тексеру символарын анықтайды. Жүйелік кодтың тексеру матрицасы, дәл солай өзіндік түрге ие. Мысалы,жүйелік код түрі үшін, тексеру матрицасы келесі құрылымға ие болады

$$\mathbf{H} = \left[-\mathbf{P}^T | \mathbf{I} \right] \tag{1.27}$$

Базисті векторлардың ортогоналді шартын тексеру оңай

$$GH^T = [\mathbf{I} \mid \mathbf{P}] \begin{bmatrix} -\mathbf{P} \\ \mathbf{I} \end{bmatrix} = -\mathbf{P} + \mathbf{P} = \mathbf{0}. \tag{1.28}$$

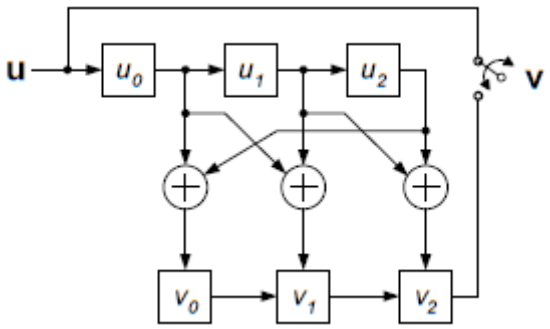
Жүйелі сызықты кодтардың туғызушы матрицамен мысалын қарастырамыз. [6]

$$G = \begin{pmatrix} 1\,1\,0\,1\,0\,0 \\ 0\,1\,1\,0\,1\,0 \\ 1\,0\,1\,0\,0\,1 \end{pmatrix}$$

Өрнектің қасиеттерін қолдана отырып, берілген кодтың тексеру матрицасы келесі түрде жазылуы мүмкін

$$G = \begin{pmatrix} 1\,0\,0\,1\,0\,1 \\ 0\,1\,0\,1\,1\,0 \\ 0\,0\,1\,0\,1\,1 \end{pmatrix}$$

Ақпаратты тізбек векторы $u=(u_0, u_1, u_2)$ үшін, кодті сөз $c= (u_0+ u_2, u_0+ u_1, u_1+ u_2, u_0, u_1, u_2)$ сәйкес келеді.



1.3 Сурет – Сызықты блокті кодтың кодері

Жоғарыда көрсетілген схема бойынша кіріс сигнал регистрлердің көмегімен оңға ығысу процесі бойынша жұмыс істейді. Келген сигналдар қосқыштар көмегімен қосылып нәтижелері алынады.

1.4 Сызықты блокті кодтардың стандартты орналасуы және синдромды декодтау

Біз бұл бөлімде тиімді декодтау(қайта кодтау) үшін, n ұзындықты тізбекте мүмкін болатын барлық әдісті қарастырамыз. Сызықты кодтың анықтамасы бойынша,екі кодті сөздің әртүрлі болуы , дәл солай кодті сөз болып табылады.егер нөлдік кодті сөзге жақын орналасқан көптеген тізбектер белгілі болса, онда бастапқы координатты жылжыту арқылы, көптеген қабылданған тізбектерді анықтауға болады.

Минималды кодті ара қашықтық тақ және $d_{min}=2t+1$ болсын. Радиусы t кеңістік ішінде , нөлдік кодті сөзде көптеген нүктелер орналасқан.

$$S0=\{\mathbf{v}|\, d(\mathbf{0},\mathbf{v})\le t\}. \qquad (1.29)$$

Бұл кеңістік нөлдік кодті сөзге декодталатын ,барлық тізбектерден тұрады. Радиусы t кеңістік ішінде , кодті с сөзінде көптеген нүктелер орналасқан.

$$S_C=\{\mathbf{v}|\, d(\mathbf{c},\mathbf{v})\le t\} \tag{1.30}$$

Онда

$$S_C= S0+\mathbf{c}=\{\mathbf{v}+\mathbf{c}|\mathbf{v}\in S0\} \tag{1.31}$$

Осылайша,нөлдік кодті сөзде кеңістік ортасында жатқан нүктелерді білген жеткілікті.Стандартты орналасу, осы сфералардың сипаттау тәсілдерін көрсетеді. Кодті сөздер $c_0=0,c_{1,\dots,}c_{qk-1}$ берілген болсын.

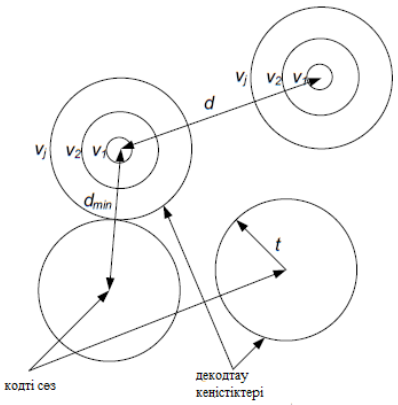
Бірінші қатарда барлық кодті сөздерді жазып шығарамыз. Қалғандардың ішінен gf^n (q) тізбегінде,0 ден 1дейін ара қашықтықта жатқан кез келген нүктені таңдап v_1 деп белгілейміз. Екінші қатарда $0+ v_1$, $c_1+ v_{1,\dots,}$ $c_{qk-1}+ v_1$ жазамыз. Осылайша келесі қатарды түземіз. J-ші қадамда, нөлдік қатарға жақын және алдыңғы қатарларда қатыспайтын v_j сөзін таңдаймыз. J-ші қатарда $0+ v_j$, $c_j+ v_{j,\dots,}$ $c_{qk-1}+ v_j$ деп жазып шығамыз. Кезекті қадамнан соң қолданбаған тізбек қалмаған жағдайда, іс шара аяқталады. Стандартты орналасудың кестесін толтыру шарасы сурет 8-де көрсетілген.

Декодтардың екі тобы болады:

1. Толық декодтар әрбір қабылданған тізбектерді жақын орналасқан кодті сөздермен салыстырады.

2. Толық емес декодтар әрбір қабылданған тізбектерді, жақын орналасқан радиусы t кеңістікте кодті сөздермен салыстырады. Егер қабылданған тізбек бірде-бір кеңістікке түспесе, онда декод декодтаудан бас тартады.

Осылайша,толық емес декодтар нүкте сызығына дейінгі кездесетін тізбектерді ғана өңдеу мүмкін.



Сурет 1.5 - Стандартты орналасуды құру көрінісі (иллюстрациясы)

Сызықты блокті код үшін, тудырушы матрицамен стандартты орналасу мысалы

Белгілі болғандай, n және k үлкен мәндері үшін,мұндай кестені құру тиімсіз болып табылады. Алайда бірінші бағанды сақтай отырып ,және

қажеттілігіне орай өзге бағандарды қалпына келтіре отырып кестені қысқартуға болады. Мұны қате синдромы ұғымын еңгізу арқылы жүзеге асыруға болады.

$$s = vH^T \tag{1.32}$$

Ендеше аралас сыныптың барлық векторлары , осы сынып қа жататын бір синдромға ие болады.шынымен де,егер бір аралас сыныпқа тиіеслі екі қабылданған тізбектер v және v', онда $v=c_i+y$ және $v^{/}= c_j+y$ кейбір y және и кодті сөз үшін c_i және c_j болады.Қабылданған векторлар үшін синдромдар сәйкесінше келесі түрде болады.

$$s = vH^T = yH^T, s' = v'H^T = yH^T \tag{1.33}$$

Сондықтан $s=s^{/}$. Керісінше айталық, $s=s^{/}$ болса, онда $(v-v^{/})h^t=0$ тең болады және $v-v^{/}$ айырмашылық, кодті сөз болып табылады.сондықтан, $v,v^{/}$ бір аралас сыныпқа тиеслі болады. [7]

Аралас сыныптың барлық элементтері бір синдромға ие болғандықтан, ендеше тек бір бағанды және синдромды сақтай отырып, декодтау кестесін айтарлықтай қысқартуға болады.

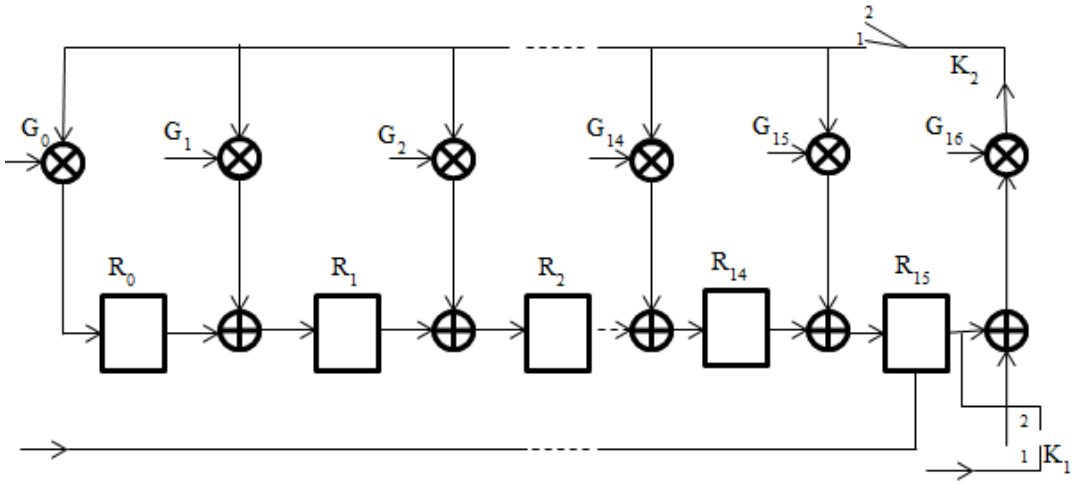
Берілген кесте стандартты орналасуға қарағанда айтарлықтай оңай, және қабылданған тізбек үшін декодтауға қолдануға болады. Мысалы, векторы (10010) қабылданған деп пайымдасақ.осы вектор (10010) $н^т$=(101) үшін синдром есептейміз. Бұл синдромға қатесі (01000) сәйкес келеді. Қабылданған тізбектен анықталған қатені шығара отырып, берілген сөз (10010)-(01000)=(11010) тең болатынын анықтаймыз. Код жүйелі болғандықтан, сәйкесінше ақпаратты сөз тең болады.

2 Сызықты блокты кодтарды кодтау және декодтау

2.1 БЧХ коды

Боуза-Чоудхури-Хоквингем кодтары(БЧХ) - еселік қателерді түзететін циклдік кодтар класы, яғни екі және одан көп($d_0 \geq 5$). Теориялық тұрғыдан БЧХ кодтары ерікті мөлшердегі қателер санын түзете алады, бірақ бұл ретте кодтық комбинациялардың ұзақтығы артады, бұл ақпарат берілу жылдамдығының азаюына және қабылдап-жеткізуші аппаратураның күрделенуіне әкеліп соқтырады (кодер және декодер сызбалары).

БЧХ кодтарын құру әдістемесі әдеттегі циклден ерекшеленеді, негізінен анықтаушы полинома P(x) таңдауымен. БЧХ кодтары кодтық сөздің берілген n ұзындығы және S түзетілетін қателердің саны бойынша құрылады, бұл ретте k ақпараттық разрядтарының саны анықтаушы полинмен таңдалғанға дейін белгісіз.



Сурет 1.6 – БЧХ кодерінің функционалды сұлбасы

БЧХ кодын қолдану арқылы кодтау рәсімін нақты мысалдарда қарастырайық.

Мысалы: Кодтық комбинацияда екі қатені түзететін (яғни n = 15, S=2) 15-разрядты БЧХ кодын құру.

Шешімі:

1.Бақылау m және ақпараттық разрядтардың k санын анықтаймыз

$$m \leq h\, S \qquad (2.1)$$

Формуладан h көрсеткішін анықтаймыз

$$n = 2^h-1,\ h = log_2(n+1) = log_216 = 4,$$

бұл ретте:

$$m \le h\ S = 4 \cdot 2 = 8;\ k = n-m = 15-8 = 7.$$

Осылайшы (15, 7) -кодын алдық.

2. Құраушы полиномның параметрлерін анықтаймыз:

- құраушыға кіретін ең аз көпмүше саны

$$L = S = 2 \qquad (2.2)$$

-үлкен минималды көпмүшенің реті (барлық минималдылар- тақ)

$$\rho = 2S-1 = 3 \qquad (2.3)$$

-көпмүше құраушының деңгейі

$$\beta = m \le 8 \qquad (2.4)$$

3.Көпмүше құраушының таңдауы.

4. БЧХ кодтары үшін ,кестеден минималды көпмүше үшін (қосымша 4) 4 бағаннан(себебі $l = h = 4$) минималды 1 және 3 көпмүшені таңдаймыз (себебі $\rho = 3$):

$$M_1(x) = 10011;$$
$$M_2(x) = 11111.$$

Бұл ретте

$$P(x) = M_1(x) \cdot M_2(x) = 10011 \times 11111 = 111010001 = x^8 + x^7 + x^6 + x^4 + 1.$$

Құраушы матрицаны құрамыз. Алдыңғы нөлдері бар полиномадан тұратын матрицаны құрайтын бірінші жолды жазамыз, бұл ретте кодтық комбинацияның жалпы ұзындығы n = 15 тең. Матрицаның қалған жолдарын матрицаның бірінші жолының оңнан солға қарай k-еселі циклдық жылжуы нәтижесінде алынады.

$$G(15,7) = \begin{vmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{vmatrix}$$

Матрицаның құраушы жолдары БЧХ кодының 7 кодтық комбинациясынан тұрады, ал қалғандары 2 модуль бойынша матрица жолдарының барлық ықтимал үйлесімдерін қосу жолымен алынуы мүмкін. Қабылданған кодтық комбинациядағы қателерді декодтау, анықтау және түзету рәсімі, $d_0 < 5$ бар циклдық кодтар үшін де дәл солай.

Мысалы: Кодтық комбинацияда үш қатені түзететін 31-разрядты БЧХ кодын құру (яғни n = 31, S = 3).

Шешімі:

1. m бақылау разрядтары және k ақпараттық разрядтардың санын анықтаймыз.

$$m \leq h\,S \tag{2.5}$$

Формуладан hпараметрін анықтаймыз

$$n = 2^h\text{-}1, h = log_2(n+1) = log_2 32 = 5 \tag{2.6}$$

мұнда :

$$m \leq h\,S = 5 \cdot 3 = 15;\ k = n\text{-}m = 31\text{-}15 = 16.$$

Осылайша, (31, 16)-кодын алдық.

2.Құраушы полиноманың параметрін анықтаймыз:

$$L = S = 3 \tag{2.7}$$

Құраушыға кіретін,көпмүшенің минималды саны;
Үлкен минималды көпмүшенің реті

$$\rho = 3S\text{-}1 = 5 \tag{2.8}$$

Көпмүше құраушының деңгейі

$$\beta = m \leq 15 \tag{2.9}$$

3.Көпмүше құраушының таңдауы:

БЧХ кодтары үшін ,кестеден минималды көпмүше үшін (қосымша 4) 5 бағаннан(себебі $l = h = 5$) минималды 1,3 және 5 көпмүшені таңдаймыз (себебі $\rho = 5$):

$$\begin{aligned} M_1(x) &= 100101; \\ M_2(x) &= 111101; \\ M_3(x) &= 110111 \end{aligned} \tag{2.10}$$

Бұл ретте

$$P(x) = M_1(x) \cdot M_2(x) \cdot M_3(x) = 1000111110101111 =$$
$$= x^{15} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^5 + x^3 + x^2 + x + 1.$$

4. Құраушы матрицаны құрамыз. Алдыңғы нөлдері бар полиномадан тұратын матрицаны құрайтын бірінші жолды жазамыз, бұл ретте кодтық комбинацияның жалпы ұзындығы n = 31-ге тең. Матрицаның қалған жолдарын матрицаның бірінші жолының оңнан солға қарай k-еселі циклдық жылжуы нәтижесінде алынады.

$$G(31,16) = \begin{matrix} 0000000000000001000111110111111 \\ 0000000000000010001111101111110 \\ 1000111110111110000000000000000 \end{matrix}$$

Матрицаны құрастырушы жолдары БЧХ кодының 16 кодтық комбинациясынан тұрады, ал қалғандары 2 модуль бойынша матрица жолдарының барлық мүмкін тіркестерін қосу жолымен алынуы мүмкін.

2.2 БЧХ кодын декодтау

БЧХ кодтары циклдық кодтар болып табылады, сондықтан оларға циклдық кодтарды декодтаудың кез келген әдістері қолданылады. БЧХ кодтарын ашу, кодер мен декодерлерді іске асырудың жаңа алгоритмдері мен әдістерін іздеу қажеттілігін тұғызды. БЧХ кодтары үшін арнайы әзірленген ең жақсы алгоритмдер алынды. Бұл Питерсон, Берлекэмпа және т.б. алгоритмдері.

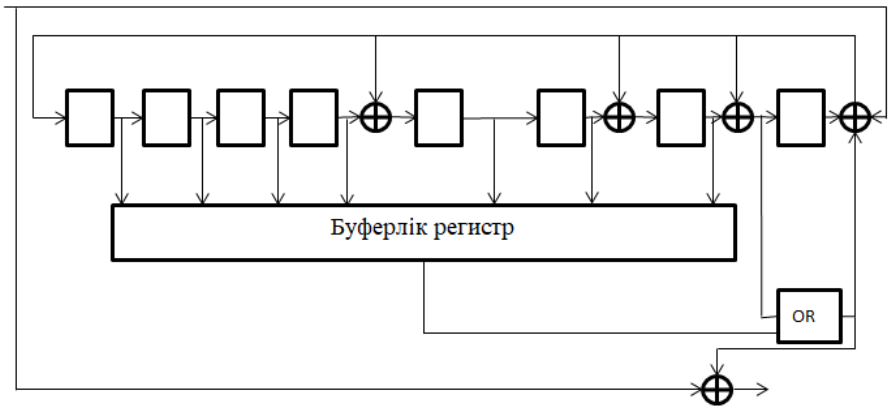
Қабылданған r(x) сөзді r(x) = c(x) + e(x) деп жазуға болады, мұндағы e(x)— қателер полиномы. $u \leqslant t = (d-1)/2$ қателері $i_1, i_2, \ldots, i_u$ позициясында (t түзетілетін қателердің максималды саны), орын алды деп есептейік, демек $e(x) = e_{i_1}x^{i_1} + e_{i_2}x^{i_2} + \ldots + e_{i_u}x^{i_u}$, $e_{i_1}, e_{i_2}, \ldots, e_{i_u}$- қателер көлемі.

Қабылданған Sj сөзінің j-ші синдромын құрауға болады r (x):

$$S_j = r(\beta^{l_0-1+j}) = e(\beta^{l_0-1+j}), \quad j = 1, \ldots, d-1 \qquad (2.11)$$

Тапсырма u қателер санын, олардың позицияларын $i_1, i_2, \ldots, i_u$ және олардың мәндерін $e_{i_1}, e_{i_2}, \ldots, e_{i_u}$ белгілі Sj синдромдарында қателер санын анықтаудан тұрады.

Бастамасы ретінде u нақтырақ t тең деп болжаймыз. сызықты емес теңдеулер жүйесі түрінде анық жазамыз:



Сурет 1.7 – БЧХ декодерінің функционалды сұлбасы

$$\begin{cases} S_1 = e_{i_1}\beta^{l_0 i_1} + e_{i_2}\beta^{l_0 i_2} + \cdots + e_{i_t}\beta^{l_0 i_t} \\ S_2 = e_{i_1}\beta^{(l_0+1) i_1} + e_{i_2}\beta^{(l_0+1) i_2} + \cdots + e_{i_t}\beta^{(l_0+1) i_t} \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ S_{d-1} = e_{i_1}\beta^{(l_0+d-2) i_1} + e_{i_2}\beta^{(l_0+d-2) i_2} + \cdots + e_{i_t}\beta^{(l_0+} \end{cases} \quad (2.12)$$

$X_k = \beta^{i_k}$ локатор арқылы k-ші қатені белгілейміз, ал $Y_k = e_{i_k}$ арқылы $k = 1, \ldots, t$ қателер көлемін белгілейміз.Сонымен қатар Xk әр түрлі,себебі βэлементінің реті n тең, және сол себепті әйгілі Xk кезінде ik-ны ik = logβXk секілді анықтауға болады. [8]

$$\begin{cases} S_1 = Y_1 X_1^{l_0} + Y_2 X_2^{l_0} + \cdots + + Y_t X_t^{l_0} \\ S_2 = Y_1 X_1^{l_0+1} + Y_2 X_2^{l_0+1} + \cdots + + Y_t X_t^{l_0+1} \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ S_{d-1} = Y_1 X_1^{l_0+d-2} + Y_2 X_2^{l_0+d-2} + \cdots + + Y_t X_t^{l_0+d-2} \end{cases} \quad (2.13)$$

Қателер локаторының полиномын құрамыз:

$$\Lambda(x) = (1 - xX_1)(1 - xX_2)\ldots(1 - xX_t) = \Lambda_t x^t + \Lambda_{t-1} x^{t-1} + \ldots + \Lambda_1 \quad (2.14)$$

Бұл полиномның негізі -кері қателер локаторларының элементтері болып табылады. Осы полиномның екі бөлігін $Y_l X_l^{\vartheta+t}$ -ге көбейтеміз . Алынған теңдік әділ болады егер

$$\vartheta = l_0, l_0 + 1, \ldots, l_0 + d - 1, \quad l = 1, \ldots, t \quad (2.15)$$

$$\Lambda(x) Y_l X_l^{\vartheta+t} = \Lambda_t x^t Y_l X_l^{\vartheta+t} + \Lambda_{t-1} x^{t-1} Y_l X_l^{\vartheta+t} + \ldots + \Lambda_1 x Y_l X_l^{\vartheta+t} + Y_l \quad (2.16)$$

Қоямыз $x = X_l^{-1}$ және (3) орналастырамыз. Әрбіріне $l \in 1, 2, ..., t$ және барлығында $\vartheta \in l_0, l_0 + 1, \ldots, l_0 + d - 1$ әділ теңсіздік шығады :

$$0 = \Lambda_t Y_l X_l^{\vartheta} + \Lambda_{t-1} Y_l X_l^{\vartheta+1} + \ldots + \Lambda_1 Y_l X_l^{\vartheta+t-1} + Y_l X_l \tag{2.17}$$

Осылайша, әрбір 1 үшін өзінің теңсіздігін жазуға болады. Егер оларды 1 ге қосып отырсақ, онда әрбіріне әділ теңсіздік шығады

$$\vartheta \in l_0, l_0 + 1, \ldots, l_0 + d - 1 \tag{2.18}$$

$$0 = \Lambda_t \sum_{l=1}^{t} Y_l X_l^{\vartheta} + \Lambda_{t-1} \sum_{l=1}^{t} Y_l X_l^{\vartheta+1} + \ldots + \Lambda_1 \sum_{l=1}^{t} Y_l X_l^{\vartheta+t-1} + \sum_{l=1}^{t} Y_l \tag{2.19}$$

Ескере отырып және мұны

$$S_{j+p} = \sum_{l=1}^{t} Y_l X_l^{l_0+j+p-1} = \sum_{l=1}^{t} Y_l X_l^{\vartheta+p}, \quad j = 1, \ldots, d-1, \quad \vartheta = l_0 + \tag{2.20}$$

Яғни ϑ бұрыңғы шектер секілді өзгереді) сызықты теңдеулер жүйесін аламыз:

$$\begin{cases} S_1\Lambda_t + S_2\Lambda_{t-1} + \cdots + S_t\Lambda_1 = -S_{t+1} \\ S_2\Lambda_t + S_3\Lambda_{t-1} + \cdots + S_{t+1}\Lambda_1 = -S_{t+2} \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ S_t\Lambda_t + S_{t+1}\Lambda_{t-1} + \cdots + S_{2t-1}\Lambda_1 = -S_{2t} \end{cases} \tag{2.21}$$

Немесе матрицалық түрде аламыз

$$S^{(t)}\bar{\Lambda}^{(t)} = -\bar{s}^{(t)} \tag{2.22}$$

Мұнда

$$S^{(t)} = \begin{bmatrix} S_1 & S_2 & \ldots & S_t \\ S_2 & S_3 & \ldots & S_{t+1} \\ \ldots & \ldots & \ldots & \\ S_t & S_{t+1} & \ldots & S_{2t-1} \end{bmatrix}, \tag{2.23}$$

$$\bar{\Lambda}^{(t)} = \begin{bmatrix} \Lambda_t \\ \Lambda_{t-1} \\ \cdots \\ \Lambda_1 \end{bmatrix}, \qquad \bar{s}^{(t)} \begin{bmatrix} S_{t+1} \\ S_{t+2} \\ \cdots \\ S_{2t} \end{bmatrix} \tag{2.24}$$

Егер қателердің саны шын мәнінде t тең болса, онда жүйе рұқсат етіледі және $\Lambda_1, \ldots, \Lambda_t$ коэффициенттердің мәнін табуға болады. Егер де u < t саны болса, онда жүйенің S(t) матрицасын анықтаушы 0 тең болады. Бұл қателер саны t-дан аз екенін белгісі болып табылады. Сондықтан $t-1$ тең қателердің санын болжай отырып, жүйені құру қажет. Қателердің шынайы санын анықтағанға дейін $S(t-1)$ жаңа матрицаның анықтаушысын есептеу қажет .

Осыдан кейін жүйені шешуге болады және қателер локаторлар полином коэффициенттерін алуға болады. Оның түп негізі (элементтер, кері қателер локаторларын) GF (qm) өрісінің барлық элементтері бойынша қарапайым аралықпен табуға болады. Оларға көбейту бойынша теріс элементтерді табу-бұл $X_k, \quad k = 1, \ldots, u$ қателер локаторы. Локаторлар бойынша қателердің позицияларын (ik = logβXk), ал t = u қабылдай отырып, жүйеден YK қателіктерінің мәндерін табуға болады. Декодтау аяқталды.

2.3 Рид Соломон коды

Келесі сұрақ бақылау байтын қандай жағдайда есептеуге болатынын қарастырамыз,кез-келген ақпаратты хабарламаларының ұзындығы k кеңістік ақпараттық хабарламалар, минималды кодтық қашықтықты $d = 1$, ұзындығы $n = k + 1$ болатын «руқсат етілген»кадрлардың көмегімен түрлендіреміз , n-өлшемді қашықтық кадырында минималды кодты қашықтық $d = r + 1$ ге тең, мұнда $r = 2t$.

Кодтау теориясының келесібір тізбегі ретінде белгілі бір соңғы өріс Галуа $GF(p^m)$тәсілді, Рида-Соломон кодын колдану арқылы ұсынамыз. Тудырушы полиномында мынандай тұжырымдама бар , ортақ жағдайда Галуа $GF(p^m)$ өрісі үшін , осы өрістің қарабайыр элементі $a \in GF(p^m)$ минималды кодты қашықтық d мынандай жағдайда беріледі :

$$g(x) = \sum_{\mathrm{i}=0}^{d-1} g_{\mathrm{i}} x^{\mathrm{i}} \prod_{s=b}^{b+d-2} (x - a^s) = 2 \prod_{s=1}^{d-1} (x - a^{s+b-1}); \quad a.g_{\mathrm{i}} \in GF(p^m) \tag{2.25}$$

Осы жерде b-кейбірі тұрақты , $LR(p^m - 1)$ сақина логарифміне жатады. Негізінде 0 ден $p^m - 2$ диапазонында b-теріс емес бүтін сан. Кодтау технологиясы негізінде b=1 қолданылады, бірақ тәжірибе жүзінде $b = 0$ жағдайы кеңінен қолданылады.

Әсіресе қарабайыр элементінің күш қасиеттері$a^{p^m-1}=1$, ал ол дегеніміз $a^s=a^{s\,mod(p^m-1)}$ және де $a^{s+b-1}=a^{(s+b-1)\,mod(p^m-1)}$ осы сияқты белгілеуге болады. Сондықтан тудырушы полиномының дурыс формуласы былай көрсетіледі:

$$g(x)=\sum_{\mathrm{i}=0}^{d-1} g_{\mathrm{i}}\cdot x^{\mathrm{i}}=\prod_{s=1}^{d-1}\left(x-a^{(s+b-1)mod(p^m-1)}\right)\qquad a.\,g_{\mathrm{i}}\in GF(p^m)\qquad(2.26)$$

Осымен s+b+1 дәрежелі көрсеткіші ,қарабайыр элементі a , p^m-1 көп немесе тең , демек ол $0...p^m-2$диапазонында «сақинамен іске қосылады» , логарифмдер сақинасында $LR(p^m-1)$, модуль қалдықтарын есептеуp^m-1 жолымен алынған.

Демек енді 2 сипаттамасындатехнология құрылымында біз тек $GF(2^m)$ өрісінқараймыз. Мұндай өрісте қосу операциясы және элементтер өрісін алып тастау «ұрланған » XOR жұмысына алып келеді, $\oplus$ белгіленеді. Сонымен қоса бақылау байттардын адал сан жағдайын қарастырамыз, осында кодты қашықтық мынаған тең: d=r+1=2t+1. Ақыр соңында біз Рида-Соломон кодын қарастырамыз, белгілі бір Галуа $GF(2^8)$ өрісі мысалында берілген p(x) басқарылмайтын көпмүше көмегімен алынған және қарабайыр элементімен a берілген. Мұндай жағдайда тудырушы полиномы мынандай түрге келеді:

$$g(x)=\sum_{\mathrm{i}=0}^{r} g_{\mathrm{i}}\cdot x^{\mathrm{i}}=\prod_{s=1}^{r}\left(x\oplus a^{(s+b-1)mod(2^8-1)}\right)\ ;\ g_{\mathrm{i}}\in GF(2^8);\mathrm{r}=2\mathrm{t}\quad(2.27)$$

Тудырушы полиномы кодтау теориясы бойынша кез келген ақпараттық хабарлама үшін «ұрпақ» $\mathrm{r}=2\mathrm{t}$ артық байттарды қамтамасыз етеді, k байттардан тұратын, қорытынды кадр n=k+r байттардан тұрады , k ақпаратты байттар r қорытынды байттардын қосындысынан тұрады, олар n– өлшемді кадрлар қашықтығында «руқсат етілген»кадр болып табылады.

Осыдан белгілеуге болады тудырушы полиномы g(x), $\mathrm{r}=2\mathrm{t}$ дәрежсін алады, келеси теңдеудін g(x)= 0 түбірі Галуа $GF(2^8)$ өрісінің элементі болады:

$a^{bmod(2^8-1)}$,$a^{(b+1)mod(2^8-1)}$..., $a^{(\mathrm{r}+b-1)mod(2^8-1)}$, Рида-Соломон коды үшін барлық түбірлері әр түрлі болуы қажет. Сосын t=128 бастап мына теңдікті аламыз $\mathrm{r}=256\ \Rightarrow a^{(\mathrm{r}+b-1)mod(2^8-1)}=a^{(256+b-1)mod(2^8-1)}=a^{bmod(2^8-1)}$, былайша айтканда түбірлер қайталананады. Осыдан түзетілген қатенің қысқартылған максималды мүмкіндігі Галуа $GF(2^8)$ өрісіне байланысты, $\mathrm{r}<256$ болғанда :

$$t_{max}=\frac{(2^8-2)}{2}=127\qquad(2.28)$$

Осыдан біз қысқартылып түзетілген қатені шектейміз, t≤127, және соған орай қорытынды байттар $\mathrm{r} \leq 256$. Осыған орай тудырушы полином формуласында $1 \leq s \leq 256$тізбекті аламыз себебі $1 \leq s \leq \mathrm{r}$. Тағыда алатынымыз

$a^{(s+b-1)mod(2^8-1)} = a^{smod(2^8-1)} \cdot a^{(b-1)mod(2^8-1)}$. Және ескеретініміз $1 \leq s \leq 254$, осыдан аламыз $smod(2^8-1) = s$ сонда $a^{(s+b-1)mod(2^8-1)} = a^s \cdot a^{(b-1)mod(2^8-1)}$. Келесі көріністі енгіземіз :

$$\beta = a^{(b-1)mod(2^8-1)} = \begin{cases} \alpha^{b-1}, b = 1 \dots 2^8 - 2 \\ \dfrac{1}{\alpha}, b = 0 \end{cases} \quad (2.29)$$

Егердеb константтүрінде 1 алынаса онда β=α^0=1 .
Онда тудырушы полином формуласы келесі түрге келеді:

$$g(x) = \sum_{\mathrm{i}=0}^{r} g_{\mathrm{i}} \cdot x^{\mathrm{i}} = \prod_{s=1}^{r} (x \oplus \beta \cdot a^S) \; ; \quad g_{\mathrm{i}} \in GF(2^8); \mathrm{r} = 2\mathrm{t} \quad (2.30)$$

Тудырушы полиномды қалыптастыру. Полиномды қалыптастыру g(x) мына түрдегі $(x \oplus \beta \cdot a^S); s = 1 \dots r$бірінші дәрежедегі полиномдардың көбеюіне байланысты. Көретініміз g(x) қалыптастыру урдісіті рекуррентті итерационды рәсім турінде корсетуге болады: [9]

$$\begin{cases} g^{(s)}(x) = g^{(s-1)}(x)(x \oplus \beta \cdot a^S) \\ s = 1 \dots r; g^{(0)}(x) = 1 \end{cases} \quad (2.31)$$

Сосын нөлдік деңгейдегі полиномнан бастағандықтан ары қарай әр бір итерацияда $s = 1 \dots r$, бірінші дәрежедегі полиномды көбейтуден бастаймыз,осыдан көрініп тұр $g^{(s)}(x)$ дәреже s ке тең. Осыдан көруге болады $x \oplus \beta \cdot a^S$ көбейту полиномы , хте 1 ге тең коэффициентті құрайды. Оңтайландыру мақсатында s итерациясын есептеуді толығырақ қарастырамыз:

$$g^{(s)}(x) = g^{(s-1)}(x)(x \oplus \beta \cdot a^S) = \left(\sum_{\mathrm{i}=0}^{s-1} g_{\mathrm{i}}^{(s-1)} \cdot x^{\mathrm{i}}\right) \cdot (x \oplus \beta \cdot a^S) = \quad (2.32)$$
$$\sum_{\mathrm{i}=0}^{s-1} g_{\mathrm{i}}^{(s-1)} \cdot x^{\mathrm{i}+1} \oplus \sum_{\mathrm{i}=0}^{s-1} g_{\mathrm{i}}^{(s-1)} \cdot \beta \cdot a^S \cdot x^{\mathrm{i}}$$

Бірінші сомадан қосымшаларды ауыстырамыз индексі j= i + 1және осыдан:

$$\sum_{j=1}^{s} g_{j-1}^{(s-1)} \cdot x^j \oplus \sum_{\mathrm{i}=0}^{s-1} g_{\mathrm{i}}^{(s-1)} \cdot \beta \cdot a^S \cdot x^{\mathrm{i}} \text{ . j=s} \quad (2.33)$$

Болғанда бірінші сомадан алып тастаймыз, ал екінші қосымша $\mathrm{i} = 0$ болғанда аламыз:

$$g_{s-1}^{(s-1)} \cdot x^s \oplus \left(\sum_{j=1}^{s-1} g_{j-1}^{(s-1)} \cdot x^j \oplus \sum_{\mathrm{i}=1}^{s-1} g_{\mathrm{i}}^{(s-1)} \cdot \beta \cdot a^S \cdot x^{\mathrm{i}}\right) \oplus g_0^{(s-1)} \beta \cdot a^S. \quad (2.34)$$

Анализдеу арқылы алынған формуланы, рекуррентті итерационды рәсімді полином коэффициентін $g^{(s)}(x)$ есептеу үшін енгіземіз мынандай итерацияда $s = 1 \ldots r$:

$$g_j^{(s)} = \begin{cases} g_{s-1}^{(s-1)}; j = s \\ g_{j-1}^{(s-1)} \oplus g_j^{(s-1)} \cdot \beta \cdot a^S; j = 1 \ldots s-1 \\ g_0^{(s-1)} \cdot \beta \cdot a^S; j = 0 \end{cases} \quad (2.35)$$

$$\mathrm{S}=1\ldots\mathrm{r};\ g_0^{(0)} = 1; g_1^{(0)} = \cdots g_r^{(0)} = 0;$$

Соңғы r- итерацияда біз қаланған ұрықтандыру полиномын аламыз $g(x)$.Келесі маңызды мәселе-барлық мүмкін кадрлардың жалпы санының арасында "рұқсат берілетін" кадрлардың нақты қандай саны бар. Бұдан басқа, кадрлардың n-өлшемді кеңістігінің құрылымын талдау тұрғысынан алғанда, "рұқсат етілген" кадрлар қандай саны белгілі бір қашықтықта $0 \leq \theta \leq n$ берілген "рұқсат етілген" кейбір кадрларда. Басқаша айтқанда, бізді қызықтыратын ол n-өлшемді кадрлар кеңістікте "рұқсат берілетін" кадрлардың сандық көлемінің бөліну функциясы.

Кодтау теориясына сәйкес барлық байттары нөлге тең "нөлдік" кадр – "рұқсат етілген» болып табылады. Біз "нөлдік" кадрды сандық бөлу функциясын шығару үшін кадрлар кеңістігінде "есептеу нүктесі" ретінде пайдалана аламыз. Бұл ретте, шығарылған функция сондай-ақ кез келген басқа "рұқсат етілген" кадр үшін де әділ болады санау "нүктесі " ретінде таңдалынған. Жай ғана " нөлдік "кадрға қатысты пайымдаулар кішкене жеңіл болады және олар басқа" рұқсат етілген " кадрға қарағанда анағұрлым көрнекі болады.

Сонымен , n байттан тұратын нөлі бар "нөлдік" кадр θ бар болсын және бұл кадр "рұқсат етілген"болып табылады. Берілген қашықтық үшін тура нөлдік емес байттар бар кадрлардың жалпы саны $0 \leq \theta \leq n$ есептеу қиын емес,оларды нөлдік емес θ байттар саны $\mathrm{C}_n^\theta * 255^\theta$ тең. Геометриялық тұрғыдан – бұл " сфера бетінің θ радиусі" және барлық нөлдік θ емес байттар бар кадрлар осы сфера бетінде жатыр.

Осылайша, біз алған нәтижені математикалық түрде келесідей көрсетуге болады:

$$|\{X\}|=\mathrm{C}_n^\theta * 255^\theta,\ \forall X \epsilon \Gamma^n \div D(X) \quad (2.36)$$

Сондай-ақ, 0-ден w-ге дейінгі радиустары бар барлық "сфералар" жиынтығы " w радиусының шарын" құрайды, онда w нөлдік емес байттардан аспайтын барлық кадрлар (яғни олар "нөлдік" кадрдан w-ден аспайтын қашықтықта θ) орналасқан. Әлбетте, тиісті "сферадағы" 0-ден w-ге дейінгі радиустары бар кадрлар санын ескере отырып, "радиус W шарындағы" кадрлардың жалпы санын есептеуге болады. Басқаша айтқанда, "нөлдік" кадрдан w аспайтын қашықтықта орналасқан кадрлардың жалпы саны:

$$|\{X\}| = \sum_{\theta=0}^{w} C_n^{\theta} \cdot 255^{\theta}$$
$$\forall X \in \Gamma^n : 0 \le D(X,\Theta) \le w; \quad \Gamma = GF(2^8) \qquad (2.37)$$

Егер w = n қойсақ, онда "радиусы n шарын " аламыз, ол, әлбетте, кеңістіктің барлық кадрларынан тұрады, олардың саны: $\sum_{\theta=0}^{n} C_n^{\theta} \cdot 255^{\theta}$=256 ^{n}

Енді біз A_{θ}арқылы "нөлдік" кадрдан θ тең қашықтықта орналасқан " рұқсат етілген " кадрлар санын белгілейміз. Әлбетте, бұл сан "нөлдік" кадрдан θ қашықтықтағы барлық мүмкін кадрлардың жалпы санынан аспауы мүмкін.

Бастапқыда ескеретін жағдай, $\theta = 0$ болған жағдайда, тек бір ғана кадр болады- ол “нөлдік кадрдың” өзі, және ол “рұқсат етілген” болып табылады.Осылайша $A_{\theta} = 1$ тең болады. Тағы да ексеретін жағдай,$1 \le \theta \le 2 \cdot t$ анықтама бойыншарұқсат етілген кадрлар болуы мүмкін емес, себебі минималды код ара қашықтығы $d = 2 \cdot t + 1$ тең, сондықтан алдағы рұқсат етілген кадрлар «нөлдік» кадрдан $d = 2 \cdot t + 1$ кем емес ара қашықтықта орналасады. Басқаша айтқанда, «рұқсат етілген» кадрлар саны $1 \le \theta \le 2 \cdot t$ кезінде нөлге тең:A_1=…=A_{2t}=0 .

Ең қарапайым жағдайды қарастырамыз: A_{2t+1}. Бұл жағдайда $\theta = 2 \cdot t + 1$ тең байттар бір жағынан нөлдік емес болуы тиіс, сонымен қатар $2 \cdot t + 1$ нөлдік емес байттар жиынтығынан барлық «рұқсат етілген» байттар бір бірінен $2 \cdot t + 1$ барлық байттар бойынша айрмашылық болуы тиіс. Егер $2 \cdot t + 1$ байттарының бірін 255 мәннің кез келгенін қабылдайтын еркін деп санайтын болсақ, ал өзгелерін $2 \cdot t$ байттарға байланысты тәуелді деп есептейтін болсақ, онда барлық жиынтық 255 тең болады. Одан өзге , $2 \cdot t + 1$ позициясын n позициядан $C^{2t+1}{}_n$ тәсілі арқылы таңдауға болады, онда нәтижесінде $A_{2t+1} = C^{2t+1}{}_n$ *255 аламыз.Сонымен қатар бұл формуланы келесі эквивалент түрінде де жаза аламыз $A_{2t+1} = C^{2t+1}{}_n$ (256-1)$C^0{}_{2t+1}$.

Ұқсас, бірақ комбинаторлық талдаудың күрделі әдістерін пайдалана отырып, көрсетілген құрамнан, $A_{2t+1} = C^{2t+1}{}_n$ (255^2-(2t)*255)= $C^{2t+1}{}_n$ ((256^2-1)-(2t+2)*255)= $C^{2t+1}{}_n$ ((256^2-1)* $C^0{}_{2t+2}$-(256-1) $C^1{}_{2t+2}$) аламыз.

Онда,жоғарыда баяндалғанның барлығын қорытындылай келе, "рұқсат етілген" кадрларды сандық бөлу функциясы үшін түпкілікті формуланыжазааламыз

$$\begin{cases} A_0 = 1; \quad A_1 = \ldots = A_{2t} = 0 \\ A_\theta = C_n^\theta \cdot \left(\sum\limits_{i=0}^{\theta-2t-1} (-1)^i \cdot C_\theta^i \cdot (256^{\theta-2t-i} - 1) \right); \quad 2t+1 \le \theta \le n \end{cases} \tag{2.38}$$

"Жол берілетін кадрларды" сандық бөлу функциясын алып, енді біз кадрлардың n-өлшемдік кеңістігінде "жол берілетін" кадрлардың жалпы санын бағалай аламыз. Ол үшін барлық үлестіру функциясының сомасын есептеу қажет $0 \le \theta \le n$ (барлық ықтимал қашықтықтағы " рұқсат етілген " барлық кадрларды $0 \le \theta \le n$ «нөлдік» кадрдан санау): $A_0=1$ $A_1=\ldots=A_{2t}=0$ тең екенін ескеретін болсақ, онда ішінара сомма$\sum_{\theta=0}^{2t} A_\theta$ болса, онда бізге тек $\sum_{\theta=0}^{n} A_\theta$ соммасын шығару керек.Соны мен,

$$\sum_{\theta=2t+1}^{n} A_\theta = \sum_{\theta=2t+1}^{n} C_n^\theta \cdot \left(\sum_{i=0}^{\theta-2t-1} (-1)^i \cdot C_\theta^i \cdot (256^{\theta-2t-i} - 1) \right) \tag{2.39}$$

$$\cdot q = \theta - 2t - i$$

белгілейміз. Онда

$$\cdot \sum_{\theta=2t+1}^{n} C_n^\theta \cdot \left(\sum_{q=1}^{\theta-2t} (-1)^{\theta-2t-q} \cdot C_\theta^{\theta-2t-q} \cdot (256^q - 1) \right) \tag{2.40}$$

Теңдігін аламыз. Байқайтын болсақ, биномиалды коэффициент $C_\theta^{\theta-2t-q}$ нөлге тең. Онда,

$$\cdot \sum_{\theta=2t+1}^{n} C_n^\theta \cdot \left(\sum_{q=1}^{n} (-1)^{\theta-2t-q} \cdot C_\theta^{\theta-2t-q} \cdot (256^q - 1) \right) \tag{2.41}$$

Мәніне ие боламыз. Енді біз ішкі қосылым шектері θ болмағандықтан, қосылым тәртібін оңай ауыстыра аламыз, және келесідей теңдікті аламыз:

$$\cdot \sum_{q=1}^{n} (256^q - 1) \left(\sum_{\theta=2t+1}^{n} C_n^\theta \cdot (-1)^{\theta-2t-q} \cdot C_\theta^{\theta-2t-q} \right) \tag{2.42}$$

Енді $C_\theta^{\theta-2t-q}$ коэффициенті $\theta \le 2t+q$ кезінде нөлге тен екенін ескере отырып, ішкі қосындының төменгі шегін $2t+q$ дейін көтере аламыз. Сонымен қатар $C_n^\theta C_\theta^{\theta-2t-q}$ өрнегін келесідеі түрде өрнектей аламыз:

$$\frac{n!}{\theta!(n-\theta)!}\cdot\frac{\theta!}{(2t+q)!(\theta-(2t+q))!}=$$
$$:\frac{n!}{(n-\theta)!}\cdot\frac{1}{(2t+q)!(\theta-(2t+q))!}\cdot\frac{(n-(2t+q))!}{(n-(2t+q))!}=C_n^{2t+q}\cdot C_{n-(2t+q)}^{n-\theta}. \quad (2.43)$$

Енді биномиалды коэффициенттердің бірі жоқ, оны ішкі жиынтықтан тыс шығаруға болады:

$$\sum_{q=1}^{n}(256^q-1)\cdot C_n^{2t+q}\cdot\left(\sum_{\theta=2t+q}^{n}\cdot C_{n-(2t+q)}^{n-\theta}\cdot(-1)^{\theta-(2t+q)}\right. \quad (2.44)$$

Енді j= $\theta-(2t+q)$ деп белгілейміз, бұл ретте қосынды шегі : j= 0 ... $n-(2t+q)$ болады.

Онай байқағанымыздай, ішкі жиынтық соммасы $(1-1)^{n-(2t+q)}$өрнектер қатарына жіктеу секілді өзгеше емес,ол барлық жағдайда нөлге айналады, тек $n-(2t+q)=0\rightarrow q=n-2t$ жағдайдан өзге, және бұл жағдайда $(1-1)^0=1$.Осылайша, барлық $q\neq n-2t$ үшін ішкі сомма0-ге тең, және тек$q=n-2t$ кезінде ол 1-ге тең болады. Онда, сыртқы жиынтықтау үшін жалғыз нөл емес қосылыс $q=n-2t$ кезінде болады, және ол келесідей болады: $(256^{n-2t}-1)\cdot C_{n}^{n}=256^{n-2t}-1$. Онда нақты түрдеаламыз:

$$\sum_{\theta=2t+1}^{n}A_\theta=256^{n-2t}-1 \quad (2.45)$$

Біз өте маңызды нәтиже алдық. d= 2•t+ 1 ең аз кодтық арақашықтығы бар кадрлардың n-өлшемдік кеңістігіндегі" рұқсат етілген " кадрлардың жалпы саны дәл ақпараттық хабарламалардың к-өлшемдік кеңістігіндегі барлық мүмкін болатын ақпараттық хабарламалардың жалпы санына тең, бұл ретте кеңістіктің өлшемі: к = n-2•t

2.4 Рида-Соломон кодын декодерлеу

С кадр n=k+r ұзындығы алынсын, k ақпаратты және r артық байттардан тұратын желі ішінен алынған немесе тасымалдаушыдан оқылған. Онда полином С(х) кадры зақымданбаған F кадрда шыққан F (х) полином сомасы деп көрсетуге болады, мұнда желі арқылы немесе тасымалдаушыда жазылған және Е (х) қателіктің кейбір полиномы арқылы жіберілген.

$$C(x)=F(x)\oplus E(x) \quad (2.46)$$

Онда оны қателік синдромы (синдром- ауруды сипаттайтын жиынтық белгісі) деп атап $S_j, j = 1 \dots r$ компоненттер жиынтығын , $\beta \cdot \alpha^1, \dots, \beta \cdot \alpha^r$ түпті С(х)полиномын қолдану арқылы есептеледі мұнда g(х) туындатқыш полином. Алдында орнатқандай зақымданбаған кадр F (х) полиномы $\beta \cdot \alpha^1, \dots, \beta \cdot \alpha^r$ түпке қойғанда нөлге айналады содан келесі теңдеу болады.

$$S_j = C\left(\beta \cdot \alpha^j\right) = E\left(\beta \cdot \alpha^j\right), j = 1 \dots r \qquad (2.47)$$

Басқаша айтқанда синдром шыққын зақымданбаған F кадрына тәуелді емес және Е қатесін толық сипаттайды.Демек қате локаторын және оның ұзындығын табу мақсатында синдромды анықтауда барлық технологиялар негізделген .

Сонымен қатар S(х) қател синдром полином ұғымы еңгізіледі, ол былай беріледі:

$$S(\text{х})=S_1 \oplus S_2 \cdot x \oplus \dots \oplus S_r \cdot x^{r-1} = \sum_{j=0}^{r-1} S_{j+1} \cdot x^j \qquad (2.48)$$

Сыдан белгілеуге болады синдром полином коэффициенті ретінде синдром компоненттерін қолданады 0 ден $r-1$ге дейінгі коэффициент түрінде емес, 1 ден r ге дейінгі көрсеткіште номірленеді.

Егер компоненттер синдромы нөлге тең болса, онда зақымдану болмайды несирек кездеседі зақымдану берілген n-өлшемді қашықтық кадрда басқа «жарамды»кадрға айналады, мұнда синдром нөлге тең – оны біз максималды зақымдану дейміз. Басқаша жағдайда егер синдром S нөлдік болса онда декодрлеуге болады , кадрде болған қатені түзетуге болады.

Е(х) полином қателігі арқылы S синдром компоненттері жеңіл түрде анықталатынына қарамастан, Е(х) полиномының керісінше есептелуі, белгілі бір синдром қателігінің компонентімен өте қиын және нетривиалды емесесеп. Сонымен қанша байттар зақымданғанын білмегеннен жағдай нашарлайды.

τ-С кадрдағы зақымданған байттардың берілген саны, мұнда $\tau \leq t$.

Полином қателіктерін келесі түрде көрсетуге болады.

$$E(x) = \sum_{l=1}^{\tau} v_l \cdot x^{u_l} \qquad (2.49)$$

u_l- локатор қателігі, ал v_l- қатенің ұзындығы, l =1... τ.

Кодірлеу теориясы бойынша [6-14] шын декаторлардың декодрлеуі және қате ұзындығы шыққан F кадрының қалпына келуі, t- қысқартылып түзетілген қатеден зақымданған байттар санынан нақты аспайды. Жанама белгілер бойынша r-локаторын таба алмаймыз, n ұзындық кадрының шекарасы ішінде байттар позициясынан көрсетуі мүмкін немес тиісті түзету бойынша. Тиісті

түзету берілген $\tau \le t$ байттардың зақымдану санымен көрсетіледі және t көп болған нақты санымен көрсетіледі.

Онда $S_j = E\left(\beta \cdot \alpha^j\right), j = 1 \dots r$ ескере отырып жәнеде

$$(\beta \cdot \alpha^j)^u = \beta^u (\alpha^u)^j \tag{2.50}$$

деп ескерсек онда синдром компоненттерін келесі түрде корсетуге болады:

$$S_j = \sum_{l=1}^{\tau} v_l \cdot \left(\beta \cdot \alpha^j\right)^{u_l} = \sum_{l=1}^{\tau} v_l \cdot \beta^{u_l} \cdot (\alpha^{u_l})^j \,,\ j = 1 \dots r \tag{2.51}$$

Көрнекілік үшін системаныңтеңдеуінің кеңейтілген түрін көрсетеміз:

$$\begin{cases} v_1 \cdot \beta^{u_1} \cdot (\alpha^{u_1})^1 \oplus \dots \oplus v_\tau \cdot \beta^{u_\tau} \cdot (\alpha^{u_\tau})^1 = S_1 \\ v_1 \cdot \beta^{u_1} \cdot (\alpha^{u_1})^r \oplus \dots \oplus v_\tau \cdot \beta^{u_\tau} \cdot (\alpha^{u_\tau})^r = S_r \end{cases} \tag{2.52}$$

Белгілі болғандай жүйе2τ белгісізr теңдеуден тұрады(τ локаторларжәне r қатенің ұзындығы) теңдедің өзі сызықты емес, себебі есептеу қиындатылған. Шешімдердің қарапайым толық тізбесі(локаторлар мен ұзындықтары үшін мәндердің барлық мүмкін комбинациясы) тиімді емес, себебі n=255 кадр ұзындығы және беріоген қателіктің қысқартылған түрі t=2, ол дегеніміз $(255 \cdot 254/2) \cdot 255^2 > 2$ кадр комбинациясынан тұрады деген сөз. Сондықтан кодірлеу теориясы , локаторлардың және қате ұзындығының тиімді және талғампазды түрін іздейді. [10]

Қате локаторының полиномұғымын келесі түрде көрсетеміз:

$$\Lambda(x) = 1 \oplus \sum_{l=1}^{\tau} \Lambda_l \cdot x^{\mathrm{i}} = \prod_{l=1}^{\tau} (1 \oplus x \cdot \alpha^{u_l})\,;\ \Lambda_0 = 1 \tag{2.53}$$

Қате локаторның полиномы мынандай түрде беріледі, $1/\alpha^{u_1}$,...,$1/\alpha^{u_\tau}$ элементтері болатын $\Lambda(x) = 0$ теңдеуінің түптері болу үшін, ал өз дәрежелері С кадрде берілген қатенің орын локаторы болады. [11]

Сонда біз теңдеудің келесі түрін көрсетеміз, қате локаторлар полиномын 1-ші қосымша сомасына көбейте отыра j-компонентінің синдромын табамыз:

$$\begin{aligned} &\Lambda(x) \cdot v_l \beta^{u_l} (\alpha^{u_l})^j \\ &\quad = v_l \beta^{u_l} (\alpha^{u_l})^j \cdot 1 \oplus v_l \beta^{u_l} (\alpha^{u_l})^j \cdot \Lambda_1 \cdot x \oplus \dots \oplus v_l \beta^{u_l} (\alpha^{u_l})^j \cdot \Lambda_\tau \cdot x^\tau \end{aligned} \tag{2.54}$$

Енді біз барлығына $l = 1 \dots \tau$теңдікті алатын x элементін $\Lambda(x) = 0$ теңдеуіне қоямыз.Соңында сол жағы нөлге тең L теңдік аламыз, себебі жоғарыда көрсетілгендей $\Lambda(x)$ локаторының полином аргументінің мәні нөлге

айналады. Содан кейін біз барлық теңдеуді мерзімді мерзімге бөлеміз және соңында мынандай теңдік аламыз:

$$0 = 1 \cdot \sum_{l=1}^{\tau} (v_l \beta^{u_l} (\alpha^{u_l})^j) \oplus \Lambda_1 \cdot \sum_{l=1}^{\tau} (v_l \beta^{u_l} (\alpha^{u_l})^{j-1}) \oplus \ldots \oplus \Lambda_\tau \cdot \sum_{l=1}^{\tau} (v_l \beta^{u_l} (\alpha^{u_l})^{j-\tau}) \tag{2.55}$$

Ал енді $l = 1 \ldots \tau$ жиынтығында синдром компаненттеріне ие боламыз: $S_j, S_{j-1} \ldots S_{j-\tau}$. Онда барлығына $j = \tau + 1 \ldots r$мынандай теңдеу аламыз:

$$0 = S_j \oplus \Lambda_1 \cdot S_{j-1} \oplus \ldots \oplus \Lambda_\tau \cdot S_{j-\tau}. \tag{2.56}$$

Енді S_j ді сол жақ теңдеуіне ауыстыра отыра декодрлеудің кілттік теңдеу жүйесін аламыз,мұнда S синдром компаненттерімен $\Lambda(x)$ қате локатор полином коэффициенті:

$$S_j = \sum_{\mathrm{i}=1}^{\tau} \Lambda_l \cdot S_{j-\mathrm{i}}; \;\; j = \tau + 1 \ldots r \tag{2.57}$$

Егер жүйені r=2·t ескере отырып кеңейтілген түрде қайта жазатын болсақ, онда біз аламыз:

$$\begin{cases} \Lambda_1 \cdot S_\tau \oplus \ldots \oplus \Lambda_\tau \cdot S_1 = S_{\tau+1} \\ \Lambda_1 \cdot S_{\tau+1} \oplus \ldots \oplus \Lambda_\tau \cdot S_2 = S_{\tau+2} \\ \vdots \\ \Lambda_1 \cdot S_{2t-1} \oplus \ldots \oplus \Lambda_\tau \cdot S_{2t-\tau} = S_{2t} \end{cases} \tag{2.58}$$

Көріп отырғанымыздай, бұл жай ғана теңдеулер жүйесі емес, белгісіз $2t$ теңдеулердің жүйесі және τ параметрдің өзі белгісіз.Бірақ, кем дегенде, жүйенің теңдеулері сызықтық болып табылады. [12]

k=5 символынан тұратын Хакер ақпараттық шығыс хабарламасы бар болсын делік. ASCII 8 биттік кодтауға сәйкес,әрбір кодқа 0 мен 255 диопазон аралығында сәйкес келетін кодты жазуға болады.Біздің жағдайда М шығыс хабарламасы кодты символдар түрінде келесідей болады:

213 224 234 229 240

Сәйкесінше,ақпараттық хабарлама полиномы келесідей түрге ие болады:

$$M(x)= 213 \cdot x^4 \oplus 224 \cdot x^3 \oplus 234 \cdot x^2 \oplus 229 \cdot x \oplus 240 \quad (2.59)$$

Мысал ретінде, d=2 дейінгі бұрмаланған байттарды түзету үшін Рида- Соломон кодтарын қолданғымыз келеді делік.Онда, мұндай жағдайда бізге r=2*t =4 артық байттар қажет болады. Кодтау үшін түрленбейтін көпмүшеден $p(x)= x^8 \oplus x^4 \oplus x^3 \oplus x^2 \oplus 1$ және қарабайыр $\alpha = 2$ элементерінен тұратын Галуа өрісін $GF(8^2)$ қолданамыз. b көрсеткішін =1 деп аламыз,онда $\beta = 1 -$ге тең болады. Онда тұғызушы полином келесідей болады:

$$g(x)=\prod_{s=1}^{4}(x \oplus 1 \cdot 2^s) = x^4 \cdot 30 \cdot x^3 \oplus 216 \cdot x^2 \oplus 231 \cdot x \oplus 116 \quad (2.60)$$

Онда кодтау кезінде біз:

$$M(x)\cdot x^4 = 213 \cdot x^8 \oplus 224 \cdot x^7 \oplus 234 \cdot x^6 \oplus 229 \cdot x^5 \oplus 240 \cdot x^4 \oplus 0 \cdot x^3 \oplus 0 \cdot x^2 \oplus 0 \cdot x \oplus x \quad (2.61)$$

$$M(x)\cdot x^4 = 213 \cdot x^8 \oplus 224 \cdot x^7 \oplus 234 \cdot x^6 \oplus 229 \cdot x^5 \oplus 240 \cdot x^4 \oplus 0 \quad (2.62)$$

Полиномын g(x) полиномына бөлгендегі қалдықты есептеуіміз қажет. Бөлу нәтижесінде : $R(x)= 5 \cdot x^3 \oplus 61 \cdot x^2 \oplus 81 \cdot x \oplus 228$ қалдықты аламыз.

Осыдан соң, алынған қалдықты $M(x)\cdot x^4$ қоса отырып , полином кадрын аламыз:

$$F(x)= 213 \cdot x^8 \oplus 224 \cdot x^7 \oplus 234 \cdot x^6 \oplus 229 \cdot x^5 \oplus 240 \cdot x^4 \oplus 5 \cdot x^3 \oplus 61 \cdot x^2 \oplus 81 \cdot x \oplus 228 \quad (2.63)$$

Ақырында F ұзындықтың n=k+r=9 нәтиже кадры келесідей болады:

213 224 234 229 240 5 61 81 228

Енді байланыс арнасы арқылы кадрды жеткізу немесе тасушыда сақтау кезінде кадрда екі байт бұрмаланды деп есептейік, онда нәтижесінде біз келесідей *C* бұрмаланған кадрды аламыз:

203 224 236 229 240 5 61 81 228

Егер ақпараттық байттарды ASCII кодтау кестесе бойынша құрайтын болсақ, онда Ламер сөзінің шығатынын көреміз-және бұл сөз негізінен қарама- қарсы мағына береді.

Ал енді алынған кадрды декодтап көрейік. Сонымен, полиномиалды түрде алынған кадр келесідей көрініске ие болады:

$$C(x)= 203 \cdot x^8 \oplus 224 \cdot x^7 \oplus 236 \cdot x^6 \oplus 229 \cdot x^5 \oplus 240 \cdot x^4 \oplus \quad (2.64)$$

$5 \cdot x^3 \oplus 61 \cdot x^2 \oplus 81 \cdot x \oplus 228$

Синдром компоненттерін анықтаймыз:

$$\begin{cases} S_1 = C(1 \cdot 2^1) = 203 \cdot 2^8 \oplus 224 \cdot 2^7 \oplus 236 \cdot 2^6 \oplus 229 \cdot 2^5 \oplus 240 \cdot 2^4 \oplus 5 \cdot 2^3 \oplus 61 \cdot 2^2 \oplus 81 \cdot 2 \oplus 228 = 246 \\ S_2 = C(1 \cdot 2^2) = 203 \cdot 2^{16} \oplus 224 \cdot 2^{14} \oplus 236 \cdot 2^{12} \oplus 229 \cdot 2^{10} \oplus 240 \cdot 2^8 \oplus 5 \cdot 2^6 \oplus 61 \cdot 2^4 \oplus 81 \cdot 2^2 \oplus 228 = 207 \\ S_3 = C(1 \cdot 2^3) = 203 \cdot 2^{24} \oplus 224 \cdot 2^{21} \oplus 236 \cdot 2^{18} \oplus 229 \cdot 2^{15} \oplus 240 \cdot 2^{12} \oplus 5 \cdot 2^9 \oplus 61 \cdot 2^6 \oplus 81 \cdot 2^3 \oplus 228 = 255 \\ S_4 = C(1 \cdot 2^4) = 203 \cdot 2^{32} \oplus 224 \cdot 2^{28} \oplus 236 \cdot 2^{24} \oplus 229 \cdot 2^{20} \oplus 240 \cdot 2^{16} \oplus 5 \cdot 2^{12} \oplus 61 \cdot 2^8 \oplus 81 \cdot 2^4 \oplus 228 = 213 \end{cases}$$

Осылайшы S_1=246, S_2=207, S_3=255, S_4=213 , синдром нөлдік емес екендігі анық, және бұрмалаудың орынды болғандығы ешқандай күмән тудырмайды. Алайда декодтау сатысындашын мәнінде қанша байт бұрмаланғандығы ешқашан анық болмайды. Берлекемме-Месси алгоритмі бойынша Λ(x) полином локаторын табамыз, және сонымен қатар зақымдалған байттардын τ санын анықтаймыз.

Алгоритмнің инициализациясы:

$$\Lambda(x)=1,\ q=0\ ,\ m=-1,\ L=0, B(x)=x \qquad (2.65)$$

Итерация q=0 : Келіспеушілікті есептейміз:

$$\Delta_0=\sum_{i=0}^{0} \Lambda_i \cdot S_{0-i+1} = \Lambda_0 S_1 = 1 * 246 = 246 \qquad (2.66)$$

Келіспеушілік нөл,сондықтан есептейміз:

$$\Lambda^* = \Lambda(x) \emptyset \Lambda_0 \cdot B(x) = 246 \cdot x \oplus 1. \qquad (2.67)$$

Ары қарай

$$L<q-m \rightarrow 0 < 0 - (-1) \rightarrow 0 < 1 \qquad (2.68)$$

Орындалады, онда келесі

$$L^* = q - m = 0 - (-1) = 1.\ m=q-L=0-0=0\ ,\ L=L^* = 1\ ,\ B(x)=\Delta_0^{-1} \cdot \Lambda(x) = 246^{-1} \cdot 1 = 211 \qquad (2.69)$$

Осыдан кейін келесі орындалады

$$\Lambda(x)= \Lambda^*(x) = 246 \cdot x \oplus 1\ ,\ B(x) = x \cdot B(x) = 211 \cdot x \oplus 0 \qquad (2.70)$$

Осыдан кейін q=q+1=1<2t=4 болғанда келесі итерацияға көшеміз.

Итерация q=1 : Келіспеушілікті есептейміз:

$$\Delta_1=\sum_{i=0}^{0} \Lambda_i \cdot S_{1-i+1} = \Lambda_1 S_1 \oplus \Lambda_0 S_2 = 246 \cdot 246 \oplus 1 \cdot 207 = 108 \quad (2.71)$$

Келіспеушілік нөл,сондықтан есептейміз

$$\Lambda^* = \Lambda(x) \oplus \Lambda_1 \cdot B(x) = (246 \cdot x \oplus 1) \emptyset 108 \cdot (211 \cdot x \oplus 0) = 202 \cdot x \oplus 1 \quad (2.72)$$

Ары қарай

$$L<q-m \rightarrow 1 < 1 - 0 \rightarrow 1 < 1 \quad (2.73)$$

Орындалмайды, келесі теңдеуге көшеміз

$$\Lambda(x) = \Lambda^*(x) = 202 \cdot x \oplus 1,\ B(x) = x \cdot B(x) = 211 \cdot x^2 \oplus 0 \cdot x \oplus 0 \quad (2.74)$$

Осыдан кейін q=q+1=2<2t=4 болғанда келесі итерацияға көшеміз.

Итерация q=2 : Келіспеушілікті есептейміз

$$\Delta_2=\sum_{i=0}^{2} \Lambda_i \cdot S_{2-i+1} = \Lambda_2 S_1 \oplus \Lambda_1 S_2 \oplus \Lambda_0 S_3 = 1 * 246 \oplus 202 \cdot 207 \oplus 1 \cdot 255 = 160 \quad (2.75)$$

Келіспеушілік нөл,сондықтан есептейміз

$$\Lambda^* = \Lambda(x) \oplus \Lambda_2 \cdot B(x) = (202 \cdot x \oplus 1) \oplus 160 \cdot (211 \cdot x^2 \oplus 0 \cdot x \oplus 0) = 158 \cdot x^2 \oplus 202 \cdot x \oplus 1 \quad (2.76)$$

Ары қарай

$$L<q-m \rightarrow 1 < 2 - 0 \rightarrow 1 < 2 \quad (2.78)$$

Орындалады, онда келесі

$$L^* = q - m = 2 - 0 = 2.\ m=q-L=2-1=1\ ,\ L=L^* = 2\ ,\ B(x)=\Delta_2^{-1} \cdot \Lambda(x) = 160^{-1} \cdot (202 \cdot x \oplus 1) = 45 \cdot x \oplus 28 \quad (2.79)$$

Осыдан кейін келесі орындалады

$$\Lambda(x) = \Lambda^*(x) = 158 \cdot x^2 \oplus 202 \cdot x \oplus 1,\ B(x) = x \cdot B(x) = 45 \cdot x^2 \oplus 28 \cdot x \oplus 0 \quad (2.80)$$

Осыдан кейін q=q+1=3<2t=4 болғанда келесі итерацияға көшеміз

Итерация q=3 : Келіспеушілікті есептейміз:

$$\Delta_3=\sum_{i=0}^{3}\Lambda_i \cdot S_{3-i+1} = \Lambda_3 S_1 \oplus \Lambda_2 S_2 \oplus \Lambda_1 S_3 \oplus \Lambda_0 S_4 = 0 \cdot 246 \oplus 158 \cdot 207 \oplus 202 \cdot 255 \oplus 213 = 75 \quad (2.81)$$

Келіспеушілік нөл,сондықтан есептейміз

$$\Lambda^* = \Lambda(x) \oplus \Lambda_3 \cdot B(x) = (158 \cdot x^2 \oplus 202 \cdot x \oplus 1) \oplus 75 \cdot (45 \cdot x^2 \oplus 28 \cdot x \oplus 0) = 19 \cdot x^2 \oplus 93 \cdot x \oplus 1 \quad (2.82)$$

Ары қарай

$$L<q-m \rightarrow 2 < 3 - 1 \rightarrow 2 < 2 \quad (2.83)$$

Орындалмайды осыдан кейін келесі орындалады

$$\Lambda(x) = \Lambda^*(x) = 19 \cdot x^2 \oplus 93 \cdot x \oplus 1, B(x) = x \cdot B(x) = 45 \cdot x^2 \oplus 28 \cdot x \oplus 0 \cdot x \oplus 0 \quad (2.84)$$

Осыдан кейін

$$q=q+1=4<2t=4 \quad (2.85)$$

Болғанда итерация циклынан шығамыз. Себебі блокатор полином дәрежесі

$$\deg \Lambda(x) = 19 \cdot x^2 \oplus 93 \cdot x \oplus 1 = 2 \quad (2.86)$$

Дәл L=2 сияқты локатор полиномы табылды деген сөз.Демек біз минималды дәреженің локатор полиномын таптық

$$\Lambda(x) = 19 \cdot x^2 \emptyset 93 \cdot x \emptyset 1 \quad (2.87)$$

Осыдан нағыз керекті дәрежесі 2 ге тең және ол дегеніміз зақымданған байттардың саны $\tau = 2$.

Галуа өрісінің нөлдік элементтердің толық анықтаған соң 1,...,255 және локатор полиномдарына қоя отыра, локатор полиномдарының нөлге айналуынан түбірлерді табамыз. Түбірлер, мына элементтер $x_1^* = 131$ және $x_2^* = 54$.

Байқайтынымыз түбірлер саны 2 ге тең қате локатор полиномының дәрежесімен сәйкес келеді, сондықтан декодрлеуді жалғастыруға болады.

$$\Lambda(x) = 19 \cdot 131^2 \oplus 93 \cdot 131 \oplus 1 = 0 \text{ , } \Lambda(x) = 19 \cdot 54^2 \oplus 93 \cdot 54 \oplus 1 = 0 \quad (2.88)$$

Осыдан кейін қарабайыр элементінің логарифмін қолдана отырып, ескі қате локаторларын аламыз $\alpha = 2$:

$$\begin{cases} u_1 = log_2\left(\frac{1}{131}\right) = 8 \\ u_2 = log_2\left(\frac{1}{54}\right) = 6 \end{cases} \quad (2.89)$$

8 бен 6 ға тең локаторлар (0,8) шегінен шықпайды, кадр ұзындығы n=9 сондықтан локаторлар дұрыс болады, дкодрлеуді жалғастыруға болады.

қате ұзындығының полиномын есептейміз:

$$\Omega(x)=\sum_{q=0}^{1} x^q \cdot \left(\sum_{i=0}^{q} \Lambda_i \cdot S_{q-i+1}\right) = (\Lambda_0 S_1) \oplus x(\Lambda_0 S_2 \oplus S_1) = 1 \cdot 246 \oplus x(1 \cdot 207 \oplus 93 \cdot 246) = 181 \cdot x \oplus x246 \quad (2.90)$$

Блокатор полтномының формальді бөлінгішін есептейміз:

$$\Lambda'(x) = \sum_{j=0}^{1} x^j \cdot (\Lambda_{j+1} \cdot ((j+1) mod 2)) = \Lambda_1 \cdot (1 mod 2) \oplus \cdot (2 mod 2) = \Lambda_1 = 93 \quad (2.91)$$

Енді қажетті локаторларлы қолдана отырып, қате ұзындығынын таба аламыз($\beta = 1$ ол деген $\beta^{u_1} = \beta^{u_2} = 1$). [13]

$$\begin{cases} v_1 = \frac{\Omega\left(\frac{1}{2^8}\right)}{\Lambda'\left(\frac{1}{2^8}\right)} = (181 \cdot (131) \oplus \frac{246}{1 \cdot 93} = 30 \\ v_2 = \frac{\Omega\left(\frac{1}{2^6}\right)}{\Lambda'\left(\frac{1}{2^6}\right)} = (181 \cdot (54) \oplus \frac{246}{1 \cdot 93} = 6 \end{cases} \quad (2.92)$$

Онда қате полиномының қорытындысын аламыз:

$$E(x)= \sum_{l=1}^{2} v_l \cdot x^{u_l} = v_1 \cdot x^{u_1} \oplus v_2 \cdot x^{u_2} = 30 \cdot x^8 \oplus 6 \cdot x^6 \quad (2.93)$$

Зақымданған полиномды қате полиноммен бірге қосу қалады:

$$C(x)=203 \cdot x^8 \oplus 224 \cdot x^7 \oplus 236 \cdot x^6 \oplus 229 \cdot x^5 \oplus 240 \cdot x^4 \oplus 5 \cdot x^3 \oplus 61 \cdot x^2 \oplus 81 \cdot x \oplus 228 \quad (2.94)$$

$$E(x)=30\cdot x^8\oplus 0\cdot x^7\oplus 6\cdot x^6\oplus 0\cdot x^5\oplus 0\cdot x^4\oplus 0\cdot x^3\oplus 0\cdot x^2\oplus 0\cdot x\oplus 0, \quad (2.95)$$

$$F(x)=213\cdot x^8\oplus 224\cdot x^7\oplus 234\cdot x^6\oplus 229\cdot x^5\oplus 240\cdot x^4\oplus 5\cdot x^3\oplus 61\cdot x^2\oplus 81\cdot x\oplus 228$$

Полиномның кадрға айналуынан аламыз:

213 224 234 229 240 5 61 81 228

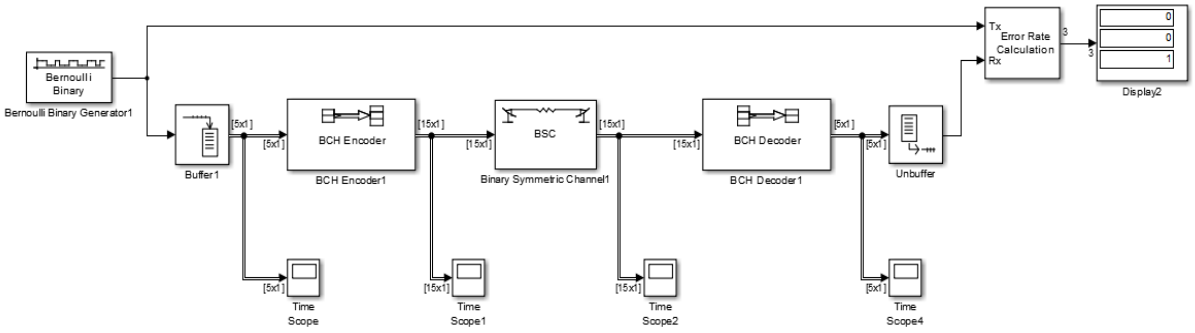
көріп тұрғандай түзетілген кадр желімен берілген кадрға тұтастай ұқсап тұр. Сондықтан шыққан кадрдың қалпына келтіруін көріп тұрмыз.

3 БЧХ кодтарының түзету қабілеттерін зерттеу

Зерттеулерді орындау үшін келесі операцияларды орындау арқылы байланыс арнасының үлгісін жасау қажет:

1. Commlibv2 командасын пайдалана отырып, экранда байланыс арнасының құрылымдық сұлбасын шақыру және Error control coding ақпаратты кодтау блогын іске қосу;
2. Demo Error-ControlCoding/DecodingLibraryпайда болған терезелерде BCH codeстерезесін таңдау;
3. жаңатерезеде BCH Binarysequence BCH encoder кодтық комбинациясы екілік элементтерді тізбектей беру жүйесінтаңдау;
4. БЧХ Sequencecodecdemoкодтарыныңэталондықмоделіналуғамүмкіндікберетінжасылтүстітерезенііскеқосу;

1. Жаңа терезенің басты мәзірінің жолында File сөзін белсендіріп, пайда болған мәзірде New басыңыз, одан әрі оң жақта Model мәзірін басыңыз, бос терезе пайда болады;
2. Сүйреу әдісін пайдалана отырып, көрсетілген үлгі бойынша жинау.



Сурет 3.1 – БЧХ коды бар арнаны сынауға арналған моделдің үлгі

Статистикалық деректерді жинау үшін модельді іске қоспас бұрын, модельденетін жүйенің әрбір блогы үшін көрсеткіштерді орнату қажет. Бұл импульстер бойынша модель блоктарының келісілген өзара іс-қимылына қол жеткізіледі. Осы іс шараны орындау үшін, қызығушылық тудыратын блоктың өрісіне тышқанның сол жақ батырмасын екі рет басып, ашылған панельге қажетті көрсеткіштерді орнату қажет.

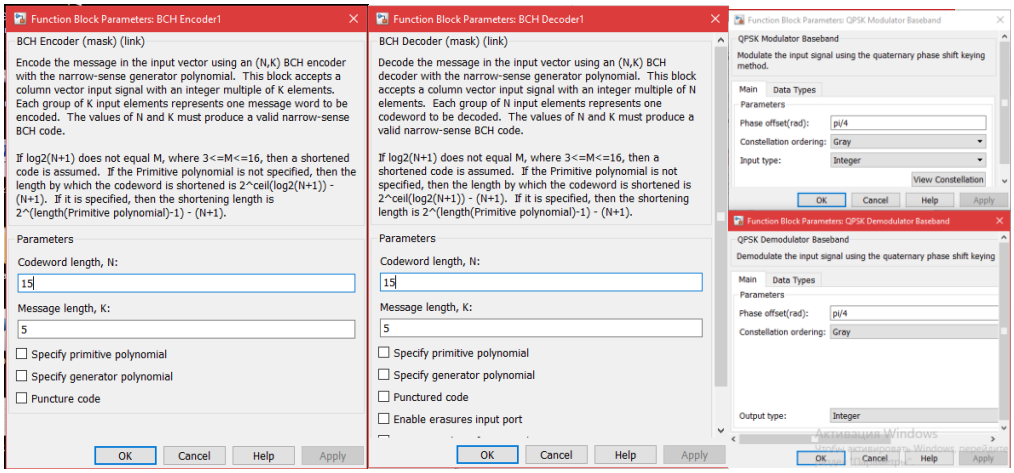
Блок параметрлерін баптауды дискретті дабыл көзі мысалында қарастырайық. Дабыл көзі параметрлерін тек бір кезеңде орнатуға арналған панель түрі көрсетілген.

Бірінші жолда сигналдардың жүру кезеңі секундтартарда және белсенді шығу нөмірі белгіленеді. Мысалы, 5,1 мәндерін орнату, хабарлама көзінің кездейсоқ комбинациясының жүру кезеңі 5 секунд, ал блоктың белсенді шығуы

1 нөмірімен шығу дегенді білдіреді. Екінші жол кездейсоқ сан датчигінен ақпараттық таңбаларды оқу жиілігін көрсетеді. Әдетте бұл жиілікті 1/kқатынасынасәйкес орнатады , мұндak – кодтық комбинациядағы ақпараттық символдар саны.

Үшінші жолда кездейсоқ кодтық комбинацияның жүру циклі белгіленеді. 1 орнату кезінде цикл модельдік уақыт аяқталғанға дейін қайталанады. 0 орнату кезінде цикл тек бір рет қайталанады. Көрсетілген әдістер модельді жөндеу үшін қажет.

Төртінші жолда блоктың белсенді шығуы анықталады.



Сурет 3.2 – Сигнал көзі параметрлерін орнату үшін панельдер түрі

Бірінші зерттеу жұмысының тәжірибесін пайдалана отырып, тұрақты параметрлері бар ECA-да БЧХ кодтарын қолдана отырып, жүйені зерттеуді орындау. 0.2 тең ECA (екілік симметриялық арна)символына қате ықтималдығын орнату ұсынылады.

1. T мәнін дәлел ретінде қабылдай отырып, тәуелділік графигін құру, ал функцияның символына қатенің ықтималдығы бойынша алынған статистикалық деректер. Кестені құру үшін функционалдық тәуелділіктің бейнелеу үлгісі алдыңғы зерттеу жұмысында келтірілген.

2. K/N ақпаратты берудің салыстырмалы жылдамдығын аргументке ала отырып, тәуелділік графигін құру, ал функцияның символына қателердің ықтималдығы бойынша кодтық деректер.

3. Кестелерді шығару бағдарламасының мысалдары төменде келтірілген:

```
1. x = [4  11  26  59];
2. y=[0.010.020.060.1];
3. x1 = [4  11  26  59];
4. y1 = [0.001 0.01 0.012 0.1];
5. semilogy(x,y,x1,y1), grid
```

Зерттеу нәтижелерін оқытушыға тексеру үшін ұсыну және есепке енгізу. Байланысшылардың Гаусс арнасын пайдаланған кезде БЧХ кодтарымен деректерді беру жүйесін зерттеу

Тәжірибиенің осы бөлігін орындау үшін:

a) БЧХ кодтарын пайдалана отырып эталондық үлгі негізінде модель құру;

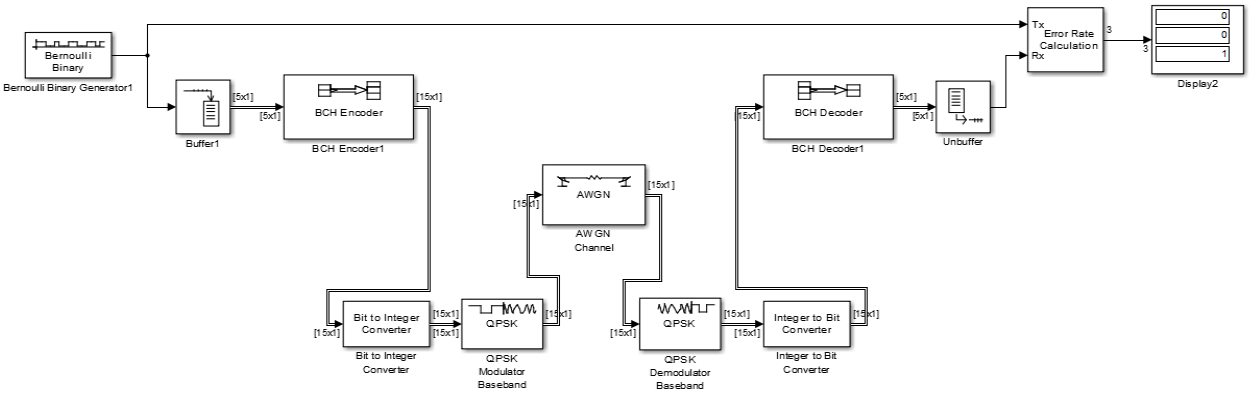
b) модулятор мен демодуляторды пайдалана отырып, Гаусс кедергілері бар арнаға бөгет тұрақты коды бар жүйені қосу;

c) артық кодсыз арнаны және арналарды кодтаумен салыстыруды жүргізу;

d) нәтижелерді кесте түрінде ресімдеу.

Commlibv1 командасын пайдалана отырып, экранда байланыс арнасының құрылымдық сұлбасын шақыру және Error control coding ақпаратты кодтау блогын белсендіру. Modulation блогын белсендіру және ашылған Librarутерезесінде: com_modu Digital mo/dem блогын екі рет басыңыз. Сандық модемдер терезесі ашылады. Бұл терезеде екі рет басу арқылы MASS demoжасыл түс блогын белсендіріп, виртуалды осциллографтан кейін шығару үшін монитордың экранында ашылған терезені сақтау қажет.

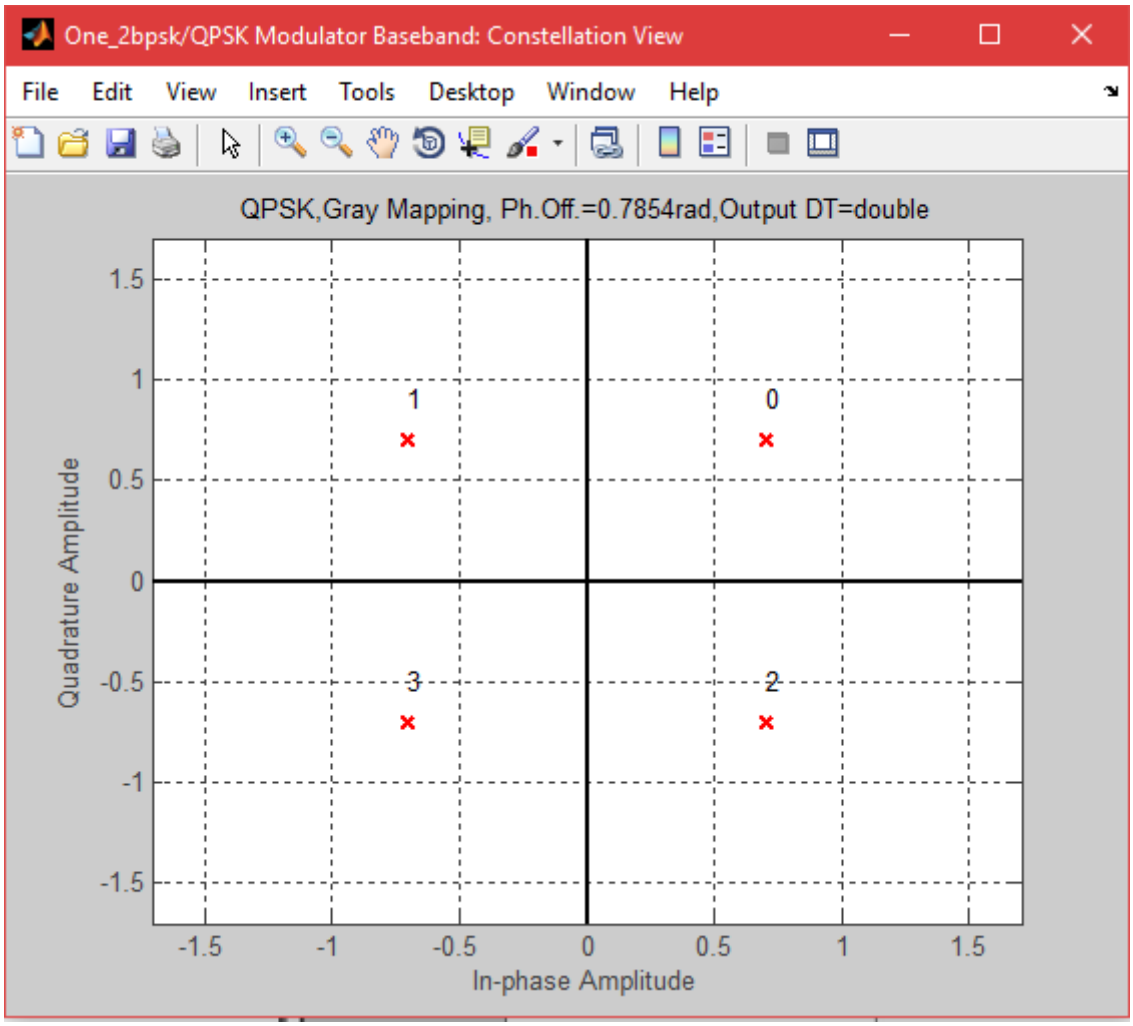
Library: com_mode терезесінде қажетті модельді дайындау үшін S-QASKdemo2 жасыл түсті демо блогін іске қосып және 15 суреттегі үлгі бойынша моделді жинаңыз.



Сурет 3.3 – QPSK модуляция кезінде БЧХ кодтарын зерттеуге арналған үлгі

Бұл модельде 4 позициядағы квадраттық-фазалық модуляция қолданылады.Дабыл көзі деректерді ондық ретпен 0-ден 15-ке дейін береді, олар байланыс арнасында өңделетін екілік векторға айналады.Мұндай жеткізу тәсілінің себебі, энергетикаға және жиіліктер белдеуіне елеулі шектеулер болған кезде ақпаратты берудің сенімділігі мен жылдамдығын бір мезгілде арттыру қажеттігінен тұрады.Дабылдарды нөмірленуі 16 суретте көрсетілген. Модельде жаңа элемент Displayблогын қолдану болып табылады. Бұл блок скаляр тәрізді , векторлық шамаларды шығару үшін пайдаланылуы мүмкін. Егер көрсетілген мән вектор болса, онда бастапқы терезе автоматты түрде өзгереді, ол блоктың төменгі оң жақ бұрышында кішкентай қара үшбұрыштың

пайда болуын көрсетеді. Вектордың әрбір элементі үшін өз шағын терезесі жасалады, бірақ олар көрінетін болуы үшін блок кескінін созу қажет. Ол үшін блокты бөліп алу керек, курсорды оның бұрыштарының біріне апарып, тышқанның сол батырмасын басу керек және оны босатпай, блоктың бейнесін қара үшбұрыш жоғалатындай етіп созу керек.



Сурет 3.4 – Сигналдық-кодтық құрылымдағы элементтердің нөмірленуі

Демек, ақпарат көзі жүйеге түсіретін ақпараттық элементтердің саны 4-ке еселенген болуы тиіс.

Жұмыс барысында модельдің әрбір блогының параметрлерін зерттеу қажет және Гауссовск байланыс арнасындағы символдың бұрмалану ықтималдығын өзгертіп, олардың ұзындығы әр түрлі, бірақ бірдей түзету қабілеті кезінде БЧХ кодтарының мүмкіндіктерін зерттеу қажет. Хабарлама көзі, БЧХ код кодері және байланыс арнасы үшін бастапқы деректер 17 суретте көрсетілген.

Бұл модельде оны іске қосу үшін басты мәзір жолында Simulation және одан әрі Start таңдаңыз. Модельдің атрибуттары жинақталған жұмыс

тәжірибесіне сүйене отырып, хаттамада және есепте міндетті түрде көрсете отырып орнату.

Есеп дайындау үшін зерттеу нәтижелерін бір кестеге еңгізу ұсынылады. Аргумент үшін k көрсеткішін, ал таңбаны қате қабылдаудың алынған ықтималдығы үшін қабылдаған орынды. Тапсырманың осы тармағын орындау үшін, командалық жолда кестелерді шығару бағдарламасын теру қажет. Мысалы, екі кестені шығару бағдарламасы келесідей түрге ие:

```
1. x = [4  11  26  59];
2. y=[0.010.020.060.1];
3. x1 = [4  11  26  59];
4. y1 = [0.001 0.01 0.012 0.1];
5. semilogy(x,y,x1,y1),
```

Enter-ді басу және оқытушыға электрондық түрде тексеру кестесін ұсыну, содан кейін кестені зерттеу жұмысы бойынша есепке көшіру.

ҚОРЫТЫНДЫ

Дипломдық жұмыста бөгеуілге тұрақты сызықты блокты кодтардың қазіргі заманда маңыздылығы жайында жазылды. Ақпараттың тұтынушыға бұрмаланусыз жеткізілуін қамтамассыз ететін кодтарға аналитикалық шолу жасалынып, оларға сипаттама берілді. Сызықты блокты кодтардың қолданылуы, артықшылығы мен параметрлері айтылды. Бөгеуілге тұрақты кодтардың код аралығының маңыздылығы айтылып, есептеулер арқылы көрсетілді. Қателерді тауып оларды түзету коэффициенттерінің формуласы көрсетіліп, оған сараптама жасалынды. Келесі кезеңде БЧХ коды мен Рид – Соломон кодтары қарастырылды және мысалдар келтіріліп, оларға есептеулер жүргізілді. БЧХ кодын кодтаған жағдайда n = 15, S = 2деп алып, ақпараттардың соңына қосымша символдар қосылды, S мәнінебайланысты екі палиномды көбейту арқылы құраушы полиномды алдық, ол полином мына түрге ие болды $x^8+ x^7+ x^6+ x^4+1$.Алынған шешімдер бойынша құраушы матрицалары мен тексеруші матрицаның жұмысы түсіндірілді. Рид – Соломон кодына мысал ретінде бес символдан тұратын «Хакер» сөзі «лемма» сөзіне кодталды.

Компьютерлік MATLAB бағдарламасында БЧХ кодына мысалдар келтіріліп және көріністері көрсетілді. Көріністерде кодерге дейінгі және кодерден кейінгі сұлбалары сипатталды. Квадратты фазалық модуляция қолданылып, алынған нәтижелердің сұлбасы көрсетіліп түсіндірілді.

Дипломдық жұмысты орындау барысындағы жинақталған мәліметтер мен есептеулерден алынған нәтижелерді бөгеуілге тұрақты кодтарды зерттеу мақсатындағы зертханалық жұмыстарда қолдануға болады.

ПАЙДАЛАНЫЛҒАН ӘДЕБИЕТТЕР ТІЗІМІ

1 Блейхут Р. Теория и практика кодов, контралирующих ошибки. – Москва «Мир», 2008

2 Вернер М. Основы кодирования.–Техносфера, 2004

3 Давыдов А. В. Введение в теорию помехоустойчивого кодирования.– Нижный Новгород, 2014.

4 Журавлев В. Г. Помехоустойчивые коды. - Владимир, 2013

5 Зюко А. Г. Помехоустойчивость и эффективность систем передачи информации.– Радио связь, 2007.

6 Кларк, Дж. Кодирование с исправлением ошибок в системах цифровой связи.– Радио и связь, 2009.

7 Злотник Б. М. Помехоустойчивые коды в системах связи.– Радио и связь, 2009.

8 Макаров А. А. Методы повышения помехоустойчивости систем связи.– Новисибирск, 2012.

9 Лазарев Ю. MatLAB 5.X. – Киев: Ирина,2010

10 Васильев К.К. Основы помехоустойчивых кодов.– Ульяновск УлГТУ, 2008.

11 Прокс Дж. Цифровая связь.- М: Радио и связь,2000.

12 Витерби А. Д. Принципы цифроввой связь и кодирования. – М: Радио и связь, 1982.

13 Мак-Вильямс Ф. Дж. Теория кодов, испровляющих ощибок. – М: Связь,1979.

14 Питерсон У. Коды, испровляющие ощибки.– М: Мир,1979

15 Хэмминг Р.В. Теория кодирования и теория информации. – М: Раддио и связь, 1999.

16 Кларк Дж, Кейн Дж. Кодирование с испровлением ошибки в системах цифровой связи. –М: радио и связь, 2004.

17 Афанасьев В. Б. Помехоустойчивое кодирование и надежность ЭВМ.– М: Наука , 1987.

18 Берлекэмп Э. Алгебраическая теория кодирования. – М: Мир, 1971.

19 Габидулин Э.М. Кодирование в радиоэлектронике. – М: Радио и связь, 1986.

20 Дуденко С.М. Минемальная блоковая длина линейного q-ичного кода с заданным размерностью и кодовым расстоянием. – М: Мир, 1984.

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ және ҒЫЛЫМ МИНИСТРЛІГІ
Қ.И. СӘТБАЕВ атындағы ҚАЗАҚ ҰЛТТЫҚ ТЕХНИКАЛЫҚ ЗЕРТТЕУ УНИВЕРСИТЕТІ

СЫН ПІКІР

дипломдық жұмыс

Темирханов Орайбек Абдыхамитулы

5В071900-Радиотехника, электроника және телекоммуникациялар

Тақырыбына: «Бөгеуілге тұрақты LBC кодының қолданылуының анализі»

Орындалды:
а) графикалық бөлімі 11 бет;
ә) түсіндірме жазбасы 50 бет.

ЖҰМЫСҚА ЕСКЕРТУ ЖАСАУ

Бұл дипломдық жұмыста бөгеуілге тұрақты сызықты блокты кодтарды зерттеу мақсаты қойылған.

Дипломдық жұмыстың бірінші бөлімінде сызықты блокты кодтарға сипаттама беріліп олардың параметрлері мен артықшылықтары көрсетілген.

Жұмыстың екінші бөлімінде бөгеуілге тұрақты кодтардың формулалары мен мысалдар келтіріліп олардың өзара айырмашылықтар көрсетілген. Ол айырмашылықтарды көру үшін екі түрлі LBC кодтарды алып олардың кодталу және декодталу процестерінің есептеулері жасалынған.

Компьтерлік бағдарлама көмегімен бөгеуілге тұрақты БЧХ кодының моделі іске асырылып, олардың кодталған және декодталған мәндері алынып көріністеріне сипаттама берілді.

Дипломдық жұмыста стилистикалық және грамматикалық қателер орын алған, бірақ бұл дипломдық жұмыстың өзектілігін төмендетпейді.

Дипломдық жұмыс жоғары оқу орындарының талаптарына сай жағары дәрежеде жазылған және көрсетілген нәтижелер мамандық бойынша ғылыми бағытқа жауап береді.

Жұмыстың бағасы

Жалпы, дипломдық жұмыс "90" (А-) өте жақсы деген бағаға, ал студент Темирханов О.А дипломдық жұмыс 5В071900 – Радиотехника, электроника және телекоммуникация мамандығы бойынша техника және технологиялар «бакалавр» академиялық дәрежесіне ұсынылады.

Пікір беруші
ҚазҰАУ, ЭУжА каф. меңгерушісі,
доктор PhD.,
қауымдастырылған профессор
Ж.С. Шыныбай
«25» 04 2019

Ф ҚазҰТЗУ 704-24. Пікір

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ және ҒЫЛЫМ МИНИСТРЛІГІ
Қ.И. СӘТБАЕВ атындағы ҚАЗАҚ ҰЛТТЫҚ ТЕХНИКАЛЫҚ ЗЕРТТЕУ УНИВЕРСИТЕТІ

ҒЫЛЫМИ ЖЕТЕКШІНІҢ
СЫН-ПІКІРІ

дипломдық жұмысына

Темирханов Орайбек Абдыхамитулы

Мамандық 5В071900-Радиотехника, электроника және телекоммуникациялар

Тақырыбына: «Бөгеуілге тұрақты LBC кодының қолданылуының анализі»

Дипломдық жұмыста бөгеуілге тұрақты кодтардың анализін жасап оларды зерттеу мақсаты қойылған

Дипломдық жұмысқа келесі бағыттар бойынша зерттеу тапсырмалары қойылған:

–Бөгеуілге тұрақты кодтардың түрлеріне аналитикалық шолу жасалынған;

–LBC кодтарының параметрлері мен алгоритмдерін көрсету;

–Бөгеуілге тұрақты кодтардың мысалдарын есептеу;

–Сызықты блокты кодтарға бағдарламалық көріністерін көрсету.

Дипломдық жұмыста бөгеуілге тұрақты сызықты блокты кодтарға аналитикалық шолу жасалынды.

Сызықта блокты кодтарды бағдарлама арқылы зерттеу үшін MATLAB бағдарламасы қолданылды. Ол үшін келген сигналды екілік код түріне түрлендіретін зерттеуге керек ақпарттарды толығымен анықтап сипаттама жасалынды.

Сигналдарды бөгеуілге тұрақты код ретінде түрлендіруі және қателерін табауға есептері шығарылды..

Сызықты блокты кодтарды MATLAB бағдарламасында ақпараттарды кодтауға арналған схемалардың кірісіндегі және шығысындағы көріністері көрсетілді

Дипломдық жұмыс жоғары оқу орындарының талаптарына сай жағары дәрежеде жазылған және көрсетілген нәтижелер мамандық бойынша ғылыми бағытқа жауап береді.

Жалпы, дипломдық жұмысты "90" (А-) өте жақсы деген бағаға, ал студент Темирханов О.А. 5В071900 – Радиотехника, электроника және телекоммуникация мамандығы бойынша техника және технологиялар «бакалавр» академиялық дәрежесіне ұсынылады.

Ғылыми жетекші
ЭТжҒТ кафедрасының
қауымдастырылған профессоры
_____ Л.Б. Илипбаева
«24» 04 2019 ж.