Лекция №11. Шеннон-Фано әдістемесі және Хаффманның криптографиялық шифрлау алгоритмі.

Лекцияның оқыту нәтижиелері: Шеннон-Фано әдісінің құрылымы және алгоритмін, Хаффман шифрлау алгоритмінің тиімділігі мен ерекшеліктерін біледі. Шеннон-Фано және Хаффман әдістерін салыстыра алады.

Лекция мазмұны:

1. Шеннон-Фано әдісі

Деректерді қысу қазіргі заманғы ақпараттық технологияларда негізгі рөл атқарады, берілетін және сақталатын ақпараттың көлемін азайтуға мүмкіндік береді. Тиімді кодтау алгоритмдері сапаны жоғалтпай деректерді сақтау және беру шығындарын қысқартуға көмектеседі. Бұл саладағы неғұрлым маңызды бағыттардың бірі префикстік кодтау болып табылады, ол кезде әрбір символға бірегей екілік код беріледі. Бұл жұмыста екі белгілі алгоритм қарастырылады: Шеннон-Фано кодтау және Хаффман кодтау.

Шеннон-Фано кодтауы XX ғасырдың ортасында әзірленді және ақпаратты оңтайлы кодтаудың алғашқы әрекеттерінің бірі болды. Оның қағидаты олардың пайда болу жиілігіне байланысты символдарды топтарға бөлуге негізделген. Бұл әдіс біркелкі кодтаумен салыстырғанда кодтық сөздің орташа ұзындығын едәуір азайтуға мүмкіндік береді. Алайда ол әрдайым жақсы нәтиже бере бермейді, бұл одан әрі тиімді алгоритмдерді жасауға әкелді. Осыған қарамастан, Шеннон-Фаноны кодтау ақпарат теориясының даму тарихының маңызды бөлігі болып қала береді.

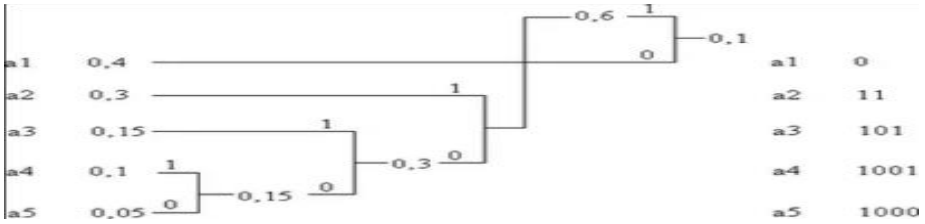
Хаффман коды префикстік кодты құрудың жетілдірілген әдісін білдіреді. Ол кездесетін жиілігі неғұрлым аз символдар түбірінен алшақ орналасқан бинарлық ағашты құруға негізделген. Нәтижесінде бұл алгоритм әрқашан мүмкін болатын ең төменгі орташа ұзындықтағы кодты генерациялайды. Хаффманды кодтау ZIP, JPEG және MP3 сияқты қазіргі заманғы деректерді сығу жүйелерінде кеңінен қолданылады. Оның тиімділігі мен қарапайымдылығы оны осы саладағы ең көп сұранысқа ие алгоритмдердің біріне айналдырды.

Кодтаудың екі әдісін салыстыру олардың артықшылықтары мен кемшіліктерін бағалауға мүмкіндік береді. Хаффман коды, Шеннон-Фанодан айырмашылығы, әрқашан оңтайлы код жасайды, бірақ көбірек есептеу ресурстарын талап етеді. Сонымен қатар, Шеннон-Фано әдісін іске асыру оңай, бірақ ол кодтардың ең аз ұзындығын бермейді. Бұл айырмашылықтарды түсіну тиімді кодтау принциптерін жақсы түсінуге көмектеседі.

Шеннон-Фано кодтау - деректерді қысу үшін пайдаланылатын префикстік кодтау әдісі. Ол бастапқы хабардағы таңбаларды бөлу

ықтималдығына негізделген. Символдар пайда болу жиілігінің азаюы бойынша реттеледі, содан кейін шамамен тең жиынтық ықтималдығы бар екі топқа бөлінеді. Әрбір топқа бит (0 немесе 1) беріледі және әрбір кіші топ үшін процесс рекурсивті түрде жалғасады. Нәтижесінде әрбір символға қысу үшін пайдалануға болатын бірегей екілік код беріледі.

Әдістің басты артықшылығы - іске асырудың салыстырмалы қарапайымдылығы және әртүрлі деректер жиынтығына бейімделу мүмкіндігі. Алайда, Шеннон-Фаноны кодтау әрдайым кодтардың оңтайлы ұзындығын бермейді, себебі таңбаға биттердің ең аз орташа санына кепілдік бермейді. Кейбір жағдайларда алынған код Хаффман алгоритмін пайдаланғаннан ұзын болуы мүмкін. Бұл әдіс топтарға бөлудің оңтайлылығын әрдайым ескермейтіндіктен болып отыр. Осыған қарамастан, Шеннона-Фано алдын ала кодтауды түсіну үшін жақсы негіз болып табылады.



1-сурет. Шеннона-Фано шифрлау әдісі алгоритмі

Алгоритм деректерді қысу жүйелерінде қолданылады, бірақ қазіргі заманғы технологияларда оны неғұрлым тиімді әдістер жиі ауыстырады. Мысалы, Хаффман коды әрдайым символдардың статикалық ықтималдығы үшін оңтайлы шешім береді. Алайда, Шеннона-Фано кодтарды құру принциптерін түсінуге көмектесетіндіктен, оқу мақсаттарында маңызды болып қала береді. Бұдан басқа, ол ақпарат теориясында пайдаланылған алғашқы алгоритмдердің бірі болды. Оны Клод Шеннон мен Роберт Фано 1949 жылы хабарламаларды тиімді кодтау жөніндегі зерттеулер шеңберінде әзірлеген.

Алгоритм:

1) Символдардың кездесу жиілігін анықтау
2) Символдарды жиілік бойынша кему ретімен орналастыру
3) Символдар тізімін ықтималдықтары тең екі топқа бөлу
4) Бірінші топқа «0», екінші топқа «1» беру
5) Әр топқа рекурсивті түрде қайталау

2. Хаффман алгоритмі

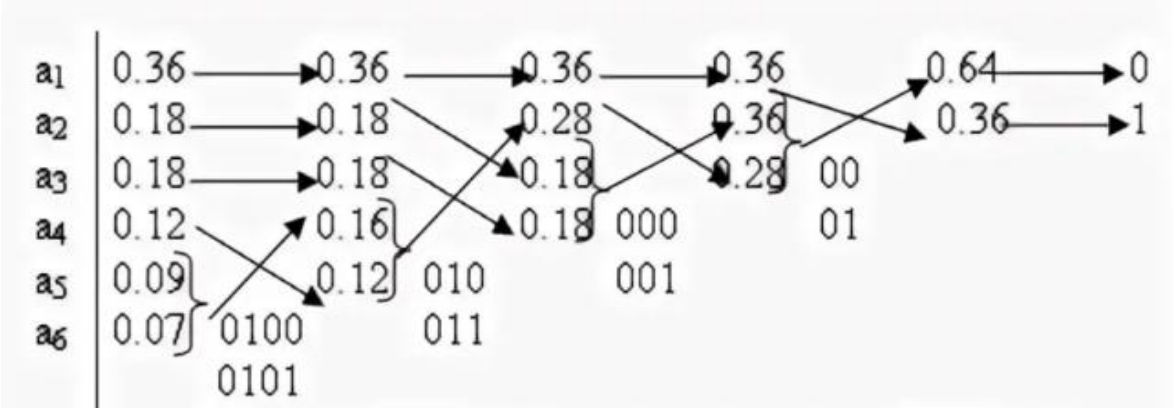
Дэвид Хаффман (David A. Huffman) информатика саласындағы американдық математик және инженер болған. Ол 1925 жылы туылған және оның атына аталған кодтау алгоритмін әзірлеудің арқасында танымал болды. 1951 жылы Массачусетс технологиялық институтының (MIT) студенті ретінде ол символдарды алдын ала кодтаудың оңтайлы әдісін тапты. Оның жұмысы ақпаратты сақтау мен берудің қазіргі заманғы жүйелерінде қолданылатын деректерді қысуға негіз болды. Хаффманды кодтау бейнелер, аудио және мәтіндік құжаттар сияқты файлдарды қысу саласындағы маңызды құралға айналды. Оның ашылуы студенттік жоба аясында жасалғанымен, ол информатиканың дамуына зор ықпал етті.

Хаффман оңтайлы кодтау алгоритмдерін зерттеді және ақпаратты өңдеумен байланысты міндеттермен айналысады. Оның әдісі таңбалардың пайда болу жиілігіне байланысты кодтардың айнымалы ұзындығын пайдалану арқылы файлдардың өлшемін азайтуға мүмкіндік берді. Әрбір символға бірдей бит саны берілетін біркелкі кодтаудан айырмашылығы, Хаффман кодтауы жиі символдарға қысқа кодтар және сирек кездесетін ұзын кодтар тағайындайды. Бұл принцип ZIP, JPEG және MP3 сияқты алгоритмдерде қолданылады, бұл оны әмбебап етеді. Осы әдістің арқасында деректерді сақтау және оларды байланыс арналары арқылы беру тиімділігі артты. Хаффманның ғылымға қосқан үлесі ондаған жылдан кейін де елеулі болып қала береді.

Хаффман кодтаудан басқа, схемотехника және ақпаратты өңдеу саласындағы зерттеулермен айналысқан. Ол оңтайландырудың, оның ішінде электрондық схемаларды автоматты жобалауға байланысты әртүрлі міндеттермен жұмыс істеді. Мансап бойы ол Санта-Круздағы Калифорния университетінде сабақ беріп, ғылыми зерттеулерін жалғастырды. Оның жұмыстары қысқарту және деректерді тиімді беру әдістерін одан әрі дамытуға алып келді. Ол әзірлеген алгоритмдердің күрделілігіне қарамастан, оның идеялары күнделікті өмірде қолданылады - суреттердің қысылуынан бастап интернетте деректерді таратуға дейін. Дэвид Хаффман 1999 жылы қайтыс болды.

Хаффманды кодтау - бұл символдардың жиілік талдауына негізделген деректерді қысу әдісі. Ол берілетін немесе сақталатын ақпараттың көлемін шығынсыз тиімді азайтуға мүмкіндік береді. Алгоритм таңбаларға айнымалы кодтар береді: таңба неғұрлым жиі кездессе, оның коды соғұрлым қысқа болады. Нәтижесінде неғұрлым кең таралған таңбалар биттердің азымен, ал сирек белгілер - үлкенімен кодталады. Бұл Хаффманды кодтауды ASCII тіркелген 8-биттік кодтау

сияқты стандартты әдістерге қарағанда тиімдірек етеді. Бұл алгоритм ZIP, JPEG және MP3 қоса алғанда, деректерді қысу пішімдерінде кеңінен қолданылады.



2-сурет. Хаффман шифрлау әдісі алгоритмі

Ағаш отырғызылғаннан кейін әрбір символға бірегей екілік код тағайындалады. Ағаштың солға қарай қозғалысы «0», ал оңға қарай - «1» деп белгіленеді. Түбіріне жақын орналасқан символдар неғұрлым қысқа кодтар алады, ал одан әрі орналасқандар - ұзын. Бұл мәтінді кодтаудың орташа ұзындығын барынша азайтуға мүмкіндік береді. Алынған кодтар жиыны кіріс деректеріндегі таңбаларды олардың екілік көріністеріне ауыстыру үшін пайдаланылады. Осылайша, бастапқы мәтін айтарлықтай қысқа болады, бұл тиімді қысуды қамтамасыз етеді.

Алгоритм:

1) Әр символды түйін ретінде қарастыру
2) Ең кіші жиілікті екі түйінді біріктіру
3) Бір түйін қалғанша жалғастыру
4) Сол жаққа «0», оң жаққа «1» тағайындау

3. Мысал

Берілсін мәтін: «ААААББВД»

Жиіліктер: А-3, Б-2, В-1, Д-1

Хаффман кодтау нәтижесі: А=0, Б=10, В=110, Д=111

Шифрланған мәтін: 000101101111

4. Салыстыру

Шеннон–Фано әдісі – логикалық топтастыруға негізделеді, ал Хаффман әдісі – ең тиімді код ұзындығын қамтамасыз етеді. Қазіргі компрессия жүйелерінде (ZIP, JPEG, MP3) Хаффман кең қолданылады.

Оқытудың техникалық құралдары: Компьютер, ноутбук, интернет, интерактивті тақта.

Лекция оқудың тәртібі, оқыту әдістері мен түрлері:

Оқудың тәртібі:

- Лекция түрінде түсіндіру және мысалдар арқылы көрсету
- Шифрлау тәсілдерін кезең-кезеңмен талдау және тәжірибе жүзінде орындау
- Қорытынды сұрақтар мен талқылау

Оқыту әдістері мен түрлері:

- Түсіндірмелі-баяндамалық әдіс
- Көрнекілік және демонстрациялық әдіс
- Практикалық тапсырмалар орындау
- Интерактивті сұрақ-жауап және топтық талқылау

БӨЖ және ОБӨЖ тапсырмалары,олардың түрлері мен орындалуына қойылатын ұпайлардың үлестері:

БӨЖ: Шеннона-Фано және Хаффманның криптографиялық шифрлау алгоритмі арқылы шифрлау мысалдарын орындау, берілген мәтінді шифрлап және дешифрлап орындауы қажет. Бұл жұмыс жалпы бағалаудың 60-баллды құрайды.

БӨЖ бағалау критерийлері:

- Теориялық материалды түсіну және қолдану -20 балл
- Бағдарламаны дұрыс жазу немесе есепті шешу -25 балл
- Нәтижелердің дәлдігі мен түсіндіру сапасы -15 балл

Барлығы: 60 балл

ОБӨЖ: Шеннона-Фано мен Хаффманның криптографиялық шифрлау алгоритмі арқылы шифрлау алгоритмін қолданып мәтінді шифрлау және екі әдістің айырмашылығын талдау бойынша қысқаша есеп дайындау. Бұл жұмыс жалпы бағалаудың 40-баллды құрайды.

ОБӨЖ бағалау критерийлері:

- Тапсырманың толық және уақытылы орындалуы -15 балл
- Теориялық және практикалық түсіндіру сапасы -15 балл
- Топтық жұмысқа белсенді қатысу, сұрақтарға жауап беру-10 балл

Барлығы: 40 балл

Жалпы бағалау үлесі:

- **БӨЖ — 60% (60 балл)**
- **ОБӨЖ — 40% (40 балл)**

Пайдалынатын әдебиеттер тізімі:

Негізгі:

1. Г. Камалова, А. Х. Касымова, Л. Б. Диярова. «Ақпараттық қауіпсіздікті басқару». Оқу құралы. /- Алматы: Альманахъ, 2020. - 128 с.

2. Кауфман Ч., Перлман Р., Спеснер М. *Network Security: Private Communication in a Public World.* – Prentice Hall, 2016.

3. Stallings W. *Cryptography and Network Security: Principles and Practice.* – Pearson, 2022.Таненбаум Э. Компьютерлік желілер. – Алматы: Эверо, 2019

4. Нечаев В.И. Элементы криптографии основы теории защиты информации. / В. И. Нечаев. - М.: Высшая школа, 1999. - 109 с.

Қосымша:

1. Ахметова, С. Бағдарламалау технологиясы: Лекция жинағы. / ЮКГУ им. М.О.Ауезова - Шымкент: ОҚМУ, 2007.-51б. https://rmebrk.kz/book/50006

2. Ж.З.Сатмаганбетова. Бағдарламалау тілдері және технологиясы: Оқу-әдістемелік куралы./Қостанай: А. Байтұрсынов атындағы ҚМУ, 2014. - 64 б. http://rmebrk.kz