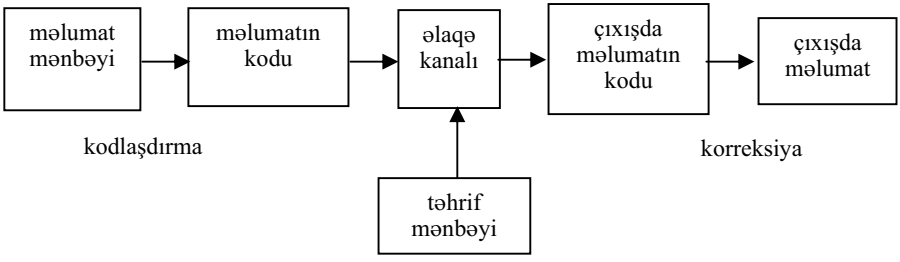
Mənsimov K.B., Feyziyev F.G., Aslanova N.X.

KODLAŞDIRMA NƏZƏRİYYƏSİ



«Bakı Universiteti» Nəşriyyatı

BAKI – 2009

Mənsimov K.B., Feyziyev F.G., Aslanova N.X.

KODLAŞDIRMA NƏZƏRİYYƏSİ

(Dərs vəsaiti)

Azərbaycan Respublikası Təhsil Nazirliyi tərəfindən (10 iyul 2009-cu il tarixli 921 №-li əmr) dərs vəsaiti kimi təsdiq edilmişdir.

«Bakı Universiteti» Nəşriyyatı

BAKI – 2009

UOT 519.7

Elmi redaktor: **AMEA-nın Kibernetika İnstitutunun direktoru, akademik T.A.Əliyev**

Rəy verənlər: **- Bakı Dövlət Universitetinin «İnformasiya texnologiyaları və proqramlaşdırma» kafedrasının dosenti, f.-r.e.n. C.K.Kazımov.**
- Bakı Dövlət Universitetinin «Hesablama riyaziyyatı» kafedrasının dosenti, f.-r.e.n. A.Y.Əliyev.

K.B.Mənsimov, F.G.Feyziyev, N.X.Aslanova. Kodlaşdırma nəzəriyyəsi. Dərs vəsaiti. – Bakı, «Bakı Universiteti» nəşriyyatı,
2009, 226 s.

Dərs vəsaitində kodlaşdırma nəzəriyyəsinin bir sıra məsələləri şərh olunur.

Kitab universitetin mexanika-riyaziyyat, tətbiqi riyaziyyat, informatika ixtisaslarında oxuyan bakalavr və magistrantlar üçün nəzərdə tutulmuşdur və müəlliflərin Bakı Dövlət Universitetində və Sumqayıt Dövlət Universitetində «Diskret riyaziyyat», «Kodlaşdırma nəzəriyyəsi» və s. kimi ümumi fənlər və xüsusi ixtisas fənləri çərçivəsində oxuduqları mühazirələr əsasında yazılmışdır.

Dərs vəsaitindən elmi işçilər, aspirantlar və məlumat ötürmə sistemlərinin qurulması ilə məşğul olan digər mütəxəssislər də istifadə edə bilərlər.

$M\frac{1602020000-0000}{M-658(07)-000}-2009$

MÜNDƏRİCAT

GİRİŞ……...…5
FƏSİL I. KODLAŞDIRMA NƏZƏRİYYƏSİNİN ƏSAS ANLAYIŞLARI. EFFEKTİV KODLAŞDIRMA……...8
§1. Kodlaşdırma nəzəriyyəsi və onun problemləri……..……8
§2. Birqiymətli dekodlaşdırma meyarı……..11
§3. Minimal izafilikli kodlar……..…24
§4. Səhvlərə nəzarətedici kodlar nəzəriyyəsinin əsas anlayışları…37
FƏSİL II. KODLAŞDIRMA NƏZƏRİYYƏSİNİN CƏBRİ ƏSASLARI……..47
§1. Cəbri əməl və cəbri struktur……...……47
§2. Qruppoid, yarımqrup, monoid…….……51
§3. Qrup anlayışı……...53
§4. Halqa……...……60
§5. Meydan anlayışı. Sonlu meydanın növləri……..…66
§6. Tam ədədlər halqası və ona əsaslanan sonlu meydanlar……69
§7. Çoxhədlilər halqası……..…72
§8. Çoxhədlilər halqasına əsaslanan sonlu meydanlar……79
§9. Sonlu meydanın primitiv elementi……..……84
§10. Sonlu meydanın strukturu……88
FƏSİL III. XƏTTİ BLOK KODLARI……...…96
§1. Xətti blok kodlarının strukturu……96
§2. Xətti kodların matris təsviri……97
§3. Standart düzüm qaydası……....102
§4. Xemminq kodları……..105
§5. Mükəmməl və kvazi mükəmməl kodlar……...107
FƏSİL IV. DÖVRİ KODLAR……....…109
§1. Kodlara meydanın genişlənməsi nöqteyi nəzərindən baxılması……...109
§2. Kodların polinomial təsvirləri……...112
§3. Minimal çoxhədlilər və qoşmalar……..…117
§4. Dövrü kodların matris təsvirləri……126
§5. Dövri kodlaşdırmanın realizəsi……129

FƏSİL V. BOUZ-ÇOUDXURİ-XOKVİNQEM KODLARI……..139
§1. BÇX kodlarının təyini……..….139
§2. Piterson-Qorensteyn-Çirler üsulu……..……145
§3. Rid-Solomon kodları…….……155
§4. Berlekemp-Messi alqoritmi……...157
§5. BÇX kodlarının cəld dekodlaşdırılması. Forni alqoritmi……..169
§6. İkilik BÇX kodlarının dekodlaşdırılması……..181
§7. Evklid alqoritminin köməkliyi ilə dekodlaşdırma……....182
Yoxlama tapşırıqları……195
FƏSİL VI. SPEKTRAL ÜSULLARA ƏSASLANAN KODLAR.196
§1. Qalua meydanlarında Furye çevirmələri……...196
§2. Qoşmalığa məhdudiyyətlər və idempotentlər……..199
§3. Dövri kodların spektral yazılışı…….207
§4. Dekodlaşdırmanın spektral üsulları……...216
Cavablar……..….227
Ədəbiyyat……229

GİRİŞ

Kodlaşdırma nəzəriyyəsi bir əlifba üzərində verilən sözləri – simvollar ardıcıllığını (zəncirini) başqa bir əlifba üzərində verilən sözlərə çevrilməsini – inikasını və bu inikasın qarşılılqlı birqiymətli olması, tərs inikasa malik olması, texniki olaraq realizə oluna bilməsi, səhvlərə qarşı davamlı olmasını və s. bu kimi xassələrini öyrənir. Bu nəzəriyyənin böyük tətbiqi əhəmiyyəti mövcuddur, xüsusilə də məlumatların ötürülməsi və saxlanması proseslərində.

Kodlaşdırma prosesi dekodlaşdırma, yəni koda əsasən ilkin sözün tapılması prosesi ilə sıx bağlıdır. Bu bağlılıq kodlaşdırma nəzəriyyəsinin tətbiqində xüsusi əhəmiyyət kəsb edir.

Kodlaşdırma nəzəriyyəsi üç istiqamətə malikdir. Birinci istiqamət məlumtların daha aydın, daha sərfəli kodlaşdırılması, texniki olaraq kodlaşdırmanın daha asan realizə oluna bilməsi, ümumiyyətlə desək, müəyyən bir meyara əsasən daha səmərəli olması ilə bağlı məsələlərlə məşquldur. Bu istiqamət statistik yaxud effektiv kodlaşdırma istiqaməti adlanır.

İkinci istiqamət məlumatların ötürülməsi və məlumat daşıyıcılarında saxlanması prosesində texniki səbəblər və yaxud da subyektiv səbəblər üzündən onların tamlığının pozulması, yəni təhriflərə məruz qalması hallarında ilkin məlumatların bərpa oluna bilməsi məsələlərinin tədqiqi ilə bağlıdır. Bu istiqamət təhrifə davamlı kodlaşdırma istiqaməti adlanır.

Kodlaşdırma nəzəriyyəsində üçüncü istiqamət sözlərin yığcam halda təsvir edilməsi məsələlərini tədqiq edir.

Dərs vəsaiti kodlaşdırma nəzəriyyəsinin ilk iki istiqamətinin bəzi məsələlərinə həsr olunur və beş fəsildən ibarətdir.

Birinci fəsildə kodlaşdırma nəzəriyyəsinin əsas anlayışları şərh olunur. Burada əlifba kodlaşdırması, müntəzəm kodlaşdırma, birqiymətli kodlaşdırma, effektiv kodlaşdırma haqqında əsas məlumatlar verilir. Effektiv kodlaşdırma üsullarından olan Xafman, Fano və Şennon üsulları şərh olunur və onların tətbiqinə nümunələr göstərilir. Bundan başqa, bu fəsildə səhvlərə nəzarətedici kodlar haqqında əsas anlayışlar, sadə kodlaşdırma üsulları, səhvlərə nəzarətedici kodların təsnifatı, belə kodların yaradılması zərurəti, onların qısa inkişaf tarixi, tətbiq sahələri və s. şərh olunur.

İkinci fəsildə kodlaşdırma nəzəriyyəsinin cəbri əsasları şərh olunur. Burada qruppoid, yarımqrup, monoid, qrup, halqa, meydan anlayışları, onların növləri, onlara nümunələr, onların bəzi xassələri verilir. Bu fəsildə ən çox diqqət kodlaşdırma nəzəriyyəsində böyük əhəmiyyətə malik olan sonlu meydanlara yetirilir – sonlu meydanların növləri, tam ədədlər halqasına, çoxhədlilər halqasına əsaslanan sonlu meydanların təyini və bir sıra xassələri, sonlu meydanların primitiv elementləri və strukturları şərh olunur.

Üçüncü fəsildə xətti blok kodlarına baxılır. Burada xətti blok kodlarının təyini, onların matris təsvirləri üçün istifadə olunan əməlgətirici və yoxlayıcı matrislər, kodlaşdırma qaydası, qəbul edilən kodlarda təhrifləri axtarıb tapmaq üçün standart düzüm qaydası şərh olunur. Bu fəsildə nümunə kimi Xemminq kodlarına baxılır. Fəsilin sonunda mükəmməl və kvazimükəmməl kodlar şərh olunur.

Dördüncü fəsil xətti blok kodlarının bir sinfi olan dövri kodlar nəzəriyyəsinə həsr olunur. Burada dövri kodların polinomial və matris təsvirlərinə baxılır, dövri kodların əsas anlayışları şərh olunur. Dövri kodların əməlgətirici çoxhədlilərinin qurulması üsulları, dövri kodların təyin olunduğu sonlu meydanların elementlərinin minimal çoxhədliləri və qoşmaları haqqında ətraflı məlumatlar verilir. Əməlgətirici çoxhədlilərin, minimal çoxhədlilərin və sonlu meydanların qurulmasına nümunələr göstərilir. Bu fəsildə həmçinin dövri kodlaşdırmanın fiziki realizəsi üçün texniki vasitələr haqqında məlumatlar şərh olunur.

Beşinci fəsildə dövri kodların ən geniş yayılmış sinfi olan Bouz, Roy Çoudxuri və Xokvinqem (BÇX) kodları adlanan sinifə baxılır. Əvvəlcə bu kodların təyini və onların qurulması üsulu və belə kodların dekodlaşdırılması üçün olan Piterson-Qorensteyn-Çirler üsulu şərh olunur. Bu fəsildə həmçinin BÇX kodlarının bir sinfi olan Rid-Solomon kodları sinfinə də baxılır. Sonra isə həm ümumi BÇX və həm də Rid-Solomon kodlarının dekodlaşdırılması üçün olan Berlekemp-Messi və Forni alqoritmləri və Evklid alqoritminə əsaslanan dekodlaşdırma üsulu təsvir olunur. Hər bir şərh olunan üsulun tətbiqinə aid nümunələr göstərilir. Bu fəslin sonunda sərbəst yerinə yetirmək üçün tapşırıqlar siyahısı verilir.

Spektral üsullara əsaslanan kodlar və onların dekodlaşdırılmasına altıncı fəsil həsr olunur. Bu fəsildə həmçinin Qalua meydanlarında düz və tərs Furye çevirməsinin təyininə və onun xassələrinə, qoşmalığa

məhdudiyyətlərə və idempotentlərə və s. baxılır və onlara nümunələr verilir.

Cavablar hissəsində V fəsildə təklif olunan tapşırıqların cavabları verilir.

Dərs vəsaitinin əlyazmasını diqqətlə oxuyub və öz qiymətli fikirlərini bildirən f.-r.e.n. S.T.Əliyevaya, f.-r.e.n. J.B.Əhmədovaya, rəyçilər dos. C.K.Kazımova və dos. A.Y.Əliyevə öz təşəkkürlərimizi bildiririk.

Dərs vəsaitinin elmi redaktoru, AMEA-nın Kibernetika İnstitutunun direktoru, akademik T.A.Əliyevə öz dərin minnətdarlığımızı bildiririk.

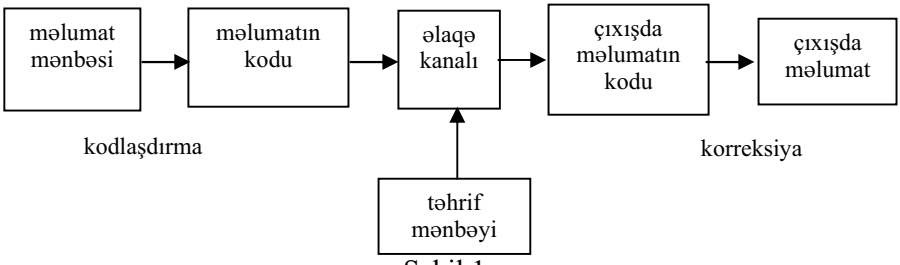
K.B.Mənsimov, F.G.Feyziyev, N.X.Aslanova

FƏSİL I. KODLAŞDIRMA NƏZƏRİYYƏSİNİN ƏSAS ANLAYIŞLARI. EFFEKTİV KODLAŞDIRMA

§ 1. Kodlaşdırma nəzəriyyəsi və onun problemləri

1. Məlumat mənbələri və onların təsvir üsulları. Kodlaşdırma məsələləri riyaziyyatda böyük əhəmiyyətə malikdir. Kodlaşdırma obyektlərin öyrənilməsini digər bir obyektlərin öyrənilməsinə gətirməyə imkan verir. Buna nümunə olaraq ədədlərin onluq say sistemində təsvirini, analitik həndsədə koordinatlar üsulu ilə həndəsi təsvirlərin analitik ifadələrlə təsvirini və s. göstərmək olar. Lakin bu nümunələrdə kodlaşdırma vasitəsi köməkçi vasitədir və o tədqiqat predmeti deyildir. İdarəedici sistemlərlə əlaqədar olaraq kodlaşdırma nisbətən başqa xarakterə malikdir. Bununla əlaqədar olaraq kodlaşdırma nəzəriyyəsində sistematik tədqiqata zərurət yaranmışdır.

Kodlaşdırmanın tətbiq olunduğu ən mühüm sahələrdən biri də rabitə sahəsidir. Burada əsas məsələlər şəkil 1 əsasında izlənilə bilər.



Şəkil 1.

Tutaq ki, sonlu sayda simvollardan-hərflərdən ibarət olan $\mathsf{U} = \{a_1,...,a_r\}$ əlifbası verilmişdir. $A = a_{i_1} a_{i_2} ... a_{i_n}$ şəklində olan sonlu simvollar ardıcıllığı U üzərində söz adlanır, hansı ki, $a_{i_\ell} \in \mathsf{U}$, $\ell = \overline{1,n}$. Tutaq ki, $S(\mathsf{U})$ — U əlifbası üzərində olan bütün sözlər çoxluğudur, S' isə $S(\mathsf{U})$ çoxluğunun hər hansı bir alt çoxluğudur. S' alt çoxluğundan olan sözlərə məlumatlar, S' alt çoxluğundan olan sözləri yaradan (əmələ

gətirən) obyektə isə məlumatların mənbəyi deyilir. Obyekt avtomat, insan və s. ola bilər.

Kodlaşdırma nəzəriyyəsi məsələlərində adətən məlumat mənbələri haqqında əlavə irformasiyalar da istifadə olunur. Bu irformasiyalar məlumat mənbələrinin hər hansı bir qaydada təsviri şəklində olur. Məlumat mənbələrinin aşağıdakı təsvir üsulları mövcuddur:

a) Nəzəri-çoxluq təsvir üsulu. Bu üsul halında güc xarakteristikaları qeyd olunur, məsələn, $S' — m$ uzunluqlu bütün sözlər çoxluğudur və s.;

b) Statistik təsvir üsulu. Bu üsul halında S' çoxluğunun ehtimal xarakteristikaları verilir. Məsələn, $S' = S$ və məlumatlarda $a_1, a_2, ..., a_r$ hərflərinin əmələ gəlməsinin uyğun olaraq $p_1, p_2, ..., p_r$ ehtimalları verilir $(p_1 + p_2 + ... + p_r = 1)$;

c) Məntiqi təsvir. Bu üsul halında S' çoxluğu hər hansı bir «dil» kimi təsvir olunur. Bu «dil» S' çoxluğunun qurulma üsulunu xarakterizə edir. Məsələn, S' hər hansı bir avtomat vasitəsilə yaradıla bilər və s.

2. Kodlaşdırma anlayışı. Tutaq ki, $\mathsf{B} = \{b_1, b_2, ..., b_q\}$ əlifbası verilib. Bu əlifba üzərində olan sözü B ilə işarə edək. Bütün belə sözlər çoxluğunu isə $S(\mathsf{B})$ ilə işarə edək.

Tutaq ki, $S(\mathsf{U})$ çoxluğundan olan hər bir sözü $S(\mathsf{B})$ çoxluğundan olan sözə çevirən F inikası verilmişdir, yəni $B \in S(\mathsf{B})$ və $A \in S(\mathsf{U})$ üçün $B = F(A)$. Bu halda B sözünə A sözünün kodu deyilir, A sözündən onun B koduna keçilməsinə (qurulmasına) isə kodlaşdırma deyilir. Kodlaşdırma nəzəriyyəsində F inikası hər hansı bir alqoritmlə verilir.

Kodlaşdırma nəzəriyyəsində müxtəlif kodlaşdırma üsulları öyrənilir. Bu üsullardan bəzilərinə baxaq.

Əlifba kodlaşdırması. U əlifbasının simvolları (hərfləri) ilə B əlifbası üzərində olan bəzi sözlər arasında aşağıdakı uyğunluğa baxaq:

$$a_1 — B_1,\ a_2 — B_2, ..., a_r — B_r. \qquad (\Sigma)$$

Bu uyğunluq sxem adlanır və Σ ilə işarə olunur. Σ sxemi aşağıdakı qaydada əlifba kodlaşdırması təyin edir: $S'(\mathsf{U})$-dan olan hər bir

$A = a_{i_1} a_{i_2} ... a_{i_n}$ sözünə $B = B_{i_1} B_{i_2} ... B_{i_n}$ sözü qarşı qoyulur və bu söz A sözünün kodu adlandırılır. $B_1, B_2, ..., B_r$ sözləri elementar kodlar adlanır.

Müntəzəm kodlaşdırma. Tutaq ki, $\{A_1, A_2, ..., A_s\}$ çoxluğu U əlifbası üzərində cüt-cüt müxtəlif olan m uzunluqlu sözlərin altçoxluğudur. Aydındır ki, $A = A_{i_1} A_{i_2} ... A_{i_n}$ şəklində ayrılışa malik olan A sözü yeganə ayrılışa malikdir. Tutaq ki, $S'(\mathsf{U})$ çoxluğu U əlifbasından yuxarıdakı şəkildə ayrılışa malik olan sözlərin hər hansı bir altçoxluğudur. Aşağıdakı sxemə baxaq:

$$A_1 — B_1,\ A_2 — B_2, ..., A_s — B_s. \qquad (\Sigma)$$

Σ sxemi müntəzəm kodlaşdırmanı aşağıdakı qaydada həyata keçirir: $S'(\mathsf{U})$-dan olan hər bir $A = A_{i_1} A_{i_2} ... A_{i_n}$ sözünə $B = B_{i_1} B_{i_2} ... B_{i_n}$ sözü qarşı qoyulur və bu A sözünün kodu adlanır.

q-lük kodlaşdırma. $\mathsf{B} = \{0,1,...,q-1\}$ əlifbasına baxaq, harada ki, $q \geq 2$. Tutaq ki, A ixtiyari çoxluqdur. A çoxluğunun q-lük kodlaşdırılması dedikdə bu çoxluğun elementlərinin B əlifbası üzərində olan sözlərə ixtiyari bir inikası başa düşülür. Xüsusi halda, $q = 2$ olduqda belə kodlaşdırmaya nümunə kimi ikilik say sistemində təsvir göstərilə bilər. Məsələn, natural ədədlər aşağıdakı kimi ikilik kodlaşdırılır: 0 – «0», 1 – «1», 2 – «10», 3 – «11» və i.a.

Tutaq ki, $\mathsf{B} = \{0,1\}$ əlifbası (bu əlifba binar əlifba adlanır) üzərində $B = \{\upsilon_i, i = 0,1,...\}$ elementar kodlar çoxluğu verilib. $\mathsf{A} = \{a_i, i = 0,1,...\}$ əlifbasının kodları $a_i - \upsilon_i$ sxemi ilə verilir. Əgər belə əlifba kodlaşdırması halında

$$\upsilon_{i_1} \upsilon_{i_2} ... \upsilon_{i_k} = \upsilon_{j_1} \upsilon_{j_2} ... \upsilon_{j_\ell}$$

bərabərliyindən alınarsa ki, $\ell = k$ və $i_t = j_t$, $t = 1,...,k$, onda $V = \{\upsilon_i, i = 0,1,...\}$ kodları ayrılabilən (bölünəbilən) kodlar adlanır.

Kodlar müxtəlif xüsusiyyətlər əsasında seçilirlər (qurulurlar). Bu xüsusiyyətlərə aşağıdakılar aiddir:

1) Kodların ötürülməsinin asanlığı nöqteyi-nəzərindən. Məsələn, ikilik kodları texniki olaraq asan istifadə etmək olar;

2) Anlaşıqlıq nöqteyi-nəzərindən. Məsələn, maşın kodları prosessorun işi üçün çox əlverişlidir;

3) Rabitə kanalında yüksək ötürmə qabiliyyəti təmin etmək nöqteyi-nəzərindən;

4) Təhriflərə davamlılıq nöqteyi-nəzərindən;

5) Kodlaşdırma alqoritmində müəyyən bir xassələrin əldə edilməsi nöqteyi-nəzərindən (məsələn, kodlaşdırmanın sadəliyi, birqiymətli dekodlaşmanın mümkünlüyü) və s.

4. Rabitə kanalı və məlumatların təhrifi. Rabitə kanalına bir girişdən və bir çıxışdan ibarət olan qurğu kimi baxıla bilər. Kanalın girişinə B kod sözü daxil olur, çıxışda isə B' kod sözü alınır. B' hər hansı bir B' əlifbası üzərində olan sözdür və $B' = f(B)$. İdeal əlaqə kanalı halında $B' = B$ (təhrifsiz kanal halında) və həm də $\mathsf{B}' = \mathsf{B}$ olur.

Təhrif mənbələri rabitə kanalında səhvlər yaradır və bunun da nəticəsində kanalın girişinə daxil olan məlumatla onun çıxışında alınan məlumat arasında fərq yaranır. Bu fərqin əmələ gəlməsi məlumatın təhrif olunması adlanır. Təhrif mənbələrinin təsviri üçün iki üsul istifadə olunur:

a) məntiqi-kombinator təsvir üsulu. Bu üsul ayrı-ayrı təsadüf olunan səhvlərin sayına məhdudiyyətlə bağlıdır;

b) statistik təsvir üsulu. Bu üsul mənbənin ehtimal xarakteristikalarının verilməsi ilə bağlıdır.

4. Məlumatların dekodlaşdırılması. Rabitə kanalında məlumatlar təhrifə məruz qaldıqda $B' \neq B$ olur. Burada B' rabitə kanalının çıxışında olan məlumatdır.

Kanalın çıxışında məlumat kodlarının korreksiyası ancaq xüsusi məlumat kodları halında mümkündür. Korreksiya əməliyyatından sonra dekodlaşdırma baş verir. Aydındır ki, dekodlaşdırma heç də bütün kodlar üçün mümkün deyildir. Əgər F^{-1} əks inikası mövcuddursa onda dekodlaşdırma mümkündür. Ümumiyyətlə, dekodlaşdırma koddan uyğun məlumata keçid prosesidir.

§ 2. Birqiymətli dekodlaşdırma

1. Birqiymətli dekodlaşdırma meyarı. U və B əlifbaları üçün aşağıdakı Σ sxemi ilə verilən əlifba kodlaşdırmasına baxaq:

$$a_1 — B_1,\ a_2 — B_2,\ldots,a_r — B_r\ . \qquad (\Sigma)$$

$S'(\mathsf{U}) = S(\mathsf{U})$ götürək, yəni məlumatlar mənbəsi U əlifbasında olan bütün sözləri yaradır (əmələ gətirir). Aydındır ki, əlifba kodlaşdırması $S(\mathsf{U})$ çoxluğunun $S(\mathsf{B})$ çoxluğuna inikasını əmələ gətirir. $S_\Sigma(\mathsf{B})$ ilə $S(\mathsf{U})$ çoxluğunun bu inikasda obrazını işarə edək.

$S(\mathsf{U})$-nun $S_\Sigma(\mathsf{B})$-yə inikası qarşılıqlı birqiymətli olduğu halda dekodlaşdırma mümkündür, yəni B koduna görə ilkin A məlumatını bərpa etmək olar, harada ki, A məlumatının kodu B sözüdür.

Nümunə 1. Tutaq ki, $\mathsf{U} = \{a_1, a_2\}$, $\mathsf{B} = \{b_1, b_2\}$ və əlifba kodlaşmasının sxemi aşağıdakı kimidir:

$$a_1 — b_1,\ a_2 — b_1 b_2\ .$$

Tutaq ki, B' və B'' sözləri uyğun olaraq A' və A'' sözlərinin kodlarıdır. Aydındır ki, $A' \neq A''$, onda $B' \neq B''$.

Dekodlaşdırma prosesi aşağıdakı kimi aparılır. $B \in S_\Sigma(\mathsf{B})$ sözü elementar kodlara ayrılır. Qeyd edək ki, B sözündə b_2 hərfinin hər bir daxil olmasında b_1 hərfi də iştirak edir. Bu da bütün $(b_1 b_2)$ cütlərinin ayrılmasına imkan yaradır. B sözündə qalan hissələr b_1 hərflərindən ibarət olar. Əgər B sözündə hər bir $(b_1 b_2)$ cütünü a_2 ilə, qalan b_1 hərflərini a_1 ilə əvəz etsək, onda B kodunun proobrazı olan A sözünü alarıq. Tutaq ki, $B = b_1 b_1 b_2 b_1 b_2 b_1 b_1 b_1 b_2$. Cütləri ayırdıqdan sonra alarıq: $B = b_1 (b_1 b_2)(b_1 b_2) b_1 b_1 (b_1 b_2)$. Burada b_1-i a_1 ilə, $(b_1 b_2)$-ni a_2 ilə əvəz etsək $A = a_1 a_2 a_2 a_1 a_1 a_2$ alarıq.

Aydındır ki, əlifba kodlaşdırması ancaq və ancaq o zaman qarşılıqlı birqiymətli olar ki, o, ayrılabilən kodlar vasitəsilə verilsin.

Çoxlu sayda nümunə göstərmək olar ki, əlifba kodlaşması qarşılıqlı birqiymətliliyə malik olmasın. Bununla əlaqədar olaraq belə bir sual ortaya çıxır: əlifba kodlaşdırmasının Σ sxeminə görə onun qarşılıqlı birqiymətlilik xassəsinə malik olmasını müəyyən etmək mümkündürmü. Bu məsələnin həll edilməsinin çətinliyi ondan ibarətdir ki, sonsuz sayda sözləri bilavasitə yoxlamaq lazım gəlir.

Əlifba kodlaşdırmasının qarşılıqlı birqiymətliliyinin ümumi

əlamətini verməzdən əvvəl qarşılıqlı birqiymətlilik üçün sadə bir kafi əlamətə baxaq.

Tərif 1. Tutaq ki, B sözü $B = B'B''$ şəklindədir. Onda B' sözü B sözünün əvvəli və ya prefiksi, B'' sözü isə B sözünün sonu adlanır.

Tərif 2. Əgər istənilən i və j üçün $(1 \le i,\ j \le r,\ i \ne j)$ B_i sözü B_j sözünün başlanğıcı (prefiksi) deyildirsə, onda deyirlər ki, Σ sxemi prefiks xassəsinə malikdir.

Aydındır ki, perefiks kod ayrılabilən koddur (əksi ümumiyyətlə desək, doğru deyildir).

Teorem 1. Əgər Σ sxemi prefiks xassəsinə malikdirsə, onda əlifba kodlaşdırması qarşılıqlı birqiymətli olar.

İsbatı. Əksini fərz edək, yəni fərz edək ki, $S_\Sigma(\mathsf{B})$ -dən olan hər hansı bir B sözü iki proobraza malikdir, deməli, həm də iki elementar kodlara parçalanma mövcuddur:

$$B = B_{i_1} B_{i_2} \ldots B_{i_s}, \qquad B = B_{j_1} B_{j_2} \ldots B_{j_t}.$$

Tutaq ki, $B_{i_1} = B_{j_1}, \ldots, B_{i_{n-1}} = B_{j_{n-1}}$, $B_{i_n} \ne B_{j_n}$. Bu halda B_{i_n} və B_{j_n} sözlərindən biri digərinin prefiksidir. Bu isə Σ sxeminin prefikslik xassəsinə malik olmasına ziddir. Deməli, prefiks xassəsinə malik Σ sxeminin əmələ gətirdiyi əlifba kodlaşdırması qarşılıqlı birqiymətlidir. □

Asanlıqla göstərmək olar ki, prefikslik şərti qarşılıqlı birqiymətli kodlaşdırma üçün zəruri şərt deyildir. Məsələn, nümunə 1-ə baxmaq olar.

Tutaq ki, $B = b_{i_1} \ldots b_{i_n}$ sözü $S(\mathsf{B})$ -dən olan sözdür. $\widetilde{B}$ ilə B sözünün «əks olunması»-nı işarə edək, yəni $\widetilde{B} = b_{i_n} \ldots b_{i_1}$. $\widetilde{\Sigma}$ ilə aşağıdakı kodlaşma sxemini işarə edək.

$$a_1 — \widetilde{B}_1,\ a_2 — \widetilde{B}_2, \ldots, a_r — \widetilde{B}_r. \qquad (\widetilde{\Sigma})$$

Aydındır ki, Σ və $\widetilde{\Sigma}$ sxemləri ilə təyin olunan əlifba kodlaşdırması eyni vaxtda ya qarşılıqlı birqiymətli olar, ya da ki, qarşılıqlı birqiymətli olmaz. Bu fikir də teorem 1-i aşağıdakı kimi gücləndirməyə imkan verir.

Teorem 2. Əgər ya Σ sxemi, ya da $\widetilde{\Sigma}$ sxemi prefiks xassəsinə malik olarsa, onda Σ sxemi ($\widetilde{\Sigma}$ sxemi) ilə verilən əlifba

kodlaşdırması qarşılıqlı birqiymətli olar.

Σ sxeminə malik əlifba kodlaşdırmasına elə nümunə göstərmək olar ki, Σ və $\widetilde{\Sigma}$ prefiks xassəsinə malik olmasın, lakin əlifba kodlaşdırması qarşılıqlı birqiymətli olsun. Bunun üçün aşağıdakı nümunəyə baxaq.

Nümunə 2. Tutaq ki, $\mathsf{U}=\{a_1,a_2,a_3\}$ və $\mathsf{B}=\{b_1,b_2,b_3\}$ əlifbaları verilmişdir. Aşağıdakı Σ kodlaşdırma sxeminə baxaq:

$$a_1 — b_1,\ a_2 — b_1b_2,\ a_3 — b_3b_1. \qquad (\Sigma)$$

Aydındır ki, Σ və $\widetilde{\Sigma}$ sxemləri prefiks xassəsinə malik deyildirlər, lakin əlifba kodlaşdırması qarşılıqlı birqiymətlidir. Həqiqətən də, əgər $B\in S_{\Sigma}(\mathsf{B})$ olarsa, onda bu söz birqiymətli olaraq elementar kodlara parçalanır:

- b_2 hərfindən solda bilavasitə b_1 dayanırsa (b_1b_2) cütünü ayırırıq;
- b_3 hərfindən sağda bilavasitə b_1 dayanırsa (b_3b_1) cütünü ayırırıq;
- bütün (b_1b_2) və (b_3b_1) cütlərini ayırdıqdan sonra ancaq b_1 simvolları qalır.

Bundan sonra hesab edəcəyik ki, Σ sxemində elementar kodlar cüt-cüt müxtəlifdir. Bir sıra işarələmələri daxil edək. $\ell(B)$ ilə B sözünün uzunluğunu, yəni bu sözdə olan simvolların sayını işarə edək. Xüsusi halda, B_i elementar kodunun uzunluğunu $\ell(B_i)=\ell_i$ götürək. L ilə $\ell(B_1\ldots B_r)$ -i işarə edək, yəni Σ sxeminin «uzunluğunu» işarə edək.

$V=\{\upsilon_0,\upsilon_1,\ldots,\upsilon_{m-1}\}$ elementar kodlar çoxluğuna baxaq, hansı ki, $m\geq 2$ və υ_i elementar kodları $\mathsf{B}=\{0,1\}$ əlifbası üzərindədir. υ_i $(i=0,\ldots,m-1)$ kodunun uzunluğunu ℓ_i ilə işarə edək. Tutaq ki,

$$\ell_{\max}=\max_{0\leq i\leq m-1}\ell_i.$$

Teorem 3. Tutaq ki, $\ell_0,\ell_1,\ldots,\ell_{m-1}$ - natural ədədlərin ixtiyari yığımıdır $(m\geq 2)$. $\ell(\upsilon_i)=\ell_i$, $i=\overline{0,m-1}$ uzunluqlu

$V=\{\upsilon_0,\upsilon_1,...,\upsilon_{m-1}\}$ ayrılabilən kodunun mövcud olması üçün zəruri və kafi şərt aşağıdakı bərabərsizliyin ödənməsidir

$$\sum_{i=0}^{m-1} 2^{-\ell_i} \le 1 .$$

İsbatı. Zərurilik. İxtiyari $V=\{\upsilon_0,\upsilon_1,...,\upsilon_{m-1}\}$ kodu üçün

$$h_V(x)=\sum_{i=0}^{m-1} x^{-\ell(\upsilon_i)}$$

funksiyasını daxil edək.

V kodunun n sayda sözündən ixtiyari ardıcıllıqla düzəldilmiş sözlər çoxluğuna baxaq (burada mümkündür ki, sözlər üst-üstə düşsün, məsələn,

$$\underbrace{\upsilon_0\upsilon_0...\upsilon_0}_{n\ \text{söz}},\ \underbrace{\upsilon_0\upsilon_0...\upsilon_1}_{n\ \text{söz}},...,\underbrace{\upsilon_0\upsilon_0...\upsilon_{m-1}}_{n\ \text{söz}},...,\underbrace{\upsilon_{m-1}\upsilon_{m-1}...\upsilon_{m-1}}_{n\ \text{söz}}) .$$

Bu kodlar çoxluğunu $V^{(n)}$ ilə işarə edək. Onda

$$V^{(n)}=\{\omega_i \,|\, i=\overline{0,m^n-1},\ \omega_i=\upsilon_{i_1}\upsilon_{i_2}...\upsilon_{i_n},\ i_1,i_2,...,i_n\in\{0,1,...,m-1\}\ \text{və}$$

$$i=\sum_{j=1}^{n} i_j m^{n-j}\} .$$

$V^{(n)}$ çoxluğunun elementlərinə nümunə olaraq aşağıdakıları göstərmək olar:

$$\omega_0=\upsilon_0\upsilon_0...\upsilon_0,\ \omega_1=\upsilon_0\upsilon_0...\upsilon_1,...$$

$$...,\omega_{m-1}=\upsilon_0\upsilon_0...\upsilon_{m-1},...,\omega_{m^n-1}=\upsilon_{m-1}\upsilon_{m-1}...\upsilon_{m-1}$$

ω_i sözünün uzunluğunu $\lambda(\omega_i)$ ilə işarə edək. Aydındır ki,

$$\lambda(\omega_i)=\ell(\upsilon_{i_1})+\ell(\upsilon_{i_2})+...+\ell(\upsilon_{i_n}) .$$

Asanlıqla göstərmək olar ki,

$$h_{V^{(n)}}(x)=[h_V(x)]^n .$$

İndi fərz edək ki, $V=\{\upsilon_0,\upsilon_1,...,\upsilon_{m-1}\}$ ayrılabilən koddur və $\ell_i=\ell_i(\upsilon_i)$. M_i ilə $V^{(n)}$ kodunda i uzunluğuna malik sözlərin sayını işarə edək. Aydındır ki,

$$h_{V^{(n)}}(2)=\sum_{i=0}^{m^n-1}2^{-\ell(\omega_i)}=\sum_{i=1}^{n\ell_{\max}}M_i2^{-i}$$

(burada $n\ell_{\max}-V^{(n)}$ kodunda ən uzun kodun uzunluğudur).

Kod ayrılabilən olduğundan $V^{(n)}$ kodunun bütün sözləri müxtəlifdir və, beləliklə, 1-dən $n\ell_{\max}$-a qədər bütün i-lər üçün $M_i\le 2^i$ (burada 2^i 0 və 1-dən ibarət i uzunluqlu bütün mümkün yığımların sayıdır). Bunu və son bərabərliyi istifadə etməklə alarıq:

$$\left(\sum_{i=0}^{m-1}2^{-\ell_i}\right)^n=\sum_{i=1}^{n\ell_{\max}}M_i2^{-i}\le\sum_{i=1}^{n\ell_{\max}}1=n\ell_{\max}.$$

Buradan da

$$\sum_{i=0}^{m-1}2^{-\ell_i}\le\sqrt[n]{n\ell_{\max}}.$$

$\lim\limits_{n\to\infty}\sqrt[n]{n\ell_{\max}}=1$ olduğundan alırıq: $\sum\limits_{i=0}^{m-1}2^{-\ell_i}\le 1$.

Kafilik. Tutaq ki, $\ell_0,\ell_1,...,\ell_{m-1}$ - natural ədədlərin ixtiyari yığımıdır $(m\ge 2)$ və

$$\sum_{i=0}^{m-1}2^{-\ell_i}\le 1 \qquad (1)$$

şərtini ödəyir. Göstərək ki, $\ell(\upsilon_i)=\ell_i$, $i=\overline{0,m-1}$ uzunluqlu $V=\{\upsilon_0,\upsilon_1,...,\upsilon_{m-1}\}$ kodu mövcuddur. Ümumiliyi pozmadan fərz edək ki, $\ell_0\le\ell_1\le...\le\ell_{m-1}$. Aşağıdakı $q_0,...,q_{m-1}$ ədədlərinə baxaq: $q_0=0$,

$$q_i=\sum_{j=0}^{i-1}2^{-\ell_j},\ i=\overline{1,m-1}.$$

Aydındır ki, $0\le q_i<1$, belə ki, (1) qüvvədədir. q_i yeganə təsvirə malikdir:

$$q_i=\sum_{j=1}^{\ell_i}c_j^{(i)}2^{-j},$$

hansı ki, $c_j^{(i)} \in \{0,1\}$.

$V = \{\upsilon_0, \upsilon_1, ..., \upsilon_{m-1}\}$ koduna baxaq, hansı ki,

$$\upsilon_i = c_1^{(i)} c_2^{(i)} ... c_{\ell_i}^{(i)}.$$

$h > i$ olduğundan $\ell_h \geq \ell_i$ və $q_h \geq q_i + 2^{-\ell_i}$. Odur ki, kod prefiks koddur və, beləliklə, ayrılabilən koddur. ·

Nümunə 3. $\ell_0 = 2, \ell_1 = 2, \ell_2 = 3, \ell_3 = 4$ uzunluqlu $V = \{\upsilon_0, \upsilon_1, \upsilon_2, \upsilon_3\}$ prefiks kodunu qurmalı.

Aydındır ki,

$$\sum_{i=0}^{3} 2^{-\ell_i} = 1/2^2 + 1/2^2 + 1/2^3 + 1/2^4 =$$
$$= 1/4 + 1/4 + 1/8 + 1/16 = 11/16 < 1.$$

Odur ki, teorem 3-ə görə axtarılan kodu qurmaq olar. Əvvəlcə q_0, q_1, q_2, q_3 ədədlərini tapaq:

$$q_0 = 0,\ q_1 = 1/2^2,\ q_2 = 1/2^2 + 1/2^2 = 1/2,\ q_3 = 1/2 + 1/2^3.$$

Bu halda

$$c_1^{(0)} = 0,\ c_2^{(0)} = 0;\ c_1^{(1)} = 0,\ c_2^{(1)} = 1;\ c_1^{(2)} = 1,\ c_2^{(2)} = 0,\ c_3^{(2)} = 0;$$
$$c_1^{(3)} = 1,\ c_2^{(3)} = 0,\ c_3^{(3)} = 1,\ c_4^{(3)} = 0.$$

Beləliklə, $\upsilon_0 = 00,\ \upsilon_1 = 01,\ \upsilon_2 = 100,\ \upsilon_3 = 1010$.

Deməli, $V = \{00,01,100,1010\}$.

Nəticə 1. İstənilən $V = \{\upsilon_0, \upsilon_1, ..., \upsilon_{m-1}\}$ ayrılabilən kodu üçün bu kodun kod sözlərinin uzunluqları ilə eyni uzunluqlara malik olan kod sözləri yığımından ibarət olan prefiks kod mövcuddur.

(1) bərabərsizliyi ayrılabilən kodlar üçün Kraft-Makmillan bərabərsizliyi adlanır.

Nümunə 4. a) Verilən $V = \{01,10,100,111,011\}$ ayrılabilən kodunun kod sözləri uzunluqları ilə eyni uzunluqlu kod sözləri yığımından ibarət olan prefiks kodu qurmalı.

Aydındır ki, $\ell_0 = 2, \ell_1 = 2, \ell_2 = 3, \ell_3 = 3, \ell_4 = 3$. Kodun ayrılabilən kod olmasını yoxlayaq:

$$2^{-\ell_0} + 2^{-\ell_1} + 2^{-\ell_2} + 2^{-\ell_3} + 2^{-\ell_4} = 1/2 + 3/8 = 7/8 \leq 1.$$

Deməli, kod ayrılabilən koddur. q_0, q_1, q_2, q_3 və q_4 kəmiyyətlərini hesablayaq:

$$q_0 = 0, q_1 = 1/2^2, q_2 = 1/2^2 + 1/2^2 = 1/2,$$

$$q_3 = 1/2 + 1/8,\ q_4 = 1/2 + 1/8 + 1/8 = 1/2 + 1/4.$$

Beləliklə, $\upsilon_0 = 00,\ \upsilon_1 = 01,\ \upsilon_2 = 100,\ \upsilon_3 = 101,\ \upsilon_4 = 110$. Buradan da prefiks kod aşağıdakı kimi olar:

$$V_1 = \{00,01,100,101,110\}$$

b) $V = \{10,101,111,1011\}$ ayrılabilən kodunun kod sözləri uzunluqları ilə eyni uzunluqlu kod sözləri yığımından ibarət olan prefiks kodu qurmalı.

Əvvəlcə verilən kodun ayrılabilən olmasını yoxlayaq.

$$2^{-2} + 2^{-3} + 2^{-3} + 2^{-4} = 1/4 + 1/4 + 1/16 = 9/16 < 1.$$

Deməli, kod ayrılabiləndir. Aydındır ki, $\ell_0 = 2,\ \ell_1 = 3,$ $\ell_2 = 3,\ \ell_3 = 4.$

$$q_0 = 0,\ q_1 = 2^{-2}, q_2 = 2^{-2} + 2^{-3},\ q_3 = 2^{-2} + 2^{-3} + 2^{-3} = 2^{-1}.$$

Buradan da alırıq: $\upsilon_0 = 00, \upsilon_1 = 010,\ \upsilon_2 = 011, \upsilon_3 = 1000$.

Deməli, axtarılan prefiks kod: $V_1 = \{00,010,011,1000\}$ kodudur.

Tutaq ki, $\mathsf{B} = \{0,1\}$ əlifbası üzərində olan bütün sözlər çoxluğu B^* ilə, V üzərində olan bütün sözlər çoxluğu V^* ilə işarə olunub və $\vec{V}^*$ isə V^*-dan olan bütün sözlərin əvvəli olan sözlər çoxluğudur. Əgər $\vec{V}^* = \mathsf{B}^*$ olarsa, onda B əlifbası üzərində olan V koduna tam kod deyilir.

Teorem 4. $V = \{\upsilon_0, \upsilon_1, ..., \upsilon_{m-1}\}$ ayrılabilən kodunun tam kod olması üçün zəruri və kafi şərt onun prefiks kod olması və aşağıdakı şərtin ödənməsidir:

$$\sum_{i=0}^{m-1} 2^{-\ell(\upsilon_i)} = 1.$$

Nümunə 5. $V_1 = \{00,01,100,101,110,111\}$ kodu tam koddur, belə ki,

$$\sum_{i=0}^{5} 2^{-\ell(\upsilon_i)} = 2^{-2} + 2^{-2} + 2^{-3} + 2^{-3} + 2^{-3} + 2^{-3} = 1.$$

$V_2 = \{00,01,100,101,110\}$ kodu tam deyildir. Çünki

$$2^{-2} + 2^{-2} + 2^{-3} + 2^{-3} + 2^{-3} = 1/2 + 3/8 = 7/8 < 1.$$

Tutaq ki,

$$B_i = \beta' B_{i_1} \ldots B_{i_w} \beta''. \qquad (2)$$

B_i kodunun trivial olmayan ayrılışıdır, yəni $B_i = B_i$ ($\beta' = \beta'' = \Lambda$, Λ-boş sözdür – heç bir simvola malik deyildir) ayrılışından fərqli ayrılışdır. Bu ayrılışda hesab olunur ki, aşağıdakılar ödənir:

a) β' elementar kodla qurtara bilməz;

b) β'' başlanğıc (prefiks) kimi elementar kodu özündə saxlamır;

(2)-də w sıfırdan böyük və ya ona bərabər olan tam ədəddir. (2)-nin mənası ondan ibarətdir ki, B_i elementar kodunda hər hansı bir β' başlanğıcını və hər hansı bir β'' sonunu atmaq olar ki, qalan hissə elementar kodlara parçalansın.

Aydındır ki, hər bir B_i üçün (2) şəkilli ayrılış sonludur. Bütün i-lər və B_i-nin bütün ayrılışları halında w ədədləri arasında ən böyüyünü W ilə işarə edək: $W = \max w$.

Nümunə 6. Tutaq ki, $\mathsf{U} = \{a_1, a_2, a_3, a_4, a_5\}$, $\mathsf{B} = \{b_1, b_2, b_3\}$ və Σ kodlaşma sxemi aşağıdakı kimidir:

$$a_1 — b_1 b_2,\ a_2 — b_1 b_3 b_2,\ a_3 — b_2 b_3, \qquad (\Sigma)$$
$$a_4 — b_1 b_2 b_1 b_3,\ a_5 — b_2 b_1 b_2 b_2 b_3.$$

$2 \le \ell_2 < 6$ olduğundan $W < 3$. Digər tərəfdən, $B_5 = b_2 b_1 b_2 b_2 b_3 = b_2 B_1 B_3$, odur ki, $W = 2$.

U əlifbası üzərində olan və uzunluğu N ədədini aşmayan bütün sözlər çoxluğunu $S^N(\mathsf{U})$ ilə işarə edək. Aydındır ki, $S^N(\mathsf{U})$ sonlu çoxluqdur və gücü $r + r^2 + \ldots + r^N$-ə bərabərdir.

Əlifba kodlaşdırmasının qarşılıqlı birqiymətlilik meyarı aşağıdakı kimidir:

Teorem 5. Σ sxemli hər bir əlifba kodlaşdırması üçün elə N_0 ədədi mövcuddur ki, əlifba kodlaşdırmasının qarşılıqlı birqiymətlilik problemi $S^{N_0}(\mathsf{U})$ sonlu çoxluğunun kodlaşdırılmasının analoji probleminə gəlir və

$$N_0 \le \left[(W+1)(L-r+2)/2\right].$$

Burada $[x]$ ilə x ədədinin tam hissəsi, yəni x ədədini aşmayan ən böyük tam ədəd işarə olunmuşdur.

2. Birqiymətli kodlaşdırmanın tanınması alqoritmi. Bu alqoritm qraflar nəzəriyyəsi dilində şərh olunur. Tutaq ki, Σ sxemli kodlaşdırma aşağıdakı kimidir:

$$a_1 - B_1,\ a_2 - B_2, \ldots, a_r - B_r. \qquad (\Sigma)$$

Hər bir B_i elementar kodu üçün

$$B_i = \beta' B_{i_1} \ldots B_{i_\omega} \beta'' \qquad (3)$$

şəklində bütün trivial olmayan təsvirlərə baxaq.

B_0 ilə aşağıdakıları özündə saxlayan çoxluğu işarə edək:

a) Λ boş sözünü;

b) (3) şəklində həm sözönü (prefiks), həm də ki, sözsonu kimi rast gələn β sözünü.

B_0-dan olan hər bir sözə müstəvi üzərində bir nöqtə qarşı qoyaq.

Tutaq ki, $\beta', \beta'' \in \mathsf{B}_0$. Aşağıdakı şəkildə bütün ayrılışlara baxaq:

$$B_i = \beta' B_{i_1} \ldots B_{i_\omega} \beta''.$$

Hər bir belə ayrılış üçün β' və β'' sözlərinə uyğun olan nöqtələri istiqamətlənmiş (β'-dən β''-ə) parça ilə birləşdirək və həmin parçanın üzərinə $B_{i_1} \ldots B_{i_\omega}$ yazaq. Bu qayda ilə alınan qrafı $\Gamma(\Sigma)$ ilə işarə edək.

Teorem 6. Σ sxemli əlifba kodlaşdırmasının qarşılıqlı birqiymətlilik xassəsinə malik olmaması üçün zəruri və kafi şərt $\Gamma(\Sigma)$ qrafının Λ təpəsindən keçən oriyentasiyalı dövrədən ibarət olmasıdır.

Nümunə 7. Tutaq ki, $\mathsf{U} = \{a_1, a_2, a_3, a_4, a_5\}$, $\mathsf{B} = \{b_1, b_2, b_3\}$. Aşağıdakı sxemli əlifba kodlaşdırmasına baxaq.

$a_1 - b_1b_2,\ a_2 - b_1b_3b_2,\ a_3 - b_2b_3,\ a_4 - b_1b_2b_1b_3, a_5 - b_2b_1b_2b_2b_3$. (Σ)

Aydındır ki, aşağıdakı trivial olmayan ayrılışlar mövcuddur:

$$B_1 = (b_1)(b_2);\quad B_2 = (b_1)(b_3b_2) = (b_1b_3)(b_2);\quad B_3 = (b_2)(b_3);$$

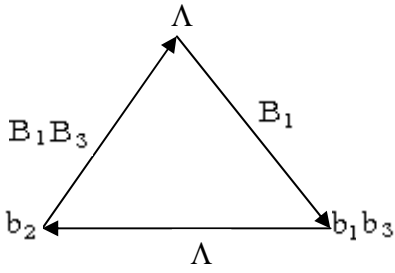
$$B_4 = (b_1)(b_2b_1b_3) = (b_1b_2)(b_1b_3) = (b_1b_2b_1)(b_3);$$

$$B_5 = (b_2)(b_1b_2b_2b_3) = (b_2)(b_1b_2)(b_2b_3) = (b_2b_1)(b_2b_2b_3) =$$
$$= (b_2b_1b_2)(b_2b_3) = (b_2b_1b_2b_2)(b_3).$$

Deməli,

$$B_2 = (b_1b_3)(b_2),\quad B_4 = (b_1b_2)(b_1b_3) = B_1(b_1b_3),$$
$$B_5 = (b_2)(b_1b_2)(b_2b_3) = (b_2)B_1B_3.$$

Buradan da $B_0 = \{\Lambda, b_2, b_1b_3\}$ alınır. Bu çoxluq əsasında qurulan $\Gamma(\Sigma)$ qrafı şəkil 1-dəki kimidir. Göründüyü kimi $\Gamma(\Sigma)$ -da



Şəkil 1.

oriyentasiyalı dövrə olduğundan (Σ) kodlaşma sxemi qarşılıqlı birqiymətli deyildir. Bu dövrə $B = B_1b_1b_3b_2B_1B_3$ sözünü əmələ gətirir və bus söz aşağıdakı iki proobraza malikdir:

$$B = (B_1b_1b_3)(b_2B_1B_3),\ \text{yəni}\ A' = a_4a_5$$

və

$$B = B_1(b_1b_3b_2)B_1B_3,\ \text{yəni}\ A'' = a_1a_2a_1a_3.$$

Nümunə 8. Tutaq ki, $U = \{a_1, a_2, a_3, a_4, a_5\}$, $B = \{b_1, b_2\}$.

Aşağıdakı Σ kodlaşdırma sxeminə baxaq:

$a_1 - b_1,\ a_2 - b_2b_1,\ a_3 - b_1b_2b_2,\ a_4 - b_2b_1b_2b_2,\ a_5 = b_2b_2b_2b_2$. (Σ)

Aşağıdakı trivial olmayan ayrılışlar mövcuddur:

$$B_2 = (b_2)b_1 = b_2B_1,$$

$$B_3 = (b_1)(b_2b_2) = B_1(b_2b_2), \quad B_3 = (b_1b_2)(b_2),$$

$$B_4 = (b_2)(b_1)(b_2b_2) = (b_2)B_1(b_2b_2), \quad B_4 = (b_2)(b_1b_2b_2) = b_2B_3,$$

$$B_4 = (b_2b_1)(b_2b_2) = B_2(b_2b_2), \quad B_4 = (b_2b_1b_2)(b_2),$$

$$B_5 = (b_2)(b_2b_2b_2) = (b_2b_2)(b_2b_2) = (b_2b_2b_2)(b_2).$$

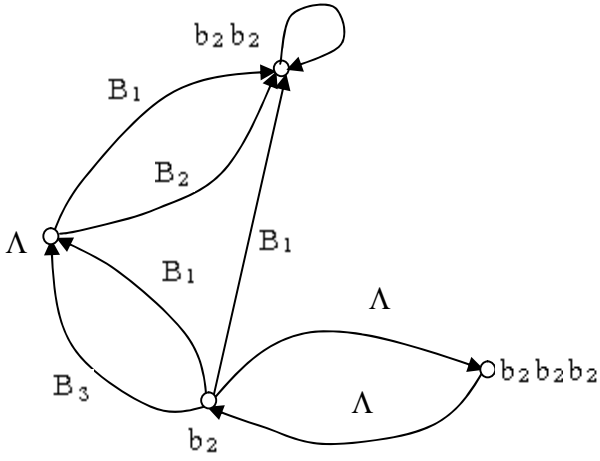
Deməli,

$$B_2 = b_2B_1;\ B_3 = B_1(b_2b_2);$$

$$B_4 = (b_2)B_1(b_2b_2);\ B_4 = b_2B_3;\ B_4 = B_2(b_2b_2);$$

$$B_5 = (b_2)(b_2b_2b_2) = (b_2b_2)(b_2b_2) = (b_2b_2b_2)(b_2).$$

Buradan da, $B_0 = \{\Lambda, b_2, b_2b_2, b_2b_2b_2\}$. Beləliklə, şəkil 2-də təsvir olunan və Λ-dan keçən oriyentasiyalı dövrəyə malik olmayan $\Gamma(\Sigma)$ qrafını alırıq. Odur ki, Σ əlifba kodlaşdırması qarşılıqlı birqiymətlilik xassəsinə malikdir.



Şəkil 2.

3. Qarşılıqlı birqiymətli kodların xassəsi. Tutaq ki, Σ sxemli əlifba kodlaşdırması verilmişdir:

$$a_1 - B_1,\ a_2 - B_2, ..., a_r - B_r .$$

B əlifbasının elementlərinin sayını q ilə işarə edək. Tutaq ki, $\ell_i = \ell(B_i),\ i = \overline{1,r}$.

Teorem 7. (Makmillan bərabərsizliyi). Əgər Σ sxemli əlifba kodlaşdırması qarşılıqlı birqiymətlilik xassəsinə malikdirsə, onda

$$\sum_{i=1}^{r} \frac{1}{q^{\ell_i}} \le 1 .$$

İsbatı. U əlifbası üzərində olan və n uzunluğuna malik bütün mümkün olan sözlərə baxaq. Bütün bu sözlər aşağıdakı ifadənin köməkliyi ilə yaranır:

$$(a_1 + ... + a_r)^n .$$

Burada mötərizə açıldıqdan sonra (vurma yerinə yetdikdən sonra) kommutativlik nəzərə alınmır, hər bir toplanana bir söz kimi baxılır və bu zaman

$$a_{i_1} a_{i_2} ... a_{i_n}$$

hasilinə U əlifbasında sözlərin yazılışı kimi baxılır. Aydındır ki, a_{i_1} simvolu birinci, a_{i_2} simvolu ikinci, ..., a_{i_n} simvolu n-ci mötərizə daxilinə aiddir. Beləliklə, alırıq:

$$(a_1 + ... + a_r)^n = \sum_{(i_1,...,i_n)} a_{i_1} a_{i_2} ... a_{i_n} .$$

Bu sözlərə aid kodlar a_1-i B_1-lə, ..., a_r-i B_r-lə əvəz etməklə alınır. Beləliklə, alırıq:

$$(B_1 + ... + B_r)^n = \sum_{(i_1,i_2,...,i_n)} B_{i_1} B_{i_2} ... B_{i_n} . \qquad (4)$$

Əlifba kodlaşdırmasının qarşılıqlı birqiymətliliyinə görə, əgər $(i_1,...,i_n) \ne (j_1,...,j_n)$, yəni $a_{i_1} ... a_{i_n} \ne a_{j_1} ... a_{j_n}$ olarsa, onda

$$B_{i_1} ... B_{i_n} \ne B_{j_1} ... B_{j_n} .$$

(4) eyniliyi aşağıdakı eyniliyə uyğundur:

$$\left(q^{-\ell_1}+\ldots+q^{-\ell_r}\right)^n=\sum_{(i_1,\ldots,i_n)}q^{-(\ell_{i_1}+\ldots+\ell_{i_n})}. \qquad (5)$$

Aydındır ki, burada sağ tərəfdə eyni bir məxrəcli hədlərə (4)-dən eyni uzunluqlu $B_{i_1}B_{i_2}\ldots B_{i_n}$ sözləri uyğun gəlir.

t ilə $\ell_{i_1}+\ldots+\ell_{i_n}$ cəmini işarə edək. (4)-dən t uzunluğuna malik olan $B_{i_1}B_{i_2}\ldots B_{i_n}$ sözlərinin sayını $\nu(n,t)$ ilə işarə edək. Aydındır ki, verilən söz t uzunluğuna malik söz olmazsa, onda $\nu(n,t)=0$ olar. Tutaq ki, $\ell=\max\limits_{1\le i\le r}\ell_i$. Onda alarıq:

$$\sum_{(i_1,\ldots,i_n)}q^{-(\ell_{i_1}+\ldots+\ell_{i_n})}=\sum_{t=1}^{n\ell}\nu(n,t)\cdot q^{-t}.$$

Əlifba kodlaşdırmasının qarşılıqlı birqiymətliliyinə görə alınır ki, $\nu(n,t)\le q^t$ və, beləliklə,

$$\sum_{t=1}^{n\ell}\nu(n,t)\cdot q^{-t}\le n\ell.$$

Bu bərabərsizliyi (3) bərabərsizliyi ilə birləşdirsək, alarıq:

$$\sum_{i=1}^{r}q^{-\ell_i}\le\sqrt[n]{n\ell}.$$

Bu bərabərsizlik bütün n-lər üçün doğrudur. Sol tərəf n-dən asılı deyildir. Ona görə də $n\to\infty$ olmaqla bərabərsizliyin hər tərəfində limitə keçsək alarıq:

$$\sum_{i=1}^{r}\frac{1}{q^{\ell_i}}\le 1,$$

belə ki, $\lim\limits_{n\to\infty}\sqrt[n]{n\ell}=1$.

§3. Minimal izafilikli kodlar

Tutaq ki, $U=\{a_1,\ldots,a_r\}\ (r\ge 2)$ əlifbası və $p_1,p_2,\ldots,p_r$ ehtimallar yığımı verilmişdir, belə ki, $p_i\ (i=\overline{1,n})$ ehtimalı a_i

simvolunun əmələ gəlməsi ehtimalıdır və $p_1 + p_2 + ... + p_r = 1$. Tutaq ki, həm də $B = \{b_1, ..., b_q\}$ əlifbası da verilmişdir $(q \geq 2)$. Onda çoxlu sayda Σ əlifba kodlaşdırması qurmaq olar

$$a_1 - B_1,\ a_2 - B_2, ..., a_r - B_r, \qquad (\Sigma)$$

harada ki, bu sxemlər hamısı qarşılıqlı birqiymətli olar. Xüsusi halda elementar $B_1, B_2, ..., B_r$ kodlarını eyni bir ℓ uzunluğunda götürmək olar, harada ki, $\ell =]\log_q r[$. Burada $]x[$ ilə x ədədindən kiçik olmayan ən kiçik tam ədəd işarə olunmuşdur.

Hər bir Σ sxemi üçün kodlaşdırma izafiliyi adlanan və elementar kodların uzunluqlarının riyazi gözləməsi kimi təyin olunan ℓ_{ort} kəmiyyəti daxil etmək olar:

$$\ell_{ort} = \sum_{i=1}^{r} p_i \ell_i, \quad \ell_i = \ell(B_i).$$

Aydındır ki, ℓ_{ort} Σ sxemi ilə kodlaşdırma zamanı sözlərin uzunluğunun neçə dəfə artmasını göstərir.

ℓ_{ort} kəmiyyəti $V = \{B_1, ..., B_r\}$ kodunun dəyəri kimi də adlandırılır və $L_V(P)$ kimi də işarə olunur, belə ki, $P = \{p_1, ..., p_r\}$ -dir.

Nümunə 1. Tutaq ki, $r = 5, q = 2$ və $p_1 = 0{,}20$, $p_2 = 0{,}20$, $p_3 = 0{,}25$, $p_4 = 0{,}20$, $p_5 = 0{,}15$.

Tutaq ki, Σ kodlaşdırma sxemi aşağıdakı kimidir.

$$a_1 - 000,\ a_2 - 111,\ a_3 - 01,\ a_4 - 1,\ a_5 - 001.$$

Bu kod qarşılıqlı birqiymətlilik xassəsinə malikdir. Kodun izafiliyini hesablayaq:

$$\ell_{ort} = 3 \cdot 0{,}20 + 3 \cdot 0{,}20 + 2 \cdot 0{,}25 + 1 \cdot 0{,}20 + 3 \cdot 0{,}15 = 2{,}35.$$

Aydındır ki, izafilik kəmiyyəti bir kodlaşdırma sxemindən başqa bir sxemə keçdikdə dəyişir. Ona görə də hər bir məlumatlar mənbəyi üçün ℓ_* kəmiyyətini daxil etmək olar və bu kəmiyyət

$$\ell_* = \inf_{\Sigma} \ell_{ort}^{\Sigma}$$

düsturu ilə təyin olunur. Burada infimum qarşılıqlı birqiymətlilik xassəsinə malik bütün mümkün Σ kodlaşdırma sxemləri üzrə götürülür. Aydındır ki,

$$1 \le \ell_* \le]\log_q r[.$$

Bu düstur onu göstərir ki, ℓ_* kəmiyyətinə yaxın olan ℓ_{ort} izafilikli kodları qurduqda $]\log_q r[$ kəmiyyətindən böyük olan izafiliyə malik kodları nəzərə almamaq olar. Deməli, belə sxemlər üçün

$$p_i \ell_i \le]\log_q r[.$$

ℓ_{ort} hesablandıqda $p = 0$-a uyğun hədlər nəzərə alınmadığından $p_* = \min\limits_{i:p_i \neq 0} p_i$ qəbul etməklə alarıq ki, istənilən i üçün

$$\ell_i \le \frac{]\log_q r[}{p_*},$$

harada ki, $p_i \neq 0$. Deməli, $\ell_* \le \ell_{ort} \le]\log_q r[.$

Tərif 1. Σ sxemi ilə təyin olunan və $\ell_{ort} = \ell_*$ şərtini ödəyən kod minimal izafilikli kod və ya Xafman kodu adlanır.

Qarşılıqlı birqiymətli əlifba kodlaşdırması haqqında teoremlərə görə minimal izafilik verən və prefiks xassəsinə malik olan əlifba kodlaşdırması mövcuddur. Ona görə də minimal izafilikli kodları tapmaq üçün prefiks xassəsinə malik kodlara baxmaq kifayətdir.

Minimal izafilikli kodların qurulması məsələlərinə baxaq. Hər bir prefiks xassəli əlifba kodlaşdırmasına kod ağacı qarşı qoymaq olar. Buna aşağıdakı nümunə halında baxaq.

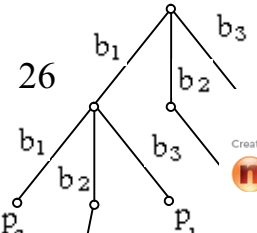
Nümunə 2. Tutaq ki, $\mathsf{U} = \{a_1, a_2, a_3, a_4, a_5, a_6\}$, $\mathsf{B} = \{b_1, b_2, b_3\}$.

$$a_1 - b_1 b_3 \ , \quad p_1 = 0{,}22 ,$$
$$a_2 - b_3 \ , \quad p_2 = 0{,}20 ,$$
$$a_3 - b_1 b_1 \ , \quad p_3 = 0{,}14 ,$$
$$a_4 - b_2 b_1 \ , \quad p_4 = 0{,}11 ,$$
$$a_5 - b_1 b_2 b_3 \ , \quad p_5 = 0{,}33 .$$

Bu kod prefiks xassəsinə malikdir və orta izafiliyi aşağıdakı kimidir

$$\ell_{ort} = 2 \cdot 0{,}22 + 1 \cdot 0{,}20 + 2 \cdot 0{,}14 + 2 \cdot 0{,}11 + 3 \cdot 0{,}33 = 2{,}13 .$$

Elementar kodlar şəkil 1-də verilən kod ağacını əmələ gətirir.



Şəkil 1.

Kod ağacında son təpə nöqtələri ağacın kökündən başlayan yolun (budağın) təyin etdiyi elementar koda uyğun gəlir və bu təpələrə elementar kodun əmələ gəlməsi ehtimalı yazılır. Asanlıqla görmək olar ki, son təpələrinə ehtimallar yazılan kod ağacı prefiks xassəinə malik əlifba kodlaşdırması verir.

Ümumiliyi pozmadan fərz edək ki,

$$p_1 \geq p_2 \geq \ldots \geq p_r .$$

Lemma 1. Minimal izafilikli kodlar üçün $p_j < p_i$ şərtindən alınır ki, $\ell_j > \ell_i$.

Nəticə 1. Minimal izafilikli kodlar üçün kod ağacında ℓ' yarusunda son təpədə yazılan ehtimal qiymətləri $\ell'' > \ell'$ şərtini ödəyən ℓ'' yarusunda son təpədə yazılan ehtimal qiymətlərindən kiçik deyildir.

Kod ağaclarında təpələrdən çıxan tillərin sayı həmin təpənin uyğun olaraq budaqlanma dərəcəsi adlanır.

Tərif 2. Əgər sonlu ağacda bütün təpələrin (ola bilsin ki, sondan əvvəlki yarusda olan bir təpə istisna olmaqla) budaqlanma dərəcələri 0 və ya q -yə (istisna olunan təpədə budaqlanma dərəcəsi isə q_0 -a bərabərdir, harada ki, $2 \leq q_0 < q$) bərabər olarsa, onda belə ağac ifrat ağac adlanır.

Asanlıqla görmək olar ki, q_0 ədədi

$$r = t(q-1) + q_0$$

münasibətindən təyin olunur. r ədədini $(q-1)$ -ə bölərək qalığı tapaq (əgər istisna olunan təpə olarsa, onda qalıq 1-ə bərabər olmaz):

$$q_0 = \begin{cases} q-1, & \text{əgər qalıq } 0-\text{a bərabərdirsə,} \\ \text{qalığa,} & \text{əgər qalıq} \geq 2 \text{ isə.} \end{cases} \qquad (1)$$

Lemma 2. (1) məhdudiyyəti daxilində kod ağacı ifrat olan minimal izafilikli kod mövcuddur.

İsbatı. İsbat üçün yuxarıda göstərilən tipli kod ağacı üzərində iki çevirməyə baxaq, harada ki, bu çevirmələr izafiliyi artırmır.

1. Sonuncu yarusda tilin ləğvi. Əgər sonuncu yarusda kod ağacında düz bir til mövcuddursa, onda bu tillə $B = B'b$ elementar kodu p ehtimalı ilə bağlıdır, həm də B' heç bir başqa elementar kodun prefiksi deyildir. Bu tili ləğv etməklə və p ehtimalını tilin çıxdığı təpəyə gətirməklə yeni kod ağacı alarıq. Bu çevirmədən Σ sxemindən Σ' sxeminə keçid alınır, belə ki, Σ sxemində B kodu B' kodu ilə əvəz olunur. Aydındır ki,

$$\ell'_{ort} = \ell_{ort} - p \le \ell_{ort}.$$

2. Kod ağacının sonuncu yarusundan tilin ifrat olmayan ağacın tilinə köçürülməsi. Tutaq ki, kod ağacında sonuncu yarusda ən azı iki til mövcuddur. Deməli, son təpəsinə p ehtimalının yazıldığı til və hər hansı bir elementar B kodu mövcuddur. Tutaq ki, ℓ' yarusunda $(\ell' \le \ell - 1)$ təpə mövcuddur və ifrat deyildir. B^0 ilə bu təpəyə uyğun sözü işarə edək. Təpənin ifrat olmadığı üçün $B^0 b_j$-nin heç bir elementar kodun prefiksi olmadığı b_j simvolu mövcuddur. Bu halda sonuncu yarusun adı çəkilən tilini verilən ifrat olmayan təpənin j-ci istiqamətinə köçürmək olar. Beləliklə, B elementar kodunu $B^0 b_j$ koduna dəyişməklə Σ sxemindən Σ' sxemini alırıq və bu zaman

$$\ell_{ort} = \ell_{ort} - p\ell + p(\ell(B^0) + 1) \le \ell_{ort}.$$

1 və 2 çevirmələri baxılan sinifdən istənilən prefiks kodu, o cümlədən minimal izafilikli kodu, izafiliyi dəyişmədən ağacı ifrat olan koda çevirməyə imkan verir. □

Qeyd. Kod ağacı ifrat olan minimal izafilikli koda baxaq. İstisna olunan təpədən çıxan və sonuncu yarusda olan tillər dəstəsini götürək. Əgər belə təpə yoxdursa, onda sonuncu yarusdan istənilən tillər dəstəsini götürək. Tutaq ki, götürülən dəstədə tillərin sayı q_0-dır, $2 \le q_0 \le q$. Maksimal uzunluqlu elementar kodların yerdəyişməsi ilə götürülən dəstənin son təpələrində aşağıdakı ehtimal qiymətlərinin yazılmasına nail olmaq olar

$$p_{r-q_0+1},\ldots,p_r.$$

Alınan kodu gətirilən kod adlandıracağıq. Aydındır ki, gətirilmiş kod üçün $p_{r-q_0+1},\ldots,p_r$ ehtimalları birqiymətli təyin olunurlar, belə ki, onlar tənlikdən birqiymətli olaraq tapılan q_0 parametri ilə verilir. Məsələn, $r=8,\ q=4$ olduqda

$$8=3t+q_0$$

tənliyindən $t=q_0=2$ alırıq. Bu zaman ayrılan dəstəyə p_7 və p_8 ehtimalları yazılır.

Teorem 1 (reduksiya). Tutaq ki, (r,q) parametrli və $p_1,\ldots,p_r$ ehtimallı minimal izafilikli prefiks kod verilmişdir. Uyğun kod ağacında ancaq son təpələrə aparan və $2\le q_0\le q$ bərabərsizliyini ödəyən q_0 sayda tillərin çıxdığı təpələrə baxaq. $p_{i_1},\ldots,p_{i_{q_0}}$ $(p_{i_1}\ge\ldots\ge p_{i_{q_0}})$ ilə verilən tillər dəstəsinin son təpələrinə yazılan ehtimalları işarə edək. Əgər $r>q$ isə, onda verilən tillər dəstəsini ləğv etməklə və onların çıxdığı təpəyə $p=p_{i_1}+\ldots+p_{i_{q_0}}$ ehtimalını yazmaqla (r',q) parametrli

$$p_1,\ldots,p_{i_1-1},p_{i_1+1},\ldots,p_{i_{q_0}-1},p_{i_{q_0}+1},\ldots,p_r,p \qquad (1)$$

ehtimallı minimal izafilikli koda uyğun kod ağacı alarıq, harada ki, $r'=r-q_0+1$ $(i_1=1$ və ya $i_{q_0}=r$ olduqda (1) ardıcıllığı p_{i_1+1} ilə başlayır və ya $p_{i_{q_0}-1}$ ilə qurtarır).

Teorem 1 lemma 1-lə birlikdə minimal izafilikli kodların qurulması üçün alqoritm verir. Alqoritm teorem 1-in (r,q) parametrli və $p_1,\ldots,p_r$ $(p_1\ge\ldots\ge p_r)$ ehtimallarlı gətirilmiş koda tətbiqinə əsaslanır. Tillər dəstəsi olaraq q_0 sayda tildən ibarət $(2\le q_0\le q)$ tillər dəstəsi götürülür. q_0 parametri birqiymətli olaraq ilkin verilənlər əsasında təyin olunur. Dəstənin son təpələrinə yazılan

$$p_{r-q_0+1},\ldots,p_r$$

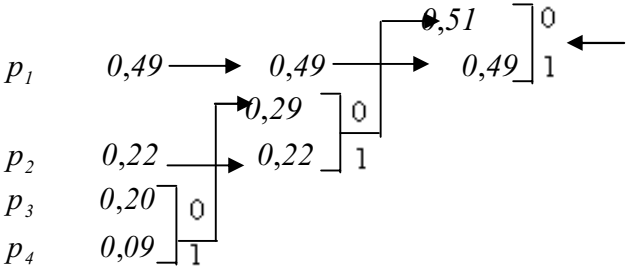
ehtimalları da həmçinin ilkin verilənlər əsasında birqiymətli təyin olunurlar, bu da ki, $r>q$ olduqda reduksiya vasitəsilə alınan kodun parametrlərini

tapmağa imkan verir. Biz $r' = r - q + 1 < r,\ q' = q$ və $p_1,...,p_{r-q_0},p$ ehtimallarını alırıq, harada ki, $p = p_{r-q_0+1} + ... + p_r$.

Beləliklə, reduksiyanın çoxsaylı tətbiqi nəticəsində $r \le q$ olduğu məsələ alınır və əgər elementar kodlar üçün birsimvollu elementar kodlar götürülərsə onda bu məsələ trivial həllə malikdir.

Nümunə 3. 1) Tutaq ki, $r = 4, q = 2$ və $p_1 = 0,49,\ p_2 = 0,22,$ $p_3 = 0,20,\ \ p_4 = 0,09$. Optimal kodu qurmalı.

Qurma prosesini aşağıdakı kimi təsvir etmək olar:



Reduksiya ilə bağlı üç addıma malik oluruq. Təsvirdə bağlanan kvadrat mötərizə ilə birləşdirilən hədlər göstərilir. Kodları qurmaq üçün hər bir mötərizə üçün ehtimallar ilə B-dən olan simvolların altçoxluğu arasında qarşılıqlı birqiymətli uyğunluq qurmaq lazımdır. Bu nümunə halında yuxarı sırada olan birləşdirilən ədədə 0, aşağıda olan ədədə isə 1 simvolu qarşı qoyulur. Sonra isə əks istiqamətdə $p_1,...,p_r$ simvollarına doğru hərəkətə başlanılır və mötərizələrdən keçməklə uyğun kod yazılır. Məsələn,

$$0,51 - 0,29 - 0,20 - p_3$$

yolu 000 kodunu,

$$0,51 - 0,22 - p_2$$

yolu isə 01 kodunu verir. Beləliklə, aşağıdakı kodlaşdırma sxemini alırıq:

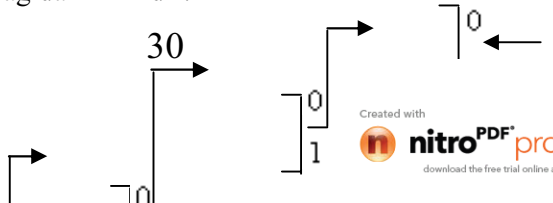
$$a_1 - 1,\ a_2 - 01,\ a_3 - 000,\ a_4 - 001\ .$$

2) Tutaq ki,

$r = 5, q = 2, p_1 = 0,34, p_2 = 0,18, p_3 = 0,17, p_4 = 0,16, p_5 = 0,15$.

Optimal kodu qurmalı.

Qurma prosesi aşağıdakı kimidir:



$0,65$

$0,35$ $0,35$

p_1 $0,34$ $0,34$ $0,34$

$0,31$ $0,31$

p_2 $0,18$ $0,18$

p_3 $0,17$ $0,17$

p_4 $0,16$

p_5 $0,15$

Aşağıdakı yolları alırıq:

$$0,65-0,31-0,15-p_5; \quad 0,65-0,31-0,16-p_4;$$

$$0,35-0,17-p_3; \quad 0,35-0,18-p_2;$$

$$0,65-0,34-p_1.$$

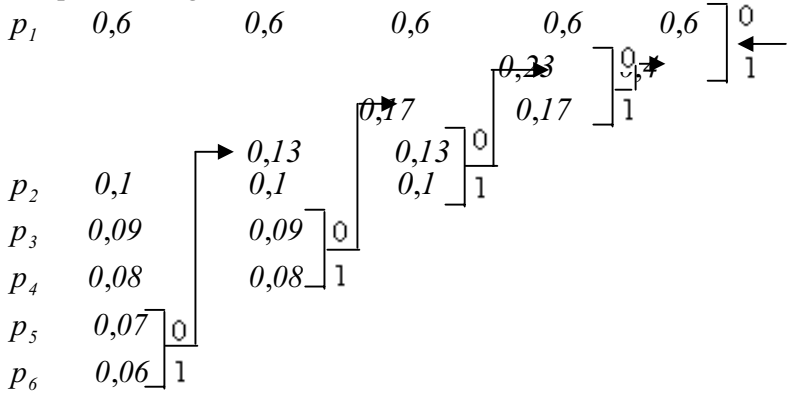
Beləliklə,

$$a_1-00, \quad a_2-10, \quad a_3-11, \quad a_4-010, \quad a_5-011,$$

$$\ell_{ort}=0,34\cdot 2+0,18\cdot 2+0,17\cdot 2+0,16\cdot 3+0,15\cdot 3=2,31.$$

3) Tutaq ki, $r=6$, $q=2$, $p_1=0,6$, $p_2=0,1$, $p_3=0,09$, $p_4=0,08$, $p_5=0,07$, $p_6=0,06$. Optimal kodu qurmalı və onun çəkisini tapmalı.

Qurma prosesi aşağıdakı kimidir:



Sxemdən aşağıdakı yolları alırıq:

$$0,6 - p_1;$$

$$0,4 - 0,23 - 0,1 - p_2;$$

$$0,4 - 0,17 - 0,09 - p_3;$$

$$0,4 - 0,17 - 0,08 - p_4;$$

$$0,4 - 0,23 - 0,13 - 0,07 - p_5;$$

$$0,4 - 0,23 - 0,13 - 0,06 - p_6.$$

Beləliklə, optimal kodlaşdırma sxemi aşağıdakı kimidir:

$$a_1 - 0,\ a_2 - 101,\ a_3 - 110,\ a_4 - 111,$$

$$a_5 - 1000,\ a_6 - 1001.$$

$$L(p) = 0,6 \cdot 1 + (0,1 + 0,09 + 0,08) \cdot 3 + (0,07 + 0,06) \cdot 4 = 1,93.$$

Reduksiya zamanı hər bir addımda ehtimallar qiymətlərinə görə nizamlandırılır. Bu nizamlanma heç də həmişə birqiymətli olmur, belə ki, eyni qiymətə bərabər olan ehtimallar da yarana bilər.

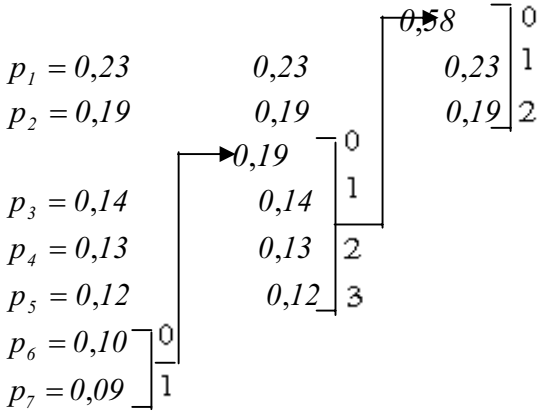
Nümunə 4. Tutaq ki, $r = 7,\ q = 4$ və

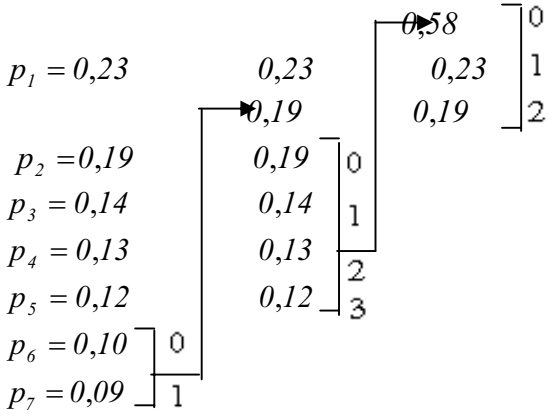
$$p_1 = 0,23,\ p_2 = 0,14,\ p_3 = 0,15,\ p_4 = 0,13,$$

$$p_5 = 0,12,\ p_6 = 0,10,\ p_7 = 0,09.$$

Tutaq ki, $\mathsf{B} = \{0,1,2,3\}$.

Bu nümunə halında reduksiyanı iki üsulla aparmaq olar.





Bu üsullar əsasında kvadrat mötərizə daxilində olan elementləri yuxarıdan aşağı 0,1,2 və 3 ədədləri ilə nömrələməklə aşağıdakı iki əlifba kodlaşdırması sxemini alarıq:

$$a_1 - 1,\ a_2 - 2,\ a_3 - 01,\ a_4 - 02,\ a_5 - 03,\ a_6 - 000,\ a_7 - 001\,, \qquad (\Sigma)$$

$$a_1 - 1,\ a_2 - 00,\ a_3 - 01,\ a_4 - 02,\ a_5 - 03,\ a_6 - 20,\ a_7 - 21\,. \qquad (\Sigma'')$$

Yuxarıda şərh olunan kodlaşdırma üsulunda hesab olunurdu ki, $p_1, p_2, ..., p_r$ ehtimalları arasında ən çoxu biri sıfıra bərabər ola bilər.

$p_1, ..., p_r$ ehtimallarının müxtəlif və $p_1 \geq ... \geq p_r$ və həm də bu ehtimallardan sıfra bərabər olanların sayı vahiddən böyük olduğu halda minimal izafilikli kodların qurulması halına baxaq. Tutaq ki, $p_1 \geq ... \geq p_{r_0} > 0$ və

$$p_{r_0+1} = ... = p_r = 0,\ r - r_0 > 1\,.$$

Əvvəlcə məsələ $(r_0 + 1)$ giriş simvoluna malik əlifba və $p_1, ..., p_{r_0}, p_{r_0+1}$ (burada $p_{r_0+1} = 0$) ehtimalları halında həll olunur. Tutaq ki, $B_1, ..., B_{r_0}, B_{r_0+1}$ minimal izafilikli kodlar üçün elementar kodlardır. Sonra isə B_{r_0+1} elementar kodu atılır və $a_{r_0+1}, ..., a_r$ hərfləri üçün elementar kod olaraq aşağıdakı şəkildə sözlər götürülür:

$$B'_{r_0+1} = B_{r_0+1}B^{(r_0+1)}, ..., B_r = B_{r_0+1}B^{(r)},$$

harada ki, $\ell(B^{(r_0+1)}) = ... = \ell(B^{(r)})$ və bütün $B^{(r_0+1)},...,B^{(r)}$ müxtəlifdirlər. Aydındır ki, belə qurulan kod minimal izafiliklidir və prefiks xassəsini ödəyir.

Minimal izafilikli kodların qurulması üçün yuxarıda təsvir olunan üsul Xafman üsulu adlanır. İndi isə optimal kodlara yaxın olan kodların qurulması üçün iki üsula baxaq. Bu üsullardan biri Fano, digəri isə Şennon üsuludur. Bu üsullarda $B = \{0,1\}$ hesab olunur.

Fano üsulu kifayət qədər sadədir. U əlifbasının simvolları ehtimallarının artmaması ardıcıllığı ilə nizamlanır. Sonra isə simvollar siyahısı iki ardıcıl hissəyə bölünür. Bu hissəyə bölmə zamanı elə edilir ki, həm birinci və həm də ikinci hissəyə daxil olan simvolların ehtimallarının cəmi mümkün qədər bir-birinə yaxın olsun. Birinci hissəyə aid olan simvollara 0, ikinci hissəyə aid olan simvollara 1 simvolu uyğun qoyulur. Sonra isə hər bir hissəyə daxil olan simvollar da yuxarıdakı qaydada iki ardıcıl hissəyə bölünür və onlara da 0 və 1 simvolları uyğun qoyulur. Bu proses alınan hissədə ən azı iki simvol olduqda təkrarlanır və i.a. Proses qurtardıqdan sonra hər bir simvola hissələrə bölmə zamanı uyğun qoyulan simvollar (0 və ya 1 simvolları) ardıcıllığı qarşı qoyulur. Bu qayda ilə alınan kod prefiks və tam kod olur.

Nümunə 5. 1) Tutaq ki, $r = 11$ və

$$p_1 = 0,21,\ p_2 = 0,19,\ p_3 = 0,15,\ p_4 = 0,07, p_5 = 0,06,\ p_6 = 0,06,$$
$$p_7 = 0,06,\ p_8 = 0,05,\ p_9 = 0,05,\ p_{10} = 0,05,\ p_{11} = 0,05\ .$$

Fano üsulu ilə optimala yaxın kodu qurmalı.

Qurma prosesini aşağıdakı cədvəl vasitəsilə təsvir edək.

a_i	p_i	1	2	3	4
a_1	0,21	0	00		
a_2	0,19	0	01	010	
a_3	0,15	0	01	011	
a_4	0,07	1	10	100	1000
a_5	0,06	1	10	100	1001
a_6	0,06	1	10	101	1010

a_7	0,06	1	10	101	1011
a_8	0,05	1	11	110	1100
a_9	0,05	1	11	110	1101
a_{10}	0,05	1	11	111	1110
a_{11}	0,05	1	11	111	1111

Cədvəldən göründüyü kimi kodlaşdırma sxemi aşağıdakı kimidir:

$a_1 - 00,\ a_2 - 010, a_3 - 011,\ a_4 - 1000,\ a_5 - 1001,\ a_6 - 1010,\ a_7 - 1011,$

$a_8 - 1100, a_9 - 1101,\ a_{10} - 1110,\ a_{11} - 1111$.

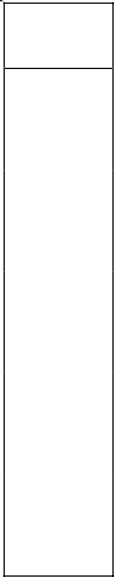
Kodun izafiliyi isə aşağıdakı kimidir:

$\ell_{ort} = 0,21 \cdot 2 + (0,19 + 0,15) \cdot 3 + 4(0,07 + 3 \cdot 0,06 + 4 \cdot 0,05) = 3,24$.

2) Tutaq ki, $r = 5, q = 2,\ p_1 = 0,34,\ p_2 = 0,18,\ p_3 = 0,17,$

$p_4 = 0,16,\ p_5 = 0,15$. Fano üsulu ilə optimala yaxın kodu qurmalı və kodun qiymətini tapmalı.

Qurma prosesini aşağıdakı cədvəl vasitəsilə təsvir edək:



0

1

0

1 10

1 11

Deməli, $a_1 - 00, a_2 - 01, a_3 - 10, a_4 - 110, a_5 - 111$.

$$L(p) = (0,34 + 0,18 + 0,17) \cdot 2 + (0,16 + 0,15) \cdot 3 = 2,31 .$$

3) Tutaq ki, $r = 6,\ q = 2,\ p_1 = 0,6,\ p_2 = 0,1,\ p_3 = 0,09,$ $p_4 = 0,08,\ p_5 = 0,07,\ \ p_6 = 0,06$. Fano üsulu ilə optimala yaxın kodu qurmalı və kodun qiymətini tapmalı.

Qurma prosesi aşağıdakı cədvəl vasitəsilə təsvir edək:

a_i	p_i	1	2	3	4
a_1	0,6	0			
a_2	0,1	1	10	100	
a_3	0,09	1	10	101	
a_4	0,08	1	11	110	
a_5	0,07	1	11	111	1110
a_6	0,06	1	11	111	1111

Deməli, $a_1 - 0, a_2 - 100, a_3 - 101, a_4 - 110, a_5 - 1110, a_6 - 1111$.

$$L(p) = 0,6 \cdot 1 + (0,1 + 0,09 + 0,08) \cdot 3 + (0,07 + 0,06) \cdot 4 = 1,93 .$$

Optimal kodlara yaxın olan kodların Şennon üsulu ilə qurulmasına baxaq. Bu üsul ancaq bütün ehtimallar sıfırdan böyük olduğu halda istifadə olunur. Şennon üsulu aşağıdakılardan ibarətdir.

Simvollar ehtimalların azalması ardıcıllığı ilə nizamlanırlar. p_i ehtimalına malik a_i hərfinə q_i ədədinin sonsuz ikilik kəsrə ayrılışının vergüldən sonrakı ilk $\ell_i =]\log 1/p_i[$ sayda rəqəmlər ardıcıllığı uyğun qoyulur, harada ki,

$$q_i = \sum_{j=0}^{i-1} p_j \qquad (i = \overline{0, m-1}) .$$

Aydındır ki, $h > i$ olduqda (və, beləliklə, $p_h \le p_i$) $\ell_h \ge \ell_i$ və $1 > q_h \ge q_i + p_i \ge q_i + 2^{-\ell_i}$ olur. Odur ki, alınan kod prefiks kod olar. Sonra alınmış koddan kəsilmiş kod (rəqəmlərin sayı məhdud) alırıq, hansı ki, optimal koda yaxın kod olur.

Teorem 2. İstənilən $P = \{p_0, p_1, ..., p_{m-1}\}$ paylanması halında

$$\sum_{i=1}^{m-1} p_i \log \frac{1}{p_i} \le L(P) \le \sum_{i=0}^{m-1} p_i \log \frac{1}{p_i} + 1$$

münasibətinin qüvvədə olması üçün zəruri və kafi şərt elə $\ell_0, \ell_1, ..., \ell_{m-1}$ tam ədədlərinin mövcud olmasıdır ki,

$$p_i = 2^{-\ell_i}, \quad i = 0, ..., m-1$$

olsun. Burada

$$L(P) = \sum_{i=0}^{m-1} p_i \log \frac{1}{p_i}.$$

Nümunə 6. Tutaq ki, $a_0, a_1, a_2, a_3, a_4, a_5, a_6$ simvollarının əmələgəlmə ehtimalları $p_0 = 0{,}20$, $p_1 = 0{,}20$, $p_2 = 0{,}19$, $p_3 = 0{,}12$, $p_4 = 0{,}11$, $p_5 = 0{,}09$, $p_6 = 0{,}09$ -dır. Optimal kodlaşdırmanı tapmalı.

Sennon üsuluna uyğun kodlaşdırma aşağıdakı cədvəldə verilir.

a_i	p_i	ℓ_i	q_i	Şennon kodu
a_0	0,20	3	0,00 = 0,000	000
a_1	0,20	3	0,20 = 0,001	001
a_2	0,19	3	0,40 = 0,011	01
a_3	0,12	4	0,59 = 0,1001	100
a_4	0,11	4	0,71 = 0,1011	101
a_5	0,09	4	0,82 = 0,1101	110
a_6	0,09	4	0,91 = 0,1110	111
Kodun dəyəri				2,81

§4. Səhflərə nəzarətedici kodlar haqqında qısa məlumatlar

Rabitə sistemləri verilənlər (məlumatlar) mənbəsini verilənləri qəbul edənlərlə kanal vasitəsilə birləşdirir. Kanala rabitə kanalı da deyilir. Kanala

nümunə koaksial kabellər, telefon şəbəkəsi, optik liflər şəbəkəsi, kiçik dalğalı elektromaqnit xətləri və hətta maqnit lentləri və diskləri ola bilər. Rabitə sistemlərinin layihələndirilməsi zamanı kanalın girişini hazırlayan və çıxışını emal edən qurğular yaradılır.

Verilənlər mənbəsindən rabitə sisteminə daxil olan verilənlər (məlumatlar) ilkin olaraq mənbə koderi vasitəsilə emal olunur və daha yığcam halda təşkil olunur. Bu aralıq təsvir simvollar ardıcıllığından ibarət olur və mənbənin kod sözü adlanır. Sonra məlumatlar kanal koderində emal olunaraq mənbə kod sözləri ardıcıllığından kanal kod sözləri adlanan simvollar ardıcılığına çevrilirlər. Kanal kod sözləri mənbə kod sözlərinə nisbətən daha uzun ardıcıllıqdan ibarət olur və bu da izafi hesab olunur. Kod sözünün hər bir simvolu bit şəklində və ya mümkündür ki, bitlər qrupu şəklində olur.

Buradan sonra modulyator qurğusu kanalın kod sözünün hər bir simvolunu mümkün sonlu analoq siqnalları çoxluğundan olan uyğun analoq siqnalına çevirir. Analoq simvolları ardıcıllığı kanal vasitəsilə ötürülür. Kanalda müxtəlif təhrifedici təsirlər olduğundan kanalın çıxışı ilə girişi bir-birindən fərqlənir. Kanalın çıxışı demodulyasiya olduqdan sonra alınan simvollar ardıcıllığı qəbuledilən söz adlanır. Kanalda təhriflər, yaxud interferensiyalar olduğundan qəbul edilən söz kanalın kod sözü ilə heç də həmişə üst-üstə düşmür.

Kanal dekoderi qəbul edilən sözdə səhvləri tapa bilməsi üçün izafilikdən (artıqlıqdan) istifadə edir və bunun nəticəsində mənbə kod sözünün «qiymətləndirilməsini» yaradır. Əgər bütün səhvlər düzəldilibsə, onda mənbə kod sözünün «qiymətləndirilməsi» ilə mənbənin ilkin kod sözü üst-üstə düşür. Mənbənin dekoder qurğusu koder qurğusunun yerinə yetirdiyi əməliyyatı əksinə yerinə yetirir və nəticədə alınan məlumat istifadəçiyə verilir.

Səhvlərə nəzarətedici kodların tarixi amerika alimi Klod Şennonun 1948-ci ildə çap etdirdiyi işlərdən sonra başlamışdır. Aydındır ki, hər bir kanal üçün kanalın ötürmə qabiliyyəti adlanan və saniyədə ötürüləbilən bitlərin maksimal sayını göstərən C ədədi mövcuddur. Şennonun fikrincə əgər sistemdən tələb olunan informasiya ötürmə sürəti R (saniyədə bitlərlə ölçülür) C –dən kiçik isə, onda səhvlərə nəzarətedici kodlardan istifadə etməklə elə rabitə sistemi qurmaq olar ki, çıxışda səhvin olması ehtimalı istənilən qədər kiçik olsun. Şennonun bu nəzəriyyəsindən çıxır ki, həddən artıq yaxşı rabitə sistemi qurmaq çox vəsait tələb edir. İqtisadi cəhətdən

sərfəlidir ki, kodlaşdırma nəzəriyyəsi istifadə olunsun. Lakin Şennon yaxşı kodların necə tapılması haqqında heç bir məlumat verməmişdir, ancaq belə kodların mövcud olmasını isbat etmişdir. XX əsrin 50-ci illərində «yaxşı» kodların axtarılmasına çoxlu qüvvələr cəlb edilməsinə baxmayaraq o qədər də yaxşı nəticələr əldə edilməmişdir. Sonrakı on illiklər bu maraqlı məsələyə az fikir verilmişdi. Bunun əvəzinə kod tədqiqatçıları əsas iki istiqamətdə uzunmüddətli tədqiqat işləri aparmışlar.

Birinci istiqamət təmiz cəbri xarakter daşımışdır və əsasən blok kodlarına baxılmışdır. İlk blok kodu Xemminq tərəfindən 1950-ci ildə daxil edilmişdir. Bu kodlar bir səhvi düzəltməyə müvəffəq olur. 50-ci illərin sonunadək bu sahədə irəliləyiş olmamışdır. Eyni bir nəzəriyyəyə əsaslanmayan kiçik uzunluqlu çoxlu kodlar tapılmışdır. Əsas irəliləyiş, Bouz və Roy-Çoudxuri tərəfindən 1960-cıildə, Xokvinqem tərəfindən isə 1959-cu ildə çoxqat səhvləri düzəltməyə imkan verən kodlar sinfinin tapılması ilə bağlı olmuşdur. Belə kodlar BÇX kodları adlanır.

Rid və Solomon 1960-ci ildə BÇX kodları ilə bağlı olan və ikilik olmayan kanallar üçün kodlar sinfi tapmışlar.

BÇX kodlarının kəşfi «bərk» və «yumşaq» koder və dekoder qurğularının qurulmasının praktik üsullarının axtarılmasına təkan verdi. İlk yaxşı üsul Piterson tərəfindən verilmişdir. Sonralar Pitersonun təsvir etdiyi hesablamaları yerinə yetirməyin güclü alqoritmi Berlekemp və Messi tərəfindən təklif edilmişdir. Bu alqoritmlərin realizasiyası yeni rəqəm texnikası yaranan kimi praktikada istifadə olunmağa başladı.

Kodlaşdırma sahəsində tədqiqatların ikinci istiqaməti ehtimal xarakterinə malikdir. İlkin tədqiqatlar hələ məlum olmayan blok kodları siniflərinin ən yaxşılarının səhvlərinin ehtimallarının qiymətləndirilməsi ilə əlaqədar idi. Bu tədqiqatlar kodlaşdırma və dekodlaşdırmanın ehtimal nöqteyi-nəzərindən başa düşülməsi cəhdi ilə bağlı idi və bu cəhd ardıcıl dekodlaşdırmaya gətirib çıxartdı. Ardıcıl dekodlaşdırmada bloklu olmayan sonsuz uzunluqlu kodlar sinfi daxil edilir. Belə kodları ağaclar vasitəsilə təsvir etmək və ağaclarda axtarış alqoritmlərinin köməkliyi ilə dekodlaşdırmaq olur. Ən səmərəli ağacvari kodlardan bağlı kodları nümunə göstərmək olar. Bu kodları xətti sürüşdürmə registrlər dövrəsi ilə, ardıcıllıqlı maşınlar vasitəsilə yaratmaq olar. Bu zaman məlumatlar ardıcıllığının bağlanması əməliyyatı həyata keçirilir. 50-ci illərin sonunda bağlı kodlar üçün ardıcıl dekodlaşdırma alqoritmləri yaradılmışdır. Belə kodlar üçün Biterbi alqoritmi kimi ən sadə alqoritm 1967-ci ildə

yaradılmışdır. Bağlı kodlar üçün olan və çox kiçik mürəkkəbliyə malik Biterbi alqoritmi çox geniş tətbiq olunur. Lakin çox qüvvətli kodlar üçün o məqsədə uyğun deyildir.

70-ci illərdə yuxarıda adı çəkilən iki tədqiqat istiqaməti bir-birinə qarışmışdır. Bağlı kodlar nəzəriyyəsi ilə cəbrçilər məşğul olmağa başlamış və onu yeni yanaşmalar ilə zənginləşdirmişlər. Bloklu kodlar nəzəriyyəsində Şennonun vəd etdiyi kodlara yaxın olan kodların alınması müyəssər olmuşdur. Belə ki, kodlaşdırma üçün iki müxtəlif kodlaşdırma sxemi - biri Yusteson tərəfindən, digəri isə Qopp tərəfindən təklif edilmişdir. Bu sxemlər vasitəsilə həm çox böyük uzunluğa və həm də yaxşı xarakteristikalara malik kodlar sinfi yaratmaq mümkün olmuşdur. Lakin bu sxemlər praktik məhdudiyyətlərə malikdirlər.

80-ci illərin əvvəlindən başlayaraq koder və dekoderlər yeni rəqəm rabitə sistemləri və yaddaşa malik rəqəm sistemləri konstruksiyalarında qurulurlar. Səhvlərə nəzarətedici kodların inkişafı ilkin olaraq rabitə məsələləri ilə stimullaşdırıldığından terminologiya rabitə nəzəriyyəsindən götürülmüşdür. Lakin kodların qurulması başqa tətbiqlərlə də bağlıdır. Məsələn, hesablama qurğularının yaddaşında olan məlumatların qorunmasında kodlar istifadə olunur (həm əməli yaddaşda, və həm də xarici yaddaş qurğularında, verilənlər bazasında). Kodlar rəqəm məntiqi dövrələrinin təhriflərin təsirindən qorunmasında da istifadə olunur. Kodlar verilənlərin sıxlaşdırılmasında, kriptoqrafiyada da istifadə olunur. Kodlaşdırma nəzəriyyəsinin rabitə məsələlərində tətbiqi müxtəlif xarakterlərə malik olur. İkilik verilənlər (məlumatlar) adətən hesablama terminalları arasında, uçan aparatlar arasında, sputniklər arasında mübadilə olunurlar. Kodlaşdırma etibarlı mübadilə təşkil etmək üçün istifadə oluna bilər. Getdikcə efir insanlar tərəfindən yaradılan elektromaqnit dalğaları ilə doldurulduğundan kodlaşdırma nəzəriyyəsi getdikcə daha güclü qorunma vasitəsinə çevrilir. Çünki kodlaşdırma nəzəriyyəsi rabitə xətlərində interferensiyalar olduğu halda da etibarlı işləməyə imkan verir.

Kodlaşdırma nəzəriyyəsi hərbi tətbiqlərdə tez-tez rəqib tərəfin bilərəkdən yaratdığı interferensiyalar mühitində etibarlı işləməyi təmin edir.

Bir çox rabitə sistemlərində məlumatların mübadiləsində ötürmə güclərinə məhdudiyyətlər mövcuddur. Məsələn, sputnik vasitəsilə retranslyasiyada gücün artırılması çox baha başa gəlir. Səhvlərə nəzarətedici kodların tətbiqi zəruri gücün azaldılmasında çox yaxşı

vasitədir. Belə ki, onlar vasitəsilə zəiflədilmiş məlumatların düzgün bərpasını təşkil etmək olur. Səhvlərə nəzarətedici kodların tətbiqi nəticəsində xarici yaddaş qurğularında məlumatları daha yığcam (sıx) yerləşdirmək mümkün olur.

Kompüter sistemlərində, şəbəkələrində çox böyük uzunluqlu məlumatlar paketlərə bölünür və mübadilə olunur. Sistemin çox yükləndiyi dövrlərdə, yaxud digər səbəblərdən bu və ya digər paket itə bilər. Uyğun səhvlərə nəzarətedici kodların tətbiqi belə itkilərin qarşısının alınmasına kömək edə bilər. Belə ki, itmiş paketləri məlum paketlər vasitəsilə bərpa etmək olar.

Fərz edək ki, bizi maraqlandıran bütün məlumatlar (verilənlər) ikilik məlumatlar kimi təsvir oluna bilər, yəni «0» və «1»-lər ardıcıllığı kimi. Bu ikilik məlumatlar ötürmə kanalı ilə ötürüldükdə təsadüfi səhvlərə məruz qalır. Kodlaşdırma məsələsi aşağıdakından ibarətdir: məlumat simvollarına əlavə simvollar elə qoşulur ki, qəbuledicidə təhriflər tapılıb düzəldilə bilsin. Başqa sözlə desək verilənlər simvolları ardıcıllığı nisbətən uzun simvollar ardıcıllığı ilə əvəz olunur və bu artıqlıq (izafilik) verilənlərin qorunmasına kifayət edir.

M gücünə malik və n uzunluqlu ikilik kod M sayda n uzunluqda ikilik sözlərdən ibarət çoxluq kimi təsəvvür olunur. Adətən $M = 2^k$, harada ki, k hər hansı bir müsbət tam ədəddir. Belə kod (n,k) – kodu adlanır.

Tutaq ki, x və y n uzunluqlu ikilik simvollar ardıcıllığıdır. x və y arasında Xemminq məsafəsi dedikdə bu ardıcıllıqlarda bir-birindən fərqlənən mövqelərin sayı nəzərdə tutulur və $d(x,y)$ kimi işarə olunur.

Tutaq ki, $C = \{c_i, i = 0,1,..., M-1\}$ kodu verilib

$$d^* = \min_{\substack{c_i, c_j \in C \\ i \neq j}} d(c_i, c_j)$$

kimi təyin olunan d^* kəmiyyəti C kodunun minimal məsafəsi adlanır.

Nümunə 1. Tutaq ki, $C = \{1010, 1100, 0010, 1101\}$. Aydındır ki,

$$d(1010,1100) = 2,\ \ d(1010,0010) = 1,\ d(1010,1101) = 3,$$

$$d(1100,0010) = 3,\ d(1100,1101) = 1,\ d(0010,1101) = 4.$$

Deməli, $d^* = 1$.

d^* minimal məsafəsinə malik (n,k)-kodu (n,k,d^*) - kodu kimi də adlandırılır.

Fərz edək ki, kod sözü ötürülüb və kanalda bir səhv baş verib. Onda qəbul edilən söz ötürülən sözdən bir xemminq məsafəsində olar. Başqa kod sözlərinə qədər məsafə 1-dən böyük olduğu halda dekoder səhvi düzəldə bilər, yəni qəbul edilən sözə ən yaxın olan kod sözünü ötürülən söz kimi götürə bilər.

Ümumi halda əgər kodların ötürülməsi zamanı t sayda səhv (təhrif) baş veribsə və əgər qəbul edilən söz ilə kod sözləri arasında məsafə t-dən çox olarsa,onda dekoder bu səhvi düzəldə bilər və bu zaman qəbul edilən sözə ən yaxın kod sözü ötürülən kod sözü kimi götürülə bilər. Deyilənlər $d^* \geq 2t+1$ şərti ödənildiyi halda mümkün olar. Bəzən bu şərt ödənmədiyi halda da səhvlər düzəldilə bilir, lakin onun doğruluğuna zəmanət verilmir. Deyilənlərə həndəsi şərh aşağıdakı kimi verilir: q-lük n-ardıcıllıqların hamısının əmələ gətirdiyi fəzada n-ardıcıllıqların müəyyən bir çoxluğu ayrılır və onlara kod sözləri deyilir. Əgər kod sözlərinin minimal məsafəsi d^* isə və t ədədi $d^* \geq 2t+1$ şərtini ödəyən ən böyük tam ədəddirsə, onda hər bir kod sözü ətrafında t radiuslu bir-biri ilə kəsişməyən kürələr çəkmək olar. Bu kürələr dekodlaşdırma kürələri adlanırlar. Qəbul edilən söz hər hansı bir kürəyə daxil olur. Dekodlaşdırma zamanı qəbul edilən söz onun daxil olduğu kürənin mərkəzində yerləşən kod sözünə dekodlaşdırılır. Məlumatların ötürülməsi zamanı t-dən çox olmayan sayda səhv baş verərsə, onda qəbul edilən söz həmişə uyğun kürəyə daxil olar və dekodlaşdırma düzgün olar. Əgər t-dən çox sayda səhv baş verərsə qəbul edilən sözlərdən bəzisi başqa dekodlaşdırma kürəsinə daxil olacaq və dekodlaşdırma düzgün olmayacaq. Bəzi qəbul edilən sözlər t-dən çox sayda səhv baş vermiş olduğu halda sferalar arası sahəyə düşür.

Dekoderlər iki qrupa bölünür: natamam dekoderlər və tam dekoderlər.

Natamam dekoderlər ancaq dekodlaşdırma sferası daxilinə düşən qəbul edilmiş sözləri dekodlaşdırır. Qalan sözləri isə, harada ki, t-dən çox sayda səhvdən ibarət olur, dekoder düzəldilə bilməyən söz kimi götürür.

Tam dekoderlər isə qəbul edilən sözü ona ən yaxın olan kod sözünə (ən yaxın sfera mərkəzinə) dekodlaşdırır. Əgər ən yaxın kod sözünün sayı birdən çox isə (yəni bərabər məsafələrdə isə), onda onlardan hər hansı biri

göndərilən kod sözü elan edilir. t saydan çox səhv baş verdiyi halda tam dekoderlər çox vaxt dekodlaşdırmanı düzgün həyata keçirmir.

(n,k) - kodunda $R = k/n$ kimi təyin olunan kəmiyyətə kodun sürəti deyilir.

Tutaq ki, c kod sözü verilib. c kodunun sıfırdan fərqli simvollarının (mövqelərinin) sayını göstərən $w(c)$ kəmiyyəti c kod sözünün Xemminq çəkisi adlanır.

Verilən $C = \{c_1, c_2, ..., c_M\}$ kodunda d^* minimal məsafəsi üçün aşağıdakı münasibət doğrudur:

$$d^* = \min_{\substack{c \in C \\ c \neq 0}} w(c) = w^*.$$

t sayda səhvi düzəltmək üçün w^* minimal çəkisi $w^* \geq 2t+1$ şərtini ödəyən kod tapmaq lazımdır.

Ən əvvəl sadə kodlar adlanan kodlara baxaq. Sadə kodlara aşağıdakı kodlar aiddir: cütlüyə tamamlamaqla sadə kod; təkrarlamaqla sadə kod, Xemminq kodları.

Cütlüyə tamamlamaqla sadə kodlar. Bu kodlar yüksək sürətli, lakin pis korreksiyaedici xarakteristikalıdırlar. Verilmiş k sayda informasiyaya bir bit əlavə olunur və beləliklə $k+1$ sayda bit alınır. $k+1$ -ci bitin məzmunu k sayada bitin məzmunundan asılı olur. Əgər ilk k sayda mövqedə «1»-ə bərabər məzmunlu bitlərin sayı cüt olarsa, $k+1$-ci bitə «0», tək olarsa – «1» yazılır. Belə kodlar $(k+1, k)$ yaxud $(n, n-1)$ kodlardır və $d^* = 2$ - dir. Odur ki, bu kodlar vasitəsilə heç bir səhv düzəldilə bilmir. Belə kodlar bir səhvi aşkar etmək üçün istifadə olunur. Bəzən təkliyə tamamlamaqla sadə kodlar da istifadə olunur.

Təkrarlamaqla sadə kodlar. Bu kodlar kiçik sürətli kodlardır və yaxşı korreksiyaedici xarakteristikaya malikdir. Təkrarlamaqla sadə kodlar bir informasiya sözünü n dəfə təkrarlamaqla (adətən n tək ədəd olur) alınır. Belə kodlar $(n,1)$ -kodlardır və minimal məsafə n -dir. Bu kodlarla $(n-1)/2$ sayda səhv düzəldilə bilər.

Xemminq kodları. Hər bir m tam ədədi üçün $(2^m - 1,\ 2^m - 1 - m)$ - Xemminq kodu mövcuddur. Xemminq kodları bir səhvi düzəltməyə imkan verir və böyük m -lər üçün bu kodların sürəti vahidə yaxındır.

Xemminq kodlarının qurulmasına baxaq: Tutaq ki, məlumat mövqeləri $\alpha_1, \alpha_2, ..., \alpha_m$ -dir. Bu mövqelər $\beta_1, \beta_2, ..., \beta_\ell$ mövqelərinə kodlaşır, harada ki, ℓ

$$2^m \le \frac{2^\ell}{\ell + 1}$$

şərtini ödəyən ən kiçik tam ədəddir.

$1,2,..., \ell$ ədədlərini aşağıdakı kimi qruplara bölək: $R_1, R_2, ..., R_k$, harada ki, $k = \ell - m$. Qeyd olunmuş i üçün R_i çoxluğuna o ədədləri daxil edək ki, onların ikilik say sistemində yazılışında i-ci mövqe (vahiddən başlamaqla saydıqda) «1»-dən ibarət olsun. Aydındır ki, $R_1, R_2, ..., R_k$ çoxluqlarının birinci elementləri uyğun olaraq $1 = 2^0$, $2 = 2^1, ..., 2^{k-1}$, yəni ikinin qüvvətləri olacaq. β_i, $i = 1,2,..., \ell$ mövqelərindən indeksləri $1,2,...,2^{k-1}$ kəmiyyətlərinə bərabər olanları nəzarət mövqeləri adlanır, qalanları isə informasiya mövqeləri adlanır. β_i, $i = 1,2,..., \ell$ mövqelərindən informasiya mövqelərini indekslərin artmasına görə ardıcıl düzərək onlara uyğun olaraq $\alpha_1, \alpha_2, ..., \alpha_m$ informasiya mövqelərinin qiymətlərini mənimsədək:

$$\beta_3 = \alpha_1,\ \beta_5 = \alpha_2,\ \beta_6 = \alpha_3, ..., \beta_{2^{k-1}+1} = \alpha_m .$$

Sonra isə nəzarət mövqeləri aşağıdakı kimi müəyyən edilir

$$\beta_{2^{i-1}} = \sum_{j \in R_i \setminus \{2^{i-1}\}} \beta_j,\ \ GF(2)\ ,\ \ i = 1,2,...,k .$$

Burada $GF(2)$ yazısı cəmləmənin mod 2-yə görə aparılmasını göstərir.

Sonuncu düsturdan göründüyü kimi Xemminq kodları yaradılan zaman ardıcıllıqlı maşınlardan istifadə oluna bilər.

İndi Xemminq kodlarının dekodlaşdırılması sxeminə baxaq. Tutaq ki, $\beta'_1, \beta'_2, ..., \beta'_\ell$ simvolları qəbul edilmişdir. Aşağıdakı kimi hesablama aparılır:

$$s_i = \sum_{j \in R_i} \beta'_j,\ \ GF(2),\ \ i = 1,2,...,k .$$

Əgər $s_i = 0$, $i = 1,2,...,k$ olarsa, onada heç bir səhv baş verməmişdir. Əks halda $(s_k s_{k-1}...s_1)$ ikilik koduna uyğun olan ədəd müəyyən edilir və bu indeks kimi götürülür. Tutaq ki, bu indeks γ-dır. Onda $\beta'_\gamma := 1 \oplus \beta'_\gamma$ korreksiyası həyata keçirilir. Sonra isə ötürülən kodun mövqelərini $\beta'_1, \beta'_2,..., \beta'_\ell$ kimi götürməklə dekodlaşdırma prosesi sona yetmiş hesab olunur.

Nümunə 2. Tutaq ki, informasiya sözləri $m = 4$ ikilik mövqedən ibarətdir: i_1, i_2, i_3, i_4. Belə sözlərin sayı $2^m = 16$ ədədinə bərabərdir və onlar cədvəl 1-də verilir. Bu m sayda mövqeyə k sayda mövqe əlavə edək. Nəticədə $\ell = m + k$ sayda mövqe alarıq, yəni $\ell = 4 + k$. k ədədini elə seçək ki,

$$2^m \le \frac{2^\ell}{\ell + 1} \quad \text{və ya} \quad 2^4 \le \frac{2^{4+k}}{4 + k + 1}$$

şərti ödənsin. Bu şərti ödəyən ən kiçik k ədədi 3-ə bərabərdir. Deməli, (i_1, i_2, i_3, i_4) sözlərinin kodlaşdırılması nəticəsində alınan kod $(\ell, m) = (7,4)$ kodu olacaq.

R_1, R_2, R_3 çoxluqları aşağıdakı çoxluqlardır:

$$R_1 = \{1,3,5,7\},\ R_2 = \{2,3,6,7\},\ R_3 = \{4,5,6,7\}.$$

(i_1, i_2, i_3, i_4) sözü $(\beta_1, \beta_2,..., \beta_7)$ sözünə kodlaşır. $\beta_1, \beta_2, \beta_4$ mövqeləri nəzarət mövqeləri, $\beta_3, \beta_5, \beta_6, \beta_7$ isə informasiya mövqeləridir. Kodlaşdırma zamanı

$$\beta_3 = i_1,\ \beta_5 = i_2,\ \beta_6 = i_3,\ \beta_7 = i_4 \qquad (1)$$

götürülür. Sonra isə $\beta_1, \beta_2, \beta_4$ yoxlayıcı mövqelərinin qiymətləri aşağıdakı düsturla təyin olunur.

$$\beta_1 = \beta_3 \oplus \beta_5 \oplus \beta_7,\ \beta_2 = \beta_3 \oplus \beta_6 \oplus \beta_7,\ \beta_4 = \beta_5 \oplus \beta_6 \oplus \beta_7. \qquad (2)$$

(i_1, i_2, i_3, i_4) sözünə uyğun $(\beta_1, \beta_2, \beta_3, \beta_4, \beta_5, \beta_6, \beta_7)$ kodunun hər bir mövqesinin qiyməti (1) və (2) münasibətləri ilə hesablanaraq cədvəl 1-də verilmişdir.

Cədvəl 1.

i_1	i_2	i_3	i_4	β_1	β_2	β_3	β_4	β_5	β_6	β_7
0	0	0	0	0	0	0	0	0	0	0
0	0	0	1	1	1	0	1	0	0	1
0	0	1	0	0	1	0	1	0	1	0
0	0	1	1	1	0	0	0	0	1	1
0	1	0	0	1	0	0	1	1	0	0
0	1	0	1	0	1	0	0	1	0	1
0	1	1	0	1	1	0	0	1	1	0
0	1	1	1	0	0	0	1	1	1	1
1	0	0	0	1	1	1	0	0	0	0
1	0	0	1	0	0	1	1	0	0	1
1	0	1	0	1	0	1	1	0	1	0
1	0	1	1	0	1	1	0	0	1	1
1	1	0	0	0	1	1	1	1	0	0
1	1	0	1	1	0	1	0	1	0	1
1	1	1	0	0	0	1	0	1	1	0
1	1	1	1	1	1	1	1	1	1	1

Tutaq ki, ötürülən informasiya mövqeləri

$$\beta_1' = 1,\ \beta_2' = 1,\ \beta_3' = 0,\ \beta_4' = 0,\ \beta_5' = 0,\ \beta_6' = 0,\ \beta_7' = 1$$

kimi olan söz şəklində qəbul olunub. Ötürmə prosesində təhrif baş verib verməməsini yoxlayaq. Bunun üçün aşağıdakı hesablamaları aparaq:

$$s_1 = \beta_1' \oplus \beta_3' \oplus \beta_5' \oplus \beta_7' = 1 \oplus 0 \oplus 0 \oplus 1 = 0,$$

$$s_2 = \beta_2' \oplus \beta_3' \oplus \beta_6' \oplus \beta_7' = 1 \oplus 0 \oplus 0 \oplus 1 = 0,$$

$$s_3 = \beta_4' \oplus \beta_5' \oplus \beta_6' \oplus \beta_7' = 0 \oplus 0 \oplus 0 \oplus 1 = 1.$$

$s_3 \neq 0$ olduğundan təhrifin baş verməsi aydın olur. $(s_3\, s_2\, s_1) = 100_2 = 4_{10}$ olduğundan təhrifə məruz qalan mövqe dördüncü mövqedir. Deməli, dördüncü mövqe $\beta_4 = 1 \oplus \beta_4' = 1 \oplus 0 = 1$ kimidir, ötürülən kod sözü isə $(\beta_1, \beta_2, \beta_3, \beta_4, \beta_5, \beta_6, \beta_7) = (1101001)$ sözüdür.

Kod sinifləri aşağıdakı qruplara bölünürlər:

-blok kodları;

-ağacvari kodlar;

-hesabı kodlar və i.a.

Blok kodları xətti və qeyri-xətti blok kodlarına bölünürlər.

FƏSİL II. KODLAŞDIRMA NƏZƏRİYYƏSİNİN CƏBRİ ƏSASLARI

§1. Cəbri əməl və cəbri struktur anlayışı

Tutaq ki, hər hansı bir G çoxluğu verilmişdir. Bu çoxluğun elementləri ədədlərdən və ya həndəsi təbiətə malik obyektlərdən və ya da ixtiyari əşyalardan ibarət ola bilər. Əgər G çoxluğunun müəyyən nizamla götürülmüş a və b elementləri cütlüyünə G çoxluğunun üçüncü bir c elementi müəyyən bir qayda üzrə birqiymətli olaraq qarşı qoyulursa, onda deyirlər ki, G çoxluğunda binar cəbri əməl təyin olunmuşdur.

Analoji olaraq «unar», «ternar» və i.a. «n-ar» cəbri əməl təyin olunur: unar cəbri əməl zamanı G çoxluğunun bir elementinə G çoxluğunun başqa bir elementi, ternar cəbri əməl zamanı G çoxluğunun üç elementinə G çoxluğunun başqa bir elementi və i.a. n -ar əməl zamanı isə G çoxluğunun n sayda elementlərinə G çoxluğunun başqa bir elementi qarşı qoyulur.

Xüsusi hallarda, cəbri əməli toplama və ya vurma adlandıraraq onu «+» və ya «·» (nöqtə) kimi işarə edirlər. Çox vaxt cəbri əməli ümumilik üçün «∗» simvolu ilə də işarə edirlər. G çoxluğunda * əməlinin təyin edilməsi o deməkdir ki, $a,b \in G$ olarsa, onda həm də $a * b \in G$ olar. Bu halda, başqa sözlə, $G \times G \to G$ inikası təyin olunmuşdur.

Nümunə 1.

1. Tam ədədlər çoxluğunda toplama və vurma cəbri əməlləri təyin olunub;

2. Tam ədədlər çoxluğunda bölmə əməli cəbri əməl təşkil etmir. Belə ki, bir tərəfdən sıfıra bölmə təyin olunmayıb, digər tərəfdən isə iki tam ədədin nisbəti tam ədəd olmaya bilər;

3. Natural ədədlər çoxluğunda çıxma əməli cəbri əməl təşkil etmir;

4. İrrasional ədədlər çoxluğunda vurma əməli cəbri əməl təşkil etmir. Belə ki, iki irrasional ədədin hasili irrasional olmaya bilər. Məsələn, $\sqrt[3]{5}$ və $\sqrt[3]{25}$ ədədləri üçün (çünki $\sqrt[3]{5} \cdot \sqrt[3]{25} = 5$);

5. Mülahizələr çoxluğunda konyunksiya (məntiqi vurma) və dizyunksiya (məntiqi toplama) kimi adlandırılan əməllər riyazi məntiqdə cəbri əməllər təşkil edir.

6. Tam ədədlər çoxluğunda kvadrata yüksəltmə əməli unar cəbri əməl təşkil edir.

7. Mülahizələrin inkarı əməli riyazi məntiqdə unar cəbri əməl təşkil edir.

8. Natural ədədlər çoxluğunda iki ədədin ən böyük ortaq böləni və ən kiçik ortaq bölünəninin tapılması əməlləri binar cəbri əməllər təşkil edirlər.

9. $(n \times n)$ -ölçülü matrislərin toplanması və vurulması belə matrislər çoxluğunda cəbri əməllər təşkil edirlər.

Cəbri əməllər müxtəlif xassələrə malik ola bilərlər. Bu xassələrə kommutativlik, assosiativlik xassələri aiddir. Məsələn, tam ədədlər çoxluğunda vurma və toplama əməlləri həm kommutativlik və həm də assosiativlik xassələrinə malikdirlər. Tam ədədlər çoxluğunda çıxma əməli, $(n \times n)$ -ölçülü matrislərin vurulması əməli kommutativlik xassəsinə malik deyildirlər.

Bir cəbri əməl başqa bir cəbri əmələ nəzərən müəyyən bir xassəyə malik ola bilər. Məsələn, vurma əməlinin toplama əməlinə nəzərən distributivlik qanunu.

Müasir cəbrin ümumi cəbr adlanan bölməsi cəbri strukturları öyrənməklə məşğuldur. Cəbri strukturları cəbri sistemlər, universal cəbrlər kimi də adlandırırlar.

Cəbri strukturlar müəyyən xassələrə malik olan bir neçə cəbri əməlin təyin olunduğu müxtəlif təbiətli elementlərə malik çoxluqlara deyilir.

Qeyd edək ki, G çoxluğu üzərində n -ar cəbri əməli riyazi olaraq aşağıdakı inikas kimi təyin olunur:

$$f : G \times G \times ... \times G \to G ,$$

harada ki, «×» çoxluqların Dekart hasili əməlinin işarəsidir. Beləliklə, cəbri əməl n -dəyişənli (n -yerli) funksiya (inikas) kimi təyin olunur. Hər hansı bir A cəbri strukturu riyazi olaraq G çoxluğu ilə onda təyin olunmuş əməllərin S çoxluğunun yığımı kimi təyin olunur və

$$A = (G, S)$$

kimi yazılır. Burada G çoxluğu A cəbri strukturunun daşıyıcısı, S isə onun siqnaturası adlanır. S siqnaturası aşağıdakı kimidir:

$$S = \{f_1, ..., f_m\}.$$

Burada f_i, $i = \overline{1,m}$, i-ar əməliyyatdır (i-dəyişənli funksiyadır).

Bəzən cəbri sistemi aşağıdakı üçlük kimi də təyin edirlər:

$$A = (G, \Omega_F, \Omega_P). \quad (1)$$

Burada G əsas çoxluq (daşıyıcı çoxluq), $\Omega_F = \{F_0, F_1, ..., F_i\}$ və $\Omega_P = \{P_0, P_1, ..., P_j\}$ isə G-də təyin olunmuş uyğun olaraq cəbri əməllər və predikatlardan ibarət çoxluqlardır:

$$F_\ell : \underbrace{G \times G \times ... \times G}_{\ell} \to G, \; P_k : \underbrace{G \times G \times ... \times G}_{k} \to \{0,1\},$$

$$\ell = \overline{1,i}, \; k = \overline{1,j}.$$

Əgər cəbri sistem ancaq əməllərlə təyin olunursa, onda ona cəbr, ancaq predikatlarla təyin olunursa, onda ona relyasiya modeli deyilir. (1) münasibətinə uyğun olaraq cəbr $A =< G, \Omega_F >$, relyasiya modeli isə $A =< G, \Omega_P >$ kimi cütlüklə təyin olunur.

Cəbri strukturlar nəzəriyyəsində daşıyıcı çoxluğun neytral elementi və bu çoxluqdan olan elementlərə simmetrik elementlər anlayışları mühüm rol oynayır. Bu elementlər cəbri strukturun siqnaturasına daxil olan bu və ya digər əməllərə nəzərən hesab olunur.

Tutaq ki, a elementi G çoxluğunun hər hansı bir elementidir və G çoxluğunda $*$ binar cəbri əməli təyin olunub. Əgər istənilən $b \in G$ üçün $a * b = b$ və ya $b * a = b$ şərti ödənərsə, onda a elementinə G çoxluğunun $*$ cəbri əməlinə nəzərən neytral elementi deyilir.

Nümunə 2.

1. G çoxluğunun alt çoxluqları arasında birləşmə cəbri əməlinə nəzərən neytral element $\varnothing$ boş çoxluq elementidir;

2. G çoxluğunun alt çoxluqları arasında kəsişmə cəbri əməlinə görə G çoxluğu özü neytral elementdir;

3. Z tam ədədlər çoxluğunda toplama əməlinə görə sıfır – 0 neytral elementdir;

4. Z tam ədədlər çoxluğunda vurma əməlinə görə 1-vahid neytral elementdir.

G çoxluğunda toplama əməlinə görə neytral elementi adətən «sıfır element» adlandırırlar və «0» simvolu ilə işarə edirlər. Vurma əməlinə görə

neytral elementi isə «vahid element» adlandırırlar və «ε» və ya «e» və ya da «1» ilə işarə edirlər.

Lemma 1. Əgər G çoxluğunda $*$ cəbri əməlinə görə neytral element mövcuddursa, onda o, yeganədir.

İsbatı. Əksini fərz edək – fərz edək ki, G çoxluğunda iki neytral element mövcuddur. Bu elementləri e və e' ilə işarə edək. Aydındır ki, e neytral element olduğundan e' üçün də $e + e' = e'$ ödənəcək. Digər tərəfdən e' də neytral element olduğundan e elementi üçün də $e + e' = e$ münasibəti ödənəcək. Alınan münasibətləri müqayisə etsək $e = e'$ alarıq. □

Tutaq ki, G çoxluğunda $*$ cəbri əməli təyin olunub və e elementi bu əmələ nəzərən G çoxluğunda neytral elementdir. $a \in G$ elementi üçün $a * a' = e$ şərtini ödəyən $a' \in G$ elementinə a-nın $*$ əməlinə nəzərən simmetrik elementi deyilir.

Nümunə 3.

1. Tam ədədlər çoxluğunda verilmiş a elementinə + (toplama) əməlinə nəzərən simmetrik element «$-a$» ədədidir.

2. Rasional ədədlər çoxluğunda sıfırdan fərqli a elementinə $\times$ (vurma) əməlinə nəzərən simmetrik element «$\frac{1}{a}$» elementidir.

3. k-qiymətli məntiqdə verilmiş a elementinə $(a \neq 0)$ mod k üzrə toplama əməlinə nəzərən simmetrik element $k - a$ kimi (burada «-» işarəsi adı çıxma əməliyyatının işarəsidir) təyin olunan elementdir.

Cəbrlərin (cəbri sistemlərin) bir çox növləri mövcuddur. Qrup, halqa, meydan və bir sıra digər cəbri strukturları fundamental cəbri strukturlar adlandırırlar. Bəzi cəbri sistemləri görkəmli riyaziyyatçıların adları ilə adlandırırlar. Məsələn, Abel qrupu, Qalua meydanı, Kantor cəbri, Jeqalkin cəbri, Post cəbri, Rosser-Turgett sistemi, Klini cəbri və s.

Cəbri strukturların ən sadəsi bir cəbri əməlin təyin olunduğu sistemlərdir. Bunlara qruppoid, yarımqrup, monoid və qrup kimi sistemlər aiddir.

§2. Qruppoid, yarımqrup və monoid

Bir cəbri əməlin təyin olunduğu G çoxluğuna qruppoid deyilir. Deməli, qruppoiddə istənilən $a, b \in G$ üçün $a * b \in G$ şərti ödənir, harada

ki, $*$ əməli G çoxluğunda təyin olunan əməldir. Bu şərtdən başqa, əgər istənilən a, b və c üçün $*$ əməli $c*(a*b)=(c*a)*b$ şərtini də ödəyərsə onda G çoxluğuna assosiativ qruppoid və ya yarımqrup deyilir.

$*$ əməli toplama əməli olarsa, qruppoid və yarımqrupa uyğun olaraq additiv qruppoid və additiv yarımqrup deyilir.

$*$ əməli vurma əməli olarsa, bu halda G çoxluğuna multiplikativ qruppoid və ya multiplikativ yarımqrup deyilir.

Tutaq ki, G çoxluğu $*$ əməlinə nəzərən yarımqrupdur. Əgər $*$ əməlinə nəzərən G çoxluğunda neytral element olarsa, onda G çoxluğuna monoid deyilir. Analoji olaraq additiv və multiplikativ monoid anlayışları təyin olunur.

Əgər qruppoid, yarımqrup və monoiddə cəbri əməl kommutativlik xassəsinə malik olarsa, onda onlar uyğun olaraq kommutativ qruppoid, kommutativ yarımqrup və kommutativ monoid adlanırlar.

Əgər baxılan G çoxluğu sonlu isə, yəni sonlu sayda elementlərdən təşkil olunmuşdursa, onda götürülən cəbri əmələ nəzərən qruppoid, yarımqrup və monoid uyğun olaraq sonlu qruppoid, yarımqrup və monoid adlanır.

Nümunə 1.

1. Natural ədədlər çoxluğu adi toplama əməlinə nəzərən həm qruppoid və həm də yarımqrup əmələ gətirir;

2. Natural ədədlər çoxluğu adi vurma əməlinə nəzərən həm qruppoid və həm də yarımqrup əmələ gətirir;

3. Tam ədədlər çoxluğu həm adi toplama və həm də adi vurma əməllərinə nəzərən monoid əmələ gətirir;

4. $\{0,1,...,m-1\}$ ədədlər çoxluğu mod m üzrə toplama əməlinə nəzərən qruppoid, yarımqrup və monoid əmələ gətirir.

Yarımqrupları işarə etmək üçün uyğun daşıyıcı çoxluğun və cəbri əməlin mötərizə daxilində yazılışından istifadə olunur. Məsələn:

$(N,+)$ və $(N,\cdot)$ - uyğun olaraq adi toplama və adi vurma əməlinə nəzərən natural ədədlər çoxluğundan əmələ gəlmiş yarımqruplardır;

$(Z,+)$ və $(Z,\cdot)$ - uyğun olaraq adi toplama və adi vurma əməlinə nəzərən tam ədədlər çoxluğundan əmələ gəlmiş yarımqruplardır;

$(Q,+)$ və $(Q,\cdot)$-uyğun olaraq adi toplama və adi vurma əməlinə nəzərən rasional ədədlər çoxluğundan əmələ gəlmiş yarımqruplardır;

Bu yarımqruplardan $(Z,+)$ və $(Q,+)$ həm də monoid əmələ gətirirlər.

Əvvəlcə bir anlayışla tanış olaq. Tutaq ki, A və B çoxluqları verilmişdir və φ inikası A çoxluğunun elementlərini B çoxluğunun elementlərinə inikas etdirir: $\varphi : A \to B$. Əgər istənilən $b \in B$ üçün elə $a \in A$ mövcud olarsa ki, $\varphi(a) = b$ olsun, onda φ inikası suryektiv və ya üzərinə inikas adlanır.

Əgər istənilən $a', a'' \in A$ üçün $\varphi(a') = \varphi(a'')$ münasibətindən alınarsa ki, $a' = a''$, onda φ inikası inyektiv və ya daxilə inikas adlanır. İnyektiv inikas halında A çoxluğunun müxtəlif elementləri B çoxluğunun müxtəlif elementlərinə inikas olunur.

Əgər φ inikası eyni zamanda həm suryektiv və həm də inyektiv inikas olarsa, onda ona biyektiv inikas deyilir.

$S = (S,\circ)$ və $T = (T,*)$ kimi iki yarımqrupa baxaq.

Tutaq ki, φ inikası S çoxluğundan T çoxluğuna hər hansı bir inikasdır. Əgər istənilən $x, y \in S$ üçün $\varphi(x \circ y) = \varphi(x) * \varphi(y)$ olarsa, onda φ inikası homomorfizm və ya homomorf uyğunluq adlanır.

Verilən $S = (S,\circ)$ və $T = (T,*)$ yarımqrupları arasında homomorf φ inikası olarsa, onda S və T yarımqrupları arasında «$\circ$» və «$*$» əməllərinə nəzərən homomorf uyğunluq mövcuddur. φ homomorfizmi suryektiv inikas olarsa, onda S və T arasında münasibət epimorfizm, inyektiv olarsa, onda monomorfizm, biyektiv olduqda isə izomorfizm adlanır.

§ 3. Qrup anlayışı

1. Qrupların tərifi və onlara nümunələr. Qrup anlayışı cəbrin əsas anlayışlarından biridir və qrup dedikdə müəyyən bir cəbri struktur nəzərdə tutulur. Qruplara konkret nümunələr olmağına baxmayaraq onları ümumi halda tədqiq etmək üçün riyaziyyatda abstrakt qrup anlayışı daxil edilir.

Tərif 1. Tutaq ki, G çoxluğu verilmişdir və burada $*$ cəbri əməli təyin olunmuşdur. Əgər aşağıdakı xassələr ödənərsə, onda G çoxluğuna qrup deyilir:

1) *qapalılıq:* hər bir $a \in G$ və $b \in G$ elementlərindən ibarət cütlük üçün $c = a * b$ elementi G çoxluğuna daxildir;

2) *assosiativlik:* hər bir $a, b, c \in G$ üçün

$$a * (b * c) = (a * b) * c .$$

3) *neytral elementin mövcudluğu:* G çoxluğunda neytral adlanan e elementi mövcuddur və elədir ki, istənilən $a \in G$ elementi üçün

$$a * e = e * a = a .$$

4) *simmetrik elementin mövcudluğu:* G-dən olan istənilən a elementi üçün ona simmetrik adlanan elə b elementi mövcuddur ki,

$$a * b = b * a = e$$

ödənir.

Əgər G qrupunda sonlu sayda element mövcuddursa, onda ona sonlu qrup, elementlərin sayına isə G qrupunun tərtibi deyilir.

Bəzi qruplar aşağıdakı əlavə xassəyə malik olur: onların istənilən a və b elementi üçün

$$a * b = b * a .$$

Bu xassə kommutativlik xassəsi adlanır. Kommutativlik xassəsinə malik qruplar kommutativ və ya Abel qrupları adlanırlar.

Bəzi qruplarda qrup əməliyyatı $+$ ilə işarə olunur və toplama adlanır (hətta adi toplama əməliyyatı belə olmadığı halda). Bu halda neytral element sıfır adlanır və «0» ilə işarə olunur. a elementinə simmetrik olan element «$-a$» kimi yazılır, belə ki,

$$a + (-a) = (-a) + a = 0 .$$

Bəzən qrup əməliyyatı $\times$ ilə işarə olunur və vurma adlanır (hətta o adi hesabi vurma əməliyyatı olmadıqda belə). Bu halda neytral elementi vahid

adlanır və «1» ilə işarə olunur. a ədədinə simmetrik olan element «a^{-1}» kimi işarə olunur, belə ki,

$$a \cdot a^{-1} = a^{-1} \cdot a = 1 .$$

Teorem 1. Hər bir qrupda neytral element yeganədir. Qrupun hər bir elementinə simmetrik olan element də yeganədir və $(a^{-1})^{-1} = a$.

İsbatı. Tutaq ki, e və e' qrupun neytral elementləridir. Onda $e = e * e' = e'$. Tutaq ki, b və b' elementləri a elementinə simmetrik olan elementlərdir. Onda

$$b = b * (a * b') = (b * a) * b' = b'$$

Nəhayət, $a^{-1}a = aa^{-1} = 1$, beləliklə, a elementi a^{-1} elementinə simmetrik elementdir. Simmetrik elementin yeganəliyinə görə $(a^{-1})^{-1} = a$. □

Qruplara çoxlu nümunələr mövcuddur. Əksər qruplar sonsuz sayda elementdən ibarətdir.

Nümunə 1. Sonsuz qruplara nümunələr:

1. Adi toplama əməlinə görə tam ədədlər çoxluğu.
2. Adi vurma əməlinə nəzərən müsbət rasional ədədlər çoxluğu.
3. Matrislərin toplanması əməlinə nəzərən 2×2-ölçülü həqiqi qiymətli matrislər çoxluğu.

Bir çox qruplar ancaq sonlu sayda elementlərdən ibarət olur.

Nümunə 2. Sonlu qruplara nümunələr:

1. mod 2 üzrə toplama əməlinə görə $G = \{0,1\}$ çoxluğu.
2. mod 10 üzrə toplama əməlinə görə $G = \{0,1,...,8,9\}$ çoxluğu.
3. Vahidin n-ci dərəcədən kökləri çoxluğu kompleks ədədlərin vurulması əməlinə görə və i.a.

Bir qədər mürəkkəb nümunə kimi qeyri-abel qrupu quraq. Tutaq ki, bərabər tərəfli üçbucaq verilib və onun təpələri saat əqrəbi istiqamətində A, B və C ilə nömrələnib. Bu üçbucağı fırlatmaqla, yaxud oxa nəzərən əks etdirməklə altı qaydada özü-özünə inikas etdirmək olar, həm də bu inikasların tərs çevirmələri də mövcuddur. Çevirmələri $1, a, b, c, d$ və ℓ ilə işarə edək. Bu çevirmələr aşağıdakılardır:

$1 = (ABC \to ABC)$ (dəyişiklik yoxdur);

$a = (ABC \to CAB)$ (saat əqrəbi istiqamətində fırlanma);

$b = (ABC \to BCA)$ (saat əqrəbinin əks istiqamətində fırlanma);

$c = (ABC \to ACB)$ (A bucağının tənbölənina nəzərən əks olunma);

$d = (ABC \to CBA)$ (B bucağının tənbölənina nəzərən əks olunma);

$\ell = (ABC \to BAC)$ (C bucağının tənbölənina nəzərən əks olunma);

Burada $ABC \to BCA$ çevirməsi A təpəsinin B təpəsinə, B təpəsinin C təpəsinə, C təpəsinin A təpəsinə keçməsini göstərir. Beləliklə, üçbucaq 120^0 çevrilir. Tutaq ki, $(G,*)$ qrupu $G = \{1, a, b, c, d, \ell\}$ çoxluğu ilə təyin olunur və $y * x$ əməliyyatı əvvəlcə y çevirməsinin, sonra isə x çevirməsinin ardıcıl yerinə yetirilməsinin nəticəsini göstərir. Məsələn:

$$a * d = (ABC \to CAB) * (ABC \to CBA) = (ABC \to BAC) = \ell$$

Beləliklə, $x * y$ üçün aşağıdakı cədvəli qurmaq olar:

x \ y	1	a	b	c	d	ℓ
1	1	a	b	c	d	ℓ
a	a	b	1	d	ℓ	c
b	b	1	a	ℓ	c	d
c	c	ℓ	d	1	b	a
d	d	c	ℓ	a	1	b
ℓ	ℓ	d	c	b	a	1

Cədvəl qurulduqdan sonra, məsələnin həndəsi mənşəyini unutmaq olar. Cədvəl özü qrup təşkil edir. Qeyd edək ki, baxılan nümunə qeyri-abel qruplarına nümunədir, belə ki, $a * c \neq c * a$.

Dövri qruplar. Qrupların bir növü də dövri qrupdur. Eyni bir a elementinin müsbət və mənfi dərəcəli qüvvətlərindən (və ya müsbət və mənfi misillərindən) ibarət olan qrup dövri qrup adlanır. a elementi bu *qrupun doğuranı* adlanır. Aydındır ki, a^{-1} elementi də doğuran adlandırıla bilər.

$\ldots, a^{-n}, \ldots, a^{-1}, 1, a, \ldots, a^n, \ldots$ elementləri cüt-cüt müxtəlif ola bilərlər. Bu halda qrup sonsuz (və ya sərbəst) dövri qrup adlanır.

Sərbəst dövri qruplara toplama əməlinə nəzərən tam ədədlər çoxluğu nümunə ola bilər.

Dövri qrupun elementləri arasında bərabər olanları ola bilər. Əgər $k > m$ olduqda $a^k = a^m$ olarsa, onda $a^{k-m} = 1$. Beləliklə, doğuran elementin hər hansı bir dərəcəli qüvvəti vahidə bərabər olur. Bu şərti ödəyən ən kiçik natural dərəcəyə a elementinin *tərtibi* deyilir. Əgər a elementinin tərtibi n natural ədədidirsə, onda $1, a, a^2, ..., a^{n-1}$ elementləri arasında bərabər olanları yoxdur, çünki bərabər olanları olsaydı, onda onların dərəcələri fərqi n-dən kiçik olardı və bu da n-in tərtib olmasına ziddir. Hər bir a^m elementi $1, a, ..., a^{n-1}$ elementlərinin biri ilə, məsələn, a^r ilə üst-üstə düşür, harada ki, r ədədi m ədədi n-ə bölündükdə alınan qalıqdır.

Simmetrik qruplar. Qrupların başqa bir növü də simmetrik qruplardır. Simmetrik qrup verilmiş n natural ədədi halında n-ci dərəcəli əvəzləmələr çoxluğunun əvəzləmələrin vurulması əməlinə görə əmələ gətirdiyi qrupdur. Aydındır ki, əvəzləmələrin vurulması assosiativlik xassəsinə malikdir, lakin kommutativlik xassəsinə malik deyildir. Bu qrupda vahid kimi

$$E = \begin{pmatrix} 1 & 2 \dots n \\ 1 & 2 \dots n \end{pmatrix}$$

elementi çıxış edir. Verilən

$$S = \begin{pmatrix} 1 & 2 \dots n \\ i_1 & i_2 \dots i_n \end{pmatrix}$$

elementinə tərs element

$$S^{-1} = \begin{pmatrix} i_1 & i_2 \dots i_n \\ 1 & 2 \dots n \end{pmatrix}$$

əvəzləməsidir. Simmetrik qruplar abel qrupu deyildirlər.

2. Altqrup. Qonşuluq sinifləri. Tutaq ki, G hər hansı bir qrupdur və H isə G-nin hər hansı alt çoxluğudur. Əgər H çoxluğu G-də təyin olunan $*$ əməliyyatına görə qrup təşkil edirsə, onda H alt çoxluğuna G qrupunun altqrupu deyilir. Məsələn, cüt ədədlər çoxluğu və üçün misilləri olan ədədlər çoxluğu bütün tam ədədlər çoxluğunda toplama əməlinə görə altqruplardır.

Teorem 2. $(G,*)$ qrupunun H alt çoxluğunun altqrup olması üçün zəruri və kafi şərt aşağıdakıların olmasıdır:

1) $\forall\ a,b \in H$ üçün $a*b \in H$;

2) $a \in H$ üçün $a^{-1} \in H$.

İsbatı. Zərurilik. Tutaq ki, H alt çoxluğu $(G,*)$ qrupunun alt-qrupudur. Onda $\forall\ a,b \in H$ üçün $a*b \in H$ və $\forall\ a \in H$ üçün $a * a^{-1} = e$ şərtini ödəyən a^{-1} mövcuddur və $a^{-1} \in H$.

Kafilik. $\forall a,b \in H$ üçün $a*b \in H$ olması burada $*$ əməlinin təyin olunduğunu göstərir. $*$ əməlinin H-da assosiativlik şərtini ödəməsi əməliyyatda iştirak edən elementlərin həm də G qrupunun elementləri olmasından alınır.

Tutaq ki, $a \in H$. Şərtə görə $a^{-1} \in H$. Digər tərəfdən $a * a^{-1} \in H$. Bu isə o deməkdir ki, $e = a * a^{-1} \in H$. Bu isə onu göstərir ki, H çoxluğunun elementləri $*$ əməlinə görə qrupun bütün aksiomlarını ödəyir, yəni o, G qrupunun altqrupudur. □

G sonlu qrupunun H altqrupunu qurmaq üçün G qrupunun ixtiyari bir h elementini götürüb onu özü-özünə istənilən dəfə vurmaqla alınan elementlərdən ibarət alt çoxluğu götürmək lazımdır. Beləliklə, aşağıdakı elementlər ardıcıllığını alırıq:

$$h,\ h*h,\ h*h*h,... \qquad (1)$$

Burada $*$ əməli vurma əməli əvəzinə toplama əməli kimi də istifadə oluna bilər.

(1) ardıcıllıqlarını $h, h^2, h^3, h^4,...$ kimi işarə edək. G sonlu olduğundan bu elementlərin ancaq sonlu saydası bir-birindən fərqlənəcək. Odur ki, müəyyən həddən sonra bu elementlər təkrarlanmağa başlayacaq. İlk təkrarlanacaq element h özü olmalıdır, belə ki, əgər iki müxtəlif element h^i və h^j bərabərdirsə, onda onları h^{-1}-ə vurub h^{i-1} və h^{j-1} elementlərinin də bərabər olduğunu alarıq. Qeyd edək ki, əgər $h^j = h$-dırsa, onda $h^{j-1} = 1$ - qrupun vahid elementi olar. Belə qurulan H altqrupuna h elementinin doğurduğu altqrup deyilir və $\{h\}$ kimi işarə olunur. H qrupunda olan elementlərin c sayı h elementinin *tərtibi* adlanır. $h, h^2,..., h^c = 1$ elementlər çoxluğu *dövr* adlanır. Dövr altqrupdur,

belə ki, belə növ iki elementin hasili də belə növ elementdir, h^i elementinə tərs element isə h^{c-i} elementidir və uyğun olaraq dövrün elementlərindən biridir. Yuxarıda deyildiyi kimi bir elementinin dərəcələrindən ibarət olan qrupa dövri qrup deyilir.

Verilmiş G qrupu və H altqrupu arasında bir mühüm əməliyyat mövcuddur. Bu əməliyyat G qrupunun H-a görə qonşuluq siniflərinə (yaxud da yanaşı siniflərinə) bölünməsi əməliyyatı adlanır. $h_1, h_2, h_3, ..., h_n$ ilə H altqrupunun elementlərini işarə edək və həm də h_1 ilə vahid elementi $(h_1 = 1)$ işarə edək. Cədvəl aşağıdakı kimi qurulur: Birinci sətrin elementləri H altqrupunun elementlərindən ibarət olur, həm də sətrdə soldan ilk olaraq h_1 vahid element yazılır və hər bir element sətrdə bircə dəfə yazılır. G qrupunun birinci sətrə daxil olmayan ixtiyari bir elementini götürək, onu g_2 adlandıraraq ikinci sətrin birinci elementi kimi götürək. İkinci sətrin qalan elementləri H altqrupunun elementlərinin bu g_2 elementinə sağdan vurulması nəticəsində alınır. Analoji olaraq üçüncü, dördüncü, beşinci və i.a. sətrlərin elementləri qurulur: hər dəfə birinci element kimi G qrupunun əvvəlki sətrlərdə olmayan ixtiyari bir elementi götürülür və i.a. Təbii ki, G -nin elementlərinin sayı sonlu olduğundan hər hansı bir addımdan sonra məlum olur ki, G -nin əvvəlki sətrlərdə iştirak etməyən elementləri artıq yoxdur. Bu zaman qurma prosesi qurtarır. Nəticədə aşağıdakı cədvəl alınır:

$$\begin{array}{ccc} h_1 = 1 & h_2 & h_3 \ldots h_n \\ g_2 * h_1 = g_2 & g_2 * h_2 & g_2 * h_3 \ldots g_2 * h_n \\ g_3 * h_1 = g_3 & g_3 * h_2 & g_3 * h_3 \ldots g_3 * h_n \\ \vdots & \vdots & \vdots \\ g_m * h_1 = g_m & g_m * h_2 & g_m * h_3 \ldots g_m * h_n \end{array}$$

Cədvəldə soldan birinci element *qonşuluq sinfinin lideri* adlanır. Cədvəlin hər bir sətri *sol qonşuluq (yanaşı) sinifi* adlanır, abel qrupları halında isə sadəcə olaraq qonşuluq sinifi adlanır. Əgər qurma prosesində element soldan vurularsa, onda sətrlər *sağ qonşuluq sinifləri* adlanır.

Ümumi halda, G qrupunun x elementinin ixtiyari bir H altqrupuna görə doğurduğu sol yanaşı sinif xH ilə işarə olunur və aşağıdakı kimi təyin olunur:

$$xH = \{x * a \mid a \in H\}.$$

Analoji olaraq sağ yanaşı sinif - Hx sinfini də təyin etmək olar. xH və Hx yanaşı sinifləri halında x elementi onların doğuranı adlanır.

Teorem 3. G qrupu qonşuluq siniflərinə ayrıldıqda hər bir element ancaq və ancaq bircə dəfə rast gəlinir.

İsbatı. Hər bir element heç olmazsa bircə dəfə rast gəlinir. Əks halda qurma prosesi dayandırılmaz. İsbat edək ki, eyni bir element bir sətrdə iki dəfə rast gələ bilməz və həm də eyni bir element iki müxtəlif sətrdə rast gələ bilməz.

Tutaq ki, eyni bir sətrin iki elementi - $g_i * h_j$ və $g_i * h_k$ - elementləri eynidir: $g_i * h_j = g_i * h_k$. Bu münasibətin hər tərəfini soldan g_i^{-1}-ə vurduqda $h_j = h_k$ alırıq. Bu isə H altqrupunun elementlərinin birinci sətrdə ancaq bir dəfə yazılmasına ziddir.

Tutaq ki, müxtəlif sətrlərdə yerləşən iki element eynidir, yəni $g_i * h_j = g_k * h_\ell$ və $k < i$. Sonuncu bərabərliyi sağdan h_j^{-1}-ə vuraq. Onda alarıq:

$$g_i = g_k * h_\ell * h_j^{-1}.$$

Buradan çıxır ki, g_i elementi k-cı qonşuluq sinfini doğurur, belə ki, $h_\ell * h_j^{-1}$ elementi H altqrupuna məxsusdur. Bu isə yuxarıda göstərilən qaydaya ziddir. □

Yanaşı siniflərə aid bəzi faktları da qeyd edək (aydındır ki, bu faktlar asanlıqla isbat oluna bilər):

1. Hər bir xH yanaşı sinfinə x doğuranı da daxildir.
2. Yanaşı sinfin hər bir elementi bu sinfin doğuranıdır.

Teorem 3 və bu faktları nəzərə alaraq G qrupununu onun kəsişməyən yanaşı siniflərinə nəzərən ayırmaq olar. Tutaq ki, G qrupunun elementləri $x_0 = e, x_1, ..., x_{k-1}$-dir. H isə istənilən alt- qrupdur. Onda

$$G = H \bigcup x_1 H \bigcup ... \bigcup x_{k-1} H$$

və ya

$$G = H \bigcup Hx_1 \bigcup ... \bigcup Hx_{k-1}.$$

Teorem 4 (Laqranj teoremi). Əgər H altqrupu sonlu G qrupunun altqrupudursa, onda H altqrupunun tərtibi G qrupunun tərtibinin bölənidir.

İsbatı. Tutaq ki, G sonlu qrupunun tərtibi n, H altqrupunun tərtibi k, G qrupunun bir-biri ilə üst-üstə düşməyən yanaşı siniflərinin sayı isə s-dir. G qrupunun kəsişməyən yanaşı siniflərə ayrılışına baxaq:

$$G = H \cup x_1 H \cup ... \cup x_{s-1} H \ . \qquad (2)$$

H- altqrupunda k sayda element və $H, x_1 H, ..., x_{s-1} H$ sinifləri ortaq elementlərə malik olmadıqlarından (2)-in sağ tərəfində alınan çoxluqda $n \cdot k$ sayda element olar. (2) ayrılışından aydın olur ki, $n = k \cdot s$. Bu isə o deməkdir ki, k ədədi n-in bölənidir. □

Bu teoremdən aşağıdakı nəticələr alınır :

Nəticə 1. Sonlu qrupun tərtibi onun istənilən elementinin tərtibinə bölünür.

Nəticə 2. Sonlu qrupun tərtibi sadə p ədədidirsə, onda qrup dövri qrupdur.

§4. Halqa

Halqalar abel qrupudur və bundan başqa əlavə xassələrə də malikdirlər.

Tərif 1. R halqası toplama ($+$ ilə işarə olunur) və vurma (vuruqlar yanaşı yazılmaqla işarə olunur və ya $\times$ yaxud $\cdot$ ilə işarə olunur) əməllərinin təyin olunduğu çoxluqdur və bu əməllər üçün aşağıdakı aksiomlar nəzərdə tutulur:

1) toplama $(+)$ əməlinə görə R çoxluğu abel qrupudur;

2) qapalılıq: istənilən $a, b \in R$ üçün ab hasili R-ə daxildir;

3) assosiativlik qanunu: $a(bc) = (ab)c$;

4) distributivlik qanunu:

$$a(b+c) = ab + ac, \quad (b+c)a = ba + ca \ .$$

Halqada toplama həmişə kommutativdir, vurmanın kommutativ olması vacib deyildir. *Kommutativ halqa* dedikdə vurma əməlinin kommutativ olması, yəni istənilən $a, b \in R$ üçün $ab = ba$ olması nəzərdə tutulur.

Distributivlik qanunu vurma və toplama əməlini bir-biri ilə əlaqələndirir. Bu qanundan aşağıdakı nəticələr çıxır:

Teorem 1: R halqasında istənilən a və b elementləri üçün:

1) $a0 = 0a = 0$,

2) $a(-b) = (-a)b = -(ab)$.

İsbatı. 1) $a0 = a(0+0) = a0 + a0$. Bu bərabərliyin hər tərəfindən $a0$-ı çıxsaq, onda $0 = a0$ alarıq. İkinci hissə analoji isbat olunur.

2) $0 = a0 = a(b-b) = ab + a(-b)$. Beləliklə, $a(-b) = -(ab)$. İkinci hissə analoji isbat olunur. □

Halqada toplama əməli neytral elementə malikdir və bu da sıfır adlanır və 0 kimi yazılır. Vurma əməlinin neytral elementinin olması zəruri deyildir, lakin varsa, o yeganədir. Vurma əməlinə görə neytral elementinə malik halqaya *vahidli halqa* deyilir. Bu neytral element vahid adlanır və 1 simvolu ilə işarə olunur. Onda R-dən olan bütün a elementləri üçün aşağıdakı bərabərlik doğrudur:

$$1a = a1 = a.$$

Toplama əməlinə görə hər bir element simmetrik (əks) elementə malikdir. Vurma əməlinə görə verilən elementə simmetrik (tərs) olan elementin olması o qədər də vacib deyildir, lakin vahidli halqada tərs element ola bilər. Bu o deməkdir ki, verilən a elementi üçün elə b elementi mövcud ola bilər ki, $ab = 1$ olsun. Əgər bu belə olarsa, onda b elementi a elementinə sağ tərs element adlanır. Analoji olaraq, əgər elə c elementi varsa ki, $ca = 1$, onda c elementi a elementinə sol tərs element adlanır. Əgər a elementi həm b sağ tərs və həm də c sol tərs elementə malikdirsə, onda a elementi tərsi ola bilən (dönən) element adlanır.

Teorem 2. Vahidli halqada aşağıdakılar doğrudur: 1) Vahid yeganədir; 2) əgər a tərsi ola bilən elementdirsə, onda ona tərs olan element yeganədir (və a^{-1} kimi işarə olunur); 3) $(a^{-1})^{-1} = a$.

Teoremin isbatı teorem 1-in isbatına analoji aparılır.

Vahidli halqanın tərsi ola bilən elementləri *vahid* adlanır. Halqada bütün vahidlər çoxluğu vurma əməlinə görə qapalıdır, belə ki, əgər a və b vahidlərdirsə, onda $c = ab$ tərs elementə malikdir və bu tərs element $c^{-1} = b^{-1}a^{-1}$-dir.

Teorem 3. Halqada aşağıdakılar doğrudur: 1) Halqada vahidlər çoxluğu halqanın vurma əməlinə görə qrup əmələ gətirir; 2) Əgər $c = ab$ və c -vahiddirsə, onda a sağ tərs, b isə sol tərs elementə malikdir.

İsbatı bilavasitə yoxlamaqla həyata keçirmək olar.

Nümunə 1. Halqalara aşağıdakı nümunələri göstərmək olar:

1. Bütün həqiqi ədədlər çoxluğu adi toplama və vurma əməlinə nəzərən vahidli kommutativ halqa əmələ gətirir.

2. Bütün tam ədədlər çoxluğu adi toplama və vurma əməlinə görə vahidli kommutativ halqa əmələ gətirir. Bu halqa Z kimi işarə olunur. Onun vahidləri ancaq ± 1 -dir.

3. Elementləri həqiqi ədədlər olan $(n \times n)$ - ölçülü kvadrat matrislər çoxluğu matrislərin toplanması və vurulması əməllərinə nəzərən kommutativ olmayan vahidli halqa əmələ gətirir. Vahid kimi $(n \times n)$ - ölçülü vahid matris nəzərdə tutulur. Bütün cırlaşmayan matrislərin tərsi mövcuddur və bunlar vahidlərdir.

4. Elementləri tam ədədlər olan $(n \times n)$ - ölçülü matrislər çoxluğu matrislərin toplanması və vurulması əməlinə nəzərən kommutativ olmayan vahidli halqa əmələ gətirir.

5. x dəyişənindən asılı həqiqi əmsallı bütün çoxhədlilər çoxluğu çoxhədlilərin toplanması və vurulması əməlinə görə vahidli kommutativ halqa əmələ gətirir. Halqanın vahidi sıfır dərəcəsinə malik $p(x) = 1$ çoxhədlisidir.

İxtiyari halqalarda cəbri əməllər ədədlər üzərində əməllərin bir sıra xassələrinə malik ola bilərlər. Lakin nəzərə almaq lazımdır ki, toplama və vurmanın ədədlər üzərində heç də bütün xassələri ixtiyari halqalarda saxlanılmır. Məsələn, ədədlər üzərində vurma əməlində nəzərdə tutulur ki, əgər iki ədədin hasili sıfıra bərabərdirsə, onda onlardan heç olmazsa biri sıfıra bərabərdir. Lakin bu xassə bütün halqalara şamil oluna bilməz. Bəzi halqalarda elə a və b elementləri cütü göstərmək olar ki, $a \neq 0$ və $b \neq 0$, lakin $a \cdot b = 0$ olsun. Bu xassəyə malik a və b elementləri sıfırın bölənləri adlanır.

Ədədi halqalarda (elementləri ədədlər olan halqalar), ədədi əmsallardan ibarət çoxhədlilər halqasında sıfırın bölənləri yoxdur. Funksiyalar halqasının çoxunda sıfırın bölənləri mövcuddur. Qeyd edək ki, hər bir funksiyalar halqasında sıfır element x-in bütün qiymətlərində sıfra

bərabər qiymət alan funksiyadır. x-ın bütün həqiqi qiymətlərində təyin olunmuş aşağıdakı $f(x)$ və $g(x)$ funksiyalarını quraq:

$$f(x)=\begin{cases}0, & \text{əgər } x\le 0\\ x, & \text{əgər } x>0\end{cases},\quad g(x)=\begin{cases}x, & \text{əgər } x\le 0\\ 0, & \text{əgər } x>0\end{cases}.$$

Aydındır ki, həm $f(x)$ və həm də $g(x)$ sıfırdan fərqlidir, lakin $f(x)\cdot g(x)$ hasili sıfra bərabərdir.

Əgər $a\cdot b=0$, harada ki, $a\neq 0, b\neq 0$, onda a və b elementlərinə uyğun olaraq sıfırın sağ və sol bölənləri deyilir. Sıfırın bölənləri olmayan kommutativ halqaya *tamlıq oblastı* deyilir. Məsələn, adi toplama və vurma əməllərinə nəzərən halqa əmələ gətirən ədədi çoxluqlar tamlıq oblastıdır.

Tamlıq oblastı olmayan halqalara yuxarıda göstərilən funksiyalar halqasından başqa iki tərtibli matrislər halqasını da nümunə göstərmək olar. Məsələn, bu halqada

$$A=\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}\neq 0,\qquad B=\begin{pmatrix}0 & 0\\ 1 & 3\end{pmatrix}\neq 0$$

olduğu halda, yəni iki tərtibli sıfır matrisdən fərqli olduğu halda $A\cdot B=0$ olur.

Tərif 2. K halqasının boş olmayan H alt çoxluğu öz növbəsində K-da təyin olunan toplama və vurma cəbri əməllərinə nəzərən halqa əmələ gətirərsə, onda H-a K-ın althalqası deyilir.

Nümunə 2. Alt halqalara aşağıdakı nümunələri göstərmək olar:

1. Cüt ədədlər halqası tam ədədlər halqasının alt halqasıdır.

2. $x=a+\sqrt{2}$ şəklində olan ədədlər çoxluğunun əmələ gətirdiyi halqa həqiqi ədədlər halqasının alt halqasıdır.

3. Hər bir halqanın özü və onun sıfır elementi onun alt halqasıdır.

Asanlıqla isbat etmək olar:

Teorem 4. K halqasının boş olmayan H alt çoxluğunun alt- halqa olması üçün zəruri və kafi şərt aşağıdakı şərtlərin ödənməsidir:

1. $\forall a,b\in H$ üçün $a-b\in H$;

2. $\forall a,b\in H$ üçün $a\cdot b\in H$.

Tərif 3. K halqasının H althalqası özünün hər bir $a\in H$ elementi ilə K halqasının x elementinin ax hasilini (xa hasilini) öz daxilinə alarsa, onda H-a K halqasının sol (sağ) idealı deyilir.

K halqasının eyni zamanda həm sol və həm də sağ idealı olan H althalqasına ikitərəfli ideal və sadəcə ideal deyilir.

Aydındır ki, kommutativ halqada sol ideal həm də sağ ideal olur və əksinə.

Teorem 5. K halqasının H althalqasının sağ (sol) ideal olması üçün zəruri və kafi şərt aşağıdakı şərtlərin ödənməsidir:

1. $\forall a,b \in H$ üçün $a \pm b \in H$;
2. $x \in K$ və $a \in H$ üçün $ax \in H (xa \in H)$.

Nümunə 3. Halqanın ideallarına aşağıdakı nümunələri göstərmək olar:

1. Hər bir halqa özü-özünün idealıdır. Bu halqa vahid ideal adlanır.
2. Tam ədədlər halqasında qeyd olunmuş m ədədi üçün onun misilləri çoxluğu tam ədədlər halqasının idealıdır.
3. n tərtibli kvadrat matrislər halqasında sonuncu sütunu (sətri) sıfırlardan ibarət olan matrislər çoxluğu matrislər halqasının sol (sağ) idealıdır.
4. Sıfır althalqa iki tərəfli idealdır və bu sıfır ideal adlanır.

Vahid və sıfır ideallardan başqa digər idealları olmayan halqalara *sadə halqalar* deyilir.

Halqa, althalqa, ideal anlayışlarında baş ideal anlayışı da böyük əhəmiyyət kəsb edir.

Yalnız bir elementin doğurduğu ideala *baş ideal* deyilir. Deməli, baş ideal hər hansı bir elementin misillərindən ibarət olan idealdır. Əgər element a elementidirsə, onda uyğun ideal (a) ilə işarə olunur.

Doğuranları birdən çox sayda elementlərdən ibarət olan ideallar da mövcuddur. Məsələn, $a_1, a_2, ..., a_n$ elementlərinin doğurduğu ideal elementləri

$$\sum_{i=1}^{n} x_i a_i + \sum_{i=1}^{n} n_i a_i$$

kimi təyin olunan çoxluğun əmələ gətirdiyi idealdır. Belə ideal adətən $(a_1, a_2, ..., a_n)$ kimi yazılır, $a_1, a_2, ..., a_n$ elementləri isə idealın bazisi adlandırılır.

a elementini özündə saxlayan ideallar arasında (a) baş idealı ən kiçik ideal adlanır.

Xüsusi halda hər hansı bir halqanın (0) idealı (sıfır idealı) baş ideal, halqada 1 vahidi varsa, onda (1) idealı baş ideal olur.

Vahid elementi olan tamlıq oblastının baş idealı olarsa, onda bu halqa baş ideallar halqası adlanır. Buna nümunə olaraq aşağıdakıları göstərmək olar:

1. Tam ədədlər halqası.
2. Birdəyişənli çoxhədlilər halqası.

Tutaq ki, R assosiativ, kommutativ və vahidli tamlıq oblastıdır. Tutaq ki, $\varepsilon \in R$ elementi üçün elə $\varepsilon^{-1} \in R$ mövcuddur ki, $\varepsilon \cdot \varepsilon^{-1} = 1$ olur. Təyinə görə ε elementi tərsi olan və ya vahid element adlanır. Bir-birindən vahid vuruqla fərqlənən elementlər assosiasiya olunmuş elementlər adlanır. Aydındır ki, istənilən element assosiasiya olunmuş elementlərə və vahidə bölünür. Belə bölənlər trivial bölənlər adlanır. Trivial bölənlərdən başqa bölənləri olmayan elementlərə ayrıla bilməyən və ya sadə elementlər deyilir. R halqasının istənilən elementlərinin ayrıla bilməyən elementlərin hasili şəklində təsvir edilə bilməsi xarakteri R halqasında böyük əhəmiyyətə malikdir. Əgər istənilən element üçün belə təsvir mövcuddursa və vuruqların yazılma ardıcıllığı və vuruqların assosiativ vuruqlarla əvəzlənməsi dəqiqliyi ilə yeganədirsə, onda R halqasına faktor halqa deyilir.

Faktor halqalara nümunə olaraq tam ədədlər halqasını göstərmək olar. Bu halqada iki vahid element – «1» və «-1» elementləri mövcuddur. Ayrıla bilməyən elementlər sadə ədədlərdir. Bu halqada ədədlərin sadə ədədlər vasitəsilə kanonik təsvirləri haqqında teorem qüvvədədir. Odur ki, tam ədədlər halqası faktor halqadır.

Hər hansı bir K çoxluğu üzərində olan, yəni əmsalları bu çoxluqdan olan bir dəyişənli çoxhədlilər çoxluğuna baxaq.

Tutaq ki, K çoxluğu kompleks ədədlər çoxluğudur. Baxılan çoxhədlilərin $K[x]$ çoxluğu çoxhədlilərin K çoxluğu üzərində toplanması və vurulması əməllərinə görə halqa əmələ gətirir. $K[x]$ halqasında ayrıla bilməyən elementlər ancaq bir dərəcəli çoxhədlilərdir və $x - c$ şəklində xətti ikihədlilərlə assosiasiya olunandırlar.

$K[x]$ halqasında vahid elementlər K çoxluğunun sıfır elementindən başqa yerdə qalan sıfır dərəcəli çoxhədlilərdir. İstənilən $n \geq 2$ halında n dərəcəli istənilən çoxhədli üçün yeganə

$$f(x) = a_0(x - c_1)(x - c_2)...(x - c_n)$$

ayrılışı qüvvədə olduğundan $K[x]$ halqası faktorial halqadır. Bu halqada bir-birindən K-dan olan vuruqla fərqlənən çoxhədlilər assosiasiya olunan elementlərdir.

§5. Meydan anlayışı. Sonlu meydanların növləri

Qeyd edək ki, qrup elementləri arasında toplamanın və çıxmanın mümkün olduğu, halqa isə elementləri arasında toplamanın, çıxmanın və vurmanın mümkün olduğu çoxluqdur. Nisbətən daha güclü cəbri struktur meydan adlanan strukturdur və bu da elementləri arasında toplama, çıxma, vurma və bölmə əməllərinin mümkün olduğu çoxluqdur.

Tutaq ki, G çoxluğunada toplama (+ ilə işarə olunur) və vurma ($\times$ yaxud $\cdot$ ilə işarə olunur və ya da vuruqlar yanaşı yazılmaqla işarə olunur) əməli təyin olunmuşdur.

Tə'rif 1. G çoxluğunada toplama və vurma əməllərinə görə aşağıdakı aksiomlar qüvvədə olarsa, onda ona bu əməllərə görə meydan deyilir:

1) Çoxluq toplamaya görə abel qrupu əmələ gətirir;

2) Çoxluq vurma əməlinə görə qapalıdır və sıfır elementdən fərqli elementlər vurmaya görə abel qrupu əmələ gətirir;

3) Distributivlik qanunu: istənilən a, b və c üçün

$$(a + b)c = ac + bc .$$

Meydanda toplamaya nəzərən neytral elementin «0» ilə işarə olunması qəbul edilib, a elementinə toplamaya nəzərən simmetrik olan element (additiv tərs) «$-a$» ilə, vurmaya görə neytral elementi «1» ilə, a elementinə vurmaya nəzərən simmetrik olan element (multiplikativ tərs) «a^{-1}» ilə işarə olunması qəbul olunub. $a - b$ çıxma əməli «$a + (-b)$», a / b bölmə əməli «$b^{-1} a$» kimi başa düşülür.

Meydana aşağıdakı nümunələri göstərmək olar:

1) R - həqiqi ədədlər çoxluğu;
2) C - kompleks ədədlər çoxluğu;
3) Q - rasional ədədlər çoxluğu.

Bütün bu meydanlar sonsuz sayda elementdən ibarətdir. Sonlu sayda elementə malik meydanlar da maraq kəsb edir. q sayda elementdən ibarət meydan sonlu meydan yaxud Qalua meydanı adlanır və $GF(q)$ ilə işarə olunur.

Ən kiçik meydan necədir və hansı elementlərdən ibarətdir? Ən kiçik meydan sıfır və vahid elementdən ibarət olmalıdır.

0 və 1 ədədlərindən ibarət meydan $GF(2)$ meydanıdır və ondan kiçik meydan yoxdur. Qalua meydanlarına $GF(3)=\{0,1,2\}$ və $GF(4)=\{0,1,2,3\}$ meydanları da aiddir. Bu meydanlarda toplama və vurma şəkil 1-də verilən cədvəllərdəki kimidir:

$GF(2)$

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

$GF(3)$

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$GF(4)$

+	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

Şəkil 1. Sonlu meydanlara nümunələr

$GF(3)$ meydanında toplama və vurma əməlləri mod 3 üzrə əməllərdir. Qeyd edək ki, $GF(4)$-də toplama və vurma mod 4 üzrə toplama və vurma deyildir. $GF(2)$ meydanı $GF(4)$ meydanına aiddir, lakin $GF(3)$ meydanına aid deyildir.

Tə'rif 2. Tutaq ki, F-hər hansı bir meydandır. F-dən olan hər hansı bir alt çoxluq F-də təyin olunan toplama və vurma əməlinə görə meydan olarsa, onda bu çoxluq F-də altmeydan, F isə bu alt meydanın genişlənməsi meydanı adlanır.

Sonlu meydanın alt çoxluğunun altmeydan olmasını isbat etmək üçün, onun sıfırdan fərqli elementə və toplama və vurma əməlinə görə qapalı olmasını isbat etmək kifayətdir. Qalan xassələr F meydanından altmeydana keçir. β elementinin toplama və vurmaya görə simmetrik elementi β elementinin uyğun olaraq toplama və vurmaya görə doğurduğu dövri qrupa daxil olur.

İndi isə meydanlar üçün böyük əhəmiyyətə malik olan meydanın xarakteristikası anlayışı ilə tanış olaq.

Tutaq ki, $k \cdot 1$ və $\ell \cdot 1$ P meydanının vahidinin uyğun olaraq k və ℓ misilləridir. Əgər $k \neq \ell$ olduqda $k \cdot 1 \neq \ell \cdot 1$ olarsa, onda deyirlər ki, P meydanı sıfır xarakteristikasına malikdir. Yuxarıda adı çəkilən R həqiqi ədədlər, Q rasional ədədlər və C kompleks ədədlər meydanı sıfır xarakteristikalı meydanlardır.

Əgər elə k və ℓ tam ədədləri mövcuddursa ki, $k > \ell$ və $k \cdot 1 = \ell \cdot 1$ ödənir, onda $(k - \ell) \cdot 1 = 0$, yəni P meydanında vahidin sıfıra bərabər olan müsbət misli mövcuddur. Bu halda P meydanına sonlu xarakteristikalı meydan deyilir. P meydanında $k \cdot 1 = 0$ şərtini ödəyən ən kiçik müsbət k ədədi P meydanının xarakteristikası adlanır. Sonlu xarakteristikalı meydanlara sonlu meydanları nümunə göstərmək olar. Sonlu xarakteristikalı sonsuz meydanlar da mövcuddur.

Teorem 1. Əgər P meydanı p xarakteristikasına malikdirsə, onda p sadə ədəddir.

İsbatı. Əksini fərz edək. Fərz edək ki, p mürəkkəb ədəddir, yəni $p = s \cdot t$, harada ki, $s < p, t < p$. Beləliklə, $(s \cdot 1) \cdot (t \cdot 1) = p \cdot 1 = 0$. Meydanda sıfırın bölənləri olmadığı üçün ya $s \cdot 1 = 0$, ya da ki, $t \cdot 1 = 0$. Lakin bu nəticələr p ədədinin meydanın xarakteristikası olması şərtinə ziddir. Deməli p sadə ədəddir. □

Teorem 2. Əgər P meydanın xarakteristikası p ədədidirsə, onda bu meydanın istənilən a elementi üçün $pa = 0$ olur.

İsbatı. Doğrudan da

$$pa = a(p \cdot 1) = a \cdot 0 = 0.$$ □

Teorem 3. Tutaq ki, P meydanının xarakteristikası 0 ədədi, a bu meydanın elementi, n isə tam ədəddir. Əgər $a \neq 0$ və $n \neq 0$, onda $na \neq 0$.

İsbatı. Əksini fərz edək: $na = 0$. Onda bu bərabərlikdən $a(n \cdot 1) = 0$ alınır. Buradan da $a \neq 0$ olduqda $n \cdot 1 = 0$ alınar. Buradan meydan sıfır xarakteristikalı meydan olduğundan $n = 0$ olur. Bu isə şərtə ziddir. Deməli, $na \neq 0$. □

Meydan halqanın bütün xassələrinə və həmçinin mühüm xassə olan həmişə ixtisar xassəsinə malikdir. İxtisar bölmənin zəif forması hesab olunur və mənası o deməkdir ki, əgər $ab = ac$ isə, onda $b = c$-dir.

Teorem 4. Əgər ixtiyari bir meydanda $ab = ac$ və $a \neq 0$ isə, onda $b = c$ -dir.

İsbatı. İsbat üçün hər tərəfi a^{-1}-ə vurmaq lazımdır. □

Bəzi halqalar ixtisar xassəsinə malik ola bilərlər, lakin meydan olmaya bilərlər. Buna sadə nümunə tam ədədlər halqasıdır. Bu halqada ixtisar mümkündür, lakin o meydan deyildir, çünki a^{-1} elementi təyin olunmayıb. İxtisarın mümkün olduğu halqa xüsusi ada malikdir.

§6. Tam ədədlər halqası və ona əsaslanan sonlu meydanlar

Bütün tam ədədlər çoxluğu adi toplama və vurma əməlinə görə halqa əmələ gətirir. Bu halqa Z ilə işarə olunur.

Əgər $ra = s$ olarsa, onda deyirlər ki, s tam ədədi r tam ədədinə bölünür (və ya r ədədi s-in bölənidir), harada ki, a hər hansı bir tam ədəddir. Əgər r ədədi s ədədini bölürsə və həm də ona bölünürsə, onda $r = \pm s$. Həqiqətən də, hər hansı tam a və b ədədləri üçün $r = sa$ və $s = rb$ olarsa, onda $r = rab$ alarıq və, beləliklə, $ab = 1$ alarıq. a və b tam olduğundan onlar ya «1» , ya da ki, «-1» ola bilərlər.

$p > 1$ şərtini ödəyən tam müsbət ədəd ancaq $\pm p$ və ya ± 1-ə bölünərsə, onda ona sadə ədəd deyilir. Birdən böyük olan və sadə olmayan müsbət tam ədədə mürəkkəb ədəd deyilir. r və s ədədlərinin ən böyük ortaq böləni (ƏBOB) bu iki ədədi bölən ən böyük tam ədədə deyilir və ƏBOB (r, s) kimi işarə olunur. r və s tam ədədlərinin ən kiçik ümumi

bölünəni (misilləri) ƏKOB (r,s) kimi işarə olunur və bu ədədlərin hər ikisinə bölünən ən kiçik tam ədədə deyilir. İki ədədin ƏBOB-u 1-ə bərabərdirsə, onda onlara qarşılıqlı sadə ədədlər deyilir.

Ümumi halda tam ədədlər halqasında bölmə əməli heç də həmişə təyin olunmayıb. Lakin bu halqada ixtisar və qalıqlı bölmə kimi əməliyyatlar mümkündür.

Teorem 1 (Qalıqlı bölmə alqoritmi). Hər bir c və d tam ədədləri cütü üçün $(d \neq 0)$ elə yeganə q (natamam qismət) və s (qalıq) tam ədədləri tapıla bilər ki, $c = dq + s$ olsun, belə ki, $0 \le s \le |d|$.

Əgər $c = d \cdot q + s$, $0 \le s \le |d|$ isə, onda $s = R_d[c]$ kimi işarə olunur, yəni s ədədi c ədədinin d ədədinə bölünməsindən alınan qalıqdır. Bunu aşağıdakı kimi də yazmaq olar:

$$s \equiv c \pmod{d}.$$

Belə münasibət müqayisə adlanır və «s və c ədədi modul d-yə görə müqayisə olunandır» oxunur.

Teorem 2. Aşağıdakı münasibətlər doğrudur:

1) $R_d[a+b] = R_d\{R_d[a] + R_d[b]\}$,

2) $R_d[a \cdot b] = R_d\{R_d[a] \cdot R_d[b]\}$.

ƏBOB(r,s) qalıqlı bölmə alqoritminin iterativ tətbiqi ilə müəyyən edilə bilər. Tutaq ki, $r < s$ və hər iki ədəd müsbətdir. Onda alqoritm aşağıdakı kimi olur:

$$\begin{aligned} s &= q_1 \cdot r + r_1, && r_1 < r, \\ r &= q_2 \cdot r_1 + r_2, && r_2 < r_1 \\ r_1 &= q_3 \cdot r_2 + r_3, && r_3 < r_2, \\ &\dots \\ r_{n-2} &= q_n\ r_{n-1} + r_n, && r_n < r_{n-1}, \\ r_{n-1} &= q_{n+1} \cdot r_n. \end{aligned} \qquad (1)$$

İterativ proses alınan qalıq sıfra bərabər olduqda saxlanılır.

Teorem 3 (Evklid alqoritmi). Tutaq ki, r və s müsbət tam ədədlərdir və $s > r$. Onda s və r-in ən böyük ortaq böləni (1) rekurrent düsturlarında son sıfırdan fərqli qalığa bərabərdir, yəni

$$\text{ƏBOB}\ (r,s) = r_n.$$

Nəticə 1. İstənilən r və s tam ədədləri üçün elə a və b ədədləri mövcuddur ki,

$$\text{ƏBOB } (r,s) = ar + bs$$

ödənir.

İsbatı. Teoremin şərtinə görə ƏBOB $(r,s) = r_n$. Yuxarıdakı ifadələrdən axırdan əvvəlki bərabərlikdən başlayaraq alarıq:

$$r_n = r_{n-2} - q_n r_{n-1},$$
$$r_{n-1} = r_{n-3} - q_{n-1} r_{n-2},$$
$$\dots$$
$$r_2 = r - q_2 \cdot r_1,$$
$$r_1 = s - q_1 \cdot r.$$

Bu münasibətlərdə r_1-in qiymətini r_2-də r_1 və r_2-in qiymətini r_3-də və i.a. nəzərə almaqla r_n üçün $r_n = a \cdot r + b \cdot s$ münasibətini alarıq. □

Verilən halqa əsasında nisbətlər halqası adlanan yeni bir halqanın qurulması üçün konstruksiyalar mövcuddur. İxtiyari halqa halında nisbətlər halqası qurulan zaman qonşuluq sinifləri qurulur, lakin tam ədədlər halqası halında nisbətlər (münasibətlər) halqası çox sadə qurulur.

Tərif 1. Tutaq ki, q - müsbət tam ədəddir.

$$a + b = R_q[a + b], \quad a \cdot b = R_q[a \cdot b]$$

münasibətləri vasitəsilə toplama və vurma əməllərinin təyin olunduğu $\{0,1,\dots,q-1\}$ çoxluğuna q - moduluna görə nisbətlər halqası yaxud q moduluna görə tam ədədlər halqası deyilir. Bu halqa $Z/(q)$ ilə işarə olunur.

$0,1,\dots,q-1$ ilə işarə olunan elementlər həm Z və həm də $Z/(q)$-yə daxildirlər. $Z/(q)$-yə daxil olan elementlər yaxşı olar ki, Z-in ilk q elementi deyil başqa obyektlər, lakin $0,1,2,\dots,q-1$ kimi işarə olunan obyektlər kimi başa düşülsün. Z-in ixtiyari a elementini $a' = R_q[a]$ kimi $Z/(q)$ halqasında əks etdirmək olar. Z çoxluğunun $Z/(q)$ halqasının eyni bir elementinə əks etdirilən a və b elementləri q

moduluna görə müqayisə olunandır, yəni hər hansı bir müsbət tam m ədədi üçün $a = b + m \cdot q$ olur.

Teorem 4. $Z/(q)$ nisbətlər halqası halqa təşkil edir.

Teorem 5. $Z/(q)$ nisbətlər halqasının meydan olması üçün zəruri və kafi şərt q ədədinin hər hansı bir sadə p ədədinə bərabər olmasıdır.

İsbatı. Kafilik. Tutaq ki, q sadə ədəddir. Halqanın meydan olmasını isbat etmək üçün göstərək ki, hər bir sıfırdan fərqli element multiplikativ tərs elementə malikdir. Tutaq ki, s halqanın sıfırdan fərqli elementidir. Onda $1 \le s \le q-1$. q sadə ədəd olduğundan ƏKOB $(s,q)=1$ və nəticə 1-ə görə elə a və b ədədləri mövcuddur ki, $1 = a \cdot q + b \cdot s$ ödənir. Beləliklə,

$$1 = R_q[1] = R_q[aq + bs] = R_q\{R_q[aq] + R_q[bs]\} = R_q[bs] =$$
$$= R_q\{R_q[b] \cdot R_q[s]\} = R_q\{R_q[b] \cdot s\}.$$

Deməli, $1 = R_q\{R_q[b] \cdot s\}$. Bu isə o deməkdir ki, $R_q[b]$ elementi s elementi üçün q moduluna görə multiplikativ tərs elementdir.

Zərurilik. Fərz edək ki, $Z/(q)$ halqası meydan təşkil edir. Göstərək ki, q sadə ədəddir. Əksini fərz edək: q mürəkkəb ədəddir və $q = r \cdot s$. $Z/(q)$ meydan olduğundan r elementi r^{-1} tərs elementinə malikdir və ona görə də

$$s = R_q[s] = R_q[r^{-1} \cdot r \cdot s] = R_q[r^{-1} \cdot q] = 0.$$

Lakin $s \neq 0$ olduğundan ziddiyyət alırıq. Deməli, q sadə əddədir.

□

$Z/(q)$ nisbətlər halqası meydan olduqda onu $GF(q)$ kimi də işarə edirlər.

§7. Çoxhədlilər halqası

$GF(q)$ meydanı üzərində çoxhədli aşağıdakı riyazi ifadəyə deyilir:

$$f(x) = f_{n-1}x^{n-1} + f_{n-2}x^{n-2} + \ldots + f_1 x + f_0. \qquad (1)$$

Burada x qeyri-müəyyən dəyişən, $f_0, f_1, \ldots, f_{n-1}$ əmsalları isə $GF(q)$ meydanının elementləridir. İndekslər və qüvvət dərəcələri mənfi olmayan

tam ədədlərdir. Sıfır çoxhədli $f(x)=0$ çoxhədlisinə deyilir. $f_{n-1}=1$ olarsa çoxhədli çevrilmiş çoxhədli adlanır. Əgər iki çoxhədlinin uyğun əmsalları bərabər olarsa, bu çoxhədlilərə bərabər çoxhədlilər deyilir.

Sıfırdan fərqli (1) çoxhədlisinin dərəcəsi dedikdə f_{n-1} əmsalının indeksi nəzərdə tutulur və deg $f(x)$ ilə işarə olunur. Sıfırdan fərqli çoxhədlinin dərəcəsi sonludur. Sıfır çoxhədlinin dərəcəsi $-\infty$ kimi qəbul olunub.

$GF(q)$ meydanı üzərində təyin olunan çoxhədlilər çoxluğu çoxhədlilərin toplanması və vurulması üçün qəbul edilmiş toplama və vurma əməllərinə görə halqa əmələ gətirir. Belə polinomial halqalar bütün $GF(q)$ Qalua meydanları üçün təyin oluna bilər. Bu halqalar $GF(q)[x]$ ilə işarə olunur. Bu halda $GF(q)$ meydanının elementləri skalyarlar adlandırılır.

$GF(q)[x]$ halqasından olan $f(x)$ və $g(x)$ çoxhədlisinin cəmi

$$f(x)+g(x)=\sum_{i=0}^{m}(f_i+g_i)x^i$$

kimi təyin olunan çoxhədliyə deyilir. Burada $g_i \in GF(q)$ elementi $g(x)$ çoxhədlisində x^i həddinin əmsalıdır $(i=0,...,\deg g(x))$, m isə $m=\max\{\deg f(x), \deg g(x)\}$ kimi təyin olunur. Aydındır ki, cəmin dərəcəsi $f(x)$ və $g(x)$ çoxhədlilərindən ən böyük dərəcəyə malik olanın dərəcəsinə bərabərdir. Qeyd edək ki, yuxarıdakı münasibətdə f_i+g_i əməliyyatı $GF(q)$ üzrə aparılır.

Nümunə 1. $GF(2)$ meydanı üzərində $f(x)=x^3+x^2+x$ və $g(x)=x^4+x^3+1$ çoxhədlilərin cəmini tapmalı.

$$f(x)+g(x)=x^4+x^2+x+1.$$

$f(x)$ və $g(x)$ çoxhədlilərinin hasili də $GF(q)[x]$ halqasından olan çoxhədlidir və aşağıdakı kimi təyin olunur:

$$f(x)g(x)=\sum_{i=0}^{m}\left(\sum_{j=0}^{i}f_j g_{i-j}\right)x^i.$$

Hasilin dərəcəsi $f(x)$ və $g(x)$ çoxhədlilərinin dərəcələrinin cəmi kimi təyin olunur, yəni $m = \deg f(x) + \deg g(x)$.

Nümunə 2. Tutaq ki, $f(x) = x^3 + x^2 + x + 1$, $g(x) = x^3 + x^2$. Bu çoxhədlilərin hasilini tapmalı.

$$f(x) \cdot g(x) = (x^3 + x^2 + x + 1)(x^3 + x^2) = x^6 + x^5 + x^5 + x^4 + x^4 + x^3 + x^3 + x^2 = x^6 + x^2.$$

Çoxhədlilər halqası çox münasibətlərdə tam ədədlər halqasına oxşardır.

Tutaq ki, $s(x)$ və $r(x)$ çoxhədliləri verilib. Əgər elə $a(x)$ çoxhədlisi varsa ki, $r(x) \cdot a(x) = s(x)$ ödənirsə, onda deyirlər ki, $s(x)$ çoxhədlisi $r(x)$ çoxşədlisinə bölünür və ya $r(x)$ çoxhədlisi $s(x)$ çoxhədlisini bölür. Əgər $p(x)$ çoxhədlisi ancaq və ancaq $\alpha p(x)$ çoxhədlisinə $(\alpha \in GF(q))$ və ya α ədədinə bölünürsə, onda $p(x)$ çoxhədlisinə gətirilməyən çoxhədli deyilir. Çevrilmiş gətirilməyən çoxhədliyə sadə çoxhədli deyilir.

$r(x)$ və $s(x)$ çoxhədlilərinin ən böyük ortaq böləni ƏBOB $[r(x), s(x)]$ ilə işarə olunur və bu iki çoxhədlinin eyni vaxtda hər ikisini bölən ən böyük dərəcəli çevrilmiş çoxhədliyə deyilir.

$r(x)$ və $s(x)$ çoxhədlilərinin ən kiçik ortaq bölünəni (və ya misli) ƏKOB$[r(x), s(x)]$ kimi işarə olunur və hər iki çoxhədliyə bölünən ən kiçik dərəcəli çevrilmiş çoxhədliyə deyilir. Əgər ƏBOB$[r(x), s(x)] = 1$ olarsa, onda $r(x)$ və $s(x)$ çoxhədlilərinə qarşılıqlı sadə çoxhədlilər deyilir. Əgər $r(x)$ eyni vaxtda $s(x)$ çoxhədlisini bölür və həm də ona bölünürsə, onda $r(x) = a \cdot s(x)$, harada ki, $a \in GF(q)$.

Həqiqi ədədlər meydanı üzərində təyin olunmuş çoxhədlilər üçün diferensiallama əməliyyatı təyin olunmuşdur. Sonlu meydan üzərində təyin olunmuş çoxhədlilər üçün də analoji diferensiallama əməliyyatı təyin edilə bilər. Qeyd edək ki, sonlu meydan üzərində limitə keçid mümkün olmadığından bu halda diferensiallama formal xarakter daşıyır, lakin nəticə etibarı ilə əsil diferensialın və törəmənin effekti alınır.

Tərif 1. Tutaq ki, $r(x) = r_{n-1}x^{n-1} + r_{n-2}x^{n-2} + ... + r_1 x + r_0$ çoxhədlisi $GF(q)$ üzərində çoxhədlidir. $r(x)$-ın formal törəməsi aşağıdakı kimi təyin olunur:

$$r'(x) = ((n-1))r_{n-1}x^{n-2} + ((n-2))r_{n-2}x^{n-3} + ... + r_1,$$

harada ki, $((i))$ əmsalları $GF(q)$ meydanının ədədləri adlanır və $GF(q)$ üzərində i sayda vahidin cəmi kimi hesablanır:

$$((i)) = \underbrace{1+1+...+1}_{i \text{ sayda}},\ GF(q).$$

Nümunə 3. $GF(2)$ üzərində $f(x) = x^5 + x^3 + x^2 + 1$ çoxhədlisinin törəməsini tapmalı.

$$f'(x) = ((1+1+1+1+1))x^4 + (1+1+1)x^2 + (1+1)x = x^4 + x^2.$$

Asanlıqla göstərmək olar ki, törəmənin əksər xassələri baxılan halda da qüvvədədir, məsələn:

$$[r(x)\cdot s(x)]' = r'(x)s(x) + r(x)s'(x)$$

və əgər $a^2(x)$ çoxhədlisi $r(x)$ çoxhədlisini bölürsə, onda $a(x)$ çoxhədlisi $r'(x)$ çoxhədlisini bölür və.i.a.

Ümumi halda sonlu meydan üzərində təyin olunmuş çoxhədlilər halqasında bölmə mümkün deyildir, lakin ixtisar və qalıqlı bölmə əməliyyatları qüvvədədir.

Teorem 1 (Çoxhədlilərdə qalıqlı bölmə alqoritmi). Hər bir $c(x)$ və $d(x)$ çoxhədliləri $(d(x) \neq 0)$ üçün elə yeganə $q(x)$ (natamam qismət) və $s(x)$ (qalıq) çoxhədlilər cütü mövcuddur ki,

$$c(x) = q(x)\cdot d(x) + s(x),\quad \deg s(x) < \deg d(x).$$

$c(x)$ çoxhədlisinin $d(x)$ çoxhədlisinə bölünməsindən alınan $s(x)$ qalıq çoxhədlisi

$$s(x) = R_{d(x)}[c(x)]$$

kimi işarə olunur. Qalıq çoxhədlilərini $c(x)$ çoxhədlisinin $d(x)$ çoxhədlisi moduluna görə çıxıqı da adlandırırlar. Müqayisə anlayışından istifadə etməklə bu aşağıdakı kimi də yazıla bilər:

$$s(x) \equiv c(x) \pmod{d(x)}.$$

Bunun mənası belədir: $s(x)$ və $c(x)$ çoxşədlilərinin $d(x)$ çoxhədlisinə bölünməsi eyni qalıq verir, lakin bu zaman $\deg s(x) < \deg d(x)$ olması lazım gəlmir.

Teorem 2. Tutaq ki, $d(x)$ çoxhədlisi $g(x)$ çoxhədlisinin mislidir. Onda istənilən $a(x)$ üçün

$$R_{g(x)}[a(x)] = R_{g(x)}[R_{d(x)}[a(x)]]. \qquad (2)$$

İsbatı. Tutaq ki, hər hansı bir $h(x)$ üçün $d(x) = g(x) \cdot h(x)$ ödənir.Teorem 1-ə görə alarıq:

$$a(x) = Q_1(x)d(x) + R_{d(x)}[a(x)] = Q_1(x)g(x)h(x) +$$
$$+ Q_2(x)g(x) + R_{g(x)}[R_{d(x)}[a(x)]],$$

harada ki, qalığın dərəcəsi $g(x)$ çoxhədlisinin dərəcəsindən kiçikdir. Sol tərəfi açsaq, alarıq:

$$a(x) = Q(x)g(x) + R_{g(x)}[a(x)].$$

Qalıqlı bölmə alqoritminə görə qalığın dərəcəsi $g(x)$ çoxhədlisinin dərəcəsindən kiçik olduqda belə yazılış birqiymətlidir. Teoremin doğruluğu hər iki tərəfdə oxşar hədləri eyniləşdirməkdən alınır. □

Teorem 3.

$$R_{d(x)}[a(x) + b(x)] = R_{d(x)}[a(x)] + R_{d(x)}[b(x)], \qquad (3)$$

$$R_{d(x)}[a(x) \cdot b(x)] = R_{d(x)}\{R_{d(x)}[a(x)] \cdot R_{d(x)}[b(x)]\}. \qquad (4)$$

Teorem 4 (Birqiymətli ayırma haqqında teorem). Hər hansı bir meydan üzərində sıfırdan fərqli $p(x)$ çoxhədlisi meydanın elementləri və bu meydan üzərində sadə çoxhədlilərin hasilinə ayrılır.

İsbatı. Aydındır ki, hasilə daxil olan meydanın elementi p_{n-1} əmsalı olmalıdır, harada ki, $n-1$ kəmiyyəti $p(x)$ çoxhədlisinin dərəcəsidir. Ona görə də bu elementi nəzərə almamaq olar və teoremi çevrilmiş çoxhədlilər üçün isbat etmək olar.

Fərz edək ki, teorem doğru deyildir. Tutaq ki, $p(x)$ çoxhədlisi teoremin doğru olmadığı ən kiçik dərəcəli çoxhədlidir və bu çoxhədli üçün iki ayrılış mövcuddur:

$$p(x) = a_1(x)a_2(x)...a_k(x) = b_1(x)b_2(x)...b_j(x),$$

harada ki, $a_i(x), i=\overline{1,k}$ və $b_\ell(x), \ell=\overline{1,j}$ - sadə çoxhədlilərdir.

Bütün $a_i(x)$ çoxhədliləri $b_\ell(x)$ çoxhədlilərindən fərqlənməlidirlər, belə ki, əks halda ümumi hədləri ixtisar edib, iki müxtəlif üsullarla ayrılabilən və $p(x)$-ın dərəcəsindən kiçik dərəcəyə malik çoxhədli almaq olardı.

Ümumiliyi pozmadan fərz edək ki, $b_1(x)$ çoxhədlisinin dərəcəsi $a_1(x)$ çoxhədlisinin dərəcəsindən böyük deyil. Onda

$$a_1(x)=b_1(x)h(x)+s(x),$$

harada ki, $\deg s(x) < \deg b_1(x) \le \deg a_1(x)$. Nəhayət,

$$s(x)a_2(x)a_3(x)...a_k(x)=b_1(x)[b_2(x)...b_j(x)-h(x)a_2(x)...a_k(x)].$$

$s(x)$ çoxhədlisini və kvadrat mötərizə daxilində qalan çoxhədlini sadə vuruqlara ayıraq və əgər lazım gələrsə onları meydanın uyğun elementinə bölək ki, bütün vuruqlar çevrilmiş olsun. $b_1(x)$ sol tərəfdə olmadığından dərəcəsi $p(x)$-ın dərəcəsindən kiçik olan çevrilmiş çoxhədli üçün iki müxtəlif ayrılış alırıq. Bu ziddiyyətdir.

□

Çoxhədlilərin bölünməsindən çoxhədlilər üçün Evklid alqoritmi adı ilə məlum olan mühüm alqoritm alınır.

$GF(q)$ meydanı üzərində olan $r(x)$ və $s(x)$ çoxhədlilərinin ən böyük ortaq bölənini qalıqlı bölmə alqoritminin iterativ tətbiqinin köməyi ilə hesablamaq olar. Əgər $\deg s(x) \ge \deg r(x) \ge 0$ olarsa, onda hesablama ardıcıllığı belə olar:

$$\begin{aligned}
s(x) &= Q_1(x)r(x)+r_1(x),\\
r(x) &= Q_2(x)r_1(x)+r_2(x),\\
r_1(x) &= Q_3(x)r_2(x)+r_3(x),\\
&\vdots\\
r_{n-2}(x) &= Q_n(x)r_{n-1}(x)+r_n(x),\\
r_{n-1}(x) &= Q_{n+1}(x)\cdot r_n(x).
\end{aligned} \qquad (5)$$

Hesablama prosesi qalıq sıfıra bərabər olan kimi dayandırılır.

Teorem 5 (Çoxhədlilər üçün Evklid alqoritmi). $GF(q)$ meydanı üzərində olan $r(x)$ və $s(x)$ çoxhədlilərinin ən böyük ortaq böləni (5) iterativ sxemində alınan son sıfırdan fərqli qalığa bərabərdir, yəni

$$r_n(x) = \alpha \cdot \text{ƏBOB}[r(x), s(x)].$$

Burada α hər hansı skalyardır, yəni $GF(q)$ meydanının elementidir.

İsbatı. (5) sxemində birinci tənlikdən başlayaraq görərik ki, ƏBOB $[r(x), s(x)]$ həm böləni və həm də bölünəni və beləliklə, həm də qalığı bölür. Bu araşdırmanı növbəti bütün tənliklər üçün apararaq görərik ki, ƏBOB$[r(x), s(x)]$ həm də $r_n(x)$ çoxhədlisini bölür. Axırıncı tənlikdən başlayaraq araşdırma aparsaq, görərik ki, $r_n(x)$ həm böləni və həm də qalığı bölür, deməli, o, həm də bölünəni bölür. Bu araşdırmanı sonuncudan başlayaraq birinci tənliyə qədər bütün tənliklər üçün aparsaq görərik ki, $r_n(x)$ çoxhədlisi ƏBOB$[r(x), s(x)]$-ı bölür. Deməli, $r_n(x)$ həm ƏBOB $[r(x), s(x)]$ çoxhədlisini bölür və həm də ona bölünür. □

Nəticə 1. $r(x)$ və $s(x)$ çoxhədliləri üçün aşağıdakı doğrudur:

$$\text{ƏBOB}\ [r(x), s(x)] = a(x) \cdot r(x) + b(x) \cdot s(x),$$

harada ki, $a(x)$ və $b(x)$ çoxhədliləri $GF(q)$ üzərində hər hansı bir çoxhədlilərdirlər.

$GF(q)$ meydanının ixtiyari β elementi üçün $GF(q)$ üzərində çoxhədlilərin bu nöqtədə qiymətini hesablamaq olar. Məsələn, tutaq ki, $p(x) = 2x^5 + x^4 + x^2 + 2$ çoxhədlisi $GF(3)$ üzərindədir. Onda şəkil 1-də verilən əməliyyat cədvəllərinə əsasən alarıq:

$$p(0) = 2 \cdot 0^5 + 0^4 + 0^2 + 2 = 2,$$

$$p(1) = 2 \cdot 1^5 + 1^4 + 1^2 + 2 = 0, \quad p(2) = 2 \cdot 2^5 + 2^4 + 2^2 + 2 = 2.$$

Həqiqi ədələr meydanı halında bu meydanın genişlənməsində çoxhədlilərin qiymətlərinin hesablanması üçün məlum prosedura istifadə olunur. Yəni həqiqi əmsallı çoxhədlilərin qiymətləri kompleks ədədlər meydanında hesablanır. Analoji olaraq $GF(q)$ üzərində çoxhədlilərin qiymətlərini bu meydanın genişlənməsində hesablamaq olar. Belə

hesablama qeyri-müəyyən x dəyişəninin yerinə genişlənmiş meydandan olan elementləri yazmaqla aparılır.

Məsələn, tutaq ki, $p(x)=x^3+x+1$ çoxhədlisi $GF(2)$ üzərindədir. Onda $GF(4)$ meydanının elementləri üçün alarıq:

$$p(0)=0^3+0+1=1\ ;\quad p(2)=2^3+2+1=2\,,$$
$$p(1)=1^3+1+1=1\ ;\quad p(3)=3^3+3+1=2\,.$$

Əgər $p(\beta)=0$ olarsa, onda β elementi $p(x)$ çoxhədlisinin kökü, yaxud $p(x)=0$ tənliyinin kökü adlanır. Çoxhədlinin özünün təyin olunduğu meydanda kökü olmaya da bilər. Məsələn x^3+x+1 çoxhədlisinin $GF(2)$-də və həmçinin $GF(4)$-də kökü yoxdur.

Teorem 6. β elementinin $p(x)$ çoxhədlisinin kökü olması üçün zəruri və kafi şərt $p(x)$ çoxhədlisinin $x-\beta$-yə bölünməsidir.

§8. Çoxhədlilər halqasına əsaslanan sonlu meydanlar

Tutaq ki, F meydanı üzərində $F[x]$ çoxhədlilər halqası verilmişdir. $F[x]$- dan ixtiyari $p(x)$ çoxhədlisini götürək və, beləliklə, $p(x)$ moduluna görə $F[x]$-ın elementlərindən nisbətlər halqası düzəldək.

Tərif 1. F meydanı üzərində sıfırdan fərqli dərəcəyə malik istənilən çevrilmiş $p(x)$ çoxhədlisi üçün dərəcəsi $p(x)$-ın dərəcəsindən kiçik və $p(x)$ modulu üzrə çoxhədlilərin toplanması və vurulması əməliyyatlarının təyin olunduğu F meydanı üzərində çoxhədlilər çoxluğuna $p(x)$ modulu üzrə çoxhədlilər halqası deyilir. Bu halqa $F[x]/(p(x))$ ilə işarə olunur.

$F[x]$ halqasından olan istənilən $r(x)$ elementi $F[x]/(p(x))$ halqasının elementinə $r(x)\to R_{p(x)}[r(x)]$ uyğunluğu ilə inikas oluna bilər. $F[x]$ halqasının iki $a(x)$ və $b(x)$ elemntləri $F[x]/(p(x))$ halqasının eyni elementinə inikas olunarsa, onda bu elementlərə $p(x)$ moduluna görə müqayisə olunandır deyirlər:

$$a(x)\equiv b(x)\pmod{p(x)}\,.$$

Bu zaman $b(x) = a(x) + Q(x) \cdot p(x)$ münasibəti ödənir, harada ki, $Q(x)$ hər hansı bir çoxhədlidir.

Teorem 1. $F[x]/(p(x))$ çoxluğu halqadır.

Nümunə 1. $GF(2)$ üzərində çoxhədlilər halqasından, məsələn, $p(x) = x^3 + 1$ çoxhədlisini götürək. Onda $p(x)$ çoxhədlisi moduluna görə halqa $GF(2)[x]/(x^3 + 1)$ çoxluğudur və elementləri aşağıdakılardan ibarətdir:

$$\{0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1\}.$$

Bu halqada vurma, məsələn, aşağıdakı kimi yerinə yetirilir:

$$(x^2+1)\cdot x^2 = R_{x^3+1}[(x^2+1)\cdot x^2] = R_{x^3+1}[x(x^3+1)+x^2+x] = x^2+x, \quad (1)$$

harada ki, (1)-də $x^4 = x(x^3+1)+x$ qaydası üzrə reduksiya istifadə olunmuşdur.

Nümunə 2. $GF(2)$ meydanı üzərində çoxhədlilər halqasından $p(x) = x^4 + x + 1$ sadə çoxhədlisini götürək. Onda $p(x) = x^4 + x + 1$ sadə çoxhədlisi moduluna görə halqa $GF(2)[x]/(x^4 + x + 1)$ çoxluğudur və bu çoxluq aşağıdakıdır:

$$\{0, 1, x, x+1, x^2, x^2+1, x^2+x+1, x^2+x, x^3, x^3+1, x^3+x,$$
$$x^3+x^2, x^3+x+1, x^3+x^2+1, x^3+x^2+x, x^3+x^2+x+1\}.$$

$GF(2)[x]/(x^4 + x + 1)$ halqasında vurma əməli, məsələn, aşağıdakı kimi yerinə yetirilir:

$$(x^2+1)\cdot(x^2+x+1) = R_{x^4+x+1}[(x^2+1)(x^2+x+1)] =$$

$$= R_{x^4+x+1}[x^4+x^3+x+1] = R_{x^4+x+1}[(x^4+x+1)+x^3] = x^3.$$

Teorem 2. Çevrilmiş $p(x)$ çoxhədlisi moduluna görə çoxhədlilər halqasının meydan olması üçün zəruri və kafi şərt $p(x)$ çoxhədlisinin sadə çoxhədli olmasıdır.

Qeyd: Halqanın meydan olmsı üçün $p(x)$ çoxhədlisi gətirilmiş çoxhədli ola bilər.

İsbatı. Kafilik. Tutaq ki, $p(x)$ çoxhədlisi sadə çoxhədlidir. Baxılan halqanın meydan olmasını isbat etmək üçün istənilən sıfırdan fərqli elementin multiplikativ tərs elementinin olmasını göstərmək kifayətdir. Tutaq ki, $s(x)$ hər hansı sıfırdan fərqli elementdir. Onda $\deg s(x) < \deg p(x)$. $p(x)$ sadə olduğundan ƏBOB $[s(x), p(x)] = 1$. Nəticə 7.1-ə görə hər hansı $a(x)$ və $b(x)$ üçün $1 = a(x)p(x) + b(x)s(x)$ doğqudur. Beləliklə,

$$1 = R_{p(x)}[1] = R_{p(x)}[a(x) \cdot p(x) + b(x) \cdot s(x)] = R_{p(x)}\{R_{p(x)}[b(x)] \times$$

$$\times R_{p(x)}[s(x)]\} = R_{p(x)}\{R_{p(x)}[b(x)] \cdot s(x)\}.$$

Deməli, $p(x)$ moduluna görə çoxhədlilər halqasında $R_{p(x)}[b(x)]$ çoxhədlisi $s(x)$ çoxhədlisinin multiplikativ tərs elementidir.

Zərurilik. Fərz edək ki, baxılan halqa meydandır. Göstərək ki, $p(x)$ çoxhədlilsi sadədir. Əksini fərz edək. Fərz edək ki $p(x)$ sadə deyildir və dərəcəsi ən azı ikidir. Onda $p(x) = r(x) \cdot s(x)$, harada ki, $r(x)$ və $s(x)$ dərəcələri ən azı birə bərabər olan hər hansı çoxhədlilərdirlər. Halqa meydan olduğundan $r(x)$ çoxhədlisi $r^{-1}(x)$ tərs elementinə malikdir və ona görə də

$$s(x) = R_{p(x)}[s(x)] = R_{p(x)}[r^{-1}(x) \cdot r(x) \cdot s(x)] = R_{p(x)}[r^{-1}(x) \cdot p(x)] = 0.$$

Lakin $s(x) \neq 0$ və ona görə də ziddiyyət alırıq. Beləliklə, belə halqa meydan ola bilməz. Deməli, $p(x)$ sadə çoxhədlidir. □

Əgər $GF(q)$ meydanı üzərində n dərəcəli sadə çoxhədli tapılıbsa, onda q^n sayda elementdən ibarət Qalua meydanı qurmaq olar. Bu qurmada meydanın elementləri $GF(q)$ üzərində $n-1$ dərəcədən böyük olmayan dərəcəli çoxhədlilərlə təsvir olunurlar.

Cəmi q^n sayda belə çoxhədlilər mövcuddur.

Nümunə 3. Sadə $p(x) = x^2 + x + 1$ çoxhədlisini istifadə edərək $GF(2)$ meydanı əsasında $GF(4)$ meydanını quraq. Asanlıqla göstərmək olar ki, $p(x)$ çoxhədlisi gətirilməyən çoxhədlidir. Meydanın elementləri $\{0, 1, x, x+1\}$ çoxluğunun elementləridir. Şəkil 2-də qurulan meydanın

toplama və vurma cədvəli verilir. Aydındır ki, çoxhədlilərlə olan işarələmələri tam qiymətli və ya başqa arzuolunan işarələmələrlə əvəz etmək olar.

Cədvəl 1-də $GF(2)$ üzərində sadə çoxhədlilərin siyahısı verilir. Bu çoxhədlilərin sadə olmalarını bilavasitə yoxlamaqla göstərmək olar. Cədvəl 1-də sadə çoxhədlilərin xüsusi halları olan və primitiv çoxhədli kimi adlanan çoxhədlilər verilmişdir. Onlar meydanların genişlənməsinin daha asan təsvir edilməsində istifadə olunurlar (§9-a bax!).

Çoxhədlilərlə işarələmə	**Ikilik işarələmə**	Tamqiymətli işarələmə	Dərəcəli işarələmə
0	00	0	0
1	01	1	x^0
x	10	2	x^1
x+1	11	3	x^2

a)

+	0	1	x	x+1
0	0	1	x	x +1
1	1	0	x+1	x
x	x	x+1	0	1
x+1	x+1	x	1	0

·	0	1	x	x+1
0	0	0	0	0
1	0	1	x	x+1
x	0	x	x+1	1
x+1	0	x+1	1	1

b)

Şəkil 2. $GF(4)$ meydanının quruluşu

Cədvəl 1.

$GF(2)$ meydanı üzərində sadə çoxhədlilər

Dərəcəsi	Sadə çoxhədli	**Dərəcəsi**	**Sadə çoxhədli**
2	x^2+x+1	16	$x^{16}+x^{12}+x^3+x+1$
3	x^3+x+1	17	$x^{17}+x^3+1$
4	x^4+x+1	18	$x^{18}+x^7+1$
5	x^5+x^2+1	19	$x^{19}+x^5+x^2+x+1$
6	x^6+x+1	20	$x^{20}+x^3+1$
7	x^7+x^3+1	21	$x^{21}+x^2+1$
8	$x^8+x^4+x^3+x^2+1$	22	$x^{22}+x+1$
9	x^9+x^4+1	23	$x^{23}+x^5+1$

10	$x^{10}+x^3+1$	24	$x^{24}+x^7+x^2+x+1$
11	$x^{11}+x^2+1$	25	$x^{25}+x^3+1$
12	$x^{12}+x^6+x^4+x+1$	26	$x^{26}+x^6+x^2+x+1$
13	$x^{13}+x^4+x^3+x+1$	27	$x^{27}+x^5+x^2+x+1$
14	$x^{14}+x^{10}+x^6+x+1$	28	$x^{28}+x^3+1$
15	$x^{15}+x+1$		

Aşağıdakı bəzi faktları qeyd edək:

1) Hər bir Qalua meydanı üzərində istənilən dərəcəli sadə çoxhədli mövcuddur;

2) Yuxarıda şərh edilən üsulla bütün Qalua meydanlarını qurmaq olar. Belə qayda ilə qurulan Qalua meydanlarından başqa Qalua meydanları yoxdur;

3) Hər bir meydanda primitiv adlanan element mövcuddur.

Qalua meydanlarına aid olan bəzi mühüm nəticələr aşağıdakılardır:

1. İstənilən Qalua meydanının elementlərinin sayı hər hansı bir sadə ədədin qüvvətinə bərabərdir;

2. İstənilən p sadə və müsbət tam m ədədi üçün $GF(p^m)$ meydanının ən kiçik altmeydanı $GF(p)$ meydanıdır. $GF(p)$ meydanının elementləri $GF(p^m)$ meydanının tam ədədləri, p-ədədi isə onun xarakteristikası adlanır.

3. Xarakteristikası 2 ədədinə bərabər olan sonlu meydanlarda hər bir β elementi üçün $-\beta = \beta$ bərabərliyi ödənir.

4. İstənilən p sadə və m müsbət tam ədədi üçün p^m sayda elementdən ibarət Qalua meydanı mövcuddur.

5. Hər bir $GF(q)$ Qalua meydanı heç olmazsa bir primitiv elementə malikdir.

6. Hər bir Qalua meydanı üzərində istənilən dərəcəli heç olmazsa bir primitiv çoxhədli mövcuddur.

7. Hər bir primitiv elementin istənilən alt meydan üzərində sadə minimal çoxhədlisi mövcuddur.

8. Eyni sayda elementə malik iki Qalua meydanı izomorfdur.

9. Sadə ədədin dərəcəsi olan istənilən q ədədi və istənilən m tam müsbət ədədi üçün $GF(q)$ meydanı $GF(q^m)$ meydanının altmeydanıdır, $GF(q^m)$ isə $GF(q)$ meydanının genişlənməsidir.

10. Əgər n ədədi m ədədini bölmürsə, onda $GF(q^n)$ meydanı $GF(q^m)$ meydanının altmeydanı deyildir.

11. $GF(q^m)$ meydanının istənilən elementi üçün $GF(q)$ üzərində minimal çoxhədlinin dərəcəsi m -in bölənidir.

§9. Sonlu meydanın primitiv elementi

Tərif 1. $GF(q)$ meydanının primitiv elementi elə α elementinə deyilir ki, meydanın sıfırıncı elementindən başqa bütün elementləri bu elementin dərəcəsi kimi göstərilə bilsin.

Məsələn, $GF(5)$ meydanında $2^1 = 2,\ 2^2 = 4, 2^3 = 3,\ 2^4 = 1$, beləliklə, 2 elementi bu meydanının primitiv elementidir.

Meydanların qurulmasında primitiv elementlər çox böyük əhəmiyyətə malikdir. Belə ki, bunlardan biri tapılıbsa, onda onların qüvvətlərini vurmaqla meydanının vurma cədvəlini qurmaq olar.

Bu paraqrafda qrup dedikdə vurma əməlinə görə qrup nəzərdə tutacağıq.

Teorem 1. Tutaq ki, $\beta_1, \beta_2, ..., \beta_{q-1}$ elementləri $GF(q)$ meydanının sıfırdan fərqli elementləridirlər. Onda

$$x^{q-1} - 1 = (x - \beta_1)(x - \beta_2)...(x - \beta_{q-1}).$$

İsbatı. $GF(q)$ meydanının sıfırdan fərqli olan elementləri vurma əməlinə görə sonlu qrup əmələ gətirirlər. Tutaq ki, β elementi $GF(q)$ meydanının sıfırdan fərqli elementidir və tutaq ki, h - bu elementin vurmaya görə tərtibidir. Məlum teoremə görə sonlu qrupun tərtibi onun

istənilən elementinin tərtibinə bölünür. Odur ki, h ədədi $q-1$ ədədini bölür. Beləliklə,

$$\beta^{q-1} = (\beta^h)^{\frac{q-1}{h}} = 1^{\frac{q-1}{h}} = 1.$$

Deməli, β elementi $x^{q-1}-1$ çoxhədlisinin köküdür. □

Teorem 2. $GF(q)$ meydanının sıfırdan fərqli elementlərinin vurma əməlinə görə əmələ gətirdikləri qrup dövri qrupdur.

İsbatı. Əgər $q-1$ sadə ədəddirsə, onda teoremin hökmü trivialdır. Belə ki, sıfırdan və birdən fərqli bütün elementlərin tərtibi $(q-1)$-dir. Deməli, bütün belə elementlər primitivdirlər. Teoremi $q-1$ mürəkkəb ədəd olduğu halda isbat edək. $(q-1)$-in sadə vuruqlara ayrılışına baxaq:

$$q-1 = \prod_{i=1}^{s} p_i^{\nu_i}.$$

$GF(q)$ meydan olduğundan, onun $q-1$ sayda sıfırdan fərqli elementləri arasında $x^{(q-1)/p_i}-1$ çoxhədlisinin kökü olmayan heç olmazsa bir element tapılmalıdır, belə ki, bu çoxhədlinin $(q-1)/p_i$-dən çox olmayan sayda kökü ola bilər. Beləliklə, hər bir i üçün $GF(q)$ meydanının sıfırdan fərqli elə a_i elementini tapmaq olar ki, $a_i^{(q-1)/p_i} \neq 1$ olsun. Tutaq ki, $b_i = a_i^{(q-1)/p_i^{\nu_i}}$-dir və tutaq ki,

$$b = \prod_{i=1}^{s} b_i.$$

İsbat edək ki, b ədədinin tərtibi $(q-1)$-dir və, beləliklə, qrup dövri qrupdur.

Addım 1. b_i elementinin tərtibi $p_i^{\nu_i}$-yə bərabərdir. Bunu isbat edək. Aydındır ki, $b_i^{p_i^{\nu_i}} = 1$, beləliklə, b_i ədədinin tərtibi $p_i^{\nu_i}$ ədədini bölür. Onda b_i-nin tərtibi $p_i^{n_i}$ kimi ədədə bərabərdir. Əgər n_i ədədi ν_i-dən kiçik isə, onda

$$b_i^{p_i^{\nu_i-1}} = 1.$$

Lakin

$$b_i^{p_i^{v_i-1}} = a_i^{\frac{q-1}{p_i}} \neq 1.$$

Addım 2. b elementinin tərtibi $(q-1)$-dir. Bunu isbat edək. Fərz edək ki, $b^n = 1$. Əvvəlcə göstərək ki, hər bir $i = 1,..., s$ üçün buradan $n = 0 \pmod{p_i^{v_i}}$ bərabərliyi alınır. Hər bir i üçün aşağıdakını yazmaq olar:

$$b^{\left(n\prod_{j\neq i} p_j^{v_j}\right)} = 1.$$

b-ni $\prod_{i=1}^{s} b_i$ ilə əvəz edərək və $b_i^{p_i^{v_i}} = 1$ bərabərliyini istifadə edərək aşağıdakını alarıq:

$$b^{\left(n\prod_{j\neq i} p_j^{v_j}\right)} = 1.$$

Beləliklə,

$$n\prod_{j\neq i} p_j^{v_j} = 0 \pmod{p_i^{v_i}}.$$

Belə ki, p_i-lər müxtəlif sadə ədədlərdirlər, ona görə hər bir i üçün $n = 0 \pmod{p_i^{v_i}}$. Beləliklə,

$$n = \prod_{i=1}^{s} p_i^{v_i}. \qquad \square$$

Teorem 3. Hər bir Qalua meydanında primitiv element mövcuddur.

İsbatı. $GF(q)$ meydanının sıfırdan fərqli elementləri dövri qrup əmələ gətirdiklərindən, onların arasında $q-1$ tərtibinə malik element mövcuddur. Bu element primitiv elementdir. $\square$

Primitiv elementin meydanda vurma cədvəlinin qurulmasında istifadəsini göstərmək üçün aşağıdakı nümunəyə baxaq:

Nümunə 1. $GF(8)$ meydanında hər bir sıfırdan fərqli elementin tərtibi 7-ni bölür. 7 sadə ədəd olduğundan sıfırdan və 1-dən fərqli elementlər 7-yə bərabər tərtibə malikdirlər və beləliklə, primitivdirlər. $GF(8)$ meydanını $p(z) = z^3 + z + 1$ çoxhədlisi vasitəsilə qurmaq olar. $\alpha = z$ primitiv elementinə əsaslanaraq aşağıdakıları alarıq:

$$\alpha = z, \quad \alpha^2 = z^2, \quad \alpha^3 = z+1, \quad \alpha^4 = z^2+z,$$
$$\alpha^5 = z^2+z+1, \quad \alpha^6 = z^2+1, \quad \alpha^7 = 1 = \alpha^0.$$

Bu təsvirdə vurma asanlıqla yerinə yetirilir, məsələn $\alpha^4 \cdot \alpha^5 = \alpha^7 \cdot \alpha^2 = \alpha^2$.

Nümunə 2. $GF(16)$ meydanında hər bir elementin tərtibi 15-i bölür. Elementlər 1,3,5 və 15 tərtibinə malik ola bilər. $GF(16)$ meydanını $p(z) = z^4 + z + 1$ çoxhədlisinin və $\alpha = z$ primitiv elementinin köməkliyi ilə qurmaq olar. Aşağıdakıları alırıq:

$$\alpha = z, \quad \alpha^2 = z^2, \quad \alpha^3 = z^3, \quad \alpha^4 = z+1, \quad \alpha^5 = z^2+z,$$
$$\alpha^6 = z^3+z^2, \quad \alpha^7 = z^3+z+1, \quad \alpha^8 = z^2+1, \quad \alpha^9 = z^3+z,$$
$$\alpha^{10} = z^2+z+1, \quad \alpha^{11} = z^3+z^2+z, \quad \alpha^{12} = z^3+z^2+z+1,$$
$$\alpha^{13} = z^3+z^2+1, \quad \alpha^{14} = z^3+1, \quad \alpha^{15} = 1.$$

Meydanın belə təsvirində vurma sadədir; məsələn,

$$\alpha^{11} \cdot \alpha^{13} = \alpha^{15} \cdot \alpha^9 = \alpha^9.$$

Nümunə 3. $GF(27) = GF(3^3)$ meydanında hər bir element 26 tərtibinə malikdir. Bu meydanı $p(x) = x^3 + 2x + 1$ çoxhədlisinin və $\alpha = x$ primitiv elementinin köməkliyi ilə qurmaq olar. Primitiv elementə əsaslanaraq aşağıdakını alarıq:

$\alpha = x$, $\alpha^9 = x+1$, $\alpha^{18} = x^2+2x+1$,
$\alpha^2 = x^2$, $\alpha^{10} = x^2+x$, $\alpha^{19} = 2x^2+2x+2$,
$\alpha^3 = x+2$, $\alpha^{11} = x^2+x+2$, $\alpha^{20} = 2x^2+x+1$,
$\alpha^4 = x^2+2x$, $\alpha^{12} = x^2+2$, $\alpha^{21} = x^2+1$,
$\alpha^5 = 2x^2+x+2$, $\alpha^{13} = 2$, $\alpha^{22} = 2x+2$,
$\alpha^6 = x^2+x+1$, $\alpha^{14} = 2x$, $\alpha^{23} = 2x^2+2x$,
$\alpha^7 = x^2+2x+2$, $\alpha^{15} = 2x^2$, $\alpha^{24} = 2x^2+2x+1$,
$\alpha^8 = 2x^2+2$, $\alpha^{16} = 2x+1$, $\alpha^{25} = 2x^2+1$,
$\alpha^{17} = 2x^2+x$, $\alpha^{26} = 1$.

Bu meydanda vurma əməlini, məsələn, aşağıdakı kimi yerinə yetirmək olar

$$(2x^2+2)\cdot(2x^2+2x+1) = \alpha^8 \cdot \alpha^{24} = \alpha^{32} = \alpha^{26+6} =$$
$$= \alpha^{26} \cdot \alpha^6 = \alpha^6 = x^2+x+1.$$

x çoxhədlisinə meydanın primitiv elementinin uyğun olduğu halda meydanın çoxhədlilər çoxluğu şəklində genişlənməsinin qurulması daha asan olur. Bu halda vurma cədvəlində $(x-1)$-i loqarifmin əsası kimi istifadə etmək olar və bu da mümkün əsasların ən sadəsidir. Meydanın belə qurulmasını primitiv çoxhədlilər adlanan xüsusi şəkilli çoxhədlilər vasitəsilə həyata keçirmək olar.

Tərif 2. $GF(q)$ meydanın üzərində $p(x)$ primitiv çoxhədlisi $GF(q)$ üzərində elə sadə çoxhədliyə deyirlər ki, $p(x)$ modulu üzrə qurulan genişlənmiş meydanda x çoxhədlisinə uyğun meydan elementi primitiv element olsun.

Primitiv çoxhədli kökü primitiv element olan çoxhədliyə deyilir.

§10. Sonlu meydanın strukturu

Tərif 1. $GF(q)$ meydanının ən kiçik altmeydanının elementlərinin sayı $GF(q)$ meydanının xarakteristikası adlanır.

Teorem 1. Hər bir Qalua meydanı elementlərinin sayı sadə ədəd olan yeganə ən kiçik altmeydana malikdir. Beləliklə, hər bir Qalua meydanının xarakteristikası sadə ədəddir.

İsbatı. Meydan «0» və «1» ədədlərinə malikdir. Alt meydanı təşkil etmək üçün $G = \{0,1,1+1,1+1+1,...\}$ alt çoxluğuna baxaq və onun elementlərini $\{0,1,2,3,...\}$ ilə işarə edək. Bu alt çoxluq toplamaya görə dövri qrup əmələ gətirir və elementləri sonlu p saydan ibarət olmalıdır. Göstərək ki, p sadə ədəddir və $G = GF(p)$. G-də toplama p modulu üzrə toplama əməlidir, belə ki, G toplama üzrə dövri qrup əmələ gətirir. Distiributivlik qanununa görə vurma da mod p üzrə vurma əməli olmalıdır:

$$\alpha \cdot \beta = (1 + ... + 1) \cdot \beta = \beta + ... + \beta,$$

harada ki, β ədədi α dəfə toplanır. Vurma əməliyyatına görə hər bir element tərs elementə malikdir, belə ki, $\{\beta, 2\beta, 3\beta, ...\}$ ardıcıllıqları G-də dövri altqrup əmələ gətirir .

Beləliklə, G altçoxluğunun vahid elementi mövcuddur, toplama və vurma əməlinə görə qapalıdır, toplama və vurma əməlinə görə elementlərin tərs elementləri mövcuddur. Deməli, o, meydandır və bu meydanda

əməliyyatlar mod p üzrə əməliyyatlardır. Teorem 6.5-ə görə p sadə ədəd olmalıdır. □

İki meydan ancaq təsvir üsullarına görə fərqlənərlərsə, onda onlar izomorf adlanarlar.

Tərif 2. Tutaq ki, $GF(q)$ hər hansı bir meydandır və $GF(Q)$ onun genişlənməsidir. Tutaq ki, β elementi $GF(Q)$-nün elementidir. $f(\beta)=0$ şərtini ödəyən $GF(q)$ üzərində ən kiçik dərəcəyə malik $f(x)$ çoxhədlisinə β elementinin minimal çoxhədlisi deyilir.

Teorem 2. $GF(Q)$ meydanının hər bir β elementi $GF(q)$ üzərində yeganə minimal çoxhədliyə malikdir. Əgər $f(x)$ çoxhədlisi β elementinin minimal çoxhədlisidirsə və β elementi $g(x)$ çoxhədlisinin kökü isə, onda $f(x)$ çoxhədlisi $g(x)$ çoxhədlisini bölür.

İsbatı. Hər şeydən əvvəl β elementi $GF(q)$ üzərində $x^Q - x$ çoxhədlisinin köküdür. Birqiymətli ayrılış teoremindən istifadə edək:

$$x^Q - x = f_1(x)\cdot f_2(x)\ldots f_k(x).$$

Burada sağ tərəfdə bütün vuruqlar $GF(q)$ üzərində sadə çoxhədlilərdirlər. Əgər β sol tərəfin kökü isə, onda sağ tərəfdə hər hansı bir vuruq tapılmalıdır ki, β onun da kökü olsun. Lakin, sağ tərəfdə ancaq bir vuruq ola bilər, belə ki, sadə çoxhədlilər $GF(Q)$ genişlənməsi üzərində sabitlər və xətti hədlərin hasilinə ayrılırlar və β ancaq bu xətti hədlərin birinin kökü ola bilər.

Teoremin ikinci hissəsini isbat etmək üçün

$$g(x) = f(x)\cdot h(x) + s(x)$$

götürək, hansı ki, $\deg s(x) < \deg f(x)$. Deməli, β $s(x)$ çoxhədlisinin kökü ola bilməz. Lakin

$$0 = g(\beta) = f(\beta)h(\beta) + s(\beta) = s(\beta).$$

Beləliklə, $s(x)=0$ olur. □

Nəticə 1. Əgər $f_1(x),\ldots,f_k(x)$ çoxhədlilərinin hamısı $GF(q)$ üzərində müxtəlif çoxhədlilərsə və $GF(Q)$-dən olan bir və ya bir neçə elementin minimal çoxhədlilərindirlərsə, onda

$$x^Q - x = f_1(x)\cdot f_2(x)\ldots f_k(x).$$

Nəticənin isbatı teoremdən çıxır, belə ki, hər bir β elementi $x^Q - x$ çoxhədlisinin köküdür.

$Q = q$ olduqda ayrılış aşağıdakı bərabərliyə çevrilir:

$$x^q - x = x(x-\beta_1)(x-\beta_2)...(x-\beta_{q-1}).$$

β elementinin $GF(q)$ üzərində minimal çoxhədlisi $f(x) = x - \beta$ çoxhədlisi olur.

Teorem 3. Tutaq ki, $g(x)$ çoxhədlisi $GF(q)$ meydanı üzərində ixtiyari çoxhədlidir. Onda bu meydanın $GF(Q)$ genişlənməsi mövcuddur və $GF(Q)$ meydanında $g(x)$ xətti vuruqların hasilinə çevrilir.

İsbatı. Ümumiliyi pozmadan hesab edək ki, $g(x)$ gətirilmiş çoxhədlidir. $GF(q) \subset GF(Q_1) \subset GF(Q_2) \subset ... \subset GF(Q)$ genişlən-mələr ardıcıllığını aşağıdakı qaydada quraq. Hər bir addımda $g(x)$ çoxhədlisini $GF(Q_j)$ üzərində sadə çoxhədlilərin hasili şəklində yazaq. Əgər yenə qeyri-xətti vuruq olarsa, onda onlardan birini, deyək ki, $g_j(x)$ çoxhədlisini götürək və $g_j(y)$ çoxhədlisini sadə modul götürməklə $GF(Q_j)$ meydanının genişlənməsini quraq. Bu genişlənmədə $g(x)$-ın ayrılışını davam etdirək, belə ki, yeni $\beta = y$ elementi $g_j(x)$ çoxhədlisinin köküdür. Beləliklə (zəruri olduğu halda işarələmələri unifikasiya etməklə), bütün vuruqlar xətti olanadək prosesi davam etdiririk. $g(x)$ çoxhədlisinin dərəcəsi sonlu olduğundan bu proses sonlu sayda addımdan sonra yekunlaşır. □

Tərif 3. $GF(q)$ meydanının istənilən genişlənməsi, harada ki, $GF(q)$ meydanı üzərində olan $g(x)$ çoxhədlisi bu genişlənmədə xətti vuruqların və sabitlərin hasilinə çevrilir, $g(x)$ çoxhədlisinin ayrılma (parçalanma) meydanı adlanır.

Teorem 4. Tutaq ki, α elementi $GF(q)$ meydanının genişlənməsi olan $GF(Q)$ meydanının primitiv elementidir və m ədədi α elementinin $GF(q)$ üzərində $f(x)$ minimal çoxhədlisinin dərəcəsidir. Onda $GF(Q)$ meydanının elementlərinin sayı $Q = q^m$ ədədinə bərabərdir və onun hər bir β elementi aşağıdakı kimi təsvir
oluna bilər:

$$\beta = a_{m-1}\alpha^{m-1} + a_{m-2}\alpha^{m-2} + ... + a_1\alpha + a_0,$$

burada $a_{m-1}, a_{m-2}, ..., a_0$ ədədləri $GF(q)$ meydanının elementləridir.

İsbatı. Aydındır ki,

$$\beta = a_{m-1}\alpha^{m-1} + a_{m-2}\alpha^{m-2} + ... + a_1\alpha + a_0,$$

kimi təyin olunan hər bir β elementi $GF(Q)$ meydanına məxsusdur. Belə ayrılış yeganədir, belə ki, əgər

$$\beta = b_{m-1}\alpha^{m-1} + b_{m-2}\alpha^{m-2} + ... + b_1\alpha + b_0$$

ifadəsi β elementinin başqa təsviri isə, onda

$$0 = (a_{m-1} - b_{m-1})\alpha^{m-1} + ... + (a_1 - b_1)\alpha + (a_0 - b_0)$$

və, beləliklə, α ədədi $m-1$ dərəcəli çoxhədlinin köküdür, bu isə α ədədinin seçilməsi ilə ziddiyyət təşkil edir. Bütövlükdə q^m sayda belə elementlər mövcuddur və, beləliklə, $GF(Q)$ meydanının elementlərinin sayı q^m-dən kiçik deyil.

Digər tərəfdən meydanının sıfırdan fərqli hər bir elementi α elementinin hər hansı bir dərəcəsi kimi təsvir oluna bilər. Lakin, əgər $f(x)$ çoxhədlisi α elementinin minimal çoxhədlisi isə, onda $f(\alpha) = 0$.

Beləliklə,

$$\alpha^m + f_{m-1}\alpha^{m-1} + ... + f_1\alpha + f_0 = 0.$$

Bu münasibət α^m elementini α elementinin m-dən kiçik dərəcəli qüvvətlərinin cəmi kimi təsvir etmək üçün istifadə oluna bilər:

$$\alpha^m = -f_{m-1}\alpha^{m-1} - ... - f_1\alpha - f_0.$$

Bu münasibət α-nın m-dən böyük istənilən dərəcəli qüvvətlərini $\alpha^{m-1}, \alpha^{m-2}, ..., \alpha^1, \alpha^0$ qüvvətlərinin xətti kombinasiyası şəklində alınması üçün istifadə oluna bilər:

$$\alpha^{m+1} = -f_{m-1}(-f_{m-1}\alpha^{m-1} - ... - f_1\alpha - f_0) - f_{m-2}\cdot\alpha^{m-1} - ... - f_1\alpha^2 - f_0\alpha$$

və i.a. Beləliklə, $GF(Q)$ meydanının istənilən elementi $\alpha^{m-1}, \alpha^{m-2}, ..., \alpha^1, \alpha^0$ elementlərinin xətti kombinasiyası kimi təsvir oluna bilər. Deməli, Q ədədi q^m-dən böyük ola bilməz. □

Nəticə 2. Hər bir Qalua meydanı p^m sayda elementdən ibarətdir, burada p-sadə ədəd, m isə müsbət tam ədəddir.

Qeyd edək ki, teorem 4 meydanın hər bir elementini α elementinin qeyri-müəyyən x dəyişəni ilə sadə əvəz edilməsi yolu ilə hər hansı bir $m-1$ dərəcəli çoxhədli ilə əlaqələndirmək üçün istifadə oluna bilər. Bu çoxhədliyə meydanın bir elementi kimi baxıla bilər. Onların toplanması və vurulması α elementinin minimal çoxhədlisi olan $f(x)$ modulu üzrə aparılır. Əgər sadə çoxhədli kimi $f(x)$ çoxhədlisi götürülərsə, onda bu teorem 8.2-də alınan meydanla eyni bir meydan olar. Beləliklə, hər bir Qalua meydanında elementlərin sayı sadə ədəd dərəcəsinə bərabərdir və hər bir Qalua meydanı sadə çoxhədlilər modulu hesabının köməkliyi ilə qurula bilər.

Bəzi nəticələri qeyd edək:

Teorem 5. Tutaq ki, $GF(q)$ meydanının xarakteristikası p-dir. Onda $GF(q)$-dən olan istənilən α və β ədədləri və istənilən müsbət tam m ədədi üçün

$$(\alpha \pm \beta)^{p^m} = \alpha^{p^m} \pm \beta^{p^m}.$$

İsbatı. Tutaq ki, teorem $m=1$ olduqda doğrudur:

$$(\alpha \pm \beta)^{p} = \alpha^{p} \pm \beta^{p}.$$

Bu bərabərliyi p qüvvətinə yüksəldək:

$$((\alpha \pm \beta)^{p})^{p} = (\alpha^{p} \pm \beta^{p})^{p}$$

və teoremi $m=1$ üçün yenidən istsfadə edək:

$$(\alpha \pm \beta)^{p^2} = \alpha^{p^2} \pm \beta^{p^2}.$$

Bu proseduranı $m-1$ dəfə təkrar etsək, alarıq:

$$(\alpha \pm \beta)^{p^m} = \alpha^{p^m} \pm \beta^{p^m}.$$

Beləliklə, teoremi ancaq $m=1$ halında isbat etmək lazımdır. Binomial ayrılışa görə

$$(\alpha \pm \beta)^p = \sum_{i=0}^{p} C_p^i \alpha^i (\pm\beta)^{p-i}.$$

İsbat edək ki, $C_p^i = 0,\ i = 1,2,\ldots,p-1$. Lakin hər bir i üçün

$$C_p^i = \frac{p!}{i!(p-i)!} = \frac{p(p-1)!}{i!(p-i)!}$$

tam ədəddir, p isə sadə ədəddir. Beləliklə, p sadə ədəd olduğundan məxrəc ancaq $(p-1)!$-ı bölür, C_p^i-isə p-nin misli olur. Beləliklə, $C_p^i = 0 \pmod p$. $GF(q)$-də tam ədədlər hesabı $\bmod p$ üzrə olduğundan, $i \neq 0$ və $i \neq p$ hallarında binomial əmsal $C_p^i = 0$ olur. Nəhayət, əgər $p=2$ isə, onda $(\pm\beta)^2 = \beta^2$, əgər p-tək ədəddirsə, onda $(\pm\beta)^p = \pm\beta^p$.

Teorem 6. Tutaq ki, p sadə, m isə müsbət tam ədəddir. Onda $GF(p)$ üzərində $g(x) = x^{p^m} - x$ çoxhədlisinin ən kiçik parçalanma meydanı p^m sayda elementdən ibarətdir.

İsbatı. $GF(p)$ meydanı üzərində hər bir çoxhədli ən kiçik ayrılma (parçalanma) meydanına malikdir. Tutaq ki, $GF(Q)$ meydanı $g(x) = x^{p^m} - x$ çoxhədlisinin ən kiçik ayrılma meydanıdır. Onda $GF(Q)$ meydanında $g(x)$ çoxhədlisinin p^m sayda (təkrar köklər də mümkündür) kökü mövcuddur. Göstərək ki, bütün köklər müxtəlifdir və meydan əmələ gətirirlər. Onda buradan alınacaq ki, $GF(Q)$ meydanı p^m sayda elementdən ibarətdir.

Köklər çoxluğunun meydan əmələ gətirməsini isbat etmək üçün bu çoxluğun toplama və vurma əməlinə görə qapalı olmasını və hər bir sıfırdan fərqli elementin tərs elementə malik olmasını göstərmək kifayətdir. Tutaq ki, α və β elementləri $g(x)$ çoxhədlisinin kökləridir. Teorem 5-ə görə

$$(\alpha \pm \beta)^{p^m} = \alpha^{p^m} \pm \beta^{p^m} = \alpha \pm \beta,$$

deməli, $\alpha \pm \beta$ -elementi də çoxhədlinin köküdür və, deməli, köklər çoxluğu toplamaya nəzərən qapalıdır.

$$(\alpha\beta)^{p^m} = \alpha^{p^m} \cdot \beta^{p^m} = \alpha \cdot \beta .$$

Beləliklə, $\alpha\beta$ elementi də $g(x)$ çoxhədlisinin köküdür və, deməli, köklər çoxluğu vurmaya nəzərən qapalıdır.

Əgər α kökdürsə, onda $-\alpha$ elementi də kökdür. Asanlıqla yoxlamaq olar ki, α çoxhədlinin kökü isə, onda α^{-1} də çoxhədlinin köküdür.

Nəhayət göstərək ki, $g(x) = x^{p^m} - x$ çoxhədlisinin bütün p^m sayda kökləri müxtəlifdir. Bu, formal törəmədən çıxır:

$$d[x^{p^m} - x]/dx = ((p^m))x^{p^m-1} - 1 = -1,$$

belə ki, $GF(Q)$ -də $((p)) = 0$. Beləliklə, $x^{p^m} - x$ çoxhədlisi təkrar kökə malik deyildir. □

Nəticə 3. Hər bir sadə p və müsbət m tam ədədləri üçün p^m sayda elementə malik Qalua meydanı mövcuddur.

Nəhayət göstərək ki, əgər q sadə ədəd deyildirsə, lakin sadə ədədin qüvvətidirsə, onda $GF(q^m)$ meydanını $GF(q)$ meydanının genişlənməsi kimi qurmaq olar. Bunun üçün $GF(q)$ meydanı üzərində m dərəcəli sadə çoxhədlinin mövcudluğunun isbatı kifayətdir.

Teorem 7. Hər bir tam müsbət m ədədi üçün hər bir $GF(q)$ sonlu meydanı üzərində m dərəcəli heç olmazsa bir sadə çoxhədli mövcuddur.

İsbatı. q ədədi sadə ədədin dərəcəsi olduğundan q^m də həmçinin sadə ədədin dərəcəsidir. Nəticə 3-ə görə q^m elementə malik sonlu meydan mövcuddur. Bu meydan α primitiv elementinə malikdir və teorem 4-ə görə bu primitiv elementin $GF(q)$ üzərində minimal çoxhədlisi m dərəcəli sadə çoxhədlidir. □

Nəticə 4. Hər bir tam müsbət m ədədi üçün hər bir $GF(q)$ sonlu meydanı üzərində m dərəcəli heç olmazsa bir primitiv çoxhədli mövcuddur.

İsbatı. Tutaq ki, α elementi $GF(q^m)$ meydanının primitiv elementidir və tutaq ki, $f(x)$ çoxhədlisi α elementinin $GF(q)$ üzərində minimal çoxhədlisidir. Onda $f(x)$ modulu üzrə çoxhədlilər meydanında $\alpha = x$ primitiv elementi $f(x)$ çoxhədlisinin köküdür. Beləliklə, x çoxhədlisi özünü meydanın primitiv elementi kimi aparır. □

Teorem 8. $GF(2^m)$ meydanının hər bir elementi bu meydanda kvadrat kökə malikdir. Cüt olmayan sadə p üçün $GF(p^m)$ meydanının sıfırdan fərqli elementlərinin yarısı $GF(p^m)$-də kvadrat kökə malikdir. $GF(p^m)$ meydanının sıfırdan fərqli elementlərinin yarısı $GF(p^m)$ meydanında deyil, genişlənmiş $GF(p^{2m})$ meydanınında kvadrat kökə malikdir.

İsbatı. Sıfıra bərabər element istənilən meydanda kvadrat kökə malikdir. Ona görə də sıfırdan fərqli elementlərə baxmaq lazımdır. Əvvəlcə 2 xarakteristikasına malik və α primitiv elementli $GF(2^m)$ meydanınına baxaq. Onda α elementinin tərtibi tək ədəd olar. Meydanın hər bir β elementi hər hansı bir i üçün α^i kimi yazıla bilər və ona görə də əgər i cütsə $\sqrt{\beta} = \alpha^{i/2}$, əgər i təksə, onda $\sqrt{\beta} = \alpha^{\frac{i+n}{2}}$ olar, harada ki, $n = q^m - 1$-dir. İstənilən halda β meydanın elementi olur.

İndi isə xarakteristikası p tək sadə ədəd, primitiv elementi isə $\alpha = \gamma^{q+1}$ olan $GF(q)$ meydanına baxaq, harada ki, γ elementi $GF(q^2)$ genişlənmiş meydanın primitiv elementidir, onun tərtibi $q^2 - 1 = (q-1)(q+1)$ ədədinə bərabərdir və $q+1$ cütdür, belə ki, q ədədi tək sadə ədədin dərəcəsinə bərabərdir. İstənilən β elementi hər hansı bir i üçün α^i və ya $\gamma^{(q+1)i}$ kimi yazıla bilər. Onda i cüt olduqda $\sqrt{\beta} = \alpha^{i/2}$ və $GF(q)$ meydanına daxildir. i tək olduqda $\sqrt{\beta} = \gamma^{(q+1)i/2}$ və bu $GF(q)$ meydanına deyil, $GF(q^2)$ meydanına daxildir, belə ki, bu halda $i(q+1)/2$ ədədi $(q+1)$ ədədinin misli deyildir. □

FƏSİL III. XƏTTİ BLOK KODLARI

§1. Xətti blok kodlarının strukturu

$GF^n(q)$ vektor fəzası $GF(q)$-dən olan elementlərin n-ardıcıllıqlarından yaxud n-ölçülü vektorlardan ibarət olan çoxluqdur və burada komponentlər üzrə toplama və $GF(q)$-dən olan skalyara vurma əməli mövcuddur. Bu fəzanın ən əhəmiyyətli xüsusi halı $GF^n(2)$ fəzasıdır. Bu fəzada iki vektorun komponentlər üzrə toplanması mod 2-üzrə aparılır.

Tərif 1. $GF^n(q)$ fəzasından olan istənilən altfəzaya xətti kod deyilir.

Beləliklə, xətti kodlar $GF(q)$ üzərində kod sözü adlanan n-ardıcıllıqların boş olmayan çoxluğudur və elədirlər ki, iki kod sözünün cəmi və ya kod sözünün meydan elementi ilə hasili də kod sözüdür. İstənilən kodda sıfır söz koordinat başlanğıcı kimi götürülən kod sözüdür. Daha dəqiq desək, əgər c kod sözüdürsə, onda $-c$ də kod sözüdür və, beləliklə, $c+(-c)$ də həmçinin kod sözü olar.

Xətti kodlarda hər bir sözün başqa sözlərlə bağlılığı (əlaqəsi) istənilən başqa kodlarda olduğu kimidir. Sıfır sözün ətrafında qonşu kod sözlərinin yerləşməsi istənilən başqa kod sözləri ətrafında kodların yerləşməsinin tipik nümunəsidir. Məsələn, tutaq ki, c hər hansı bir kod sözüdür və $c_1, c_2, ..., c_r$ sözləri bu sözdən hər hansı bir d məsafəsində yerləşən sözlərdir. Onda $c-c$ sıfır söz və $c_1-c, c_2-c, ..., c_r-c$ kodları isə sıfır sözdən d məsafəsində (Xemminq məsafəsində) yerləşən kod sözləridir. Beləliklə, xətti kodların minimal məsafələrini təyin etmək üçün sıfır sözlə ona yaxın başqa kod sözləri arasında məsafənin təyin edilməsi kifayətdir.

Tərif 2. c kod sözünün sıfırdan fərqli komponentlərinin sayına c kod sözünün Xemminq çəkisi deyilir və $w(c)$ kimi işarə olunur.

Teorem 1. Xətti kodlar üçün d^* minimal məsafəsi üçün

$$d^* = \min_{c \neq 0} w(c) = w^*$$

doğrudur, harada ki, bu bərabərlikdə minimum sıfır kod sözündən başqa bütün kod sözləri üzrə götürülür.

İsbatı. Tutaq ki, B xətti koddur. Onda

$$d^* = \min_{\substack{c_i, c_j \in B \\ i \neq j}} d(c_i, c_j) = \min_{\substack{c_i, c_j \in B \\ i \neq j}} d(0, c_i - c_j) = \min_{\substack{c \in B \\ c \neq 0}} w(c).$$ □

Beləliklə, t-sayda səhvi düzəldən xətti kodu tapmaq üçün minimal çəkisi $w^* \geq 2t+1$ şərtini ödəyən xətti kodun tapılması zəruridir.

§2. Xətti kodların matris təsviri

B xətti kodu $GF^n(q)$ fəzasında altfəza təşkil edir. Bu fəzanın bazis vektorlarının istənilən bir çoxluğunun elementləri kodların əmələgətirici matrisi adlanan $(k \times n)$-ölçülü G matrisinin sətrləri kimi istifadə oluna bilər. G matrisinin sətrləri fəzası B xətti kodlarıdır, istənilən kod sözü G matrisinin sətrlərinin xətti kombinasiyasıdır. q^k sayda kod sözlərinin əmələ gətirdiyi çoxluq (n,k) - xətti kodları adlanır.

G matrisinin sətrləri xətti asılı deyildirlər və sətrlərin sayı k altfəzasının ölçüsünə bərabərdir. Bütövlükdə $GF^n(q)$ fəzasının ölçüsü n - dir. Cəmi q^k sayda kod sözü mövcuddur və $GF(q)$ üzərində q^k sayda müxtəlif k -ardıcıllıqları kod sözləri çoxluğuna inikas oluna bilər.

k -ardıcıllıqlarının və kod sözlərinin istənilən qarşılıqlı birqiymətli uyğunluğu kodlaşdırma üçün istsfadə oluna bilər, lakin ən təbii kodlaşdırma üsulu

$$c = i \cdot G \qquad (1)$$

inikasını istifadə edir, harada ki, i informasiya sözü olub kodlaşdırılan informasiya sözlərinin k -ardıcıllığı, c isə əmələ gələn kod sözünün n - ardıcıllığıdır.

(1) münasibəti ilə verilən informasiya sözü ilə kod sözü arasında uyğunluğu koder qurğusu verir və G matrisinin sətrləri kimi istifadə olunan bazis vektorlarının seçilməsindən asılıdır.

Tutaq ki, əmələgətirici matris aşağıdakı kimidir:

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

Bu halda $i = (0\ 11)$ informasiya sözü aşağıdakı kimi kodlaşacaq:

$$c = (0\ 11)\cdot \begin{pmatrix} 1\ 0\ 0\ 1\ 0 \\ 0\ 1\ 0\ 0\ 1 \\ 0\ 0\ \ 1\ 1\ 1 \end{pmatrix} = (01110).$$

Əməlgətirici matris xətti kodların qısa yazılışıdır.

B altfəza olduğundan o, ortoqonal $B^{\perp}$ tamamlayıcısına malikdir, yəni $B^{\perp}$ tamamlayıcısı B altfəzasına ortoqonal olan vektorlardan ibarətdir. Ortoqonal tamalayıcı altfəza olduğundan ona kod kimi baxmaq olar. $B^{\perp}$-yə kod kimi baxdıqda ona B koduna ikili olan (dual) kod deyilir. $B^{\perp}$ ortoqonal tamamlayıcının ölçüsü $(n-k)$-dır və onun istənilən bazisi $n-k$ sayda vektordan ibarətdir. Tutaq ki, H matrisinin sətrləri $B^{\perp}$-nin bazis vektorları sistemidir. Onda c n-ardıcıllığı o zaman kod sözü olar ki, o, H matrisinin bütün sətrlərinə ortoqonal olsun, yəni:

$$c \cdot H^{T} = 0. \qquad (2)$$

(2) münasibəti c-nin kod sözü olub olmadığını yoxlamaq üçün istifadə edilə bidər. H matrisi kodun yoxlayıcı matrisi adlanır. (2) münasibəti hər bir kod sözü üçün ödənildiyindən aşağıdakı alınır:

$$G \cdot H^{T} = 0. \qquad (3)$$

G üçün yuxarıdakı nümunəyə uyğun olaraq H üçün alırıq:

$$H = \begin{pmatrix} 1\,0\,1\,1\,0 \\ 0\,1\,1\,0\,1 \end{pmatrix}.$$

G matrisinin çoxsaylı seçmək üsulu olduğu kimi H matrisini də çoxlu üsulla seçmək olar.

Teorem 1. B kodunun əməlgətirici matrisi $B^{\perp}$ dual kodunun yoxlayıcı matrisidir.

Kodların minimal çəkiləri ilə yoxlayıcı matrislər arasında əlaqə aşağıdakı teorem vasitəsilə təyin olunur:

Teorem 2. B kodu w-dən böyük olmayan Xemminq çəkili sıfırdan fərqli kod sözlərinə malik olması üçün zəruri və kafi şərt H yoxlayıcı matrisinin w sayda xətti asılı olan sütunlar çoxluğuna malik olmasıdır.

İsbatı. Zərurilik. İstənilən c kod sözü üçün $cH^T = 0$ bərabərliyi ödənir. Tutaq ki, c kod sözü w çəkisinə malikdir. c-dən sıfıra bərabər olan komponentləri ataq. Onda alınan bərabərliklər H matrisində w sayda sütunların xətti asılılıq münasibətləri olacaq. Beləliklə, H matrisi w sayda xətti asılı sütunlardan ibarət olar.

Kafilik. Əgər H matrisi w sayda xətti asılı sütunlar çoxluğundan ibarətdirsə, onda w –dan çox olmayan sayda sütundan təşkil olunmuş sıfıra bərabər xətti kombinasiya tapmaq olar. w sayda sıfırdan fərqli əmsallara uyğun olan əmsallar w-dan çox böyük olmayan çəkiyə malik vektor əmələ gətirir və bu vektor üçün $cH^T = 0$ olur. □

Nəticə 1. Kodun w-dan kiçik olmayan çəkiyə malik olması üçün zəruri və kafi şərt H- dan olan $w-1$ sayda sütuna malik hər bir çoxluğun vektorlarının xətti asılı olmamasıdır.

Bu nəticədən belə görünür ki, t sayda səhvi düzəldə bilən (n,k)-kodu tapmaq üçün, kifayətdir ki, istənilən $2t$ sayda sütunları xətti asılı olmayan $(n-k)\times n$ - ölçülü H matrisi mövcud olsun.

Minimal məsafəsi d^*-a bərabər olan verilmiş (n,k) - kodunda əgər hər bir kod sözündə iki mövqe seçib və bu mövqelərdə olan simvolların yerini dəyişsək, onda yeni eyni bir parametrli kod almaq olar. Bu halda əvvəlki koddan trivial olaraq fərqlənən kod alınır. Alınan koda əvvəlki koda ekvivalent kod deyilir.

Ekvivalent kodların G və G' əmələgətirici matrisləri bir-biri ilə bağlıdır. Kod G matirsinin sətrlər fəzasıdır və odur ki, matisin sətrləri üzərində elementar əməliyyatlar yerinə yetirildikdə o, dəyişməz qalır. Kodun koordinatlarının dəyişməsi G matrisində sütunların yerdəyişməsinə ekvivalentdir. Beləliklə, iki kod ancaq və ancaq o zaman ekvivalent olur ki, onların birinin əmələgətirici matrisi o birisinin əmələgətirici matrisindən: 1) sütunların yerdəyişməsi və 2) sətrlər üzərində elementar əməliyyatların aparılması nəticəsində alınır.

Hər bir G əməlgətirici matris hər hansı bir kanonik pilləvari matrisə ekvivalentdir və G matrisinin sətrləri xətti asılı olmadığından ekvivalent matrisin bütün sətrləri sıfırdan fərqlidir. Beləliklə, sütunların yerdəyişməsi dəqiqliyi ilə istənilən əməlgətirici matris ilk k sütununda $k \times k$-ölçülü vahid altmatrisdən ibarət olan matrisə ekvivalentdir. Ekvivalent matrisi aşağıdakı kimi yazmaq olar:

$$G = (I_{k\times k} \vdots P),$$

belə ki, P matrisi $k \times (n-k)$ ölçülü matrisdir, $I_{k\times k}$ isə $k \times k$ - ölçülü vahid matrisdir. Belə şəkildə olan əməlgətirici matris sistematik şəkildə olan əməlgətirici matris adlanır. Tutaq ki, $G = (I_{k\times k} \vdots P)$-dir. Onda H matrisi $H = (-P^T \vdots I_{(n-k)\times(n-k)})$ kimi təyin olunur, belə ki,

$$G \cdot H^T = (I_{k\times k} : P) \cdot \begin{pmatrix} -P \\ \cdots\cdots\cdots \\ I_{(n-k)\times(n-k)} \end{pmatrix} = -P + P = 0 .$$

İndi fərz edək ki, H yoxlayıcı matrisi $H = (P \vdots I_{(n-k)\times(n-k)})$ şəklindədir. Aydındır ki, P altmatrisi $(n-k) \times k$ - ölçülü matrisdir. (3) şərtinə uyğun olaraq G matrisi üçün kanonik pilləvari şəkili tapaq. Aydındır ki, H^T matrisi aşağıdakı şəkildə olar

$$H^T = \begin{pmatrix} P^T \\ \cdots\cdots\cdots\cdots \\ I_{(n-k)\times(n-k)} \end{pmatrix}.$$

Tutaq ki, G matrisi $G = (I_{k\times k} \vdots X)$ şəklində matrisdir, hansı ki, X altmatrisi $k \times (n-k)$ - ölçülü matrisdir. (3) şərtinə görə alarıq:

$$G \cdot H^T = I_{k\times k} \cdot P^T + X \cdot I_{(n-k)\times(n-k)} = P^T + X = 0 .$$

Buradan da $X = -P^T$ alınır. Deməli, G matrisi $G = (I_{k\times k} \vdots -P^T)$ şəklində matris olar.

Nümunə 1. Tutaq ki, $n = 7$, $k = 4$ və H yoxlayıcı matrisi

$$H = \begin{pmatrix} 1010 \vdots 100 \\ 1001 \vdots 010 \\ 0101 \vdots 001 \end{pmatrix}$$

kimidir. Onda buradan P və P^T aşağıdakı kimi olar:

$$P = \begin{pmatrix} 1010 \\ 1001 \\ 0101 \end{pmatrix}, \quad P^T = \begin{pmatrix} 110 \\ 001 \\ 100 \\ 011 \end{pmatrix}.$$

Beləliklə,

$$G = \left(\begin{array}{cccc:ccc} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{array}\right).$$

Tərif 1. Hər bir kod sözü informasiya simvolları ilə başlayan koda sistematik kod deyilir. Qalan simvollar yoxlayıcı simvollar adlanır.

Teorem 3. Hər bir xətti kod xətti sistematik koda ekvivalentdir.

Nümunə 2.

$$G = \begin{pmatrix} 1 & 0 & 0 & : & 1 & 0 \\ 0 & 1 & 0 & : & 0 & 1 \\ 0 & 0 & 1 & : & 1 & 1 \end{pmatrix}, \quad H = \begin{pmatrix} 1 & 0 & 1 & : & 1 & 0 \\ 0 & 1 & 1 & : & 0 & 1 \end{pmatrix}.$$

Bu halda $i = (011)$ informasiya sözü sistematik kod sözü olan $c = (01110)$ sözünə əks olunur.

Koda sistematik halda baxmaqla kodun parametrləri üçün sadə bərabərsizliklər almaq olar. Tutaq ki, hər hansı (n,k) - sistematik xətti kod verilmişdir və d^* minimal məsafədir.

Teorem 4 (Sinqlton sərhədi haqqında). İstənilən xətti (n,k) - kodunun minimal məsafəsi (minimal çəkisi) aşağıdakı bərabərsizliyi ödəyir:

$$d^* \le 1 + n - k .$$

İsbatı. Kodlarda sıfırdan fərqli sözlərin minimal çəkisi d^*-dur. Bir sıfırdan fərqli informasiya simvoluna və $n-k$ sayda yoxlayıcı simvola malik sistematik kod sözü mövcuddur. Belə kod sözü $1+n-k$ -dan böyük çəkiyə malik ola bilməz. Beləliklə, minimal çəki $1+n-k$ kəmiyyətindən çox ola bilməz. □

Tərif 2. $d^* = 1 + n - k$ şərtini ödəyən minimal məsafəyə malik istənilən kod minimal məsafəli kod adlanır.

Sinqlton sərhədi göstərir ki, t sayda səhvi düzəltmək üçün $2t$-dən az olmayan sayda yoxlayıcı simvol olmalıdır (2 yoxlayıcı simvol 1 səhvə). Əksər kodlar, hətta optimallar da, sinqlton sərhədindən olduqca çox sayda yoxlayıcı simvollara malikdirlər, lakin bəzi kodların parametrləri bu sərhəddi bərabərlik halında ödəyirlər. Maksimal məsafəli kodlar dəqiq $2t$ sayda yoxlayıcı simvollara malikdirlər.

§3. Standart düzüm qaydası

Xətti kodların iki kod sözünün fərqi də kod sözü olduğu üçün sıfır söz də kod sözü olacaq. Əgər biz biliriksə ki, xətti kodların hansı alt çoxluğu sıfır sözə ən yaxında yerləşir, onda koordinat başlanğıcının sadə sürüşməsilə asanlıqla müəyyən etmək olar ki, qəbul olunan sözlərin hansı istənilən başqa kod sözlərinə ən yaxında yerləşir.

Tutaq ki, d^* tək ədəddir və $d^* = 2t+1$. Mərkəzində sıfır söz olan t radiuslu kürənin daxilində aşağıdakı nöqtələr çoxluğu yerləşir:

$$S_0 = \{\upsilon \mid d(0,\upsilon) \le t\}.$$

Bu kürə sıfır sözə dekodlaşdırılan bütün qəbul olunan sözləri özündə saxlayır. Mərkəzi c kod sözü olan t radiuslu kürənin daxilində

$$S_c = \{\upsilon \mid d(c,\upsilon) \le t\}$$

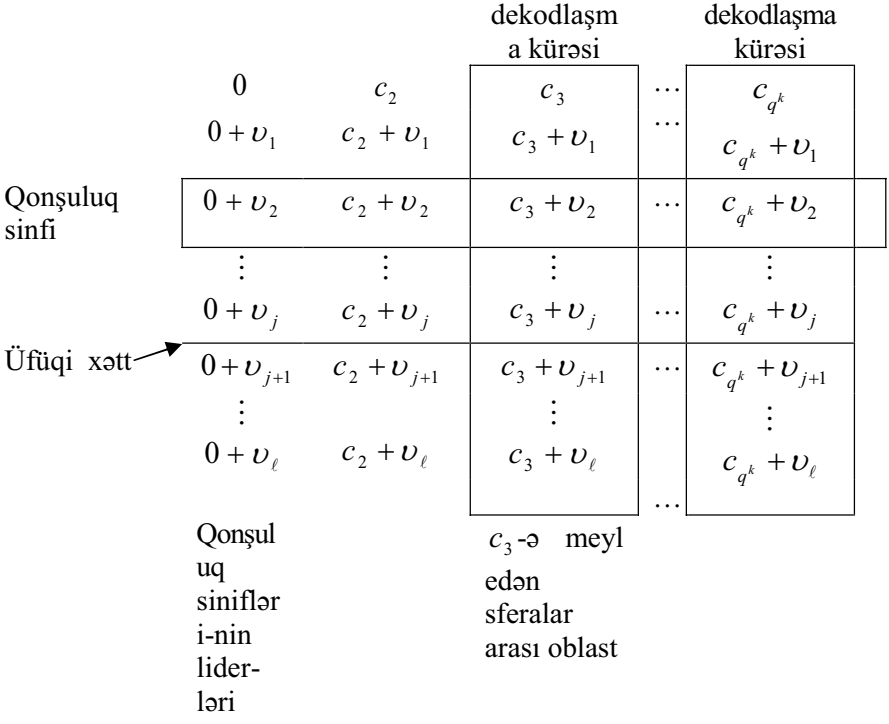
çoxluğundan olan nöqtələr – sözlər yerləşir; onda

$$S_c = S_0 + c = \{\upsilon + c \mid \upsilon \in S_0\}.$$

Standart düzüm bütün dekodlaşdırma kürələrinin təsvir üsulunu özündə əks etdirir. Tutaq ki, $0, c_2, c_3, ..., c_{q^k}$ bütün q^k sayda olan və (n,k) - koduna məxsus olan kod sözləridir. Aşağıdakı şəkildə təsvir olunan standart düzüm cədvəlini belə quraq: Birinci sətrdə bütün kod sözlərini yazaq. $GF^n(q)$ fəzasından qalan sözlər arasından sıfır sözdən 1 məsafəsində yerləşən istənilən sözü götürək və onu υ_1 ilə işarə edək. İkinci sətrə $0+\upsilon_1, c_2+\upsilon_1, c_3+\upsilon_1, ..., c_{q^k}+\upsilon_1$-ləri yazaq. Bu qayda ilə növbəti, yəni üçüncü, dördüncü və s. sətrlər qurulur. j-ci addımda sıfır sözə ən yaxın olan və əvvəlki sətrlərdə rast gəlinməyən kod sözünü götürək, onu υ_j ilə işarə edək və j-ci sətrə $0+\upsilon_j, c_2+\upsilon_j, c_3+\upsilon_j, ..., c_{q^k}+\upsilon_j$ yazaq.

Bu proses o qədər davam etdirilir ki, axırda istifadə olunmamış kod sözü qalmasın.

Əgər koda altqrup kimi baxılarsa, onda bu prosedura bir altqrup üzrə qonşuluq sinifləri əmələ gətirir. Aydındır ki, bu cədvəldə q^{n-k} sətr olacaq. Birinci sütunda olan sözlər qonşuluq siniflərinin liderləri adlanır.



Şəkil 1. Standart düzüm

Cədvəlin qurulma qaydasına görə sıfır sözdən başlayaraq, birinci sütun mərkəzi sıfır sözdə olan dekodlaşdırma kürəsinin daxilində yerləşən bütün sözləri, yəni sıfır sözdən t məsafəsindən çox olmayan məsafədə yerləşən sözləri özündə saxlamalıdır. Sətrlər mərkəzi sıfır kod sözündə olan t radiuslu kürənin daxilini tam doldurduqdan sonra cədvəldə üfüqi xətt çəkilir. Bu xətdən yuxarıda olmayan kod sözləri qala bilər. Onda onlar ən yaxın olan kod sözləri ilə müqayisə olunurlar. Həm tam və həm də

natamam dekoderlər standart düzüm vasitəsilə təsvir oluna bilər. Tam dekoder qəbul olunmuş sözləri ən yaxın kod sözləri ilə tutuşdurur. Qəbul edilən söz cədvəldə tapılır və onun olduğu sütun müəyyən edilir və sütunda ən yuxarıda - birinci sətrdə yerləşən kod sözünə dekodlaşdırılır.

Natamam dekoder qəbul olunmuş sözün ancaq üfüqi xətdən yuxarıda olduğu halda onu dekodlaşdırır.

Nümunə kimi (5,2) - koduna baxaq və tutaq ki, bu kodun əməlgətirici matrisi aşağıdakı kimidir:

$$G = \begin{pmatrix} 10111 \\ 01101 \end{pmatrix}.$$

Bu kod bir səhvi düzəldə bilir. Standart düzüm aşağıdakı kimidir:

00000	10111	01101	11010
00001	10110	01100	11011
00010	10101	01111	11000
00100	10011	01001	11110
01000	11111	00101	10010
10000	00111	11101	01010
00011	10100	01110	11001
00110	10001	01011	11100

1 radiuslu kürələr kəsişmirlər. Hər birində 6 nöqtə - söz olmaqla 4 kürə mövcuddur. 8 nöqtə kürələrdən kənarda qalır.

n və k böyük olduqda standart düzümün sətr və sütunları artır və yuxarıda göstərilən qaydada tətbiq çətinləşir. Ancaq birinci sütunu yadda saxlamaqla cədvəli qısaltmaq olar. Qalan sütunları isə lazım gəldikdə tapmaq olar. Bundan ötrü səhvin sindromu anlayışından istifadə etmək olar.

İstənilən qəbul edilmiş υ vektoru (sözü) üçün sindrom aşağıdakı bərabərliklə təyin olunur:

$$s = \upsilon \cdot H^T.$$

Teorem 1. Bir qonşuluq sinfindən olan vektorların hamısı ancaq bu qonşuluq sinfi üçün olan eyni bir sindroma malikdirlər.

İsbatı. Əgər υ və υ' eyni bir qonşuluq sinfinə aiddirlərsə, onda hər hansı bir y, c_i və c_j kod sözləri üçün $\upsilon = c_i + y$ və $\upsilon' = c_j + y$ olur. İstənilən c kod sözü üçün $c \cdot H^T = 0$ bərabərliyi doğrudur. Buradan aşağıdakını alarıq:

$$s = \upsilon \cdot H^T = y \cdot H^T,\ s' = \upsilon' H^T = y \cdot H^T$$

və, beləliklə, $s = s'$ alınır. Əksinə baxaq, tutaq ki, $s = s'$. Onda $(\upsilon - \upsilon')H^T = 0$ və ona görə $\upsilon - \upsilon'$ kod sözüdür. Beləliklə, υ və υ' eyni bir qonşuluq sinfinə aiddirlər. □

Bir qonşuluq sinfindən olan iki vektor eyni bir sindroma malikdir. Beləliklə, cədvələ sindromu və qonşuluq sinfinin liderini daxil etmək kifayətdir. Bu halda dekodlaşdırma aşağıdakı kimi aparıla bilər. Qəbul edilən υ vektorunun sindromu hesablanır və sindroma əsasən qonşuluq sinfinin lideri tapılır. Bu lider qəbul edilən sözlə dekodlaşdırma kürəsinin mərkəzi olan kod sözünün fərqidir. υ qəbul edilən sözdən qonşuluq sinfinin liderin çıxmaqla səhvi düzəltmək olar. Nümunə kimi aşağıdakı yoxlayıcı matrisi götürək:

$$H = \begin{pmatrix} 11100 \\ 10010 \\ 11001 \end{pmatrix}.$$

Yeni standart düzüm cədvəli aşağıdakı kimidir:

Qonşuluq siniflərinin lideri	Sindromlar
00000	000
00001	001
00010	010
00100	100
01000	101
10000	111
00011	011
00110	110

Bu cədvəl əvvəlki cədvəldən çox sadədir. Tutaq ki, $\upsilon = 10010$ qəbul olunub. Onda $s = \upsilon \cdot H^T = 101$. Uyğun qonşuluq sinfi 01000 kod sözüdür. Buradan alırıq ki, göndərilmiş söz 10010-01000=11010 sözünə bərabərdir, informasiya sözü 11-ə bərabərdir.

§4. Xemminq kodlarının matris təsvirləri

Minimal kod məsafəsi üçdən az olmayan kodlar Nəticə 2.1-ə görə bütün sütunları sıfırdan fərqli və müxtəlif olan yoxlayıcı matrisə malik olmalıdırlar. Əgər ikilik kodlar m sayda sətrə malik olarsa, onda bütün sütunlar m uzunluqlu ikilik ədədlər olur. $2^m - 1$ sayda mümkün olan sütunlar mövcuddur. Uyğun olaraq, əgər H matrisi $d^* \geq 3$ olan ikilik kodların yoxlayıcı matrisi isə və bu matris m sətrə malikdirsə, onda o, ($2^m - 1$)-dən çox olmayan sayda sütuna malik ola bilər. Nəticədə $(2^m - 1, 2^m - 1 - m)$ - kod alınır. Ən sadə və trivial olmayan nümunə $m = 3$ ədədinə uyğundur. Bu halda H və G matrisləri sistematik halda aşağıdakı kimidir:

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

Belə $(2^m - 1, 2^m - 1 - m)$ - kodlar Xemminq kodları adlanırlar.

Aydındır ki, istənilən sütunlar cütlüyü xətti asılı deyil, lakin bəzi üç sütundan ibarət sistem xətti asılı olar. Odur ki, teorem 2.2-yə görə kodun minimal çəkisi 3-ə bərabərdir və kod 1 səhvi düzəldə bilər.

Xemminq kodlarının təyinini ikilik olmayan hallar üçün də ümumiləşdirmək olar. Belə kodların qurulmasının əsas ideyası istənilən iki sütunu xətti asılı olmayan H matrisnin qurulmasından ibarətdir. H matrisinin qurulması üçün $GF(q)$ üzərində $(q \neq 2)$ sıfırdan fərqli olan m - ardıcıllıqların hamısının istifadə etmək lazım deyildir, belə ki, bunlardan bəziləri xətti asılı ola bilər. Xətti asılı olmamazlığı təmin etmək üçün H matrisinin sütunlarının qurulması zamanı ilk sıfırdan fərqli elementi vahidə bərabər olan m -ardıcıllıqları götürmək lazımdır. Belə olduqda bütün sütunlar cüt-cüt xətti asılı olmayacaqlar, lakin sütunların bəzi üçlükləri xətti asılı ola bilərlər və kodda minimal məsafə 3-ə bərabər olar. Bütünlükdə $(q^m - 1)/(q - 1)$ sayda belə müxtəlif sütunlar ola bilər. Beləliklə, alınan kod $[(q^m - 1)/(q - 1), (q^m - 1)/(q - 1) - m]$ - kodu olar. Bir səhvi düzəldən Xemminq kodu hər bir q (hansı ki, bu ədəd üçün $GF(q)$ meydanı mövcuddur) və m üçün mövcuddur.

Bəzi (n,k) - Xemminq kodlarının parametrləri

GF(2)	GF(4)	GF(8)	GF(16)	GF(27)
(7,4)	(5,3)	(9,7)	(17,15)	(28,26)
(15,11)	(21,18)	(73,70)	(273,270)	(757,754)
(31, 26)	(85,81)	(585,581)		
(63,57)	(341,336)			
(127,120)				

Məsələn, $GF(3)$ üzərində (13,10) - Xemminq kodu aşağıdakı H yoxlayıcı və G əməlgətirici matrislər vasitəsilə verilir:

$$H=\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 & 1 & 1 & 0 & 1 & 0 \\ 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 1 & 2 & 0 & 0 & 1 \end{pmatrix},$$

$$G=\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 2 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 2 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 2 & 2 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 2 & 2 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 2 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 2 & 1 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 2 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 2 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 2 & 1 \end{pmatrix}.$$

§5. Mükəmməl və kvazimükəmməl kodlar

Kod sözlərinin altfəza olduğu bütün n - ardıcıllıqları fəzasına baxaq. Bu fəzada dekodlaşdırma kürələri eyni bir radiuslara malikdirlər və hər bir kürənin mərkəzində bir kod sözü dayanır. Tutaq ki, kürələrin radiusları tam ədəd olmaqla artır. Bu artmaq o qədər davam edir ki, artıq radiusların artması kürələrin kəsişməsi olmadan mümükün deyil. Radiusun bu son həddə olan qiyməti kod sözlərinin düzəldilə bilən səhvlərinin sayına bərabərdir. Belə radius kodun sferik bağlanma radiusu adlanır. Radiusun artırılmasını fəzanın bütün nöqtələrinin heç olmazsa bir kürəyə daxil olmasına kimi davam etdirək. Bu son həddə uyğun radius kodların örtülmə radiusu adlanır.

Kodun bağlanma və örtülmə radiusları üst-üstə düşə bilər. Əgər bu belədirsə, onda standart düzümün qurtarması t radiusu daxilində bütün kodların tükənməsi anında baş verir. Bu halda fəzanın bütün nöqtələri kürələrin daxilində qalır və kürələrdən xaricdə heç bir nöqtə qalmır.

Tərif 1. Əgər hər hansı bir eyni radiuslu kod ətrafı kürələr kəsişmədən bütün fəzanı örtürsə, onda belə koda mükəmməl kod deyilir.

$n = (q^m - 1)/(q - 1)$ uzunluqlu Xemminq kodları mükəmməl kodlardır. Bu ona görədir ki, radiusu 1-ə bərabər olan kürə daxilində $1 + n(q-1) = q^m$ nöqtə vardır və fəzada olan nöqtələrin sayının kürələrin sayına nisbəti $q^n / q^k = q^m$ ədədinə bərabərdir, belə ki, $n - k = m$.

Mükəmməl kodlar çox əhəmiyyətli xassələrə malikdirlər, lakin onlar çox az olduqlarından məhdud tətbiq əhəmiyyətinə malikdirlər.

Tərif 2. Əgər hər bir kod sözü ətrafında olan t radiuslu kürələr kəsişmirlərsə və bu kürələrə daxil olmayan bütün sözlər heç olmazsa bir kod sözündən $t+1$ məsafədə yerləşərsə, onda belə kodlara kvazimükəmməl kodlar deyirlər.

Kvazimükəmməl kodlar mükəmməl kodlara nisbətən tez-tez rast gəlinir. Verilmiş n və k üçün kvazimükəmməl kodlar olduğu halda (mükəmməl kodlar mövcud olmadığı halda), onda bu n və k üçün böyük d^*-lara malik kodlar olmur.

FƏSİL IV. DÖVRİ KODLAR

§1. Kod meydanın genişlənməsi nöqteyi nəzərindən

$GF(q)$ üzərində dövri kodlar xətti kodların bir sinfidir və onların xüsusi təsvir imkanı mövcuddur. Bu kodlar $GF(q)$ meydanı üzərində olsalar da onları $GF(q^m)$ üzərində daha aydın təsəvvür etmək olur.

$GF(q)$ üzərində xətti kodlar elementləri $GF(q)$-dən olan matrislər vasitəsilə təsvir oluna bilərlər. Bu matrislər yoxlayıcı matrislər adlanırlar. $GF(q)$ üzərində c o vaxt kod olur ki, $c \cdot H^T = 0$ olsun. Məsələn, (7,4) - Xemminq kodunun yoxlayıcı matrisinə baxaq:

$$H = \begin{pmatrix} 1001011 \\ 0101110 \\ 0010111 \end{pmatrix}.$$

Genişlənmiş meydana keçməklə bu matrisi daha kompakt şəkildə yazmaq olar. H matrisinin sütunlarını $GF(8)$ meydanının elementləri ilə eyniləşdirmək olar. Bu meydanın elementləri çoxhədlilərdir. Matrisin birinci sətrinin elementlərini z^0-a uyğun əmsal, ikinci sətrin elementlərini z^1-ə uyğun əmsal, üçüncü sətrin elementlərini isə z^2-a uyğun əmsal kimi götürək. Onda $GF(8)$ meydanını qurmaq üçün $p(z) = z^3 + z + 1$ çoxhədlisinin istifadə edilməsini nəzərə alaraq və z-i α primitiv elementi kimi götürərək H matrisini aşağıdakı kimi yazaq

$$H = [\alpha^0 \alpha^1 \alpha^2 \alpha^3 \alpha^4 \alpha^5 \alpha^6].$$

$GF(8)$ genişlənmiş meydanı üzərində yoxlayıcı matris (1×7)- ölçülü matrisdir. H matrisini istifadə edərək, kod sözünü $GF(2)$ üzərində elə vektor kimi təyin etmək olar ki, onlar $GF(8)$ genişlənmiş meydanında $cH^T = 0$ və ya $c_0 + c_1\alpha + ... + c_6\alpha^6 = 0$ şərtini ödəsin. Beləliklə, biz kod sözlərini çoxhədlilər kimi təsvir etmək ideyasına gəlirik: c kod sözü $c(x) = c_0 + c_1 x_1 + ... + c_{n-1}x^{n-1}$ çoxhədlisi kimi təsvir olunur və kod sözünün H yoxlayıcı matrisinə vurulması əməliyyatı $c(x)$ çoxhədlisinin

$x=\alpha$ nöqtəsində qiymətinin hesablanması əməliyyatına çevrilir. $c(x)$ çoxhədlisinin kod sözünü əks etdirməsi şərti $c(\alpha)=0$ bərabərliyinə çevrilir. Başqa sözlə desək, $c(x)$ çoxhədlisi ancaq və ancaq o zaman kod sözü olar ki, α elementi $c(x)$ çoxhədlisinin kökü olsun. (7,4) –Xemminq kodunun çoxhədlilərlə təsviri dərəcəsi 6-dan çox olmayan və $GF(2)$ meydanı üzərində təyin olunan çoxhədlilər çoxluğudur. Bu çoxhədlilərin kökü $GF(8)$ üzərində olan α elementidir.

Fərz edək ki, xətti kodun yoxlayıcı H matrisi n sütun və $(n-k)$ sayda sətrə malikdir. Tutaq ki, sətrlərin sayı m -ə bölünür. Belə matrisin m sayda sətrdən ibarət hər bir qrupu $GF(q^m)$ -dən olan elementlərdən ibarət sətrlər kimi təsvir oluna bilər. Beləliklə, H yoxlayıcı matrisi aşağıdakı kimi matrisə çevrilir:

$$H=\begin{pmatrix} \beta_{11}\ \beta_{12}\ldots\beta_{1n} \\ \beta_{21}\ \beta_{22}\ldots\beta_{2n} \\ \ldots\ldots\ldots\ldots\ldots \\ \beta_{r1}\ \beta_{r2}\ldots\beta_{rn} \end{pmatrix}.$$

Burada $r=(n-k)/m$, $\beta_i=(\beta_{i1},\beta_{i2},\ldots,\beta_{in})$ $(i=\overline{1,n})$ sətri isə yoxlayıcı matrisin $m(i-1)+1$, $m(i-1)+2$, $m(i-1)+3$ -cü sətrləri yığımına uyğun gələn və $GF(q^m)$ meydanının elementlərindən ibarət olan sətrdir. Beləliklə, $GF(q)$ meydanı üzərində $(n-k)\times n$ - ölçülü matris əvəzinə $GF(q^m)$ meydanı üzərində $r\times n$ - ölçülü matris alırıq. Biz yoxlayıcı matrisin ancaq aşağıdakı şəkildə yazıldığı bir xüsusi hala baxacağıq

$$H=\begin{pmatrix} \gamma_1^0\ \gamma_1^1\ \ldots\ \gamma_1^{n-2}\ \gamma_1^{n-1} \\ \gamma_2^0\ \gamma_2^1\ \ldots\ \gamma_2^{n-2}\ \gamma_2^{n-1} \\ \vdots\qquad\quad\vdots \\ \gamma_r^0\ \gamma_r^1\ \ldots\ \gamma_r^{n-2}\ \gamma_r^{n-1} \end{pmatrix}. \qquad (1)$$

Burada $n=q^m-1$ və $\gamma_j\in GF(q^m)$, $j=1,\ldots,r$.

Hər bir c kod sözü $GF(q)$ meydanı üzərində vektordur. Beləliklə, $GF(q^m)$ genişlənməsində

$$c \cdot H^T = 0$$

matris bərabərliyi ödənir. Bu bərabərlik H matrisinin yuxarıda götürülən (1) xüsusi şəkli üçün aşağıdakı kimi yazıla bilər:

$$\sum_{i=0}^{n-1} c_i \gamma_j^i = 0,\ j = 1,...,r.$$

Bu münasibət $\gamma_1, \gamma_2, ..., \gamma_r$ elementlərinin $c(x)$ kod çoxhədlisinin kökü olması barədə fikirlə üst-üstə düşür. Baxılan kod $n-1$ dərəcədən çox olmayan,

$$c(x) = \sum_{i=0}^{n-1} c_i x^i$$

kimi təsvir olunan və $c(\gamma_j) = 0,\ j = 1,...,r$ şərtlərini ödəyən çoxhədlilər çoxluğu kimi təyin olunur.

Beləliklə, xətti kodların matris təsvirlərindən onların xüsusi bir alt siniflərinin polinomial təsvirlərinə keçdik. Polinomial təsvir yaxşı kodların axtarışını, koder və dekoder qurğularının qurulmasını asanlaşdırır. Xətti kodların bu alt sinifləri dövri kodlar adlanır.

Məsələn, $GF(16)$ meydanının hər hansı bir primitiv α elementini götürək və hesab edək ki, kodun uzunluğu 15-ə bərabərdir. Kodun $GF(2)$ meydanı üzərində yoxlayıcı matrisini qurmaq üçün $\gamma_1 = \alpha$ və $\gamma_2 = \alpha^3$ götürək. Onda alarıq:

$$H = \begin{pmatrix} \alpha^0 & \alpha^1 & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 & \alpha^8 & \alpha^9 & \alpha^{10} & \alpha^{11} & \alpha^{12} & \alpha^{13} & \alpha^{14} \\ \alpha^0 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & \alpha^{15} & \alpha^{18} & \alpha^{21} & \alpha^{24} & \alpha^{27} & \alpha^{30} & \alpha^{33} & \alpha^{36} & \alpha^{39} & \alpha^{42} \end{pmatrix}. \qquad (2)$$

γ_1 və γ_2 elementlərinin başqa cür seçimi başqa bir H matrisinə – bəzən yaxşı, bəzən isə pis matrisə gətirib çıxarır.

Lazım olduqda yuxarıda (2)-də göstərilən H matrisini $GF(2)$ üzərində olan matrislə əvəz etmək olar. Onun üçün $GF(16)$ meydanının təsvirindən istifadə etmək lazımdır. α elementinin hər bir dərəcəsini 4 bitlik sütunlarla əvəz etmək lazımdır və bu zaman sütunun ən yuxarıdan birinci elementini polinomial yazılışda z^0-ın

əmsalı, ikinci elementini z^1-in əmsalı və i.a. kimi götürmək lazımdır. Beləliklə, alarıq:

$$H = \begin{pmatrix} 1&0&0&0&1&0&0&1&1&0&1&0&1&1&1 \\ 0&1&0&0&1&1&0&1&0&1&1&1&1&0&0 \\ 0&0&1&0&0&1&1&0&1&0&1&1&1&1&0 \\ 0&0&0&1&0&0&1&1&0&1&0&1&1&1&1 \\ \multicolumn{15}{c}{\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots} \\ 1&0&0&0&1&1&0&0&0&1&1&0&0&0&1 \\ 0&0&0&1&1&0&0&0&1&1&0&0&0&1&1 \\ 0&0&1&0&1&0&0&1&0&1&0&0&1&0&1 \\ 0&1&1&1&1&0&1&1&1&1&0&1&1&1&1 \end{pmatrix}.$$

H matrisinin sətrləri xətti asılı deyildir və (15,7) - kodlarını təyin edir. Kodun minimal məsafəsi 5-dir. Bu kodlar $GF(2)$ üzərində 14 dərəcədən böyük olmayan və $GF(16)$ meydanında $c(\alpha)=0$ və $c(\alpha^3)=0$ bərabərsizliklərini ödəyən çoxhədlilər çoxluğu kimi də təsvir edilə bilər. Başqa sözlə, kod sözləri α və α^3 köklərinə malik çoxhədlilərdirlər.

§2. Dövri kodların polinomial təsvirləri

Tərif 1. B xətti kodunda $c=(c_0,c_1,\dots,c_{n-1})$ ixtiyari kod sözü olduqda $c'=(c_{n-1},c_0,c_1,\dots,c_{n-2})$ sözü də B koduna daxil olarsa, onda B kodu dövri kod adlanır.

c' kod sözü c kod sözündən bütün komponentlərin bir mövqe sağa dövri sürüşməsi nəticəsində alınır. Dövri koda nümunə olaraq Xemminq kodlarını göstərmək olar. $GF(q)$ üzərində n uzunluqda hər bir xətti kodlar $GF^n(q)$ fəzasının altfəzasıdır, dövri kodlar isə altfəzanın əlavə dövrülük xassəsinə malik xüsusi halıdır.

$GF^n(q)$ fəzasında hər bir vektor x-ın $n-1$ dərəcədən böyük olmayan çoxhədliləri kimi yazıla bilər. Vektorun komponentləri çoxhədlinin əmsalları kimi götürülür. Çoxhədlilər çoxluğu vektor fəzasının strukturuna malikdir və $GF^n(q)$ fəzasının strukturu ilə identikdir. Bu

çoxhədlilər çoxluğu $GF(q)[x]/(x^n-1)$ halqasının strukturuna malikdir. $GF(q)[x]/(x^n-1)$ halqasında vurma aşağıdakı kimi təyin olunur:

$$p_1(x)\cdot p_2(x)=R_{x^n-1}[p_1(x)\cdot p_2(x)]. \qquad (1)$$

(1) münasibətində bərabərlik işarəsindən sağdakı vurma $GF(q)[x]$ halqasında vurma, soldakı isə - $GF(q)[x]/(x^n-1)$ halqasında vurmadır. Qeyd edək ki, $R_{x^n-1}[f(x)]$ ilə $f(x)$-ın x^n-1 çoxhədlisinə bölünməsindən alınan qalıq işarə olunmuşdur.

Dövri sürüşdürmə $GF(q)[x]/(x^n-1)$ halqasında vurma əməliyyatı kimi yazıla bilər:

$$x\cdot p(x)=R_{x^n-1}[xp(x)].$$

Beləliklə, əgər hər hansı bir kodun kod sözləri çoxhədlilər şəklində verilirsə, onda kod $GF(q)[x]/(x^n-1)$ halqasının altçoxluğudur. Əgər belə koda hər bir $c(x)$ kod sözü ilə yanaşı həm də $x\cdot c(x)$ kod sözü daxildirsə, onda kod dövri koddur.

Teorem 1. $GF(q)[x]/(x^n-1)$ halqasının B alt çoxluğunun dövri kod əmələ gətirməsi üçün zəruri və kafi şərt aşağıdakı iki şərtin ödənməsidir:

1) B alt çoxluğu $GF(q)[x]/(x^n-1)$ halqasında toplama əməlinə görə altqrup əmələ gətirir;

2) əgər $c(x)\in B$ və $a(x)\in GF(q)[x]/(x^n-1)$, onda $R_{x^n-1}[a(x)c(x)]\in B$.

Qeyd. B çoxluğu halqanın idealı adlanır. Ümumi halda I altçoxluğu və R halqası üçün əgər aşağıdakı şərtlər ödənərsə, onda I alt çoxluğu R-in idealı adlanır: 1) I altçoxluğu R halqasının additiv altqrupudur; 2) $r\in R$ və $a\in I$ -dən alınır ki, $a\cdot r\in I$.

İsbatı. Kafilik. Tutaq ki, B alt çoxluğu üçün yuxarıda göstərilən iki şərt ödənir. Onda o toplama və skalyara vurma əməllərinə görə qapalıdır və, beləliklə, alt fəzadır. B alt çoxluğu halqanın bütün elementlərinə, xüsusi halda x elementinə vurma əməlinə görə qapalıdır və, beləliklə, o dövri kod əmələ gətirir.

Zərurilik. İndi fərz edək ki, baxılan alt çoxluq dövri koddur və ona görə də toplama və x elementinə vurma əməlinə görə qapalıdır. Onda o, x elementinin qüvvətlərinə vurma və bu qüvvətlərin xətti kombinasiyalarına nəzərən qapalıdır, yəni istənilən çoxhədliyə vurma əməlinə nəzərən qapalıdır. Beləliklə, o, şərtlərin ikisini də ödəyir. □

B çoxluğundan sıfırdan fərqli və ən kiçik dərəcəyə malik çoxhədlini götürək və onun dərəcəsini $n-k$ ilə işarə edək (bu dərəcə n-dən kiçik olmalıdır). Bu çoxhədlini meydanın elementinə vurmaqla onu çevrilmiş çoxhədli şəklinə (böyük həddinin əmsalı bir ədədinə bərabər olan çoxnədliyə) gətirək. B kodu xətti olduğundan, alınan çoxhədli də B çoxluğuna daxil olacaq. B çoxluğunda $n-k$ dərəcəli çevrilmiş başqa çoxhədli olmayacaq.

B kodunda ən kiçik dərəcəli çevrilmiş çoxhədli B kodunun əməlgətirici çoxhədlisi adlanır və $g(x)$ ilə işarə olunur.

Teorem 2. $g(x)$ əməlgətirici çoxhədlisinin $k-1$ dərəcədən böyük olmayan dərəcəyə malik çoxhədlilərə vurulmasından alınan çoxhədlilər dövri kodlardır.

İsbatı. Teorem 1-ə görə bütün belə çoxhədlilər B koduna daxildir. Əgər hər hansı bir $c(x)$ çoxhədlisi koda daxildirsə, onda bölmə alqoritminə görə

$$c(x) = Q(x)g(x) + s(x),$$

harada ki, $\deg s(x) < \deg g(x)$, və

$$s(x) = c(x) - Q(x)g(x)$$

çoxhədlisi də koddur, çünki sağ tərəfdə hər iki çoxhədli koda daxildir və kod xəttidir. Lakin $s(x)$-in dərəcəsi $n-k$-dan kiçikdir, yəni ən kiçik dərəcəyə malik sıfırdan fərqli çoxhədlinin dərəcəsindən də kiçikdir. Bu isə ziddiyyətdir. Deməli, $s(x) = 0$ və $c(x) = Q(x) \cdot g(x)$. □

Teorem 3. $g(x)$ əməlgətirici çoxhədlisinə malik n uzunluqlu dövri kodun mövcud olması üçün zəruri və kafi şərt $g(x)$ çoxhədlisinin $x^n - 1$ çoxhədlisinin böləni olmasıdır.

İsbatı. Bölmə alqoritminə görə

$$x^n - 1 = Q(x)g(x) + s(x),$$

harada ki, $\deg s(x) < \deg g(x)$. Onda

$$0 = R_{x^n-1}[x^n - 1] = R_{x^n-1}[Q(x)g(x) + s(x)].$$

Beləliklə,

$$0 = R_{x^n-1}[Q(x)g(x) + s(x)].$$

Teorem 1-dən çıxır ki, bu münasibətdə sağ tərəfdə olan birinci çoxhədli kod çoxhədlisidir. Onda $s(x)$ çoxhədlisi də dərəcəsi $g(x)$ çoxhədlisinin dərəcəsindən kiçik olan kod çoxhədlisidir. Yeganə belə çoxhədli $s(x) = 0$ çoxhədlisidir. Beləliklə, $x^n - 1$ çoxhədlisi $g(x)$ çoxhədlisinə bölünür. Sonra, $x^n - 1$ çoxhədlisini bölən hər bir çoxhədli dövri kodların əmələ gətirici çoxhədlisi kimi götürülə bilər. □

Teorem 3-ə görə istənilən dövri kodun $g(x)$ əmələgətirici çoxhədlisi üçün aşağıdakı bərabərlik ödənir:

$$x^n - 1 = g(x)h(x).$$

Burada $h(x)$ hər hansı bir çoxhədlidir və bu çoxhədli yoxlayıcı çoxhədli adlanır. Hər bir $c(x)$ kod sözü aşağıdakı bərabərliyi ödəyir:

$$R_{x^n-1}[h(x)c(x)] = 0,$$

belə ki, hər hansı bir $a(x)$ üçün

$$h(x)c(x) = h(x)g(x)a(x) = (x^n - 1)a(x).$$

Tutaq ki, $c(x)$ ötürülən kod sözüdür. Bu o deməkdir ki, ötürülən kod sözünün simvolları $c(x)$ çoxhədlisinin əmsallarıdır. Tutaq ki, $\upsilon(x)$ ilə qəbul edilən kod sözü işarə edilmişdir və $e(x) = \upsilon(x) - c(x)$. Burada $e(x)$ çoxhədlisi səhv çoxhədlisidir. Bu çoxhədlinin sıfırdan fərqli əmsallarının olduğu mövqelər kanalda ötürmə zamanı səhvlərin baş verdiyi mövqeləri göstərir.

İnformasiya çoxhədlisini $(k-1)$-dən böyük olmayan dərəcəyə malik $i(x)$ çoxhədlisi kimi təsvir edək. Sadə kodlaşdırma aşağıdakı kimidir.

$$c(x) = i(x) \cdot g(x).$$

Bu düstura uyğun koder qurğusu sistematik deyildir, belə ki, bu $c(x)$ koda görə $i(x)$ kodunu ayırmaq mümkün deyildir. Sistematik kodlaşdırma üsulu bir qədər mürəkkəb şəklə malikdir. İdeya informasiya sözünün kod

sözünün böyük əmsalları (komponentləri) kimi yazmaqdan və kiçik əmsalları elə seçməkdən ibarətdir ki, nəticədə mümkün kod alınsın. Beləliklə, kod sözü aşağıdakı kimi yazılır:

$$c(x) = x^{n-k} \cdot i(x) + t(x),$$

harada ki, $t(x)$ elə seçilir ki,

$$R_{g(x)}[c(x)] = 0$$

olsun. Bu ifadələr o deməkdir ki,

$$R_{g(x)}[x^{n-k} i(x)] + R_{g(x)}[t(x)] = 0$$

və $t(x)$ çoxhədlisinin dərəcəsi $(n-k)$-dan, yəni $g(x)$ çoxhədlisinin dərəcəsindən kiçikdir. Beləliklə,

$$t(x) = -R_{g(x)}[x^{n-k} i(x)]$$

və kodlaşdırma qaydası qarşılıqlı birqiymətlidir, belə ki, çoxhədlinin k sayda böyük əmsalları birqiymətli təyin olunub.

Həm sistematik və həm də sistematik olmayan kodlaşdırma qaydası eyni bir kod sözləri çoxluğunu təyin edir, lakin $i(x)$ və $c(x)$ arasında uyğunluq fərqlidir.

Dekodlaşdırma üçün istifadə olunacaq $s(x)$ sindrom çoxhədlisini aşağıdakı kimi təyin edək:

$$s(x) = R_{g(x)}[\upsilon(x)] = R_{g(x)}[c(x) + e(x)] = R_{g(x)}[e(x)].$$

Sindrom çoxhədlisi ancaq $e(x)$ çoxhədlisindən asılıdır, $c(x)$ və $i(x)$ çoxhədlilərindən asılı deyildir.

Beləliklə, aşağıdakı çoxhədliləri daxil etdik:

Əmələgətirici çoxhədli: $g(x)$, $\deg g(x) = n-k$,

Yoxlayıcı çoxhədli: $h(x)$, $\deg h(x) = k$,

İnformasiya çoxhədlisi: $i(x)$, $\deg i(x) = k-1$,

Kod çoxhədlisi: $c(x)$, $\deg c(x) = n-1$,

Səhv çoxhədlisi $e(x)$, $\deg e(x) = n-1$,

Qəbul edilən çoxhədli: $\upsilon(x)$, $\deg \upsilon(x) = n-1$,

Sindrom çoxhədlisi: $s(x)$, $\deg s(x) = n-k-1$.

Teorem 4. Tutaq ki, d^* ədədi B dövri kodunun minimal məsafəsidir. $d^*/2$-dən kiçik çəkiyə malik olan hər bir səhv çoxhədlisinə yeganə sindrom çoxhədlisi uyğundur.

İsbatı. Tutaq ki, $e_1(x)$ və $e_2(x)$ çoxhədlilərinin çəkiləri $d^*/2$-dən kiçikdir və onlara eyni bir sindrom çoxhədlisi uyğundur. Onda

$$e_1(x) = Q_1(x)g(x) + s(x), \quad e_2(x) = Q_2(x)g(x) + s(x)$$

və

$$e_1(x) - e_2(x) = [Q_1(x) - Q_2(x)]g(x). \qquad (2)$$

Fərziyyəyə görə $e_1(x)$ və $e_2(x)$ çoxhədlilərinin hər birinin çəkisi $d^*/2$-dən kiçikdir, onda onların fərqlərinin çəkisi d^*-dan kiçikdir. (1) münasibətdə sağ tərəfdə kod sözü durur. Əgər bu söz sıfırdan fərqli isə, onda onun çəkisi d^*-dan, yəni kodun minimal çəkisindən kiçik deyildir. Beləliklə, sağ tərəfdə sıfır dayanır və ona görə də $e_1(x)$ və $e_2(x)$ bərabərdirlər. □

Beləliklə, səhvlərin düzəldilməsi məsələsi $s(x) = R_{g(x)}[e(x)]$ şərtini ödəyən ən az sayda sıfırdan fərqli əmsallara malik olan $e(x)$ çoxhədlisinin birqiymətli hesablanmasına gətirilir. Çox da böyük olmayan giriş halında bu məsələ cədvəl qurmaq yolu ilə həll oluna bilər. Hər bir $e(x)$ çoxhədlisi üçün $s(x)$ çoxhədlisi hesablanır və cədvəldə saxlanılır. Bu cədvəl sindromlar qiymətinin cədvəli adlanır. $\upsilon(x)$ qəbul edilən kod əsasında $s(x)$ çoxhədlisini hesablayaraq dekoder $s(x)$-i sindromların qiymətləri cədvəlindən tapır və sonra uyğun $e(x)$ çoxhədlisini tapır. Sonra isə $c(x) = \upsilon(x) - e(x)$ düsturu əsasında ötürülən kod sözü tapılır.

§3. Minimal çoxhədlilər və qoşmalar

Məlum olduğu kimi $GF(q)$ meydanı üzərində $x^n - 1$ çoxhədlisini bölən hər bir $g(x)$ çoxhədlisi üçün n uzunluqlu dövri kod mövcuddur. n uzunluqlu dövri kodların əmələgətirici çoxhədlilərini tapmaq məsələsinə baxaq. Bunun üçün $x^n - 1$ çoxhədlisini sadə vuruqlara ayıraq:

$$x^n - 1 = f_1(x) f_2(x) \ldots f_s(x).$$

Burada s ədədi sadə vuruqların sayıdır. Bu vuruqların istənilən alt çoxluqlarına daxil olan elementlərin hasilindən alınan $g(x)$ əmələgətirici

çoxhədli olur. Əgər (x^n-1)-in bütün sadə vuruqları fərqlidirlərsə, onda cəmi 2^s-2 sayda müxtəlif trivial olmayan n uzunluqlu dövri kod vardır ($g(x)=1$ və $g(x)=x^n-1$ trivial hallar nəzərə alınmır).

Tutaq ki, $g(x)$ əmələgətirici çoxhədlidir. Bu x^n-1 çoxhədlisini bölür və, beləliklə,

$$g(x)=\prod_{i\in S} f_i(x),$$

hansı ki, S yuxarıda göstərilən çoxhədlilərin hər hansı bir altçoxluğuna daxil olanlarının indeksləridir. $g(x)$ çoxhədlisi ilə yaradılan dövri kod hər bir $f_i(x), i\in S$, çoxhədlisinə bölünən çoxhədlidən ibarətdir. $g(x)$ çoxhədlisini tapmaq üçün onun bütün sadə çoxhədlilərini tapmaq lazımdır.

Sadə çoxhədlilərin genişlənmiş meydanda kökləri ilə bu çoxhədli arasında əlaqəni araşdıraq.

Tərif 1. $GF(q)$ üzərində kodun $n=(q^m-1)$ uzunluğu primitiv uzunluq adlanır. $GF(q)$ üzərində primitiv uzunluğa malik dövri kod primitiv dövri kod adlanır.

$GF(q^m)$ meydanı $GF(q)$ meydanının genişlənməsi adlanır. Birqiymətli ayırma teoreminə görə $GF(q)$ üzərində

$$x^{q^m-1}-1=f_1(x)f_2(x)...f_s(x)$$

ayrılışı birqiymətlidir. $g(x)$ çoxhədlisi $x^{q^m-1}-1$ çoxhədlisini böldüyü üçün o, yuxarıdakı vuruqların bəzilərinin hasilinə bərabərdir. Digər tərəfdən $GF(q^m)$ meydanının sıfırdan fərqli elementləri $x^{q^m-1}-1$ çoxhədlisinin köklərıdir. Beləliklə, $GF(q^m)$ üzərində

$$x^{q^m-1}-1=\prod_j(x-\beta_j), \qquad (1)$$

harada ki, β_j elementləri $GF(q^m)$-in sıfırdan fərqli elementləridir. Buradan belə çıxır ki, $f_\ell(x), \ell=1,...,s$, çoxhədlilərinin hər biri (1)-də olan xətti vuruqların hasili kimi yazıla bilər və, beləliklə, hər β_j dəqiq bir $f_\ell(x)$ çoxhədlisinin köküdür. Bu $f_\ell(x)$ çoxhədlisi β_j elementinin

minimal çoxhədlisidir və sadəlik üçün o çoxhədlini də $f_j(x)$ kimi işarə edək.

Teorem 1. Tutaq ki, $GF(q^m)$ meydanının $\beta_1,...,\beta_r$ elementləri primitiv kodun $g(x)$ əmələ gətirici çoxhədlisinin kökləridir. $GF(q)$ üzərində $c(x)$ çoxhədlisinin kod olması üçün zəruri və kafi şərt

$$c(\beta_1)=c(\beta_2)=...=c(\beta_r)=0$$

olmasıdır.

İsbatı. Əgər $c(x)=a(x)g(x)$ isə, onda $c(\beta_j)=a(\beta_j)g(\beta_j)=0$ olur. Tərsinə, tutaq ki, $c(\beta_j)=0$. $c(x)$ çoxhədlisini $c(x)=Q(x)\cdot f_j(x)+s(x)$ kimi yazaq, harada ki, $\deg s(x)<\deg f_j(x)$ və $f_j(x)$ çoxhədlisi β_j-ın minimal çoxhədlisidir. Lakin onda

$$0=c(\beta_j)=Q(\beta_j)f_j(\beta_j)+s(\beta_j)=s(\beta_j)$$

bərabərliyindən $s(x)=0$ alınır. Beləliklə, $c(x)$ çoxhədlisi hər bir $j=1,...,r$ üçün $f_j(x)$ çoxhədlisinə bölünməlidir, və ona görə də

$$\text{ƏKOB}\ [f_1(x),f_2(x),...,f_r(x)]=g(x).$$ □

Nümunə 1. $n=15$ uzunluğuna malik bütün dövri kodları tapmalı.

$x^{15}-1$ çoxhədlisini sadə vuruqlara ayıraq:

$$x^{15}-1=(x+1)(x^2+x+1)(x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1).$$

Bərabərliyin sağ tərəfində olan sadə çoxhədlilər çoxluğunun $2^5=32$ altçoxluğu mövcuddur və, beləliklə, 15 uzunluğuna malik dövri kodların 32 əmələ gətirici çoxhədlisi mövcuddur. Bunlardan ikisi ($g(x)=x^{15}-1$, $k=1$ və $g(x)=1$, $k=n$) trivialdır, 30-u isə trivial olmayan dövri kodlar yaradır. Nümunə kimi onlardan birinə baxaq:

$$g(x)=(x^4+x^3+1)(x^4+x^3+x^2+x+1)=x^8+x^4+x^2+x+1.$$

$g(x)$ çoxhədlisinin dərəcəsi 8-dir, ona görə də $n-k=8$, $k=7$-dir. Bu $g(x)$ çoxhədlisinin çəkisi 5 olduğundan, minimal məsafə 5-dən böyük olmur. Beləliklə, baxılan kod (15,7,5)-kodudur və iki səhvi düzəltməyə imkan verir. Yoxlayıcı münasibətlər aşağıdakı kimi yazıla bilər:

$$c(\alpha^i)=0,\quad c(\alpha^j)=0,$$

burada α^i və α^j elementləri x^4+x^3+1 və $x^4+x^3+x^2+x+1$ çoxhədlilərinin $GF(16)$ genişlənmiş meydanında hər hansı bir köklərdir. Xüsusi halda, $c(\alpha)=0$ və $c(\alpha^3)=0$ (əlbəttə, $g(x)$ çoxhədlisinin başqa kökləri də vardır, lakin bu iki kök $g(x)$-ı təyin etməyə kifayətdir və başqa kökləri yoxlamağa ehtiyac yoxdur).

Fərz edək ki, biz kökləri $\beta_1,\beta_2,...,\beta_r$ olan $g(x)$ əmələgətirici çoxhədlisini qurmaq istəyirik. $f_1(x),f_2(x),...,f_r(x)$ ilə bu elementlərin minimal çoxhədlilərini işarə edək. Onda

$$g(x)=\text{ƏKOB}\ [f_1(x),f_2(x),...,f_r(x)].$$

Beləliklə, məsələ verilən β elementi üçün minimal çoxhədlinin tapılması məsələsinə çevrilir.

Tutaq ki, β elementinin $f(x)$ minimal çoxhədlisinin dərəcəsi m'-dir. Onda $GF(q^m)$ meydanında bu çoxhədli m' sayda kökə malik olmalıdır. Bu əlavə köklər aşağıdakı teoremlər vasitəsilə təsvir olunurlar.

Teorem 2. Tutaq ki, $GF(q)$ meydanının xarakteristikası p-dir. Onda $GF(q)$ üzərində istənilən $s(x)$ çoxhədlisi və ixtiyari tam m ədədi üçün aşağıdakı bərabərlik ödənir

$$\left[\sum_{i=0}^{\ell} s_i x^i\right]^{p^m}=\sum_{i=0}^{\ell} s_i^{p^m}\cdot x^{i\cdot p^m}.$$

Bu bərabərlik həm də p-ni onun istənilən qüvvəti ilə əvəz etdikdə də ödənir.

İsbatı. $m=1$ halından başlayaq. $s'(x)$ çoxhədlisini $s(x)=s'(x)\cdot x+s_0$ bərabərliyi ilə təyin edək, onda

$$[s(x)]^p=\sum_{i=0}^{p} C_p^i[s'(x)x]^i s_0^{p-i}.$$

Lakin

$$C_p^i=\frac{p!}{i!(p-i)!}=\frac{p(p-1)!}{i!(p-i)!}$$

və $i=0$ və $i=p$ hallarını çıxmaq şərtiylə sadə p ədədi bu bərabərliyin məxrəcinə daxil deyildir. Deməli, C_p^i tam ədəd olub p-nin misillərinə bərabərdir, yəni mod p-yə görə sıfırdır. Beləliklə,

$$[s(x)]^p = [s'(x)]^p x^p + s_0^p .$$

Həmin müzakirəni $s'(x)$ çoxhədlisi üçün də aparaq və hesablamanı davam etdirək. Bu $m=1$ üçün hökmün isbatını verər:

$$[s(x)]^p = \sum_{i=0}^{\ell} s_i^p x^{ip} .$$

Sonra

$$[s(x)]^{p^2} = [[s(x)]^p]^p = \left[\sum_{i=0}^{\ell} s_i^p x^{ip}\right]^p = \sum_{i=0}^{\ell} s_i^{p^2} x^{ip^2} .$$

Bu hesablamanı ixtiyari sayda təkrarlamaq olar, beləliklə, p-ni onun istənilən qüvvəti ilə əvəz etmək olar. □

Teorem 3. Tutaq ki, $GF(q)$ meydanı üzərində $f(x)$ çoxhədlisi $GF(q^m)$ meydanından olan β elementinin minimal çoxhədlisidir. Onda $f(x)$ həm də β^q elementinin də minimal çoxhədlisidir.

İsbatı. q ədədi meydanın xarakteristikası olan p-nin qüvvəti olduğu üçün, teorem 2-dən alırıq:

$$[f(x)]^q = \sum_{i=0}^{\deg f(x)} f_i^q (x^q)^i .$$

f_i əmsalları $GF(q)$ meydanının elementləridir, bu meydanın elementləri isə $\gamma^q = \gamma$ şərtini ödəyir. Beləliklə,

$$[f(x)]^q = \sum_{i=0}^{\deg f(x)} f_i (x^q)^i = f(x^q) .$$

$f(\beta)=0$ olduğundan, ona görə də $0=[f(\beta)]^q=f(\beta^q)$ və, beləliklə, β^q elementi $f(x)$-in kökü olur. $f(x)$ sadə çoxhədli olduğundan o , β^q üçün də minimal çoxhədlidir. □

Tərif 2. $GF(q)$ meydanı üzərində olan eyni bir minimal çoxhədlinin kökü olan $GF(q^m)$ meydanının iki elementi $GF(q)$ meydanına nəzərən qoşma elementlər adlanırlar.

Ümumi halda elementin m sayda qoşma elementləri mövcuddur. Qeyd edək ki, qoşmalıq münasibəti əsas meydandan asılıdır. Məsələn, $GF(16)$ meydanının iki elementi $GF(2)$ meydanına nəzərən qoşma ola bilər, lakin $GF(4)$ meydanına nəzərən qoşma olmaya bilər.

Teorem 3-ü istifadə etməklə β elementi ilə qoşma olan bütün elementləri yazmaq olar. Əgər $f(x)$ çoxhədlisi β elementi üçün minimaldırsa, onda $f(x)$ çoxhədlisi β^q,β^{q^2} və i.a. elementləri üçün də minimaldır. Beləliklə, aşağıdakı çoxluğun bütün elementləri qoşmadır:

$$\{\beta,\beta^q,\beta^{q^2},...,\beta^{q^{r-1}}\}. \qquad (2)$$

Burada r ədədi $\beta^{q^r}=\beta$ şərtini ödəyən ən kiçik tam ədəddir. Qeyd edək ki, $\beta^{q^m}=\beta$, ona görə də $r\le m$. Yuxarıda göstərilən (2) çoxluğu qoşma elementlər çoxluğu adlanır. Bütün qoşma elementlər $f(x)$ çoxhədlisinin köklərıdir. Aşağıdakı teorem göstərir ki, onlardan başqa köklər yoxdur.

Teorem 4. β elementinin minimal çoxhədlisi aşağıdakı kimidir:

$$f(x)=(x-\beta)(x-\beta^q)...(x-\beta^{q^{r-1}}). \qquad (3)$$

İsbatı. Teorem 3-ə görə (3)-ün sağ tərəfində iştirak edən bütün elementlər β elementinin minimal çoxhədlisinin kökü olmalıdır və minimal çoxhədlinin dərəcəsi $f(x)$-ın dərəcəsindən kiçik olmamalıdır. Ona görə də göstərmək lazımdır ki, $f(x)$-in bütün əmsalları $GF(q)$ meydanındandır. x^q-x çoxhədlisinin köklərinin $GF(q^m)$-də altmeydan əmələ gətirmə faktından istifadə edək.

Hər şeydən əvvəl $[f(x)]^q$-nü hesablayaq:

$$[f(x)]^q = (x-\beta)^q (x-\beta^q)^q \ldots (x-\beta^{q^{r-1}})^q = (x^q-\beta^q)(x^q-\beta^{q^2})\ldots(x^q-\beta).$$

Burada sonuncu bərabərlik teorem 2-dən və $\beta^{q^r} = \beta$ olması faktından çıxır. Beləliklə,

$$[f(x)]^q = f(x^q) = \sum_i f_i x^{iq}.$$

Eyni zamanda teorem 2-nin hökmünə görə

$$[f(x)]^q = [\sum_i f_i x^i]^q = \sum_i f_i^q x^{iq}.$$

Beləliklə, hər bir i üçün $f_i^q = f_i$ və f_i əmsalı $GF(q)$ altmeydanına daxildir. □

Nümunə 2. Tutaq ki, α elementi $GF(256) = GF(2^8)$ meydanının primitiv elementidir. α elementinin minimal çoxhədlisini quraq.

α elementinə qoşma olan elementlər çoxluğu aşağıdakı çoxluqdur:

$$\{\alpha, \alpha^2, \alpha^4, \alpha^8, \alpha^{16}, \alpha^{32}, \alpha^{64}, \alpha^{128}\}.$$

Bu çoxluq α^{128} elementi ilə qurtarır, belə ki, $\alpha^{255} = 1$ və, beləliklə, $\alpha^{256} = \alpha$ - çoxluqda olan elementə bərabərdir. α elementinin minimal çoxhədlisi:

$$f(x) = (x-\alpha)(x-\alpha^2)(x-\alpha^4)(x-\alpha^8)(x-\alpha^{16})(x-\alpha^{32})(x-\alpha^{64})(x-\alpha^{128}).$$

Mötərizələr açıldıqdan sonra alınan əmsallar $GF(2)$ meydanından olar.

Nümunə 3. $GF(256) = GF(2^8)$ meydanı üzərində α^7 elementinin minimal çoxhədlisini qurmalı.

α^7 elementini özündə saxlayan qoşma elementlər çoxluğu aşağıdakıdır:

$$\{\alpha^7, \alpha^{14}, \alpha^{28}, \alpha^{56}, \alpha^{112}, \alpha^{224}, \alpha^{193}, \alpha^{131}\}.$$

α^7 elementinin minimal çoxhədlisi:

$$f(x) = (x-\alpha^7)(x-\alpha^{14})(x-\alpha^{28})(x-\alpha^{56})(x-\alpha^{112}) \times$$

$$\times (x-\alpha^{224})(x-\alpha^{193})(x-\alpha^{131}).$$

Bu münasibətdə mötərizələr açıldıqdan sonra əmsallar $GF(2)$ meydanının elementləri olar.

Nümunə 4. $GF(256)$ meydanı üzərində α^7 elementinin minimal çoxhədlisini qurmalı və əsas meydan kimi $GF(4)$ meydanını götürməli.

α^7 elementini özündə saxlayan qoşma elementlər çoxluğu aşağıdakı çoxluq olar:

$$\{\alpha^7, \alpha^{28}, \alpha^{112}, \alpha^{193}\}.$$

α^7 elementinin $GF(4)$ üzərində minimal çoxhədlisi aşağıdakı çoxhədlidir:

$$f(x) = (x-\alpha^7)(x-\alpha^{28})(x-\alpha^{112})(x-\alpha^{193}),$$

harada ki, mötərizələr açıldıqdan sonra alınan əmsallar $GF(4)$ meydanının elementləri olar. Bu elementlərin $GF(4)$-dən olmasını göstərmək üçün $GF(4)$ altmeydanının elementlərini $GF(256)$ meydanının elementləri arasından ayırmaq lazımdır. $GF(256)$ meydanının $GF(4)$ altmeydanını təşkil edən elementlər $\{0,1,\alpha^{85},\alpha^{170}\}$ çoxluğunu təşkil edirlər, belə ki, $GF(256)$ meydanının elementləri arasında ancaq α^{85} və α^{170} elementləri üç tərtibinə malikdirlər.

Nümunə 5. $GF(3^3)$ meydanının elementlərinin $GF(3)$ meydanı üzərində minimal çoxhədlilərini tapmalı.

$GF(3^3)$ meydanı $GF(3)$ meydanı üzərində $p(x) = x^3 + 2x + 1$ sadə çoxhədlisi əsasında qurulur və II fəsildə §9-da bu meydanın elementləri təsvir olunmuşdur.

α, α^3 və α^9 elementləri qoşma elementlərdir. Odur ki,

$$f_\alpha(x) = f_{\alpha^3}(x) = f_{\alpha^9}(x) = x^3 + 2x + 1.$$

α^2, α^6 və α^{18} elementləri qoşma elementlərdir. Odur ki,

$$f_{\alpha^2}(x) = f_{\alpha^6}(x) = f_{\alpha^{18}}(x) = (x-\alpha^2)(x-\alpha^6)(x-\alpha^{18}) =$$

$$= x^3 - (\alpha^2 + \alpha^6 + \alpha^{18})x^2 + (\alpha^8 + \alpha^{20} + \alpha^{24})x - \alpha^{26} =$$

$$= x^3 + x^2 + x + 2.$$

α^4, α^{12} və α^{10} elementləri qoşma elementlərdir. Odur ki,

$$f_{\alpha^4}(x) = f_{\alpha^{12}}(x) = f_{\alpha^{10}}(x) = (x-\alpha^4)(x-\alpha^{12})(x-\alpha^{10}) =$$

$$= x^3 - (\alpha^4 + \alpha^{12} + \alpha^{10})x^2 + (\alpha^{16} + \alpha^{14} + \alpha^{22})x - \alpha^{26} = x^3 + x^2 + 2.$$

İndi isə primitiv olmayan dövri kodlara baxaq. Tutaq ki, kodun uzunluğu n ədədi $(q^m - 1)$-dən fərqlənir.

Teorem 5. Tutaq ki, $GF(q)$ sonlu meydanıdır. Əgər n və q qarşılıqlı sadədirlərsə, onda hər hansı bir m üçün $x^n - 1$ çoxhədlisi $x^{q^m-1} - 1$ çoxhədlisini bölür və $x^n - 1$ çoxhədlisi $GF(q)$ meydanının genişlənməsi olan $GF(q^m)$ meydanında düz n sayda müxtəlif köklərə malikdir.

İsbatı. Hər hansı bir m üçün ancaq n-in $(q^m - 1)$-i bölməsini isbat etmək zəruridir. n-in $(q^m - 1)$-i bölməsi halında, yəni hər hansı bir b üçün $q^m - 1 = nb$ olması halında aşağıdakı doğrudur:

$$x^{q^m-1} - 1 = (x^n)^b - 1 = (x^n - 1)(x^{n(b-1)} + x^{n(b-2)} + \ldots + x^n + 1).$$

Beləliklə, $x^n - 1$ çoxhədlisi $x^{q^m-1} - 1$ çoxhədlini bölür. Beləliklə, $x^n - 1$ çoxhədlisi $GF(q^m)$ üzərində n sayda müxtəlif köklərə malikdir, belə ki, $x^{q^m-1} - 1$ çoxhədlisi bu meydan üzərində $q^m - 1$ sayda müxtəlif köklərə malikdir.

n-in hər hansı bir m üçün $(q^m - 1)$-i bölməsini isbat etmək üçün bölmə alqoritmindən istifadə edək və aşağıdakı $n+1$ sayda bərabərliyi yazaq:

$$\begin{aligned}
q &= Q_1 \cdot n + s_1, \\
q^2 &= Q_2 \cdot n + s_2, \\
q^3 &= Q_3 \cdot n + s_3, \\
&\vdots \\
q^n &= Q_n \cdot n + s_n, \\
q^{n+1} &= Q_{n+1} \cdot n + s_{n+1}.
\end{aligned}$$

Bu münasibətlərdə bütün qalıqlar 0 və $n-1$ ədədləri arasında yerləşirlər. Bu qalıqlar cəmi $n+1$ saydadırlar və ona görə onlardan ən azı ikisi bir-birinə bərabərdirlər. Tutaq $s_i = s_j$ və $i < j$. Onda

$$q^i - q^j = Q_i \cdot n + s_i - (Q_j \cdot n + s_j)$$

və ya

$$q^j (q^{i-j} - 1) = (Q_i - Q_j) n .$$

q və n qarşılıqlı sadə ədədlər olduğundan, n ədədi $(q^{i-j} - 1)$ ədədini bölməlidir. $m = i - j$ qəbul etsək teoremin isbatı yekunlaşar. □

Bu teoremi istifadə edərək n və q qarşılıqlı sadə ədədlər olduğu halda istənilən dövri kodu uyğun genişlənmiş meydanda təsvir etmək olar. n uzunluqlu dövri kodun $g(x)$ əmələgətirici çoxhədlisi $x^n - 1$ çoxhədlisini bölür. Öz növbəsində sonuncu da $x^{q^m-1} - 1$ çoxhədlisini bölür. Deməli, $g(x)$ çoxhədlisi $x^{q^m-1} - 1$ çoxhədlisini də bölür. Tutaq ki, α elementi $GF(q^m)$ meydanının primitiv elementidir. Tutaq ki, $q^m - 1 = nb$ və $\beta = \alpha^b$. Ona görə də $x^n - 1$ çoxhədlisinin (və həm də $g(x)$-in) bütün kökləri β-nın qüvvətləri kimi nəzərə çarpır. $(x^n - 1)$-in sadə bölənlərinin kökləri ancaq belə elementlərdir.

Beləliklə, deyə bilərik ki, əgər α əvəzinə $\beta = \alpha^b$-ni istifadə ediriksə və əmələgətirici çoxhədlinin kökləri çoxluğunu ancaq β-nın dərəcələri ilə məhdudlaşdırırıqsa, onda biz $n = (q^m - 1)/b$ uzunluqlu dövri kod alırıq.

§4. Dövri kodların matris təsvirləri

§3-də kodların yoxlayıcı matrisləri ilə çoxhədlilərin genişlənmiş meydandan olan kökləri arasında əlaqə verilmişdir. Yoxlayıcı matrislərin yaradılması üçün çoxlu üsullar mövcuddur. Əgər $g(x)$-ın sıfırları $\gamma_j \in GF(q^m),\ j = 1,...,r$ isə, onda

$$\sum_{i=0}^{n-1} c_i \gamma_j^i = 0, \quad j = 1,...,r. \tag{1}$$

(1) münasibətini aşağıdakı matris şəklində yazmaq olar

$$c \cdot H^T = 0. \tag{2}$$

Burada $c = (c_1, c_2, ..., c_{n-1})$, H isə aşağıdakı matrisdir:

$$H = \begin{pmatrix} \gamma_1^0 & \gamma_1^1 \dots \gamma_1^{n-1} \\ \gamma_2^0 & \gamma_2^1 \dots \gamma_2^{n-1} \\ \vdots \\ \gamma_r^0 & \gamma_r^1 \dots \gamma_r^{n-1} \end{pmatrix}. \tag{3}$$

(3)-də olan $r \times n$ - ölçülü və $GF(q^m)$ üzərində olan H matrisini $GF(q)$ üzərində olan və $rm \times n$ ölçüsünə malik matrislə əvəz edək. Bunun üçün hər bir β elementini onu $GF(q)$ meydanında təmsil edən çoxhədlisinin əmsallarının sütun vektoru ilə əvəz etmək lazımdır. Nəticədə alınan yoxlayıcı matrisinin bəzi sətrləri xətti asılı ola bilər və, beləliklə, artıq ola bilər. Bu matrisdən xətti asılı olmayan sətrli matris qurmaq üçün zəruri olan ən az sayda sətrləri atılmasıdır. Bu, kodun yoxlayıcı matrisinə gətirib çıxarır.

Təsvir olunan prosedura kodun əmələgətirici çoxhədlisinin kökləri ilə kodun yoxlayıcı matrisi arasında əlaqəni aydınlaşdırsa da o, istifadə üçün çox çətindir.

Genişlənmiş meydana keçmədən də əmələgətirici çoxhədliyə görə zəruri olan matrisi qurmaq olar. Bunu etmək üçün olan üsullardan biri əmələgətirici çoxhədliyə görə bilavasitə əmələgətirici matrisin qurulmasıdır. Kod sözü $c(x) = i(x) \cdot g(x)$ kimi yazıldığından matris şəklində aşağıdakını əldə edirik:

$$G = \begin{pmatrix} 0 & \dots & 0 & g_{n-k} & g_{n-k-1} \dots g_2 & g_1 & g_0 \\ 0 & \dots & g_{n-k} & g_{n-k-1} & g_{n-k-2} \dots g_1 & g_0 & 0 \\ 0 & \dots & g_{n-k-1} & g_{n-k-2} & g_{n-k-3} \dots g_0 & 0 & 0 \\ \vdots & & & & & \vdots & \\ g_{n-k} \dots & & & & & 0 & 0 \end{pmatrix}.$$

Onda yoxlayıcı matris aşağıdakı kimi olar.

$$H=\begin{pmatrix} 0 & 0 & 0 & \dots & & & h_{k-1} & h_k \\ \vdots & & & & & & \vdots & \vdots \\ 0 & h_0 & h_1 & \dots & h_{k-1} & h_k & 0 & 0 \\ h_0 & h_1 & h_2 & \dots & h_k & 0 & 0 \dots 0 & 0 \end{pmatrix}.$$

Burada $h(x)$ dövri kodun yoxlayıcı çoxhədlisidir. $G\cdot H^T=0$ bərabərliyini yoxlamaq üçün $u_r=\sum_{i=0}^{r} g_{r-i}h_i$ kəmiyyətinə baxaq. $h(x)\cdot g(x)=x^n-1$ olduğundan, $u_r=0,\ \ 0<r<n$ olmalıdır. Onda

$$G\cdot H^T=\begin{pmatrix} u_{n-1} & u_{n-2} & \dots & u_k \\ u_{n-2} & u_{n-3} & \dots & u_{k-1} \\ \dots & \dots & \dots & \dots \\ u_{n-k} & u_{n-k-1} & \dots & u_1 \end{pmatrix}=0.$$

Beləliklə, H matrisi doğrudan da yoxlayıcı matrisdir.

Dual kodun əməlgətirici çoxhədlisi $\tilde{h}(x)=x^k h(x^{-1})$ kimi təyin oluna bilər.

Əməlgətirici matrisi sistematik şəkildə də çox sadə almaq olar. Qalıqlı bölmə alqoritmindən istifadə edək və hər bir $i=1,\dots,k$ informasiya mövqesi üçün aşağıdakı çoxhədlini yazaq:

$$x^{n-i}=Q_i(x)g(x)+s_i(x),\ \ i=1,\dots,k,$$

harada ki,

$$s_i(x)=\sum_{j=0}^{n-k-1} c_{ji}x^j.$$

Onda $x^{n-i}-s_i(x)$ çoxhədlisi kod sözüdür, belə ki,

$$x^{n-i}-s_i(x)=Q_i(x)g(x).$$

Bu münasibətin sol tərəfində olan çoxhədlinin əmsallarından istifadə etməklə əməlgətirici matrisi aşağıdakı kimi yazmaq olar:

$$G=\begin{pmatrix} -s_{0,k} & \dots & -s_{(n-k-1),k} & 1 & 0 & \dots & 0 \\ -s_{0,k-1} & \dots & -s_{(n-k-1),k-1} & 0 & 1 & \dots & 0 \\ \vdots & & & & & & \\ -s_{0,1} & \dots & -s_{(n-k-1),1} & 0 & 0 & \dots & 1 \end{pmatrix}. \qquad (4)$$

Bu sistematik əməlgətirici matrisdə informasiya simvollarının koordinatlarının indeksləri $(n-k)$-dan $(n-1)$-ə kimi dəyişir. Belə əməlgətirici matrisi təsvir etmək üçün x^i -ni $g(x)$ -a bölməklə alınan $s_i(x)$ qalıq çoxhədlisini hesablamaq lazımdır.

(4) əməlgətirici matrisinə əsasən H yoxlayıcı matrisini də yazmaq olar:

$$H=\begin{pmatrix} 1 & 0 & \dots & 0 & s_{0,k} & \dots & s_{0,1} \\ 0 & 1 & \dots & 0 & s_{1,k} & \dots & s_{1,1} \\ \vdots & & & \vdots & & & \vdots \\ 0 & 0 & \dots & 1 & s_{(n-k-1),k} & \dots & s_{(n-k-1),1} \end{pmatrix}.$$

§5. Dövri kodlaşdırmanın realizəsi

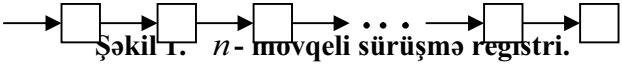
Dövri kodlaşdırmanın realizəsini, yəni informasiya sözünü kod sözünə çevirən koder, qəbuledilən sözdə səhvlərin aşkarlanmasını və korreksiyasını həyata keçirən, koddan informasiya sözünü ayıran dekoder qurğularının realizəsini iki üsulla qurmaq olar. Birinci üsul sxem üsuludur, ikinci üsul isə proqram üsuludur.

Dövri kodların sxem üsulu ilə realizəsi onların rəqəm məntiqi qurğuları vasitəsilə realizə edilməsidir. Rəqəm məntiqi qurğularını sürüşmə registrləri vasitəsilə asanlıqla realizə etmək olar. Bundan başqa sxemlərin qurulmasında triggerlər, sayğaclar və s. istifadə olunduğundan belə sxemləri ardıcıllıqlı maşınlar kimi də təsvir etmək olar.

1. Sonlu meydan cəbri üçün məntiqi dövrələr. Qalua meydanları cəbrinin əməliyyatlarını məntiqi dövrələr vasitəsilə çox asanlıqla realizə etmək olar, xüsusilə də q kəmiyyəti iki ədədinin qüvvəti olduqda. Dövri kodların realizəsi zamanı meydanın elementlərini yadda saxlamaq üçün sürüşmə registrlərinin mövqeləri adlanan dövrə elementi və sonlu meydanda hesab əməliyyatlarını yerinə yetirmək üçün dövrə elementləri lazım gəlir. Bu elementlər istənilən $GF(q)$ meydanı üçün təyin olunur, lakin buna baxmayaraq onlar ikilik elementlər vasitəsilə qurulur.

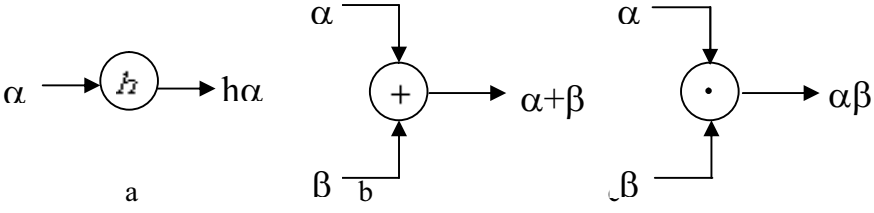
Sürüşmə registri şəkil 1-də verilir və yaddaş elementləri ardıcıllığı kimi təsvir olunurlar. Bu yaddaş elementləri mövqelər, yaxud da mərtəbələr adlanır. Bu yaddaş elementləri triggerlərdir. Hər bir mövqe $GF(q)$ meydanının bir elementini saxlaya bilər. Hər mövqedə olan simvol onu tərk etdikdə bu mövqedən ox işarəsi ilə ayrılan növbəti mövqeyə yazılır. Əgər

sürüşmə registrində n sayda yaddaş elementi (mövqe) olarsa, onda o n-mövqeli yaxud da n-uzunluqlu sürüşmə registri adlanır. Hər bir mövqe giriş xətti ilə təmin olunur. Bu xətlə mövqeyə $GF(q)$ meydanının elementi daxil olur. Əgər giriş üçün başqa göstəriş yoxdursa, onda giriş simvolu meydanın sıfır elementinə bərabər götürülür. Takt adlanan diskret zaman anlarında yaddaş elementlərində yerləşən meydan elementləri giriş xəttində olan meydan elementləri ilə əvəz olunur. Müasir elektron registrləri saniyədə milyardlarla taktları aşan takt tezliklərində işləməyə imkan verir.



Şəkil 1. n- mövqeli sürüşmə registri.

Məntiqi dövrələrdə sürüşmə registrləri ilə yanaşı skalyara vurucu (şəkil 2,a), cəmləyici (şəkil 2,b) və vurucu (şəkil 2,c) elementləri istifadə olunur. Skalyara vurucu bir dəyişənli funksiya kimi təsvir olunur, yəni giriş dəyişəni $GF(q)$ meydanının qeyd olunmuş elementinə vurulur. Cəmləyici və vurucu $GF(q)$ meydanından qiymət alan iki giriş dəyişənli funksiya kimi təsəvvür olunur. İkilik halda cəmləyici «və yanını istisnası» və ya $\mathrm{mod}2$ üzrə toplama elementi, vurucu isə «və» yaxud da məntiqi vurma (konyunksiya) elementi adlanır.

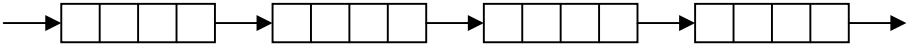


Şəkil 2. a-skalyara vurucu, b-cəmləyici, c - vurucu.

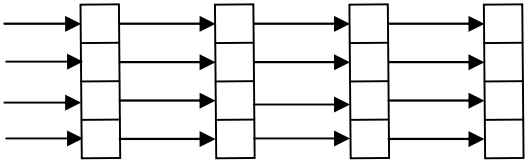
Yuxarıda adı çəkilən dövrə elementlərini istənilən $GF(q)$ meydanı üçün ikilik elementlərdən qurmaq olar. q ədədi ikinin qüvvəti olduqda bunun necə edilməsini təsvir edək. $GF(2^m)$ meydanının elementləri m sayda bitlərin yığımı kimi yazılır və dövrələrdə paralel (bir zaman anında m xəttin (naqilin) hər birində bir bit) və ya ardıcıl (bir zaman anında bir xətdə bir bit) olaraq realizə oluna bilər. $GF(2^m)$ meydanının

elementlərinin ikilik sürüşmə registrlərində iki realizə üsulu şəkil 3-də təsvir olunur. Bu təsvir $GF(16)$ meydanı halında nəzərdə tutulur. Meydanın hər bir elementi 4 bitlə təmsil olunur, meydan elementlərinin ardıcıllığı isə 4-bitlik ədədlər ardıcıllığı ilə yazılır. Meydanın elementləri ardıcıl və ya paralel olaraq, yəni bir və ya dörd xətlə (naqillə) qurulur. Ardıcıl qurma halında $GF(16)$ üçün sürüşmə registri uzunluğu dörd dəfə böyük olan ikilik registr şəklində realizə olunur. Meydanın elementlərinin növbəti mövqeyə sürüşməsi üçün dörd takt tələb olunur.

Şəkil 4-də $GF(16)$ meydanında elementlərin toplanması dövrəsi həm ardıcıl və həm də paralel qurma halında verilir. Hər bir halda cəmləmə yerinə yetirilməzdən əvvəl toplananlar uyğun sürüşmə registrlərinə daxil edilir, cəm isə üçüncü sürüşmə registrində əmələ gəlir. Ardıcıl qurma halında toplama əməlinin yerinə yetirilməsi üçün dörd takt, paralel variantda isə cəmi bir takt lazım gəlir, lakin cəmləyici daha çox sayda naqillərdən və mod *2* üzrə cəmləyicidən ibarət olur. Lazım olduqda toplananlar əvvəllər yerləşdikləri sürüşmə registrinə qaytarıla bilərlər.

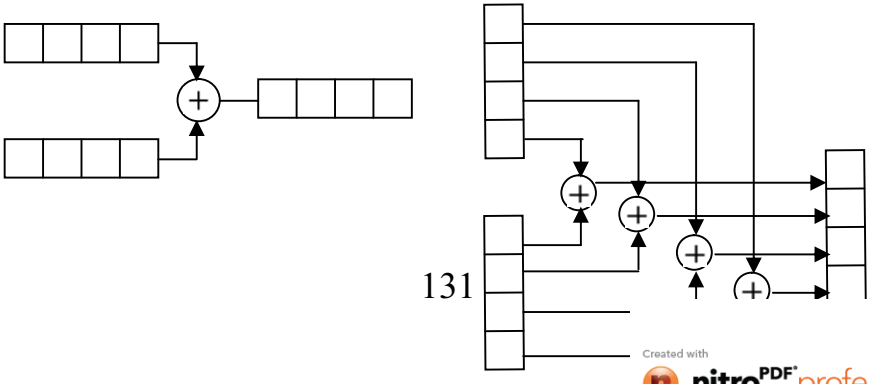


a



Şəkil 3. 16 elementdən ibarət olan meydan üçün ikilik komponentlərdən

sürüşmə registrlərinin qurulması. a - ardıcıl qurma; b -paralel qurma.



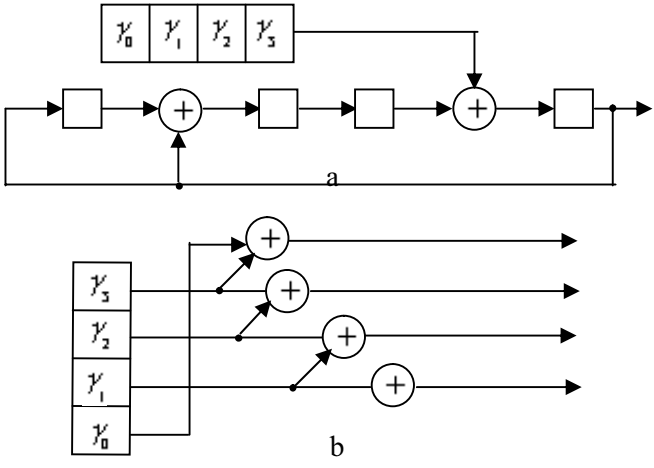
b

Şəkil 4. Meydanın iki elementinin toplanması.
a-ardıcıl variant; b-paralel variant.

Şəkil 5-də $GF(16)$ meydanının ixtiyari bir elementinin $GF(16)$ meydanının $\beta = z^3$ sabitinə vurucusu təsvir olunur. Bu qurğunu təsvir etmək üçün $GF(16)$ meydanının təsvirini konkretləşdirmək lazımdır. Tutaq ki, meydan $p(z) = z^4 + z + 1$ primitiv çoxhədlisi vasitəsilə qurulmuşdur və $\gamma = \gamma_3 z^3 + \gamma_2 z^2 + \gamma_1 z + \gamma_0$ meydanın ixtiyari bir elementidir. Onda

$$\begin{aligned} \beta\gamma &= \gamma_3 z^6 + \gamma_2 z^5 + \gamma_1 z^4 + \gamma_0 z^3 = \\ &= (\gamma_3 + \gamma_0) z^3 + (\gamma_3 + \gamma_2) z^2 + (\gamma_2 + \gamma_1) z + \gamma_1. \end{aligned} \qquad (1)$$

Bu bərabərlikdən bilavasitə skalyara vurucunun paralel variantı alınır. Bu vurucunun ardıcıl variantda (1) bərabərliyinin hər iki sətri istifadə olunur: Əvvəlcə $\gamma_3 z^6 + \gamma_2 z^5 + \gamma_1 z^4 + \gamma_0 z^3$ hesablanır, sonra isə $z^4 + z + 1$ moduluna görə müqayisə olunur. Vurma əməlini yerinə yetirmək üçün ardıcıl variantda dörd takt istifadə olunur.



Şəkil 5. Meydanın $\beta = z^3$ sabitinə vurma.

a - ardıcıl variant; b - paralel variant.

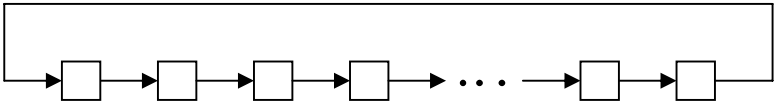
2. Rəqəm filtrləri. Sürüşmə registrləri $GF(q)$ meydanı üzərində çoxhədlilərin vurulması və bölünməsi üçün istifadə olunduğundan onlardan koder və dekoderlərin qurulmasında geniş istifadə oluna bilər. Bundan başqa sürüşmə registrləri çoxhədlilər üzərində bəzi əməliyyatların daha yaxşı başa düşülməsinə köməklik edən psevdoriyazi işarələmə kimi istifadə olunmaqla koder və dekoderlərin nəzriyyəsinin inkişafında çox faydalıdır. Sürüşmə registrləri dövrəsini həm də filtrlər kimi də adlandırırlar.

n uzunluqlu registrlərdə saxlanılan n simvolu $n-1$ dərəcəli çoxhədlinin əmsalları kimi interpretasiya etmək olar. Adətən şərti olaraq qəbul olunur ki, registrlər soldan sağa sürüşürlər. Bu da çoxhədlinin əmsallarının sürüşmə registrində azalma çırası ilə sağdan sola əmələ gəlməsinə gətirib çıxarır.

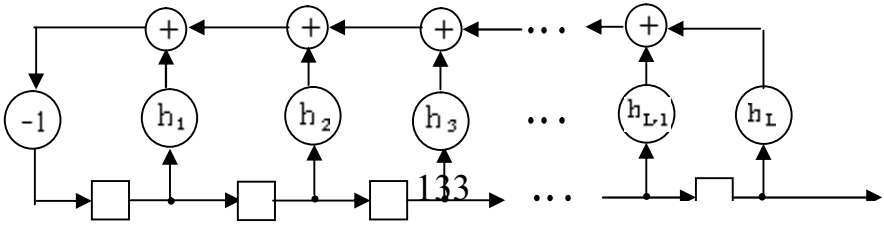
Çoxhədliləri dövri sürüşdürmək üçün sürüşdürmə registrlərinin qapalı dairəsi istifadə olunur. Şəkil 6-da $n-1$ dərəcəli çoxhədliləri dövri sürüşdürmək üçün n-mövqeli registr təsvir olunmuşdur. Bu registr $x\upsilon(x) \pmod{x^n - 1}$-i hesablayır. Bu xətti əks əlaqəli sürüşmə registrinə sadə nümunədir.

Xətti əks əlaqəli sürüşmə registrinin ümumi şəkli şəkil 7-də təsvir olunmuşdur. Bu dövrə aşağıdakı rekursiyanı hesablamaq üçün istifadə olunur.

$$p_j = -\sum_{i=1}^{L} h_i p_{j-i}, \quad j \geq L. \tag{2}$$

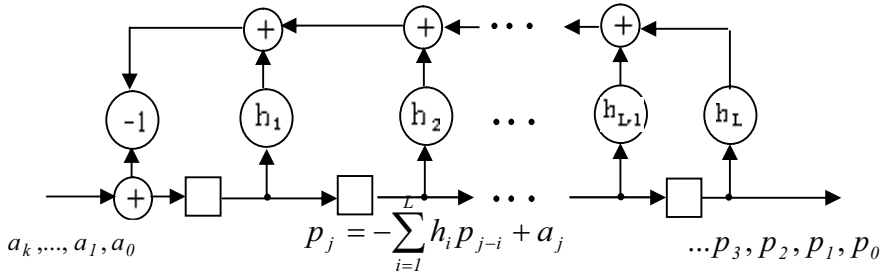


Şəkil 6. Çoxhədlilərin dövri sürüşdürməsi qurğusu.



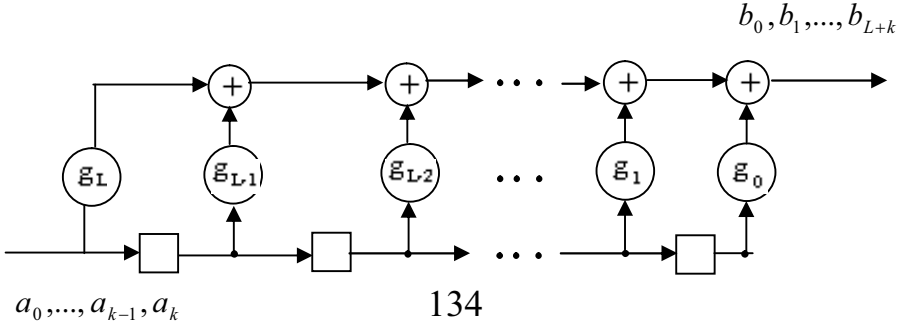
Şəkil 7. Xətti əks əlaqəli sürüşmə registri.

Əgər başlanğıc anda registr L sayda $(p_0, p_1, ..., p_{L-1})$ simvolları ilə yüklənibsə, onda registrin çıxışında p_0 ilə başlayan və (2) rekurrent münasibəti əsasında təyin olunan sonsuz simvollar ardıcıllığı əmələ gəlir. Əgər bu filtr şəkil 8-də təsvir olunan dövrə olarsa, onda o avtoreqresiya filtri adlanır. Belə ki, onda əks əlaqə mövcuddur və ona görə də o rekurrent filtrlər adlanan geniş bir sinfə aiddir.



Şəkil 8. Avtoreqresiya filtri.

Filtrin girişinə əks əlaqə xətti ilə onun çıxış simvolunu vermək əvəzinə giriş siqnalı olaraq kənardan əmələ gələn ardıcıllığı istifadə etmək olar. Əks əlaqəsiz belə xətti sürüşmə registri şəkil 9-da təsvir olunmuşdur. O həmçinin sonlu impuls reaksiyalı (SİR – filtr) və ya rekurrent olmayan filtr adlanır.



$$b_j = \sum_{i=0}^{L} g_i a_{j-i}$$

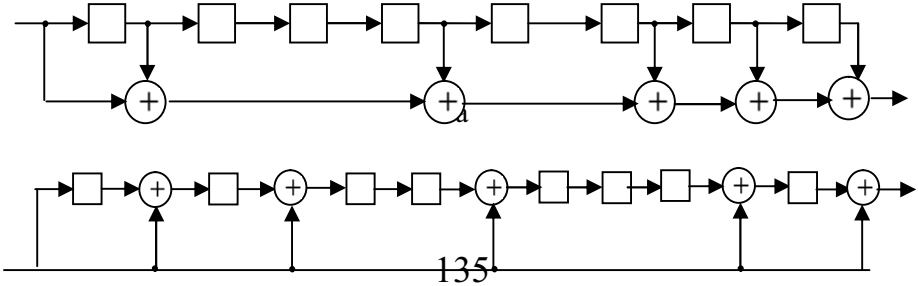
Şəkil 9. Əks əlaqəsiz sürüşmə registri.

Tutaq ki, $g(x) = g_L x^L + ... + g_1 x + g_0$ çoxhədlisinin əmsalları əks əlaqəsiz sürüşmə registrinin budaqlarında olan çəki vuruqlarına bərabərdir və tutaq ki, giriş və çıxış ardıcıllıqları uyğun olaraq $a(x) = a_k x^k + ... + a_1 x + a_0$ və $b(x) = b_{k+L} x^{k+L} + ... + b_1 x + b_0$ çoxhədliləri ilə yazılır. Onda bu çoxhədlilərin $b(x) = g(x)a(x)$ hasili şəkil 9-da təsvir olunan sürüşmə registrində baş verən prosesləri təsvir edir və nəzərdə tutulur ki, başlanğıc halda registrdə ancaq sıfırlar yerləşir və a_0 elementi L sayda sıfırdan sonra daxil edilir. Bu zaman deyirlər ki, $a(x)$ və $g(x)$ çoxhədlilərinin əmsalları sürüşmə registri vasitəsi bağlanır, belə ki,

$$b_j = \sum_{i=0}^{L} g_i a_{j-i} .$$

SİR-filtrlərinə ixtiyari $a(x)$ çoxhədlisinin qeyd olunmuş $g(x)$ çoxhədlisinə vurulması qurğusu kimi baxıla bilər. Bu filtrlərə $g(x)$ çoxhədlisinə vurma dövrəsi də deyilir.

Şəkil 10,a-da $g(x) = x^8 + x^7 + x^4 + x^2 + x + 1$ üçün $g(x)$ çoxhədlisinə vurma dövrəsi verilmişdir. Bu filtr SİR-filtridir. Qeyd edək ki, sürüşmə registrinin daxili mövqeləri oxunur, lakin dəyişdirilmir. Vurma qurğusunun elə variantını göstərmək olar ki, onun daxıli mövqeləri dəyişsin. Bu varianta nümunə olaraq şəkil 10,b-də $g(x) = x^8 + x^7 + x^4 + x^2 + x + 1$ çoxhədlisinə vurma dövrəsi verilmişdir. SİR-filtrinin belə şəkli o qədər də geniş istifadə olunmur.



b

Şəkil 10. $x^8 + x^7 + x^4 + x^2 + x + 1$ **çoxhədlisinə vurma dövrələri.**

Sürüşmə registrlərini ixtiyari çoxhədliləri qeyd olunmuş çoxhədlilərə bölmək üçün istifadə etmək olar. Belə dövrələr çoxhədlilərin adi bölmə prosedurasını istifadə edir. Fərz edək ki, bölən çevrilmiş çoxhədlidir. Bucaqlı bölmə aşağıdakı kimi yazılır:

$$
\begin{array}{l|l}
 & a_{n-1}x^{k-1} + (a_{n-2} - a_{n-1}g_{n-k-1})x^{k-2} + \ldots \\
\hline
x^{n-k} + g_{n-k-1}x^{n-k-1} + \ldots + g_0 & a_{n-1}x^{n-1} + \quad a_{n-2}x^{n-2} + \ldots + a_1x + a_0 \\
 & a_{n-1}x^{n-1} + \quad a_{n-1}g_{n-k-1}x^{n-2} + \ldots \\
\cline{2-2}
 & (a_{n-2} - a_{n-1}g_{n-k-1})x^{n-2} + \ldots \\
 & (a_{n-2} - a_{n-1}g_{n-k-1})x^{n-2} + \ldots \\
\cline{2-2}
 & \ldots
\end{array}
$$

Bu hesablamaları iki rekurrent bərabərliklər sistemi ilə yazmaq olar. Tutaq ki, $Q^{(r)}(x)$ və $R^{(r)}(x)$ rekursiyanın r-ci addımda uyğun olaraq qismət və qalıq çoxhədlisidir və bu kəmiyyətlərin başlanğıc qiymətləri $Q^{(0)}(x) = 0$ və $R^{(0)}(x) = a(x)$. Burada $a_{n-1}x^{n-1} + \ldots + a_1x + a_0$ və $x^{n-k} + g_{n-k-1}x^{n-k-1} + \ldots + g_0$ uyğun olaraq bölünən və bölən çoxhədlilərdir.

Rekurrent bərabərlikləri aşağıdakı kimi yazmaq olar:

$$Q^{(r)}(x) = Q^{(r-1)}(x) + R_{n-r}^{(r-1)}x^{k-r}, \tag{3}$$

$$R^{(r)}(x) = R^{(r-1)}(x) - R_{n-r}^{(r-1)}x^{k-r}g(x). \tag{4}$$

Aydındır ki, k addımdan sonra $Q^k(x)$ qismətini və $R^{(k)}(x)$ qalığını alarıq.

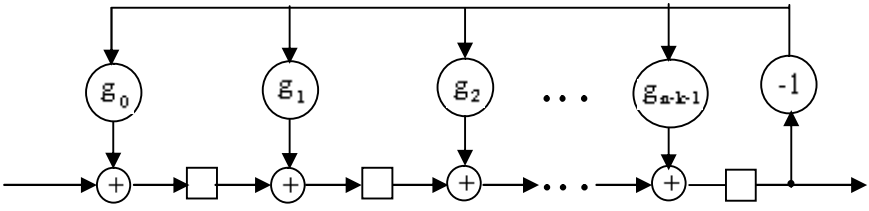
Şəkil 11-də istənilən çoxhədlini qeyd olunmuş $g(x)$ coxhədlisinə bölən dövrə təsvir olunur. Burada $g(x)$ çoxhədlisi qeyd olunmuş bölən, $b(x)$ çoxhədlisi isə bölünən çoxhədlidir və onlar aşağıdakı kimidir:

$$g(x) = -x^{n-k} + g_{n-k-1}x^{n-k-1} + ... + g_1 x + g_0 ,$$

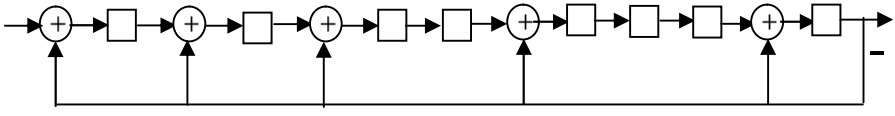
$$b(x) = b_{n-1}x^{n-1} + b_{n-2}x^{n-2} + ... + b_1 x + b_0 .$$

n sürüşmədən sonra registrin çıxışında qismət (natamam qismət), registrdə (yəni mövqelərdə) isə bölmədə alınan qalıq olar.

Şəkil 12-də $GF(2)$ üzərində verilən istənilən çoxhədlini $g(x) = x^8 + x^7 + x^4 + x^2 + x + 1$ çoxhədlisinə bölən dövrəyə nümunə verilir.



Şəkil 11. $g(x)$ çoxhədlisinə bölmə dövrəsi.



Şəkil 12.

Şəkil 12-də göstərilən dövrədə registrin daxili mövqeləri arasında cəmləyicilər qoyulmuşdur və bu da tez-tez dövrənin işini çətinləşdirir. Bu dövrə əvəzinə registrin daxili mövqelərinin məzmununu dəyişmədən oxumağa imkan verən bölmə dövrəsi istifadə etmək olar. Belə dövrələri qurmaq üçün çoxhədlilərin bölünməsini başqa cür təşkil edək, yəni yuxarıda şərh olunan «bucaqlı bölmədə» (3), (4) rekurrent bərabərliklərini aşağıdakı kimi yazaq:

$$R^{(r)}(x) = a(x) - Q^{(r)}(x)g(x) ,$$

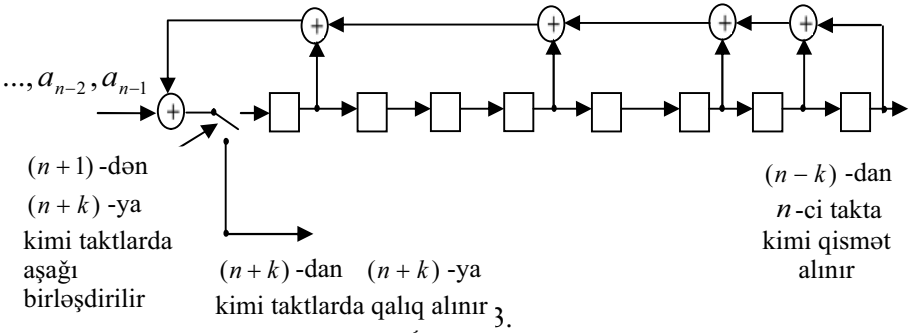
belə ki,

$$R_{n-r}^{(r-1)} = a_{n-r} - \sum_{i=1}^{n-1} g_{n-r-i} Q_i^{(r-1)}$$

və

$$Q^{(r)}(x) = g^{(r-1)}(x) + R_{n-r}^{(r-1)} x^{k-r}.$$

Bu bərabərlikləri şəkil 13-də göstərilən dövrə ilə realizə etmək olar ($g(x) = x^8 + x^7 + x^4 + x^2 + x + 1$ halında)



3.

FƏSİL V. BOUZ-ÇOUDXURİ-XOKVİNQEM KODLARI

Bouz-Çoudxuri-Xokvinqem kodları bir neçə səhvi düzəltməyə imkan verən kodlardır və dövri kodlar ailəsinə aiddirlər.

Əvvəlcə t sayda səhvi düzəltməyə imkan verən, $GF(q)$ üzərində təyin olunan və $q^m - 1$ uzunluğuna malik Bouz-Çoudxuri-Xokvinqem (BÇX) kodlarına baxaq.

§1. BÇX kodlarının təyini

Dövri kodların əmələgətirici çoxhədlilərini aşağıdakı kimi təsvir etmək olar:

$$g(x) = \text{ƏKOB}\,[f_1(x), f_2(x),..., f_r(x)]$$

Burada $f_1(x),..., f_r(x)$ çoxhədliləri $g(x)$ çoxhədlisinin köklərinin minimal çoxhədlilərıdirlər. Belə yanaşmadan istifadə etməklə öz kökləri vasitəsilə verilən əmələgətirici çoxhədlilər vasitəsilə müəyyən olunan kodlar qurulur.

Tutaq ki, $c(x)$ kod çoxhədlisi, $e(x)$ isə səhvlər çoxhədlisidir. Əmsalları $GF(q)$-dən olan qəbul edilən çoxhədli

$$\upsilon(x) = c(x) + e(x)$$

şəklində yazılır. Bu çoxhədlinin qiymətlərini $GF(q^m)$ elementlərində hesablamaq olar. Tutaq ki, $\gamma_1, \gamma_2,..., \gamma_r$ elementləri $g(x)$ çoxhədlisinin köklərıdir. $c(\gamma_j) = 0,\ j = 1,..., r$, olduğundan aşağıdakı doğrudur:

$$\upsilon(\gamma_j) = c(\gamma_j) + e(\gamma_j) = e(\gamma_j).$$

Beləliklə,

$$\upsilon(\gamma_j) = \sum_{i=0}^{n-1} e_i \gamma_j^i, \quad j = 1,...,r. \tag{1}$$

Nəticədə r sayda tənlikdən ibarət sistem alınır və bu sistemdə ancaq səhvdən asılı olan, lakin kod sözündən asılı olmayan kəmiyyətlər iştirak edir. (1) tənliklər sistemini $e_1, e_2,..., e_r$-lərə nəzərən həll etsək, onda səhv çoxhədlisini tapa bilərik. $\gamma_i,\ i = 1,..., r$, kökləri elə seçilməlidir ki, hər

dəfə t saydan çox olmayan sıfırdan fərqli məchullar halında (1) tənliklər sistemi e_i-lərə görə həll oluna bilsin.

$\gamma_1, \gamma_2, ..., \gamma_r$ köklərinə malik $g(x)$ əməlgətirici çoxhədlili ixtiyari dövri kod üçün sindromun komponentlərini təyin edək:

$$S_j = \upsilon(\gamma_j), \quad j = 1, ..., r .$$

Meydanın bu elementləri $s(x)$ sindrom çoxhədlisindən fərqlənir, lakin ekvivalent informasiyaya malikdirlər. Biz $\gamma_1, \gamma_2, ..., \gamma_r$-köklərini elə seçməliyik ki, $S_1, S_2, ..., S_r$-lərə əsasən t səhvi tapmaq mümkün olsun. Əgər α elementi $GF(q^m)$ meydanının primitiv elementi olarsa, onda köklər üçün belə çoxluq

$$\{\alpha, \alpha^2, \alpha^3, ..., \alpha^{2t}\}$$

çoxluğu ola bilər. Tutaq ki, bu çoxluğa daxil olan elementlər $g(x)$ çoxhədlisinin köküdür. Kodun uzunluğunu hər hansı bir m üçün $n = q^m - 1$ götürək və aşağıdakı kimi hərəkət edək:

1. m dərəcəli primitiv çoxhədli götürək və $GF(q^m)$ meydanını quraq;
2. Hər bir $\alpha^j, j = 1, ..., 2t$ üçün $f_j(x)$ minimal çoxhədlisini tapaq;
3. $g(x) = \text{ƏKOB}[f_1(x), ..., f_{2t}(x)]$ qəbul edək.

Belə qurulan dövrü kodlar t səhvi düzəldə bilər. Bəzi hallarda isə t-dən çox səhvləri də düzəldə bilər. Ona görə də $d = 2t + 1$ kimi təyin olunan kəmiyyət kodun konstruktiv məsafəsi adlanır. Kodun əsl minimal məsafəsi olan d^* kəmiyyəti konstruktiv məsafədən böyük ola bilər. Cədvəl 1-də $GF(16)$ meydanı $GF(2)$ meydanının genişlənməsi kimi verilir. Bu qurmada $p(z) = z^4 + z + 1$ primitiv çoxhədlisi istifadə olunur. Cədvəldə $GF(16)$-meydanının hər bir elementinin minimal çoxhədlisi də verilir. $\alpha = z$ elementi $GF(16)$ meydanının primitiv elementidir. Qeyd edək ki, α-nın istənilən cüt dərəcəsində minimal çoxhədli artıq cədvəlin əvvəlki sətrlərindən birində iştirak etmiş olur. Bu, o teoremin nəticəsidir ki, β və β^2 elementləri istənilən β üçün $GF(2)$ meydanı üzərində eyni bir

minimal çoxhədliyə malikdirlər. Bu fakt $g(x)$ çoxhədlisinin hesablanmasında istifadə oluna bilər.

Cədvəl 1.

$GF(2^4)$ meydanının təsviri

Dərəcə şəklində	Çoxhədli şəklində	İkilik şəkildə	Onluq şəkildə	Minimal çoxhədli
0	0	0000	0	
α^0	1	0001	1	x+1
α^1	z	0010	2	x^4+x+1
α^2	z^2	0100	4	x^4+x+1
α^3	z^3	1000	8	x^4+x^3+x^2+x+1
α^4	z+1	0011	3	x^4+x+1
α^5	z^2+ z	0110	6	x^2+x+1
α^6	z^3+ z^2	1100	12	x^4+x^3+x^2+x+1
α^7	z^3+ z+1	1011	11	x^4+x^3+1
α^8	z^2+1	0101	5	x^4+x+1
α^9	z^3+ z	1010	10	x^4+x^3+x^2+x+1
α^{10}	z^2+ z+1	0111	7	x^2+x+1
α^{11}	z^3+ z^2+ z	1110	14	x^4+x^3+1
α^{12}	z^3+ z^2+ z+1	1111	15	x^4+x^3+x^2+x+1
α^{13}	z^3+ z^2+1	1101	13	x^4+x^3+1
α^{14}	z^3+ 1	1001	9	x^4+x^3+1

İki səhvi düzəltmək üçün 15 uzunluğuna malik BÇX kodunun əmələgətirici çoxhədlisi aşağıdakı kimi qurulur:

$$g(x) = \text{ƏKOB}\,[f_1(x), f_2(x), f_3(x), f_4(x)] =$$

$$= \text{ƏKOB}\,[x^4 + x + 1,\ x^4 + x + 1,\ x^4 + x^3 + x^2 + x + 1,\ x^4 + x + 1] =$$

$$= (x^4 + x + 1)(x^4 + x^3 + x^2 + x + 1) = x^8 + x^7 + x^6 + x^4 + 1.$$

$g(x)$ -in dərəcəsi 8-ə bərabərdir, deməli, $n - k = 8$. Buradan da $k = 7$ - dir. Beləliklə, (15,7) - BÇX kodu alınır və bu 2 səhvi düzəltməyə imkan

verir. Qeyd edək ki, BÇX-kodu verilmiş n və t halında qurulur. $g(x)$ çoxhədlisi tapılmayanadək k -nın qiyməti naməlum qalır.

Eyni qayda ilə 15 uzunluğuna malik başqa primitiv BÇX kodu qurula bilər.

Tutaq ki, $t = 3$. Onda

$$g(x) = \text{ƏKOB}\,[f_1(x), f_2(x), f_3(x), f_4(x), f_5(x), f_6(x)] =$$
$$= (x^4 + x + 1)(x^4 + x^3 + x^2 + x + 1)(x^2 + x + 1) =$$
$$= x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1.$$

Beləliklə, 3 səhvi düzəltməyə imkan verən (15,5) – BÇX kodunun əmələgətirici çoxhədlisi quruldu.

Tutaq ki, $t = 4$:

$$g(x) =$$
$$= \text{ƏKOB}\,[f_1(x), f_2(x), f_3(x), f_4(x), f_5(x), f_6(x), f_7(x), f_8(x)] =$$
$$= (x^4 + x + 1)(x^4 + x^3 + x^2 + x + 1)(x^2 + x + 1)(x^4 + x^3 + 1) =$$
$$= x^{14} + x^{13} + x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 +$$
$$+ x^3 + x^2 + x + 1.$$

Deməli, dörd səhvi düzəltməyə imkan verən (15,1)-BÇX kodunun əmələgətirici çoxhədlisini aldıq.

$t = 5,6,7$ hallarının hər birində alınan əmələgətirici çoxhədli $t = 4$ halında olduğu kimidir. $t > 7$ olduğu halda BÇX kodu mövcud deyildir. Belə ki, $GF(16)$ meydanının sıfırdan fərqli elementlərinin sayı cəmi 15-dir.

Cədvəl 2-də $GF(16)$ meydanı $GF(4)$ meydanının ($GF(4)$ meydanda vurma və torlama cədvəli fəsil II-də şəkil 1-də verilir) genişlənməsi kimi təsvir edilir. Bu zaman $p(z) = z^2 + z + 2$ primitiv çoxhədlisi istifadə olunur. Bu cədvəldə həmçinin $GF(16)$ meydanının bütün elementləri üçün $GF(4)$ üzərində minimal çoxhədlilər verilir. $GF(16)$ meydanında $\alpha = z$ primitiv elementdir.

$GF(4)$ üzərində 15 uzunluğuna malik olan və bir səhvi düzəltmək üçün nəzərdə tutulan BÇX kodunun əmələgətirici çoxhədlisi aşağıdakı kimi qurulur:

$$g(x) = \text{ƏKOB}[f_1(x), f_2(x)] = (x^2 + x + 2)(x^2 + x + 3) = x^4 + x + 1.$$

Cədvəl 2.

$GF(4^2)$ meydanının təsviri

Qüvvət şəklində	Çoxhədli şəklində	Dördlük şəklində	Onluq şəklində	Minimal çoxhədlilər
0	0	00	0	
α^0	1	01	1	x+1
α^1	z	10	4	x^2+x+2
α^2	z+2	12	6	x^2+x+3
α^3	3z+2	32	14	x^2+3x+1
α^4	z+1	11	5	x^2+x+2
α^5	2	02	2	x+2
α^6	2z	20	8	x^2+2x+1
α^7	2z+3	23	11	x^2+2x+2
α^8	z+3	13	7	x^2+x+3
α^9	2z+2	22	10	x^2+2x+1
α^{10}	3	03	3	x+3
α^{11}	3z	30	12	x^2+3x+3
α^{12}	3z+1	31	13	x^2+3x+1
α^{13}	2z+1	21	9	x^2+2x+2
α^{14}	3z+3	33	15	x^2+3x+3

Beləliklə, $GF(4)$ üzərində 1 səhvi düzəldən (15,11)-BÇX kodu üçün əmələgətirici çoxhədli quruldu. Bu kodla 11 dördlük simvollardan ibarət ardıcıllıq (22 bitə ekvivalentdir) 15 dördlük simvollar ardıcıllığına kodlaşır. Belə koda Xemminq kodu deyildir.

Belə qayda ilə $GF(4)$ üzərində 15 uzunluğuna malik başqa BÇX kodlarını da tapmaq olar.

Tutaq ki, $t = 2$:

$$g(x) = \text{ƏKOB}[f_1(x), f_2(x), f_3(x), f_4(x)] = (x^2 + x + 2)(x^2 + x + 3) \times$$

$$\times (x^2 + 3x + 1) = x^6 + 3x^5 + x^4 + x^3 + 2x^2 + 2x + 1.$$

Bu (15,9)-BÇX kodunun əmələgətirici çoxhədlisidir. Belə kodla 2 səhv düzəldilir.

Tutaq ki, $t = 3$:

$$g(x) = x^9 + 3x^8 + 3x^7 + 2x^6 + x^5 + 2x^4 + x + 2.$$

Bu əmələgətirici çoxhədli üç səhvi düzəltməyə imkan verən $GF(4)$ üzərində (15,6)-BÇX kodunu yaradır.

Tutaq ki, $t = 4$. Onda

$$g(x) = x^{11} + x^{10} + 2x^8 + 3x^7 + 3x^6 + x^5 + 3x^4 + x^3 + x + 3.$$

Bu çoxhədli dörd səhvi düzəldən $GF(4)$ üzərində (15,4)-BÇX kodunu yaradır.

$t = 5$ olduqda

$$g(x) = x^{12} + 2x^{11} + 3x^{10} + 2x^9 + 2x^8 + x^7 + 3x^6 + 3x^4 + 3x^3 + x^2 + 2$$

alınır və bu da $GF(4)$ üzərində (15,3)-BÇX kodunu yaradır. Bu kod beş səhvi düzəldir.

$t = 6$ olduqda

$$g(x) = x^{14} + x^{13} + x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 +$$

$$+ x^4 + x^3 + x^2 + x + 1.$$

Bu $GF(4)$ meydanı üzərində (15,1)-BÇX kodunun əmələgətirici çoxhədlisidir və o yeddi səhvi düzəldir. Həqiqətdə bu, təkrarlamaqla olan koddur.

BÇX kodlarının formal təyinini verək. Bu tərif yuxarıda verilən təyindən daha ümumidir. $g(x)$ çoxhədlisinin kökləri kimi meydanın ixtiyari β elementinin $2t$ sayda qüvvətləri ardıcıllığı götürülür (β primitiv element olmaya da bilər). Kodun uzunluğu β elementinin tərtibinə, yəni $\beta^n = 1$ şərtini ödəyən ən kiçik n ədədinə bərabər olar.

Tərif 1. Tutaq ki, q və m verilib və β elementi $GF(q^m)$ meydanının istənilən n tərtibli elementidir. Onda istənilən müsbət t tam

ədədi və istənilən j_0 tam ədədi üçün uyğyn BÇX kodu əmələgətirici çoxhədlisi

$$g(x) = \text{ƏKOB}\,[f_{j_0}(x), f_{j_0+1}(x), ..., f_{j_0+2t-1}(x)]$$

olan n uzunluqlu dövri koddur. Burada $f_j(x)$ çoxhədlisi β^j elementinin minimal çoxhədlisidir və $GF(q)$ meydanı üzərindədir.

Tez-tez $j_0 = 1$ seçilir. Bu da ən kiçik dərəcəli $g(x)$ çoxhədlisini əmələ gətirir. Adətən böyük uzunluqlu kodlar tələb olunur. Onda β elementi kimi meydanın ən böyük tərtibə malik elementi, yəni primitiv elementi götürülür.

Nümunə 1.

$GF(3)$ üzərində $t = 2$ səhvi düzəldən (26,17) - BÇX kodunun əmələgətirici çoxhədlisini qurmalı.

Aydındır ki, $n = 26$. $n = q^m - 1 = 3^3 - 1 = 26$ olduğundan $q = 3$, $m = 3$ alırıq. Deməli, bu (26,17) – BÇX kodu $GF(3^3)$ meydanı üzərində koddur.

Təyinə görə axtarılan əmələgətirici çoxhədli aşağıdakı kimi qurulur:

$$g(x) = \text{ƏKOB}[f_1(x), f_2(x), f_3(x), f_4(x)].$$

Fəsil IV-də §3-də nümunə 5-də $f_1(x), f_2(x), f_3(x), f_4(x)$ üçün aşağıdakı ifadələr alınmışdır:

$$f_1(x) = x^3 + 2x + 1, \quad f_2(x) = x^3 + x^2 + x + 2,$$
$$f_3(x) = x^3 + 2x + 1, \quad f_4(x) = x^3 + x^2 + 2.$$

Beləliklə,

$$g(x) = (x^3 + 2x + 1)(x^3 + x^2 + x + 2)(x^3 + x^2 + 2) =$$
$$= x^9 + 2x^8 + x^7 + x^6 + x^5 + 2x^4 + 2x^3 + 2x^2 + x + 1.$$

§2. Piterson-Qorensteyn-Çirler üsulu

BÇX kodu dövri koddur və, beləliklə, bu kodlara dövri kodları dekodlaşdırmaq üçün olan bütün üsullar tətbiq oluna bilər. Lakin, xüsusi olaraq BÇX kodları üçün yaradılmış yaxşı alqoritmlər mövcuddur. Bu alqoritmlərdən birinə baxaq. Bu alqoritm ilk dəfə Piterson tərəfindən ikilik

kodlar üçün təklif edilmişdir. Sonralar həmin alqoritm Qorensteyn və Çirler tərəfindən ümumiləşdirilmişdir.

Alqoritmin şərhində sadəlik üçün $j_0 = 1$ hesab edəcəyik. Lakin alınan nəticələr hamısı heç bir dəyişiklik olmadan istənilən j_0 üçün də alına bilər. Hesab edəcəyik ki, t sayda səhvi düzəldən üsuldan söhbət gedir.

Fərz edək ki, BÇX kodunun konstruksiyasının əsasında meydanın α elementi durur və mümkündür ki, α primitiv element deyildir. Tutaq ki, səhv çoxhədlisi aşağıdakıdır:

$$e(x) = e_{n-1}x^{n-1} + e_{n-2}x^{n-2} + ... + e_1 x + e_0$$

və t-dən böyük olmayan sayda əmsalları sıfırdan fərqlidir. Fərz edək ki, əslində ν sayda, $0 \le \nu \le t$ səhv baş vermişdir və bu səhvlərə naməlum $i_1, i_2, ..., i_\nu$ mövqeləri uyğundur. Bu halda səhvlər çoxhədlisini aşağıdakı kimi yazmaq olar:

$$e(x) = e_{i_1}x^{i_1} + e_{i_2}x^{i_2} + ... + e_{i_\nu}x^{i_\nu}.$$

Burada e_{i_ℓ} əmsalı ℓ-ci səhvin qiymətidir (ikilik halda $e_{i_\ell} = 1$). Bu münasibətlərdə nə $i_1, i_2, ..., i_\nu$ indekslərinin (və ya qüvvət dərəcələrinin) nə də ki, $e_{i_1}, e_{i_2}, ..., e_{i_\nu}$ əmsallarının qiymətlərini bilmirik. Əslində ν kəmiyyətinin də qiyməti bilinmir. Səhvləri düzəltmək üçün bu kəmiyyətlərin hamısını hesablamaq lazımdır. S_1 sindrom komponentini əldə etmək üçün qəbul edilmiş $\upsilon(x)$ çoxhədlisinin α nöqtəsində qiymətini tapmaq lazımdır:

$$S_1 = \upsilon(\alpha) = c(\alpha) + e(\alpha) = e(\alpha) = e_{i_1}\alpha^{i_1} + e_{i_2}\alpha^{i_2} + ... + e_{i_\nu}\alpha^{i_\nu}.$$

Sadəlik üçün $Y_\ell = e_{i_\ell}$ (səhvin qiyməti), $X_\ell = \alpha^{i_\ell}$ (səhvin lokatoru) işarələmələrini qəbul edək. α elementinin tərtibi n olduğundan baxılan səhvlər konfiqurasiyasının lokatoru müxtəlifdir. Bu qəbul edilən işarələmələrə əsasən:

$$S_1 = Y_1X_1 + Y_2X_2 + ... + Y_\nu X_\nu.$$

Analoji olaraq qəbul edilən çoxhədlinin qiymətini α-nın bütün qüvvətlərində ($g(x)$- a daxil olan qyvvətlərində) hesablamaq olar. $j = 1, ..., 2t$ üçün sindromları təyin edək:

$$S_j = \upsilon(\alpha^j) = c(\alpha^j) + e(\alpha^j) = e(\alpha^j).$$

Onda naməlum $X_1, X_2, ..., X_\nu$ lokatorları və naməlum $Y_1, Y_2, ..., Y_\nu$ səhvlərin qiymətləri üçün $2t$ sayda tənlikdən ibarət sistem alarıq:

$$\begin{cases} S_1 = Y_1 X_1 + Y_2 X_2 + ... + Y_\nu X_\nu, \\ S_2 = Y_1 X_1^2 + Y_2 X_2^2 + ... + Y_\nu X_\nu^2, \\ \vdots \\ S_{2t} = Y_1 X_1^{2t} + Y_2 X_2^{2t} + ... + Y_\nu X_\nu^{2t}. \end{cases} \quad (1)$$

Sindromun təyininə görə (1) tənliklər sistemi heç olmazsa bir həllə malik olmalıdır. Biz görəcəyik ki, bu həll yeganədir. Bizim məsələ verilmiş sindroma görə naməlum kəmiyyətləri tapmaqdan ibarətdir. Tənliklər sistemi qeyri-xəttidir.

Bu tənliklər sistemini bilavasitə həll etmək çətindir. Sindrom komponentlərinə görə hesablana bilən və onlara görə sonradan səhvlərin lokatorunun hesablana bilməsi mümkün olan bəzi aralıq dəyişənlər təyin etməklə süni bir üsuldan istifadə edək.

Tutaq ki,

$$\Lambda(x) = \Lambda_\nu x^\nu + \Lambda_{\nu-1} x^{\nu-1} + ... + \Lambda_1 x + 1. \quad (2)$$

Bu çoxhədli səhvlərin lokatoru çoxhədlisi adlanır və kökləri X_ℓ^{-1}, $\ell = 1, ..., \nu$ - kəmiyyətləridir. Beləliklə,

$$\Lambda(x) = (1 - x \cdot X_1)(1 - x \cdot X_2)...(1 - x \cdot X_\nu).$$

Əgər $\Lambda(x)$ -ın əmsalları məlum olarsa, onda səhvlərin lokatorlarını tapmaq üçün onun köklərini tapmaq lazım gələr. Ona görə də sindromun verilən komponentlərinə görə $\Lambda_1, ..., \Lambda_\nu$ əmsallarının hesablanmasına cəhd edək. Əgər bu bizə müyəssər olarsa, onda məsələ həll edilməyə yaxın olar. (2) çoxhədlisinin hər tərəfini $Y_\ell \cdot X_\ell^{j+\nu}$ kəmiyyətinə vuraq və $x = X_\ell^{-1}$ götürək. Onda sol tərəf sıfıra çevrilər və beləliklə, aşağıdakını alarıq:

$$0 = Y_\ell \cdot X_\ell^{j+\nu}(1 + \Lambda_1 X_\ell^{-1} + \Lambda_2 X_\ell^{-2} + ... + \Lambda_{\nu-1} X^{-(\nu-1)} + \Lambda_\nu X_\ell^{-\nu})$$

və ya

$$Y_\ell (X_\ell^{j+\nu} + \Lambda_1 X_\ell^{j+\nu-1} + ... + \Lambda_\nu X_\ell^j) = 0. \quad (3)$$

(3) münasibəti hər bir ℓ və j üçün yerinə yetirilir. (3) münasibətini ℓ-ə görə 1-dən ν -yə qədər cəmləsək, alarıq:

$$\sum_{\ell=1}^{\nu} Y_\ell (X_\ell^{j+\nu} + \Lambda_1 X_\ell^{j+\nu-1} + ... + \Lambda_\nu X_\ell^{j}) = 0$$

və ya

$$\sum_{\ell=1}^{\nu} Y_\ell X_\ell^{j+\nu} + \Lambda_1 \sum_{\ell=1}^{\nu} Y_\ell X_\ell^{j+\nu-1} + ... + \Lambda_\nu \sum_{\ell=1}^{\nu} Y_\ell X_\ell^{j} = 0 . \qquad (4)$$

(4) münasibətində hər bir cəm sindrom komponentidir. Ona görə də tənlik aşağıdakı şəklə düşür:

$$S_{j+\nu} + \Lambda_1 S_{j+\nu-1} + \Lambda_2 S_{j+\nu-2} + ... + \Lambda_\nu S_j = 0 .$$

$\nu \le t$-dir, onda $1 \le j \le \nu$ olduqda j üçün bütün indekslər məlum sindrom komponentlərini təşkil edir. Beləliklə, tənliklər sistemi alarıq:

$$\Lambda_1 S_{j+\nu-1} + \Lambda_2 S_{j+\nu-2} + ... + \Lambda_\nu S_j = -S_{j+\nu}, \quad j = 1,2,...,\nu .$$

Bu matris şəklində aşağıdakı kimidir:

$$\begin{pmatrix} S_1 & S_2 & S_3 & \dots & S_{\nu-1} & S_\nu \\ S_2 & S_3 & S_4 & \dots & S_\nu & S_{\nu+1} \\ \vdots & \vdots & \vdots & & \vdots & \\ S_\nu & S_{\nu+1} & S_{\nu+2} & \dots & S_{2\nu-2} & S_{2\nu-1} \end{pmatrix} \cdot \begin{pmatrix} \Lambda_\nu \\ \Lambda_{\nu-1} \\ \vdots \\ \Lambda_1 \end{pmatrix} = \begin{pmatrix} -S_{\nu+1} \\ -S_{\nu+2} \\ \vdots \\ -S_{2\nu} \end{pmatrix} .$$

Əgər sistemin matrisi cırlaşan deyildirsə, onda bu tənliklər sistemini matrisin tərsini tətbiq etməklə həll etmək olar. İsbat edək ki, əgər ν sayda səhv baş veribsə, onda matris cırlaşan deyildir. Əvvəlcə Vandermond matrisi haqqında bir faktı qeyd edək:

Teorem 1. Tutaq ki,

$$A = \begin{pmatrix} 1 & 1 & \dots & 1 \\ X_1 & X_2 & & X_\mu \\ X_1^2 & X_2^2 & \dots & X_\mu^2 \\ \vdots & \vdots & & \vdots \\ X_1^{\mu-1} & X_2^{\mu-1} & & X_\mu^{\mu-1} \end{pmatrix} .$$

A matrisi ancaq və ancaq $X_i \ne X_j$, $i \ne j$, $i, j = \overline{1, \mu}$ olduqda sıfırdan fərqli determinanta malikdir.

Teorem 2. Tutaq ki, M sindrom komponentlərindən düzəldilmiş matrisdir:

$$M = \begin{pmatrix} S_1 & S_2 & \dots & S_\mu \\ S_2 & S_3 & \dots & S_{\mu+1} \\ \vdots & & & \\ S_\mu & S_{\mu+1} & \dots & S_{2\mu-1} \end{pmatrix}.$$

Əgər μ kəmiyyəti baş vermiş səhvlərin sayı olan ν kəmiyyətinə bərabərsə, onda M matrisi cırlaşan matris deyildir. Əgər $\mu > \nu$ isə M matrisi cırlaşandır.

İsbatı. Tutaq ki, $\mu > \nu$ şərtlərini ödəyən μ üçün $X_\mu = 0$; A matrisi $A_{ij} = X_j^{i-1}$ elementli matrisdir, yəni

$$A = \begin{pmatrix} 1 & 1 & \dots & 1 \\ X_1 & X_2 & \dots & X_\mu \\ \vdots & & \vdots & \\ X_1^{\mu-1} & X_2^{\mu-1} & \dots & X_\mu^{\mu-1} \end{pmatrix};$$

B matrisi diaqonal matrisdir və elementləri $B_{ij} = Y_i X_i \delta_{ij}$ kəmiyyətləridir ($\delta_{ij} = 1, i = j; \delta_{ij} = 0, i \neq j$). Onda ABA^T matrisinin elementləri aşağıdakı kimi olacaq:

$$(ABA^T)_{ij} = \sum_{\ell=1}^{\mu} X_\ell^{i-1} \sum_{k=1}^{\mu} Y_\ell X_\ell \delta_{\ell k} X_k^{j-1} = \sum_{\ell=1}^{\mu} X_\ell^{i-1} Y_\ell X_\ell X_\ell^{j-1} = \\ = \sum_{\ell=1}^{\mu} Y_\ell X_\ell^{i+j-1},$$

yəni M matrisinin elementləri ilə üst-üstə düşür. Beləliklə,

$$\det(M) = \det(A) \cdot \det(B) \cdot \det(A).$$

Əgər $\mu > \nu$, onda $\det(B) = 0$. Buradan alınır ki, $\det(M) = 0$ və, beləliklə, M cırlaşandır. Əgər $\mu = \nu$ olarsa, onda $\det(B) \neq 0$. A matrisi Vandermond matrisi olduğundan onun determinantı sıfırdan fərqli o zaman olur ki, matrisin sütunları fərqli olsunlar. Bu da $\mu = \nu$ halında olur. Deməli, $\mu = \nu$ olduqda $\det(M) \neq 0$ olur. □

Bu teorem dekodlaşdırma alqoritminin qurulmasının əsasıdır. Hər şeydən əvvəl aşağıdakı kimi yanaşmaqla ν üçün düzgün qiyməti tapaq. Başlanğıc olaraq $\nu = t$ götürək və M matrisinin determinantını hesablayaq. Əgər o, sıfıra bərabər deyilsə, onda ν üçün düzgün qiymət almışıq. Əks halda ν -dən «1» çıxaq və proseduranı təkrar edək. Prosesi determinant sıfırdan fərqli alınana kimi davam etdiririk. Onda biz ν kəmiyyətinin qiymətini, yəni neçə səhv baş verdiyini tapmış oluruq. Sonra M matrisinin tərs matrisini hesablayıb bunun əsasında $\Lambda(x)$ çoxhədlisinin əmsallarını tapırıq. $\Lambda(x)$ -ın köklərini tapıb, beləliklə, lokatorları müəyyən edirik. Əgər kod ikilik kod isə, onda səhvlər məlumdur. Əks halda sindromun komponentlərini təyin edən (1) tənliklər sisteminə qayıdırıq. Səhvlərin lokatorları məlumdur və ona görə də biz səhvlərin ν sayda naməlum qiymətlərindən ibarət olan $2t$ sayda xətti tənliklərə malik oluruq. Bu tənliklərin ilk ν saydasının əmsalları matrisinin determinantı sıfırdan fərqli olarsa, onda bu ilk ν sayda tənliklər səhvlərin qiymətlərinə nəzərən həll edilə bilər. Lakin

$$\det\begin{pmatrix} X_1 & X_2 & \dots & X_\nu \\ X_1^2 & X_2^2 & \dots & X_\nu^2 \\ \vdots & & & \\ X_1^\nu & X_2^\nu & \dots & X_\nu^\nu \end{pmatrix} = (X_1 X_2 \dots X_\nu) \det\begin{pmatrix} 1 & 1 & \dots & 1 \\ X_1 & X_2 & \dots & X_\nu \\ \vdots & & & \\ X_1^{\nu-1} & X_2^{\nu-1} & \dots & X_\nu^{\nu-1} \end{pmatrix}.$$

Teorem 1-ə görə əgər ν sayda səhv baş veribsə, axırıncı matrisin determinantı sıfırdan fərqlidir belə ki, $X_1, X_2, \dots, X_\nu$ bir-birindən fərqlidir və sıfra bərabər deyildirlər. Dekodlaşdırma alqoritmi şəkil 1-də verilir.

Baxmayaraq ki, mühakimə xüsusi halda - $j_0 = 1$ halında aparılır, biz fərz edirik ki, j_0 ixtiyaridir.

Meydanın elementləri sonlu olduğundan, adətən, $\Lambda(x)$ -ın köklərinin tapılmasının ən sadə yolu «nümunə və səhv» üsuludur. Bu üsul Çen prosedurası adı ilə məşhurdur. Bu prosedura hər bir j üçün $\Lambda(\alpha^j)$ -in ardıcıl hesablanmasından və alınan qiymətlərin sıfıra bərabər olmasının yoxlanmasından ibarətdir. $\Lambda(x)$ -ın β -nöqtəsində hesablanmasının ən sadə üsulu Hörner sxemidir:

$$\Lambda(\beta) = (\dots(((\Lambda_\nu \beta + \Lambda_{\nu-1})\beta + \Lambda_{\nu-2})\beta + \Lambda_{\nu-3})\beta + \dots + \Lambda_0).$$

Bu sxem vasitəsilə $\Lambda(\beta)$-nın hesablanması üçün ν sayda vurma və ν sayda toplama lazımdır.

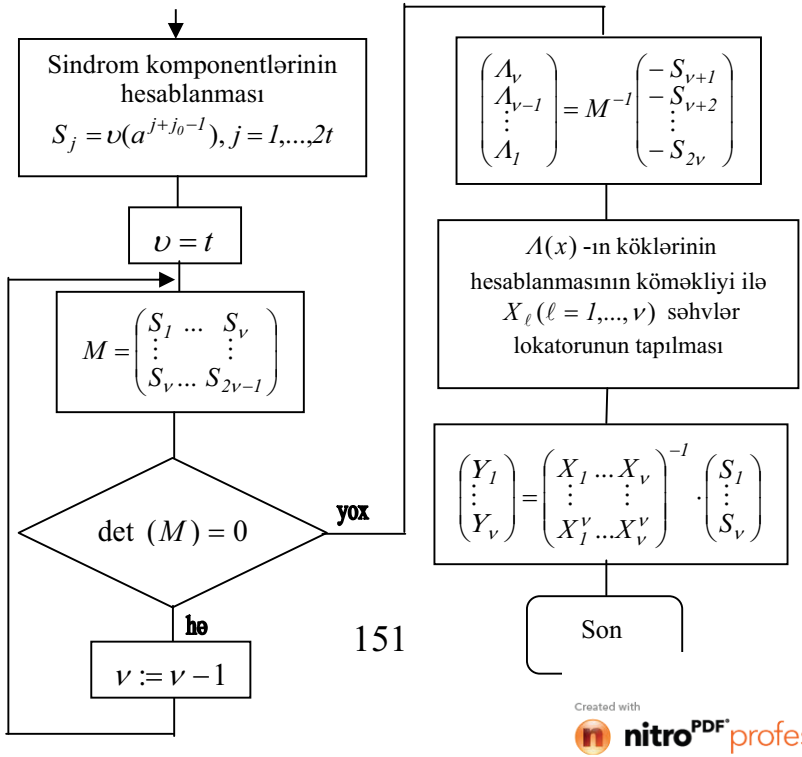
Nümunə 1. (15,5)-BÇX kodunun dekodlaşdırılmasına baxaq. Bu kod üç səhvi düzəltməyə imkan verir və əmələgətirici çoxhədlisi aşağıdakı kimidir:

$$g(x) = x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1.$$

Nümunə kimi hesab edək ki, $\upsilon(x) = x^7 + x^2$ çoxhədlisi qəbul olunub. Aydındır ki, əgər üçdən çox olmayan sayda səhv baş verərsə, onda kod sözü sıfır olmalıydı və $\upsilon(x) = e(x)$, lakin dekoder bu nəticəyə gələ bilməz. Dekodlaşdırma alqoritminin bütün addımlarını həyata keçirək. Əvvəlcə $GF(16)$ meydanı hesabından istsfadə etməklə sindrom komponentlərini hesablayaq:

$$S_1 = \alpha^7 + \alpha^2 = \alpha^{12}, \quad S_2 = \alpha^{14} + \alpha^4 = \alpha^9,$$
$$S_3 = \alpha^{21} + \alpha^6 = 0, \quad S_4 = \alpha^{28} + \alpha^8 = \alpha^3,$$
$$S_5 = \alpha^{35} + \alpha^{10} = \alpha^0, \quad S_6 = \alpha^{42} + \alpha^{12} = 0.$$

Tutaq ki, $\upsilon(x)$-ın daxil



Şəkil 1.

$$M=\begin{pmatrix} S_1 & S_2 & S_3 \\ S_2 & S_3 & S_4 \\ S_3 & S_4 & S_5 \end{pmatrix}=\begin{pmatrix} \alpha^{12} & \alpha^{9} & 0 \\ \alpha^{9} & 0 & \alpha^{3} \\ 0 & \alpha^{3} & 1 \end{pmatrix}.$$

$\det(M)=0$. Beləliklə, $\nu=2$ qəbul edirik. Onda

$$M=\begin{pmatrix} S_1 & S_2 \\ S_2 & S_3 \end{pmatrix}=\begin{pmatrix} \alpha^{12} & \alpha^{9} \\ \alpha^{9} & 0 \end{pmatrix}.$$

M matrisinin determinantı sıfırdan fərqlidir. Deməli, $\nu=2$ sayda səhv baş verib. M^{-1} matrisini hesablayaq:

$$M^{-1}=\begin{pmatrix} 0 & \alpha^{6} \\ \alpha^{6} & \alpha^{9} \end{pmatrix}.$$

Onda

$$\begin{pmatrix} \Lambda_2 \\ \Lambda_1 \end{pmatrix}=\begin{pmatrix} 0 & \alpha^{6} \\ \alpha^{6} & \alpha^{9} \end{pmatrix}\cdot\begin{pmatrix} 0 \\ \alpha^{3} \end{pmatrix}=\begin{pmatrix} \alpha^{9} \\ \alpha^{12} \end{pmatrix}.$$

Beləliklə, $\Lambda(x)=\alpha^9x^2+\alpha^{12}x+1$. Çen prosedurasını istifadə etməklə aşağıdakı parçalanmanı alarıq:

$\Lambda(x)=(\alpha^7x+1)(\alpha^2x+1)=a^9(x-\alpha^8)(x-\alpha^{13})$. $\Lambda(x)$ çoxhədlisi α^8 və α^{13} köklərinə malikdir. Səhvin lokatorları köklərin tərsinə bərabərdir.

Beləliklə, ikinci və yeddinci mövqelərdə səhv baş verib. Kod ikilik olduğundan səhv «1» -ə bərabərdir və $e(x)=x^7+x^2$.

Nümunə 2. $GF(3^3)$ meydanı üzərində dekodlaşdırma məsələsinə baxaq. Tutaq ki, əməlgətirici çoxhədli

$$g(x)=x^9+2x^8+x^7+x^6+x^5+2x^4+2x^3+2x^2+x+1$$

çoxhədlisidir. Aydındır ki, bu çoxhədli $(n,k)=(26,17)$ - BÇX kodunu əmələ gətirir. Kodun Xemminq çəkisi $w=10$ -a bərabərdir. Belə kodlar

$t = 2$ sayda səhvi düzəldə bilir (§1-ə bax!). Tutaq ki, bu koda daxil olan hər hansı bir kod sözü ötürülmüşdür və

$$\upsilon(x) = x^9 + x^7 + x^6 + 2x^4 + 2x^3 + 2x^2 + x + 1$$

sözü qəbul edilmişdir. Qəbul edilən kod sözünün düz qəbul olunub olunmadığını yoxlamalı. Əgər ötürmə zamanı səhv baş veribsə, onda səhvi düzəltməli.

S_1, S_2, S_3 və S_4 lokatorlarını hesablayaq:

$$S_1 = \upsilon(\alpha) = \alpha^9 + \alpha^7 + \alpha^6 + 2\alpha^4 + 2\alpha^3 + 2\alpha^2 + \alpha + 1 = \alpha^{14},$$

$$S_2 = \upsilon(\alpha^2) = \alpha^{18} + \alpha^{14} + \alpha^{12} + 2\alpha^8 + 2\alpha^6 + 2\alpha^4 + \alpha^2 + 1 = \alpha^{20},$$

$$S_3 = \upsilon(\alpha^3) = \alpha + \alpha^{21} + \alpha^{18} + 2\alpha^{12} + 2\alpha^9 + 2\alpha^6 + \alpha^3 + 1 = \alpha^{16},$$

$$S_4 = \upsilon(\alpha^4) = \alpha^{10} + \alpha^2 + \alpha^{24} + 2\alpha^{16} + 2\alpha^{12} + 2\alpha^8 + \alpha^4 + 1 = \alpha^{15}.$$

Tutaq ki, $\nu = 2$.

$$\begin{vmatrix} S_1 & S_2 \\ S_2 & S_3 \end{vmatrix} = \begin{vmatrix} \alpha^{14} & \alpha^{20} \\ \alpha^{20} & \alpha^{16} \end{vmatrix} = \alpha^4 - \alpha^{14} = \alpha^2 \neq 0.$$

Deməli, məlumatların ötürülməsi zamanı 2 səhv baş vermişdir. $\Lambda(x) = \Lambda_2 x^2 + \Lambda_1 x + 1$ səhvlərin lokatoru çoxhədlisinin Λ_1 və Λ_2 əmsallarını təyin etmək üçün

$$\begin{pmatrix} S_1 & S_2 \\ S_2 & S_3 \end{pmatrix} \cdot \begin{pmatrix} \Lambda_2 \\ \Lambda_1 \end{pmatrix} = \begin{pmatrix} -S_3 \\ -S_4 \end{pmatrix}$$

və ya

$$\begin{pmatrix} \alpha^{14} & \alpha^{20} \\ \alpha^{20} & \alpha^{16} \end{pmatrix} \cdot \begin{pmatrix} \Lambda_2 \\ \Lambda_1 \end{pmatrix} = \begin{pmatrix} -\alpha^{16} \\ -\alpha^{15} \end{pmatrix}$$

tənliklər sistemini həll edək. Bunun üçün Kramer qaydasından istifadə edək. Uyğun determinantları hesablayaq.

$$\Delta = \begin{vmatrix} S_1 & S_2 \\ S_2 & S_3 \end{vmatrix} = \alpha^2,$$

$$\Delta_1 = \begin{vmatrix} -\alpha^{16} & \alpha^{20} \\ -\alpha^{15} & \alpha^{16} \end{vmatrix} = -\alpha^6 + \alpha^9 = \alpha^{15},$$

$$\Delta_2 = \begin{vmatrix} \alpha^{14} & -\alpha^{16} \\ \alpha^{20} & -\alpha^{15} \end{vmatrix} = -\alpha^3 + \alpha^{10} = \alpha^{22}.$$

Buradan da $\Lambda_1 = \alpha^{21} / \alpha^2 = \alpha^{19}$, $\Lambda_2 = \alpha^{15} / \alpha^2 = \alpha^{13}$. Deməli, $\Lambda(x) = \alpha^{13} x^2 + \alpha^{19} x + 1$. Bu çoxhədlinin köklərini tapaq. Ondan ötrü x kəmiyyətinin yerinə $GF(3^3)$ meydanının elementlərini yazaq və $\Lambda(x)$ çoxhədlisinin qiymətlərini hesablayaq:

$\Lambda(\alpha) = \alpha^{13} \cdot \alpha^2 + \alpha^{19} \cdot \alpha + 1 = \alpha^{15} + \alpha^{20} + 1 = \alpha^{11} \neq 0$,

$\Lambda(\alpha^2) = \alpha^{17} + \alpha^{21} + 1 = \alpha^3 \neq 0$,

$\Lambda(\alpha^3) = \alpha^{19} + \alpha^{22} + 1 = \alpha^{20} \neq 0$,

$\Lambda(\alpha^4) = \alpha^{21} + \alpha^{23} + 1 = \alpha^{22} \neq 0$,

$\Lambda(\alpha^5) = \alpha^{11} \neq 0$, $\Lambda(\alpha^6) = \alpha^{12} \neq 0$, $\Lambda(\alpha^7) \neq 0$,

$\Lambda(\alpha^8) \neq 0$, $\Lambda(\alpha^9) \neq 0$, $\Lambda(\alpha^{10}) \neq 0$,

$\Lambda(\alpha^{11}) \neq 0$, $\Lambda(\alpha^{12}) \neq 0$, $\Lambda(\alpha^{13}) \neq 0$,

$\Lambda(\alpha^{14}) \neq 0$, $\Lambda(\alpha^{15}) \neq 0$, $\Lambda(\alpha^{16}) \neq 0$,

$\Lambda(\alpha^{17}) \neq 0$, $\Lambda(\alpha^{18}) = 0$, $\Lambda(\alpha^{19}) \neq 0$,

$\Lambda(\alpha^{20}) \neq 0$, $\Lambda(\alpha^{21}) = 0$.

Beləliklə, $\Lambda(x)$ çoxhədlisinin kökləri $X_1^{-1} = \alpha^{18}, X_2^{-1} = \alpha^{21}$. Buradan da $X_1 = \alpha^8$, $X_2 = \alpha^5$. Deməli, səhvlərin baş verdiyi mövqelər 8-ci və 5-ci mövqelərdir. Səhvlərin qiymətini tapaq. Bundan ötrü

$$\begin{cases} Y_1 X_1 + Y_2 X_2 = S_1 \\ Y_1 X_1^2 + Y_2 X_2^2 = S_2 \end{cases}$$

və ya

$$\begin{cases} \alpha^8 Y_1 + \alpha^5 Y_2 = \alpha^{14} \\ \alpha^{16} Y_1 + \alpha^{10} Y_2 = \alpha^{20} \end{cases}$$

tənliklər sistemini həll edək.

$$\Delta = \begin{vmatrix} \alpha^8 & \alpha^5 \\ \alpha^{16} & \alpha^{10} \end{vmatrix} = \alpha^{18} - \alpha^{21} = \alpha^{14},$$

$$\Delta_1 = \begin{vmatrix} \alpha^{14} & \alpha^5 \\ \alpha^{20} & \alpha^{10} \end{vmatrix} = \alpha^{24} - \alpha^{25} = \alpha^{14}, \quad Y_1 = \Delta_1 / \Delta = 1;$$

$$\Delta_2 = \begin{vmatrix} \alpha^8 & \alpha^{14} \\ \alpha^{16} & \alpha^{20} \end{vmatrix} = \alpha^2 - \alpha^4 = \alpha, \quad Y_2 = \Delta_2 / \Delta = \alpha / \alpha^{14} = \alpha^{-13} = \alpha^{13} = 2 .$$

Beləliklə, səhv çoxhədlisi $e(x) = x^8 + 2x^5$ kimidir. Ötürülən kod çoxhədlisini hesablayaq:

$$c(x) = \upsilon(x) - e(x) = x^9 + x^7 + x^6 + 2x^4 + 2x^3 + 2x^2 + x + 1 +$$

$$+ 2x^8 + x^5 = x^9 + 2x^8 + x^7 + x^6 + x^5 + 2x^4 + 2x^3 + 2x^2 + x + 1.$$

Beləliklə, ötürülən kod sözü aşağıdakı kimidir:

$$c(x) = x^9 + 2x^8 + x^7 + x^6 + x^5 + 2x^4 + 2x^3 + 2x^2 + x + 1$$

və ya vektor şəklində $c = (\underbrace{1122211121}_{10\ \text{simvol}}\ \underbrace{000...00}_{16\,\text{sıfır}})$.

Aydındır ki, informasiya simvollarının sayı 17-dir. Bu informasiya çoxhədlisini tapmaq üçün $c(\text{x})$ çoxhədlisini $g(x)$ çoxhədlisinə bölmək lazımdır:

$$i(x) = c(x) / g(x) = 1 .$$

Buradan da informasiya sözünü vektor şəklində aşağıdakı kimi tapırıq: $i = (1\underbrace{00...0}_{16\,\text{sıfır}})$.

G əmələgətirici matrisi aşağıdakı kimidir:

$$G = \begin{pmatrix} 1\,1\ \ 2\ 2\ 2\ 1\ 1\ 1\ 2\ 1\ 0\ 0\ 0\ 0 ... 0\ 0\ 0 \\ 0\ 1\ \ 1\ 2\ 2\ 2\ 1\ 1\ 1\ 2\ 1\ 0\ 0\ 0 ...\ 0\ 0\ 0 \\ 0\ 0\ 1\ \ 1\ 2\ 2\ 2\ 1\ 1\ 1\ 2\ 1\ 0\ 0 ...\ 0\ 0\ 0 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 000\ 00\ 0\ 0 ...\ 1\ 2\ 1 \end{pmatrix} .$$

§3. Rid-Solomon kodu

BÇX kodlarının geniş istifadə olunan və əhəmiyyətli altçoxluğu Rid-Solomon kodlarıdır. Bu kodlarda kod sözünün simvolları əlifbasının multiplikativ tərtibi kodun uzunluğuna bölünür. Beləliklə, $m = 1$ və

$GF(q)$ simvollar meydanı ilə səhvlər lokatoru meydanı $GF(q^m)$ üst-üstə düşür. α -nı primitiv element götürəcəyik, onda

$$n = q^m - 1 = q - 1.$$

$\beta \in GF(q)$ elementinin $GF(q)$ üzərində minimal çoxhədlisi aşağıdakına bərabərdir:

$$f_\beta(x) = x - \beta.$$

Belə ki, simvollar meydanı və səhvlər lokatorlarının meydanı üst-üstə düşür, bütün minimal çoxhədlilər xəttidir. t sayda səhvi düzəldən Rid-Solomon kodlarında adətən $j_0 = 1$ olduğu nəzərə alınır və ona görə əmələgətirici çoxhədli aşağıdakı şəkildə yazılır:

$$g(x) = (x - a)(x - a^2)...(x - a^{2t}).$$

Bu $g(x)$ çoxhədlisinin dərəcəsi həmişə $2t$ -yə bərabərdir və buradan da $n - k = 2t$ alınır.

Rid-Solomon kodlarında j_0 üçün başqa qiymət də götürmək olar. j_0 -ın qiymətini ağlabatan seçməklə bəzən koderi sadələşdirmək olur. Beləliklə,

$$g(x) = (x - \alpha^{j_0})(x - \alpha^{j_0+1})...(x - \alpha^{j_0+2t-1}).$$

Nümunə kimi $GF(16)$ üzərində $t = 2$ olan (15,11) - Rid-Solomon kodları üçün $g(x)$ çoxhədlisini tapaq. j_0 üçün istənilən qiymət götürülə bilər. $j_0 = 1$ götürək. Onda

$$g(x) = (x - \alpha)(x - \alpha^2)(x - \alpha^3)(x - \alpha^4) = x^4 + (z^3 + z^2 + 1)x^3 +$$
$$+ (z^3 + z^2)x^2 + z^3 x + (z^2 + z + 1) = x^4 + \alpha^{13}x^3 + \alpha^6 x^2 + \alpha^3 x + \alpha^{10}.$$

(burada $GF(16)$ meydanının elementlərinin z dəyişəninin cədvəl 1-də verilən çoxhədliləri kimi təsvirindən istifadə edilir) $g(x)$ çoxhədlisinin dərəcəsi 4-ə bərabərdir və ona görə də $n - k = 4$ və, beləliklə, $k = 11$ alınır. İnformasiya çoxhədlisi $GF(16)$ -dan olan 11 simvollar ardıcıllığından ibarətdir və bu da 44 bitə ekvivalentdir.

İkinci nümunə kimi $GF(8)$ üzərində $t=2$ olan (7,3) - Rid-Solomon kodunun $g(x)$ çoxhədlisini tapaq. j_0 üçün istənilən qiymət götürülə bilər. $j_0=4$ götürək. Onda

$$g(x)=(x-\alpha^4)(x-\alpha^5)(x-\alpha^6)(x-\alpha^0)=$$
$$=x^4+(z^2+1)x^3+(z^2+1)x^2+(z+1)x+z=$$
$$=x^4+\alpha^6x^3+\alpha^6x^2+\alpha^3x+\alpha.$$

(burada $GF(8)$ meydanının elementlərinin z dəyişəninin çoxhədlisi kimi təsvirindən istifadə olunmuşdur) İnformasiya çoxhədlisi üç səkkizlik simvoldan (bu da 9 bitə ekvivalentdir) ibarət ardıcıllıqdan ibarətdir. Fərz edək ki,

$$i(x)=(z^2+z)x^2+x+(z+1).$$

Sistematik olmayan kod sözü aşağıdakı kimi yazılır:

$$c(x)=i(x)\cdot g(x)=(\alpha^4x^2+x+\alpha^3)(x^4+\alpha^6x^3+\alpha^6x^2+\alpha^3x+\alpha)=$$
$$=\alpha^4x^6+\alpha x^5+\alpha^6x^4+0\cdot x^3+0\cdot x^2+\alpha^5x+\alpha^4.$$

Bu da yeddi 8-lik simvol təşkil edir.

Rid-Solomon kodu Sinqlton məsafəsinə görə optimal koddur.

Teorem 1. Rid-Solomon kodu $n-k+1$ minimal məsafəsinə malikdir və maksimal məsafəli koddur.

İsbatı. Tutaq ki, $d=2t+1$ kodun konstruktiv məsafəsidir. d^* minimal məsafəsi aşağıdakı bərabərliyi ödəyir:

$$d^*\geq d=2t+1=n-k+1,$$

belə ki, Rid-Solomon kodu üçün $2t=n-k$-dır. Lakin istənilən xətti kod üçün Sinqlton sərhədi qüvvədədir: $d^*\leq n-k+1$. Deməli, $d^*=n-k+1$ və $d^*=d$. □

İsbat olunan teorem sübut edir ki, qeyd olunmuş n və k üçün minimal məsafəsi Rid-Solomon kodlarının minimal məsafəsindən çox olan kod mövcud deyildir. Lakin bu sübutu sözün həqiqi mənasında başa düşmək lazım deyildir. Tez-tez (n',k') parametrli elə kodlara üstünlük verilir ki, bu parametrli Rid-Solomon kodu mövcud deyildir. Eyni vaxtda Rid-Solomon kodları eyni bir əlifba üzərində həmişə ən qısa kodlar olur.

§4. Berlekemp-Messi alqoritmi

Piterson-Qorensteyn-Çirler alqoritmində hesablamanın əsas həcmi aşağıdakı matris tənliyinin həlli ilə bağlıdır:

$$\begin{pmatrix} S_1 & S_2 \dots S_\nu \\ S_2 & S_3 \dots S_{\nu+1} \\ & \dots \\ S_\nu & S_{\nu+1} \dots S_{2\nu-1} \end{pmatrix} \cdot \begin{pmatrix} \Lambda_\nu \\ \Lambda_{\nu-1} \\ \vdots \\ \Lambda_1 \end{pmatrix} = \begin{pmatrix} -S_{\nu+1} \\ -S_{\nu+2} \\ \vdots \\ -S_{2\nu} \end{pmatrix}. \qquad (1)$$

ν kəmiyyətinin o qədər də böyük olmayan qiymətində (1) tənliklər sistemi tərs matrisin tətbiqi ilə həll oluna bilər. $\nu \times \nu$ ölçülü tərs matrisi hesablamaq üçün ν^3 tərtibində hesablama aparılması lazım gəlir. ν -nün böyük qiymətlərində daha effektiv hesablama alqoritmi tələb olunur. Belə alqoritmlərdən biri Berlekemp üsuludur. Bu üsulun əsasında (1)-in sol tərəfində birinci matrisin ixtiyari matris deyil xüsusi struktura malik matris olması faktı durur. Belə struktur Λ vektorunun axtarılması ilə bağlı hesablamaları əhəmiyyətli dərəcədə azalda bilər. Lakin bu hesablama matrisin tərsinin hesablanmasından daha çətin qavranıla bilər.

Alqoritmin Messi tərəfindən təklif edilən variantına baxaq. Fərz edək ki, $\Lambda = (\Lambda_\nu, \dots, \Lambda_1)^T$ vektoru məlumdur. (1)-dən görünür ki, istənilən $j = \nu + 1, \dots, 2\nu$ üçün

$$S_j = -\sum_{i=1}^{\nu} \Lambda_i S_{j-i} \,. \qquad (2)$$

S_j-lərin $(j = \nu + 1, \dots, 2\nu)$ hesablanması üçün müxtəlif texniki qurğular, məsələn avtoreqresiya filtri, sonlu avtomat və ya ardıcıllıqlı maşın istifadə oluna bilər. Aydındır ki, bu qurğular gecikmə elementləri vasitəsilə qurulur. Bu zaman əmsallar kimi Λ vektorunun komponentləri istifadə olunur (məsələn, şəkil 1). Bundan sonra sxem dedikdə sürüşdürmə registri (lazım olduqada xətti əks əlaqəli) nəzərdə tutacağıq.

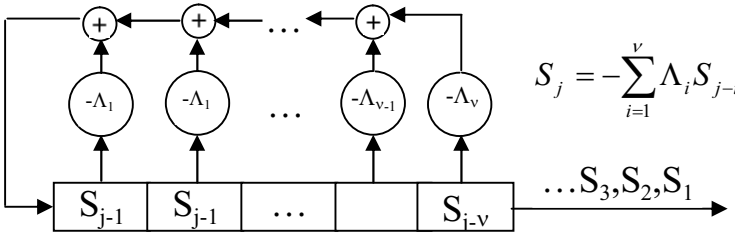
Beləliklə, məsələ sindrom komponentlərini əmələgətirən xüsusi sxemlərin qurulmasına gətirilir. Lakin belə sxemlər çoxsaylı ola bilər. Məsələ belə sxemlərdən ən qısa uzunluğa malik olanının müəyyən olunmasından ibarətdir. Bu da qəbuledilən sözdə minimal çəkili səhvlər

vektorunu təyin etməyə və ya da ən kiçik dərəcəli Λ çoxhədlisini təyin etməyə imkan verir. Minimal dərəcəli çoxhədlinin dərəcəsi ν -yə bərabərdir və yeganə qaydada təyin olunur, belə ki, ilkin sistemin $\nu \times \nu$ ölçülü matrisi tərsə malik olan matrisdir. Avtoreqresiya filtrinin qurulma prosedurası həm də (1) matris tənliyinin Λ vektoruna nəzərən həll edilməsi üsuludur. Aşağıda deyilən sxemlərin qurulması veriləcək. Təsvir olunan üsul istənilən meydan üzərində hesablamalara tətbiq olunandır və $S_1, S_2, ..., S_{2t}$ ardıcıllıqlarının hər hansı bir xüsusi xassəyə malik olmasını nəzərdə tutmur. $\Lambda(x)$ çoxhədlisinin təsvir etdiyi sxemin uzunluğu (registrlərin uzunluğu) $\Lambda(x)$ -in dərəcəsindən uzun ola bilər.

Tələb olunan sürüşmə registrini qurmaq üçün iki kəmiyyəti: sürüşmə registrinin L uzunluğunu və $\Lambda(x)$ çoxhədlisini tapmaq lazımdır:

$$\Lambda(x) = \Lambda_\nu x^\nu + \Lambda_{\nu-1} x^{\nu-1} + ... + \Lambda_1 x + 1,$$

harada ki, $\deg \Lambda(x) \le L$. Bu cütlüyü $(L, \Lambda(x))$ ilə işarə edək. Uyğun başlanğıc vəziyyəti halında $S_1, ..., S_{2t}$ ardıcıllığını yaradan ən kiçik uzunluqlu sxemin tapılması tələb olunur.



Başlanğıc vəziyyətdə $S_\nu, S_{\nu-1}, ..., S_1$ ardıcıllığından ibarət olur.

Şəkil 1. Səhvlərin lokatoru çoxhədlisi sürüşmə registrləri dövrəsində.

Axtarılan sxemin (əks əlaqəli sürüşmə registri, sonlu avtomat və ya ardıcıllıqlı maşın) qurulması induktiv olaraq həyata keçirilir. $r = 1$-dən başlamaqla hər bir r üçün ilk r sindrom komponentlərini, yəni $S_1, ..., S_r$ komponentlərini doğuran sxemi quraq. $(L_r, \Lambda^{(r)}(x))$ sxemi $S_1, ..., S_r$ komponentlərini doğuran (əmələ gətirən) minimal uzunluqlu sxemdir. O yeganə olmaya da bilər: bir neçə belə sxem ola bilər, lakin onların hamısı

eyni uzunluğa malikdirlər. r-ci iterasiyanın başlanğıcında artıq sxemlər siyahısı təyin edilmiş olur:

$$(L_1, \Lambda^{(1)}(x)),\ (L_2, \Lambda^{(2)}(x)), ..., (L_{r-1}, \Lambda^{(r-1)}(x)).$$

Berlekemp-Messi alqoritminin əsas ideyası $S_1, ..., S_{r-1}, S_r$ ardıcıllığını doğuran minimal uzunluqlu yeni $(L_r, \Lambda^{(r)}(x))$ sxeminin qurulma üsulunu tapmaqdan ibarətdir. Bu əvvəlki addımda (iterasiyada) qurulan sxemdən istifadə etməklə həyata keçirilir, harada ki, lazım gəldikdə uzunluğu və çəki vuruqları (əmsallaını) uyğun şəkildə dəyişdirilir.

r-ci iterasiyada $(r-1)$-ci sxemin çıxışını hesablayaq:

$$\hat{S}_r = -\sum_{j=1}^{n-1} \Lambda_j^{(r-1)} S_{r-j}.$$

$n-1$ ədədi $\Lambda^{(r-1)}(x)$-in dərəcəsindən böyük olduğundan, cəmdə toplananların çoxu çıfra bərabərdir, və, beləliklə, cəmi 1-dən $\deg \Lambda^{(r-1)}(x)$-a kimi yazmaq lazımdır. Yazılışın sadəliyi xatirinə cəm əvvəlki kimi yazılacaq.

Tələb olunan S_r çıxışından $\hat{S}_r$ kəmiyyətini çıxmaqla r-uyğunsuzluq adlanan Δ_r kəmiyyətini alarıq:

$$\Delta_r = S_r - \hat{S}_r = S_r + \sum_{j=1}^{n-1} \Lambda_j^{(r-1)} S_{r-j}$$

və ya

$$\Delta_r = \sum_{j=0}^{n-1} \Lambda_j^{(r-1)} S_{r-j}.$$

Əgər $\Delta_r = 0$ olarsa, onda $(L_r, \Lambda^{(r)}(x)) = (L_{r-1}, \Lambda^{(r-1)}(x))$ qəbul edirik və r-ci iterasiya sona yetir. Əks halda sxemdə çəki vuruqlarını aşağıdakı kimi dəyişirik:

$$\Lambda^{(r)}(x) = \Lambda^{(r-1)}(x) + Ax^{\ell} \Lambda^{(m-1)}(x),$$

harada ki, A meydan elementidir, ℓ tam ədəddir, $\Lambda^{(m-1)}(x)$ isə əvvəlki iterasiyaların birində rast gələn sxem çoxhədlisidir. Yeni çoxhədlidən istifadə etməklə uyğunsuzluğu yenidən hesablayaq (onu Δ'_r ilə işarə edək):

$$\Delta'_r = \sum_{j=0}^{n-1} \Lambda_j^{(r)} S_{r-j} = \sum_{j=0}^{n-1} \Lambda_j^{(r-1)} S_{r-j} + A \sum_{j=0}^{n-1} \Lambda_j^{(m-1)} S_{r-j-\ell}.$$

İndi m, ℓ və A kəmiyyətlərinin təyin edilməsinə baxaq:

m -i r-dən elə kiçik götürək ki, $\Delta_m \neq 0$ olsun. $\ell = r - m$ və $A = -\Delta_m^{-1}\Delta_r$ kimi təyin edək. Onda

$$\Delta_r' = \Delta_r - \frac{\Delta_r}{\Delta_m} = \Delta_m = 0$$

və, beləliklə, yeni sxem $S_1,\ldots, S_{r-1}, S_r$-ləri əmələ gətirəcək. Lakin bizə lazım olan heç də hər belə sxem deyil, minimal uzunluqlu sxemdir. m -in seçilməsində $\Delta_m \neq 0$ şərtini ödəyən elə m seçmək lazımdır ki, $L_m > L_{m-1}$ ödənsin. Bu halda qurulan sxem minimal uzunluqlu sxem olur.

Proseduranın dəqiq təsviri aşağıdakı teoremlə verilir.

Teorem 1 (Berlekemp-Messi alqoritmi). Tutaq ki, hər hansı bir meydandan $S_1,\ldots, S_{2t}$-lər verilmişdir və tutaq ki, $\Lambda^{(0)}(x) = 1$, $B^{(0)}(x) = 1$ və $L_0 = 1$ başlanğıc şərti halında $\Lambda^{(2t)}(x)$-in hesablanması üçün aşağıdakı rekurrent bərabərliklər doğrudur:

$$\Delta_r = \sum_{j=0}^{n-1} \Lambda_j^{(r-1)} S_{r-j}, \tag{3}$$

$$L_r = \delta_r (r - L_{r-1}) + (1 - \delta_r) L_{r-1}, \tag{4}$$

$$\begin{pmatrix} \Lambda^{(r)}(x) \\ B^{(r)}(x) \end{pmatrix} = \begin{pmatrix} 1 & -\Delta_r x \\ \Delta_r^{-1}\delta_r & (1-\delta_r)x \end{pmatrix} \cdot \begin{pmatrix} \Lambda^{(r-1)}(x) \\ B^{(r-1)}(x) \end{pmatrix}, \tag{5}$$

$r = 1,\ldots, 2t$, harada ki,

$$\delta_r = \begin{cases} 1, & \text{əgər } \Delta_r \neq 0 \text{ və } 2L_{r-1} \leq r-1, \\ 0, & \text{əks halda.} \end{cases} \tag{6}$$

Onda $\Lambda^{(2t)}(x)$ çoxhədlisi əmsalları aşağıdakı bərabərlikləri ödəyən ən kiçik dərəcəli çoxhədlidir:

$$\Lambda_0^{(2t)} = 1, \quad S_r + \sum_{j=1}^{n-1} \Lambda_j^{(2t)} S_{r-j} = 0, \quad r = L_{2t} + 1,\ldots, 2t.$$

Bu teoremdə Δ_r sıfıra bərabər ola bilər, lakin bu o halda ola bilər ki, $\delta_r = 0$ olsun. Onda təyinə görə $\Delta_r^{-1}\delta_r = 0$ qəbul edək.

Hər bir iterasiyada matrislərin vurulması üçün $2t$ -dən çox olmayan sayda vurma əməliyyatı, Δ_r -in hesablanması üçün isə t -dən çox olmayan sayda vurma əməliyyatı lazım gəlir. Cəmi $2t$ sayda iterasiya olduğundan $6t^2$ -dan çox olmayan sayda vurma əməliyyatı lazım gəlir. Beləliklə, bu alqoritm t^3 sayda əməliyyatın lazım gəldiyi matrisin tərsinin tətbiqinə əsaslanan alqoritmdən adətən effektivdir.

Teorem 1-in isbatı iki lemmaya gətirilir. Birinci lemmada L_r və L_{r-1} -ləri əlaqələndirən bərabərsizlik tapılır. Bu lemma aşağıdakı kimidir.

Lemma 1. Tutaq ki, $(L_{r-1}, \Lambda^{(r-1)}(x))$ sxemi $S_1,..., S_{r-1}$ ardıcıllığını yaradan minimal uzunluqlu sxemdir, $(L_r, \Lambda^{(r)}(x))$ isə $S_1,..., S_{r-1}, S_r$ ardıcıllığını yaradan minimal uzunluqlu sxemdir. Onda

$$L_r \geq \max\{L_{r-1}, r - L_{r-1}\}.$$

İsbatı. İsbat olunacaq bərabərsizlik iki bərabərsizliyə bölünür:

$$L_r \geq L_{r-1}, \quad L_r \geq r - L_{r-1}.$$

Birinci bərabərsizlik aydındır, belə ki, əgər sxem hər hansı bir ardıcıllığı əmələ gətirirsə, onda o bu ardıcıllığın əvvəli olan istənilən kiçik ardıcıllığı da əmələ gətirir. Əgər $L_{r-1} \geq r$, onda ikinci bərabərsizlik də aydındır. Ona görə də fərz edək ki, $L_{r-1} < r$. Əksini fərz edək. Fərz edək ki, ikinci bərabərlik yerinə yetirilmir. Ziddiyyət alınmasını göstərək. Fərziyyədən çıxır ki, $L_r \leq r - 1 - L_{r-1}$. Yazılışı sadələşdirmək üçün aşağıdakı işarələməni daxil edək: $c(x) = \Lambda^{(r-1)}(x)$, $b(x) = \Lambda^{(r)}(x)$, $L = L_{r-1}$ və $L' = L_r$. Yeni işarələmələrdə ilkin fərziyyə aşağıdakı şəklə düşür: $r \geq L + L' + 1$ və $L < r$. Bundan başqa lemmanın şərtindən alınır:

$$S_r \neq -\sum_{i=1}^{L} c_i S_{r-i},$$

$$S_j = -\sum_{i=1}^{L} c_i S_{j-i}, \; j = L+1,...,r-1,$$

və

$$S_j = -\sum_{k=1}^{L'} b_k S_{j-k}, \; j = L'+1,...,r.$$

İndi isə ziddiyyəti müəyyənləşdirək. Bir tərəfdən

$$S_r = -\sum_{k=1}^{L'} b_k S_{r-k} = \sum_{k=1}^{L'} b_k \sum_{i=1}^{L} c_i S_{r-k-i} \,, \qquad (7)$$

harada ki, S_{r-k}-ın ayrılışının doğruluğu ondan alınır ki, $r-k$ ədədi $L+1,...,r-1$ ədədləri arasında yerləşən $r-1$-dən $r-L'$-ə qədər olan tam ədədlər arasında qiymətlər alır, belə ki, $r \geq L+L'+1$. Digər tərəfdən

$$S_r \neq -\sum_{i=1}^{L} c_i S_{r-i} = \sum_{i=1}^{L} c_i \sum_{k=1}^{L'} b_k S_{r-i-k} \,, \qquad (8)$$

harada ki, S_{r-i}-nin ayrılışının doğruluğu ondan alınır ki, r tam ədədlər olan $L'+1,...,r-1$ ədədləri arasında yerləşən $r-1$-dən $r-L$-ə kimi olan tam ədədləri arasında qiymətlər alır, bu isə $r \geq L+L'+1$ fərziyyəsindən alınır. (8) bərabərliyinin sağ tərəfində cəmləmə qaydasının dəyişməsi, (7) bərabərliyində sağ tərəfdə alınan S_r üçün olan ifadəyə gətirib çıxardır. Beləliklə, $S_r \neq S_r$ ziddiyyətini alırıq. Deməli, $L_r \geq r - L_{r-1}$. □

Lemma 2. Fərz edək ki, $(L_i, \Lambda^{(i)}(x))$, $i = 1,...,r$, sxemləri minimal uzunluqlu sxemlər yığımıdır və elədirlər ki, $\Lambda^{(i)}(x)$ çoxhədlisi $S_1,...,S_i$ komponentlərini əmələ gətirir. Əgər $\Lambda^{(r)}(x) \neq \Lambda^{(r-1)}(x)$, onda

$$L_r = \max[\, L_{r-1}, r - L_{r-1}] \qquad (9)$$

və $S_1,..., S_r$ komponentlərini əmələ gətirən və (9) bərabərliyinin sağ tərəfinə bərabər olan uzunluğa malik olan istənilən sxem minimal uzunluqlu sxemdir. Belə sxem teorem 1-lə təyin olunur.

İsbatı. Lemma 1-ə görə L_r kəmiyyəti (9) bərabərliyinin sağ tərəfindən kiçik ola bilməz. Əgər tələb olunan komponentləri əmələ gətirən və uzunluğu göstərilən kəmiyyətə bərabər olan hər hansı bir sxemi qurmaq mümkün olarsa, onda o minimal uzunluqlu sxemdir. İsbatı riyazi induksiya vasitəsilə aparaq. Hər bir $k \leq r-1$ üçün ardıcıl qurulması fərz olunan və teoremi təmin edən sxemlər quraq. Hər bir k $(k = 1,...,r-1)$ üçün $(L_k, \Lambda^{(k)}(x))$ vasitəsilə $S_1,...,S_k$ komponentlərini əmələ gətirən minimal uzunluqlu sxemi işarə edək.

Hər dəfə $\Lambda^{(k)}(x) \neq \Lambda^{(k-1)}(x)$ olduqda induksiya fərziyyəsi olaraq qəbul edək:

$$L_k = \max[L_{k-1},\ k - L_{k-1}],\ k = 1,...,n-1.$$

Bu $k = 0$ olduqda doğrudur, belə ki, $L_0 = 0$ və $L_1 = 1$. Sonuncu iterasiyada uzunluğun dəyişməsinə gəti rən k qiymətini m ilə işarə edək. Sonuncu o deməkdir ki, $(r-1)$-ci iterasiya sona çatdıqda m o tam ədəddir ki, $L_{r-1} = L_m > L_{m-1}$ olur. Beləliklə, aşağıdakı bərabərlik qüvvədə olar:

$$S_j + \sum_{i=1}^{L_{r-1}} \Lambda_i^{(r-1)} S_{j-i} = \sum_{i=0}^{L_{r-1}} \Lambda_i^{(r-1)} S_{j-i} = \begin{cases} 0, & j = L_{r-1},...,r-1, \\ \Delta_r, & j = r. \end{cases}$$

Əgər $\Delta_r = 0$, onda $(L_{r-1}, \Lambda^{(r-1)}(x))$ sxemi də həmçinin komponentlərin ilk r simvolunu əmələ gətirir və, beləliklə,

$$L_r = L_{r-1}, \qquad \Lambda^{(r)}(x) = \Lambda^{(r-1)}(x).$$

Əgər $\Lambda_r \neq 0$, onda yeni sxem qurmaq lazımdır. Sxemin uzunluğunun dəyişməsinin $k = m$ olduqda baş verməsini nəzərə alsaq, beləliklə, alarıq

$$S_j + \sum_{i=1}^{L_{m-1}} \Lambda_i^{(m-1)} S_{j-i} = \begin{cases} 0, & j = L_{m-1},...,m-1, \\ \Delta_m \neq 0, & j = m, \end{cases}$$

və induksiya fərziyyəsinə görə

$$L_{r-1} = L_m = \max[L_{m-1}, m - L_{m-1}] = m - L_{m-1},$$

belə ki, $L_m > L_{m-1}$. İndi isə yeni çoxhədlini seçək:

$$\Lambda^{(r)}(x) = \Lambda^{(r-1)}(x) - \Lambda_r \Delta_m^{-1} x^{r-m} \Lambda^{(m-1)}(x).$$

$L_r = \deg \Lambda^{(r)}(x)$ qəbul edək. Bu halda

$$\deg \Lambda^{(r-1)}(x) \le L_{r-1}, \quad \deg[x^{r-m} \Lambda^{(m-1)}(x)] \le r - m + L_{m-1}$$

olduğundan

$$L_r \le \max[L_{r-1}, r - m + L_{m-1}] \le \max[L_{r-1}, r - L_{r-1}].$$

Bu bərabərsizlikdən və $\Lambda^{(r)}(x)$-in $S_1,..., S_r$ ardıcıllığını əmələ gətirməsi şərti halında lemma 1-dən alınır ki, $L_r = \max[L_{r-1}, r - L_{r-1}]$. İndi isə $(L_r, \Lambda^{(r)}(x))$

sürüşmə registrinin tələb olunan ardıcıllığı əmələ gətirməsini isbat edək. Bunu S_j ilə sürüşmə registrinin əks əlaqəsinin çıxışında olan siqnalın fərqini hesablamaqla bilavasitə isbat edək:

$$S_j - \left(-\sum_{i=1}^{L_r} \Lambda_i^{(r)} S_{j-i} \right) = S_j + \sum_{i=1}^{L_{r-1}} \Lambda_i^{(r-1)} S_{j-i} -$$

$$- \Delta_r \Delta_m^{-1} \left[S_{j-r+m} + \sum_{i=1}^{L_{m-1}} \Lambda_i^{(m-1)} S_{j-r+m-i} \right] =$$

$$= \begin{cases} 0 & , \quad j = L_r, L_r + 1, ..., r-1, \\ \Delta_r - \Delta_r \Delta_m^{-1} \Delta_m = 0, & i = r. \end{cases}$$

Beləliklə, $(L_r, \Lambda^{(r)}(x))$ sxemi $S_1, ..., S_r$ ardıcıllığını doğurur; xüsusi halda $(L_{2t}, \Lambda^{(2t)}(x))$ sxemi $S_1, ..., S_{2t}$ ardıcıllığını doğurur. □

Nümunə 1. $GF(16)$ meydanı üzərində (15,9) – Rid-Solomon koduna baxaq. Bu kod üç səhvi düzəldə bilər. Bu kodun əmələgətirici çoxhədlisi aşağıdakı çoxhədlidir (α -meydanın primitiv elementidir):

$$g(x) = (x+\alpha)(x+\alpha^2)(x+\alpha^3)(x+\alpha^4)(x+\alpha^5)(x+\alpha^6) =$$

$$= x^6 + \alpha^{10} x^5 + \alpha^{14} x^4 + \alpha^4 x^3 + \alpha^6 x^2 + \alpha^9 x + \alpha^6 .$$

Tutaq ki, $i(x) = 0$ -dır. Aydındır ki, $c(x) = 0$ olar. Tutaq ki, qəbul edilən çoxhədli

$$\upsilon(x) = \alpha x^7 + \alpha^5 x^5 + \alpha^{11} x^2$$

çoxhədlisidir. $i(x) = 0$ olduğundan $e(x) = \upsilon(x)$ olar. S_1, S_2, S_3, S_4, S_5 və S_6 sindrom komponentlərini hesablayaq:

$$S_1 = \alpha\alpha^7 + \alpha^5\alpha^5 + \alpha^{11}\alpha^2 = \alpha^{12}, \quad S_2 = \alpha\alpha^{14} + \alpha^5\alpha^{10} + \alpha^{11}\alpha^4 = 1,$$

$$S_3 = \alpha\alpha^{21} + \alpha^5\alpha^{15} + \alpha^{11}\alpha^6 = \alpha^{14}, S_4 = \alpha\alpha^{28} + \alpha^5\alpha^{20} + \alpha^{11}\alpha^8 = \alpha^{13},$$

$$S_5 = \alpha\alpha^{35} + \alpha^5\alpha^{25} + \alpha^{11}\alpha^{10} = 1, \quad S_6 = \alpha\alpha^{42} + \alpha^5\alpha^{30} + \alpha^{11}\alpha^{12} = \alpha^{11}.$$

$\Lambda(x)$ çoxhədlisini hesablamaq üçün altı iterasiya lazım gəlir. İterasiyaların nəticəsi və $\Lambda(x)$ üçün son ifadə cədvəl 1-də verilir.

Nümunə 2. $GF(2)$ üzərində (15,5) – BÇX koduna baxaq. Bu kod üç səhvi düzəldə bilər. Bu kodun əmələgətirici çoxhədlisi $g(x) = x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1$ çoxhədlisidir.

Tutaq ki, sadəlik üçün $i(x) = 0$ -dır. Aydındır ki, $c(x) = 0$ olar. Tutaq ki, qəbul edilən çoxhədli $\upsilon(x) = x^7 + x^5 + x^2$ -dır.

$i(x) = 0$ olduğundan $e(x) = \upsilon(x)$ olar.

Cədvəl 1

r	Δ_r	$T(x)$	$B(x)$		L
0			1	1	0
1	α^{12}	$1+\alpha^{12}x$	α^3	$1+\alpha^{12}x$	1
2	α^7	$1+\alpha^3 x$	$\alpha^3 x$	$1+\alpha^3 x$	1
3	1	$1+\alpha^3 x+\alpha^3 x^2$	$1+\alpha^3 x$	$1+\alpha^3 x+\alpha^3 x^2$	2
4	1	$1+\alpha^{14}x$	$x+\alpha^3 x^2$	$1+\alpha^{14}x$	2
5	α^{11}	$1+\alpha^{14}x+\alpha^{11}x^2+\alpha^{14}x^3$	$a^4+\alpha^3 x$	$1+\alpha^{14}x+\alpha^{11}x^2+\alpha^{14}x^3$	3
6	0	$1+\alpha^{14}x+\alpha^{11}x^2+\alpha^{14}x^3$	$a^4 x+\alpha^3 x^2$	$1+\alpha^{14}x+\alpha^{11}x^2+\alpha^{14}x^3$	3
$\Lambda(x) = 1+\alpha^{14}x+\alpha^{11}x^2+\alpha^{14}x^3 = (1+\alpha^7 x)(1+\alpha^5 x)(1+\alpha^2 x)$					

S_1, S_2, S_3, S_4, S_5 və S_6 sindrom komponentlərini hesablayaq:

$$S_1 = \alpha^7 + \alpha^5 + \alpha^2 = \alpha^{14}, \quad S_2 = \alpha^{14} + \alpha^{10} + \alpha^4 = \alpha^{13},$$

$$S_3 = \alpha^{21} + \alpha^{15} + \alpha^6 = 1, \quad S_4 = \alpha^{28} + \alpha^{20} + \alpha^8 = \alpha^{11},$$

$$S_5 = \alpha^{35} + \alpha^{25} + \alpha^{10} = \alpha^5, \quad S_6 = \alpha^{42} + \alpha^{30} + \alpha^{12} = 1.$$

$\Lambda(x)$ çoxhədlisini hesablamaq üçün altı iterasiya lazım gəlir. İterasiyaların nəticəsi və $\Lambda(x)$ üçün son ifadə cədvəl 2-də verilir.

Nümunə 3. $t=3$ səhvi düzəldə bilən və əmələgətirici çoxhədlisi $g(x)=x^{10}+x^8+x^5+x^4+x^2+x+1$ olan (15,5) – BÇX koduna baxaq. Tutaq ki, $\upsilon(x)=x^4+x^2+x+1$ kod sözü qəbul olunmuşdur. Ötürülən $c(x)$ çoxhədlisini tapmalı.

Sindrom komponentlərini hesablayaq:

$$S_1=\upsilon(\alpha)=\alpha^4+\alpha^2+\alpha+1=\alpha^2,$$
$$S_2=\upsilon(\alpha^2)=\alpha^8+\alpha^4+\alpha^2+1=\alpha^4,$$
$$S_3=\upsilon(\alpha^3)=\alpha^{12}+\alpha^6+\alpha^3+1=\alpha^9,$$
$$S_4=\upsilon(\alpha^4)=\alpha+\alpha^8+\alpha^4+1=\alpha^8,$$
$$S_5=\upsilon(\alpha^5)=\alpha^5+\alpha^{10}+\alpha^5+1=\alpha^5,$$
$$S_6=\upsilon(\alpha^6)=\alpha^9+\alpha^{12}+\alpha^6+1=\alpha^3,$$

Başlanğıc şərt: $\Lambda^0(x)=1,\ B^{(0)}(x)=1,\ L_0=0$.

1-ci iterasiya: Δ_1 uyğunsuzluğunu hesablayaq:

$$\Delta_1=\Lambda_0^{(0)}\cdot S_1=\alpha^2\neq 0.$$

$L_1=\delta_1(1-L_0)+(1-\delta_1)L_0$-a baxaq. Burada $\delta_1=1$, çünki $\Delta_1\neq 0$ və $2L_0\leq 0$ eyni vaxtda ödənir. Deməli $L_1=1$.

(5) münasibətinin köməkliyi ilə alarıq:

$$\begin{pmatrix}\Lambda^{(1)}(x)\\ B^{(1)}(x)\end{pmatrix}=\begin{pmatrix}1 & -\Delta_1 x\\ \Delta_1^{-1} & 0\end{pmatrix}\begin{pmatrix}1\\ 1\end{pmatrix}=\begin{pmatrix}1+\alpha^2 x\\ \alpha^{13}\end{pmatrix}.$$

Buradan da $\Lambda^{(1)}(x)=1+\alpha^2 x,\ \ B^{(1)}(x)=\alpha^{13}$ olar.

Cədvəl 2

r	Δ_r	$T(x)$	$B(x)$	$\Lambda(x)$	L
0			1	1	0
1	α^{14}	$1+\alpha^{14}x$	α	$1+\alpha^{14}x$	1
2	0	$1+\alpha^{14}x$	αx	$1+\alpha^{14}x$	1
3	α^{11}	$1+\alpha^{14}x+\alpha^{12}x^2$	$\alpha^4+\alpha^3 x$	$1+\alpha^{14}x+\alpha^{12}x^2$	2

4	0	$1+\alpha^{14}x+\alpha^{12}x^2$	$\alpha^4 x+\alpha^3 x^2$	$1+\alpha^{14}x+\alpha^{12}x^2$	2
5	α^{11}	$1+\alpha^{14}x+\alpha^{11}x^2+$ $+\alpha^{14}x^3$	$a^4+\alpha^3 x+\alpha x^2$	$1+\alpha^{14}x+\alpha^{11}x^2+\alpha^{14}x^3$	3
6	0	$1+\alpha^{14}x+\alpha^{11}x^2+$ $+\alpha^{14}x^3$	$a^4 x+\alpha^3 x^2+\alpha x^3$	$1+\alpha^{14}x+\alpha^{11}x^2+\alpha^{14}x^3$	3
$\Lambda(x)=1+\alpha^{14}x+\alpha^{11}x^2+\alpha^{14}x^3=(1+\alpha^7 x)(1+\alpha^5 x)(1+\alpha^2 x)$					

2-ci iterasiya. Δ_2 uyğunsuzluğunu (3) düsturuna əsasən hesablayaq:

$$\Delta_2=\Lambda_0^{(1)}\cdot S_2+\Lambda_1^{(1)}\cdot S_1=\alpha^4+\alpha^2\cdot\alpha^2=0.$$

Onda $\delta_2=0$ və $L_2=L_1=1$ olar.

(5) münasibətinin köməkliyi ilə alarıq:

$$\begin{pmatrix}\Lambda^{(2)}(x)\\ B^{(2)}(x)\end{pmatrix}=\begin{pmatrix}1 & 0\\ 0 & x\end{pmatrix}\begin{pmatrix}1+\alpha^2 x\\ \alpha^{13}\end{pmatrix}=\begin{pmatrix}1+\alpha^2 x\\ \alpha^{13}x\end{pmatrix}.$$

Buradan da $\Lambda^{(2)}(x)=1+\alpha^2 x,\ \ B^{(2)}(x)=\alpha^{13}x$ olar.

*3-cü iterasiya. (*3) düsturuna əsasən alarıq:

$$\Delta_3=\Lambda_0^{(2)}\cdot S_3+\Lambda_1^{(2)}\cdot S_2=\alpha^9+\alpha^2\cdot\alpha^4=\alpha^5\neq 0.$$

$2L_2\le 2$ olduğundan (6) düsturuna görə $\delta_3=1$ və $L_3=2$ olar.. (5) münasibətinə görə alarıq:

$$\begin{pmatrix}\Lambda^{(3)}(x)\\ B^{(3)}(x)\end{pmatrix}=\begin{pmatrix}1 & \alpha^5 x\\ \alpha^{10} & 0\end{pmatrix}\begin{pmatrix}1+\alpha^2 x\\ \alpha^{13}x\end{pmatrix}=\begin{pmatrix}1+\alpha^2 x+\alpha^3 x^2\\ \alpha^{10}+\alpha^{12}x\end{pmatrix}.$$

Beləliklə, $\Lambda^{(3)}(x)=1+\alpha^2 x+\alpha^3 x^2,\ \ B^{(3)}(x)=\alpha^{10}+\alpha^{12}x$ olar.

4-cü iterasiya. (3) düsturundan alarıq:

$$\Delta_4=\Lambda_0^{(3)}\cdot S_3+\Lambda_1^{(3)}\cdot S_2+\Lambda_2^{(3)}\cdot S_1=\alpha^8+\alpha^{11}+\alpha^7=0.$$

Beləliklə, $\Delta_4=0$ olduğundan (6) düsturuna görə $\delta_4=0$ və (4) düsturuna görə $L_4=L_3=2$ olar. (5) münasibətinə görə alarıq:

$$\begin{pmatrix}\Lambda^{(4)}(x)\\ B^{(4)}(x)\end{pmatrix}=\begin{pmatrix}1 & 0\\ 0 & x\end{pmatrix}\cdot\begin{pmatrix}1+\alpha^2 x+\alpha^3 x^2\\ \alpha^{10}+\alpha^{12}x\end{pmatrix}=\begin{pmatrix}1+\alpha^2 x+\alpha^3 x^2\\ \alpha^{10}x+\alpha^{12}x^2\end{pmatrix}.$$

Buradan da $\Lambda^{(4)}(x) = 1 + \alpha^2 x + \alpha^3 x^2$, $B^{(4)}(x) = \alpha^{10} x + \alpha^{12} x^2$ olar.

5-ci iterasiya. Δ_5 -i hesablayaq:

$$\Delta_5 = \Lambda_0^{(4)} \cdot S_5 + \Lambda_1^{(4)} \cdot S_4 + \Lambda_2^{(4)} \cdot S_3 = \alpha^5 + \alpha^{10} \cdot \alpha^{12} = \alpha^{11} \neq 0 .$$

Eyni vaxtda $\Delta_5 \neq 0$ və $2L_4 \leq 4$ olduğundan $\delta_5 = 1$ və $L_5 = 3$ olar. (5) münasibətinə görə

$$\begin{pmatrix} \Lambda^{(5)}(x) \\ B^{(5)}(x) \end{pmatrix} = \begin{pmatrix} 1 & \alpha^{11} x \\ \alpha^4 & x \end{pmatrix} \cdot \begin{pmatrix} 1 + \alpha^2 x + \alpha^3 x^2 \\ \alpha^{10} x + \alpha^{12} x^2 \end{pmatrix} = \begin{pmatrix} 1 + \alpha^2 x + \alpha^2 x^2 + \alpha^8 x^3 \\ \alpha^4 + \alpha^6 x + \alpha^6 x^2 + \alpha^{12} x^3 \end{pmatrix}.$$

Buradan da

$\Lambda^{(5)}(x) = 1 + \alpha^2 x + \alpha^2 x^2 + \alpha^8 x^3$, $B^{(5)}(x) = \alpha^4 + \alpha^6 x + \alpha^6 x^2 + \alpha^{12} x^3$ olar.

6-cı iterasiya. Δ_6 -nı hesablayaq:

$$\Delta_6 = \Lambda_0^{(5)} \cdot S_6 + \Lambda_1^{(5)} \cdot S_5 + \Lambda_2^{(5)} \cdot S_4 + \Lambda_3^{(5)} S_3 =$$
$$= \alpha^3 + \alpha^2 \cdot \alpha^5 + \alpha^2 \cdot \alpha^8 + \alpha^8 \cdot \alpha^9 = \alpha^3 + \alpha^7 + \alpha^{10} + \alpha^2 = 0.$$

$\Delta_6 = 0$ olduğundan $\delta_6 = 0$ və $L_6 = L_5 = 3$ olar.

$$\begin{pmatrix} \Lambda^{(6)}(x) \\ B^{(6)}(x) \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & x \end{pmatrix} \begin{pmatrix} 1 + \alpha^2 x + \alpha^2 x^2 + \alpha^8 x^3 \\ \alpha^4 + \alpha^6 x + \alpha^6 x^2 + \alpha^{12} x^3 \end{pmatrix} =$$
$$= \begin{pmatrix} 1 + \alpha^2 x + \alpha^2 x^2 + \alpha^8 x^3 \\ \alpha^4 x + \alpha^6 x^2 + \alpha^6 x^3 + \alpha^{12} x^4 \end{pmatrix}.$$

Beləliklə, $\Lambda(x) = \Lambda^{(6)}(x) = \alpha^8 x^3 + \alpha^2 x^2 + \alpha^2 x + 1$.

$\Lambda(x)$ çoxhədlisinin köklərini axtarsaq, onda $x^1 = \alpha^5$, $x^2 = \alpha^7, x^3 = \alpha^{10}$ və ya $X_1^{-1} = \alpha^5$, $X_2^{-1} = \alpha^7$, $X_3^{-1} = \alpha^{10}$.

Buradan da $X_1 = \alpha^{10}$, $X_2 = \alpha^8$, $X_3 = \alpha^5$ alınar. Beləliklə, səhv çoxhədlisi $e(x) = x^{10} + x^8 + x^5$ olar. Deməli,

$$c(x) = \upsilon(x) + e(x) = x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1$$

alarıq.

§5. BÇX kodlarının cəld dekodlaşdırılması. Forni alqoritmi

$$\Lambda'(X_\ell^{-1}) = -X_\ell \prod_{j\neq\ell}(1 - X_j X_\ell^{-1}).$$

Buradan da

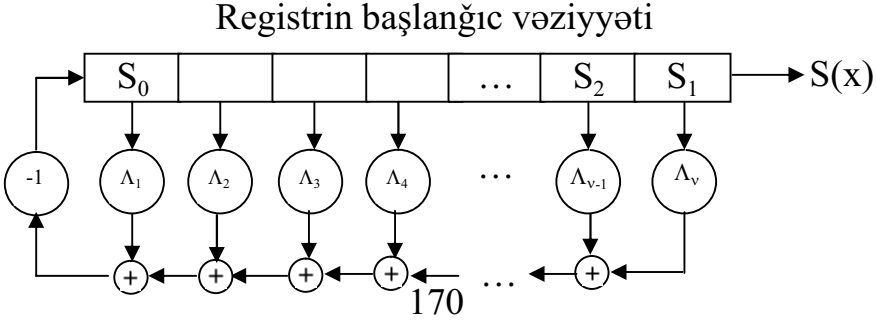
$$Y_\ell = -\frac{\Omega(X_\ell^{-1})}{\Lambda'(X_\ell^{-1})}.$$

Berlekemp-Messi alqoritmindən (teorem 4.1) istifadə etməklə səhvlər lokatoru çoxhədlisinin hesablanmasına qayıdaq. Şəkil 1.a-da bu məsələnin həlli üçün Messi tərəfindən təklif olunan variant göstərilir. Verilən $S_j, j = 1,...,2t$ üçün aşağıdakı t tənlikləri ödəyən minimal uzunluqlu Λ vektoru tapılır:

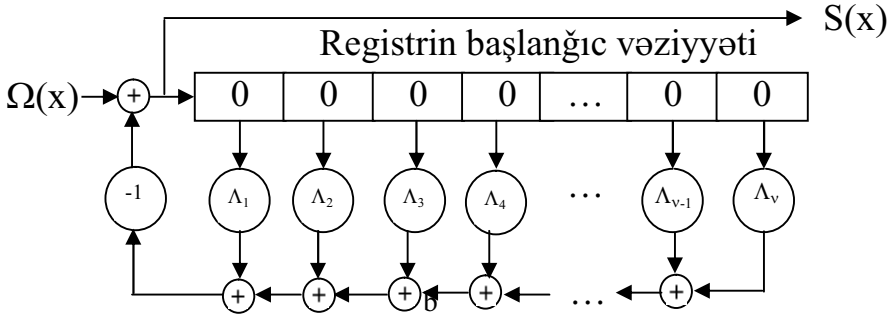
$$S_j + \sum_{k=1}^{t} S_{j-k}\Lambda_k = 0,\ j = t+1,...,2t. \qquad (3)$$

Bu o deməkdir ki, əgər məlumdursa ki, $j > t$ olduqda $\Lambda_j = 0$, onda S vektorunun $2t$ sayda komponenti əsasında Λ vektorunun hesablanması tələb olunur. (3) bərabərliyini ödəyən Λ vektoru (1) səhvlər lokatoru çoxhədlisinin əmsallarını təyin edir, harada ki, $X_\ell, \ell = 1,...,\nu$, kəmiyyətləri səhvlərin lokatorlarıdır. Səhvlərin qiymətləri çoxhədlisi olan $\Omega(x)$ çoxhədlisi (2) düsturu ilə təyin olunur.

Baxılan məsələnin həllinin Berlekemp variantı şəkil 1.b-də göstərilir və bu şəkildən görünür ki, səhvlərin qiymətlər çoxhədlisi burada böyük əhəmiyyətə malikdir.



a



Şəkil 1.

Belə variantda Λ və Ω vektorlarının axtarışında fərz olunur ki, onların komponentləri $t < k \le n$ olduqda (k komponentin nömrəsidir) sıfıra bərabərdir və aşağıdakı $2t$ tənlikləri ödəyir:

$$S_j + \sum_{k=1}^{t} S_{j-k}\Lambda_k = \Omega_j, \quad j = 1,...,2t, \tag{4}$$

harada ki, $j \le 0$ olduqda $S_j = 0$. (4) tənliklər sisteminin həlli iki çoxhədli ilə verilir: səhvlərin lokatoru çoxhədlisi və səhvlərin qiyməti çoxhədlisi.

Yuxarıda təsvir olunan iki variant ekvivalentdir. Bundan sonra Messi tərəfindən təklif olunan varianta baxılacaq. Zəruriyyət yarandıqda Berlekemp-Messi alqoritmini iterasiyanı bilavasitə $\Lambda^{(r)}(x)$ və $\Omega^{(r)}(x)$ çoxhədliləri üçün aparmaqla Berlekemp formasına çevirmək olar.

Şəkil 2-də Berlekemp-Messi alqoritminin blok-sxemi verilir. Göstərildiyi kimi bu alqoritm $2t$ sayda verilmiş $S_1,...,S_{2t}$ sindrom komponentləri vasitəsilə səhvlərin lokator çoxhədlisinin hesablanmasına imkan verir. Əgər kodda $j_0 \ne 1$ isə, onda S_j $j = 1,...,2t$, kəmiyyəti $S_j = V_{j+j_0-1}$ kimi təyin olunur. Sindromun bu komponentləri hesablamada əvvəlki komponentlər kimi iştirak edirlər. Bu halda alqoritmin özü heç bir dəyişikliyə məruz qalmır, lakin alqoritm daxili dəyişənlərin indeksləri uyğun olaraq dəyişdirilir.

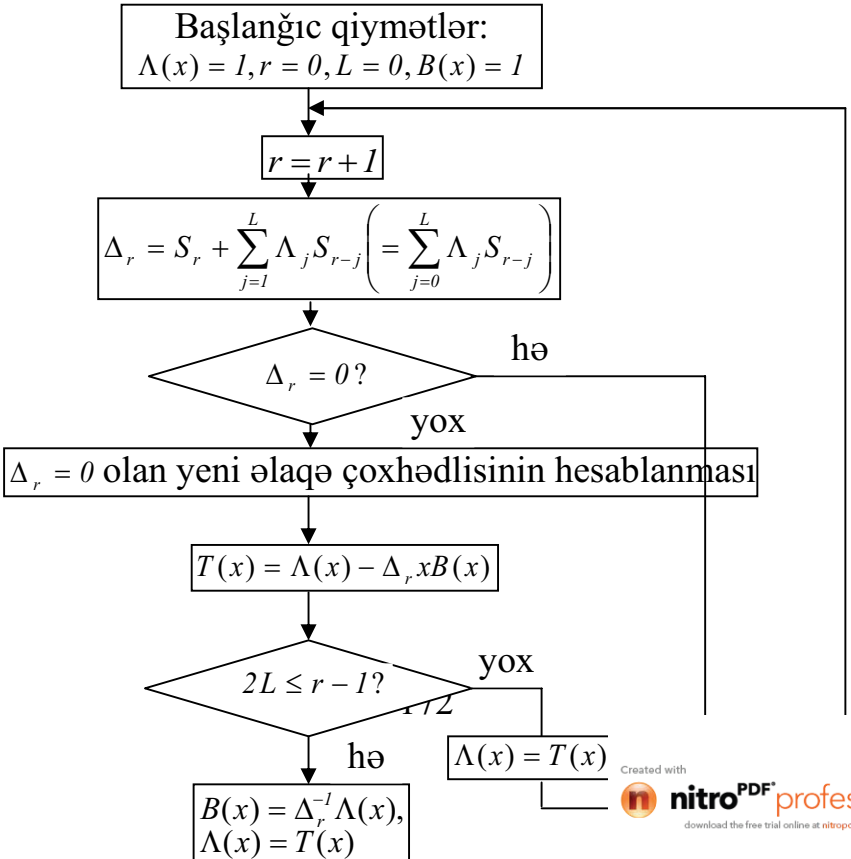
Berlekemp-Messi alqoritminin daxili məntiqi bir az müəmmalı görünə bilər. Əmələ gələn suallara cavablar mümkündür ki, aşağıdakı düşüncələri, mülahizələri tapmağa kömək etsin. Bəzi iterasiyalarda, deyək ki, r-ci iterasiyada, Berlekemp-

Messi alqoritmi ilə götürülən əks əlaqəli sxemlə eynigüclü olan və lazım olan simvolu doğuran başqa bir əks əlaqəli sxemlər mövcud ola bilərlər. Bütün bu sxemlər r sayda komponentlərin eyni bir ardıcıllığını doğurarlar; eyni zamanda bu r ardıcıllığa daxil olmayan növbəti komponentlər müxtəlif olar. Hər dəfə mümkün olduqca növbəti iterasiyada əvvəlki uzunluğa malik olan və sindromun tələb olunan növbəti komponentlərini doğuran əks əlaqəli sxem götürülür;

Əgər belə sxem olmazsa, onda sxemin uzunluğunu artırmaq lazım gəlir. Lakin sxemin uzunluğunun artırılmasının zəruriliyi məsələsi həll ediləndə sindromun növbəti komponentin qiyməti nəzərə alınmır (ancaq $\Lambda_{r+1} \neq 0$ şərtinin ödənməsi yoxlanır).

Beləliklə, $(r+1)$-ci addımda sxemlər üçün olan variantların sayı ən azı S_{r+1}-in ala biləcəyi qiymətlərin sayı qədərdir.

Təsvir olunan alqoritm kompüterlərdə proqram şəklində realizə oluna bilər. Əgər çox böyük sürətlə dekodlaşdırma tələb olunarsa, onda dekoderləri «bərk» halda qurmaq olar, yəni sxemlər vasitəsilə. Bu zaman sürüşmə registrləri, diskret sxemlər, ardıcıllıqlı maşınlar istifadə oluna bilər.



Şəkil 2.

Sürüşmə registrlərində qurulan aparat realizəsi sxemi şəkil 3-də verilir. Bu şəkildə təsvir olunan üç registr $S(x), \Lambda(x)$ və $B(x)$ çoxhədlilərinin əmsallarının qiymətlərinin saxlanması üçün istifadə olunur. Hər bir registrin uzunluğu onun saxlayacağı uyğun çoxhədli əmsallarının sayından az olmamalıdır, yəni uyğun çoxhədlinin ola biləcək ən böyük dərəcəsindən bir az çox olmalıdır. Əgər registrlər maksimal dərəcədən kiçik olan dərəcəyə malik çoxhədlilərin əmsallarını saxlayarsa, boş qalan mövqələr sıfırlarla doldurulmalıdır. $S(x)$ və $B(x)$ üçün olan registrlər maksimal dərəcə halında lazım gələn mövqe sayından bir vahid çox mövqeyə malik olmalıdırlar; $S(x)$ üçün olan registrlərdə də ehtiyat mövqelər olmalıdır.

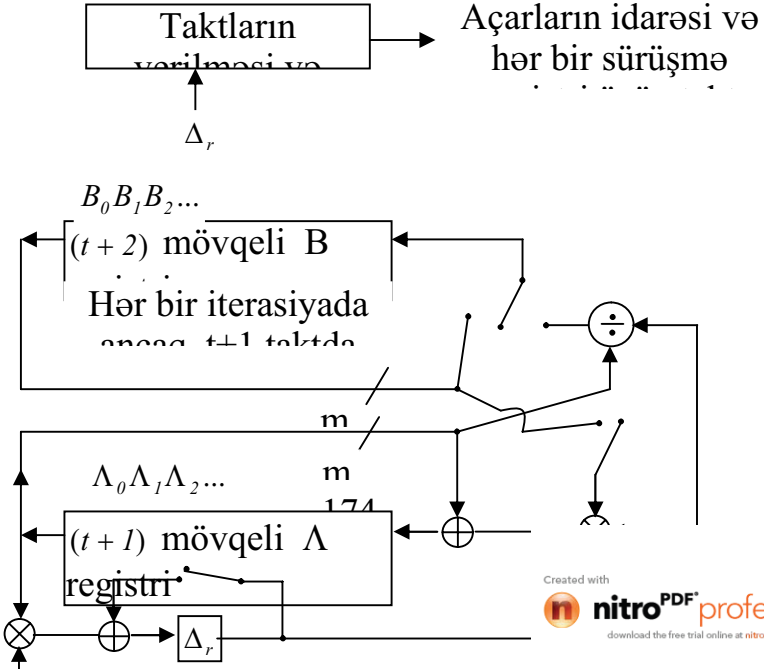
Registrlərin uzunluğunun bir iterasiya müddətində hər bir registrin iş vaxtının sayı ilə birlikdə seçilməsi ona gətirib çıxarır ki, hər bir iterasiya

nəticəsində çoxhədlilərin əmsalları ilkin vəziyyətdən bir mövqe sürüşdürülür. Bu $B(x)$-ın x-a vurulmasını və Δ_r üçün ifadəyə daxil olan S_{r-j} komponentinin alınmasına gətirib çıxaran S_j komponentlərinin indeksdəyişdirilməsini təmin edir. Bunu başa düşmək üçün şəkil 3-ə baxaq, hansı ki, burada $S(x)$ registri başlanğıc vəziyyətində göstərilmişdir. Hər bir iterasiya nəticəsində bu registrin məzmunu bir mövqe sağa sürüşür və nəticədə növbəti iterasiyada $S(x)$ və $\Lambda(x)$ çoxhədlilərinin uyğun əmsallarının düzgün vurulması təmin olunur. Λ registri bir iterasiya müddətində tam uzunluqda iki dəfə sürüşür: Λ_r hesablandıqda və bu registrə Λ-ın yeni qiyməti daxil edildikdə.

Şəkil 4-də Berlekemp-Messi və Forni alqoritmlərini istifadə edən dekoderin yerinə yetirdiyi hesablamalar ardıcıllığı təsvir olunmuşdur.

t-dən çox olmayan sayda səhv baş verdikdə dekoder səhvlərin lokatoru çoxhədlisi üçün düzgün ifadə tapır. t-dən çox sayda səhv baş verdikdə dekodlaşdırma müvəffəqiyyətsiz olur və alınan çoxhədli ya səhvlərin lokatoru çoxhədlisinin ödədiyi şərtləri ödəmir, ya da ki, mümkün çoxhədli olur, amma düzgün çoxhədli olmur.

Birinci halda dekoder səhvi aşkarlaya bilər, lakin onu düzəldilə bilməyən səhv kimi nəzərdə tutar. Düzəldilə bilməyən səhvlər konfiqurasiyasının aşkarlanması haqqında qərar qəbulu o halda olur ki, aşağıdakı iki şərtdən biri ödənmiş olsun:

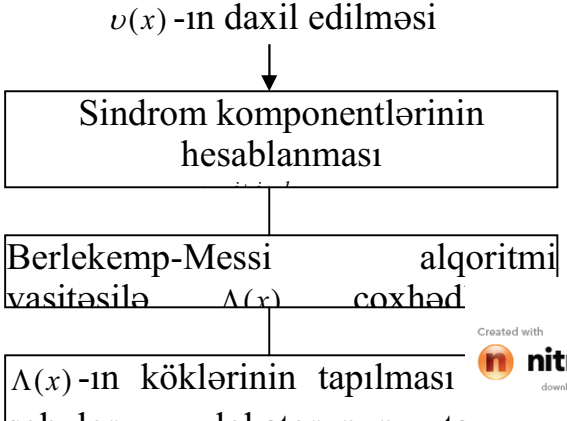


Şəkil 3.

1) $\Lambda(x)$-ın $GF(q^m)$-də yerləşən müxtəlif köklərinin sayı L-ə bərabər deyil;

2) Səhvlərin qiymətləri kodun simvolları meydanında yerləşmir.

Dekodlaşdırma zamanı əvvəlcə səhvlərin lokatorları çoxhədlisi yoxlanılır. Əgər o lazım olan şərtləri ödəyirsə, onda dekoder səhvlərin qiyməti çoxhədlisini hesablamağa başlayır. Ola bilər ki, səhvlərin qiyməti kod simvolları meydanına daxil olmasın (əgər bu meydan səhvlər lokatoru meydanından kiçik olarsa).



Şəkil 4.

Səhv dekodlaşdırma ehtimalını azaltmaq üçün dekoderin düzəldə bildiyi səhvlərin sayını elə t qiyməti ilə məhdudlaşdırmaq lazımdır ki, $2t+1<d^*$ olsun. Dekoderin düzəldilə bilməyən səhvi aşkarlaması üçün kod sözü düzgün olmayan dekodlaşdırma sferasına keçməlidir, yəni d^*-t sayda səhv baş verməlidir.

Belə dekoderdə Berlekemp-Messi alqoritmini tətbiq etmək lazımdır. $\Lambda(x)$-ı hesablamaq üçün bu alqoritmlə $2t$ sayda iterayisa etmək lazımdır. Qalan $\tau-t$ sayda iterasiya Δ_r uyğunsuzluğunun sıfra bərabər olmasının yoxlanması üçün nəzərdə tutulur, harada ki, $\tau=d^*-1-t$. Əgər bu əlavə iterasiyalardan heç olmazsa birində $\Delta_r\neq 0$ olarsa, onda qəbul edilən söz

t-dən çox səhvin baş verdiyi söz kimi elan olunur. Təsvir olunan proseduranın düzgünlüyü aşağıdakı teoremlə isbat olunur.

Teorem 3. Tutaq ki, τ -dan çox olmayan sayda səhv baş vermişdir və $j = 1,...,t+\tau$ üçün S_j-lər verilib və $\tau > t$. Tutaq ki, $(L_{2t}, \Lambda^{(2t)}(x))$ sxemi S_j, $j = \overline{1,2t}$ ardıcıllığını doğuran əks əlaqəli sürüşmə registridir və

$$\Delta_r = \sum_{j=0}^{n-1} \Lambda_j^{(2t)} S_{r-j}$$

kimi təyin olunur, özü də $r = 2t+1,...,t+\tau$ olduqda $\Delta_r = 0$ olur və $L_{2t} \le t$. Onda t-dən çox olmayan sayda səhv baş vermişdir və $\Lambda^{(2t)}(x)$ çoxhədlisi səhvlərin lokatorunun düzgün çoxhədlisi olar.

İsbatı. Teoremin şərtlərində $S_j, j = 1,...,t+\tau$ sindrom komponentləri verilmişdir. Əgər yenə $\tau - t$ sayda $S_j, j = t+\tau+1,...,2\tau$, sindrom komponentləri olarsa, onda τ sayda səhvi düzəltmək olardı. Tutaq ki, bu əlavə komponentlər də haradansa bizə məlumdur. Onda Berlekemp-Messi alqoritmini istifadə etməklə dərəcəsi səhvlərin sayına bərabər olan səhvlərin lokatoru çoxhədlisini tapa bilərik. Lakin $2t$-ci iterasiyada $L_{2t} \le t$, və fərziyyəyə görə $r = 2t+1,...,t+\tau$ olduqda $\Delta_r = 0$. Ona görə də L kəmiyyəti $t+\tau+1$ nömrəli iterasiyaya kimi dəyişməyəcək və, beləliklə, L -in dəyişməsi qaydasına görə

$$L_{2\tau} \ge (t+\tau+1) - L_{2t} \ge (t+\tau+1) - t = \tau+1 .$$

Bu isə τ -dən çox olmayan sayda səhv baş verməsi şərtinə ziddir.

□

Nümunə 1. $GF(3^3)$ meydanı üzərində $t = 2$ səhvi düzəldə bilən və əmələgətirici çoxhədlisi

$$g(x) = x^9 + 2x^8 + x^7 + x^6 + x^5 + 2x^4 + 2x^3 + 2x^2 + x + 1$$

olan (26,17)- BÇX koduna baxaq. Tutaq ki,

$$\upsilon(x) = x^9 + x^7 + x^6 + 2x^4 + 2x^3 + 2x^2 + x + 1$$

kod çoxhədlisi qəbul olunmuşdur. Ötürülən $c(x)$ çoxhədlisini tapmalı.

Əvvəlcə $\Lambda(x)$ səhvlərin lokatorları çoxhədlisini tapaq. Bunun üçün sindrom komponentlərini hesablayaq:

$$S_1 = \upsilon(\alpha) = \alpha^{14}, \quad S_2 = \upsilon(\alpha^2) = \alpha^{20}, \quad S_3 = \upsilon(\alpha^3) = \alpha^{16},$$

$$S_4 = \upsilon(\alpha^4) = \alpha^{15}$$

Baş verən səhvlərin sayını tapaq. $\upsilon = 2$ olduqda alarıq:

$$\begin{vmatrix} S_1 & S_2 \\ S_2 & S_3 \end{vmatrix} = \begin{vmatrix} \alpha^{14} & \alpha^{20} \\ \alpha^{20} & \alpha^{16} \end{vmatrix} = \alpha^4 - \alpha^{14} = \alpha^2 .$$

$\alpha^2 \neq 0$ olduğundan səhvlərin sayı $\nu = 2$ olar. Deməli, səhvlərin lokatoru çoxhədlisi $\Lambda(x) = \alpha^{13}x^2 + \alpha^{19}x - 1$ olar. Bilavasitə yoxlamaqla müəyyən etmək olar ki, bu çoxhədlinin kökləri $x_1 = X_1^{-1} = \alpha^{18}$, $x_2 = X_2^{-1} = \alpha^{21}$ kimidir. Buradan da $X_1 = \alpha^8$ və $X_2 = \alpha^5$ alırıq. Deməli, 8-ci və 5-ci mövqelərdə səhv baş vermişdir.

Forni alqoritmindən istifadə etməklə səhvlərin qiymətlərini hesablayaq. Bunun üçün $S(x)$ sindrom çoxhədlisini quraq:

$$S(x) = S_1 + S_2x + S_3x^2 + S_4x^3 = \alpha^{14} + \alpha^{20}x + \alpha^{16}x^2 + \alpha^{15}x^3 .$$

$\Omega(x) = S(x) \cdot \Lambda(x) \pmod{x^4}$ düsturu ilə $\Omega(x)$ səhvlər çoxhədlisini hesablasaq alarıq: $\Omega(x) = \alpha^{14}$.

Digər tərəfdən, $\Lambda'(x) = \alpha^{19} + 2\alpha^{13}x$.

Y_1 və Y_2 kəmiyyətlərini

$$Y_i = -\frac{\Omega(X_i^{-1})}{\Lambda'(X_i^{-1})}, \quad i = \overline{1,2}$$

düsturu ilə hesablayaq. Onda alarıq

$$Y_1 = -\frac{\alpha^{14}}{\alpha} = -\alpha^{13} = -2 = 1, \quad Y_2 = -\frac{\alpha^{14}}{\alpha^{14}} = -1 = 2,$$

Beləliklə, səhv çoxhədlisi $e(x) = x^8 + 2x^5$, ötürülən çoxhədlisi isə

$$c(x) = \upsilon(x) - e(x) =$$

$$= x^9 + 2x^8 + x^7 + x^6 + x^5 + 2x^4 + 2x^3 + 2x^2 + x + 1.$$

olar.

§6. İkilik BÇX kodlarının dekodlaşdırılması

Bu fəslin əvvəlki paraqraflarında deyilənlərin hamısı istənilən sonlu meydanlar halında doğrudur. $GF(2)$ meydanı halında aparılan bəzi mühakimələri sadələşdirmək olar. Aydındır ki, ikilik halında dekodlaşdırma zamanı ancaq səhvin mövqesini hesablamaq lazımdır, səhvin qiyməti həmişə vahidə bərabərdir.

Nümunə 4.2-dən görünür ki, Δ_r kəmiyyəti r-in cüt qiymətlərində, yəni cüt iterasiyalarda sıfıra bərabərdir. Əgər bu həmişə belə olarsa, onda cüt iterasiyalara baxmamaq olar.

İsbat edəcəyik ki, bu doğrudan da belədir. İsbat aşağıdakı fakta əsaslanır: $GF(2)$ meydanında cüt nömrəli sindromlar aşağıdakı düstur əsasında tək nömrəli sindromlar vasitəsilə təyin olunurlar:

$$S_{2j} = \upsilon(\alpha^{2j}) = \sum_{i=0}^{n-1} \upsilon_i (\alpha^{2j})^i = \left(\sum_{i=0}^{n-1} \upsilon_i (\alpha^j)^i \right)^2 = S_j^2.$$

r-in bir neçə ilkin qiymətləri halında $\Lambda^{(r)}(x)$-ın əmsalları üçün cəbri ifadələri hesablayaq. Şəkil 5.2-də verilən alqoritmdən bütün ikilik kodlar üçün doğru olan $S_4 = S_2^2 = S_1^4$ bərabərlikləri istifadə etməklə alarıq:

$$\Delta_1 = S_1, \quad \Delta_2 = S_2 + S_1^2 = 0, \quad \Delta_3 = S_3 + S_1 S_2,$$

$$\Delta_4 = S_4 + S_1 S_3 + S_1^{-1} S_2 S_3 + S_2^2 = 0,$$

$$\Lambda^{(1)}(x) = S_1 x + 1, \quad \Lambda^{(2)}(x) = S_1 x + 1,$$

$$\Lambda^{(3)}(x) = (S_1^{-1} S_3 + S_2) x^2 + S_1 x + 1.$$

Buradan alınır ki, istənilən ikilik BÇX-kodu üçün Δ_2 və Δ_4 həmişə sıfıra bərabərdir. r-in cüt qiymətlərində $\Delta_r = 0$ olması aşağıdakı teoremlə şərh olunur.

Teorem 1. Tutaq ki, $GF(2)$ meydanının genişlənməsində $2j \le 2\nu - 1$ olan $2j$ üçün $S_{2j} = S_j^2$ şərtini ödəyən ixtiyari bir $S_1, S_2, \ldots, S_{2\nu-1}$ ardıcıllığı verilmişdir; tutaq ki, həmçinin $\Lambda(x)$ xətti əks əlaqəli sürüşmə registri verilmişdir və aşağıdakı bərabərlik doğrudur:

$$S_j = \sum_{i=1}^{n-1} \Lambda_i S_{j-i}, \quad j = \nu, \ldots, 2\nu - 1.$$

Əgər ardıcıllığın növbəti həddi

$$S_{2\nu} = \sum_{i=1}^{n-1} \Lambda_i S_{2\nu-i}$$

bərabərliyi ilə təyin olunursa, onda

$$S_{2\nu} = S_\nu^2.$$

İsbatı. Göstərək ki, teoremin şərtləri daxilində S_ν^2 və $S_{2\nu}$ üçün ifadələr üst-üstə düşür.

Bir tərəfdən

$$S_\nu^2 = \left(\sum_{i=1}^{n-1} \Lambda_i S_{\nu-i} \right)^2 = \sum_{i=1}^{n-1} \Lambda_i^2 S_{\nu-i}^2 = \sum_{i=1}^{n-1} \Lambda_i^2 S_{2\nu-2i} \,. \qquad (1)$$

Digər tərəfdən isə

$$S_{2\nu} = \sum_{k=1}^{n-1} \Lambda_k S_{2\nu-k} = \sum_{k=1}^{n-1} \sum_{i=1}^{n-1} \Lambda_k \Lambda_i S_{2\nu-k-i} \,.$$

Sonuncu ifadənin simmetrikliyindən alınır ki, $i \neq k$ olduqda hər bir toplanan cəmə iki dəfə daxil olur. Hesablama $GF(2)$ meydanının genişlənməsində aparıldığından bu toplananların cəmi sıfıra bərabər olar. Ona görə də cəmdə o hədlər qalar ki, $i = k$ olsun:

$$S_{2\nu} = \sum_{i=1}^{n-1} \Lambda_i^2 S_{2\nu-2i} \qquad (2)$$

(1) və (2) bərabərliklərinin sağ tərəfləri üst-üstə düşdüyündən onların sol tərəfləri də üst-üstə düşər, yəni

$$S_\nu^2 = S_{2\nu}$$

Teorem 1-dən istifadə etməklə induksiya vasitəsi ilə ala bilərik ki, cüt qiymətli r üçün $\Delta_r = 0$. Ona görə də formal olaraq iki ardıcıl iterasiyanı birləşdirməklə ancaq tək nömrəli iterasiyalara baxmaq olar:

$$\Lambda^{(r)}(x) = \Lambda^{(r-2)}(x) - \Delta_r x^2 B^{(r-2)}(x) \,,$$

$$B^{(r)}(x) = \delta_r \Delta_r^{-1} \Lambda^{(r-2)}(x) + (1 - \delta_r) x^2 B^{(r-2)}(x) \,.$$

Bu düsturları istifadə etməklə cüt nömrəli iterasiyaları nəzərə almamaq olar və, beləliklə, dekodlaşdırmanı sürətləndirmək olar.

§7. Evklid alqoritminin köməkliyi ilə dekodlaşdırma

Evklid alqoritminin köməkliyi ilə dekodlaşdırma dekodlaşdırmanın əsas üsullarından biridir və bu üsul iki çoxhədlinin ən böyük ortaq bölәninin tapılması üçün olan rekurrent proseduraya əsaslanır. Bu proseduranın bir az genişlənməsi nəticəsində istənilən iki $s(x)$ və $t(x)$ çoxhədliləri üçün əlavə olaraq

$$\text{ƏBOB}\,[s(x),t(x)] = a(x)s(x) + b(x)t(x)$$

xətti ayrılışını ödəyən $a(x)$ və $b(x)$ çoxhədlilərini hesablamağa imkan verən üsul alınır.

İxtiyari $s(x)$ və $t(x)$ çoxhədliləri üçün Evklid alqoritmini

$$s(x) = \lfloor s(x)/t(x) \rfloor \cdot t(x) + r(x)$$

bölmə alqoritmindən istifadə etməklə matris şəklində təsvir edək. Bu təsvir aşağıdakı teoremlə şərh olunur ($\lfloor s(x)/t(x) \rfloor$ ilə $s(x)$ çoxhədlisi $t(x)$ çoxhədlisinə bölündükdə alınan natamam qismət, qalıq isə $r(x)$ ilə işarə olunur).

Teorem 1. Tutaq ki, $s(x)$ və $t(x)$ çoxhədliləri üçün $\deg s(x) \geq \deg t(x)$. Tutaq ki, $s^{(0)}(x) = s(x)$, $t^{(0)}(x) = t(x)$ və $A^0(x) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Aşağıdakı rekurrent tənliyə baxaq:

$$Q^{(r)}(x) = \left\lfloor \frac{s^r(x)}{t^{(r)}(x)} \right\rfloor, \quad A^{(r+1)}(x) = \begin{pmatrix} 0 & 1 \\ 1 & -Q^{(r)}(x) \end{pmatrix} \cdot A^{(r)}(x),$$

$$\begin{pmatrix} s^{(r+1)}(x) \\ t^{(r+1)}(x) \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -Q^{(r)}(x) \end{pmatrix} \begin{pmatrix} s^{(r)}(x) \\ t^{(r)}(x) \end{pmatrix} = A^{(r+1)} \begin{pmatrix} s^{(r)}(x) \\ t^{(r)}(x) \end{pmatrix}.$$

Onda bu tənliyin həlli

$$s^{(R)}(x) = \gamma \cdot \text{ƏBOB}[s(x), t(x)]$$

olar və həm də elə γ skalyarı tapılar ki,

$$\gamma\,\text{ƏBOB}[s(x), t(x)] = A_{11}^{(R)}(x)s(x) + A_{12}^{(R)}t(x),$$

olsun, harada ki, R elədir ki, $t^{(R)}(x) = 0$ olur.

İsbatı. Aydındır ki, $\deg t^{(r+1)}(x) < \deg t^{(r)}(x)$. Ona görə də nəhayət hər hansı bir R üçün $t^{(R)}(x) = 0$ olar və proses mütləq dayanar. Beləliklə,

$$\begin{pmatrix} s^{(R)}(x) \\ 0 \end{pmatrix} = \left\{ \prod_{r=R-1}^{0} \begin{pmatrix} 0 & 1 \\ 1 & -Q^{(r)}(x) \end{pmatrix} \right\} \begin{pmatrix} s(x) \\ r(x) \end{pmatrix}. \qquad (1)$$

Buradan da çıxır ki, $s(x)$ və $t(x)$ çoxhədlilərinin istənilən bölənləri $s^{(R)}(x)$ çoxhədlisini də bölər.

Asanlıqla yoxlamaq olar ki,

$$\begin{pmatrix} 0 & 1 \\ 1 & -Q^{(r)}(x) \end{pmatrix}^{-1} = \begin{pmatrix} Q^{(r)}(x) & 1 \\ 1 & 0 \end{pmatrix}$$

və ona görə də

$$\begin{pmatrix} s(x) \\ t(x) \end{pmatrix} = \left\{ \prod_{r=0}^{R-1} \begin{pmatrix} Q^{(r)}(x) & 1 \\ 1 & 0 \end{pmatrix} \right\} \begin{pmatrix} s^{(R)}(x) \\ 0 \end{pmatrix}, \qquad (2)$$

belə ki, $s^{(R)}(x)$ çoxhədlisi $s(x)$ və $t(x)$ çoxhədlilərini də bölməlidir və, beləliklə, ƏBOB$[s(x), t(x)]$ -i də bölməlidir. Buradan alırıq ki, ƏBOB$[s(x), t(x)]$ həm $s^{(R)}(x)$-i bölür və həm də ona bölünür. Deməli,

$$s^{(R)}(x) = \gamma\,\text{ƏBOB}[s(x), t(x)].$$

Aydındır ki, $A^{(r)}(x)$ -in təyinindən və (1) münasibətindən alarıq

$$\begin{pmatrix} s^{(R)}(x) \\ 0 \end{pmatrix} = A^{(R)}(x) \begin{pmatrix} s(x) \\ t(x) \end{pmatrix}$$

və, beləliklə,

$$s^{(R)}(x) = A_{11}^{(R)}(x) \cdot s(x) + A_{12}^{(R)}(x) \cdot t(x).$$

Burada hesab olunur ki, $A^{(R)}(x)$ matrisi aşağıdakı şəkildə matrisdir:

$$A^{(R)}(x) = \begin{pmatrix} A_{11}^{(R)}(x) & A_{12}^{(R)}(x) \\ A_{21}^{(R)}(x) & A_{22}^{(R)}(x) \end{pmatrix}$$

Teorem 1-də $A_{11}^{(R)}(x)$ və $A_{12}^{(R)}(x)$ matris elementlərinin nə üçünolması göstərilmişdir. $A^{(R)}(x)$ matrisinin qalan iki elementinin də mənasını təyin etmək olar. Bunun üçün $A^{(r)}(x)$ matrisinə tərs olan matrisi tapmaq lazımdır. Aydındır ki,

$$A^{(r)}(x) = \prod_{\ell=r-1}^{0} \begin{pmatrix} 0 & 1 \\ 1 & -Q^{(\ell)}(x) \end{pmatrix}.$$

Bu bərabərlikdən görünür ki, $A^{(r)}(x)$ matrisinin determinantı $(-1)^r$ -ə bərabərdir. Onda tərs matrisin təyininə görə tərs matris aşağıdakı matrisdir:

$$\begin{pmatrix} A_{11}^{(r)}(x) & A_{12}^{(r)}(x) \\ A_{21}^{(r)}(x) & A_{22}^{(r)}(x) \end{pmatrix}^{-1} = (-1)^r \begin{pmatrix} A_{22}^{(r)}(x) & -A_{12}^{(r)}(x) \\ -A_{21}^{(r)}(x) & A_{11}^{(r)}(x) \end{pmatrix}. \tag{3}$$

Nəticə 1. Evklid alqoritminin köməkliyi ilə alınan $A_{21}^{(r)}(x)$ və $A_{22}^{(r)}(x)$ çoxhədliləri aşağıdakı bərabərlikləri ödəyir:

$$s(x) = (-1)^R A_{22}^R(x)\gamma \cdot \text{ƏBOB}[s(x), t(x)], \quad (4)$$

$$t(x) = (-1)^R A_{21}^R(x)\gamma \cdot \text{ƏBOB}[s(x), t(x)].$$

İsbatı. (3)-dən istifadə etməklə (2)-dən alarıq:

$$\begin{pmatrix} s(x) \\ t(x) \end{pmatrix} = (-1)^R \begin{pmatrix} A_{22}^{(R)}(x) & -A_{12}^{(R)}(x) \\ -A_{21}^{(R)}(x) & A_{11}^{(R)}(x) \end{pmatrix} \cdot \begin{pmatrix} s^{(R)}(x) \\ 0 \end{pmatrix}.$$

Buradan da (4) münasibətləri alınır. □

Evklid alqoritmindən istifadə etməklə iki müxtəlif dekodlaşdırma üsulu vermək olar. Onlardan birini növbəti fəsildə şərh edəcəyik. O biri üsulu isə indi şərh edək.

Tutaq ki, $S(x)$ sindromlar çoxhədlisi, $\Lambda(x)$ səhvlərin lokatoru çoxhədlisidir. Bu çoxhədlilər aşağıdakı kimi təyin olunurlar:

$$S(x) = \sum_{j=1}^{2t} S_j x^{j-1}, \quad \Lambda(x) = \prod_{j=1}^{\nu} (1 - xX_j). \quad (5)$$

Səhvlərin qiymətləri çoxhədlisi $\Omega(x)$ çoxhədlisidir və o aşağıdakı kimi təyin olunur:

$$\Omega(x) = S(x)\Lambda(x) \pmod{x^{2t}}. \quad (6)$$

(5) və (6)-da nəzərdə tutulur ki, $\deg \Lambda(x) \le t$ və $\deg \Omega(x) \le t-1$. Evklid alqoritminin isbatını (6) tənliyinin $\Lambda(x)$ və $\Omega(x)$-lara nəzərən həll edilməsində istifadə etməyə çalışaq. Həmin isbatdan asanlıqla müəyyən etmək olar ki,

$$\begin{pmatrix} s^{(r)}(x) \\ t^{(r)}(x) \end{pmatrix} = \begin{pmatrix} A_{11}^{(r)}(x) & A_{12}^{(r)}(x) \\ -A_{21}^{(r)}(x) & A_{22}^{(r)}(x) \end{pmatrix} \cdot \begin{pmatrix} s(x) \\ t(x) \end{pmatrix}$$

və ona görə də

$$t^{(r)}(x) = t(x) A_{22}^{(r)}(x) \pmod{s(x)}. \qquad (7)$$

Əgər $t(x) = S(x)$ və $s(x) = x^{2t}$ qəbul etsək, onda (7) bərabərliyinə tənlik kimi baxmaq olar və bu tənliyin həll edilməsi lazım gələr. Bu tənlik hər bir r üçün nəzərdə tutulur. Qoyulan məsələni həll etmək üçün elə r qiymətini (əgər o mövcuddursa) tapmaq lazımdır ki, bu qiymət halında $\deg A_{22}^{(r)}(x) \le t$ və $\deg t^{(r)}(x) \le t-1$. Sonuncu şərtin ödənməsi üçün r'-i elə r qiymətinə bərabər götürmək lazımdır ki, bu r üçün

$$\deg t^{(r-1)}(x) \ge t \text{ və } \deg t^{(r)}(x) \le t-1$$

olsun. $\deg t^{(0)}(x) = 2t$ və r artdıqca $t^{(r)}(x)$-ın dərəcəsi ciddi azaldığından bu bərabərsizliklər r' üçün yeganə qiymət təyin edir.

r'-in təyininə görə alırıq:

$$\deg t^{(r')}(x) \le t-1.$$

r artdıqca $A_{22}^{(r)}(x)$ çoxhədlisinin dərəcəsi artır. Ancaq o qalır ki, göstərək ki,

$$\deg A_{22}^{(r')}(x) \le t.$$

Bu bərabərsizlik $A(x)$ matrisinin tərsinin hesablanması ilə isbat olunur. Qeyd edək ki,

$$A^{(r')}(x)=\prod_{r=r'-1}^{0}\begin{pmatrix}0 & 1\\ 1 & -Q^{(r)}(x)\end{pmatrix}.$$

Buradan da alınır ki, $\deg A_{22}^{(r)}(x)\geq \deg A_{12}^{(r)}(x)$. Həm də qeyd edək ki, $\deg s^{(r)}(x)>\deg t^{(r)}(x)$. Bu bərabərsizliklərdən və

$$\begin{pmatrix}s(x)\\ t(x)\end{pmatrix}=(-1)^{r'}\begin{pmatrix}A_{22}^{(r')}(x) & -A_{12}^{(r')}(x)\\ -A_{21}^{(r')}(x) & A_{11}^{(r')}(x)\end{pmatrix}\cdot\begin{pmatrix}s^{(r')}(x)\\ t^{(r')}(x)\end{pmatrix}$$

matris bərabərliyindən çıxır ki,

$$\deg s(x)=\deg A_{22}^{(r')}(x)+\deg s^{(r')}(x).$$

Onda $s^{(r')}(x)=t^{(r'-1)}(x)$ olduğundan alırıq ki,

$$\deg A_{22}^{(r')}(x)=\deg s(x)-\deg t^{(r'-1)}(x)\leq 2t-t=t,$$

harada ki, bu münasibətdə bərabərsizlik r'-in təyinindən alınır.

Beləliklə, aşağıdakı teoremi isbat etdik:

Teorem 2. Tutaq ki, $A^{(0)}(x)=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$, $s^{(0)}(x)=x^{2t}$, $t^{(0)}(x)=S(x)$, harada ki, $S(x)$ çoxhədlisi t sayda səhvi düzəldən BÇX kodunun sindrom çoxhədlisidir. Tutaq ki, $s^{(r)}(x), t^{(r)}(x)$ və

$$A^{(r)}(x)=\begin{pmatrix}A_{11}^{(r)}(x) & A_{12}^{(r)}(x)\\ A_{21}^{(r)}(x) & A_{22}^{(r)}(x)\end{pmatrix}$$

aşağıdakı rekurrent tənliklərin həllidir.

$$Q^{(r)}(x)=\left\lfloor\frac{s^{(r)}(x)}{t^{(r)}(x)}\right\rfloor, \qquad (8)$$

$$A^{(r+1)}(x)=\begin{pmatrix}0 & 1\\ 1 & -Q^{(r)}(x)\end{pmatrix}A^{(r)}(x), \qquad (9)$$

$$\begin{pmatrix}s^{(r+1)}(x)\\ t^{(r+1)}(x)\end{pmatrix}=\begin{pmatrix}0 & 1\\ 1 & -Q^{(r)}(x)\end{pmatrix}\cdot\begin{pmatrix}s^{(r)}(x)\\ t^{(r)}(x)\end{pmatrix}. \qquad (10)$$

Tutaq ki, r' elədir ki, $t^{(r')}(x)\le t-1$. Onda $\Omega(x)=\Delta^{-1}t^{(r')}(x)$, $\Lambda(x)=\Delta^{-1}A_{22}^{(r')}(x)$ (harada ki, $\Delta=A_{22}^{(r')}(0)$) çoxhədliləri (6) tənliyinin $\deg\Lambda(x)\le t,\ \Lambda_0=1$ və $\deg\Omega(x)<t-1$ şərtlərini ödəyən yeganə həllidir.

İsbatı. Δ-ya bölmək $\Lambda_0=1$ bərabərliyini təmin edir. Digər tərəfdən əvvəlki mühakimələrdən alınır ki, (6) tənliyi və bütün şərtlər ödənir. Alınan həllin yeganəliyi t səhvi düzəldən BÇX kodunun sindromu üçün ancaq yeganə belə bir həllin mövcud olması faktından alınır. □

$\Lambda(x)$ və $\Omega(x)$ tapılan kimi dekodlaşdırmanı Berlekemp-Messi alqoritmi üçün təklif olunan istənilən üsulla yekunlaşdırmaq olar. Uyğun dekoderin alqoritminin blok-sxemi şəkil 1-də verilir. Bu blok-sxemdə dekoder öz işini Forni alqoritmi ilə yekunlaşdırır. Aydındır ki, yekunlaşdırmada başqa üsullar da istifadə oluna bilər.

Nümunə 1. $t=3$ səhvi düzəldə bilən (15,5) – BÇX koduna baxaq. Bu kodun əmələgətirici çoxhədlisi

$$g(x)=x^{10}+x^8+x^5+x^4+x^2+x+1$$

çoxhədlisidir. $\upsilon(x)=x^{10}+x^8+x^6+x^4+1$ çoxhədlisi qəbul edildiyi halda ötürülən $c(x)$ kod çoxhədlisini tapmalı.

Əvvəlcə sindrom komponentlərini hesablayaq:

$$S_1 = \upsilon(\alpha) = \alpha^{10} + \alpha^8 + \alpha^6 + \alpha^4 + 1 = \alpha^6,$$

$$S_2 = \upsilon(\alpha^2) = \alpha^{20} + \alpha^{16} + \alpha^{12} + \alpha^8 + 1 = \alpha^5 + \alpha + \alpha^{12} + \alpha^8 + 1 = \alpha^{12},$$

$$S_3 = \upsilon(\alpha^3) = \alpha^{30} + \alpha^{24} + \alpha^{18} + \alpha^{12} + 1 = 1 + \alpha^9 + \alpha^3 + \alpha^{12} + 1 = \alpha^{13},$$

$$S_4 = \upsilon(\alpha^4) = \alpha^{40} + \alpha^{32} + \alpha^{24} + \alpha^{16} + 1 = \alpha^{10} + \alpha^2 + \alpha^9 + \alpha + 1 = \alpha^9,$$

$$S_5 = \upsilon(\alpha^5) = \alpha^{50} + \alpha^{40} + \alpha^{30} + \alpha^{20} + 1 = \alpha^5 + \alpha^{10} + 1 + \alpha^5 + 1 = \alpha^{10},$$

$$S_6 = \upsilon(\alpha^6) = \alpha^{60} + \alpha^{48} + \alpha^{36} + \alpha^{24} + 1 = 1 + \alpha^3 + \alpha^6 + \alpha^9 + 1 = \alpha^{11}.$$

Beləliklə, sindrom çoxhədlisi aşağıdakı çoxhədlidir:

$$S(x) = \alpha^{11}x^5 + \alpha^{10}x^4 + \alpha^9 x^3 + \alpha^{13}x^2 + \alpha^{12}x + \alpha^6.$$

Teorem 2-dən istifadə etməklə $\Omega(x)$ və $\Lambda(x)$ çoxhədlilərini tapaq.

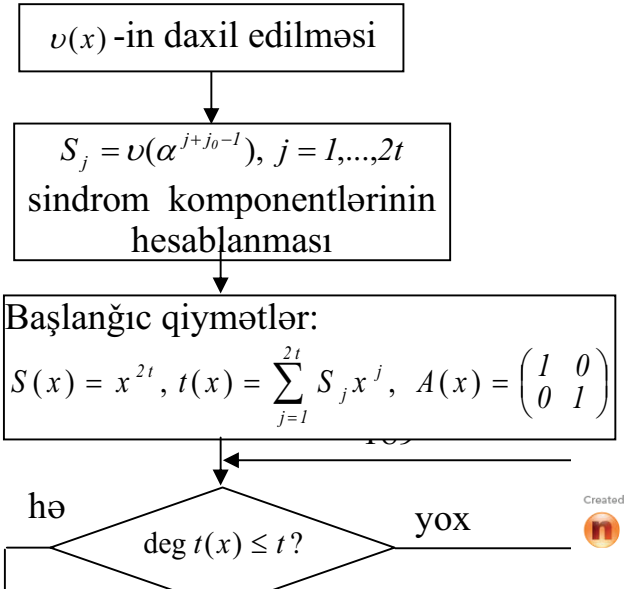
Başlanğıc qiymətlər: $A^{(0)}(x)$ iki tərtibli vahid matrisdir,

$$s^{(0)}(x) = x^6, \quad t^{(0)}(x) = \alpha^6 + \alpha^{12}x + \alpha^{13}x^2 + \alpha^9 x^3 + \alpha^{10}x^4 + \alpha^{11}x^5.$$

$r = 1$ *halı*: (8)-(10) düsturları üzrə hesablama aparaq:

$$Q^{(0)}(x) = \left\lfloor \frac{s^{(0)}(x)}{t^{(0)}(x)} \right\rfloor = \alpha^4 x + \alpha^3,$$

$$A^{(1)}(x) = \begin{pmatrix} 0 & 1 \\ 1 & \alpha^4 x + \alpha^3 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & \alpha^4 x + \alpha^3 \end{pmatrix}.$$



Şəkil 1.

$$\begin{pmatrix} s^{(1)}(x) \\ t^{(1)}(x) \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & \alpha^4 x + \alpha^3 \end{pmatrix} \cdot \begin{pmatrix} x^6 \\ \alpha^{11}x^5 + \alpha^{10}x^4 + \alpha^9 x^3 + \alpha^{13}x^2 + \alpha^{12}x + \alpha^6 \end{pmatrix} =$$

$$= \begin{pmatrix} \alpha^{11}x^5 + \alpha^{10}x^4 + \alpha^9 x^3 + \alpha^{13}x^2 + \alpha^{12}x + \alpha^6 \\ \alpha^7 x^3 + \alpha^5 x + \alpha^9 \end{pmatrix}.$$

$r = 2$ *halı*:

$$Q^{(1)}(x) = \left\lfloor \frac{s^{(1)}(x)}{t^{(1)}(x)} \right\rfloor = \alpha^4 x^2 + \alpha^3 x,$$

$$A^{(2)}(x) = \begin{pmatrix} 0 & 1 \\ 1 & \alpha^4 x^2 + \alpha^3 x \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & \alpha^4 x + \alpha^3 \end{pmatrix} =$$

$$= \begin{pmatrix} 1 & \alpha^4 x + \alpha^3 \\ \alpha^4 x^2 + \alpha^3 x & \alpha^8 x^3 + \alpha^6 x + 1 \end{pmatrix},$$

$$\begin{pmatrix} s^{(2)}(x) \\ t^{(2)}(x) \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & \alpha^4 x^2 + \alpha^3 x \end{pmatrix} \times$$

$$\times \begin{pmatrix} \alpha^{11}x^5 + \alpha^{10}x^4 + \alpha^9 x^3 + \alpha^{13}x^2 + \alpha^{12}x + \alpha^6 \\ \alpha^7 x^3 + \alpha^5 x + \alpha^9 \end{pmatrix} =$$

$$= \begin{pmatrix} \alpha^7 x^3 + \alpha^5 x + \alpha^9 \\ \alpha^8 x^2 + \alpha^6 \end{pmatrix}.$$

Qeyd edək ki, $\deg t^{(2)}(x) \le 2$. Onda teorem 2-yə görə

$$\Omega(x) = \Delta^{-1} t^{(2)}(x) = \alpha^8 x^2 + \alpha^6$$

və

$$\Lambda(x) = \Delta^{-1} A_{22}^{(2)}(x) = \alpha^8 x^3 + \alpha^6 x + 1,$$

harada ki, $\Delta^{-1} = 1$,

$$\Omega(x) = S(x)\Lambda(x) \pmod{x^6}$$

tənliyinin $\deg \Lambda(x) \le 3$, $\Lambda_0 = 1$ və $\deg \Omega(x) \le 2$ şərtlərini ödəyən yeganə həlləridir. $\Lambda(x) = \alpha^8 x^3 + \alpha^6 x + 1$ lokatorlar çoxhədlisinin

köklərini axtaraq. Bilavasitə yoxlamaqla alarıq ki, $x_1 = \alpha^4$, $x_2 = \alpha^6$, $x_3 = \alpha^{12}$ və ya $X_1 = \alpha^{11}$, $X_2 = \alpha^9$, $X_3 = \alpha^3$. Buradan da $e(x) = x^{11} + x^9 + x^3$ olar. Deməli, ötürülən kod çoxhədlisi

$$c(x) = \upsilon(x) + e(x) = x^{11} + x^{10} + x^9 + x^8 + x^6 + x^4 + x^3 + 1$$

çoxhədlisidir.

Nümunə 2. Tutaq ki, nümunə 1-də verilən koda baxırıq. $\upsilon(x) = x^4 + x^2 + x + 1$ kod çoxhədlisi qəbul olunduqda ötürülən $c(x)$ kod çoxhədlisini tapmalı.

Əvvəlcə sindrom komponentlərini hesablayaq:

$$S_1 = \upsilon(\alpha) = \alpha^4 + \alpha^2 + \alpha + 1 = \alpha^2,$$
$$S_2 = \upsilon(\alpha^2) = \alpha^8 + \alpha^4 + \alpha^2 + 1 = \alpha^4,$$
$$S_3 = \upsilon(\alpha^3) = \alpha^{12} + \alpha^6 + \alpha^3 + 1 = \alpha^9,$$
$$S_4 = \upsilon(\alpha^4) = \alpha + \alpha^8 + \alpha^4 + 1 = \alpha^8,$$
$$S_5 = \upsilon(\alpha^5) = \alpha^5 + \alpha^{10} + \alpha^5 + 1 = \alpha^5,$$
$$S_6 = \upsilon(\alpha^6) = \alpha^9 + \alpha^{12} + \alpha^6 + 1 = \alpha^3.$$

Beləliklə, sindrom çoxhədlisi aşağıdakı çoxhədli olar:

$$S(x) = \alpha^2 + \alpha^4 x + \alpha^9 x^2 + \alpha^8 x^3 + \alpha^5 x^4 + \alpha^3 x^5.$$

$\Lambda(x)$ səhvlərin lokatoru çoxhədlisi və $\Omega(x)$ səhvlərin qiymətləri çoxhədlisi aşağıdakı tənlikdən tapılır:

$$\Omega(x) = S(x)\Lambda(x) \pmod{x^6}. \qquad (11)$$

$\Lambda(x)$ və $\Omega(x)$ çoxhədlisini tapmaq üçün teorem 2-dən istifadə edək:

Başlanğıc qiymətlər: $A^{(0)}(x)$ iki tərtibli vahid matrisdir,

$s^{(0)}(x) = x^6$, $t^{(0)} = \alpha^2 + \alpha^4 x + \alpha^9 x^2 + \alpha^8 x^3 + \alpha^5 x^4 + \alpha^3 x^5$.

$r = 1$ *halı*:

$$Q^{(0)}(x) = \left\lfloor \frac{s^{(0)}(x)}{t^{(0)}(x)} \right\rfloor = \alpha^{12} x + \alpha^{14},$$

$$\Lambda^{(1)}(x) = \begin{pmatrix} 0 & 1 \\ 1 & \alpha^{12} x + \alpha^{14} \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & \alpha^{12} x + \alpha^{14} \end{pmatrix},$$

$$\begin{pmatrix} s^{(1)}(x) \\ t^{(1)}(x) \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & \alpha^{12}x+\alpha^{14} \end{pmatrix} \cdot \begin{pmatrix} x^6 \\ \alpha^3x^5+\alpha^5x^4+\alpha^8x^3+\alpha^9x^2+\alpha^4x+\alpha^2 \end{pmatrix} =$$

$$= \begin{pmatrix} \alpha^3x^5+\alpha^5x^4+\alpha^8x^3+\alpha^9x^2+\alpha^4x+\alpha^2 \\ \alpha^8x^4+\alpha^{10}x^3+\alpha^{10}x^2+x+\alpha \end{pmatrix}.$$

$r=2$ *halı*:

$$Q^{(1)}(x) = \left\lfloor \frac{s^{(1)}(x)}{t^{(1)}(x)} \right\rfloor = \alpha^{10}x,$$

$$A^{(2)}(x) = \begin{pmatrix} 0 & 1 \\ 1 & \alpha^{10}x \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & \alpha^{12}x+\alpha^{14} \end{pmatrix} = \begin{pmatrix} 1 & \alpha^{12}x+\alpha^{14} \\ \alpha^{10}x & \alpha^7x^2+\alpha^9x+1 \end{pmatrix},$$

$$\begin{pmatrix} s^{(2)}(x) \\ t^{(2)}(x) \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & \alpha^{10}x \end{pmatrix} \cdot \begin{pmatrix} \alpha^3x^5+\alpha^5x^4+\alpha^8x^3+\alpha^9x^2+\alpha^4x+\alpha^2 \\ \alpha^8x+\alpha^{10}x^3+\alpha^{10}x^2+x+\alpha \end{pmatrix} =$$

$$= \begin{pmatrix} \alpha^8x^4+\alpha^{10}x^3+\alpha^{10}x^2+x+\alpha \\ \alpha^4x^3+\alpha^{13}x^2+\alpha^{13}x+\alpha^2 \end{pmatrix}.$$

$r=3$ *halı*:

$$Q^{(2)}(x) = \left\lfloor \frac{s^{(2)}(x)}{t^{(2)}(x)} \right\rfloor = \alpha^4x+\alpha^7,$$

$$A^{(3)}(x) = \begin{pmatrix} 0 & 1 \\ 1 & \alpha^4x+\alpha^7 \end{pmatrix} \cdot \begin{pmatrix} 0 & \alpha^{12}x+\alpha^{14} \\ \alpha^{10}x & \alpha^7x^2+\alpha^9x+1 \end{pmatrix} =$$

$$= \begin{pmatrix} \alpha^{10}x & \alpha^7x^2+\alpha^9x+1 \\ \alpha^{14}x^2+\alpha^2x & \alpha^{11}x^3+\alpha^2x^2+\alpha^{11}x+\alpha \end{pmatrix},$$

$$\begin{pmatrix} s^{(3)}(x) \\ t^{(3)}(x) \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & \alpha^4 x + \alpha^7 \end{pmatrix} \cdot \begin{pmatrix} \alpha^8 x^4 + \alpha^{10} x^3 + \alpha^{10} x^2 + x + \alpha \\ \alpha^4 x^3 + \alpha^{13} x^2 + \alpha^{13} x + \alpha^2 \end{pmatrix} =$$

$$= \begin{pmatrix} \alpha^4 x^3 + \alpha^{13} x^2 + \alpha^{13} x + \alpha^2 \\ \alpha^{13} x^3 + \alpha^8 x^2 + \alpha^7 x + \alpha^3 \end{pmatrix}.$$

$r = 4$ *halı*:

$$Q^{(3)}(x) = \left\lfloor \frac{s^{(3)}(x)}{t^{(3)}(x)} \right\rfloor = \alpha^6,$$

$$A^{(4)}(x) = \begin{pmatrix} 0 & 1 \\ 1 & \alpha^6 \end{pmatrix} \cdot \begin{pmatrix} \alpha^{10} x & \alpha^7 x^2 + \alpha^9 x + 1 \\ \alpha^{14} x^2 + \alpha^2 x & \alpha^{11} x^3 + \alpha^2 x^2 + \alpha^{11} x + \alpha \end{pmatrix} =$$

$$= \begin{pmatrix} \alpha^{14} x^2 + \alpha^2 x & \alpha^{11} x^3 + \alpha^2 x^2 + \alpha^{11} x + \alpha \\ \alpha^5 x^2 + \alpha x & \alpha^2 x^3 + \alpha^{11} x^2 + \alpha^{11} x + \alpha^9 \end{pmatrix}.$$

$$\begin{pmatrix} S^{(4)}(x) \\ t^{(4)}(x) \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & \alpha^6 \end{pmatrix} \cdot \begin{pmatrix} \alpha^4 x^3 + \alpha^{13} x^2 + \alpha^{13} x + \alpha^2 \\ \alpha^{13} x^3 + \alpha^8 x^2 + \alpha^4 x + \alpha^3 \end{pmatrix} =$$

$$= \begin{pmatrix} \alpha^{13} x^3 + \alpha^8 x^2 + \alpha^7 x + \alpha^3 \\ \alpha^2 x^2 + \alpha^{11} \end{pmatrix}.$$

Qeyd edək ki, $t^{(4)}(x) \le 2$. Onda teorem 2-yə görə

$$\Omega(x) = \Delta^{-1} t^{(4)}(x) = \alpha^8 x^2 + \alpha^2$$

və

$$\Lambda(x) = \Delta^{-1} A_{22}^{(4)}(x) = \alpha^8 x^3 + \alpha^2 x^2 + \alpha^2 x + 1$$

çoxhədliləri (11) tənliyinin $\deg \Lambda(x) \le 3$, $\Lambda_0 = 1$ və $\deg \Omega(x) \le 2$ şərtlərini ödəyən yeganə həlləridir. Burada $\Delta^{-1} = \alpha^6$-dır, belə ki, $\Delta = A_{22}^{(4)}(0) = \alpha^9$.

İndi isə tapılan $\Lambda(x) = \alpha^8 x^3 + \alpha^2 x^2 + \alpha^2 x + 1$ çoxhədlisinin köklərini axtaraq. Bilavasitə yoxlamaqla alarıq: $x_1 = \alpha^5$, $x_2 = \alpha^7$, $x_3 = \alpha^{10}$. Buradan da alınır ki, $X_1 = \alpha^{10}, X_2 = \alpha^8$, $X_3 = \alpha^5$. Beləliklə, $e(x) = x^{10} + x^8 + \alpha^5$ və

$$c(x) = \upsilon(x) + e(x) = x^{10} + x^8 + x^5 + x^4 + x^2 + x + 1$$

ötürülən kod çoxhədlisidir.

YOXLAMA TAPŞIRIQLARI

Tapşırıq 1. $n = 3^3 - 1 = 26$ uzunluğuna malik, $t = 2$ sayda səhvi düzəltməyə imkan verən və informasiya sözündən $g(x) = x^9 + 2x^8 + x^7 + x^6 + x^5 + 2x^4 + 2x^3 + 2x^2 + x + 1$ əmələgətirici çoxhədlisi vasitəsilə qurulan $GF(3^3)$ meydanı üzərində BÇX - kodları halında qəbul edilən kod sözü aşağıdakı $\upsilon(x)$ çoxhədlisi olduqda ötürülən kod sözünü, səhv sözünü və informasiya sözünü tapmalı:

1) $\upsilon(x) = 2x^{10} + 2x^7 + 2x^6 + x^3 + 2x + 1$;
2) $\upsilon(x) = x^{10} + x^9 + 2x^8 + 2x^2$;
3) $\upsilon(x) = x^{11} + 2x^{10} + x^9 + x^8 + 2x^6 + 2x^5 + x^3 + x^2$;
4) $\upsilon(x) = x^{11} + x^8 + x^6 + 2x^5 + 2x^4 + 2x^3 + x^2 + 2x + 1$;
5) $\upsilon(x) = 2x^{10} + 2x^8 + 2x^6 + x^5 + 2x^3 + 2x^2 + 2x + 2$;
6) $\upsilon(x) = x^{12} + x^8 + 2x^7 + 2x^6 + 2x^5 + 2x^4 + x + 1$;

7) FƏSİL VI. SPEKTRAL ÜSULLARA ƏSASLANAN KODLAR

§1. Qalua meydanlarında Furye çevirmələri

Kompleks ədədlər meydanında kompleks komponentli $p = (p_0, p_1, ..., p_{N-1})$ vektorunun diskret Furye çevirməsi komponentləri aşağıdakı münasibətlə təyin olunan $P = (P_0, P_1, ..., P_{N-1})$ vektoru kimi təyin olunur:

$$P_k = \sum_{i=0}^{N-1} e^{-\frac{2\pi j}{N} ik} p_i, \ k = 0,1,...,N-1,$$

harada ki, $j = \sqrt{-1}$. Aydındır ki, bu çevirmənin nüvəsi olan $\exp\left(-\frac{2\pi j}{N}\right)$ kompleks ədədlər meydanında vahidin N-ci dərəcədən kökünə bərabərdir. $GF(q^m)$ sonlu meydanında n tərtibinə malik α elementi vahidin n-ci tərtibdən kökü olur. Beləliklə, α və $\exp\left(-\frac{2\pi j}{N}\right)$ arasında oxşarlığı nəzərə almaqla aşağıdakı tərifi vermək olar.

Tərif 1. Tutaq ki, $\upsilon = (\upsilon_0, \upsilon_1, ..., \upsilon_{n-1})$ vektoru $GF(q)$ üzərində vektordur və n ədədi hər hansı bir m üçün $(q^m - 1)$-i bölür. Tutaq ki, α elementi $GF(q^m)$ meydanının n tərtibli elementidir. υ vektorunun Qalua meydanı üzərində Furye çevirməsi aşağıdakı düsturla verilən $V = (V_0, V_1, ..., V_{n-1})$ vektoru kimi təyin olunur:

$$V_j = \sum_{i=0}^{n-1} \alpha^{ij} \upsilon_i, \ j = 0,1,...,n-1 \ .$$

i diskret indeksi zaman indeksi, υ - zaman funksiyası və ya siqnal adlandırmaq olar. Analoji olaraq j-ni tezlik, V-ni isə tezlik funksiyası və ya spektr adlandırmaq olar.

Furye çevirməsinin uzunluğu kimi $(q^m - 1)$ ədədinin ixtiyari bölənini götürmək olar. Ən böyük əhəmiyyətə malik $n = (q^m - 1)$ primitiv

uzunluğudur. Bu halda α elementi $GF(q^m)$ meydanının primitiv elementi olur. Kompleks ədədlər meydanından fərqli olaraq sonlu Qalua meydanlarında diskret Furye çevirməsi heç də bütün n ədədləri halında mövcud olmaya bilər. Çünki istənilən n üçün bu meydanda n tərtibinə malik olan element olmaya da bilər. Əgər ən kiçik tam m ədədi eladirsə ki, n ədədi $(q^m - 1)$-in bölənidir, onda $GF(q)$ meydanı üzərində n uzunluğuna malik diskret Furye çevirməsi mövcuddur və bu çevirmənin komponentləri $GF(q^m)$ meydanında yerləşir. Təəssüf ki, bəzi n-lər üçün Furye çevirməsi mümkün olmasına baxmayaraq çevirmənin komponentləri çox böyük Qalua meydanında yerləşməsi üzündən praktik tətbiqlri çox səmərəsiz olur.

Həqiqi qiymətli p zaman funksiyasının diskret Furye çevirməsi olan P spektri kompleks ədəd olur. Analoji olaraq $GF(q)$ meydanından olan υ zaman funksiyasının çevirməsi olan V spektri $GF(q^m)$ meydanında yerləşir.

Teorem 1. p xarakteristikasına malik $GF(q)$ meydanı üzərində vektor və onun spektri arasında aşağıdakı münasibət doğrudur:

$$V_j = \sum_{i=0}^{n-1} \alpha^{ij} \upsilon_i \,,\ \upsilon_i = \frac{1}{n} \sum_{j=0}^{n-1} \alpha^{-ij} V_j \,, \qquad (1)$$

harada ki, n meydanın ədədi kimi interpretasiya olunur, yəni mod p üzrə göstərilir.

İsbatı. İstənilən meydanda

$$x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + \ldots + x + 1)$$

olur. α elementinin təyininə görə istənilən r üçün α^r elementi sol tərəfdəki çoxhədlinin köküdür. Beləliklə, p modulu üzrə istənilən $r \neq 0$ üçün α^r elementi $x^{n-1} + x^{n-2} + \ldots + x + 1$ çoxhədlisinin köküdür. Bu aşğıdakına ekvivalentdir:

$$\sum_{j=0}^{n-1} \alpha^{rj} = 0,\ r \neq 0 \ (\mathrm{mod} n) \,.$$

Əgər $r = 0 \ (\mathrm{mod}\ n)$ olarsa, onda

$$\sum_{j=0}^{n-1}\alpha^{rj}=n \pmod p$$

və bu da n ədədi p-in misillərinə bərabər olmazsa həmişə sıfırdan fərqlidir. Bu bərabərlikləri birləşdirsək alarıq:

$$\sum_{j=0}^{n-1}\alpha^{-ij}\sum_{k=0}^{n-1}\alpha^{kj}\upsilon_k=\sum_{k=0}^{n-1}\upsilon_k\sum_{j=0}^{n-1}\alpha^{(k-i)j}=(n \bmod p)\cdot\upsilon_i$$

Nəhayət, $q^m-1=p^M-1$ ədədi n-in mislidir və ona görə də n p-in misli deyildir. Beləliklə, $n\neq 0 \pmod p$. □

Qeyd edək ki, (1) münasibətlərinin birincisi düz, ikincisi isə tərs Furye çevirməsinin təyini düsturudur.

Furye çevirməsinin çoxlu xassələri mövcuddur və bu da sonlu meydanlar halında da doğrudur.

Teorem 2 (bağlama haqqında teorem). Tutaq ki,

$$e_i=f_i\cdot g_i,\ i=0,...,n-1.$$

Onda

$$E_j=(1/n)\sum_{k=0}^{n-1}F_{((j-k))}G_k,\ \ j=0,...,n-1,$$

harada ki, burada ikiqat mötərizə onu göstərir ki, indeks $\bmod n$ hesabı üzrə hesablanır.

İsbatı. $e_i=f_i\cdot g_i$ - komponentli vektorun Furye çevirməsini hesablayaq:

$$E_j=\sum_{i=0}^{n-1}\alpha^{ij}f_i\left((1/n)\cdot\sum_{k=0}^{n-1}\alpha^{-ik}G_k\right)=$$

$$=(1/n)\sum_{k=0}^{n-1}G_k\left(\sum_{i=0}^{n-1}\alpha^{i(j-k)}f_i\right)=(1/n)\sum_{k=0}^{n-1}G_kF_{((j-k))}.$$

□

Qeyd edək ki,

$$E_j=\sum_{i=0}^{n-1}\alpha^{ij}f_ig_i=(1/n)\sum_{k=0}^{n-1}F_{((j-k))}G_k$$

bağlanmasında $j = 0$ seçilməsi Parseval tipli aşağıdakı bərabərliyə gətirib çıxarır:

$$\sum_{i=0}^{n-1} f_i g_i = (1/n)\sum_{k=0}^{n-1} F_{((n-k))} G_k \ .$$

Teorem 3 (Sürüşmənin xassəsi). Əgər $\{\upsilon_i\} \leftrightarrow \{V_j\}$ Furye çevirmələri cütlükləri isə, onda $\{\alpha^i \upsilon_i\} \leftrightarrow \{V_{((j+l))}\}$ və $\{\upsilon_{((i-l))}\} \leftrightarrow \{\alpha^j V_j\}$ cütlükləri də Furye çevirmələri cütlükləridir.

Bu teoremin isbatını düz Furye çevirməsinin düsturunda υ_i əvəzinə $\alpha^i \upsilon_i$, tərs Furye çevirməsinin düsturunda isə V_j əvəzinə $\alpha^j V_j$ götürməklə bilavasitə aparmaq olar.

Tutaq ki, υ vektoru $\upsilon(x)$ çoxhədlisi ilə verilir. Qalua meydanı üzərində Furye çevirməsi vasitəsilə

$$\upsilon(x) = \upsilon_{n-1} x^{n-1} + \ldots + \upsilon_1 x + \upsilon_0$$

çoxhədlisi

$$V(x) = V_{n-1} x^{n-1} + \ldots + V_1 x + V_0$$

çoxhədlisinə çevrilə bilər. $V(x)$ çoxhədlisi spektral çoxhədli yaxud $\upsilon(x)$ ilə assosirə olunmuş çoxhədli adlanır.

Teorem 4. Aşağıdakı hömlər doğrudur:

1) α^j elementinin $\upsilon(x)$ çoxhədlisinin kökü olması üçün zəruri və kafi şərt, j-ci V_j tezlik komponentinin sıfra bərabər olmasıdır;

2) α^{-i} elementinin $V(x)$ çoxhədlisinin kökü olması üçün zəruri və kafi şərt, i-ci υ_i zaman komponentinin sıfra bərabər omasıdır.

İsbatı. 1) Bu hökmün isbatı aydındır, belə ki,

$$\upsilon(\alpha^j) = \sum_{i=0}^{n} \upsilon_i \alpha^{ij} = V_j \ .$$

2) Bu hökmü də analoji qaydada isbat etmək olar. □

§2. Qoşmalığa məhdudiyyətlər və idempotentlər

$GF(q)$ üzərində olan n uzunluqlu Furye çevirməsi genişlənmiş $GF(q^m)$ meydanında qiymətlər alır. Əgər biz $GF(q^m)$ meydanı üzərində olan ixtiyari n - ölçülü vektoru götürüb onun tərs Furye çevirməsini hesablasaq, onda ümumi halda $GF(q)$ üzərində olan zaman vektorlarını ala bilmirik, çünki böyük meydandan olan komponentlərin alınması mümkündür. Odur ki, spektr üzərinə qoyulacaq elə məhdudiyyət şərtləri tapmaq lazımdır ki, bu məhdudiyyətlər halında zaman vektorunun komponentlərinin $GF(q)$ meydanında olması təmin olunsun.

Belə məhdudiyyət şərtləri kompleks ədədlər meydanından tanışdır. Qeyd edək ki, kompleks ədədlər meydanında $P(f)$ spektrinin həqiqi tərs Furye çevirməsinə malik olması üçün zəruri və kafi şərt, $P^*(-f) = P(f)$ olmasıdır. Aşağıdakı teorem qoşmalığa məhdudiyyətlər adlanan məhdudiyyətlər çoxluğunu təsvir edir və sonlu meydan üçün analoji şərtləri təyin edir.

Teorem 1. Tutaq ki, V vektoru komponentləri $GF(q^m)$-dən olan n-ölçülü vektordur. Onda onun tərs Furye çevirməsi olan υ vektorunun $GF(q)$-dən olan komponentlərə malik vektor olması üçün zəruri və kafi şərt aşağıdakı bərabərliklərin ödənməsidir:

$$V_j^q = V_{((qj))},\ j = 0,1,...,n-1.$$

İsbatı. Zərurilik. Təyinə görə

$$V_j = \sum_{i=0}^{n-1} \alpha^{ij} \upsilon_i,\ j = 0,1,...,n-1.$$

p xarakteristikalı meydanda istənilən tam r üçün $(a+b)^{p^r} = a^{p^r} + b^{p^r}$ bərabərliyi doğrudur. Əgər υ_i elementi $GF(q)$ meydanının elementidirsə, onda istənilən i üçün $\upsilon_i^q = \upsilon_i$. Beləliklə,

$$V_j^q = (\sum_{i=0}^{n-1} \alpha^{ij} \upsilon_i)^q = \sum_{i=0}^{n-1} \alpha^{qij} \upsilon_i^q = \sum_{i=0}^{n-1} \alpha^{qij} \upsilon_i = V_{((qi))}.$$

Kafilik. Fərz edək ki, hər bir j üçün $V_j^q = V_{((qj))}$. Onda

$$\sum_{i=0}^{n-1} \alpha^{iqj} \upsilon_i^q = \sum_{i=0}^{n-1} \alpha^{iqj} \upsilon_i,\ j = 0,...,n-1.$$

Tutaq ki, $k = qj$ ödənir. q ədədi $n = q^m - 1$ ədədi ilə qarşılıqlı sadə olduğundan j kəmiyyəti 0 -dan $(n-1)$ -ə kimi qiymətlər aldıqda k kəmiyyəti də 0 -dan $(n-1)$ -ə kimi qiymətlər alır. Uyğun olaraq,

$$\sum_{i=0}^{n-1} \alpha^{ik} \upsilon_i^q = \sum_{i=0}^{n-1} \alpha^{ik} \upsilon^i, \; k = 0,...,n-1,$$

və Furye çevirməsi qarşılıqlı birqiymətli olduğundan hər bir i üçün $\upsilon_i^q = \upsilon_i$. Beləliklə, υ_i istənilən i üçün $x^q - x$ çoxhədlisinin köküdür və bu köklər vasitəsilə $GF(q)$ meydanın bütün elementləri nəzərdə tutulur. □

İsbat olunan teoremi tətbiq etmək üçün mod n üzrə ədədləri qoşma elementlər sinifləri adı altında məlum olan alt çoxluqlara bölək:

$$A_j = \{j, jq, ..., jq^{m_j - 1}\},$$

harada ki, m_j ədədi $jq^{m_j} = j \pmod{n}$ şərtini ödəyən ən kiçik müsbət tam ədəddir. Meydan sonlu olduğuna görə belə m_j həmişə mövcuddur. Məsələn, $q = 2$ və $n = 7$ olduqda qoşma elementlər sinifləri aşağıdakılardır:

$$A_0 = \{0\}, \; A_1 = \{1,2,4\}, \; A_3 = \{3,6,5\}.$$

A_j qoşma elementlər sinifləri spektrlərdə tezliklər çoxluğunu ayırır. Bu çoxluqları vətərlər tezliyi adlandıraq. Teorem 1-də isbat olunur ki, əgər zaman siqnalları $GF(q)$ meydanında qiymət alırsa, onda bir vətərin tezliyində spektrin qiyməti bu vətərin bütün tezliklərində spektrin qiymətlərini təyin edir.

Şəkil 1-də bir sıra kiçik meydanlar üçün (bir qədər dəyişmiş işarələmələrlə) qoşma elementlər sinfi verilir. Alınmış simmetrikliyi nəzərə çapdırmaq üçün qoşma elementlər sinifləri mənfi tam ədədlərin istifadəsi ilə yazılır. Lazım gələrsə mənfi tam j ədədini müsbət tam $n + j$ ilə dəyişmək olar. 21 modulu üzrə qoşma elementlər sinifləri modul kimi istənilən tam ədədin götürülə bilməsini göstərmək üçün cədvələ daxil edilmişdir. Qeyd edək ki, 21 moduluna görə qoşma elementlər sinfinin hədlərini əgər 3-ə vursaq, onda bu siniflər 63 moduluna görə qoşma elementlərin siniflərinə çevrilir.

Tərif 1. $GF(q^m)$ meydanının β elementinin q-lük izi aşağıdakı kimi təyin olunan cəmə deyilir.

$$tr(\beta)=\sum_{i=0}^{m-1}\beta^{q^i}\ .$$

mod 7 üzrə	**127 modulu üzrə**
{-1,-2,3}, {0}, {1,2,-3}	{-21,-42,43,-41,45,-37,53}
15 modulu üzrə	{-19,-38,51,-25,-50,27,54}
{-1,-2,-4,7}, {0}, {1,2,4,-7}	{-13,-26,-52,23,46,-35,57}
{3,6,-3,-6},{5,-5}	{-11,-22,-44,39,-49,29,58}
31 modu üzrə	{-9,-18,-36,55,-17,-34,59}
{-5,-10,11,-9,13},{-3,-6,-12,7,14}	{-7,-14,-28,-56,15,30,60}
{-1,-2,-4,-8,15},{0}	{-5,-10,-20,-40,47,-33,61}
{1,2,4,8,-15},{3,6,12,-7,-14}	{-3,-6,-12,-24,-48,31,62}
{5,10,-11,9,-13}	{-1,-2,-4,-8,-16,-32,63}
21 modulu üzrə	{0}
{-3,-6,9},{-1,-2,-4,-8,5,10},{0}	{1,2,4,8,16,32,-63}
{1,2,4,8,-5,-10},{3,6,-9},{7,-7}	{3,6,12,24,48,-31,-62}
63 modulu üzrə	{5,10,20,40,-47,33,-61}
{-11,-22,19,-25,13,26},{-9,-18,27}	{7,14,28,56,-15,-30,-60}
{-5,-10,-20,23,-17,29},	{9,18,36,-55,17,34,-59}
{-3,-6,-12,-24,15,30}	{13,26,52,-23,-46,35,-57}
{-1,-2,-4,-8,-16,31},{0}	{11,22,44,-39,49,-29,-58}
{1,2,4,8,16,-31},{3,6,12,24,-15,-30}	{19,38,-51,25,50,-27,-54}
{5,10,20,-23,17,-29}	{21,42,-43,41,-45,37,-53}

{7,14,28,-7,-14,-28},{9,18,-27}	
{11,22,-19,25,-13,-26},{21,-21}	

Şəkil 1. Qoşma elementlər sinifləri

Aydındır ki, β elementinin q-lük izinin q-cü qüvvəti β elementinin q-lük izinə bərabərdir və, beləliklə, q-lük iz $GF(q)$ meydanının elementidir. Əgər β elementinin daxil olduğu qoşma elementlər sinfi m elementdən ibarətdirsə, onda $tr(\beta)$ bu sinfin bütün elementlərinin cəminə bərabərdir. Əks halda qoşma elementlər sinfində elementlərin sayı m-i bölür və elementlərin izə neçə dəfə daxil olması alınan nisbətə bərabərdir. İzin tərifinə və sonlu meydanın strukturu haqqında bəzi teoremlərə görə (teorem 4.6.10)

$$tr(\beta+\gamma)=tr(\beta)+tr(\gamma)$$

və buna görə də bütün qoşma elementlər eyni bir izə malikdirlər.

Teorem 2. $GF(q^m)$ meydanı üzərində q-lük iz $GF(q)$ meydanının hər bir ədədini q^m-1 dəfə öz qiyməti kimi alır.

İsbatı. Tutaq ki, γ ədədi $GF(q)$ meydanının elementidir, β isə $GF(q^m)$ meydanının elementidir və $tr(\beta)=\gamma$. Onda β elementi

$$x^{q^{m-1}}+x^{q^{m-2}}+\ldots+x^q+x-\gamma$$

çoxhədlisinin köküdür. Bu çoxhədlinin dərəcəsi q^{m-1}-dir və, beləliklə, o q^{m-1}- dən çox olmayan sayda kökə malikdir. Lakin cəmi q sayda belə çoxhədli mövcuddur və $GF(q^m)$ meydanının hər bir elementi bu çoxhədlilərdən birinin köküdür. □

Teorem 3. Tutaq ki, a elementi $GF(q^{2m})$ meydanının elementidir, $x^2+x+a=0$ kvadrat tənliyinin, $GF(q^{2m})$ meydanında kökünün mövcud olması üçün zəruri və kafi şərt bu elementin 2-lik izinin sıfra bərabər olmasıdır.

İsbatı. Zərurilik. Tutaq ki, β bu kvadrat tənliyinin köküdür. β nöqtəsində kvadrat üçhədliyə uyğun hesablanmış ikilik iz aşağıdakına bərabərdir.

$$tr(\beta^2+\beta+a)=tr(0)=0.$$

Toplamaya nəzərən iz distributivdir, β və β^2 elementlərinin izləri $GF(2)$-də eyni bir elementdir. Buradan da $tr(a)=0$ alınır.

Kafilik. Tutaq ki, hər bir β müəyyən bir a üçün x^2+x+a çoxhədlisinin köküdür və həqiqətən də bu a ədədi $-(\beta+\beta^2)$ ədədinə bərabərdir. İzin sıfra bərabər olduğu belə a elementlərinin sayı 2^{m-1}-dir. Bu isə kifayət edir ki, hər biri iki kökə malik 2^{m-1} sayda tənlik qurmaq mümkün olsun. □

Tutaq ki, A_k vətəri seçilib və aşağıdakı spektr təyin olunub:

$$W_j=\begin{cases}0, & j\in A_k,\\ 1, & j\notin A_k.\end{cases}$$

Teorem 1-ə görə bu spektr üçün tərs Furye çevirməsi $GF(q)$ üzərində vektordur və $w(x)$ çoxhədlisi ilə təsvir oluna bilər. Tezlik oblastında $w^2(x)$ bağlanması W_j^2 hasilinə çevrilir, ona görə də $W_j^2=W_j$ və, beləliklə, $w(x)$ çoxhədlisi aşağıdakı xüsusi xassəyə malik olur:

$$w^2(x)=w(x)\pmod{x^n-1}.$$

$w^2(x)=w(x)\pmod{x^n-1}$ şərtini ödəyən istənilən $w(x)$ çoxhədlisi idempotent adlanır.

Hər bir idempotent aşağıdakı kimi alına bilər: bir neçə vətər götürürük və əgər j bu vətərlərdən birinə daxildirsə, onda $w_j=0$, əks halda isə $w_j=1$ qəbul edirik. Tərs Furye çevirməsi zaman oblastında idempotent olan çoxhədli verir. Hər bir idempotent bu qayda ilə qurula bilər.

Alınan nəticələrin dövrü kodlara tətbiqinə baxaq:

Teorem 4. Hər bir dövrü kodda elə yeganə $w(x)$ kod çoxhədlisi mövcud olur ki, verilən $c(x)$ çoxhədlisi ancaq və anacaq

$$c(x)\cdot w(x)=c(x)\pmod{x^n-1}$$

olduqda kod çoxhədlisi olur. $w(x)$ çoxhədlisi idempotentdir.

İsbatı. Tutaq ki, $g(x)$ əməlgətirici çoxhədlidir və tutaq ki,

$$W_j = \begin{cases} 0, & \text{əgər } g(\alpha^j) = 0, \\ 1, & \text{əgər } g(\alpha^j) \neq 0. \end{cases}$$

Onda $w(x)$ idempotentdir. Onun kökləri $g(x)$-ın kökləri ilə üst-üstə düşür və, beləliklə, o kod sözü olur. Bundan başqa hər bir j üçün $W_j \cdot G_j = G_j$ və ona görə də $w(x) \cdot g(x) = g(x)$. Ancaq və ancaq $c(x) = a(x) \cdot g(x)$ bərabərliyini ödəyən hər hansı bir $a(x)$ çoxhədlisi halında $c(x)$ çoxhədlisi kod sözü olur. Buradan da alınır ki,

$$c(x) \cdot w(x) = a(x)w(x)g(x) = a(x)g(x) = c(x) \pmod{x^n - 1}$$

□

Nümunə 1. $g(x) = x^3 + x + 1$ əməlgətirici çoxhədlisinə malik (7,4)-Xemminq koduna baxaq. Bu çoxhədli $GF(8)$ meydanında $\alpha, \alpha^2, \alpha^4$ köklərinə malikdir. Aşağıdakı spektrə baxaq:

$$V = (1,\ 0,\ 0,\ 1,\ 0,\ 1,\ 1)\,.$$
$$\uparrow\ \ \uparrow\ \ \uparrow$$
$$\alpha\ \ \alpha^2\ \ \alpha^4$$

Tərs Furye çevirməsi ilə spektri V olan υ zaman vektorunu tapaq.

$\upsilon = (\upsilon_0, \upsilon_1, ..., \upsilon_6)$ vektorunun komponentlərini hesablayaq:

$$\upsilon_0 = V_0 + V_3 + V_5 + V_6 = 0,$$
$$\upsilon_1 = V_0 + \alpha^{-3}V_3 + \alpha^{-5}V_5 + \alpha^{-6}V_6 = 1 + \alpha^4 + \alpha^2 + \alpha = 1,$$
$$\upsilon_2 = V_0 + \alpha^{-6}V_3 + \alpha^{-10}V_5 + \alpha^{-12}V_6 = 1 + \alpha + \alpha^4 + \alpha^2 = 1,$$
$$\upsilon_3 = V_0 + \alpha^{-9}V_3 + \alpha^{-15}V_5 + \alpha^{-18}V_6 = 1 + \alpha^5 + \alpha^6 + \alpha^3 = 0,$$
$$\upsilon_4 = V_0 + \alpha^{-12}V_3 + \alpha^{-20}V_5 + \alpha^{-24}V_6 = 1 + \alpha^2 + \alpha + \alpha^4 = 1,$$
$$\upsilon_5 = V_0 + \alpha^{-15}V_3 + \alpha^{-25}V_5 + \alpha^{-30}V_6 = 1 + \alpha^6 + \alpha^3 + \alpha^5 = 0,$$
$$\upsilon_6 = V_0 + \alpha^{-18}V_3 + \alpha^{-30}V_5 + \alpha^{-36}V_6 = 1 + \alpha^3 + \alpha^5 + \alpha^6 = 0.$$

Beləliklə, zaman vektoru $\upsilon = (0,1,1,0,1,0,0)$ vektoru olar. İdempotent $w(x) = x + x^2 + x^4$ çoxhədlisi olar. Doğrudan da

$$w^2(x) = x^8 + x^4 + x^2 = x^4 + x^2 + x \pmod{x^7 - 1},$$

yəni $w^2(x) = w(x)$.

$u(x) = x^4 + x^3 + x^2 + 1$ çoxhədlisinə baxaq. Bu çoxhədlinin kod çoxhədlisi olmasını yoxlayaq. Bunun üçün

$$u(x)w(x) = u(x) \pmod{x^7 - 1}$$

müqayisəsinin düzgün olmasını yoxlayaq:

$$u(x)w(x) = (x^4 + x^3 + x^2 + 1)(x^4 + x^2 + x) = x^8 + x^7 + x^4 + x^3 + x = \\ = x^4 + x^3 + x^2 + 1 \pmod{x^7 - 1}.$$

Beləliklə, $u(x) = x^4 + x^3 + x^2 + 1$ çoxhədlisi kod çoxhədlisi olar. Doğrudan da, asanlıqla yoxlamaq olar ki, $u(x) = (x+1)g(x)$ ödənir.

Nümunə 2. $t = 2$ səhvi düzəldə bilən və əmələgətirici çoxhədlisi $g(x) = x^8 + x^7 + x^6 + x^4 + 1$ olan (15,7) – BÇX koduna baxaq. Bu kod üçün idempotenti tapaq.

Bilavasitə yoxlamaqla göstərmək olar ki, $g(x)$ çoxhədlisinin kökləri $GF(2^4)$ meydanının $\alpha, \alpha^2, \alpha^3$ və α^4 elementləridir. Uyğun vətərlər aşağıdakılar olar: $\{1,2,4,8\}$, $\{3,6,12,9\}$. Beləliklə,

$$V_1 = V_2 = V_4 = V_8 = V_3 = V_6 = V_{12} = V_9 = 0,$$
$$V_0 = V_5 = V_7 = V_{10} = V_{11} = V_{13} = V_{14} = V_{15} = 1.$$

Komponentləri $w(x)$ idempotentinin əmsalları olan w vektorunun spektri $V = (1,0,0,0,0,1,0,1,0,0,1,1,0,1,1,1)$ vektoru olar. w vektorunun komponentlərini tərs Furye çevirməsinin köməkliyi ilə tapaq:

$$w_0 = V_0 + V_5 + V_7 + V_{10} + V_{11} + V_{13} + V_{14} + V_{15} = 0,$$
$$w_1 = V_0 + \alpha^{-5}V_5 + \alpha^{-7}V_7 + \alpha^{-10}V_{10} + \alpha^{-11}V_{11} + \alpha^{-13}V_{13} + \alpha^{-14}V_{14} + \\ + \alpha^{-15}V_{15} = V_0 + \alpha^{10}V_5 + \alpha^8 V_7 + \alpha^5 V_{10} + \alpha^4 V_{11} + \alpha^2 V_{13} + \alpha V_{14} + \\ + V_{15} = 1 + \alpha^{10} + \alpha^8 + \alpha^5 + \alpha^4 + \alpha^2 + \alpha + 1 = 1,$$
$$w_2 = V_0 + \alpha^5 V_5 + \alpha V_7 + \alpha^{10}V_{10} + \alpha^8 V_{11} + \alpha^4 V_{13} + \alpha^2 V_{14} + V_{15} = \\ = \alpha^8 + \alpha + \alpha^{10} + \alpha^8 + \alpha^4 + \alpha^2 = 1,$$
$$w_3 = 1 + 1 + \alpha^9 + 1 + \alpha^{12} + \alpha^6 + \alpha^3 + 1 = \alpha^3 + \alpha^6 + \alpha^9 + \alpha^{12} = 1,$$

$$w_4 = 1+\alpha^{10}+\alpha^2+\alpha^5+\alpha+\alpha^8+\alpha^4 = 1,$$
$$w_5 = 1+\alpha^5+\alpha^{10}+\alpha^{10}+\alpha^5+\alpha^{10}+\alpha^5+1 = 1,$$
$$w_6 = 1+\alpha^0+\alpha^3+\alpha^0+\alpha^9+\alpha^{12}+\alpha^6+1 = 1,$$
$$w_7 = 1+\alpha^{10}+\alpha^{11}+\alpha^5+\alpha^{13}+\alpha^{14}+\alpha^7+1 = 0,$$
$$w_8 = 1+\alpha^5+\alpha^4+\alpha^{10}+\alpha^2+\alpha+\alpha^8+1 = 1,$$
$$w_9 = 1+\alpha^{12}+1+\alpha^6+\alpha^3+\alpha^9 = 1,$$
$$w_{10} = \alpha^{10}+\alpha^5+\alpha^5+\alpha^{10}+\alpha^5+\alpha^{10} = 1,$$
$$w_{11} = \alpha^5+\alpha^{13}+\alpha^{10}+\alpha^{14}+\alpha^7+\alpha^{11} = 0,$$
$$w_{12} = \alpha^0+\alpha^6+\alpha^0+\alpha^3+\alpha^9+\alpha^{12} = 1,$$
$$w_{13} = \alpha^{10}+\alpha^{14}+\alpha^5+\alpha^7+\alpha^{11}+\alpha^3 = 0,$$
$$w_{14} = \alpha^5+\alpha^7+\alpha^{10}+\alpha^{11}+\alpha^{13}+\alpha^{14} = 0.$$

Beləliklə, w vektoru $w = (0111111011\ 10100)$ kimidir. Onda

$$w(x) = x+x^2+x^3+x^4+x^5+x^6+x^8+x^9+x^{10}+x^{12}$$

idempotentdir.

$u(x) = x^9+x^6+x^5+x^4+x+1$ çoxhədlisinə baxaq. Bu çoxhədlinin kod çoxhədlisi olmasını yoxlayaq

$$u(x)w(x) = x^{21}+x^{19}+x^{15}+x^9+x^5+x \pmod{x^{15}-1} =$$
$$= x^9+x^6+x^5+x^4+x+1 \pmod{x^{15}-1}.$$

Buradan da alınır ki, $u(x)w(x) = u(x) \pmod{x^{15}-1}$ və odur ki, $u(x)$ kod çoxhədlisidir. Digər tərəfdən də bilavasitə yoxlamaqla göstərmək olar ki, $u(x) = (x+1)g(x)$, yəni $u(x)$ həqiqətən də kod çoxhədlisidir.

§3. Dövri kodların spektral yazılışları

Dövri kodun hər bir c sözü $(n-1)$ dərəcəli çoxhədli şəklində verilir. Qeyri-sistematik şəkildə o $c(x) = g(x)\cdot d(x)$ şəklində yazılır,

harada ki, $d(x)$ -informasiya çoxhədlisidir və dərəcəsi $(k-1)$ -dir. Zaman oblastında bu aşağıdakı (dövri) bağlamanı verir:

$$c_i = \sum_{k=0}^{n-1} g_{((i-k))} \cdot d_k \ .$$

Beləliklə, tezlik oblastında kodlaşdırma əməliyyatı aşağıdakı hasil şəklində yazıla bilər:

$$C_j = G_j \cdot D_j$$

Bu bərabərliyi ödəyən istənilən spektr bütün komponentlərin $GF(q)$ -dən olması şərti ilə tezlik oblastında kod sözü verir. İnformasiya spektrinin ixtiyari olması şərti ilə G_j -nin yeganə əhəmiyyətli rolu kod sözünün spektrinin sıfra bərabər olan C_j komponentinin dayandığı tezliyin təyin edilməsindən ibarətdir. Beləliklə, dövri kodun aşağıdakı kimi alternativ təyinini vermək olar. B dövri kodu $GF(q)$ üzərində olan elə sözlər çoxluğudur ki, onların yoxlayıcı tezliklər adlanan $j_1,...,j_{n-k}$ tezliklərinin verilmiş çoxluğuna məxsus spektral komponentləri sıfırdır.

Dövri kodun hər bir sözü $GF(q)$ üzərində vektordur, amma kod sözünün spektri $GF(q^m)$ üzərində vektordur. Beləliklə, dövri kod verilən tezliklər çoxluğundan olan komponentləri sıfıra bərabər olan bütün vektorlar çoxluğunun $GF(q)$ -qiymətli tərs Furye çevirmələri çoxluğu kimi təyin edilə bilər. Verilən tezliklər çoxluğunda sıfırlardan ibarət ixtiyari spektral vektor götürülə bilməz; belə vektorların bəzilərinin tərs çevirmələrinin komponentləri $GF(q)$ meydanından olmaya da bilər. Kod sözünün $GF(q)$ meydanına aid olması üçün ancaq teorem 2.1-də verilən qoşmalıq şərtini ödəyən spektri götürmək lazımdır.

BÇX kodları yoxlayıcı tezlikləri ardıcıl götürülən dövri kodlardandır. $n = q^m - 1$ uzunluqlu və t sayda səhvi düzəldən BÇX kodları $2t$ sayda ardıcıl tezliklərdən ibarət verilmiş blokda spektrləri sıfıra bərabər olan $GF(q)$ üzərində bütün kod sözləri çoxluğu kimi təyin olunur.

Teorem 1 (BÇX kodlarının sərhəddi). Tutaq ki, n ədədi hər hansı bir m üçün $(q^m - 1)$ ədədini bölür. $GF^n(q)$ -dən olan $(d-1)$ -dən çox

olmayan çəkiyə malik və spektrdə ardıcıl $(d-1)$ sayda sıfır komponentli yeganə vektor sıfır vektorudur.

İsbatı. c vektorunun ν sayda sıfırdan fərqli komponentlərinin indekslərini $i_1,...,i_\nu$ ilə işarə edək, $\nu \le d-1$. Tezlik oblastında bütün i tezliyi üçün tərs Furye çevirməsi sıfır komponentlərdən ibarət olan vektor təyin edək, harada ki, $c_i \neq 0$. Belə vektor çoxlu üsullarla seçilə bilər. Mümkün seçmələrdən biri $\Lambda(x)$ lokatorlar çoxhədlisinə əsaslanır:

$$\Lambda(x)=\prod_{k=1}^{\nu}(1-x\alpha^{-i_k})=\Lambda_\nu x^\nu+\Lambda_{\nu-1}x^{\nu-1}+...+\Lambda_1 x+\Lambda_0 .$$

Λ vektoru spektr kimi təsəvvür olunur, harada ki, onun şüurlu təyini ona gətirib çıxarır ki, onun $\lambda=(\lambda_1,\lambda_2,...,\lambda_n)$ tərs çevirməsi $c_i \neq 0$ şərtini ödəyən hər bir i zaman anı üçün sıfıra bərabərdir. Yuxarıda zaman oblastında yazılan hasil sıfıra bərabərdir ($i=0,...,n-1$ üçün $\lambda_i c_i=0$); Beləliklə, tezlik oblastında dövri bağlama sıfıra bərabərdir:

$$\Lambda * C = 0 .$$

$k > d-1$ olduqda $\Lambda_0=1$ və $\Lambda_k=0$ olduğundan bağlama aşağıdakı kimi yazıla bilər:

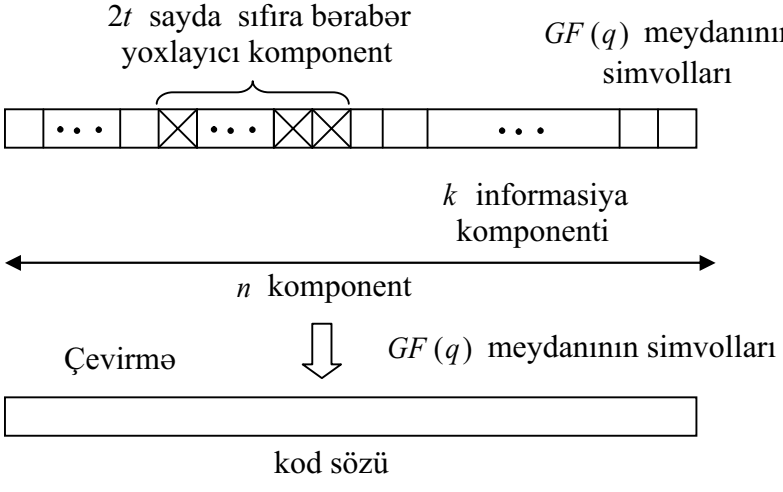
$$C_j=-\sum_{k=0}^{d-1}\Lambda_k C_{((j-k))} .$$

Lakin $d-1$ uzunluqlu blokda C vektoru sıfırdır. Beləliklə, rekursiyaya görə C vektoru hər yerdə sıfıra bərabərdir. Deməli, C vektoru sıfır vektoru olmalıdır. □

Əgər $n=q-1$ (və ya n ədədi $q-1$ ədədini bölür) isə, onda BÇX kodu Rid-Solomon kodudur; kod sözü və onun spektri eyni bir meydanda yerləşir. İnformasiya simvollarını spektral komponentlərin hesablanmasında istifadə etməklə kodlaşdırmanı bilavasitə tezlik oblatında aparmaq olar. $2t$ sayda ardıcıl komponenti sıfıra bərabər olan hər spektr kod sözüdür. Kodlaşdırma aşağıdakı kimi aparılır. Hər hansı $2t$ sayda ardıcıl tezlik (məsələn, ilk $2t$ sayda tezlik) zəruri olan məhdudiyyəti təmin etmək üçün götürülür: bu tezliklərdəki simvollar sıfır qəbul olunur. Spektrin qalan $n-2t$ koordinatı $GF(q)$-dən olan informasiya simvolları ilə doldurulur. Onda tərs Furye çevirməsi şəkil 1-də göstərilən kod sözünü

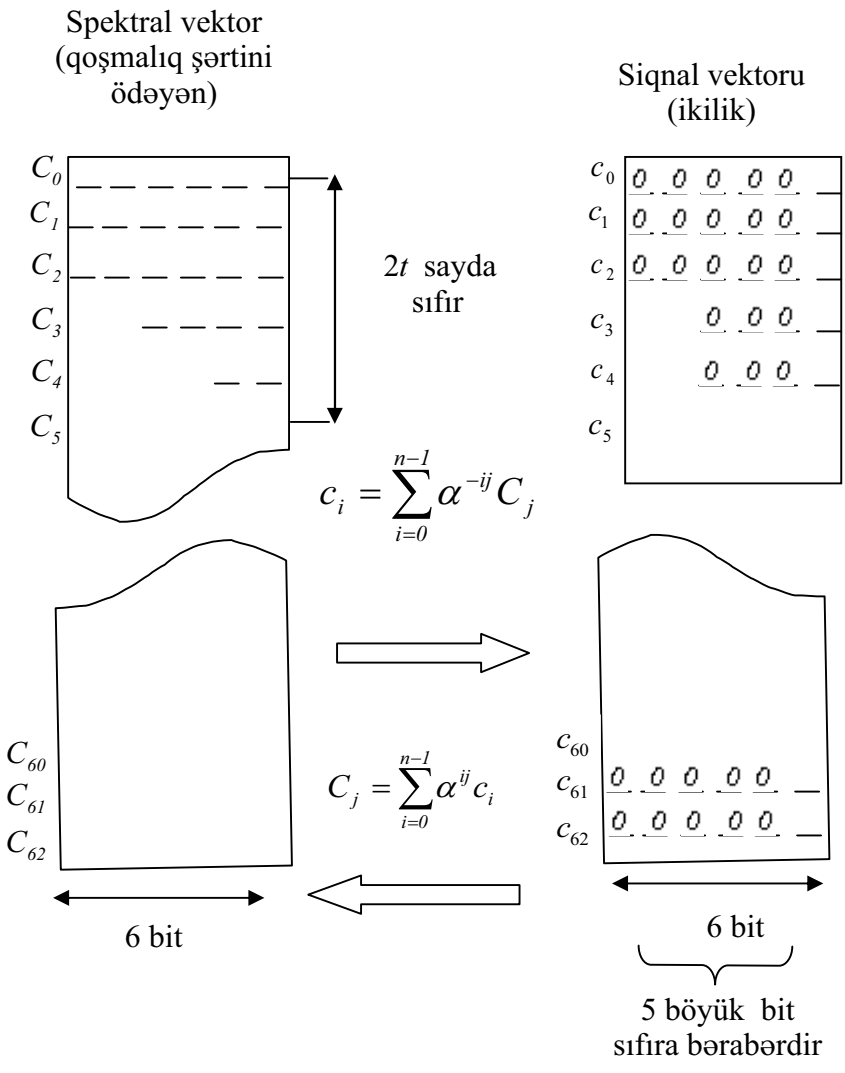
(sistematik olmayan) verir. Belə ki, informasiya simvolunun yazıldığı $n-2t$ sayda tezlik olduğundan $(n, n-2t)$ - Rid-Solomon kodu alınır.

BÇX kodlarının nisbətən daha ümumi halında kodlaşdırma daha mürəkkəbdir. İndi biz iki meydana malikik: simvolların $GF(q)$ meydanı və spektrlər üçün istifadə edilən lokatorların $GF(q^m)$ meydanı. Yenə də spektrin $2t$ sayda ardıcıl komponenti onlara sıfırlar yazılması üçün ayrılır. Qalan komponentlər k informasiya simvolları kimi təqdim olunurlar, harada ki, tərs Furye çevirməsinin $GF(q)$-dən qiymət alması üçün $GF(q^m)$-dən q^k sayda qayda ilə seçilməlidirlər. Nümunə olaraq şəkil 2-də 63 uzunluğuna malik koda uyğun prosedura verilir. Burada spektrin hər bir komponenti 6-bitlik ikilik ədəd kimi verilir, spektr vektoru isə 63 6-bitlik ədəd kimi təqdim olunur. Kod sözü də həmçinin 63 6-bitlik ikilik ədəd kimi təqdim olunur, lakin o məhdudiyyətlərlə ki, hər bir 6-bitlik ədəddə ancaq ən kiçik tərtibli bit sıfırdan fərqli ola bilər. Beləliklə, həqiqətdə kod sözü 63-bitlik ikilik sözdür. Biz istəyirik ki, spektral vektoru elə verək ki, siqnal vektoru oxşar şəkildə ikilik kod sözü olsun. Uyğun gələn spektral vektorun qurulmasında zəruri olan məhdudiyyətləri bizə teorem 2.1 verir.



Şəkil 1. Furye çevirməsi vasitəsilə Rid-Solomon kodlarının Kodlaşdırılması.

63 uzunluqlu kodun qurulmasının dərhal yerinə yetirilə bilməsinə baxmayaraq, əvvəlcədən daha sadə nümunəyə baxaq, məhz teorem 2.1-i istifadə etməklə tezlik oblastında (7,4) – Xemminq kodunu quraq. Belə qurma şəkil 3-də göstərilir. Yoxlayıcı tezlik kimi C_1 və C_2 komponentləri seçilmişdir, belə ki, yeganə səhv düzəldilə bilinər. İnformasiya C_0 və C_3 tezlik komponentlərində olur.



Şəkil 2. BÇX kodlarının Furye çevirməsi

vasitəsilə kodlaşdırılması

Qalan komponentlər teoremin verdiyi məhdudiyyətlərə görə yazılır: $C_1^4 = C_2^2 = C_4 = 0$ və $C_3^4 = C_6^2 = C_5$. Teorem 2.1-ə görə $C_0^2 = C_0$ və, beləliklə, C_0 ancaq 0 və ya 1 qiymətlərinə malik ola bilər. C_0 komponentinin ekvivalent «bit məzmunu» bir bitə bərabərdir, C_3 koordinatının ekvivalent bit məzmunu üçə bərabərdir. Beləliklə, spektrin birqiymətli verilməsi üçün Xemminq kodunun dörd informasiya bitini istifadə etmək lazımdır. Bu informasiya bitləri zaman oblastı ilə deyil tezlik oblastı ilə bağlıdır. Ümumi halda ədədlər n moduluna görə qoşma elementlər sinfinə bölünürlər:

$$A_j = \{j, jq, jq^2, ..., jq^{m_j - 1}\}$$

Tezlik oblastında kod sözü							Zaman oblastında kod sözü						
C_0	C_1	C_2	C_3	C_4	C_5	C_6	c_0	c_1	c_2	c_3	c_4	c_5	c_6
0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	α^0	0	α^0	α^0	1	1	1	0	1	0	0
0	0	0	α^1	0	α^4	α^2	0	0	1	1	1	0	1
0	0	0	α^2	0	α^1	α^4	0	1	0	0	1	1	1
0	0	0	α^3	0	α^5	α^6	1	1	0	1	0	0	1
0	0	0	α^4	0	α^2	α^1	0	1	1	1	0	1	0
0	0	0	α^5	0	α^6	α^3	1	0	0	1	1	1	0
0	0	0	α^6	0	α^3	α^5	1	0	1	0	0	1	1
1	0	0	0	0	0	0	1	1	1	1	1	1	1

1	0	0	α^0	0	α^0	α^0	0	0	0	1	0	1	1
1	0	0	α^1	0	α^4	α^2	1	1	0	0	0	1	0
1	0	0	α^2	0	α^1	α^4	1	0	1	1	0	0	0
1	0	0	α^3	0	α^5	α^6	0	0	1	0	1	1	0
1	0	0	α^4	0	α^2	α^1	1	0	0	0	1	0	1
1	0	0	α^5	0	α^6	α^3	0	1	1	0	0	0	1
1	0	0	α^6	0	α^3	α^5	0	1	0	1	1	0	0

Şəkil 3. (7,4)-Xemminq kodu

Əgər C_j spektral komponenti verilibsə, onda indeksləri j ilə qoşma elementlər sinfinə daxil olan başqa komponentlər C_j-nin qüvvəti olur və, beləliklə, ixtiyari seçilə bilməzlər. Əgər bu qoşma elementlər sinfinin gücü r -ə bərabərdirsə, onda

$$C_j^{q^r} = C_j \text{ , yaxud } C_j^{q^r-1} = 1.$$

Beləliklə, biz C_j-nin mümkün qiyməti kimi $GF(q^m)$-dən ixtiyari olaraq element seçə bilmərik: ya sıfır element və ya da ancaq tərtibi (q^r-1)-i bölən element mümkündür. $GF(q^m)$ meydanının hər bir elementinin tərtibi (q^m-1)-i bölür; uyğun olaraq (q^r-1) ədədi (q^m-1)-i bölür və aydındır ki, qoşma elementlərin hər bir sinfinin gücü m -i bölür.

Koderi təsvir etmək üçün q^m-1 ədədlər çoxluğunu qoşma elementlər sinfinə bölək və hər sinifdən nümayəndə kimi bir element götürək. Bu nümayəndələr yeganə qaydada qiymətli simvolları təyin edir. BÇX kodlarını formalaşdırmaq üçün yoxlayıcı tezlik kimi $2t$ sayda spektral komponent götürülür və onlar da sıfıra bərabər hesab olunur. Qalan qiymətli simvollar informasiya simvolları olurlar və tərtiblərinə qoyulan məhdudiyyəti nəzərə almaqla ixtiyari qiymətlər ala bilərlər. İndeksləri həmin qoşma elementlər sinfinə daxil olan qalan simvollar sərbəst olmurlar; onlar əlaqələnən tezlikləri əmələ gətirirlər.

Şəkil 4-də $GF(64)$ meydanı üçün vəziyyət təsvir olunmuşdur. Birinci sütuna sərbəst tezliklərin komponentləri daxil edilir. Əgər C_1, C_2, C_3, C_4, C_5 və C_6-lar yoxlayıcı tezliklər kimi götürülərsə, onda üç səhvi düzəldən BÇX kodu alınar. Onda $C_0, C_7, C_9, C_{11}, C_{13}, C_{15}, C_{21}, C_{23}, C_{27}$ və C_{31} informasiya simvolları olur. C_9 və C_{27} ya sıfıra bərabər, ya da ki, 7 tərtibinə malik elementə bərabər olmalıdır (belə ki, $C_9^8 = C_9$ və $C_{27}^8 = C_{27}$); bu elementlər $GF(8)$ alt meydanına aiddirlər. C_{21} ya sıfıra, ya da 3 tərtibli elementə bərabər olmalıdır (belə ki, $C_{21}^4 = C_{21}$); bu elementlər $GF(4)$ alt meydanına aiddirlər. C_0 ya sıfır, ya da 1 tərtibli elementə bərabər olmalıdır; bu elementlər $GF(2)$ alt meydanını əmələ gətirirlər.

Bütün qalan elementlər $GF(64)$ meydanının ixtiyari elementləridirlər. Bu simvolları müəyyən etmək üçün bütövlükdə 45 informasiya biti tələb olunur. Beləliklə, üç səhvi düzəldən (63,45) – BÇX kodu alınır.

Sərbəst tezliklər	Əlaqəli tezliklər	Bit məzmunları
$\{C_0\}$		1
$\{C_1$	$C_2\ C_4\ C_8\ C_{16}\ C_{32}\}$	6
$\{C_3$	$C_6\ C_{12}\ C_{24}\ C_{48}\ C_{33}\}$	6
$\{C_5$	$C_{10}\ C_{20}\ C_{40}\ C_{17}\ C_{34}\}$	6
$\{C_7$	$C_{14}\ C_{28}\ C_{56}\ C_{49}\ C_{35}\}$	6
$\{C_9$	$C_{18}\ C_{36}\}$	3
$\{C_{11}$	$C_{22}\ C_{44}\ C_{25}\ C_{50}\ C_{37}\}$	6
$\{C_{13}$	$C_{26}\ C_{52}\ C_{41}\ C_{19}\ C_{38}\}$	6
$\{C_{15}$	$C_{30}\ C_{60}\ C_{57}\ C_{51}\ C_{39}\}$	6
$\{C_{21}$	$C_{42}\}$	2
$\{C_{23}$	$C_{46}\ C_{29}\ C_{58}\ C_{53}\ C_{43}\}$	6
$\{C_{27}$	$C_{54}\ C_{44}\}$	3

Şəkil 4. $GF(64)$ ***meydanı üzərində spektrin strukturu***

Sərbəst tezliyin komponentlərini seçdikdən sonra bağlı (əlaqəli) tezliklərin komponentləri onun uyğun dərəcələri kimi təyin olunur. Belə formalaşdırılan 2^{45} kod sözü dəqiqliklə zaman oblastında kodlaşdırılan 2^{45} kod sözü olur. İnformasiyanın ayrılması momentinə qədər dekoderə kodlaşdırmanın hansı üsulla həyata keçirilməsi barədə məlumat lazım deyildir. Lakin sonuncu addımda, harada ki, səhvləri düzəldilmiş kod sözündən informasiya ayrılır, dekoderə bilmək lazım gəlir ki, bu informasiya necə kodlaşıb.

Əgər kodlaşdırma tezlik oblastında həyata keçirilibsə, onda informasiya simvolları tezlik oblastında hesablanmalıdır.

§4. Dekodlaşdırmanın spektral üsulları

BÇX kodlarının dekodlaşdırılması üçün yeni üsula baxaq. Qəbul edilən υ sözü $\upsilon_i = c_i + e_i, i = 0,1,...,n-1$ komponentlərindən ibarətdir. Burada c_i və e_i uyğun olaraq c kod sözünün və səhv vektorunun komponentləridir. Dekoder υ sözündən e vektorunun komponentlərini ləğv edir və nəticədə c kod sözü qalır.

BÇX kodunun təhrifə məruz qalmış kod sözünün, yəni qəbul edilən sözün sindromunun koordinatları aşağıdakı kimi hesablanır:

$$S_j = \sum_{i=0}^{n-1} \alpha^{i(j+j_0-1)} \upsilon_i = \upsilon(\alpha^{j+j_0-1}),\ j = 1,...,2t.$$

Aydındır ki, sindromun komponenti qəbuledilən vektorun Furye çevirməsinin $2t$ komponenti kimi hesablanır. $\upsilon = c + e$ təhrifə məruz qalmış kod sözünün Furye çevirməsinin komponentləri

$V_j = C_j + E_j$, $j = 0,..., n-1$, kimidir. Sindromun komponentləri isə bu spektrlərin j_0-dan $(j_0 + 2t - 1)$-ə kimi $2t$ komponenti kimi təqdim olunur. Lakin BÇX kodlarının qurulması qaydasına görə yoxlayıcı tezliklərdə yerləşən ($j = j_0,..., j_0 + 2t - 1$ olduqda) spektral komponentlər sıfıra bərabərdir: $C_j = 0$, $j = j_0,...j_0 + 2t - 1$. Beləliklə,

$$S_j = V_{j+j_0-1} = E_{j+j_0-1}, \quad j = 1,...,2t .$$

Sindromların komponentləri bloku səhvlərin konfiqurasiyası spektrinin n sayda komponentlərindən $2t$ saydasını müşahidə etməyə imkan verir. Lakin, əgər səhvlərin konfiqurasiyasının çəkisi t-ni aşmırsa, onda BÇX-nın sərhəddinə görə sindromun bu $2t$ komponenti səhv vektorunu birqiymətli olaraq bərpa etmək üçün kifayətdir.

Tutaq ki, $\nu < t$ sayda səhv baş vermişdir və səhvin lokatorları $\alpha^{i_1},...,\alpha^{i_\nu}$-lərdir. Səhvlərin lokatoru çoxhədlisi aşağıdakına bərabərdir

$$\Lambda(x) = \prod_{k=1}^{\nu}(1 - x\alpha^{i_k}) .$$

Λ vektorunun tərs Furye çevirməsi $\Lambda(x)$ çoxhədlisinin α^{-i} nöqtəsində $\Lambda(\alpha^{-i})$ qiyməti kimi hesablanır. Aydındır ki, i səhv mövqesini təmsil etdikdə onda və ancaq onda $\Lambda(\alpha^{-i})$ sıfıra bərabər olar. Beləliklə, $\Lambda(x)$ çoxhədlisi elə çoxhədli kimi təyin olunur ki, bu çoxhədli üçün zaman oblastında bütün $e_i \neq 0$ halında $\lambda_i = 0$. Deməli, bütün i-lər üçün $\lambda_i e_i = 0$ və, beləliklə bağlama haqqında teoremə görə tezlik oblastında bağlama sıfra bərabərdir:

$$\sum_{j=0}^{n-1} \Lambda_j E_{k-j} = 0,\ k = 0,...,n-1 .$$

$\Lambda(x)$ çoxhədlisinin dərəcəsi t-ni aşmadığından bütün $j > t$ üçün $\Lambda_j = 0$. Beləliklə,

$$\sum_{j=0}^{t} \Lambda_j E_{k-j} = 0,\ k = 0,...,n-1 .$$

$\Lambda_0 = 1$ olduğundan bu tənliyi aşağıdakı kimi yazmaq olar

$$E_k = -\sum_{j=1}^{t} \Lambda_j E_{k-j},\ k = 0,...,n-1.$$

Bu sistem $n-t$ sayda məchulu ($\Lambda(x)$-ın t sayda əmsalı və E vektorunun $n-2t$ sayda komponenti) və E vektorunun sindrom komponentləri ilə verilən məlum $2t$ sayda komponentlərini əlaqələndirən n sayda tənlikdən ibarətdir. Beləliklə, t sayda

$$S_k = -\sum_{j=1}^{t} \Lambda_j S_{k-j},\ \ k = t+1,...,2t \qquad (1)$$

tənlikləri ancaq sindromun məlum komponentlərindən və E vektorunun t sayda naməlum komponentlərindən ibarətdir. Belə sistemi Λ-ya nəzərən həmişə həll etmək olar, məsələn, Berlekemp-Messi alqoritminin köməkliyi ilə.

S spektrinin qalan komponentlərini rekurrent davam etməklə almaq olar: yuxarıda yazılan bağlama üçün olan (1) tənliyini istifadə etməklə S və Λ-nın artıq məlum olan komponentlərinə görə S_{2t+1}-i hesablamaq, sonra isə S_{2t+2}-ni tapmaq və i.a.

Şəkil 1-də dekodlaşdırma prosedurasının alqoritmi verilmişdir (Furye çevirməsi istisna olmaqla). Belə dekoder koderin hansı oblasta, yəni zaman yoxsa tezlik oblastında realizə olunmasından asılı olmayaraq realizə oluna bilər. Əgər koder zaman oblastında realizə olunubsa, onda kod sözünü zaman oblastında hesablamaq üçün korreksiya olunmuş spektrin tərs Furye çevirməsi hesablanmalıdır, sonra isə bu kod sözündən ötürülən informasiyanı ayırmaq lazımdır. Əgər kodlaşdırma tezlik oblastında aparılarsa, onda informasiya simvolları bilavasitə korreksiya olunmuş spektrə əsasən təyin olunur. Bu halda dekoderdə tərs çevirmə aparmaq lazım deyildir.

Tutaq ki, $\upsilon(x)$ qəbul edilən çoxhədlidir. Bu çoxhədlini aşağıdakı kimi yazaq:

$$\upsilon(x) = Q(x) \cdot g(x) + s(x),$$

harada ki, $g(x)$ BÇX kodunun əmələgətirici çoxhədlisi, $s(x)$ isə sindrom çoxhədlisidir. Sindrom çoxhədlisini $g(x)$-a bölmə sxemi vasitəsilə hesablamaq olar. Onda

$$S_j = \upsilon(\alpha^j) = Q(\alpha^j)g(\alpha^j) + s(\alpha^j) = s(\alpha^j),$$

$$j = j_0 + 1, \ldots, j_0 + 2t,$$

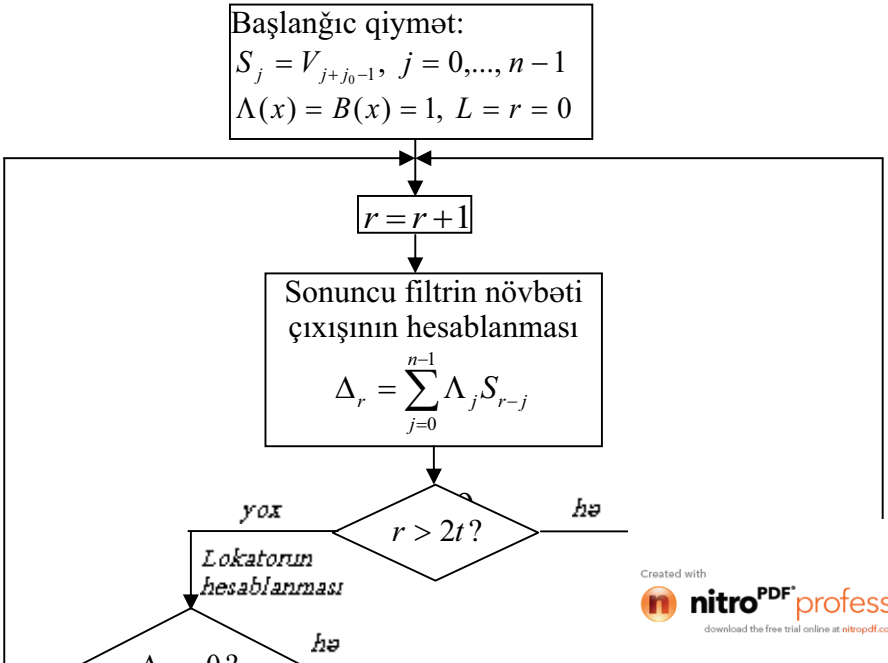
belə ki, j indeksinin bu qiymətlərində $g(\alpha^j) = 0$ bərabərliyi ödənir. Sindromun komponentlərini n deyil ancaq $n-k$ sıfırdan fərqli əmsala malik olan $s(x)$ çoxhədlisinin Furye çevirməsi kimi hesablamaq olar. Bu üsul $g(x)$ çoxhədlisinə bölmə əməliyyatı n nöqtədə Furye çevirməsini hesablamaqdan asan olduqda ancaq xeyirlidir. Evklid alqoritminə əsaslanan başqa dekodlaşdırma alqoritmi də mövcuddur. Bu üsul tezlik oblastına oriyentasiya olunub və aşağıda şərh olunur.

$GF(q^m)$ meydanında aşağıdakı ayırma qüvvədədir:

$$x^n - 1 = \prod_{i=0}^{n-1}(x - \alpha^i).$$

Aşağıdakı kimi təyin olunan və doğru-lokator çoxhədlisi adlanan $\Lambda^0(x)$ çoxhədlisini daxil edək:

$$\Lambda^0(x) = (x^n - 1)/\Lambda(x).$$



Şəkil 1. Tezlik dekoderi.

Aydındır ki, $\Lambda^0(x)$ həqiqətən də çoxhədlidir, belə ki, $\Lambda(x)$ çoxhədlisi hər biri $x^n - 1$ çoxhədlisinin böləni olan xətti vuruqların hasili kimi təsvir olunur. $\Lambda^0(x)$ çoxhədlisinin köklərini qəbuledilən vektorun düzgün komponentləri təyin edir.

Teorem 1. $E(x)$ səhvlər çoxhədlisi və $\Lambda(x)$ lokatorlar çoxhədlisi aşağıdakı bərabərliyi ödəyir:

$$\text{ƏBOB}[x^n-1, E(x)] = (x^n-1)/\Lambda(x) = \Lambda^0(x).$$

İsbatı: $E(x)$ və $\Lambda(x)$ çoxhədliləri ümumi köklərə malik deyildirlər, belə ki, ancaq və ancaq o zaman $\Lambda(\alpha^j)=0$ olur ki, $E(\alpha^j)\neq 0$ olsun. Hər bir α^i elementi ya $E(x)$, ya da ki, $\Lambda(x)$ çoxhədlisinin kökü olmalıdır. Beləliklə, $\Lambda(x)$ ilə qarşılıqlı sadə olan hər hansı bir $P(x)$ üçün

$$\Lambda(x)E(x) = P(x)(x^n-1).$$

Onda

$$\text{ƏBOB}[x^n-1, E(x)] = (x^n-1)/\Lambda(x) = \Lambda^0(x).$$

□

Müvəqqəti olaraq $E(x)$ çoxhədlisinin ümumi halda ancaq $2t$ sayda böyük əmsallarının məlum olması faktını nəzərə almaqla teorem 5.7.1-də təsvir olunan Evklid alqoritmini $s(x)=x^n-1$ və $t(x)=E(x)$ çoxhədlilərinə tətbiq edək. Bir halda ki,

$$\Lambda(x)\text{ƏBOB}[x^n-1, E(x)] = x^n-1,$$

onda nəticə 5.7.1-ə görə

$$\Lambda(x) = (-1)^R A_{22}^{(R)}(x),$$

harada ki, $A_{22}^{(R)}(x)$ Evklid alqoritminin yerinə yetmə prosesində hesablanır.

Əgər $E(x)$ çoxhədlisi məlumdursa, onda Evklid alqoritminin kökəmliyi ilə $\Lambda(x)$-i hesablaya bilərik. Lakin $E(x)$ çoxhədlisinin o əmsalları bizə məlum olur ki, $C(x)$ çoxhədlisinin həmin əmsallara uyğun əmsalları sıfra bərabərdir. Beləliklə, ilk baxışdan bu düstur $\Lambda(x)$ üçün faydasızdır. Əslində isə bu düsturu o halda da istifadə etmək olar ki, $E(x)$ çoxhədlisinin ancaq $2t$ sayda əmsalı məlum olsun (əgər onlar düzgün olarlarsa).

Əmələgətirici çoxhədlisinin kökləri $\alpha^{n-2t},...,\alpha^{n-1}$ elementləri olan BÇX kodlarına baxaq (əgər meydanın primitiv elementi kimi α^{-1} istifadə olunarsa, onda bunlar 1-dən $2t$-yə qədər qüvvət dərəcəsilə adi köklərdir). Belə BÇX kodları üçün dekodlaşdırma alqoritmini quraq. Göstərək ki, əgər t-dən çox olmayan sayda səhv baş veribsə, onda Evklid alqoritminin

iterasiyası $E(x)$ çoxhədlisinin ancaq $2t$ sayda böyük əmsallarından asılı olur. Qalan əmsallar ixtiyari olaraq seçilə bilər.

Teorem 2. Tutaq ki, $j = n-2t,\ldots,n-1$ üçün E_j verilmişdir. Onda $j = 0,\ldots,n-2t-1$ halında E_j-lərin verilməsi üçün birdən çox olmayan elə bir qayda mövcuddur ki,

$$\Lambda(x)\text{ƏBOB}[x^n-1, E(x)] = x^n-1$$

tənliyi t və ya ondan kiçik dərəcəli $\Lambda(x)$-a nəzərən həll olunandır.

İsbatı. Teoremin isbatı göstərir ki, o BÇX kodlarının sərhəddinin bir formasıdır. Fərz edək ki, $\Lambda(x)$ çoxhədlisinin dərəcəsi t-dən çox deyildir və elədir ki, o teoremin şərtini ödəyir. Evklid alqoritminin sonuncu addımını nəticə 5.7.1-in isbatında olduğu formada yazaq:

$$\begin{pmatrix} x^n-1 \\ E(x) \end{pmatrix} = (-1)^R \begin{pmatrix} A_{22}^{(R)}(x) & -A_{12}^{(R)}(x) \\ -A_{21}^{(R)}(x) & -A_{11}^{(R)}(x) \end{pmatrix} \begin{pmatrix} \text{ƏBOB}[x^n-1,\ E(x)] \\ 0 \end{pmatrix}.$$

Buradan da görünür ki, $(-1)^R A_{22}^R(x) = \Lambda(x)$. Bununla yanaşı birbaşa şəkildə sonuncu bərabərlik aşağıdakı kimidir

$$\begin{pmatrix} \text{ƏBOB}[x^n-1,\ E(x)] \\ 0 \end{pmatrix} = \begin{pmatrix} A_{11}^{(R)}(x) & A_{12}^{(R)}(x) \\ A_{21}^{(R)}(x) & A_{22}^{(R)}(x) \end{pmatrix} \begin{pmatrix} x^n-1 \\ E(x) \end{pmatrix},$$

bu da ki, aşağıdakı tələbə gətirib çıxarır:

$$0 = (-1)^R A_{21}^R(x)(x^n-1) + \Lambda(x)E(x).$$

Beləliklə, $\Lambda(x)E(x)$ çoxhədlisi x^n-1 çoxhədlisinin mislidir. Deməli, $E(x)$ çoxhədlisi $GF(q^m)$ meydanının o nöqtələrində kökə malikdir ki, bu nöqtələrdə $\Lambda(x)$ çoxhədlisi kökə malik deyildir. Bir halda ki, $\Lambda(x)$ çoxhədlisinin dərəcəsi t-ni aşmır, onda o t-dən çox olmayan sayda sıfırlara malikdir. Onda tərs Furye çevirməsinin e_i komponentləri ən azı $n-t$ dəfə sıfıra çevrilər. BÇX-nın sərhəddinə görə elə e vektoru tapılmalıdır ki, bu vektorun Furye çevirməsi $E(x)$ çoxhədlisinin $j = n-2t,\ldots,n-1$-ci mövqelərində məlum əmsalları ilə üst-üstə düşsün. □

İsbat olunan teoremin tətbiqinin bilavasitə üsullarından biri bütün mümkün üsullarla $E(x)$ çoxhədlisinin əmsallarını seçmək cəhdi və $\Lambda(x)$ çoxhədlisini hesablamaq üçün Evklid alqoritmindən istifadədir. Ancaq bir $\Lambda(x)$ çoxhədlisi t-dən böyük olmayan dərəcəyə malik olacaq. Bu çoxhədli də səhvlər lokatorunun düzgün çoxhədlisi olar, uyğun $E(x)$ çoxhədlisi isə səhvlər vektorunun düzgün spektri olar. Lakin $\Lambda(x)$ birqiymətli olaraq $E(x)$-ın məlum komponentləri birbəbir əsasında təyin olunduğundan $E(x)$-ın naməlum əmsallarının birbəbir yoxlanmasından qaçmaq imkanı daha məqsədəuyğun görünür. Belə alqoritm şəkil 2-də verilir.

Aşağıdakı qalıqlı bölmə alqoritminə baxaq:

$$s(x) = Q(x)t(x) + r(x),$$

harada ki, $\deg t(x) = a$ və $\deg s(x) = b$. Bu alqoritmdə $Q(x)$-ın dərəcəsi $b-a$-ya bərabərdir və $Q(x)$ çoxhədlisi $t(x)$-dən ancaq $t_a, t_{a-1}, ..., t_{b-a}$ əmsalları vasitəsilə asılıdır. $Q(x)$–i hesablamaq üçün $r = 0, ..., b-a$ olduqda aşağıdakı iterativ proseduradan istifadə edək:

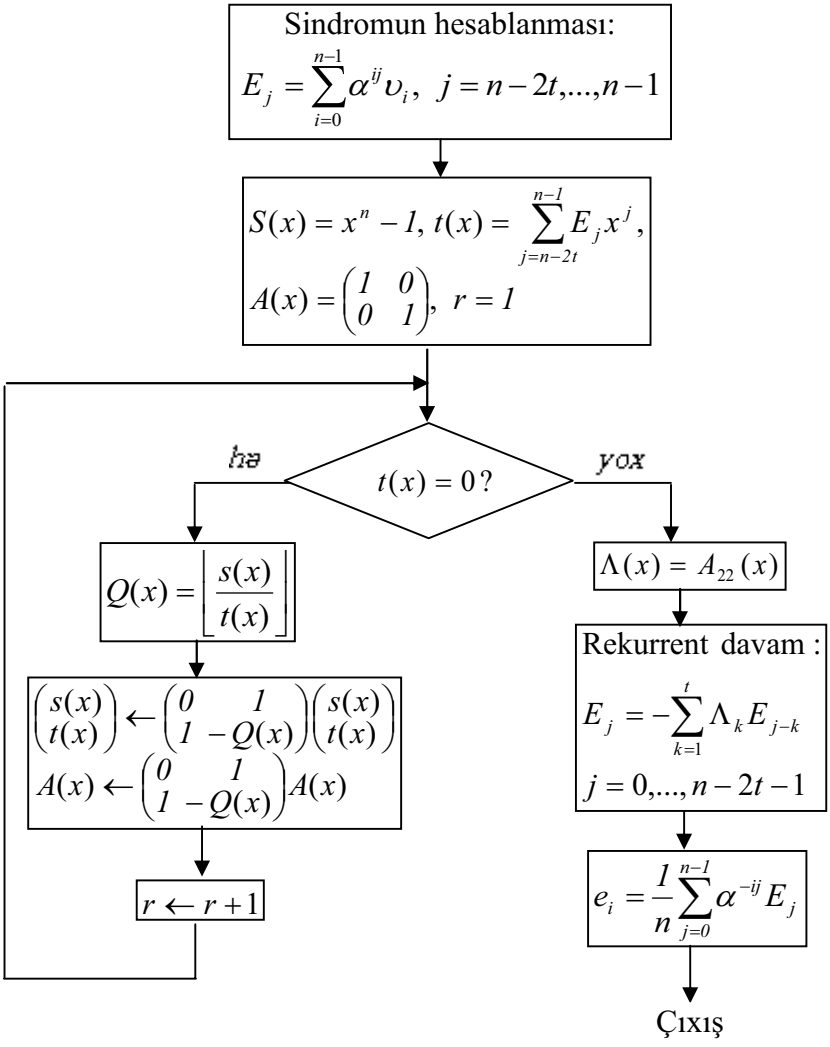
$$Q_{b-a-r} = [s_{b-r} - \sum_{\ell=0}^{r-1} Q_{b-a-\ell} t_{a+\ell-r}] / t_a .$$

Bu alqoritm adi bölmə alqoritminin zəif modifikasiyadır.

Bu qismətin hesablanması prosedurasını Evklid alqoritminin hər addımında istifadə edək. Teorem 5.7.1-in r-ci iterasiyasında j-nin $n + 2t + \sum_{\ell=1}^{r} \deg Q^{(\ell)}(x)$ qiymətindən $n-1$ qiymətinə kimi ancaq $s_j^{(r+1)}$ və $t_j^{(r+1)}$ əmsallarını hesablayaq. $s^{(r+1)}(x)$ və $t^{(r+1)}(x)$ çoxhədlilərinin bu böyük əmsalları məhz bir sıra baxılan çoxhədli-qismətlərin qurulmasında Evklid alqoritminin iterasiya addımlarının yerinə yetməsi üçün zəruri olanlardır. Belə ki,

$$\begin{pmatrix} \text{ƏBOB}\,[x^n - 1,\ E(x)] \\ 0 \end{pmatrix} = \left\{ \prod_{\ell=R-1}^{0} \begin{pmatrix} 0 & 1 \\ 1 & -Q^{(\ell)}(x) \end{pmatrix} \right\} \cdot \begin{pmatrix} x^n - 1 \\ E(x) \end{pmatrix} =$$

$$= \left\{ \prod_{\ell=R-1}^{r+1} \begin{pmatrix} 0 & 1 \\ 1 & -Q^{(\ell)}(x) \end{pmatrix} \right\} \cdot \begin{pmatrix} s^{(r+1)}(x) \\ t^{(r+1)}(x) \end{pmatrix},$$



Şəkil 2.

onda yazmaq olar

$$\left\{\prod_{\ell=R-1}^{0}\begin{pmatrix} Q^{(\ell)}(x) & 1 \\ 1 & 0 \end{pmatrix}\right\}\begin{pmatrix} \text{ƏBOB}\,[x^n-1,\ E(x)] \\ 0 \end{pmatrix}=$$

$$=\left\{\prod_{\ell=r}^{0}\begin{pmatrix} 0 & 1 \\ 1 & -Q^{(\ell)}(x) \end{pmatrix}\right\}\begin{pmatrix} x^n-1 \\ E(x) \end{pmatrix}=\begin{pmatrix} s^{(r+1)}(x) \\ t^{(r+1)}(x) \end{pmatrix}.$$

$\text{ƏBOB}\,[x^n-1, E(x)]$-in dərəcəsi ən azı $n-t$-yə bərabər olduğundan buradan alınır ki, $t^{(r+1)}(x)$-in dərəcəsi ən azı aşağıdakı kəmiyyətə bərabərdir

$$n-t+\sum_{\ell=r+1}^{R-1}\deg Q^{(\ell)}(x).$$

Beləliklə, j-nin $n-2t+\sum_{\ell=1}^{r}\deg Q^{(\ell)}(x)$-dən $n-t+\sum_{\ell=r+1}^{R}\deg Q^{(\ell)}(x)$-ə kimi bütün qiymətlərində sıfırdan fərqli yuxarı indeks halında $t_j^{(r+1)}$ məlumdur. Bu diapazon $Q^{(\ell+1)}(x)$-in hesablanması və iterasiyasının davamı üçün kifayətdir.

;

8) $\upsilon(x)=x^{13}+2x^{12}+x^{10}+2x^9+x^8+2x^5+2x^3+2x^2+1$;

9) $\upsilon(x)=x^{14}+2x^{12}+2x^6+2x^4+2x+1$;

10) $\upsilon(x)=2x^{14}+x^{13}+x^{12}+x^{11}+2x^{10}+2x^9+2x^8+x^6$;

11) $\upsilon(x)=x^{17}+2x^{16}+x^{15}+x^{14}+x^{13}+2x^{12}+2x^{11}+x^9$;

12) $\upsilon(x)=x^{17}+2x^{16}+2x^{14}+x^{12}+x^{11}+x^8+x^5+2x^4+2x^3+1$;

13) $\upsilon(x)=x^{13}+x^{12}+x^{11}+2x^8+x^6+x^5+2x^4+2x+1$;

14) $\upsilon(x)=x^{12}+x^{11}+2x^{10}+2x^9+2x^8+2x^6+2x^5+2x+2$;

15) $\upsilon(x)=x^{13}+x^{10}+x^9+x^3+x+1$;

16) $\upsilon(x)=x^{16}+2x^{12}+x^{11}+x^6+x^4+x+1$;

17) $\upsilon(x) = x^{13} + 2x^{10} + 2x^9 + 2x^8 + x^5 + 2x + 2$.

Tapşırıq 2. $n = 3^3 - 1 = 26$ uzunluğuna malik, $t = 3$ sayda səhvi düzəltməyə imkan verən və informasiya sözündən $g(x) = x^{12} + x^{11} + 2x^6 + x^3 + 2x^2 + 2x + 1$ əmələgətirici çoxhədlisi vasitəsilə qurulan $GF(3^3)$ meydanı üzərində BÇX – kodları halında qəbul edilən kod sözü aşağıdakı $\upsilon(x)$ çoxhədlisi olduqda ötürülən kod sözünü, səhv sözünü və informasiya sözünü tapmalı

1) $\upsilon(x) = x^{13} + x^4 + 2x^2 + x$;
2) $\upsilon(x) = x^{13} + 2x^{11} + x^6 + x^4 + 2x + 2$;
3) $\upsilon(x) = x^{15} + x^{11} + 2x^{10} + 2x^7 + x^6 + 2x^5 + 3x^3 + x + 1$;
4) $\upsilon(x) = x^{14} + 2x^{13} + x^{11} + 2x^9 + x^6 + x + 1$;
5) $\upsilon(x) = 2x^{15} + 2x^{14} + 2x^{11} + 2x^7 + x^5 + 2x^4 + 2x + 2$;
6) $\upsilon(x) = x^{19} + x^{12} + x^{10} + 2x^8 + x^4 + 2x^3 + 2x^2 + x$;
7) $\upsilon(x) = x^{15} + x^{12} + x^{11} + x^8 + x^5 + x^2 + 1$;
8) $\upsilon(x) = x^{14} + x^{13} + 2x^8 + 2x^5 + 2x^4 + 2x^2 + 2$.

CAVABLAR

Tapşırıq 1.

1) $c(x) = x^{10} + 2x^7 + 2x^6 + x^4 + x^3 + 2x + 1 = (x+1)g(x)$,
$e(x) = x^{10} + 2x^4$;

2) $c(x) = (x+2)g(x) = x^{10} + x^9 + 2x^8 + x^5 + 2x^2 + 2$,
$e(x) = 2x^5 + 1$;

3) $c(x) = x^2 g(x) = x^{11} + 2x^{10} + x^9 + x^8 + x^7 + 2x^6 + 2x^5 + 2x^4 + x^3 + x^2$,
$e(x) = 2x^7 + x^4$;

4) $c(x) = (x^2 + x + 1)g(x) = x^{11} + x^9 + x^8 + x^6 + 2x^5 + 2x^3 + x^2 + 2x = 1$,
$e(x) = 2x^9 + 2x^4$;

5) $c(x) = (x^2 + 2)g(x) = x^{11} + 2x^{10} + 2x^8 + x^6 + x^5 + 2x^3 + 2x^2 + 2x + 2$,
$e(x) = 2x^{11} + x^6$;

6) $c(x) = (x^3 + x^2 + 1)g(x) = x^{12} + x^8 + x^7 + 2x^6 + 2x^5 + 2x^4 + x^3 + x + 1$,
$e(x) = x^7 + 2x^3$;

7) $c(x) = (x^3 + 2x + 1)g(x) = x^{12} + 2x^{11} + 2x^8 + 2x^7 + 2x^6 + x^5 + x^4 +$
$+ x^3 + x^2 + 1$, $e(x) = 2x^{12} + x^7$;

8) $c(x) = (x^4 + 1)g(x) = x^{13} + 2x^{12} + x^{11} + x^{10} + 2x^9 + x^8 + 2x^5 + 2x^3 +$
$+ 2x^2 + x + 1$, $e(x) = 2x^{11} + 2x$;

9) $c(x) = (x^5 + x^3 + x + 1)g(x) = x^{14} + 2x^{13} + 2x^{12} + 2x^6 + 2x^4 +$
$+ 2x^3 + 2x + 1$, $e(x) = x^{13} + x^3$;

10) $c(x) = x^6 g(x) = x^{15} + 2x^{14} + x^{13} + x^{12} + x^{11} + 2x^{10} + 2x^9 +$
$+ 2x^8 + x^7 + x^6$, $e(x) = 2x^{15} + 2x^7$;

11) $c(x) = x^8 g(x) = x^{17} + 2x^{16} + x^{15} + x^{14} + x^{13} + 2x^{12} + 2x^{11} +$
$+ 2x^{10} + x^9 + x^8$, $e(x) = x^{10} + 2x^8$;

12) $c(x) = (x^8 + 2x^6 + 1)g(x) = x^{17} + 2x^{16} + 2x^{14} + x^{12} + x^{11} + x^8 +$
$+ x^5 + 2x^4 + 2x^3 + 2x^2 + x + 1$, $e(x) = x^2 + 2x$;

13) $c(x) = (x^5 + 2x^4 + 2x^3 + x + 1)g(x) = x^{14} + x^{13} + x^{12} + x^{11} +$
$+ 2x^8 + 2x^6 + x^5 + 2x^4 + 2x + 1$, $e(x) = 2x^{14} + 2x^6$;

14) $c(x)=(x^3+2x^2+2)g(x)=x^{12}+x^{11}+2x^{10}+2x^9+$
$+x^8+2x^6+2x^5+x^3+2x+2$, $e(x)=x^8+2x^3$;

15) $c(x)=(x^4+x^3+x^2+1)g(x)=x^{13}+x^{11}+x^{10}+x^9+$
$+x^6+x^3+x+1$, $e(x)=2x^{11}+2x^6$;

16) $c(x)=(x^7+x^6+x^2+1)g(x)=x^{16}+2x^{13}+2x^{12}+x^{11}+$
$+x^7+x^6+x^4+x+1$, $e(x)=x^{13}+2x^7$;

17) $c(x)=(x^4+2x^2+2)g(x)=x^{13}+2x^{12}+2x^{10}+2x^9+$
$+2x^8+2x^6+x^5+2x+2$, $e(x)=x^{12}+x^6$;

Tapşırıq 2.

1) $c(x)=xg(x)=x^{13}+x^{12}+2x^7+x^4+2x^3+2x^2+x$,
$e(x)=2x^{12}+x^7+x^3$;

2) $c(x)=(x+2)g(x)=x^{13}+2x^{11}+2x^7+x^6+x^4+x^3+2x+2$,
$e(x)=x^7+2x^3$;

3) $c(x)=(x^4+2x+1)g(x)=x^{16}+x^{15}+2x^{13}+x^{11}+2x^{10}+2x^7+$
$+x^6+2x^5+2x^3+x+1$, $e(x)=2x^{16}+x^{13}$;

4) $c(x)=(2x^4+x^3+2x+1)g(x)=2x^{16}+x^{14}+2x^{13}+x^{11}+$
$x^{10}+2x^9+x^6+x+1$, $e(x)=x^{16}+2x^{10}$;

5) $c(x)=(2x^3+x+2)g(x)=2x^{15}+2x^{14}+x^{13}+2x^{11}+x^9+2x^7+$
$+x^5+2x^4+2x+2$, $e(x)=2x^{13}+2x^9$;

6) $c(x)=(x^7+x)g(x)=x^{19}+x^{18}+x^{12}+x^{10}+2x^9+2x^8+x^4+$
$+2x^3+2x^2+x$, $e(x)=2x^{18}+x^9$;

7) $c(x)=(x^3+2x^2+1)g(x)=x^{15}+2x^{13}+x^{12}+x^{11}+2x^9+x^8+$
$+x^5+x^2+2x+1$, $e(x)=x^{13}+x^9+x$;

8) $e(x)=x^5+x^2+2$, $c(x)=x^2g(x)$.

ƏDƏBİYYAT

1. F.G.Feyziyev. Diskret riyaziyyatın bəzi fəsilləri. Dərs vəsaiti. Bakı, «Təhsil» NPM, 2008, 242 s.

2. Дискретная математика и математические вопросы кибернетики. Т.1, Под общей редакцией С.В.Яблонского и О.Б.Лупанова. М.: Наука, 1974, 311 с.

3. Яблонский С.В. Введение в дискретную математику. М.: Наука, 1986.

4. Биркоф Г., Барти Т. Современная прикладная алгебра. М.: Мир, 1976.

5. Р.Блейхут. Теория и практика кодов, контролирующих ошибки. Пер.с англ. – М.: Мир, 1986, 576 с.

6. Берлекемп Э. Алгебраическая теория кодирования. М.: Мир, 1971.

7. Питерсон У., Уэлдон Э. Коды, исправляющие ошибки, М.: Мир, 1976.

8. Касами Т., Токура Н., Ивадари Е., Инагаки Я. Теория кодирования. М.: Мир, 1978.

9. Мак-Вильямс Ф.Дж., Слоэн Н.Дж. Теория кодов, исправляющих ошибки. М.: Связь, 1979.

F.-r.e.d., prof. Kamil Bayraməli oğlu Mənsimov
F.-r.e.d., prof. Fikrət Güləli oğlu Feyziyev
F.-r.e.n. Nailə Xanbelovna Aslanova

KODLAŞDIRMA NƏZƏRİYYƏSİ
(*dərs vəsaiti*)