AZƏRBAYCAN RESPUBLİKASI TƏHSİL NAZİRLİYİ
AZƏRBAYCAN DÖVLƏT İQTİSAD UNİVERSİTETİ
MAGİSTRATURA MƏRKƏZİ

Əlyazması hüququnda

MUSTAFAYEV MUSTAFA CEYHUN oğlu

Telekommunikasiya sistemində informasiyanın qənaətlə kodlaşdırılması və səhvsiz ötürülmə məsələsinin tədqiqi

Şifrə və adı: 060632 - İnformasiya texnologiyaları və sistemləri mühəndisliyi
İxtisaslaşma: İnformasiya texnologiyaları və telekommunikasiya sistemləri

Magistr dissertasiyası

Elmi rəhbər:	**r.f.d., dos. Qasımov B.M.**
Magistratura proqramının rəhbəri:	**f.r.e.n., dos. Əliyeva T.Ə.**
Kafedra müdiri:	**tex.e.d., akad. Abbasov Ə.M.**

BAKI – 2020

Mündəricat

Giriş

Mövzunun aktuallığı. İnformasiyanı sürətli, dəqiq və səmərəli şəkildə çatdırmaq hər zaman diqqət mərkəzində olan mövzulardan biri olmuşdur.

İnsanların məsafəli ünsiyyətdə ilk cəhdləri son dərəcə məhdud idi. Qədim dövrlərdə insanlar əlaqə qurmağa cəhd edərkən məhdud bir coğrafi bölgə üzərindəki məlumatları kodlaşdırmaq üçün yanğın və tüstü siqnallarına, eləcə də baraban mesajlarına etibar edirdilər. Bu siqnalların "təhlükəsiz", "təhlükə" və ya "qələbə" kimi çox sadə, əvvəlcədən qərar verilmiş mənalara sahib olması lazım idi.

Kommunikasiya proseslərinin tarixinə nəzər salaraq müasir telekommunikasiya sisteminin yaranması üçün hansı mərhələlərin keçildiyini görə bilərik:

1. İlk mexaniki telefon - 1672-ci ildə ilk dəfə Robert Huk akustik telefonu kəşf etdi.

2. Semafor xətləri(optik teleqraflar**)** - 1790-cı ildə Çappe qardaşları ilk optik teleqraf sistemini yaratdılar. Teleqraf mexaniki qollarını çevirib bir qüllədən digərinə mesajlar göndərirdi. Bu, Avropada ilk telekommunikasiya sistemi idi.

3. Elektrikli teleqraf - Samuel B. Morze, dostları Alfred Vail və Leonard Qeyl ilə birlikdə səsyazma teleqrafı ideyası üzərində işləyirdi. 1838-ci ildə onlar iki teleqrafı kabellə bir-biri ilə əlaqələndirərək düymələrin köməyi ilə mesaj göndərə bildilər.

4. İlk trans - Atlantik teleqraf kabeli - 19-cu əsrin 60-ci illərində İngiltərə və ABŞ-da çoxlu teleqraf stansiyaları var idi və ölkə daxilində müntəzəm olaraq əlaqə qurmaq üçün istifadə edilirdi. Ancaq Nyu-Yorkdan olan Cyrus Field adlı bir mühəndis İngiltərə və ABŞ arasında ilk trans-atlantik telefon xəttini çəkmək istədi. Bu layihə bir çox uğursuzluqla qarşılaşsa da, nəhayət 1858-ci ilin avqustunda tamamlandı.

5. Telefon - 1876-cı il Alexander Qraham Bell üçün böyük bir il oldu. ABŞ-a eşitmə əngəlli insanlar üçün dərs deməyə gəldikdən sonra səsi elektrik siqnalları vasitəsilə ötürməyin yolunu tapmağa çalışırdı. 1876-cı ilin martında Alexander Qraham Bell telefonu icad etdi.

6. Simsiz teleqraf - Nikola Tesla 1893-cü ildə radio dalğalarını simsiz bir ötürücü vasitəsi ilə müvəffəqiylə ötürə bildi.

7. Radio - Qulyelmo Markoni 1896-cı ildə ilk uzun məsafəli simsiz ötürülməni həyata keçirdi. Siqnal 2 kilometr məsafəyə göndərildi.

8. Televiziya - Filip T. Farnsvorth 7 sentyabr 1927-ci ildə ilk işləyən televizoru nümayiş etdirərək tarixə keçdi. O, şəkilləri ötürmək üçün bir metod üzərində işləyirdi: kəşf etdiyi qurğu radio dalğalarını bir görüntü ilə kodlaşdırıb sonra yenidən ekrana proyeksiya edə bilirdi.

9. Fiber-optik telekommunikasiya - 1964-cü ildə Çarles Kao və George Hoçkam, məlumat ötürmək üçün istifadə olunan liflərin çirkləri olmadığı müddətcə, fiber-optik rabitənin mümkün ola biləcəyini sübut edən bir sənəd nəşr etdi. Bu da səsin işıq şüaları ilə ötürülməsinə imkan verdi.

10. Kompüter şəbəkəsi - 1969-cu ilin oktyabr ayında internetin sələfi olan ARPANET qovşaqları arasında ilk məlumatlar göndərildi. Bu ilk kompüter şəbəkəsi idi və Çarley Klin və Bill Duvall tərəfindən icad edildi.

11. Müasir dövrün ilk mobil telefonu - İxtiraçı Martin Kuper 1973-cü ildə maksimum danışıq müddəti yarım saat olan mobil telefonu kəşf etdi.

12. SMTP elektron poçtu protokolu - 1982-ci ildə Jonatan Postel, sadə mail göndərmə protokolunu hazırladı və şəbəkə vasitəsilə elektron poçtların göndərilməsi həyata keçirdi.

13. İnternet - 1 yanvar 1983-cü ildə internet rəsmi olaraq dünyada elan edildi. ARPANET köhnə şəbəkə nəzarət protokollarını(NCP) rəsmi olaraq dəyişdirdi və Transmissiya İdarəetmə Protokolu/İnternet Protokolu(TCP/IP) standart hala gəldi.

İnternetin yaranması ilə informasiya texnologiyaları sürətli inkişaf mərhələsinə keçdi.

Müasir telekommunikasiya sistemi texniki vasitələrdən və onların fəaliyyəti üçün lazım olan alqoritmlərdən ibarətdir. Telekommunikasiya sisteminin təyinatı məlumatı mənbədən alıcıya ötürməkdir.

İnformasiyanın ötürülmə prosesi ötürücü kanallar vasitəsi ilə həyata keçirilir. Ötürmə kanalının buraxıcılıq qabiliyyəti bir saniyədə ötürmə kanalından keçən informasiyanın miqdarı ilə müəyyən olunur. İnformasiyanın ötürülməsi zamanı nəzərə alınmalı olan əsas nüanslardan biri də informasiyanın təhlükəsiz və səhvsiz ötürülməsidir. Bunun üçün müxtəlif kriptoqrafiya üsullarından istifadə edilir. İnformasiya ötürülən zaman ötürmə kanalına daxil olan informasiya xüsusi alqoritm vasitəsilə şifrələnir, qəbuledici informasiyanı qəbul edən zaman şifrələnmiş informasiya dekoderin köməkliyi ilə əvvəlki halına salınır. İnformasiyanın təhlükəsiz ötürülməsi məsələsinə ilk dəfə Klod Şennon toxunmuşdur. Şennonun nəzəriyyəsində məlumatın etibarsız kanallar üzərində etibarlı şəkildə ötürülməsi prinsipləri öz əksini tapmışdır.

İnformasiya texnologiyalarının inkişafı nəticəsində emal olunan və insanlara təqdim olunan informasiyanın miqdarı sürətli şəkildə artır. İnformasiyanın miqdarının artması qərarqəbuletmə, proqnozlaşdırma, idarəetmə və digər əksər sahələrə müsbət təsir edir. Ancaq informasiyanın miqdarının artması onun məzmununun saxlanılması şərti ilə yığcam formada təqdim edilə bilməsi problemini ortaya qoyur. İnformasiyanın yığcamlaşdırılması dedikdə onun informasiya daşıyıcılarında tutduğu yerin azaldılması nəzərdə tutulur. İnformasiya daşıyıcılarına kağız parçası, sərt disk, CD, DVD və sairə misal ola bilər.

İnformasiyanın yığcamlaşdırılması qaydası onun qənaətlə kodlaşdırılması adlanır. Bu problemin üzərində ilk dəfə 1837-ci ildə Samuel Morze işləyərək yeni alqoritm təklif etmişdir. Keçən əsrin 40-cı illərində informasiya nəzəriyyəsinin

yaranması ilə informasiyanın qənaətlə kodlaşdırılması texnologiyası inkişaf etdi. İnformasiyanın yığcamlaşdırılmasının ən məşhur və sadə üsulu təkrarlanan simvolların kiçik uzunluqlu unikal simvollarla əvəz edilməsidir. İnformasiyanın yığcamlaşdırılması zamanı onun həcmi bir neçə dəfəyə qədər kiçilə bilər.

Məlumatın yığcamılaşdırılması iki üsulla edilə bilər - itkili sıxılma və itkisiz sıxılma. İtkili sıxılma, lazımsız simvolları silməklə məlumatların həcmini azaldır, itkisiz sıxılma zamanı məlumat itkisi olmur.

Huffman alqoritmi informasiyanın itkisiz yığcamlaşdırılmasında geniş istifadə edilir. Kompüter elmində və məlumat nəzəriyyəsində Huffman kodu məlumatların itkisiz sıxılması üçün istifadə olunan xüsusi prefiks kodunun müəyyən bir növüdür. Belə bir kodun tapılması və istifadəsi prosesi H.D. Huffman tərəfindən, o hələ MİT tələbəsi olan zaman hazırlanıb və "Huffman kodlaşdırması" anlayışını ortaya qoyub. Bu haqda ilk məqalə 1952-ci il tarixində "Kodların minimal sıxlaşdırılması" başlığı altında dərc edilmişdir.

İnformasiyanın yığcamlaşdırılmasının əsas məqsədləri arasında yaddaşda az yer tutması ilə yanaşı informasiyanın ötürülmə zamanını da azaltmaqdır. İnformasiyanın ötürülməsinə sərf olunan zaman dedikdə onun göndərəndən qəbulediciyə çatmasına sərf olunan zaman müddəti nəzərdə tutulur. Bu zaman müddəti informasiyanın ötürülmə sürətindən və həcmindən də asılıdır.

Şennon nəzəriyyəsində məlumatın ötürülməsi prinsiplərindən başqa onun sıxlaşdırılması prinsipləri də yer alır. Şennon-Fano alqoritmi, multimediyanın itkisiz məlumat sıxışdırılması üçün bir entropiya kodlaşdırma üsuludur.

İnformasiyanın sıxlaşdırılması və təhlükəsiz ötürülməsinin təmin edilməsinin əsas məqsədi istənilən ötürmə kanalına daxil olan informasiyanın sürətli, təhlükəsiz və itkisiz şəkildə qəbulediciyə çatdırılmasıdır.

Mövzunun məqsədi. Müasir dövrümüzdə telekommunikasiya sistemləri bütün sahələrdə tətbiq edilir. Bunun üçün də telekommunikasiya prinsiplərinin təkmilləşdirilməsi, yeni üsulların sınaqdan keçirilməsi zəruridir.

Telekommunikasiya sisteminin əsas problemlərinə informasiyanın qənaətlə kodlaşdırılması və səhvsiz ötürülmə məsələsi də daxildir. Bu problemlərin həlli üçün bir sıra üsullar tətbiq edilir. Ancaq informasiya texnologiyalarıının sürətli inkişafını nəzərə alsaq, qeyd edilən prinsiplərin də optimallaşdırılması vacibdir.

İnformasiyanın qənaətlə kodlaşdırılmasının məqsədi məzmunun saxlanılması ilə informasianın yaddaş qurğularında tutduğu yerin azaldılmasıdır. İnformasiyanı qənaətlə kodlaşdıraraq onun həcmini dəfələrlə azaltmaq mümkündür. Bunun üçün müxtəlif arxivləşdirmə proqramlarından istifadə edilir. Komputerdə arxivləşdirilmiş fayllar rar, zip və sairə kimi xüsusi formatlarda saxlanılır. İnformasiyanın qənaətlə kodlaşdırılması onun telekommunikasiya sistemi vasitəsilə mənbədən alıcıya daha sürətli ötürülməsini də təmin edir.

İnformasiyanın səhvsiz ötürülməsi maneəli və ya maneəsiz kanallar üzərindən informasiyanın mənbədən alıcıya təhrif olunmadan və təhlükəsiz yolla ötürülməsini tələb edir.

Telekommunikasiya sistemində informasiyanın qənaətlə kodlaşdırılması və səhvsiz ötürülməsi məsələsini araşdırmaq üçün informasiyanın təsviri, ehtimallı yanaşma üsulları, Şennon alqoritmi, Huffman alqoritmi ilə tanış olmaq lazımdır.

I Fəsil. Qənaətlə kodlaşdırma nəzəriyyəsində ehtimallı yanaşma üsulu

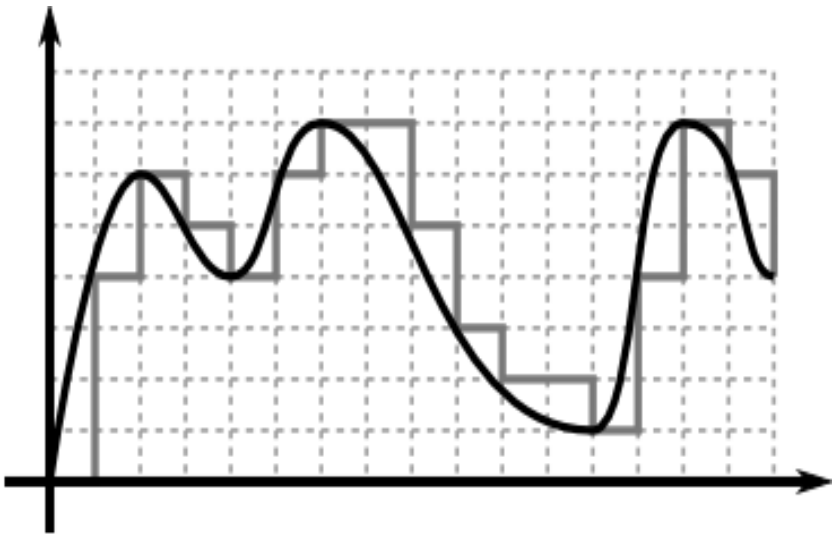
1.1 İnformasiyanın təsviri

Tətbiq sahəsinə aid informasiyanın emal, analiz və ya arxiv məqsədilə toplanmasını, saxlanmasını və istifadəçilərə çatdırılmasını təmin edən texniki, proqram və metodoloji vasitələr kompleksi informasiya sistemini təşkil edir. İnformasiya sistemi istifadəçilərin müəyyən mövzu üzrə informasiyaya olan ehtiyaclarını qarşılayır.

Təbiətdə informasiyanın ötürülməsi siqnallar vasitəsilə həyata keçirilir. Siqnalların iki növü vardır:

- analoq
- rəqəmsal

Analoq siqnallar. Bir siqnalın qrafikinə baxmaq siqnalın analoq və ya rəqəmsal olub olmadığını müəyyənləşdirməyin ən asan yoludur, bir analoq siqnalın bir dövrdə çəkdiyi trayektoriya hamar və davamlı olmalıdır.



Şəkil 1.1 Analoq siqnal hərəkət trayektoriyası

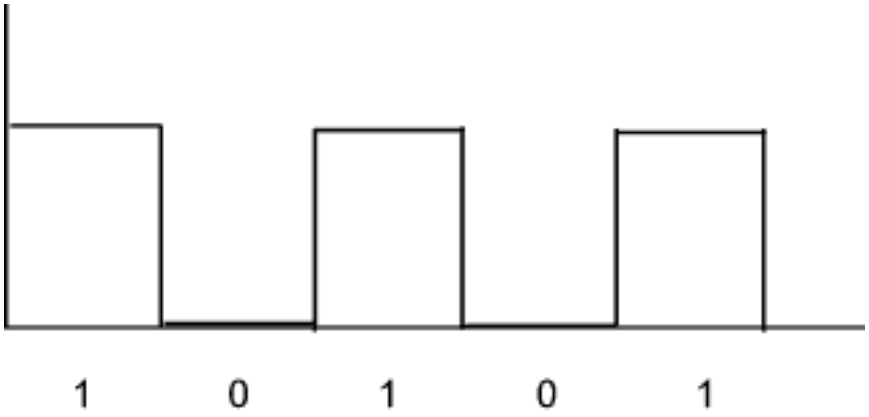
Bu siqnallar bir sıra maksimum və minimum dəyərlərlə məhdudlaşdırıla bilsə də, bu aralığın içində sonsuz sayda mümkün dəyərlər mövcuddur. Məsələn, divar yuvanızdan

çıxan analoq gərginlik -120V ilə + 120V arasında sıxışdırıla bilər, ancaq gərginlik verilmiş bu aralıqdakı istənilən dəyərə sahib ola bilər.

Video və səs ötürülməsi tez-tez analoq siqnallardan istifadə edərək ötürülür və ya yaddaşda saxlanılır. Köhnə RCA cekindən çıxan kompozit video 0 ilə 1.073V arasında dəyişən kodlaşdırılmış analoq siqnaldır. Siqnaldakı kiçik dəyişikliklər videonun rənginə və ya yerləşməsinə çox təsir edir.

Məlumatın analoq siqnallarla ötürülməsi zamanı mühitin bəzi özəllikləri istifadə edilə bilər. Fiziki dəyişən aralıq rolu oynayan çevirici tərəfindən analoq siqnalına çevrilə bilər.

Rəqəmsal siqnallar. Bu siqnalların vaxt qrafikləri kvadrat dalğalarına bənzəyir. Bütün səs və video siqnalları analoq deyildir. Video (və audio) və MIDI, I2S və ya audio üçün AC97 üçün HDMI kimi standart siqnallar hamısı rəqəmsal olaraq ötürülür.



Şəkil 1.2 Rəqəmsal siqnalın hərəkət trayektoriyası

İnteqrasiya edilmiş sxemlər arasında ən çox rəqəmsal əlaqə mövcuddur. Serial, I2C və SPI kimi interfeyslər, məlumatları rəqəmsal siqnalların kodlaşdırılmış ardıcıllığı ilə ötürür.

Rəqəmsal siqnallarda məlumatın ötürülməsi zamanı məlumat zaman aralıqlı impulslar şəkildir ötürülür və qəbul edilir.

İstənilən inormasiya istifadəyə yararlı hesab olunmur. Aşağıda şərtlər ödəndiyi halda informasiya istifadəyə yararlı hesab oluna bilər:

- tamlıq – informasiya tam şəkildə təsvir edilməlidir;
- həqiqilik – informasiya həqiqətə uyğun olmalıdır;
- qiymətlilik – informasiyanın dəyəri onun əldə edilməsinə sərf olunan resursdan daha dəyərli olmalıdır;
- əhəmiyyətlilik – informasiya ondan istifadə edəcək şəxslər üçün əhəmiyyətli olmalıdır;
- başa düşünərlik – informasiya onu əldə edən şəxslər tərəfindən aydın şəkildə başa düşülə bilməlidir.

Əldə edilmiş hər informasiya qiymətli informasiya hesab edilmir. İnformayanın qiymətli hesab edilməsi üçün onun istifadəçi şəxsə qazan gətirməsi lazımdır. Qazanc maddi, siyasi, hərbi, mənəvi və başqa formalarda ola bilər.

İnformasiyanın itirilməsinin, dəyişdirilməsinin, silinməsinin, korlanmasının qarşısını almaq üçün onun etibarlı şəkildə qorumaq lazımdır.

İnformasiya bir sıra xüsusiyyət və xarakteristikalarına görə qruplaşdırıla bilər:

- yaranmasına üsuluna görə
- ötürülmə üsuluna görə
- ifadə edilməsi formalarına görə
- ifadə edilməsi vasitələrinə görə
- istifadə yerinə görə və sairə.

Komputerin yaddaşında informasiya rəqəmsal şəkildə təsvir olunur, informasiyanın keyfiyyəti ilə daşıdığı siqnal sayı mütənasibdir. Bu formada təqdim olunan informasiya rəqəmsal informasiyadır. Beləliklə, təqdim olunma formasına görə informasiya 2 böyük qrupa ayrılır:

- analoq
- rəqəmsal

Komputer və digər rəqəmsal qurğuların yaddaşında informasiya analoq formada deyil, rəqəmsal formada saxlanılır, emal edilir. Rəqəmsal informasiya kodlaşdırılmış, diskret informasiyadır.

Analoq informasiyanı rəqəmsal informasiyaya çevirmək mümkündür. Bunun üçün analoq rəqəmsal çeviricilərdən istifadə edirlər. Analoq formalı informasiyanın rəqəmsal informasiyaya çevrilməsinə analoq-rəqəmsal çevrilməsi prosesi deyilir. Çevilmə prosesi zamanı istifadə edilən rəqəmlər nə qədər fərqli olarsa, rəqəmsal informasiyanın dəqiqliyi, diskretliyi daha çox olar. Çevrilmə zamanı əldə edilmiş informasiyanın diskretliyi nə qədər çox olarsa, rəqəmsal informasiya analoq formalı informasiyaya daha yaxın olar, informasiyanın dəqiqliyi, keyfiyyəti azalmaz. Beləliklə, analoq informasiya dedikdə, insanlar tərəfindən hissiyyat və bədən üzvləri vasitəsilə anlaşıla biləndir, rəqəmsal informasiya isə komputerin yaddaşında saxlamaq və emal edilmək üçün kodlarla təsvir edilmiş informasiyadır.

Analoq və rəqəmsal formada olmasından asılı olmayaraq informasiyanın bir sıra xassələri vardır:

- faydalı olması
- tam olması
- həqiqi olması
- qiymətliliyi
- aktual olması
- yeni olması

İnformatika elmində məlumat, fakt, xəbər anlayışları “verilənlər” termini ilə ifadə edilir. İnformatika elmində “verilən” dedikdə texniki vasitələrlə email edilməsi, saxlanılması, ötürülməsi mümkün olan rəqəmsal formada saxlanan məlumat nəzərdə tutulur.

İnformasiya resurslarından istifadə proseslərənin asanlaşdırmaq, onların operativliyini və dəqiqliyini yüksəltmək üçün informasiya proseslərini həyata keçirən

və informasiya resusrlarını texonoloji platformada cəmləşdirən metodlar, aparat və proqram vasitələrinin toplusu informasiya texnologiyasının əsasını təşkil edir.

İkilik kodlaşdırma – informasiyanın bitlər şəklində kodlaşdırılmasıdır. İkilik kodlaşdırmada hər bir simvol bit adlanır. Bit sözü ingilis dilindən "binary digit" birləşməsindən yaranıb, ikili rəqəm kimi tərcümə olunur.

Komputer texnologiyasında əsas informasiya vahidi olaraq bayt qəbul edilir, buna səbəb isə bitin həcminin kiçik olmasıdır. 1 bayt 8 bitə bərabər informasiya vahididir.

Kompüterlərdə say sistemi, simvolları fərqli yollarla təmsil etmək üçün bir yazı sistemi olaraq təyin olunur, yəni simvolları təmsil etmək üçün fərqli simvollardan istifadə edilir. İkilik, səkkizlik, onluq və onaltılıq olmaqla say sisteminin əsas dörd növü mövcuddur.

İkilik Say Sistemi, yalnız 0 və 1-lərdən istifadə edərək simvolları təsvir etməyə imkan verən say sistemidir. Hər bir say sistemində nömrələri təmsil edə biləcəyimiz yolların sayını göstərən fərqli bir baza dəyəri var. Beləliklə, ikilik say sisteminin əsası 2-dir. İkili say sistemi yalnız iki ehtimal və ya nəticə olduqda istifadə olunur. Elektrik siqnalları ilə təlimatları dəyişdirməyin ən asan yolu iki say sistemidir - açıq və söndürülmüşdür.

Ən kiçik informasiya vahidi olaraq bit qəbul edilir. Bitin ala biləcəyi qiymətlər 0 və 1 ola bilər.

Səkkizlik say sistemini 8 fərqli dəyər və ya rəqəm istifadə edərək nömrələri təmsil edə biləcəyimiz bir say sistemi olaraq təyin edə bilərik. Bu dəyərlərə 0 və 7 də daxil olmaqla bu intervaldakı rəqəmlər daxildirlər.

Say sistemləri arasında keçid mümkündür. Bunun üçün çevirmə düsturlarından istifadə edilir. Aşağıdakı nümunədə ikilik say sistemindən onluq say sisteminə keçid edilib:

Addım	İkilik say sistemi	Onluq say sistemi
Addım 1	10101_2	$((1 \times 2^4) + (0 \times 2^3) + (1 \times 2^2) + (0 \times 2^1) + (1 \times 2^0))_{10}$
Addım 2	10101_2	$(16 + 0 + 4 + 0 + 1)_{10}$
Addım 3	10101_2	21_{10}

Cədvəl 1.1.1 İkilik say sistemindən onluq say sisteminə keçid nümunəsi

1.2 Ehtimalli yanaşma üsulu

Baş verə biləcək hadisənin, situasiyanın düzgünlüyə, reallığıa olan münasibət dərəcəsi, reallaşması mümkünlüyü ehtimal anlayışını ortaya çıxarır. Ehtimal dedikdə ixtiyari hadisənin həyata keçməsinin mümkünlüyünün ədədi xarakteristikası nəzərdə tutulur.

Ehtimal elmi idrakın kateqoriyası kimi kütləvi proseslər üçün xarakterik olan hadisələr arasındakı əlaqələri özündə əks etdirir. İxtiyari hadisənin həyata keçəcəyi o zaman ehtimal edilir ki, hadisənin mövcud şəraitdə obyektiv baş verməsi mümkün olsun.

Ehtimal nəzəriyyəsi — təsadüfi hadisələri analiz edən riyaziyyatın bir bölməsidir. Tutaq ki, A hadisəsi elə bir hadisədir ki, sınaqlardan alınmış nəticəyə görə bu hadisə baş verədə bilər, verməyədə bilər.

İxtiyari C hadisəsinin ehtimalı, həmin hadisə ilə əlaqədar həyata keçirilmiş uğurlu sınaqların sayının (k) ümumi sınaqlar sayına (n) nisbətinə deyilir:

$$P(c) = k/n$$

Ehtimal dərəcəsini hesablamaq üçün əvvəlcə mümkün hadisələri hesablamaq, daha sonra isə onların arasından əlverişli hesablamaları qruplaşdırmaq lazımdır.

Ehtimalın tərifinin nəticəsi kimi aşağıdakıları vermək olar:

- Tutaq ki, k=0 qəbul edilir. Onda tərifə əsasən p=0 olur. Belə ki, hadisə üçün əlverişli sınaqlar yoxdur, hadisənin baş verməsi qeyri-mümkündür. Beləliklə də, qeyri mümlkün hadisənin ehtimalı sıfıra bərabərdir.
- Tutaq ki, k=n qəbul edilir. Onda tərifə əsasən p=1 olur. Belə ki, bütün sınaqlar əlverişli sınaqlardır, o hadisə yəqin ki, baş verəcək. Belə hadisələrə yəqin hadisələr deyilir. Beləliklə, yəqin hadisənin ehtimalı vahidə bərabərdir.
- Ümumi halda 0<=k<=n, yəni 0<=n<=1 qəbul edilsə, hadisənin baş vermə ehtimalı sıfırla bir arasında qiymət alır.

k hadisəsinin əlverişli sınaqlarının sayı, n-k isə əverişli olmayan sınaqların sayıdır. Hadisənin baş vermə ehtimalını q ilə işarə etsək onda tərifə əsasən

$$q = (n-k)/n$$

ifadəsini alarıq.

Belə ki, hadisənin baş verməməsinin qeyri-mümkünlüyü, hadisənin baş verməsinin mümkünlüyüdür.

Ehtimallı yanaşma üsulu dedikdə hər hansı bir hadisənin baş verə bilməsinin qiymətləndirilməsində ehtimal və ehtimal nəzəriyyəsində istifadə edilən üsullar nəzərdə tutulur. Bu cür yanaşma üsulunun əsas üstünlüyü risklərin müəyyən edilə, ölçüləbilən olmasıdır.

Ehtimal nəzəriyyəsində hadisələr baş vermə ehtimalına görə 2 yerə ayrılır:

- təsadüfi hadisə
- yəqin (mütləq hadisə)

Təcrübələr zamanı gah reallaşan, gah da reallaşmayan hadisə təsadüfi hadisə adlanır. Təkrarlanan nəticələrə əsasən analiz aparılır. Əgər hadisə təcrübələr zamanı hökmən baş verirsə bu mütləq və ya yəqin hadisə adlanır.

Elementar hadisə dedikdə sınağın ayrılmayan nəticələri nəzərdə tutulur. Elementar hadisələrdən ibarət çoxluq elementar hadisələr fəzası yaradır. Bu fəzanın hər

bir alt çoxluğu hadisə adlanır. X və Z hadisələrinin birləşməsi dedikdə bu hadisələrdən ən azı birinə daxil olan hadisə nəzərdə tutulur. X və Z hadisələrinin kəsişməsi dedikdə isə nəticələri hər iki hadisəyə daxili olan hadisələr nəzərdə tutulur. Uyuşmayan hadisələr dedikdə isə ortaq nəticələriə malik olmayan hadisələr nəzərdə tutulur. X hadisəsinin əks hadisəsi dedikdə X hadisəsinə daxil olmayan nəticələr çoxluğu nəzərdə tutulur.

Təqribi yanaşma üsulu vasitəsilə həll zamanı əldə edilmiş nəticələrin xətalarının qiymətləndirilməsi mütləqdir. Sınaqlar zamanı əldə edilmiş ədələrin yuvarlaqlaşdırarlən bəzən xətaların ölçüsü xeyli çox ola bilər. Bu formada hesablama mexanizmi dayanıqlı deyildir və istifadə edilməsi məsləhət görülmür.

Məlum üsullar arasından seçilən ədədi metodlardan istifadə edərkən və ya yeni üsul hazırlayarkən biz təbii olaraq məsələnin həlli üçün ayrılmış kompüterlərin xarakteristikalarını da nəzərə almalıyıq.

1.2.1 Entropiya

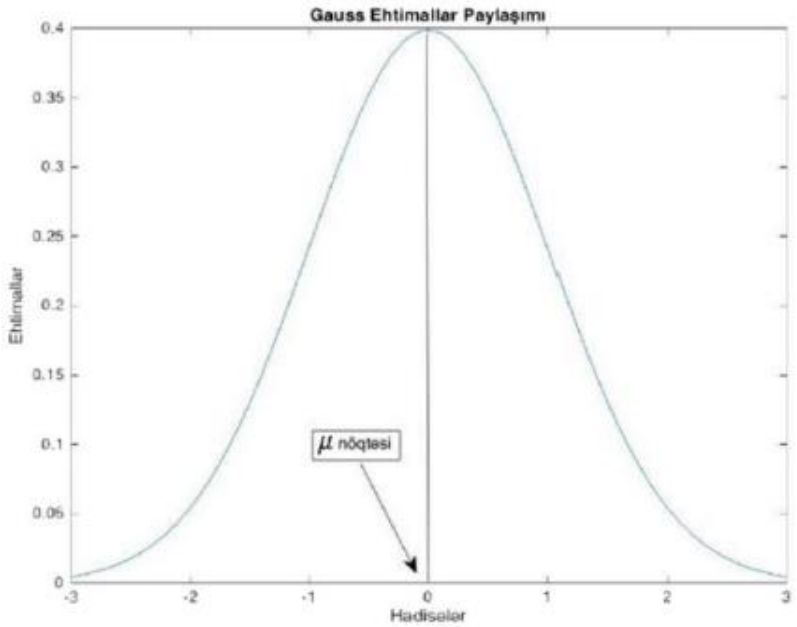
1948-ci ildə Klod Şennon entropiyanın informasiya nəzəriyyəsindəki rolu haqqında öz məqaləsində ətraflı şəkildə yazmışdır.

Nümunəyə əsasən entropiya anlayışını izah edək. Başlanğıc olaraq hər hansı hadisə ilə əlaqəli ehtimallar üzrə paylaşım təqdim edilib. Bunun vasitəsilə biz əvvəlcədən hadisənin reallaşma ehtimalları barədə fikir irəli sürə bilərik. Təbii ki, hadisə reallaşanadək biz mümkün hallardan hansının reallaşacağını dəqiq olaraq bilmirik, biz yalnız ehtimalları müqayisə edə bilərik. Ekspremineti hadisədən əvvəl və sonra olaraq iki hissəyə bölə bilərik. İnformatika elmində "sürpriz" ehtimal anlayışı vardır, bu ehtimalı az olan hadisənin baş verməsidir. Məsələn, iki D və E hadisələrinin baş vermə ehtimalları $p(D) = 0.2$ və $p(E) = 0.8$ – dir. Bu halda D hadisənin baş verməsi sürpriz ehtimal olacaq. Belə qənaətə gəlirik ki, sürpriz ilə ehtimal tərs mütənasibdir. İndi başqa bir nüansı nəzərdən keçirək. Fərz edək ki, D hadisəsinin baş verməsi ehtimalı birdir. $p(D) = 1$ olduğu halda artıq nəticə bizə məlum olmuş olur, D hadisəsi mütləq

reallaşacaq. Bu zaman sürpriz tənliyi elə qurulmalıdır ki, ehtimalı bir olan hadisə zamanı sürpriz ehtimal 0 olsun. Digər bir halda isə D hadisəsinin olma ehtimalı 0-a bərabər olsun. Bu zaman mümkün sürprizin necə təyin ediləcəyi sualı yaranır. Bu zaman sürprizi proqnozlaşdırmaq daha da çətinləşir. Burada elə tənlik qurmaq lazımdır ki, ehtimal sıfıra bərabər olduqda düstur təyin olunmasın. Bütün bunları nəzərə alarkən bir şərti də nəzərə almaq lazımdır ki, sürpriz sıfır və ya müsbət qiymətlər ala bilər. Bu istəklərə cavab verən funksiyanı Şanon məqaləsində bu cür təyin etmişdi:

$$T(i) = \log 1/(p(i)) = -\log p(i)$$

T(i) ilə i hadisəsinin yarada biləcəyi sürpriz işarə edilib. İxtiyari vəziyyətdə mümkün hadisələrin ortalama sürprizi entropiyaya bərabərdir. Sınaqdan qabaq hadisələrdən hansı birinin reallaşacağı haqda dəqiq fikir bildirmək mümkün deyil. Həyata keçirilən sınaqların sayı nə qədər çox olarsa, ehtimalların dəqiqliyi də bir o qədər yüksək olar. Sınaq nəticələrinin bir birlərinə oxşarlıq dərəcəsi çox olduqca hadisələri analiz etmək daha rahat olur. Lakin, ola biləcək orta sürprizi hesablamaq mümkündür ki, bu entropiya adlanır. Entropiya anlayışını izah etmək üçün aşağıdakı qrafiki nəzərdən keçirək.



Şəkil 1.2.1.1 Qaus ehtimallar paylaşımı qrafiki

Mümkün reallaşa biləcək hadisələri X, Y onların isə onların reallaşmasını ifadə edir. μ nöqtəsi entropiya nöqtəsi adlanır.

Müxtəlif xəbərlərdən ibarət xəbərin entropiyasının təşkiledici xəbərlərin entropiyaları cəminə bərabər olması entropiyanın əsas xassələrindən biridir. Bunu aşağıdakı düsturla ifadə etmək mümündür:

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

Müstəqil hadisələrdən təşkil edilmiş mürəkkəb (AB) hadisəsininin yekun ehtimalı onu təşkil edən hadisələrin ehtimalları hasili ilə müəyyən edilir:

$$p(A,B) = p(A)*p(B)$$

Tutaq ki, bir birləri ilə əlaqəsi olan A və B xəbərlərində ibarət AB xəbəri vardır. p(ai) ilə A xəbərinin i əlamətinə malik işarəsinin əldə edilməsi ehtimalını, p(bj) ilə isə B xəbərinin j əlamətinə malik işarəsinin əldə edilməsi ehtimalını işarə edək. Bu zaman A xəbərinin i əlamətinə malik işarəsinin B xəbərinin j əlamətinə malik işarəsinə nəzərən şərti ehtimalı aşağıdakı kimi hesablanır:

$$p(ai / bj)$$

Şərti entropiyanın əsas xassələri aşağıdakılardır:

- əgər A və B xəbərləri qarşılıqlı olaraq asılı deyillərsə, onda A xəbərinin B xəbərinə nəzərən şərti entropiyası A xəbərinin şərtsiz entropiyasına bərabərdir. Yəni:

$$H(A / B) = H(A).$$

- A və B xəbərlərinin şərti entropiyaları o zaman bərabər olur ki, onlar funksional olaraq asılı olsunlar:

$$H(A / B) = H(B / A) = 0.$$

Çünki funksional əlaqədə şərti ehtimal vahidə bərabərdir.

Şərti entropiya. Əgər sadəcə olaraq əlifbanın hərflərini deyil, müəyyən məzmunlu xəbəri ötürmək lazım olarsa, onda simvollar arasında müəyyən bağlılıqların yaranması ehtimalı yüksəkdir. Belə olduqda entropiya şərti ehtimallar əsasında

müəyyən etmək edilməlidir. Misal üçün, bir-biri ilə əlaqəsi olan A və B xəbərlərindən ibarət AB xəbərinin qəbul edildiyini fərz edək. A xəbərinin i əlamətli işarəsinin alınması ehtimalını p(ai) ilə, B xəbərinin j əlamətli işarəsinin alınması ehtimalını p(bj) ilə, A xəbərinin i əlamətli işarəsinin B xəbərinin j əlamətli işarəsinə nəzərən şərti ehtimalını p(ai / bj) ilə və B xəbərinin j əlamətli işarəsinin A xəbərinin i əlamətli işarəsinə nəzərən şərti ehtimalını p(bj / ai) ilə ifadə edək. Qarşılıqlı asılı iki hadisənin birlikdə reallaşması ehtimalı həmin hadisələrin istənilən birinin ehtimalı ilə digərinin şərti ehtimalı hasili ilə müəyyən edilir:

$$p(a_i, b_j) = p(a_i) \cdot p(b_j / a_i) = p(b_j) \cdot p(a_i / b_j)$$

Bu halda AB xəbərinin entropiyası:

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

kimi hesablanacaqdır (20, s. 54-55).

Aşağıda şərti entropiyanın xassələri verilib:

- əgər A və B xəbərləri qarşılıqlı asılı deyillərsə, onda A-nın B-yə nəzərən şərti entropiyası A-nın şərtsiz entropiyasına bərabərdir. Yəni: H(A / B) = H(A). Analoji olaraq: H(B / A) = H(B) yazmaq olar.
- A və B xəbərlərinin şərti entropiyaları o zaman sıfıra bərabər olur ki, onlar funksional olaraq asılı olsunlar:

$$H(A/B) = H(B/A) = 0$$

Çünki funksional əlaqədə şərti ehtimal vahidə bərabərdir.

Məlumat nəzəriyyəsi, səs-küylü bir kanal boyunca məlumatların ötürülməsi ilə əlaqəli bir riyaziyyat sahəsidir.

Məlumat nəzəriyyəsinin təməl daşı bir mesajda nə qədər məlumatın olması barədə fikirdir. Ümumiyyətlə, bu bir hadisədə və təsadüfi bir dəyişəndə, entropiya adlanan məlumatların miqdarını qiymətləndirmək üçün istifadə edilə bilər və ehtimaldan istifadə edilərək hesablanır.

Entropiya və hesablama məlumatları maşın öyrənməsində faydalı üsuldur. Məlumatın miqdarı məlumat nəzəriyyəsi sahəsinin əsasını təşkil edir.

Kəmiyyət məlumatının arxasındakı intuisiya, bir hadisədə nə qədər sürprizin olduğunu ölçmək fikridir. Nadir olan hadisələr (aşağı ehtimal) daha təəccüblüdür və buna görə ümumi olan hadisələr (yüksək ehtimal) haqqında daha çox məlumat vardır.

- Aşağı ehtimal hadisəsi : Yüksək məlumat (təəccüblü)
- Yüksək ehtimal hadisəsi : Aşağı məlumat (təəccüblü deyil)

Təsadüfi bir dəyişəndə nə qədər məlumatın olduğunu da müəyyən edə bilərik. Məsələn, ehtimal bölgüsü p ilə təsadüfi bir X dəyişəni üçün məlumatı hesablamaq istəsək bu H funksiyası olaraq yazıla bilər . misal üçün: H (X)
Əslində, təsadüfi bir dəyişən üçün məlumatın hesablanması hadisələrin təsadüfi dəyişən üçün ehtimal bölgüsü üçün məlumatın hesablanması ilə eynidir. (25, s. 126 - 127).
Təsadüfi bir dəyişən üçün məlumatın hesablanmasına "məlumat entropiyası", "Şannon entropiyası" və ya sadəcə "entropiya " deyilir. Fizikadan entropiya ideyası bənzətmə ilə əlaqədardır, çünki hər ikisi də qeyri-müəyyənliklə əlaqəlidir.
Entropiya üçün intuisiya, təsadüfi dəyişən üçün ehtimal paylanmasından çəkilmiş bir hadisəni təmsil etmək və ya ötürmək üçün tələb olunan orta saydır.

1.2.2 Şifrələnən və deşifrlənən kodlar

Şifrələmə düz mətn məlumatlarının (düz mətnin) təsadüfi və mənasız (şifrə) görünən bir mətnə çevrilməsi prosesidir. Şifrəni açmaq şifrə mətnini yenidən düz mətnə çevirmək prosesidir.

Sözün kodlaşdırılması, məlumatların mahiyyətinin kod şəklində bir sistemdən digər sistemə çevirmək deməkdir. Kod gizli mənanı ifadə etmək üçün istifadə olunan simvol, işarə və ya məktublar sistemidir. Con Fiskenin sözlərinə görə, kodlaşdırma "bu işarələrin necə və hansı kontekstdə istifadə edildiyini və daha mürəkkəb mesajlar yaratmaq üçün necə birləşdirildiyini müəyyən edən əlamətlərdən və qaydalardan ibarətdir".

Deşifrələmə o deməkdir ki, mənbənin kodladığı mesajı dekoder öz mahiyyətını geri qaytarır və informasiya anlaşılan vəziyyətə gətirilir. Sonra kodlanmış mesaj alıcı tərəfindən asanlıqla başa düşüləcəkdir. Beləliklə, qəbuledici mesajını yenidən asanlıqla və sürətli şəkildə açacaq.

Kodlaşdırma bir mesajın yaradılması deməkdir. Digər tərəfdən deşifrə kodlaşdırılan mesajın əvvəli vəziyyətinə qaytarılması deməkdir. Yəni şifrəni açmaq mesajın mənasını şərh etmək deməkdir.

Bütün rabitə göndərəndən başlayır. Göndərənin həyata keçirdiyi ilk addım kodlaşdırma prosesidir. Məlumatı çatdırmaq üçün göndərən ilk öncə kodlaşdırmanı etməlidir, yəni məlumatı fikir və ya konsepsiyaları təmsil edən simvollar şəklində bir mesaja çevirmək deməkdir. Bunun üçün xüsusi alqoritmlər əsasında proqramlaşdırılmış proqram təminatlarından istifadə edilir.

Göndərən mesajı müvafiq kanal vasitəsilə (danışma halında, üz-üzə qarşılıqlı əlaqədə) ötürmək üçün mesajı deşifrə edən bir qəbulediciyə kodlayır. Mənbə bir məlumatı digərlərinə çatdırmaq niyyətində olan şəxsə və ya qrupa aiddir.

Rabitə mənbəyi nəzərdə tutulan mesajı bir yerə yığdıqda, bu "şifrələmə" adlanır. Bu sözlər, işarələr, şəkillər, simvollar və səslərdən istifadə etməklə yaradılır.

Kodlanmış mesaj artıq bir mesaj kanalı vasitəsilə digərlərinə çatdırılmalıdır. Mesaj kanalı, mesajı göndərəndən alıcıya çatdıran mühiti ifadə edir.

Bu model model altı elementə qədər genişləndirilə bilər:

- mənbə
- kodlayıcı
- mesaj
- kanal

- dekoder
- qəbuledici

Şəkil 1.2.2.1 Məlumatın kommunikasiya kanalı ilə göndərilməsi mərhələləri

Kiçik miqdarda məlumatları şifrələmək üçün simmetrik şifrələmə istifadə olunur. Simmetrik bir açar həm şifrləmə, həm də deşifrələmə prosesində istifadə olunur. Müəyyən bir şifrələnmiş mətnin deşifrlənə bilməsi üçün məlumatların şifrələnməsi üçün istifadə olunan açar istifadə edilməlidir.

Hər şifrələmə alqoritminin məqsədi açarı istifadə etmədən yaradılan şifrə mətnini deşifr etməyi mümkün qədər çətinləşdirməkdir. Həqiqətən yaxşı bir şifrələmə alqoritmi istifadə olunarsa, hər mümkün açarı metodik olaraq sınamaqdan daha yaxşı bir texnika yoxdur. Belə bir alqoritm üçün açar nə qədər uzun olsa, şifrə mətninin bir hissəsini açara sahib olmadan deşifrə etmək daha çətindir.

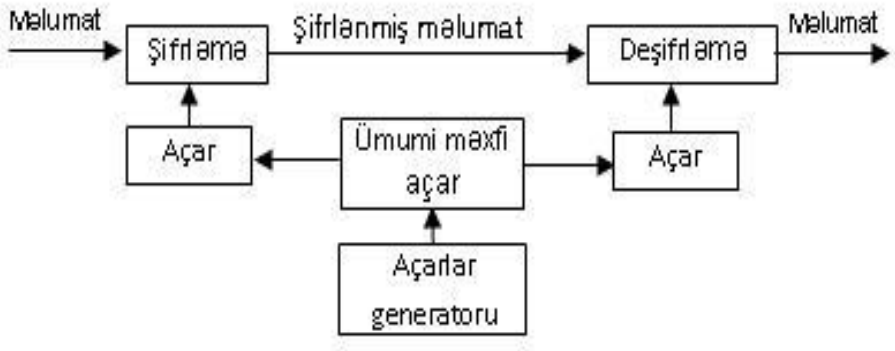
Şifrələmə alqoritminin keyfiyyətini müəyyən etmək çətindir. Ümidverici görünən alqoritmlər, lazımi hücumu nəzərə alaraq bəzən pozulmaq üçün çox asan olur.

Şifrələmə üsul və metodları istifadə edilən açarın tipinə əsasən simmetrik və asimmetrik olaraq 2 yerə ayrılır.

Şifrələmə və deşifrələmə prosesləri üçün yalnız bir gizli açarı istifadə edən ən sadə şifrələmə üsulu simmetrik şifrələmə üsuludur. Burada verilmiş məlumatı şifrələmək və şifrələnmiş məlumatı açmaq üçün eyni açar istifadə edilir. Göndərən və alıcı bütün mesajları şifrələmək və deşifr etmək üçün istifadə olunan gizli açarı

bilməlidir. Blowfish, AES, RC4, DES, RC5 və RC6 simmetrik şifrələmə nümunəsidir. Ən çox istifadə olunan simmetrik alqoritm AES-128, AES-192 və AES-256-dır.

Simmetrik açar şifrələməsinin əsas çatışmazlığı, tərəflərin hamısının məlumatları şifrələmədən əvvəl şifrələməsi üçün istifadə olunan açarı mübadiləsi etməsidir.



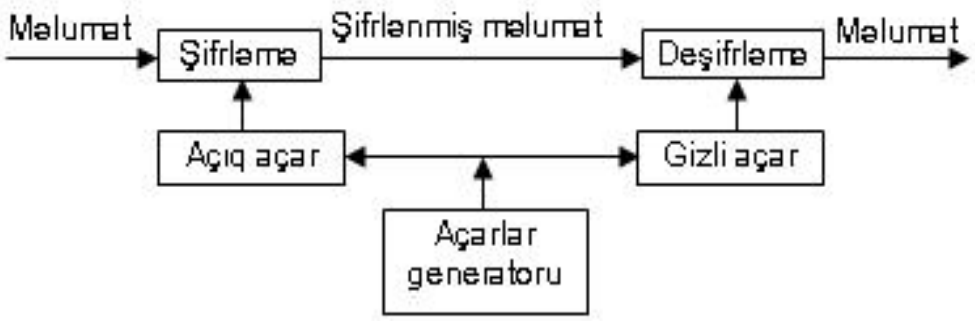
1.2.2.2 Simmetrik şifrələmənin iş prinsipi

Asimmetrik şifrələmədə mətni şifrələmək və şifrələnmiş mətni açmaq üçün 2 fərqli açardan istifadə edilir. Gizli açarlar İnternet və ya geniş bir şəbəkə vasitəsilə mübadilə olunur. Zərərli şəxslərin açarlardan sui-istifadə etməməsini təmin edir. Nəzərə almaq lazımdır ki, gizli açara sahib olan hamı məlumatı açа bilər, məhz bu səbəbdən də təhlükəsizliyin təmin edilməsi üçün iki əlaqəli açardan istifadə edilir.

Məlumat şifrələmək istəyən hər kəs üçün açıq açar əlçatan olduğu halda, gizli açar yalnız məlumatı şifrələyən və qəbul edən şəxsdə olur.

Açıq açarın köməyi ilə şifrələnmiş bir mesaj yalnız xüsusi açarın köməyi ilə deşifrlənə bilər, eyni zamanda xüsusi açardan istifadə edərək şifrələnmiş bir mesaj açıq açarın köməyi ilə deşifrlənə bilər. Açıq açarın təhlükəsizliyi tələb olunmur, çünki açıqdır və internet üzərindən ötürülə bilər. Asimmetrik açar, rabitə zamanı ötürülən məlumatların təhlükəsizliyini təmin etmək üçün daha yaxşı bir gücə malikdir.

Simmetrik və ya asimmterik üsulun seçilməsindən asılı olmayaraq şifrələmə üçün istifadə ediləcək alqoritmin güclü olması mütləq nəzərə alınmalıdır.



1.2.2.3 Asimmetrik şifrələmənin iş prinsipi

Asimmetrik şifrələmədən istifadə etmək üçün açıq açarları aşkar etmək yolu olmalıdır. Bir tipik bir texnikadır, müştəri-server ünsiyyət modelində rəqəmsal sertifikatlardan istifadə olunur. Sertifikat istifadəçi və serveri müəyyənləşdirən məlumat paketidir. Bu, bir təşkilatın adı, sertifikatı verən təşkilat, istifadəçilərin e-poçt ünvanı və ölkə və istifadəçilərin açıq açarı kimi məlumatları ehtiva edir.

Bir server və müştəri etibarlı şifrəli bir əlaqə tələb etdikdə, şəbəkə üzərindən sorğu göndərərək qarşı tərəfə sertifikat surətini göndərir. Qarşı tərəfin açıq açarı sertifikatdan çıxarıla bilər. Sahibini eyniləşdirmək üçün bir sertifikat da istifadə edilə bilər.

AES alqoritmi. Qabaqcıl şifrələmə standartı olub sabit məlumat bloklarını (128 bit) şifrələyən simmetrik şifrələmə alqoritmidir. Mətni deşifrə etmək üçün müxtəlif uzunluqlu açarlardan istifadə edilir. 256 bitlik açar vasitəsilə məlumatları 14, 192 bitlik açar ilə 12 və 128 bitlik açar isə 10 addımda şifrələmək olar. AES şifrələmə standartları bu gün ən çox istifadə olunan şifrələmə üsullarından biridir.

RSA alqoritmi. Rivest-Shamir-Adleman , iki baş ədədin kombinasiyasına əsaslanan asimmetrik şifrələmə alqoritmidir. Şifrələmə açarı təyin edilmiş iki ədəd üzərində ixtiyari əməliyyatları etməklə alınır. Yalnız bu ədədləri bilən biri mesajı uğurla deşifrə edə bilər. RSA alqoritmi rəqəmsal imzalarda geniş istifadə olunur, lakin böyük həcmdə məlumatların şifrələnməsi lazım olduqda daha az işlədilir.

Üçqat şifrələmə standartı. Bu simmetrik şifrələmə alqoritmidir və 56 bitlik açar istifadə edərək məlumat bloklarını şifrələyən DES metodunun inkişaf etmiş

formasıdır. Bu alqoritm vasitəsilə hər məlumat blokuna üç dəfə DES şifrə alqoritmi tətbiq edilir. Üçqat Şifrləmə Standartı adətən ATM PIN-lərini və UNIX şifrələrini şifrələmək üçün istifadə olunur .

Aşağıdakı hallarda məlumatların şifrələnərək saxlanılması və icra zamanı deşifrə edilməsi geniş tətbiq edilir.

- onlayn ödənişlər : PCI-DSS standartları kart məlumatlarının AES alqoritmi ilə şifrələnməsini tələb edir
- buluddakı məlumatlar : bulud texonologiyası imkan verir ki, istifadəçilər öz məlumatların bulud serverlərində saxlaya bilsinlər. Bu zaman istifadəçi məlumatları həmmin serverlərdə şifrələnmiş halda saxlanılır və məlumatın oxunması əmri verildikdə məlumatlar müvafiq alqoritmə deşifrlə edilir və istifadəçilərə onların başa düşəcəyi formada təqdim edilir.
- e-poçtlar : E-poçt şifrələməsi e-poçt kanalları vasitəsilə göndərilən həssas məlumatları qorumağa kömək edir. Rəqəmsal sertifikatlarla yanaşı açıq açar şifrələmə üsulları da e-poçt əlaqələrinin təmin edilməsi üçün istifadə olunan metodlardır.

Şifrələmə alqoritmlərini proqramlaşdırma dilində kodlar vasitəsilə tətbiq etmək mümkündür. Şəkil 1.2.2.3-dəki kod nümunəsində C# proqramlaşdırma dili vasitəsilə verilmiş mətnin açara əsasən şifrələnməsi funksiyası yazılıb.

```
public static string EncryptString(string key, string plainText)
{
    byte[] iv = new byte[16];
    byte[] array;

    using (Aes aes = Aes.Create())
    {
        aes.Key = Encoding.UTF8.GetBytes(key);
        aes.IV = iv;

        ICryptoTransform encryptor = aes.CreateEncryptor(aes.Key, aes.IV);

        using (MemoryStream memoryStream = new MemoryStream())
        {
            using (CryptoStream cryptoStream = new CryptoStream((Stream)memory
            {
                using (StreamWriter streamWriter = new StreamWriter((Stream)cr
                {
                    streamWriter.Write(plainText);
                }

                array = memoryStream.ToArray();
            }
        }
    }

    return Convert.ToBase64String(array);
}
```

Şəkil 1.2.2.4 Verilmiş mətnin açar vasitəsilə şifrələnməsi

Şifrələmə prosesi AES alqoritminin tətbiq edildiyi kitabxananın köməkliyi ilə həyata keçirilib.

Verilmiş açara əsasən şifrələnmiş məlumatı deşifrə etmək mümkündür. Şəkil 1.2.2.3-dəki kod nümunəsində şifrələnmiş məlumat deşifrə edilir.

```
public static string DecryptString(string key, string cipherText)
{
    byte[] iv = new byte[16];
    byte[] buffer = Convert.FromBase64String(cipherText);

    using (Aes aes = Aes.Create())
    {
        aes.Key = Encoding.UTF8.GetBytes(key);
        aes.IV = iv;
        ICryptoTransform decryptor = aes.CreateDecryptor(aes.Key, aes.IV);

        using (MemoryStream memoryStream = new MemoryStream(buffer))
        {
            using (CryptoStream cryptoStream = new CryptoStream((Stream)memory
            {
                using (StreamReader streamReader = new StreamReader((Stream)cr
                {
                    return streamReader.ReadToEnd();
                }
            }
        }
    }
}
```

Şəkil 1.2.2.5 Verilmiş mətnin açar vasitəsilə deşifrələnməsi

1.2.3 Optimal kod uzunluğu

Kompüter elmində və məlumat nəzəriyyəsində, Huffman kodu, məlumatların itkisiz sıxılması üçün istifadə olunan xüsusi bir prefiks kodunun müəyyən bir növüdür. Belə bir kodun tapılması və ya istifadəsi prosesi H.D. Huffman tərəfindən, o hələ MİT tələbəsi olan zaman hazırlanıb və "Huffman kodlaşdırması" başlığı altında davam edib. Bu haqda ilk məqalə 1952-ci il tarixli "Kodların minimal sıxlaşdırılması" adlı qəzetdə dərc edilmişdir.

Optimal kod – verilən mənbə üçün orta uzunluğu eyni funksiyalı digər təkrarolunmayan kodlar arasında ən kiçik olan koddur. Optimal kod həmişə mövcuddur

və bəzən ola bilir ki, bir mənbə üçün bir neçə optimal kod olur. Bu vəziyyətdə onların strukturu fərqli ola bilir, amma uzunluqları eyni qalır.

Belə bir sual ortaya çıxır ki, verilmiş simvol ehtimalları üçün optimal kod uzunluğu necə müəyyən edilir? Biz hər hansı bir variantı optimal qəbul edib onu praktikada istifadə edə bilərikmi?

Huffman kodlaşdırma proseduru optimal kod yaradır. İstənilən kodun uzunluğu əlifbanın ölçüsü və fərdi hərflərin ehtimalları da daxil olmaqla bir çox şeydən asılı olacaq. S mənbəsi üçün optimal kodun və S mənbə üçün Huffman kodunun orta kod uzunluğunun L ilə işarə edək. Bu zaman aşağıdakıları deyə bilərik:

- S mənbəsi üçün L optimal kod uzunluğu həmin mənbənin Huffman koduna bərabər və ya ondan kiçik olmalıdır
- S mənbəsi üçün L optimal kod uzunluğu həmin mənbənin Huffman kodundan 1 vahid və ondan daha çox ola bilməz

$$H(\mathcal{S}) \leqslant \bar{l} < H(\mathcal{S}) + 1$$

Aşağıdakı şərtlər ödəndiyi halda kod optimal hesab olunur: a) kod simvolunda bolluq ala biləcəyi ən aşağı qiyməti almalıdır b) təşkil edən simvollar müstəqil və bərabər ehtimallı olmalıdırlar. Komplekt kod o koda deyilir ki, xəbərlərin optimal kodunun ehtimalları bərabər olsun. Ehtimal üçün

pi = 2^-i

sıra şərtinin ödəndiyi halda, optimal kod belə olur:

$A_1 \Rightarrow p_1 = 1/2 \Rightarrow 0$
$A_2 \Rightarrow p_2 = 1/4 \Rightarrow 10$
$A_3 \Rightarrow p_3 = 1/8 \Rightarrow 110$
$A_4 \Rightarrow p_4 = 1/16 \Rightarrow 1110$
$A_5 \Rightarrow p_5 = 1/32 \Rightarrow 11110$
$A_6 \Rightarrow p_6 = 1/64 \Rightarrow 111110$

Göründüyü kimi, ehtimallar azaldıqca, kod sözü uzanır.

Müxtəlif ölçülü optimal kodlar. İlk olaraq sadə hala baxaq. Fərz edək ki, məlumatların ehtimalları aşağıdakı bərabərliklə müəyyən olunur:

$$P(x_i)=D^{-m_i}, \quad i=1,2,\ldots,M$$

$$m(X)=\frac{H(X)}{\log D}$$

düsturu ilə deşifrələmə kodlarının yaranması üçün tələb olunan kod sözlərinin orta uzunluğu hesablanır. X(i) xəbəri üçün kod uzunluğu

–logp (xi)/logD

düsturu ilə hesablanır (20, s. 72-73).

Şərh. Telekommunikasiya sistemində informasiya siqnallar şəklində ötürülür. Siqnalların 2 növü vardır:

- analoq
- rəqəmsal

Ehtimal anlayışı baş verə biləcək hadisənin reallığa olan münasibət dərəcəsi ilə izah olunur. Ehtimal dedikdə ixtiyari hadisənin həyata keçməsinin mümkünlüyünün ədədi xarakteristikası nəzərdə tutulur.

İxtiyari hadisənin baş verə bilməsinin qiymətləndirilməsində ehtimal nəzəriyyəsindən istifadə edilən üsul ehtimallı yanaşma üsul adlanır. Ehtimallı yanaşma üsulunun əsas üstünlüyü risklərin müəyyən edilə, ölçüləbilən olmasıdır.

1948-ci ildə Klod Şennon entropiyanın informasiya nəzəriyyəsindəki rolu haqqında öz məqaləsində ətraflı şəkildə yazmışdır.

Şifrələmə dedikdə anlaşılabilən məlumatların alqoritm vasitəsilə anlaşılmayan, təsadüfi simvollar yığını kimi görünən vəziyyətə gətirilməsi nəzərdə tutulur. Şifrələmə və deşifrələmə prosesində istifadə olunan açarlara görə şifrələmənin simmetrik və asimmterik olaraq 2 növü vardır. Şifrələnmiş mətni açarın və ya alqoritmin köməyi ilə deşifrə etmək mümkün olursa, belə kodlar deşifrlənən kodlar adlanır.

II Fəsil. Kodların yaradılması üsulları

2.1 Prefiks kodlaşdırma

Bir neçə rəqəmi istifadə edərək bir mesaj kodlamaq üçün, ən az rəqəmlərdən istifadə edərək mesajı necə kodlamaq mümkündür? 1952-ci ildə David Huffman, bu suala cavabı "Minimum-Redundancy kodlarının qurulması üçün bir metod" adlı məqalədə yazdı və bir metod təklif etdi. Bu üsul, HTTP-nin standart sıxılma metodlarından biri olan png, jpeg, mp3, deflate data formatı kimi fayl formatları və gzip və zlib kitabxanalarında istifadə olunan deflate formatı kimi insanlar üçün çox təsir edici olacaqdır.

Prefiks kodlaşdırmada hər bir simvol bir və ya daha çox rəqəmdən ibarət kodlar şəklində verilir. Bu kodları təyin edərkən hər hansı bir kod özündən daha uzun başqa bir kodun başlanğıcı olmamalıdır. Beləliklə, bu kodlar bir-birinin ardınca verildikdə mükəmməl bir şəkildə təhlil edilə bilər. Yuxarıdakı cədvəldə ən qısa kod a simvoluna verilir. A işarəsinə verilmiş kod 1 olduğundan, digər kodların heç biri 1 ilə başlaya bilməz. Eyni şəkildə, digər kodların heç biri 01 ilə başlaya bilməz, çünki c kodu 01-ə təyin edilmişdir. Bu xüsusiyyətlərə sahib kodlar yaratmaq üçün yuxarıdakı kimi bir ağac yarada, ağacın yarpaqlarına kodlanacaq simvollar qoyaraq hər istiqamətə 0 və bir-birinə 1 ədəd qoyun. İstədiyiniz işarəyə yuxarıdan keçdiyiniz nömrələr həmin xarakterin kodunu verir.

Huffman kodlaşdırmasının məqsədi ən çox istifadə olunan simvollara (və ya sıxdığımız məlumatda ən çox istifadə olunan baytlara) ən qısa kodu vermək üçün prefiks ağacını yaratmaqdır. Bunun üçün istifadə ediləcək alqoritm aşağıdakı kimidir.

- simvolları mətndə istifadə olunma sayına görə sıralamaq
- ən kiçik iki simvolu qruplaşdırmaq və tezliyini toplayaraq növbəyə əlavə etmək
- yalnız bir qrup qalana qədər qruplaşmaya davam etmək

Bu alqoritmi həyata keçirmək üçün BST və dinamik bir sıra məlumat quruluşundan istifadə ediləcək. Dinamik serialın əvəzinə Heap daha yaxşı bir seçim ola bilər.

Alqoritmə keçməzdən əvvəl məlumat strukturlarına nəzər salaq.

```
typedef quruluşu _huffman
{
    char c;
    int freq;
    struktur _huffman * sol;
    struktur _huffman * sağ;
} HUFFMANTREE;
typedef strukturu _huffman_array {
    int qapaq;
    int ölçüsü;
    HUFFMANTREE ** maddələr;
} HUFFMANARRAY;
```

Qruplaşdırma aparmaq üçün HUFFMANTREE məlumat quruluşundan və qruplaşmaları çeşidləmək üçün HUFFMANARRAY məlumat quruluşundan istifadə edilir. Çeşidləmə alqoritmi olaraq klassik seçim sıralama metoduna üstünlük verilir.

Başlanğıc kodu kod sisteminin bir növüdür (adətən dəyişən bir uzunluq kodu, kod kod sözündən fərqləndirən "prefiks xassəsi" tələb edən), sistemdəki hər hansı bir prefiks (birinci hissə) sistemdəki hər hansı digər kod sözüdür. Məsələn, {9, 55} kod sözü kod prefiks xüsusiyyətinə malikdir; "5", "55" ilə "59" arasındakı bir prefiksdir, çünki {9, 5, 59, 55} qurulan bir kod deyildir. Tam və dəqiq bir kod dəsti verilir: alıcı sözlər arasında xüsusi bir işarə tələb etmədən hər bir sözü eyniləşdirə bilər.

Huffman kodlaşdırmada kodları yalnız bir prefiksdən əldə etmək üçün bir çox alqoritm mövcud olsa da, ümumi kod Huffman alqoritmi tərəfindən istehsal edilməməsinə baxmayaraq prefiks kodlarına "Huffman kodları" da deyilir. Vergisız kod termini bəzən prefikssiz kodlarla sinonimdir, lakin əksər riyazi kitablar və məqalələr (məsələn), öz-özünə sinxronlaşdırılan kod, prefiks kodların vergül olmadan kod mənasını verməsi üçün istifadə olunur.

Prefiks kodları, sözlər arasındakı xüsusi markerlər üçün çərçivə mesajındakı hər hansı bir sözdən istifadə edərək mesaj olmadan birləşdirilmiş kodda sözlərin ardıcıllığı şəklində ötürülə bilər. Davamlı kod sözlərini tapmaq və yaratmaq üçün alıcı simləri ayırmaqla mesajı dəqiq bir şəkildə deşifrə edə bilir.

Dəyişən uzunluğa malik Huffman kodları, ölkə zəng kodları, UMTS W-CDMA 3G Simsiz Standartında istifadə olunan ikincil Sinxronizasiya Kodları və əmr dəstləri əksər kompüter mikroarxitekturaları (maşın dili) arasındakı prefiks kodlardır.

Prefiks kodları səhv düzəltmə kodları deyil. Təcrübədə, bir mesaj əvvəlcə bir prefiks kodu ilə sıxıla bilər.

Eyni kod sözünün uzunluğuna sahib olan bir zəng kodu var ki, bunlar hər biri üçün misilsiz kodlaşdırıla bilər. Kraft bərabərsizliyi, unikal kodla həll edilə bilən söz uzunluğu dəstlərini xarakterizə edən mümkün bir koddur.

Kodun hər sözü eyni uzunluğa malikdirsə, kodu sabit uzunluqlu bir kod və ya bir blok kodu adlandırırlar. Məsələn, ISO 8859-15 məktubları həmişə 8 bit uzunluqdadır. UTF-32/UCS-4 hərfləri həmişə 32 bit uzunluqdadır. ATM hüceyrələri həmişə 424 bit (53 bayt) uzunluqdadır. Sabit uzunluqlu mənbə bit simvollarını kodlayan sabit uzunluqlu bir koddur.

Sabit uzunluq kod prefiks kodudur. Uzun prefikslərin uzunluğunu qarşılamaq üçün sabit simvolları qısa prefikslərə doldurmaqla istənilən kodu sabit uzunluq koduna çevirmək mümkündür. Alternativ olaraq, bu cür doldurma kodları, özünü düzəltməyə və və ya sinxronizasiya etməyə imkan verən çoxluq yaratmaq üçün istifadə edilə bilər.

Ancaq bəzi sözlərin digərlərinə nisbətən daha çox ötürüldüyü hallarda sabit uzunluqlu şifrələr kifayət deyil.

Kəsilmiş ikili kodlama simvollarının sayı ilə əlaqəli sabit uzunluqlu kodların sadə ümumiləşdirilməsi hər ikisinin gücü deyil. Mənbə simvolu uzunluğu k və k + 1, k kod sözlərinə təyin olunur ki, $2^k < n \leq 2^{k+1}$ seçilsin.

Huffman kodlaşdırma dəyişkən uzunluqlu prefiks kodları yaratmaq üçün daha mürəkkəb bir texnikadır. Huffman kodlaşdırma alqoritmi giriş kimi kod sözləri olmalı olan tezlikləri yaradır və kod sözlərinin uzunluğunun orta çəkisini minimuma endirən bir prefiks kodu yaradır. (Bu, entropiyanın minimuma endirilməsi ilə əlaqədardır). Bu, entropiyanın kodlaşdırılması ilə müqayisədə zərərsiz məlumatların sıxılmasının bir formasıdır.

Bəzi kodlar bir kod sözünün sonunu normal məlumatlardan fərqli olan xüsusi "vergül" simvolu ilə qeyd edir. Bu, bir cümlədəki sözlər arasındakı boşluqlarla bir qədər oxşardır; bir sözün bitdiyini, digərinin başladığını qeyd edirlər. Hər bir kod sözü vergüllə bitərsə və başqa bir kod sözü vergüllə görünmürsə, kod avtomatik əvvəlcədən verilir. Bununla birlikdə, müasir rabitə sistemləri hər şeyi "1" və "0" ardıcıllıqla göndərir - bahalı olacaq üçüncü bir işarə əlavə edib sözlərin sonuna qədər istifadə etmək səmərəsiz olardı. Morse kodu, vergül ilə dəyişən uzunluqlu bir qeyd jurnalına misaldır. Uzun hərflər arasındakı fasilələr və daha da uzun sözlər arasında fasilə, insanlara bir hərfin (və ya sözün) harada bitdiyini və sonrakı başlanğıcın tanımasına kömək edir. Eynilə, Fibonacci kodlaşdırması hər kod sözünün sonunu qeyd etmək üçün "11" istifadə edir.

Öz-özünə sinxronlaşdırılan kodlar çərçivə sinxronizasiyasına imkan verən prefiks kodlardır.

2.2 Şennon alqoritmi

Klod Şennona görə, məlumatlar arasında informasiya miqdarının ölçüsü, yəni informasiyanın miqdarı məlumatların ehtimal xarakteristikalarına əsasən təyin edilir və

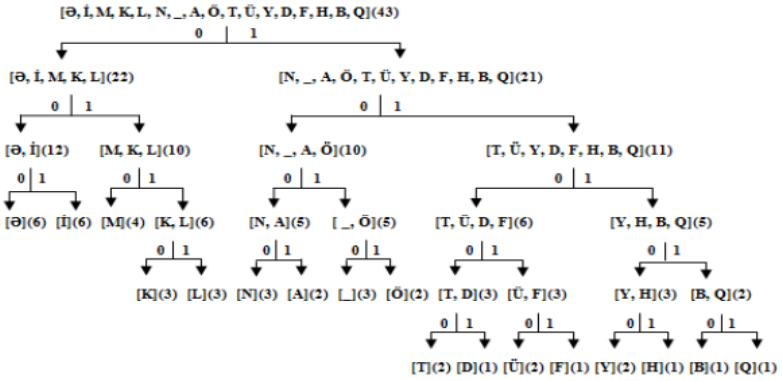
başqa xarakteristikalardan asılı deyil. Şennon nəzəriyyəsinin əsas mövzusu informasiyanın fərqli metodlarla emalı, yığcamlaşdırılması və ötürülməsi prinsipləridir.

İnformasiyanın yığcamlaşdırılması qaydası onun qənaətlə kodlaşdırılması adlanır. Bu problemin üzərində ilk dəfə 1837-ci ildə Samuel Morze işləyərək yeni alqoritm təklif etmişdir. Keçən əsrin 40-cı illərində informasiya nəzəriyyəsinin yaranması ilə informasiyanın qənaətlə kodlaşdırılması texnologiyası inkişaf etdi. İnformasiyanın yığcamlaşdırılmasının ən məşhur üsulu təkrarlanan simvolların kiçik uzunluqlu unikal simvallarla əvəz edilməsi ilə həyata keçirilir. İnformasiyanın yığcamılaşdırılması zamanı onun həcmi bir neçə dəfəyə qədər kiçilə bilər.

R.Fano və K.Şennon bir birlərindən xəbərsiz şəkildə bu metod üzərində işləyiblər. Əlifbadakı bütün simvollar çəkilərinə görə artma və ya azalma ardıcıllığı ilə sıralanır və çəkiləri cəmi təxminən bərabər olan iki hissəyə ayrılır. Müvafiq olaraq hissələrdən hansınasa daxil olan simvol kodlarına sıfır, daxil olmayanlara isə bir qiyməti mənimsədilir. Buradan aydın olur ki, hissələrdən hər biri simvolların nizamlanmış sırasını özündə göstərir. Hər bir sırada bir simvol qaldıqda proses başa çatmış hesab olunur. Binar ağacın bir nöqtəsindən şaxələnmə zamanı simvolların qruplara bölünməsi baş verir. Hərəkət marşrutuna və kodlarına uyğun olaraq ağacın kökündən yarpaqlarına qədər sıfır və bir qiymətləri mənimsədilir.

Ö(2), L(3), K(3), Ə(6), N(3), İ(6), M(4), Ü(2), D(1), A(2), F(1), Q(1), B(1), Y(2), T(2), H(1), _(3)

Məlumatda peydə olunan simvolların statistikası



Şəkil 2.2.1 Şennon – Fano alqoritmində peydə olan simvolların statistikası

Məlumatların sıxılması, məlumatları təmsil etmək üçün lazım olan bit sayının azalmasıdır. Sıxlaşdırma məlumatı saxlama qabiliyyətinə qənaət edə bilər, fayl ötürülməsini sürətləndirə bilər və saxlama avadanlığı və şəbəkə genişliyi xərclərini azalda bilər .

Sıxılma prosesi məlumatların ölçüsünün necə kiçildiləcəyini müəyyən etmək üçün bir düstur və ya alqoritm istifadə edən bir proqram tərəfindən həyata keçirilir . Məsələn, bir alqoritm ardıcıllıqla əlaqəli bir lüğət istifadə edərək təkrarlanan simvolları daha kiçik bir sətir ilə təmsil edə bilər və ya düstur arayışı və ya göstərici əlavə edə bilər.

Mətnin sıxılması bütün lazımsız simvolları silmək , təkrarlanan simvolların bir simvolunu göstərmək üçün bir təkrar simvolu qoymaq və tez-tez baş verən bit sətirinə daha kiçik bir sətir əvəz etmək kimi sadə ola bilər . Məlumatların sıxılması mətn faylını 50% -ə və ya orijinal ölçüsünün xeyli yüksək hissəsinə endirə bilər.

Məlumat ötürülməsi üçün, başlıq məlumatları daxil olmaqla, məlumatların tərkibində və ya bütün ötürmə vahidində sıxılma aparıla bilər . Məlumat internet vasitəsilə göndərildikdə və ya qəbul edildikdə, tək və ya bir arxiv sənədinin bir hissəsi kimi başqalarına aid olan böyük bir fayl ZIP, GZIP və ya digər sıxılmış formatda ötürülə bilər .

Məlumatların sıxılması bir faylın tutduğu həcmi kəskin dərəcədə azalda bilər. Məsələn, 2 : 1 sıxılma nisbətində 20 meqabayt (MB) bir fayl 10 MB boş yer tutur.

Faktiki olaraq hər hansı bir fayl sıxışdırıla bilər, ancaq hansının sıxılacağını seçərkən ən yaxşı təcrübələrə əməl etmək vacibdir. Məsələn, bəzi fayllar artıq sıxılmış vəziyyətə gələ bilər, buna görə də bu faylları sıxışdırmaq əhəmiyyətli dərəcədə təsir göstərməyəcəkdir.

Məlumat sıxışdırılması həmiçinin mənbə kodlaşdırması adı ilə də tanınır, məlumatları daha az yaddaş tutacaq şəkildə kodlaşdırma və ya çevirmə prosesidir.

Məlumatın sıxışdırılması iki yolla edilə bilər - itkili sıxılma və itkisiz sıxılma. İtkili sıxılma, lazımsız məlumatları silməklə məlumatların həcmini azaldır, itkisiz sıxılma zamanı məlumat itkisi olmur.

Şennon Fano Alqoritmi, multimediyanın itkisiz məlumat sıxışdırılması üçün bir entropiya kodlaşdırma üsuludur. Meydana çıxma ehtimallarına görə hər simvola bir kod təyin edir. (20, s. 119-120).

Şennon alqoritmi aşağıdakı addımlardan ibarətdir:

- verilən simvollar dəsti üçün ehtimalların siyahısını və ya tezlik sayımını elə yaradın ki, hər simvolun meydana gəlməsinin nisbi tezliyi məlum olsun
- rəmzlərin siyahısını ehtimalın azalan ardıcıllığına, ən çox ehtimal olunanları sola və ən azı sağa doğru sıralansın
- siyahını iki hissəyə bölün, hər iki hissə mümkün qədər bir-birinə yaxın olsun
- 0 dəyərini sol hissəyə, 1-ni isə sağ hissəyə təyin edilsin
- bütün simvollar fərdi alt qruplara bölünməyincə hər hissə üçün 3 və 4 addımları təkrarlayın.

Hər bir simvolun kodu unikaldırsa, Şenon kodları dəqiq hesab olunur.

Nümunə üçün Şennon-Fano itkisiz sıxılma texnikasından istifadə edərək verilən simvollar dəsti üçün Şennon kodlarını quraq.

Simvol	A	B	C	D	E
Ehtimal	0.22	0.28	0.15	0.30	0.05

Cədvəl 2.2.2 Verilən simvollar dəsti üçün Şennon kodları cədvəli

Burada simvol və onlara uyğun tezlik ehtimalı dəyərləri giriş parametrləri olaraq qəbul edilir.

1-ci addımı həyata keçirərək verilən simvollar dəsti üçün ehtimalların siyahısını və ya tezlik sayımını elə yaradaq ki, hər simvolun meydana gəlməsinin nisbi tezliyi məlum olsun.

P (x) x simvolunun meydana çıxma ehtimalı olsun:

Rəmzləri ehtimalı azaltma qaydasında təyin edərkən:

$$P(D) + P(B) = 0.30 + 0.2 = 0.58$$

və

$$P(A) + P(C) + P(E) = 0.22 + 0.15 + 0.05 = 0.42$$

nəticələrini alırıq.

Tezlik ehtimallarına görə simvolları azalan sıra düzsək, aşağıdakı cədvəli alarıq:

Simvol	D	B	A	C	E
Ehtimal	0.30	0.28	0.22	0.15	0.05

Cədvəl 2.2.3 Verilən simvollar dəsti üçün Şennon kodları cədvəli

İndi isə {D, B} qrupunda

$$P(D) = 0.30 \text{ və } P(B) = 0.28$$

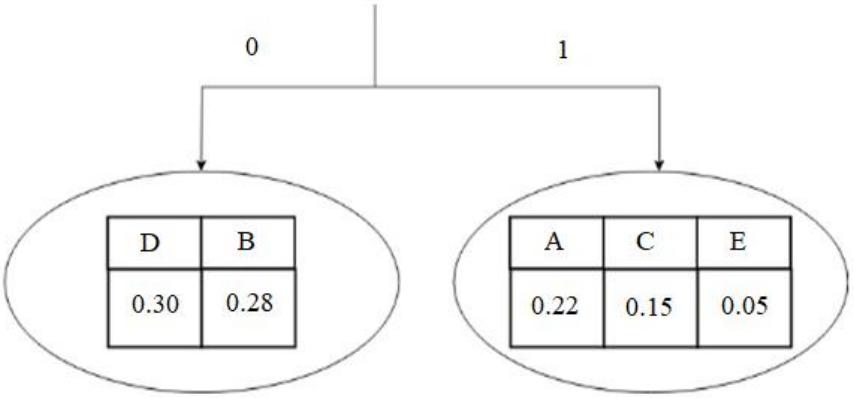
o deməkdir ki, P (D) ~ P (B) , buna görə {D, B} -ni {D} və {B} -ə bölün və D-yə 0 və B-yə 0 təyin edin.

Simvol	D	B	A	C	E
Ehtimal	0.30	0.28	0.22	0.15	0.05

Simvol	D	B
Ehtimal	0.30	0.28

Simvol	A	C	E
Ehtimal	0.22	0.15	0.05

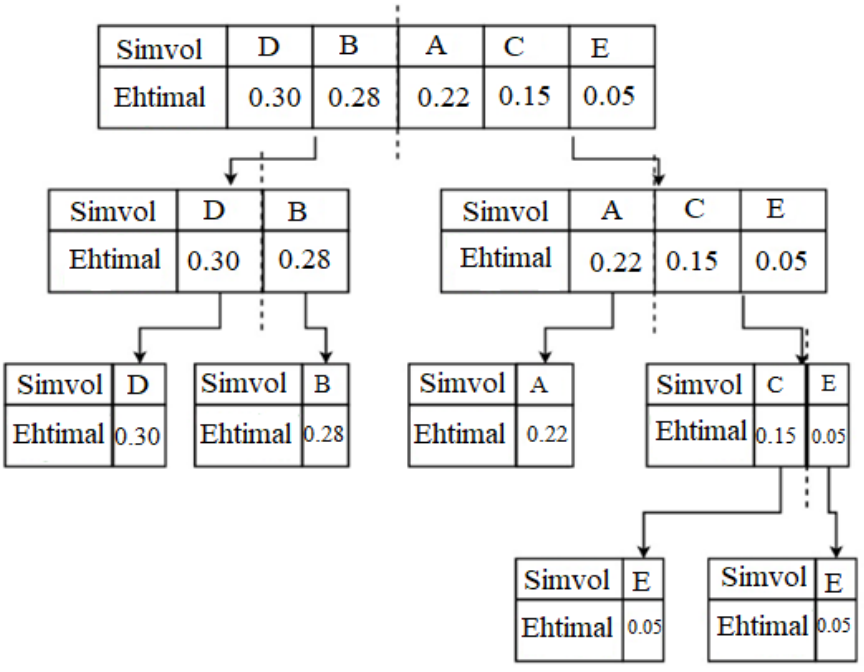
Cədvəl 2.2.4 Verilən simvollar dəsti üçün Şennon kodları cədvəli



Cədvəl 2.2.5 Verilən simvollar dəsti üçün Şennon kodları cədvəli

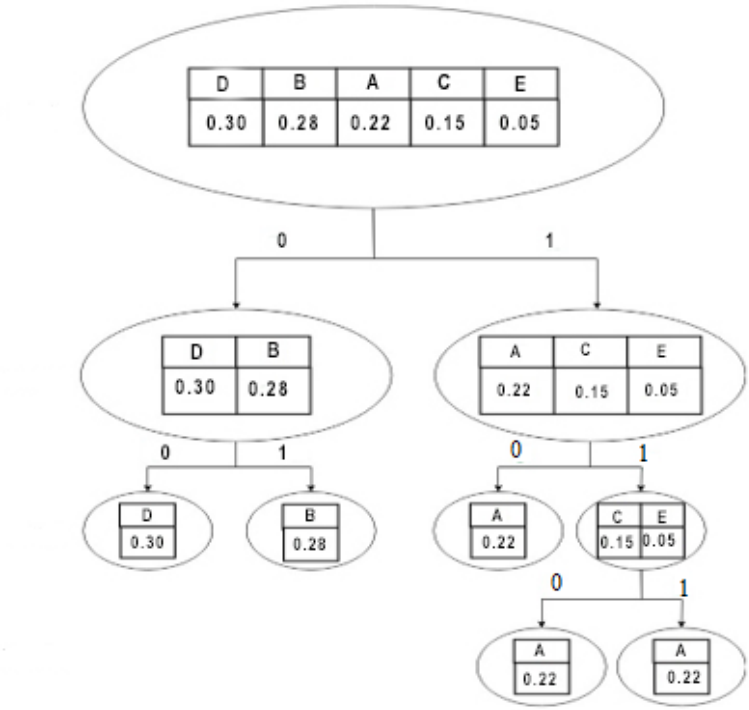
{A, C, E} qrupunda, P (A) = 0.22 **və** P (C) + P (E) = 0.20 olaraq hesablanır. Beleliklə qrup: {A} və {C, E} olaraq 2 yerə bölündür və müvafiq olaraq 0 və 1 dəyərləri aldı.

{C, E} qrupunda**,** P (C) = 0.15 **və** P (E) = 0.05 qiymətləri alıb. Beləliklə, onları {C} və {E} bölüb və 0-nı {C} və 1-ni {E} -ə təyin etmək lazımdır.



Cədvəl 2.2.6 Verilən simvollar dəsti üçün Şennon kodları cədvəli

4-cü addımdan sonra Şennon ağacı aşağıdakı kimi olacaq:



Cədvəl 2.2.7 Verilən simvollar dəsti üçün Şennon kodlar ağacı

Hər simvol ayrılıb bitdiyində artıq parçalanma prosesi saxlanılır. Addımlar nəticəsində əldə edilən simvollar dəsti üçün Şenon kodları bunlardır:

Simvol	A	B	C	D	E
Ehtimal	0.22	0.28	0.15	0.30	0.05
Şannon kodu	00	01	10	110	111

Cədvəl 2.2.8 Verilən simvollar dəsti üçün yekin Şennon kodları cədvəli

Göründüyü kimi, kodlar hamısı unikaldır və müxtəlif uzunluqdadırlar.

Bu kodlaşdırma metodu informasiya nəzəriyyəsi sahəsinə təkan verdi və onun töhfəsi ilə bir çox yeniliklərin baş verməsi sürətləndi; məsələn Huffman kodlaşdırması və ya arifmetik kodlaşdırma . Gündəlik həyatımızın bir çox hissəsi rəqəmsal məlumatlar tərəfindən əhəmiyyətli dərəcədə təsirlənir və Shannon kodlaşdırması və onun əsasında qurulna metodlarının davam etməsi olmadan bu mümkün olmazdı.

2.3 Huffman alqoritmi

Kompüter elmində və məlumat nəzəriyyəsində, Huffman kodu, məlumatların itkisiz sıxılması üçün istifadə olunan xüsusi bir prefiks kodunun müəyyən bir növüdür. Belə bir kodun tapılması və ya istifadəsi prosesi H.D. Huffman tərəfindən, o hələ MİT tələbəsi olan zaman hazırlanıb və "Huffman kodlaşdırması" başlığı altında davam edib. Bu haqda ilk məqalə 1952-ci il tarixli "Kodların minimal sıxlaşdırılması" adlı qəzetdə dərc edilmişdir.

Huffman kodlaşdırması, ASCII simvollarının məlumat sıxılmasını idarə edən bir sıxlaşdırma alqoritmidir. Alqoritm, minimal ardıcıllığı yaratmaq üçün yuxarıdan aşağıya doğru ikili ağac yaradır.

Huffman alqoritmi məlumat faylı içərisindəki simvolları ikili koda çevirir. Bununla birlikdə, fayldakı əsas simvolların ən kiçik ikili kodu, ən az meydana çıxan simvollar isə ən uzun ikili kodlara malikdir.

Huffmanın alqoritmindən çıxan nəticə odur ki, simvolu kodlaşdırmaq üçün dəyişən uzunluqlu bir kod cədvəli kimi baxmaq olar (məsələn, bir sənəddəki bir simvol). Alqoritm, bu cədvəlin mənbə simvolunun hər mümkün dəyəri üçün ehtimal olunan ehtimalından və ya baş vermə tezliyindən irəli gəlir. Digər entropiyanın kodlaşdırma metodlarında olduğu kimi, daha çox yayılmış simvollar ümumiyyətlə az ümumi simvollardan daha az bit istifadə edərək təmsil olunur. Huffman metodu, bu çəkilər sıralanırsa, giriş çəkilərinin sayına vaxtında bir kod taparaq səmərəli şəkildə həyata keçirilə bilər. Bununla birlikdə simvolları ayrıca kodlaşdıran metodlar arasında optimal olmasına baxmayaraq, Huffman kodlaşdırması bütün sıxılma metodları arasında həmişə optimal deyildir.

1951-ci ildə David A. Huffman və onun MIT məlumat nəzəriyyəsi sinif yoldaşlarına bir müddətli sənəd və ya son imtahan seçimi verildi. Professor Robert M.

Fano ən səmərəli ikili kodun tapılması problemi ilə bağlı müddətli bir sənəd təyin etdi. Heç bir kodun ən səmərəli olduğunu sübut edə bilməyən Huffman, tezlikli çeşidli ikili ağacı istifadə etmək fikrinə düşdükdə və bu üsulun ən səmərəli olduğunu tez bir zamanda sübut etmək üçün imtina edib sona hazırlaşmağa hazırlaşmışdı.

Bununla, Huffman, oxşar kod hazırlamaq üçün məlumat nəzəriyyəsi ixtiraçısı Klod Şennonla birlikdə işləyən Fanodan üstün oldu. Şennon - Fano kodlaşdırmadan fərqli olaraq, ağacı aşağıdan yuxarıya zəmanət verən optimallıq.

Kodlaşdırılmış informasiyanın deşifrə edilə bilçəsi üçün deşifrəliyicidə kod ağacı və ya kod cədvəli olmalıdır.

Əlifba üçün Huffman ağacını qurmaqdan ötrü faylın əvvəlini oxumaq lazımdır. Deşifrələyicinin ağacın budaqları ilə hərəkət etməsi üçün ilk ikilik simvolu əldə etmək lazımdır.

Sıxlaşdırma. Huffman kodlaşdırması, hər bir simvol üçün nümayəndəliyi seçmək üçün müəyyən bir metoddan istifadə edir, nəticədə bir prefiks kodu olur (bəzən "prefikssiz kodlar" deyilir, yəni müəyyən bir simvolu təmsil edən bit sətri heç bir digərini təmsil edən bit sətrinin prefiksi deyildir) simvolu). Huffman kodlaşdırması prefiks kodların yaradılması üçün belə geniş yayılmış bir metoddur ki, "Huffman kodu" termini Hufman alqoritmi tərəfindən belə bir kod istehsal olunmasa belə "prefiks kodu" üçün sinonim kimi geniş istifadə olunur.

Texnika qovşaqların ikili ağacını yaratmaqla işləyir. Bunlar ölçüsü simvolların sayına bağlı olan müntəzəm bir serialda saxlanıla bilər.

Proses, təmsil etdikləri simvolun ehtimallarını ehtiva edən yarpaq qovşaqlarından başlayır. Sonra, proses ən kiçik ehtimalı olan iki düyünü götürür və uşaq olaraq bu iki qovşaqa sahib yeni bir daxili qovşaq yaradır. Yeni nodun çəkisi uşaqların çəkisinin cəminə təyin olunur. Daha sonra prosesi yenidən, yeni daxili qovşaqda və qalan qovşaqlarda tətbiq edirik (yəni iki yarpaq düyünü xaric edirik), Huffman ağacının kökü olan yalnız bir node qalana qədər bu prosesi təkrarlayırıq.

Rəmzlər ehtimala görə sıralanırsa, iki növbədən istifadə edərək Huffman ağacı yaratmaq üçün xətti zamanlı (O (n)) metod var, birincisi, ilk çəkiləri (əlaqəli yarpaqlara göstərici ilə birlikdə) və birləşdirilmiş çəkilərdən istifadə etməklə (ağaclara göstərici ilə birlikdə) ikinci növbənin arxasına qoyulur. (13, s. 41 - 43).

Dekompozisiya. Ümumiyyətlə, dekompozisiya prosesi sadəcə prefiks kodlarının axını fərdi bayt dəyərlərinə tərcümə etmək məsələsidir, ümumiyyətlə Huffman ağac nodunu düyünlə keçməklə hər bit giriş axınından oxunur (yarpaq nodeuna çatmaq mütləq axtarışa xitam verir) müəyyən bayt dəyəri üçün). Bunun baş verməsindən əvvəl, Huffman ağacı birtəhər yenidən qurulmalıdır. Ən sadə vəziyyətdə, xarakter tezliklərinin olduqca proqnozlaşdırıldığı yerlərdə, ağac əvvəlcədən düzəldilə bilər (və hətta hər bir sıxılma dövrü statistik olaraq düzəldilə bilər) və beləliklə hər dəfə yenidən istifadə edilə bilər, heç olmasa bir sıxılma səmərəliliyi hesabına. Əks təqdirdə, ağacın yenidən qurulması üçün məlumat bir priori göndərilməlidir. Sadəlövh bir yanaşma, hər bir xarakterin tezlik sayımını sıxılma axınına üstünlük vermək ola bilər. Təəssüf ki, belə bir vəziyyətdə yerüstü xərc bir neçə kilobayt təşkil edə bilər, buna görə də bu metodun praktik istifadəsi azdır. Məlumatlar kanonik kodlaşdırma istifadə edərək sıxılırsa, sıxılma modeli yalnız {\ displaystyle B2 ^ {B}} B2 ^ {B} məlumat dəsti ilə dəqiq şəkildə yenidən qurulur (burada {\ displaystyle B} B hər simvola bitinin sayıdır)). Başqa bir üsul, Huffman ağacını bir az da azaldıqca çıxış axınına sürükləməkdir. Məsələn, 0 dəyərinin ana node və 1 yarpaq nodunu təmsil etdiyini fərz etsək, sonuncu ilə rastlaşdıqda ağacın qurulması qaydası həmin xüsusi yarpağın xarakter dəyərini təyin etmək üçün növbəti 8 biti oxuyur. Son yarpaq düyününə çatana qədər proses rekursiv şəkildə davam edir; o anda Huffman ağacı beləliklə sədaqətlə yenidən qurulacaqdır. Belə bir metoddan istifadə edən yerüstü hava təxminən 2 ilə 320 bayt arasında dəyişir. Bir çox başqa texnika da mümkündür. Hər halda, sıxılmış məlumatlar istifadə olunmamış "izləmə bitlərini" əhatə edə biləcəyi üçün dekompressor məhsul istehsalını nə vaxt dayandıracağını müəyyənləşdirməlidir. Bu ya dekompozisiya edilmiş məlumatların uzunluğunu sıxılma modeli ilə birlikdə ötürməklə və ya girişin sonunu

bildirmək üçün xüsusi kod simvolu təyin etməklə həyata keçirilə bilər (sonuncu metod kod uzunluğu optimallığına mənfi təsir göstərə bilər).

İstifadə olunan ehtimallar ortalama təcrübəyə əsaslanan tətbiq sahəsi üçün ümumi ola bilər və ya mətndə sıxılmış olan faktiki tezliklər ola bilər. Bunun üçün bir tezlik cədvəlinin sıxılmış mətnlə birlikdə saxlanılmasını tələb edir. Bu məqsədlə istifadə olunan müxtəlif texnikalar haqqında daha çox məlumat üçün yuxarıdakı dekompressiya bölməsinə baxın.

Huffmanın orijinal alqoritmi, məlum bir giriş ehtimal paylaması ilə simvolik bir simvollaşdırma üçün, yəni ayrı-ayrılıqda belə bir məlumat axınında əlaqəsiz simvollar kodlaşdırmaq üçün optimaldır. Bununla birlikdə, simvol tərəfindən simvol məhdudlaşdırılması düşdükdə və ya ehtimal olunan kütlə funksiyaları bilinməyəndə optimal deyildir. Ayrıca, simvollar müstəqil deyil və eyni şəkildə paylanmırsa, vahid bir kod optimallıq üçün qeyri-kafi ola bilər. Arifmetik kodlaşdırma kimi digər üsullar daha yaxşı sıxılma qabiliyyətinə malikdir.

Yuxarıda göstərilə göstərilən hər iki metod daha səmərəli kodlaşdırma üçün ixtiyari sayda simvolları birləşdirə və ümumiyyətlə faktiki giriş statistikasına uyğunlaşa bilsə də, hesablama və alqoritmik mürəkkəbliklərini əhəmiyyətli dərəcədə artırmadan arifmetik kodlaşdırma bunu edir (ən sadə versiya Huffman kodlaşdırmadan daha yavaş və daha mürəkkəbdir). Bu cür rahatlıq, giriş ehtimalları dəqiq məlum olmadıqda və ya axın içərisində əhəmiyyətli dərəcədə dəyişdikdə xüsusilə faydalıdır. Bununla birlikdə, Huffman kodlaşdırması ümumiyyətlə daha sürətlidir və arifmetik kodlaşdırma tarixən patent məsələlərinə dair bir narahatlıq mövzusu idi. Beləliklə, bir çox texnologiya Huffman və digər prefiks kodlaşdırma texnikalarının xeyrinə tarixən arifmetik kodlaşdırmadan çəkinmişdir. 2010-cu ilin ortalarından etibarən, Huffman kodlaşdırmasına alternativ olan ən çox istifadə edilən üsullar erkən patentlərin müddəti bitdiyindən ictimai sahəyə keçdi.

Vahid ehtimal paylaması və iki gücə sahib olan bir sıra üzv olan simvollar dəsti üçün Huffman kodlaşdırması sadə ikili blok kodlaşdırmasına, məsələn, ASCII kodlaşdırmasına bərabərdir. Bu, sıxılma üsulunun nə olursa olsun, yəni məlumatlara heç bir şey etməməyin ən optimal olan bir şey ilə sıxılmanın mümkün olmadığını əks etdirir.

Hər giriş simvolu məlum olmayan müstəqil və eyni şəkildə paylanmış təsadüfi dəyişən dəyişkən olduqda, dyadik olan bir ehtimala sahib olduqda Huffman kodlaşdırması bütün üsullar arasında optimaldır. Prefiks kodları və xüsusən Huffman kodlaşdırması kiçik əlifbalarda təsirsizliyə meyllidir, burada ehtimallar bu optimal (dyadik) nöqtələr arasında tez-tez düşür. Huffman kodlaşdırması üçün ən pis hal, ən çox ehtimal olunan simvolun ehtimalı 0.5-dən çox olduqda baş verə bilər, bu da nəticəsizliyin yuxarı həddini məhdudlaşdırmır.

Huffman kodlaşdırmasından istifadə edərkən bu təsirsizliyin ətrafında iki əlaqəli yanaşma mövcuddur. Sabit sayda simvolları bir araya gətirmək ("bloklama") sıxılma tez-tez artır (və azalmır). Blokun ölçüsü sonsuzluğa yaxınlaşdıqca nəzəri olaraq kodlaşdıran Huffman, entropiya həddinə, yəni optimal sıxılmağa yaxınlaşır. Bununla birlikdə, ixtiyari olaraq böyük simvollar qruplarının bloklanması praktik deyil, çünki Huffman kodunun mürəkkəbliyi kodlanma imkanlarının sayında, blok ölçüsündə eksponensial olan bir sıra cərəyan edir. Bu, praktikada edilən bloklama miqdarını məhdudlaşdırır (6, s. 2 - 3).

Geniş istifadədə praktik alternativ, uzun müddətli kodlaşdırmadır. Bu üsul, əvvəlcədən kodlanmış təkrar simvolların sayılması (işlənməsi) saymaqdan əvvəl, entropiyanın kodlaşdırılmasından bir addım əvvəl əlavə edir. Bernoulli proseslərinin sadə bir işi üçün, Golomb kodlaşdırması qaçış uzunluğunu kodlaşdırmaq üçün prefiks kodlar arasında optimaldır, Huffman kodlaşdırma üsulları ilə sübut olunmuş bir metoddur. Bənzər bir yanaşma dəyişdirilmiş Huffman kodlaşdırmasından istifadə

edərək faks maşınları tərəfindən qəbul edilir. Bununla birlikdə, uzun müddətli kodlaşdırma digər sıxılma texnologiyaları kimi bir çox giriş növünə uyğun deyil.

Rabitə sisteminin əsas niyyəti mesajları göndərəndən alıcıya ötürməkdir. Bu müddətdə məlumatı ötürmək üçün istifadə olunan siqnal ötürmə kanalının xüsusiyyətlərinə uyğun olmalıdır. Məlumat kodlaşdırması mesajı siqnala çevirmək üçün istifadə olunur. Huffman kodlaşdırması və Shannon Fano kodlaşdırması arasındakı əvvəlki fərq, Huffman kodlaşdırmasının dəyişən uzunluqlu bir kodlaşdırma mexanizmi istifadə etməsidir.

Huffman kodlaşdırma və Şennon - Fano kodlaşdırma arasındakı əsas fərqlər bunlardır:

- Huffman kodlaşdırması, Şennon - Fano kodlaşdırma alqorimindən faydalanaraq edərkən prefiks kod şərtlərindən istifadə edir
- Şennon - Fano kodlaşdırma üsulu ilə istehsal olunan kodlar optimal deyil, lakin Huffman kodlaşdırması optimal nəticələr verir

Hər iki kodlama metodu arasında Huffman kodlaşdırması Şennon - Fano kodlaşdırmasından daha effektiv və optimaldır.

2.4 Prefiks kodların statik sistemləri

İnformasiyada simvollar arasında qarşılıqlı əlaqələrin mövcud olması, simvollar arasında korrelyasiya əlaqələrinin olduğunu göstərir. Bu termin Markov zənciri və Markov mənbəyi anlayışlarıyla əlaqəlidir.

Fərz edək ki, informasiya istehsal edən S mənbəyi verilib. Bu məlumat mənbəyinin cari vəziyyəti, onun əvvəlki vəziyyətini yadda saxladığı üçün yaddaşlı mənbə adlanır. Yaddaşlı mənbədən çıxan simvollar Markov zənciri yaradır.

İnformasiyada meydana çıxan simvolların ehtimalları ardıcıllığı ancaq vahid simvolla müəyyən edilirsə, bu zaman birəlaqəli Markov zəncirini yaranır. Simvolun

mövcud olma ehtimalı əvvəlki Z simvoldan asılı olan halda deyilir ki, o, Z-əlaqəli Markov əmələ gətiri.

Ümumiyyətlə, Markov mənbəyi bir model kimi, real informasiya mənbəyinin xususiyyətlərinə uyğun deyil. Buna baxmayaraq, model çox fəal müxtəlif informasiya proseslərini təsvir etmək praktikası ilə məşğuldur.

D elementindən ibarət müəyyən çoxluğu B ilə işarə edək: B={b1, b2,...,bD}. Bu çoxluğu mənbənin kod əlifbası adlandıraq. B çoxluğunun elementləri isə kod simvolları adlandırılır.

Eyni səviyyəli kodlaşdırmada m uzunluqlu fərqli sözlərin sayı D^m, kod sözünün uzunluğu ən çoxu m olan fəqli uzunluqlu kodlaşdırmada müxtəlif kod sözlərinin sayı D(D^m-1)/(D-1) kəmiyyətindən çox deyil.

Fərz edək ki, uzunluğu n-ə bərabər olan məumatlar çoxluğu iki alt çoxluğa bölünüb. Birinci çoxluq o elementlərdən ibarətdir ki, həmin elementləri qarşılıq olaraq birqiymətli kod sözləri uyğun gəlir. Belə altçoxluq birqiymətli kodlaşdırılan və dekodlaşdırılan bloklar çoxluğu adlandırılır.

İkinci çoxluq isə birinci çoxluğa daxil olmayan bloklardan ibarətdir və bu çoxluqda hər bir bloka qarşı eyni kod sözü qoyulur. Uzunluğu m-ə bərabər, bütün kod sözləri D(m) ədədi ilə müəyyən olunur.

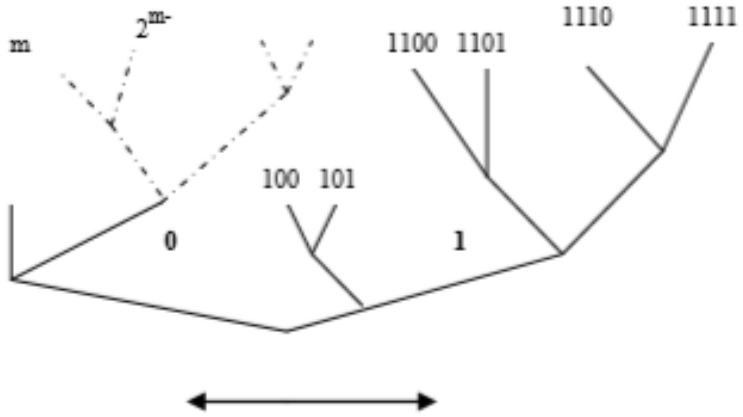
Kodlaşdırma zamanı sərf olunan simvolların sayı, məlumatdan asılıdır və buna görə özündə təsadüfi kəmiyyəti göstərir.

Prefiks kodlar – kod sözlərindən biri başqasının başlanğıcı olmayan kodlardır.

Prefiks kodlar birmənalı dekodlaşdırma xassəsinə malikdir, lakin əksi doğru deyil.

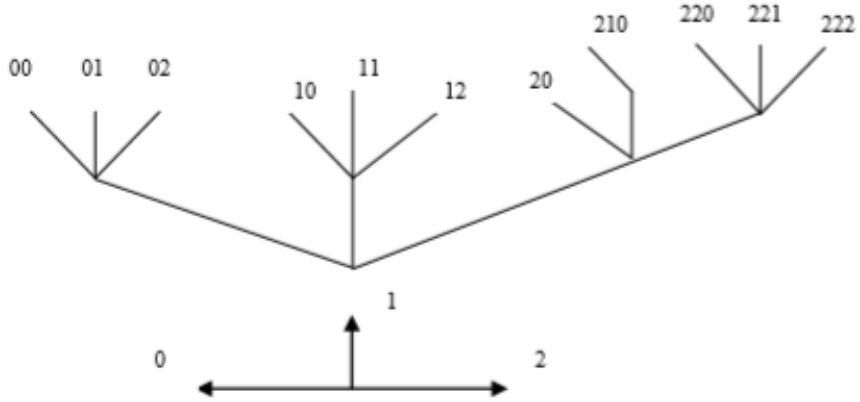
Kraft ağacı, Kraft bərabərsizliyi. Prefiks kodları birmənalı dekodlaşdırma xassəsinə malikdir. Kod ağaclarından prefiks kodlarını izah etmək üçün istifadə edirlər. Fərz edək ki, bizə ilgəyi və qapalı yolları olmayan qraf verilib. Qrafın təpə nöqtələrinə bir til daxil olur və buradan ən çoxu D til çıxır (qrafın başlanğıcı istisna olmaq şərti ilə).

Bu cür qrafa D-lik kod ağacı deyilir. Qrafın təpəsindən çıxan tillərin hər birinə kod əlifbasının bir simvolu ayrılır. Ancaq nəzərə almaq lazımdır ki, bir təpədən çıxan fərqli tilllər qarşılıq olaraq fərqli simvollar qoyulur.



Şəkil 2.4.1 İkilik kod ağacı

Hər bir sağ tilə qarşı 1, hər bir sol tilə qarşı isə 0 qoyulur. Şəkil 2.4.2 – də üçlük kod ağacı göstərilmişdir. Bu üçlük aşağıdakı kodlara uyğundur 00,01,02, 10,11,12,20, 210, 220, 221, 222.



Şəkil 2.4.2 Üçlük kod ağacı

Teorem 1 (Kraft bərabərsizliyi). Uzunluqları m1,...., mм olan kod sözlərinin prefiks kodları olması üçün mütləq və kafi şərt

$$\sum_{i=1}^{M} D^{-m_i} \leq 1$$

şərtinin ödənməsidir.

İsbatı. Teoremin isbatı son təpə nöqtələri m1,....,mм yaruslu olan qrafın mövcud olması ilə əlaqədardır. Yuxarda (1) üçün vaciblik şərtini isbat etdik. İndi isə kafilik şərtini isbat edək, yəni yuxarıdakı şərti ödəndiyi halda son təpə nöqtələri m1,....,mм yarus olan qrafı qurmaq mümkündür. Fərz edək ki, bu yığım arasında ədədi sırası s-ə bərabər olan yarusa α_s dəfə rast gəlinir. O zaman

$$\sum_{i=1}^{M} D^{-m_i} = \sum_{s=1}^{m} \alpha_s D^{-s} \leq 1$$

Bu bərabərsizliyi aşağıdakı şəkildə yazaq:

$$\sum_{s=1}^{i-1} \alpha_s D^{-s} + \alpha_i D^{-i} + \sum_{s=i+1}^{m} \alpha_s D^{-s} \leq 1$$

Cəmləri bərabərsizliyin sağ tərəfinə keçirərək tərəfləri D^i-yə vuraq. Bu zaman

$$\alpha_i \leq D^i - \sum_{s=1}^{i-1} \alpha_s D^{i-s} - \sum_{s=i+1}^{m} \alpha_s D^{i-s} \leq D^i - \sum_{s=1}^{i-1} \alpha_s D^{i-s}$$

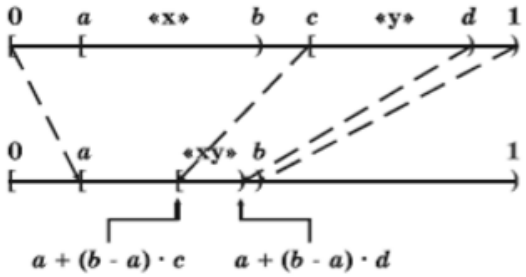
tam induksiya metodunu tətbiq edək. i=1 olduqda, ağac bir dərəcəli yarusu α_1 dəfə saxlayır. Fərz edək ki, ağacın s dərəcəli yarusu, α_s – saydadır, s = x, x+1,..., x*i-1 üçün yarusları qurmaq olar. İsbat edək ki, bu ağaca α_i sayda, i dərəcəli yarus əlavə etmək olar. Bu induksiya doğru olduğu halda, i dərəcəli yarusdan $\sum_{s=1}^{i-1} \alpha_s D^{i-s}$ mümkün sayda son təpə nöqtələrini almaq olar. Mümkün olan son təpə nöqtələrinin maksimal həddi D^i bərabərdir. i yarusundakı sərbəst təpələrin sayı

$$D^i - \sum_{s=1}^{i-1} \alpha_s D^{i-s}$$

bərabərdir.

2.5 Hesabi kodlaşdırma

Kodların yaranması üçün hesabi kodlaşdırma üsulunun tətbiq edildiyi yanaşmanın obyektiv mürəkkəbliyinə baxmayaraq, onun əsasını təşkil edən ideya çox sadədir. Ədədi intervalın uzunluğu informasiya mənbəyinin çıxışında simvolun yaranması ehtimalı ilə eyni olur. Tutaq ki, xəbərdə rast gəlinən "x" simvolu [a, b) intervalına və arxasınca gələn "y" simvolu [c, d) intervalına uyğundur. [a,b) intervalı [0,1) intervalına proyeksiya edildikdə sonra istənilən ədəd "xy" ardıcıllığını birmənalı müəyyən edəcəkdir.



Şəkil 2.5.1 Hesabi kodlaşdırmanın işinə nümunə

Əlavə simvollardan istifadə edərək intervalı kiçiltmək olar. Bunu təkrarlayaraq ilkin xəbəri birmənalı müəyyən edə biləcək kiçik interval əldə etmək olar.

İndi isə hesabi kodlaşdırmaya aid bir misala baxaq. Fərz edək ki, "aaab" xəbərini kodlaşdırmaq lazımdır. Xəbərdə "a" simvolunun yaranma tezliyi 3/4, "b" simvolunun yaranma tezliyi isə 1/4 bərabərdir. Buna görə də, "a" simvoluna uyğun olaraq [0, 3/4) intervalını, "b" simvoluna isə [3/4, 1) intervalını qarşı qoymaq olar (sıfır modeli istifadə olunur).

Simvol sayı çox olan məlumatları emal etdikdə hesabi kodlaşdırma, optimal kodlaşdırma nəzəriyyəsinə uyğun nəticə verir. Lakin sonlu həcmli informasiyalarda kodlaşdırma və optimal kodlaşdırma arasında fərq yaranır. Tutaq ki, yuxarda təsvir olunan proseslə intervalların birbirinə daxil olması nəticəsində uzunluğu p olan [d, e) intervalı əldə edilib. m mərtəbəli ədəddən kiçik olan müəyyən ədədi bu intervaldan

seçmək tələb olunur. m bu sistemin əsası hesab olunur. m(N) nöqtələr ardıcıllığını elə seçək ki, onlardan biri [d, e) intervalına aid olsun. Aydındır ki, axtarılan ədəd

$$\frac{1}{m^N} \leq p$$

şərtini ödəyəcəkdir. Burada

$$N = [-\log_m p]$$

düsturu ilə hesablanır. Beləliklə, kod ədədi

$$[-\log_m p] < [-\log_m p]+1$$

mərtəbəli olmalıdır (20, s. 132-133). Hesabi kodlaşdırmada intervalların seçilməsi şərtidir. Belə ki, yuxarda baxdığımız misalda "d" simvoluna uyğun olaraq [1/4, 1) intervalını, "e" simvoluna isə [0, 1/4) intervalını götürə bilərik. İntervalların uzunluqları dəyişməsə də simvolların [0, 1) intervalında yerləşmə yeri fərqli olacaq. Hesabi kodlaşdırma zamanı kod simvollarının kombinasiyası (birləşməsi) sərbəst götürülür.

Şərh. 1952-ci ildə David Huffman, təkrar edilən simvollar üçün "Bir neçə rəqəmi istifadə edərək bir mesaj kodlamaq lazım olarsa, ən az rəqəmlərdən istifadə edərək mesajı necə kodlamaq mümkündür?" sualına cavabı "Minimum-Redundancy Kodlarının qurulması üçün bir metod" adlı məqalədə yazdı və bir metod təklif etdi.

Prefiks kodlaşdırmada kodlanacaq hər bir simvol bir və ya daha çox rəqəmdən ibarət kodlar şəklində verilir. Bu kodları təyin edərkən hər hansı bir kod özündən daha uzun başqa bir kodun başlanğıcı olmamalıdır.

Məlumatların sıxılması, məlumatları təmsil etmək üçün lazım olan bit sayının azalmasıdır. Sıxlaşdırma məlumatı saxlama qabiliyyətinə qənaət edə bilər, fayl ötürülməsini sürətləndirə bilər və saxlama avadanlığı və şəbəkə genişliyi xərclərini azalda bilər .

Kompüter elmində və məlumat nəzəriyyəsində, Huffman kodu, məlumatların itkisiz sıxılması üçün istifadə olunan xüsusi bir prefiks kodunun müəyyən bir növüdür.

Huffman kodlaşdırması, ASCII simvollarının məlumat sıxılmasını idarə edən bir sıxlaşdırma alqoritmidir. Alqoritm minimal ardıcıllığı yaratmaq üçün yuxarıdan aşağıya doğru ikili ağac yaradır. Huffman alqoritmi məlumat faylı içərisindəki simvolları ikili koda çevirir. Bununla birlikdə, fayldakı əsas simvolların ən kiçik ikili kodu, ən az meydana çıxan simvollar isə ən uzun ikili kodlara malikdir.

Huffman alqoritminin məqsədi ən çox istifadə olunan simvollara (və ya sıxdığımız məlumatda ən çox istifadə olunan bitlərə) ən qısa kodu vermək üçün prefiks ağacını yaratmaqdır. Bunun üçün istifadə ediləcək alqoritm aşağıdakı kimidir.

- simvolları mətndə istifadə olunma sayına görə sıralamaq
- ən kiçik iki simvolu qruplaşdırmaq və tezliyini toplayaraq növbəyə əlavə etmək
- yalnız bir qrup qalana qədər qruplaşdırmaya davam etmək.

III Fəsil. Kommunikasiya kanalının xüsusiyyətləri

3.1 Müasir telekommunikasiya sistemləri

Siqnal müəyyən bir şəkildə kodlanmış məlumatı daşıyır. Kibernetikanın əsas anlayışlarından biri siqnal anlayışıdır. Siqnal termini informasiyanın emalı və ötürülməsi ilə əlaqədar olaraq, bir çox elmi texniki sahələrdə geniş istifadə olunur.

Siqnal bir sistemdə və ya bir neçə sistemin qarşılıqlı təsir prosesində yaradılmış, informasiya kanalı vasitəsilə ötürülən koddur (simvol, işarə). Siqnalın mənası və qiyməti qəbul edən sistem tərəfindən qeydiyyat prosesi zamanı ortaya çıxır.

İnformasiya və kommunikasiya nəzəriyyəsində siqnal – rabitə sistemində məlumatların ötürülməsi üçün istifadə olunan material daşıyıcısıdır. Bir siqnal yaradıla bilər, lakin məlumatdan fərqli olaraq, onun qəbul edilməsi mütləq tələb olunmur.

Müasir baxımdan TKS bir sıra texniki vasitələrdən və onların fəaliyyəti üçün lazım olan alqoritmlərdən ibarətdir. Təyinatına görə məlumatı mənbədən alıcıya ötürülməsi üçün nəzərdə tutulur.

Telekommunikasiya xidməti yerinə yetirdiyi məsələnin xarakterinə uyğun olaraq üç əsas sahəyə ayrılır:

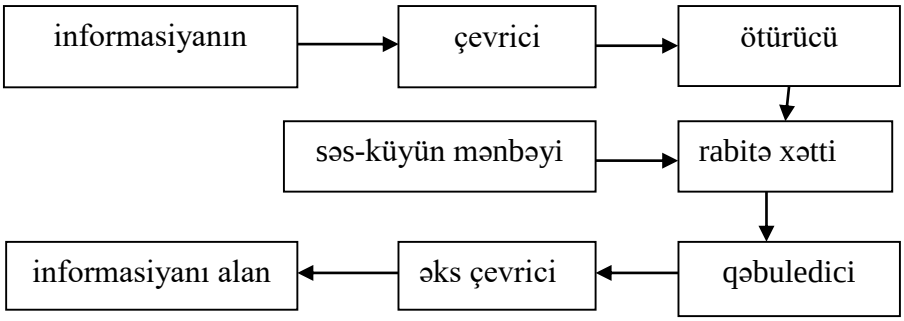
- Rabitə sistemi - buraya naqillərlə, naqillərsiz və optik liflərlə ötürmələr daxildir. Eyni zamanda, bu sahəyə yerdən və kosmosdan birbaşa translyasiyanı, eləcə də təkrar translyasiyanı tətbiq edən sistemlər aiddir.
- Radio və televiziya verlişlərini birbaşa translyasiya və təkrar translyasiya edən sistemlər.
- İnternet - bu müxtəlif cür komponentlərdən təşkil olunub (sputniklər, radiostansiyalar, kommutatorlar, kompüterlər və s.).

Ən fundamental formada telekommunikasiya sistemi, məlumat almaq və onu bir siqnala çevirmək üçün bir ötürücü, siqnal keçirmək üçün bir ötürücü vasitə və siqnalı

qəbul etmək üçün qəbuledicidən ibarətdir. Telekommunikasiya şəbəkəsinin altı əsas komponenti var:

- Giriş və çıxış cihazları, 'terminallar' olaraq da adlandırılır. Bunlar bütün rabitənin başlanğıc və dayanma nöqtələrini təmin edir. Telefon bir terminal nümunəsidir. Kompüter şəbəkələrində bu qurğular ümumiyyətlə qovşaq adlanır.
- Məlumat ötürən və qəbul edən telekommunikasiya kanalları. Buraya müxtəlif növ kabellər və simsiz vasitələr daxildir.
- Nəzarət və dəstəkləmə funksiyaları təmin edən telekommunikasiya prosessorlarına misal olaraq məlumatların analoqdan formadan rəqəmsal formaya və əksinə çevrilməsini həyata keçirən çeviriciləri göstərmək olar.
- Şəbəkənin işləməsinə və fəaliyyətinə nəzarət etmək üçün cavabdeh olan idarəetmə proqramı
- Mesajlar - ötürülən faktiki məlumatları təmsil edir
- Protokollar - hər bir telekommunikasiya sisteminin mesajları necə idarə etdiyini göstərir. Məsələn, GSM və 3G mobil telefon rabitəsi üçün protokollar, TCP / IP isə İnternet üzərindəki rabitə protokoludur.

TKS - in Şennon tərəfindən verilən struktur sxemi aşağıda göstərilmişdir.



Şəkil 3.1.1 TKS-in Şennon tərəfindən verlmiş struktur sxemi

Burada informasiyanın rabitə xətti ilə mənbədən alıcıya ötürülməsi zamanı lazım olan düzünə və əks çevrmələr göstərilmişdir. Bununla belə, informasiyanın növünün və xüsusi çevrilmə əməliyatlarının rabitə xəttinin tipi ilə əlaqəsi yoxdur. Vacib olan isə aşağıdakı iki vəziyyətdir:

- hər iki mənbədə informasiyanın yaradılma sürəti, rabitə kanalının iş sürəti ilə razılaşdırmaq lazımdır
- rabitə kanalı, əks çevirmə zamanı məlumatın alıcısını razı salan yüksək keyfiyyətlə, informasiyanın ötürülməsini təmin etməlidir

Hər bir blokun iş fəaliyyətinə baxaq.

İnformasiya mənbəyi alıcıya lazım olan informasiyanı yaradır. İnformasiya müxtəlif növ ola bilər. Məsələn, əlifbada olan hərflər ardıcıllığı, telqrafda olan tire və nöqtələr düzümü ilə ifadələr, radioqəbuledici və televiziyanın müəyyən funksiyaları və s.

Çevrici məlumatın çevrilməsi və emalı funksiyasını yerinə yetirir. Çevrici rabitə kanalına ötürmək üçün ikilik kodda simvollar ardıcıllığını özündə göstərir. Ötürücü öz növbəsində rabitə xəttinin xarakterinə uyğun olaraq siqnallar ardıcıllığını düzəldir. Rabitə xətti konkret fiziki mühitdir, siqnalları ötürücüdən, qəbulediciyə göndərmək üçün istifadə edilir. TKS rabitə xəttinə əsasən məlumatlar, danışıq, səs və video şəkillər göndərilir. Qəbuledici ötürücünün icra etdiyi əməliyyata münasibətdə, əks əməliyyatı yerinə yetirir, siqnallara görə simvollar ardıcıllığını bərpa edir. Əks çevrici simvollar ardıcıllığından məlumatı bərpa (dekodlaşdırma) edir. İnformasiyanı alan - qabaqcadan təyin edilmiş məlumatı alan şəxs yaxud texniki qurğudur.

Bütün TKS informasiyanın mənbəyinə və onların rabitə xəttinə ötürülməsi metodlarına görə iki yerə ayrılır:

- Qapalı TKS - informasiyanın mənbəsi və alıcısi insan, (telefon, teleqraf, lokal və qlobal kompüter şəbəkəsi, radio ilə əlaqə sistemi və s.) olur

- Açıq TKS - İnformasiyanın mənbəyi xarici mühit olur, qəbuledicisi ilə - insandır. Burada, üç növ sistem nəzərdə tutulur:

  1 - elmi - tədqiqat kosmik apparatlar sistemi;

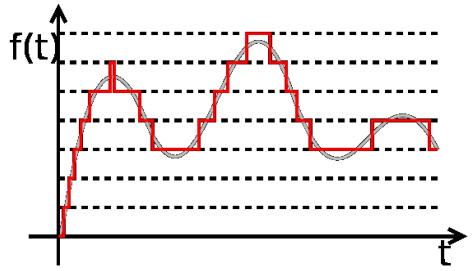
  2 - Texnoloji prosesləri idarəedən sistemlər, telemetrik sistemlər, nəzarət sistemləri;

  3 - video müşahidə sistemləri, kosmik xəritəçəkmə, meteoroloji xidmətlər, yer səthnin qabaqcadan öyrənilməsi və televiziya vasitəsilə şəkilləri uzaq məsafədən qəbul etmə üsulu.

  Zamana görə diskretlənib səviyyələrə görə kvantlaşdırılmamış siqnal diskret siqnal adlanır.

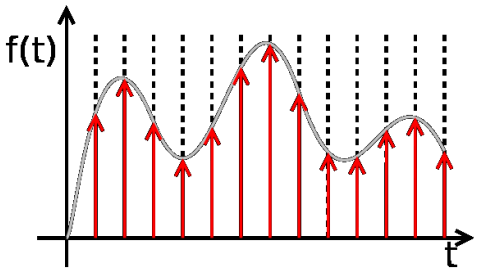
Zamana görə diskretlənib səviyyələrə görə kvantlandırılmış siqnal rəqəmsal siqnal adlanır.

Kvandtlaşdırılmış siqnalın qrafiki şəkil 3.1.2-də verilib.



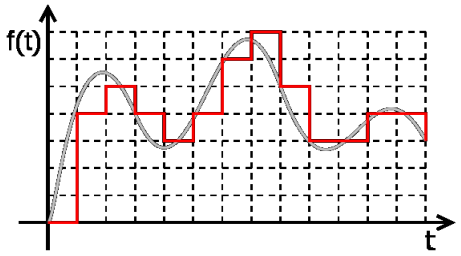
Şəkil 3.1.2 Kvantlaşdırılmış siqnal

Diskret vaxtlı kvantlaşdırılmamış siqnalın qrafiki şəkil 3.1.3-də verilib.



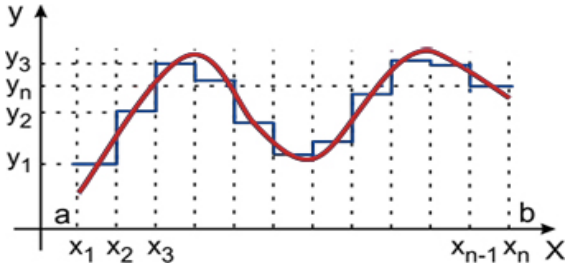
Şəkil 3.1.3 Diskret vaxtlı kvantlaşdırılmamış siqnal

Rəqəmsal siqnalın qrafiki şəkil 3.1.4-də verilib.



Şəkil 3.1.4 Rəqəmsal siqnal

Siqnalın dikretləşdirmə mərhələləri şəkil 3.1.5-də verilib.



Şəkil 3.1.5 Diskretləşdirmə mərhələləri

Aydın olur ki, kvantlaşma prosesi nəticəsində kvantlaşma səhvi yaranır, nəticədə diskret kəmiyyətin həqiqi qiyməti ilə kvantlaşma səviyyəsi üst - üstə düşmür. Kvantlaşma prosesində meydana çıxan səhvlərin yuvarlaqlaşdırılması kvantlaşdırmanın səs-küyü adlandırılır.

3.2 Maneəsiz kanallar üçün şennon teoremi

Kanalın tutumu C , kanaldan ötürülə bilən informasiyanın maksimum həcmi ilə müəyyən edilir.

Keçid matrisi Q ilə səs-küylü kanal üçün kanalın tutumu C , riyazi olaraq aşağıdakı kimi ifadə edilir:

$$C = \max_{p} \sum_{i=0}^{I-1} \sum_{j=0}^{J-1} p_i Q_{j|i} \log \frac{Q_{j|i}}{\sum_i p_i Q_{j|i}}$$

Keçid matrisində

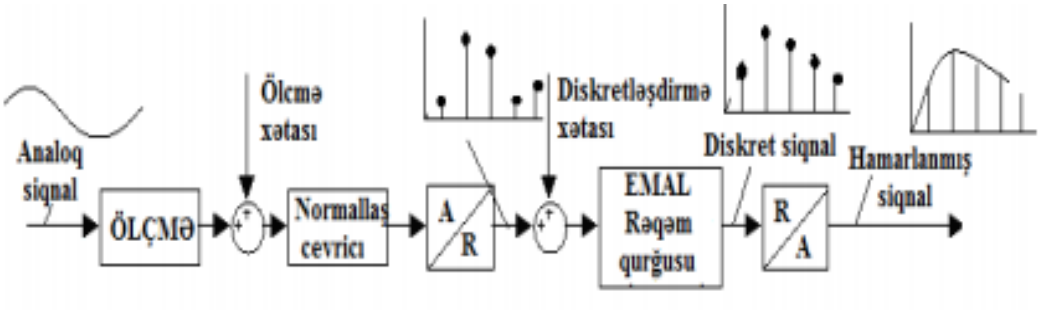
$$\begin{bmatrix} 1-p & p \\ p & 1-p \end{bmatrix}$$

olan ikili simmetrik kanalın tutumu

$$C = 1 + p \log_2 p + (1-p) \log_2 (1-p)$$

düsturu ilə hesablanır.

Rabitə sistemi üçün əsas model aşağıdakı kimidir.



Şəkil 3.2.1 Rabitə kanalı vasitəsilə məlumatın ötürülməsi sxemi

Ötürülmə kanalına daxil olan informasiya kodlaşdırıcı tərəfindən kodlaşdırılmış olur və qəbuledici informasiyanı qəbul edəndə dekodlaşdırıcı tərəfndən kodlaşdırılmış informasiya insanların anlayacağı informasiyaya çevrilir.

Diskret kanaldan informasiyanın maneəsiz ötürülməsi effektiv kodlaşma ilə əlaqədardır. effektiv kodlaşma Şenon teoreminə əsaslanır. İxtiyarı siqnalda həmişə küy olur. lakin onun səviyyəsini elə dəyişmək mümkündür ki, maneəsiz informasiya ötürülsün.

Şennonun birinci teoremi, diskret məlumatın effektiv kodlaşması sisteminin qurulmasına əsaslanıb - bir simvol informasiyaya uygun ikilik simvolların sayının orta qiyməti maneəsiz halda informasiya mənbəyinin informasiya entropiyasina asinptotik yaxınlaşır.

Şennonun birinci teoremi (maneəsiz kodlaşma) - kanalın informasiyanı buraxma qabiliyyəti, buraxma imkanı informasiya mənbəyinin məhsuldarlığından çox olmalıdır.

Şennonun ikinci teoremi, məlumatın etibarsız kanallar üzərindən etibarlı şəkildə ötürülməsi şərtinə əsaslanır.

Siqnal - bir kəmiyyətin digər kəmiyyətdən aslılığıdır. Ryazi nöqteyi - nəzərən siqnal funksiyadır. Fiziki təbiətinə görə siqnallar müxtəlif ola bilər. Əgər xüsusi qeyd edilməsə, biz siqnalı vaxtdan aslı, gərginlik (elektirik siqnalları) kimi başa düşəcəyik.

Siqnallar determinik və təsadüfi ola bilər. Determinik siqnal tam aydındır - onun qiymətini istələn vaxt anında dəqiq müəyyən etmək olar. Təsadüfi siqnal istənilən vaxt anında, özündə təsadüfi kəmiyyəti göstərir, müəyyən ehtimalla konkret qiyməti alır.

Dövri siqnallar. Dövri T olan siqnallar üçün, $s(t+nT) = s(t)$ münasibəti istənilən t üçün ödənilir. Burada, $f = 1/T$ kəmiyyəti siqnalların təkrarlanma tezliyi adlanır. Siqnallar nəzəriyyəsində çox vaxt $\omega = 2\pi F$ dövri tezlik anlayışından istifadə edilir.

Sonlu uzun müddətli siqnallar. Belə siqnallar sonlu vaxt intervalında mövcuddur, yəni sıfırdan fərqli məhdud vaxt intervalında.

Harmonik siqnallar ümumi səkildə aşağıdakı kimi yazılır:

$$s(t) = A\cos(\omega t + \varphi).$$

Harmonik siqnal üç əsas ədədi parametrlərlə tam müəyyən olunur: amplituda A, tezlik ω və faza φ. Harmonik siqnallar zəncirvari xüsusiyyətləri təhlil etmək üçün istifadə olunan, test siqnallarının ən çox yayılmış növlərindən biridir.

Delta-funksiya $\delta(t)$ (Dirakli funksiyası) - funksiyanın sıfır qiymətində ($t = 0$) aldığı, sonsuz amplitudlu, sonsuz ensiz impulusu özündə göstərir. İmpulusun "sahəsi" birdən kiçik deyil.

$$\delta(t) = \begin{cases} 0, & t \neq 0; \\ \infty, & t = 0. \end{cases} \qquad \int_{-\infty}^{\infty} \delta(t)dt = 1.$$

Delta-funksiya şəkilində siqnallı fiziki həyata keçirmək mümkün deyil, lakin siqnalların nəzəri təhlili üçün çox əhəmiyyətlidir. Əgər delta-funksiya vuruq kimi inteqral alındadırsa, onda ineqrallamanın nəticəsi

$$\int_{-\infty}^{\infty} f(t)\delta(t-t_0)dt = f(t_0)$$

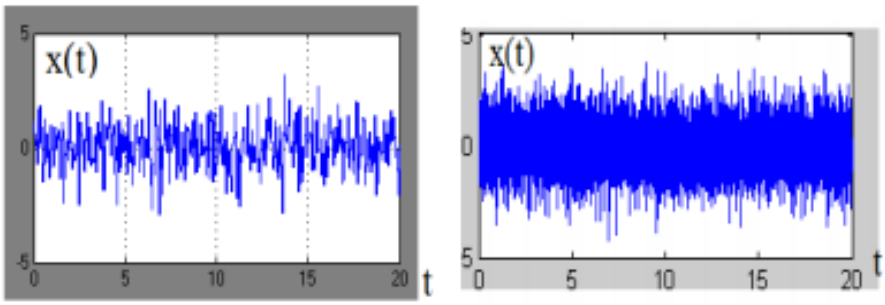
olacaqdır.

Vahid sıçrayış funksiyası (Xevsayd funksiyası) - arqumentin mənfi qiymətində sıfıra bərabərdir, müsbət qiymətləri üçün vahiddir.

$$\sigma(t) = \begin{cases} 0, & t < 0 \\ \frac{1}{2}, & t = 0 \\ 1, & t > 0 \end{cases}$$

Siqma funksiyası σ(t), t=0 qiymətində ya təyin olunmur, ya da 1/2 bərabərdir.

Determent x(t) (və ya x(kT)) siqnalının alacağı qiymət zamanın istənilən gələcək qiymətində məlum olur. Məsələn, x=sin(2t+0,4). t ∈[0,∞). Təsadüfi siqnalın gələcək qiymətləri naməlum olur, ancaq hansısa zaman aralığına düşə biləcək qiymətlərini ehtimal etmək olar.



Şəkil 3.2.2 Təsadüfi siqnal

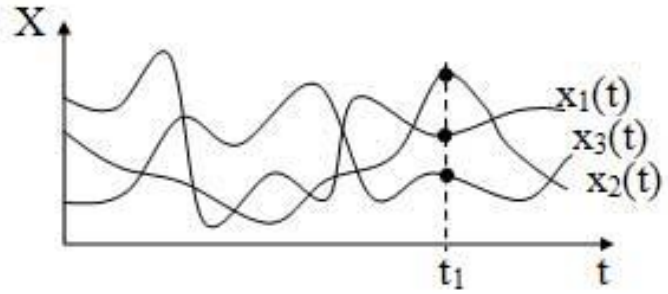
Göstərildiyi kimi, təsadüfi siqnalların ani qiymətləri əvvəlcədən məlum deyil və yalnız vahiddən kiçik ehtimal ilə proqnozlaşdırıla bilər. Belə xarakterli siqnallar, statistik yaxud ehtimallı siqnallar, adlanırlar. Kursun materialları öyrənilən zaman, ehtimal siqnallarının iki əsas sinifi istifadə olunur.

- Birincisi**,** informasiya daşıcısı olan bütün siqnallar təsadüfidirlər. Buna görə də, başa düşülən məlumatlara xas olan qanuna uyğunluqları təsvir etmək üçün ehtimal (statistik) modellərdən istifadə olunur.
- İkinci**,** səs - küy (gurultu) - bəzən müxtəlif fiziki sistemlərdə enerji daşıyıcılarının qaydasız hərəkəti üzündən, elektromaqnit dalğalarının nizamsız dəyişməsi meydana çıxır.

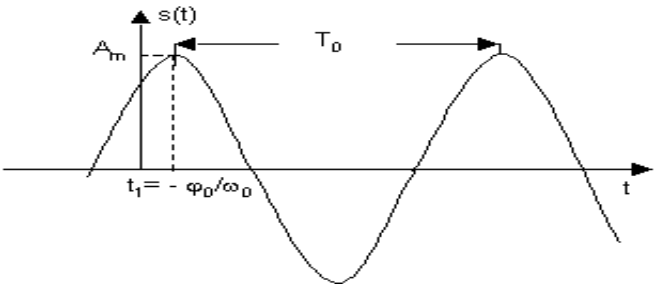
Təsadüfi siqnallara vaxtdan aslı kəsilməz funksiya kimi (analoji siqnallar kimi) baxmaq olar. Məsələn, təsadüfi başlanğıc fazalı, həm də diskret kəmiyyətlər ardıcıllığı olan harmonik siqnallar kimi göstərmək olar. Təbii ki, hər bir halda informasiyanın emal strukturu siqnalın növünə uyğun olmalıdır.

Təsadüfi siqnalların vaxtdan aslı dəyişməsini göstərən riyazi model təsadüfi proses adlanır (22, s. 123).

Tərifə görə, X(t) - istənilən t anında aldığı qiymətlərə görə təsadüfi kəmiyyətləri xarakterizə edən xüsusi növ funksiyadır. Təsadüfi siqnallara qeyd olunana qədər, təsadüfi prosesə ümumi statistik qanunlara tabe olan $\mathbf{x_i(t)}$ funksiyalar çoxluğu kimi baxmaq olar. Belə çoxluq ansambl adlanır. Müşahidələrdən sonra məlum olan ansamblın funksiyalarından biri, təsadüfi prosesin həyata keçirilməsi adlanır. Bu həyata keçmə artıq təsadüfi olmur, vaxta görə determinik funksiya olur. Aşağıdakı Şəkil 3.2.3 – də təsadüfi prosesin həyata keçirilməsi göstərilmişdir. Təsadüfi proseslərin xarakterini və xassələrini, həmçinin onun müxtəlif çevirmələrini təhlil etmək üçün təsadüfi prosesin riyazi modelini vermək lazımdır.



Şəkil. 3.2.3 Təsadüfi proseslər



Şəkil. 3.2.4 Harmonik siqnalların həyata keçirilməsi

Belə bir model təsadüfi prosesin baş verməsinin nisbi tezlik göstəricisi ilə birlikdə mümkün reallaşdırılması təsviri ola bilər. İki misala baxaq.

Təsadüfi fazalı harmonik siqnallar amplitudası və tezliyi məlum (detrminik), lakin fazası təsadüfi olan harmonik rəqsi özündə göstərir: $x(t) = A\cos(\omega t + \varphi)$. Burada A - amplituda (detrminik), ω - tezlik (detrminik) və φ - təsadüfi ilkin fazadır, hansı ki, [0, 2π] bərabər paylandığı hesab olunur. Ehtimalın paylanma sıxlığı belədir:

$$P_\varphi = \frac{1}{2\pi}, 0 \le \varphi < 2\pi$$

Təsadüfi teleqraf siqnalları +1 və -1 qiymətlərini almaqla həyata keçirilən, təsadüfi prosesdirlər, həm də nəzərə almaq lazımdır ki, səviyyə fərqləri təsadüfi vaxt anında baş verir. Müşahidə zamanı baş verən səviyyə fərqlərinin sayı diskret ehtimal paylanmasının ölçüsü olur. Səviyyələrin sıçramaları təsadüfi anda baş verdiyi üçün bunu analtik formada qeyd etmək çox çətindir. Baxmayaraq ki, təsadüfi proseslərin tam təsvirinin reallaşması ansambl verir, çox vaxt daha sadə xarakterli praktiki məsələlərin həlli üçün ədədi parametrlər və determinik funksiyalar göstərilir. Onlardan əsaslarına baxaq.

Funksional və ədədi - ehtimal xarakterli təsadüfi proseslər.

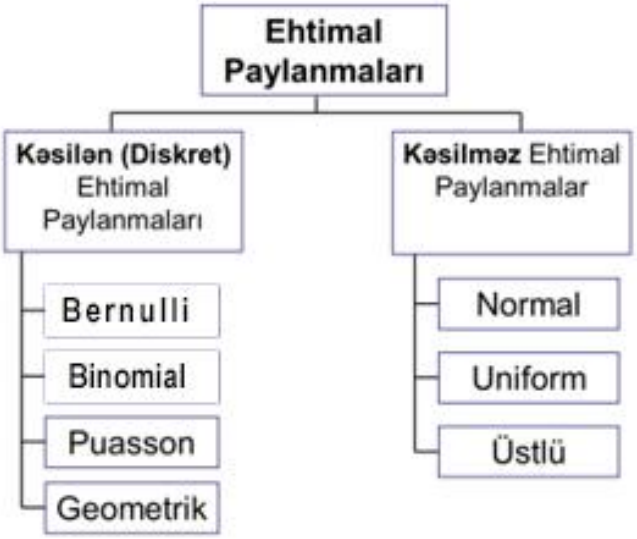
Əgər X(t) təsadüfi prosesi, $x_1(t)$, $x_2(t)$, ..., $x_n(t)$ ansablı şəkilində verilibsə, t_1 anında bütün $x_1(t_1)$, $x_2(t_1)$, ..., $x_n(t_1)$ qiymətlərini alarsa, onda bu qiymətlər çoxluğu təsadüfi prosesin birölçülü kəsiyini əmələ gətirir və özündə $X(t_1)$ təsadüfi kəmiyyəti göstərir. Qeyd edək ki, $X(t_1)$ təsadüfi kəmiyyətinin əsas xarakteri t_1 anının seçilməsindən aslıdır.

Təsadüfi siqnalların mənbəyi daxili və xarici ola bilər. Təsadüfi siqnalların ala biləcəkləri qiymətləri təxmin etmək olmur. Modelləşdirmə zamanı müxtəlif xarakteristikalı təsadüfi siqnalları generasiya etməyə ehtiyac duyulur. Ağ yük siqnalları təsadüfi siqnallarda böyük yer tutur.

Ədədi xarakteristikaları və ehtimalları bərabər olan təsadüfi siqnal üçün düzəltmə funksiyaları fərqli olma ehtimalı var. Təsadüfi siqnalın qrafiki baxaraq xarakteristikaları barədə fikir irəli sürmək asan deyil. Ehtimalların paylanması prinsiplərinə görə təsadüfi siqnalları aşağıdakı qruplara ayırmaq olar:

- bərabər paylanma qanunu.
- normal paylanma (Qaus paylanması).
- eksponensial paylanma
- reley paylanması
- loqorifmik paylanma
- binominal paylanma
- student paylanması

Bu üsulların hər biri geniş istifadə edilmir, ən geniş yayılmış prinsiplər aşağıdakı diaqramda əks olunub:



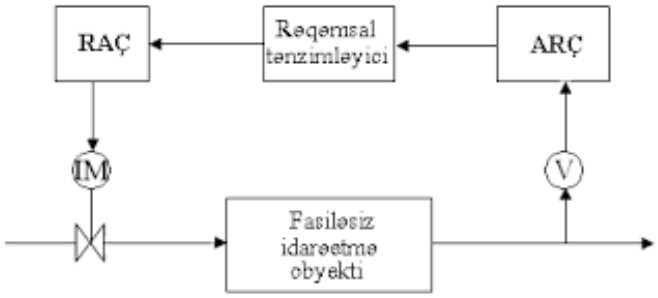
Şəkil. 3.2.5 Ehtimal paylanmalarının növləri

Paylanma funksiyası təsadüfi siqnalın əsas göstəricisi hesab olunur:

$$f(x) = P(X < x)$$

Burada x təsadüfi X kəmiyyətinin konkret qiyməti olub Pehtimal işarəsi adlanır. Məsələn x=20 iymətində f(20)=0.82 olarsa bu o deməkdir ki, təsadüfi kəmiyyətin 20-dən kiçik olma ehtmalı 0.82-yə bərabərdir: P(x<20)=0.82.

Analoq - rəqəm çevricisi (ARÇ) x(t) analoq siqnalını diskret x(tk,qn) rəqəm siqnalına və sonra onu rəqəm koduna çevirmək üçün istifadə edilir.



Şəkil. 3.2.6 Siqnalın çevrilməsi və ötürülməsi

Rəqəm – analoq çeviricisi rəqəmsal məlumatı alır və onu analoq siqnalına çevirir.

RAÇ və ARÇ rəqəmsal inqilaba böyük töhfə verən bir texnologiyadır. Təsəvvür etmək üçün adi bir şəhər telefon danışıqlarına nəzər salmaq kifayətdir. Zəng edənin səsi mikrofon tərəfindən analoq elektrik siqnalına çevrilir , sonra analoq siqnal bir ARÇ tərəfindən rəqəmsal axına çevrilir. Rəqəmsal axın, digər rəqəmsal məlumatlarla birlikdə göndərilə biləcəyi şəbəkə paketlərinə bölünür. Paketlər daha sonra təyinat yerində qəbul edilir, lakin hər bir paket tamamilə fərqli bir marşrut ala bilər və düzgün vaxt qaydasında təyinat nöqtəsinə çatdırıla da bilməz. Rəqəmsal səs məlumatları daha sonra paketlərdən çıxarılır və rəqəmsal məlumat axınına yığılır. RAÇ rəqəmsal siqnalları analoq siqnalına çevirir və bu da öz növbəsində səs çıxaran dinamik sürücüsünü idarə edir.

Şenon teoreminə əsasən kvantlama tezliyi ωk analoq x(t) siqnalının ω(max) maksimal tezliyindən 2 dəfədən böyük olmalıdır ki, analoq siqnallarını tam bərpa etmək mümkün olsun:

$$\omega k > 2\omega max$$

ω=2π/T olduğundan diskretləşdirmə intervalı üçün max Tk < π/ω bərəbarsizliyi ödənməlidir.

Tezliyi verilmiş siqnalın tezliyindən iki dəfə böyük olan kvantlama tezliyinə kaykvist tezliyi deyilir:

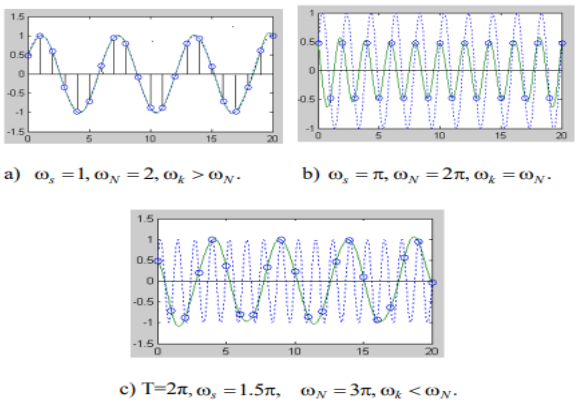
$$\omega = 2\omega max$$

Naykvist tezliyində harmonik siqnalı amplituda, tezliyə və fazaya görə itkisiz bərpa etmək mümkündür. Fasiləsiz siqnalı diskret vəziyyətlə gətirib sonra diskret siqnaldan fasiləsiz siqnalın alınmasının səbəbi ondan ibarətdir ki, ötürücü və qəbul edici arasında emal əməliyyatı edən rəqəmsal qurğu var və bu qurğu emal prosesini diskret rəqəmlərlə yerinə yetirir.

Şəkil 3.2.7 - də Kvantlama və Naykvist tezliklərində asılı olaraq yaranan situasiyalar verilib. Harmonik formalı

$$x=\sin(\omega st)$$

analoq siqnalı qırıq xətlərlə, bərpa edilmiş siqnallar isə bütov xətt ilə göstərilib. Buna görə də kvantlama tezliyi sabit olub ω= 2π/T=2π rad/san bərabərdir.



Şəkil. 3.2.7 Kvant tezliyi ilə Naykvist tezliyi arasında əlaqə

Diskret siqnalların spektri. Diskret hesablamalara görə siqnalların bərpası prosesini başa düşmək üçün diskret siqnalın spektrinə baxaq. Çevrilmələrdən sonra diskret siqnallara ədədlər ardıcıllığı kimi baxılır. Buna görə adi analiz vasitəsi kimi bu ardıcıllığa müəyyən bir funksiya qarşı qoymaq lazımdır. Hesablanmış ardıcıllığı x(k) aşağıdakı şəkildə yazaq:

$$S(t) = \sum_{k=-\infty}^{\infty} x(k)\delta(t-k) \qquad (1.1)$$

Furye çevirməsi xəttidir, spektr delta - funksiya vahidə bərabərdir, vaxta görə siqnalın gecikməsi isə spektrin kompleks eksponentə vurulmasına səbəb olur. Bütün bunlar spektrin diskret siqnallar şəkilində yazımasına imkan verir:

$$S(\omega) = \sum_{k=-\infty}^{\infty} x(k)e^{-j\omega k} \qquad (1.2)$$

Bu formuladan istənilən diskret siqnalın spektrinin əsas xasəsini görmək olar: spektr periodik olur, onun periodu indiki halda 2π bərabərdir ($\omega_D = 2\pi$):

$$S(\omega + 2\pi) = S(\omega)$$

Diskret siqnalların spektr funksiyasının ölçüsünə diqqət edək: o hesablamaların ölçüsü ilə üst - üstə düşür.

3.3 Maneəsi olan kanallar üçün şennon teoremi

Maneəli kanalın buraxıcılıq qabiliyyəti:

$$C_n = n[H(A) - H(A/B)]$$

kimi hesablanır. Burada: n - qəbul edilən işarələrin sayıdır. Bu düsturdan aydınca görünür ki, H(A) və H(B) qiymətləri yüksəldikcə kanalın buraxıcılıq qabiliyyəti də böyük olur. Yuxarıdakı düstura əsasən entropiya ilə kanalın buraxıcılığı arasında əlaqəni görə bilərik. Entropiyanı azaldaraq buraxılıq qabiliyyətini yüksəltmək mümkündür. Maneəli kanal ilə real kanalın buraxıcılıq qabiliyyəti şərti entropiyanın 0 qiymətində ödənir və bu ideal hal adlandırılır:

$$C_n = nH(A)$$

Maneəsi olan kanallar ilə informasiyanın ötürülməsinə nəzər salaq. Xəbərin uzunluğunu, yəni kanaldan istifadə müddətini T ilə işarə edək, vahid zamanda göndərilən simvol sayını isə n ilə işarə edək. Belə olduqda T zamanın müddətində

$$nTH(A)$$

simvol ötürüləcək. 2nTH(A) isə ötürülmə ehtimalı çox olan simvolların sayıdır.

Lakin maneəli kanalda başqa siqnal da alına bilər. Səhvsiz ötürülməni reallaşdırmaq üçün çoxsaylı sınaqlar keçirmək və onların nəticələrini müqayisə etmək lazımdır. Fərz edək ki, ai = 01011 kodu telekommunikasiya kanalı ilə ötürülür. Maneə nəticəsində bu kodun simvollarından biri səhv ötürülsə, qəbuledilən bj xəbəri üçün aşağıdakı kod variantları alına bilər:

$$a_i \} \Longrightarrow \{ b_j$$

01011➔11011
01011➔00001
01011➔01111
01011➔01001
01011➔01010

Nəzəri olaraq iki simvolun eyni zamanda səhv göndərilməsi ehtimalı olsa da, qəbuledicinin bütün simvolları səfv qəbuletməsi ehtimalı demək olar ki, yoxdur.

Beləliklə, siqnalın düzgün ötürülməsi ehtimalı:

$$p = 2^{nT[H(A)-H(A/B)]}$$

kimi hesablanacaqdır.

Bu halda səhvsiz qəbul ehtimalı da:

$$p = (1 - 2^{nT[H(A)-H(A/B)]}) \cdot 2^{nTH(A/B)}$$

kimi hesablanacaqdır. Burada

$$1 - 2^{nT[H(A)-H(A/B)]}$$

səhv qəbul ehtimalıdır.

Beləliklə, uğultulu kanalda kodlaşdırma haqqında Şennon teoremi aşağıdakı kimi ifadə edilir:

Əgər mənbə rabitə kanalının buraxıcılıq qabiliyyətindən kiçik olan sürətlə H(A) entropiyalı informasiya hasil edib, uğultulu kanalın girişinə verirsə, onda qəbul məntəqəsində mümkün qədər kiçik ehtimallı səhvlər əmələ gəlməsini təmin edən kod mövcuddur.

3.4 Maneəyə davamlı kodlar

Ötürmə sistemləri maneəyə davamlılıq, səmərəlilik və etibarlılıq xarakteristikaları ilə xarakterizə edilir. Rabitə xəttlərində maneələr mövcud olduğu vəziyyətdə məlumatı qəbul edə bilməl qabiliyyəti sistemin maneəyə davamlılığı adlanır.

Maneə - sistemə təsir edən və siqnalların düzgün qəbuluna əngəl törədən kənar həyəcanlanmadır.

Təsadüfi maneəyə qarşı tədbir görmək nisbətən daha çətindir. Bu tipli maneələrin 2 növü vardır:

- additiv
- multiplikativ

Siqnalla toplanan maneə additiv maneədir. Additiv maneə siqnal oldu-olmadı mövcud olur. Bunun təsiri siqnalın və maneənin gərginliyi nəzərə alınaraq aşağıdakı kəmiyyətlə xarakterizə edilir.

$$U_o(t) = U_s(t) + U_\xi(t)$$

Multiplikativ maneələr yalnız siqnal ötürülərkən əmələ gəlir. Bunlar siqnalı ya son dərəcə gücləndirir, ya da olduqca zəiflədir. Bunun təsiri aşağıdakı kəmiyyətlə xarakterizə edilir:

$$U_m(t) = \omega \cdot U_s(t)$$

Kommunikasiya kanalının parametrlərinin dəyişməsini ifadə edən parametr “w” ilə göstərilib. Multiplikativ maneələr xarici maneələrə aiddirlər. hesab olunur.

Beləliklə, bərabər güc və şəraitdə A sistemi tərəfindən qəbul edilən siqnal göndərilən siqnala B sistemindəkinə nisbətən daha yaxındırsa, A sistemi B-yə nisbətən maneəyə daha davamlıdır. Statik və dinamik olmaqla iki növ maneəyə davamlılıq vardır.

Əgər telekommunikasiya kanalında informasiya ötürülmürsə və yalançı siqnallar telekommunikasiya kanalına xarici mənbədən daxil edilirsə, bunun qarşısının alınması statik maneəyə davamlılıq adlanır.

Dinamik maneəyə davamlılıq isə yararlı siqnalları uğultulardan ayırmaq qabiliyyəti kimi meydana çıxır. Sistemin maneəyə davamlılığı:

$$H = -(1-p_{so})\log(1-p_{so}) - p_{so}\log p_{so}$$

kimi hesablanır. Burada: p(so) - səhv qəbulun orta ehtimalıdır. Bu dəyər yüksək olduqca statik maneəyə davamlılıq artsa da, ötürmə sürəti azalır və kod optimallığını itirir.

İstənilən maneəyə davamlılıq səviyyəsini təmin etmək üçün kodların mürəkkəbləşdirilməsi səviyyəsini müəyyənləşdirmək üçün ötürmə sisteminin səmərəliliyi anlayışı və prinsipləri tətbiq edilir.

Səmərəli sistem dedikdə eyni xarakteristikalı xəbəri bərabər tezlik zolağında daha tez ötürən sistem nəzərdə tutulur.

Xəbərdəki bolluq azaldıqca, sisteminin səmərəlilik göstəricisi yüksəlir. Ötürmə sürəti ilə buraxıcılıq qabiliyyəti eyni olan halda bolluğun məqsədəuyğun minimal həddi müəyyən olunur. Eyni gücə malik fərqli ehtimalları olan simvollar üçün bolluğu azaltmadan da səmərəliliyi artırmaq olar. Belə olan halda maneəyə davamlılıq artmır.

Ötürmə kanalının istifadə əmsalı

$$\eta = \frac{R}{C}$$

və ötürmə əmsalı

$$\mu = \frac{R}{H}$$

Səmərəliliyi qiymətcə ölçmək üçün istifadə edilir.

Burada

- R – siqnalın ötürülmə sürəti
- C- kanalın buraxıcılıq qabiliyyəti
- H - mənbəyin entropiyasıdır.

Etibarlılıq maneəyə davamlılıq və səmərəlilik ilə birbaşa əlaqəlidir. Səmərəlilik artanda maneəyə davamlılıq azalır. Maneəyə davamlılıq və səmərəlilik dəyərləri eyni vaxtda yüksələndə sistem mürəkkəbləşir və bunun nəticəsində etibarlılıq azalır. Tələb olunan zaman ərzində sistemin imtinasız işləmə qabiliyyəti ötürmə sisteminin etibarlılığını xarakterizə edir. Rabitənin etibarlığı və təhlükəsizliyi ilə ötürmənin etibarlılığı fərqli anlayışlardır. Ötürmənin etibarlılığı dedikdə, aparat təminatının normal işləməsi şərti altında səhvsiz ötürmə ehtimalı nəzərdə tutulur. Maneələr və təhlükələr nəzərə alınaraq məlumatın səhvsiz və təhlükəsiz ötürülməsi rabitənin etibarlılığı anlayışını ifadə edir (30, s. 2 - 3).

Rabitənin etibarlılığı rabitə sistemi, ötürmənin etibarlılığı isə kodlaşdırma və kriptoqrafiya üslubu ilə müəyyən edilir. Aşağıdakı hallarda etibarlılıq səviyyəsi aşağı olur:

- rabitə kanalında kodlaşdırma metodu düzgün seçilmədikdə
- pis layihələşdirildikdə
- elementlər düzgün tətbiq edilmədikdə
- kompleks layihələşdirmə aparılmadıqdə
- ucuz və keyfiyyətsiz materiallardan istifadə edildikdə
- mütəxəssislər qeyri-peşəkar olduqda

Uğultulu diskret rabitə kanalında ötürülən informasiyanın miqdarının hesablanması. Təsəvvür edək ki, p(a1)=p(a2)=0.5. Maneənin olmadığı hallarda alınacaq b1 və b2 siqnalları bərabər ehtimallı olurlar. Alınan siqnallar da eyni ehtimallıdır. Maneə çox olduqca ötürülən siqnalla qəbul edilən siqnal arasında statistik əlaqə zəif olduğundan siqnal və ehtimalda təhriflər yarana bilər. m sayda A siqnalı ötürüb, m sayda B siqnalı gözləyiriksə, maneənin təsiri kanal matrisi ilə təsvir edilməlidir:

$A \setminus B$	b_1	b_2	...	b_j	...	b_m
a_1	$p(b_1/a_1)$	$p(b_2/a_1)$	...	$p(b_j/a_1)$	...	$p(b_m/a_1)$
a_2	$p(b_1/a_2)$	$p(b_2/a_2)$	...	$p(b_j/a_2)$	...	$p(b_m/a_2)$
...	...	...	...	...	...	...
a_i	$p(b_1/a_i)$	$p(b_2/a_i)$	...	$p(b_j/a_i)$	...	$p(b_m/a_i)$
...	...	...	...	...	...	...
a_m	$p(b_1/a_m)$	$p(b_2/a_m)$	...	$p(b_j/a_m)$	...	$p(b_m/a_m)$

Diaqonalda yerləşən ehtimallar düzgün qəbul ehtimalları hesab olunur. Baş dioqanaldan uzaqlaşdıqca kanal matrisindəki ehtimallar kiçilir, maneənin olmadığı halda isə onların hamısı sıfır olur.

Əsas dioqanalda uzaqlaşanda kanal matrisinin ehtimalları kiçilir, maneənin olmadığı halda isə 0-a bərabər olur.

Qəbuledicidə göndərilmiş hər bir siqnala qarşılıq olaraq mütləq bir siqnal (düz və səhv) alınmalıdır. Yaxud da əgər qəbuledici hər hansı bir siqnal qəbul edibsə, belə fərz edilir ki, ötürücü hökmən öz tezaurusundakı siqnallardan birini ötürmüşdür. Beləliklə, maneənin riyazi modeli şərti entropiya düsturlarına əsaslanır.

Maneəli rabitə kanalında informasiyanın ötürülməsi problemləri kodlaşdırma qarşısında əlavə tələblər qoyur. Siqnal səviyyəsinin manea səviyyəsi üzərində müəyyən həddə qədər yüksəldilməsi üçün simolların sayının artırılması və onların ötürülmə vaxtının uzadılması, xəbərin bütövlükdə təkrarlanması, siqnalın gücünün artırılması və s. kimi bu və ya digər bolluq növündən istifadə etmək lazım gəlir ki, bu da aparatların mürəkkəbləşməsinə və bahalaşmasına səbəb olur. Rabitə sisteminin etibarlılığı:

$$Q = (p_{dg} \cdot p_{ap})^{-1}$$

düsturu ilə hesablanır. Burada: p(dg) - siqnalın düzgün qəbulu ehtimalı; p(ap) - aparatların imtinasız iş ehtimalıdır. Nəzəri cəhətdən ixtiyari maneələr səviyyəsində belə siqnalı kifayət qədər düzgün ötürmək olar. Lakin bu zaman qurğuların iqtisadi səmərəliliyi və etibarlılığı mütləq nəzərə alınmalıdır.

Rabitə sisteminin etibarlılığını yüksəltmək üçün hər bir simvolun qəbuledilməsinin etibarlılığını da artırmaq üsulu mövcuddur. Buna nail olmaq üçün, məsələn, siqnalın gücünü artırmaq, siqnalı uzatmaq və xüsusi kodlaşdırma metodundan istifadə edərək bütövlükdə xəbər qəbulunun etibarlılığını yüksəltmək kimi üsullardan istifadə etmək olar. Simvolun ötürülmə müddətinin uzadılması aparatları mürəkkəbləşdirmədən etibarlılığı artırmağa imkan verdiyindən, xeyli böyük marağa səbəb olur.

Qəbuledici-yığıcıda uzadılmış siqnalın seçilməsi (süzülməsi) üçün inteqrator və müqayisə sxemi elə qurulmalıdır ki, T müddətində eyni ehtimallı U1(t) və U2(t) siqnallarının biri ötürülüb, f (t) siqnalı qəbul edilibsə,

$$\int_0^T [U_1(t) - f(t)]^2 dt < \int_0^T [U_2(t) - f(t)]^2 dt$$

şərti ödənməlidir ki, qəbul olunmuş siqnalın məhz U1(t) olduğunu təsdiqləmək mümkün olsun. Qəbul olunmuş siqnal digər siqnallara nisbətən daha uzun olan siqnaldır. İnteqratorun siqnal və uğultunu toplaması nəticəsində siqnalın uğultudan ayrılması problemi ortaya çıxır. Bu prosesi Kotelnikov qəbuledicisinin vasitəsilə həyata keçirirlər. Bu şəraitdə siqnal uzadıldıqca maneənin səviyyəsi 0-a doğru azalır. Bu zaman siqnalın səviyyəsi sabit olmaqla yanaşı həm də sıfırdan fərqli olur. Bu səbəbdən inteqratorda siqnalın səviyyəsi uğultunun azalması nisbətində artır və nəticədə qəbulun etibarlılığı yüksəlir.

İxtiyari kodlar praktiki surətdə aşkarlayıcı kod kimi səhvlərin aşkarlanmasında və düzəldilməsində istifadə edilir. Səhvlərin aşkarlanması üçün müxtəlif metodlar mövcuddur. Belə metoda misal olaraq çoxsaylı təkrarlama üsulunu göstərə bilərik.

Qonşu kod kombinasiyaları arasındakı məsafəyə kod məsafəsi deyilir. Kodun maneəyə davamlılığını xarakterizə edən və kodun bolluğu hesab olunan paramtere kod məsafəsi adlanır. Kodun düzəldilməsi xarakteristikasını da kod məsafəsi müəyyən edir. Əgər kod məsafəsinin qiyməti sıfıra bərabərdirsə, bu halda kodun bolluğu sıfırdır və belə kod aşkarlayıcı kod deyil. Əgər kod məsafəsi iki qiymətini alarsa, belə kod bir səhvi aşkarlaya bilər. Hal-hazırda ixtiyari sayda səhvləri aşkarlayan kodlar istifadə edilir.

Özünü düzəldə bilən və kontrol edən bilən ən məşhur kodlara nümunə olaraq Hemming kodlarını göstərmək olar.

Hemminq kodu, məlumatların göndəricidən qəbulediciyə köçürüldüyü və ya saxlanıldığı zaman meydana çıxan səhvləri aşkar etmək və düzəltmək üçün istifadə edilə bilən səhv düzəltmə kodlarının məcmusudur. Səhvlərin aşkarlanması üçün R.W. Hemminq tərəfindən hazırlanmış bir texnikadır.

Lazımsız bitlər, verilənlərin ötürülməsi zamanı bitlərin itirilməməsini təmin etmək üçün verilənlərin ötürülməsinin məlumat daşıyan bitlərinə əlavə olunan ikili bitlərdir.

Hemminq alqoritmi hər hansı bir informasiyanı kodlaşdırmaya imkan verir və ötürülmə zamanı bu məlumatda bir səhv çıxarsa, onu təyin edir və mümkün olduqda bu informasiyanı bərpa edir.

Əvvəlcə ən sadə bir səhvi düzəldə bilən Xemminq alqoritminə baxaq. Çoxlu səhvləri də tapmaq və düzəltmək bu alqoritmin daha da inkişaf etdirilmiş forması mövcuddur. Xemminq kodu iki hissədən ibarətdir. Simvolları kodlaşdıraraq onlara nəzarətetməni ilk hissə yerinə yetirir. Gələn informasiyanı alaraq nəzarətedici bitləri yenidən hesablayan hissə isə ikinci hissədir. Qəbul edilmiş informasiya o zaman

səhvsiz qəbul edilmiş hesab olunur ki, hesablanmış və qəbul edilmiş bitlər eyni olsun. Alqoritmin işini anlamaq üçün bir misala baxaq. Verilmiş “habr” məlumatının səhvsiz ötürülməsi üsuluna baxaq. İlk olaraq onu Xemminq kodu ilə kodlaşdırmaq lazımdır. Bizə onu ikilik formada təqdim etmək lazımdır.

Simvol	ASCII kodu	İkilik qarşılığı
h	68	01000100
a	61	00111101
b	62	00111110
r	72	01001000

Cədvəl 3.4.1 Simvolun ASCII kodu və ikilik qarşılığı

Birinci mərhələdə sıfır və birlərlə kodlaşdırılan ifadənin uzunluğu tapılır. Tutaq ki, bizim sözün uzunluğu 16 bərabərdir. Beləliklə, "habr" məlumatını onaltı bitlik fərqli kodlar şəklində göstərmək lazımdır. Belə ki, bir ASCII simvoluna yaddaş sahəsində səkkiz bitlik yer ayrılır, onda bir kod sözündə iki ASCII simvolu yerləşəcək.

h	a
01000100	00111101

və

b	r
00111110	01001000

Sonra xəbərin hissələri müstəqil şəkildə kodlaşdırılır. Birinci hissənin necə kodlaşdırıldığına baxaq. İlk növbədə, nəzarətedici bitləri qoymaq lazımdır. Onlar ciddi, müəyyən olunmuş yerlərdə qoyulur. Müəyyən edilmiş yaddaş sahələri dedikdə ikinin qüvvətləri nəzərdə tutulur, bizim nümun bu mövqelərin nömrəsi ikinin vuruqlarına bərabərdir. Onaltı bitlik simvol üçün iki, dörd, altı, səkkiz, onaltı olacaq. Nəticədə beş nəzarətedici bit alındı.

Nəticədə, xəbərin uzunluğu cəmi 5 bit çoxaldı. Nəzarətedici bitlərə hesablanmadan əvvəl "sıfır" qiyməti mənimsədilir.

Nəzarətedici bitlərin hesablanması. Nəzarətedici bitlərin qiyməti informasiyadakı nəzarət etdiyi bitlərinin qiymətindən asılıdır. Aşağıdakı qanunauyğunluğa əsasən nəzarətedici bitin hansı bitlərə cavabdehlik daşıdığını görə bilərik:

N mövqesindən sonrakı N sayda bitə nəzarəti N nömrəsində yerləşən bir edir. Bu deyilənlər aşağıdakı şəkildə əyani olaraq göstərilmişdir.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	
0	0	0	0	1	0	0	0	0	1	0	0	0	0	1	0	1	1	1	0	1	
X		X		X		X		X		X		X		X		X		X		X	1
	X	X			X	X			X	X			X	X			X	X			2
			X	X	X	X					X	X	X	X					X	X	4
							X	X	X	X	X	X	X	X							8
															X	X	X	X	X	X	16

Cədvəl 3.4.2 Nəzarətedici bitlər cədvəli

Nəzarətedici bitlər tərəfindən nəzarət edilən bitlər “X” ilə işarə edilib. Nömrəsi N olan bitə nəzarət edən bitləri tapmaq üçün N nömrəsini ikinin dərəcələrinə ayırırlar. Bundan sonra nəzarətedici bitlərin qiymətini verilmiş üsulla hesablamaq olar: nəzarətedici bitin nəzarət etdiyi bitlərdəki birlərin sayına əsasən tam ədəd əldə edilir. Əldə edilmiş ədədin cüt və ya tək olmasına əsasən ona sıfır və ya bir qiymətləri qoyulur. Ədəd cütdürsü səfər, təkdirsə vahid ilə ifadə olunur. Bu prosesi əksinə də etmək olar. Burada əsas olan kodlaşdırma və dekodlaşdırma metodlarının eyni olmasıdır.

Biz ilk seçimdən istifadə edəcəyik. Biz informasiya sözləri üçün nəzarətedici bitləri hesablayıb aşağıdakıları alırıq:

h	a
100110000100	001011101

və ikinci hissə üçün

b	r
100101101110	010101000

Beləliklə, alqoritmin birinci hissəsi tamamlandı:

h	a
100110000110	001011101

Alqoritmin 2-ci addımındada nəzarətedici bitlər hesablanaraq müqayisə edilməlidir.

h	a
010110010110	001011101

Yekunda isə düzgün olmayan nəzarətedici bitlər ayrılır, onların nömrələri toplanır və səhv bitlərin yerləşdiyi mövqelər tapılır.

Şərh. Kibernetikanın əsas anlayışlarından biri siqnal anlayışıdır. Siqnal müəyyən bir şəkildə kodlanmış məlumatı daşıyır. Siqnal termini informasiyanın emalı və ötürülməsi ilə əlaqədar olaraq, bir çox elmi texniki sahələrdə geniş istifadə olunur.

Müasir baxımdan TKS bir sıra texniki vasitələrdən və onların fəaliyyəti üçün lazım olan alqoritmlərdən ibarətdir. Təyinatına görə məlumatı mənbədən alıcıya ötürülməsi üçün nəzərdə tutulur.

Bütün TKS informasiyanın mənbəyinə və onların rabitə xəttinə ötürülməsi metodlarına görə iki yerə ayrılır:

- Qapalı TKS - informasiyanın mənbəsi və alıcısi insan, (telefon, teleqraf, lokal və qlobal kompüter şəbəkəsi, radio ilə əlaqə sistemi və s.) olur
- Açıq TKS - İnformasiyanın mənbəyi xarici mühit olur, qəbuledicisi ilə - insandır.

Şennonun birinci teoremi, diskret məlumatın effektiv kodlaşması sisteminin qurulmasına əsaslanıb - bir simvol informasiyaya uygun ikilik simvolların sayının orta qiyməti maneəsiz halda informasiya mənbəyinin informasiya entropiyasina asinptotik yaxınlaşır.

Şennonun birinci teoremi (maneəsiz kodlaşma) - kanalın informasiyanı buraxma qabiliyyəti, buraxma imkanı informasiya mənbəyinin məhsuldarlığından çox olmalıdır.

Rabitə xəttlərində maneələr mövcud olduğu vəziyyətdə məlumatı qəbul edə bilməl qabiliyyəti sistemin maneəyə davamlılığı adlanır. Səhvsiz ötürülməni reallaşdırmaq üçün çoxsaylı sınaqlar keçirmək və onların nəticələrini müqayisə etmək lazımdır.

Özünü düzəltmə xassəsinə malik kodlardan ən məşhuru Hemminq kodlarıdır.

Hemminq kodu, məlumatların göndəricidən qəbulediciyə köçürüldüyü və ya saxlanıldığı zaman meydana çıxan səhvləri aşkar etmək və düzəltmək üçün istifadə edilə bilən səhv düzəltmə kodlarının məcmusudur. Səhvlərin aşkarlanması üçün R.W. Hemminq tərəfindən hazırlanmış bir texnikadır.

Nəticə və təkliflər

Dissertasiya işində müasir telekommunikasiya sistemlərinin son nailiyyətləri geniş təhlil edilərək öyrənilmiş və rabitə kanalı ilə ötürülən məlumatların yüksək keyfiyyətlə istifadəçiyə çatdırılması şərtləri əsaslandırılmışdır. Məlum olmuşdur ki, bu zaman informasiyanın yaradılma sürətini, rabitə kanalının iş sürəti ilə razılaşdırmaq lazımdır. Bununla belə, mənbə məlumatlarını bərpa edən zaman keyfiyyət meyarı müəyyən etmək olar və tələb etmək olar ki, göstərilən məlumatlar ardıcıllığının bərpası zamanı buraxılan səhvlər verilən meyara nisbətən kiçik olsun.

İnformasiya texnologiyalarının inkişafı nəticəsində əldə edilən və emal olunan informasiyanın miqdarı yüksək dinamika ilə artır. İnformasiyanın miqdarının artması ilə onun səmərəli istifadəsi problemi ortaya çıxır. Bu problemin əsas hissələrindən biri də telekommunikasiya sistemində (TKS) informasiyanın qənaətlə kodlaşdırılması və səhvsiz ötürülmə məsələsidir. İnformasiya texnologiyalarının və mütəxəssislərin inkişafı nəticəsində mütəmadi olaraq mövcud həllər yeniləri ilə əvəz oluna, daha yaxşı həllər təklif və tətbiq edilə bilər.

TKS-də informasiyanın qənaətlə kodlaşdırılması məsələsinin əsas mahiyyəti mövcud informasiyanın məzmununu saxlamaq şərti ilə onun yaddaş qurğularında tutduğu yeri azaltmaqdır. Bu problemin həlli nəticəsində eyni yaddaş sahəsinə malik yaddaş qurğusunda artıq daha çox informasiya saxlamaq mümkündür. İnformasiyanın yığcamlaşdırılması, onu təmsil etmək üçün lazım olan bit sayının azaldılmasıdır. Müasir yığcamlaşdırma proqram təminatları xüsusi alqoritmlərin köməyi ilə bu prosesi qısa müddət ərzində icra edirlər. Bu proqramlar vasitəsilə yaddaş sahəsinə bir neçə dəfəyə qədər qənaət etmək mümkündür.

İnformasiyanın qənaətlə kodlaşdırılması problemi yaddaşın həcminin azaldılması problemini həll etməklə yanaşı telekommunikasiya kanalı ilə ötürülən məlumatın qəbulediciyə daha tez çatmasını da təmin edir. Çünki informasiyanın bir nöqtədən digər nöqtəyə çatma müddəti şəbəkə göstəricilərindən, telekommunikasiya

kanalının xarakteristikalarından asılı olmaqla yanaşı həm də informasiyanın miqdarından da asılıdır: eyni parametrlərə malik şəbəkədə miqdarı az olan informasiya daha tez qəbulediciyə çatdırılır.

İnformasiyanın ötürülməsi zamanı problemlərdən biri də onun təhlükəsiz şəkildə ötürülməsidir. Bu problemi həll etmək üçün RSA, DES, AES və sairə kimi müxtəlif kriptoqrafik alqoritmlərdən, SSL, TLS kimi şifrələmə sertifikatlarından istifadə edilir. Bu zaman informasiya telekommunikasiya kanalına daxil olmazdan əvvəl şifrələnir və şəbəkə üzərindən ötürülən paketdə informasiya şifrələnmiş halda olur. Paket qəbuledici tərəfindən qəbul olunan zaman təyin edilmiş açar vasitəsilə şifrələnmiş informasiya əvvəlki vəziyyətinə qaytarılır.

Beləliklə, buraxılış işində aşağıdakı nəticələr əldə edilmişdir:

1. İnformasiyanın miqdarının artması ilə onun qənaətlə kodlaşdırılması problemi daha çox ortaya çıxır.
2. İnformasiyanın qənaətlə kodlaşdırılması informasiyanı ifadə etmək üçün tələb olunan bit sayının azaldılmasıdır. Bunun üçün bir çox sıxlaşdırma alqoritmləri və onların əsasında qurulmuş proqram təminatları mövcuddur.
3. Komputer texnologiyasında yığcamlaşdırma itkisiz və itkili ola bilər. Huffman alqoritmi informasiyanın itkisiz yığcamlaşdırılması problemini həll edir.
4. TKS-də informasiyanın ötürülməsi xüsusi şəbəkə protokolları ilə həyata keçirilir.
5. İnformasiyanın ötürülməsi zamanı göndərilən və qəbul edilən informasiya üst-üstə düşdüyü halda informasiya səhvsiz ötürülmüş hesab olunur.
6. TKS-in əsas problemlərində biri də informasiyanın təhlükəsiz ötürülməsidir. İnformasiyanın təhlükəsizliyini təmin etmək üçün xüsusi kriptoqrafik alqoritmlər və şifrələmə sertifikatlarından istifadə edilir.

Telekommunkiasiya sistemində informasiyanın qənaətlə kodlaşdırılması və səhvsiz ötürülmə məsələsi ilə bağlı aşağıdakı təklifləri verə bilərik:

1. Telekommunikaya sistemində informasiyanın qənaətlə kodlaşdırılmasına xüsusi diqqət ayırmaq lazımdı, çünki məlumatın göndərəndən qəbulediciyə çatma müddəti şəbəkə və kommunikasiya kanalının parametrlərindən asılı olmaqla yanaşı, informasiyanın həcmindən də asılıdır. Eyni kommunikasiya kanalında həcmi az olan informasiya data tez ötürülür.
2. İnformasiyanı yığcamlaşdırarkən yığcamlaşdırma alqoritmini diqqətlə nəzərdən keçirmək lazımdır, əks halda informasiyanın təhrif olunma riski vardır.
3. İnformasiya texnologiyalarının inkişafı nəticəsində mövcud metod və proqram təminatlarının optimalaşdırılması, bəzən isə yenidən qurulması zəruri hal alır. Yeni komanda yaradaraq informasiyanın yığcamlaşdırılması üçün yeni alqoritmlərin qurulması və test edilməsini, həmçinin proqram təminatının yaradılmasını həyata keçirmək olar.
4. Telekommunikasiya sistemində informasiyanın səhvsiz ötürülməsi mühüm yer tutur. İnformasiyanın səhvsiz ötürülməsinə nəzarət etmək üçün kommunikasiya kanallarına xüsusi nəzarətedicilərin quraşdırılması zəruridir.
5. Telekommunikasiya sistemində informasiyanın səhvsiz ötürülməsini təmin etmək üçün kommunikasiya kanalının təhlükəsizliyini təmin etmək lazımdır. Bunun üçün xüsusi protokollardan və sertifikatlardan istifadə edilməlidir. Belə protokollara misal olaraq SSL, TLS, PAP və sairə göstərmək olar.

İxtisarlar

AES	Advanced Encryption Standard
ARÇ	Analoq rəqəm çeviricisi
ASCII	American Standard Code for Information Interchange
DES	Data Encryption Standard
IP	Internet Protocol
LAN	Local Area Network
RAÇ	Rəqəmsal analoq çeviricisi
RSA	Rivest-Shamir-Adleman
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TDE	Transparent database encryption
TKS	Telekommunikasiya sistemləri
TLS	Transport Layer Security
PAP	Password Authentification Protocol

Ədəbiyyat siyahısı

1. A. Lapidoth. “The Discrete Noiseless Channel” Georg Bocherer, Master’s Thesis Winter Semester 2006/2007, 102 səh.
2. A.J. Han Vinck (2013). “Entropy properties” University of Duisburg-Essen, 31 səh.
3. Aarti Singh. (2012). Source Coding Theorem, Huffman coding London, 7 səh.
4. Allahverdiyev N., Namazov M. (2012). “Komputer və informasiya-kommunikasiya texnologiyaları. Mühazirələr konspekti” Bakı, 157 səh.
5. Anant Sahai, Salman Avestimehr, Paolo Minero. “Anytime communication over the Gilbert-Eliot channel with noiseless feedback“University of California, 5 səh.
6. Bayramov H.M., Mənsimov H.İ., Məmmədov Ə.S. (2019). “Kompyuter şəbəkəsinin əsasları” Bakı, 143 səh.
7. Chun-Jen Tsai (2014). “Huffman coding” National Chiao Tung University, 31 səh.
8. Dave Mount (2017). “Greedy Algorithms: Huffman Coding” Coordinate Metrology Society Conference, 7 səh.
9. Dea Ayu Rachesti, Tito Waluyo Purboyo, Anggunmeka Luhur Prasasti (2017). “Comparison of Text Data Compression Using Huffman, Shannon-Fano, Run Length Encoding, and Tunstall Methods”, 5 səh.
10. Əhmədov M.A., Məhəmmədli H.M. (2015). “İnformasiya sistemlərinin avtomatlaşdırılmış modelləşdirilməsi və tədqiqi üsulları” Bakı, 137 səh.
11. Əhmədova H.M. (2009). “Ehtimal nəzəriyyəsi və riyazi statistika müntəxəbatı” Bakı, 498 səh.
12. Giambruno l.,Mantaci S. (2014). “State complexities of transducers for bidirectional decoding of prefix codes” University of Palermo, 10 səh.

13. Greg Plaxton (2005). “Compression: Huffman’s Algorithm” University of Texas, 13 səh.
14. Guang Gong (2014). “Communication System Security” Department of Electrical and Computer Engineering University of Waterloo, 268 səh.
15. Guy E. Blelloch (2013), “Introduction to Data Compression” Computer Science Department Carnegie Mellon University, 55 səh.
16. Hüseynov Ə.Ə., Seyidov M.İ., Məmmədov V.M. (2018). “Qraflar nəzəriyyəsi” Bakı, 236 səh.
17. JEFFREY SCOTT VITTER (2014). “Design and Analysis of Dynamic Huffman Codes” Brown University, 21 səh.
18. Jones G.A., Mary Jones J. (2020). “Optimal codes” London, 33 səh.
19. Julie Zelenski (2012). “Huffman Encoding and Data Compression” , 11 səh.
20. Jyrki Kivinen (2012). “Information-Theoretic Modeling” University of Helsinki, 162 səh.
21. Leonardo J. Schulman. “Communication of noisy channels : a coding theorem for computation” Massachusetts Institute of Technology, 10 səh.
22. Man DU, Mordecai GOLIN, Qin ZHANG (2009). “Shannon Coding for the Discrete Noiseless Channel and Related Problems” Barcelona, 139 səh.
23. Musayev İ.K., Əlizadə M. (2014). “İnformatikanın əsasları” Bakı, 228 səh.
24. Nirmal Sharma, Gupta S.K. (2017). “A Huffman algorithm optimal tree approach for data compression and decompression” International Journal of Engineering Applied Sciences and Technology, 7 səh.
25. Peng-Hua Wang (2012). “Data compression” National Taipei University, 41 səh.
26. Qasımov B.M., Musayev İ.K., Bayramov H.M. (2018). “İnformasiyanın işlənməsinin kodlaşdırılması” Bakı, 152 səh.
27. Qəhrəmanzadə A.H., (2004). “Rəqəmli kommutasiya sistemləri və şəbəkələri” Bakı, 338 səh.

28. Robert M. Gray. (2013). “Entropy and Information Theory” Stanford University, 311 səh.
29. Rüstəmov Q.Ə. (2016). “Rəqəmsal tənzimləmə sistemləri. Mühazirələr konspekti” Bakı, 289 səh.
30. Rüstəmov Q.Ə. (2016). “Siqnalların rəqəmli emalı. Mühazirələr konspekti” Bakı, 294 səh.
31. Seminaire Poincare (2018). “A Primer on Shannon’s Entropy and Information” Paris, 35 səh.
32. Stanislav Krajchi, Chin-Fu Liu, Ladislav Mikes (2007). “Performance Analysis of Fano Coding” Signal and Information Processing Lab – Sürix, 5 səh.
33. Tom Carter (2014). “An introduction to information theory and entropy” Complex Systems Summer School, 139 səh.
34. Upamanyu Madhow (2014). “Introduction to Communication Systems” University of California, Santa Barbara, 469 səh.
35. Xəlilov M., Həsənova N. (2014). “İnformatika” Bakı, 424 səh.

Резюме

В наше время телекоммуникационные системы используются во всех областях. Для этого необходимо усовершенствовать принципы телекоммуникаций и использовать новые методы. Основными проблемами телекоммуникационной системы являются экономичное кодирование и безошибочная передача информации. Для решения этих проблем используется ряд методов. Однако, учитывая быстрое развитие информационных технологий, важно оптимизировать эти принципы.

Современные телекоммуникационные системы состоят из аппаратного и программного обеспечения на основе алгоритмов, необходимых для их работы. Цель телекоммуникационной системы - установить связь между источником и приемником, чтобы обеспечить правильную и надежную доставку передаваемой информации к приемнику по телекоммуникационному каналу.

Самая простая телекоммуникационная система состоит из передатчика для приема данных и преобразования его в сигнал, передатчика для передачи сигнала и приемника для приема сигнала.

Процесс передачи информации осуществляется по каналам передачи. Пропускная способность канала передачи определяется количеством информации, проходящей через канал передачи в секунду. Одним из основных нюансов, которые необходимо учитывать при передаче информации, является безопасная и безошибочная передача информации. Для этой цели используются различные криптографические методы. Когда информация передается, информация, поступающая в канал передачи, шифруется по специальному алгоритму, а когда получатель получает информацию, зашифрованная информация восстанавливается с помощью декодера. Клод Шеннон был первым, кто решил проблему безопасной передачи информации. Теория Шеннона отражала принципы надежной передачи информации по ненадежным каналам.

Экономное кодирование информации играет важную роль в телекоммуникационной системе. Экономное кодирование информации гарантирует, что она занимает меньше места в памяти и быстрее передается по каналу связи.

Суть проблемы экономичного кодирования информации в телекоммуникационной системе заключается в уменьшении ее пространства в устройствах памяти при условии сохранения содержания существующей информации. В результате решения этой проблемы можно хранить больше информации на устройстве памяти с той же областью памяти. Консолидация информации - это уменьшение количества битов, необходимых для ее представления.

Процедура сжатия информации называется экономным кодированием Впервые Сэмюэль Морс работал над этой проблемой и в 1837 году предложил новый алгоритм. С появлением теории информации в 40-х годах прошлого века технология экономного кодирования информации получила развитие. Самый популярный и простой способ сжатия информации - заменить повторяющиеся символы уникальными символами небольшой длины. При сжатии информации ее объем можно уменьшить в несколько раз.

Summary

In modern times, telecommunications systems are used in all areas. For this reason, it is necessary to improve the principles of telecommunications and test new methods. The main problems of the telecommunications system are the saving of coding and error-free transmission of information. A number of methods are used to solve these problems. However, given the rapid development of information technology, it is important to optimize these principles.

Modern telecommunication systems consist of hardware and software based on the algorithms required for their operation. The purpose of a telecommunications system is to establish communication between the source and the receiver, to ensure the correct and reliable delivery of transmitted information to the receiver through the telecommunications channel.

The simplest telecommunications system consists of a transmitter to receive data and convert it into a signal, a transmitter to transmit a signal, and a receiver to receive a signal.

The process of information transmission is carried out through transmission channels. The transmission capacity of a transmission channel is determined by the amount of information passing through the transmission channel per second. One of the main nuances to be considered when transmitting information is the safe and error-free transmission of information. Various cryptographic methods are used for this purpose.

When information is transmitted, the information entering the transmission channel is encrypted by a special algorithm, and when the receiver receives the information, the encrypted information is restored with the help of a decoder. Claude Shannon was the first to address the issue of secure information transfer. Shannon's theory reflected the principles of reliable transmission of information over unreliable channels.

Saving of coding of information plays an important role in the telecommunications system. Economical coding of information allows it to take up less space in memory and to be transmitted faster on the communication channel.

The essence of the issue of saving of coding of information in the telecommunications system is to reduce its space in memory devices, provided that the content of existing information is preserved. As a result of solving this problem, it is now possible to store more information on a memory device with the same memory area. Consolidating information is reducing the number of bits needed to represent it.

The procedure for summarizing information is called economical coding. Samuel Morse first worked on this problem in 1837 and proposed a new algorithm. With the emergence of information theory in the 40s of the last century, the technology of economical coding of information has developed. The most popular and simple way to summarize information is to replace repetitive characters with unique characters of small length. When compiling information, its volume can be reduced several times.