AZƏRBAYCAN MİLLİ ELMLƏR AKADEMİYASI
İDARƏETMƏ SİSTEMLƏRİ İNSTİTUTU

Əlyazması hüququnda

MEHRDAD ASLAN OĞLU BABAVƏND ƏRƏBLU

SƏHVLƏRƏ NƏZARƏTEDİCİ BLOK KODLARINDA SƏHVLƏRİN AŞKARLANMA VƏ DÜZƏLDİLMƏSİ ALQORİTMLƏRİNİN EFFEKTİV REALLAŞDIRILMASI

3338.01– Sistemli analiz, idarəetmə və informasiyanın işlənməsi

Texnika elmləri üzrə fəlsəfə doktoru alimlik dərəcəsi
almaq üçün təqdim edilmiş dissertasiyanın

AVTOREFERATI

Bakı – 2016

İş Bakı Dövlət Universitetinin "İnformasiya texnologiyaları və proqramlaşdırma" kafedrasında yerinə yetirilmişdir.

Elmi rəhbər: riyaziyyat elmləri doktoru, professor
F.G.Feyziyev

Rəsmi opponentlər: texnika elmləri doktoru, professor
S.İ.Yusifov

texnika üzrə fəlsəfə doktoru, dosent
A.H.Rzayev

Aparıcı təşkilat: Milli Aviasiya Akademiyasının
"İnformasiya texnologiyaları" kafedrası

Müdafiə "28" fevral 2016-cı ildə saat 15^{00}-da Azərbaycan Milli Elmlər Akademiyasının İdarəetmə Sistemləri İnstitutu nəzdindəki D01.121 Dissertasiya şurasının iclasında keçiriləcəkdir.
Ünvan: AZ1141, Bakı şəh., B.Vahabzadə küç., 9.

Dissertasiya ilə Azərbaycan Milli Elmlər Akademiyasının İdarəetmə Sistemləri İnstitutunun kitabxanasında tanış olmaq olar.

Avtoreferat "28" yanvar 2016-cı il tarixində göndərilmişdir.

D01.121 Dissertasiya şurasının elmi katibi,
riyaziyyat üzrə fəlsəfə doktoru, dosent **A.B.Paşayev**

İŞİN ÜMUMİ XARAKTERİSTİKASI

Mövzunun aktuallığı. İnformasiya şəbəkələrinin normal fəaliyyəti üçün informasiyaların qorunması məsələsi müasir riyazi kibernetikanın və nəzəri informatikanın əsas məsələlərindən biridir. İnformasiyaların tamlığının qorunmasının riyazi üsulları dedikdə diskret riyaziyyatın kodlaşdırma və kriptologiya nəzəriyyələri kimi bölmələrində yaradılmış riyazi üsullar nəzərdə tutulur. Kodlaşdırma nəzəriyyəsinin əsas bölmələrindən biri məlumatların ötürülməsi və məlumat daşıyıcılarında saxlanılması zamanı obyektiv (texniki) və ya subyektiv səbəblərdən onların təhriflərə məruz qalması hallarında ilkin məlumatların bərpa oluna bilməsi məsələləri ilə bağlı olan təhriflərə (səhvlərə) nəzarətedici kodlaşdırma bölməsidir. Səhvlərə nəzarətedici kodlaşdırma sahəsində müxtəlif kod sistemləri yaradılmışdır. Belə sistemlərin biri də blok kodlarıdır. Blok kodlarının xətti, dövri və Bouz-Çoudxuri–Xokvinqem (BÇX) kodları geniş istifadə olunur.

Diskret informasiyanın rabitə kanallarında (RK) təhrifsiz ötürülməsinin təşkilində blok kodlarının istifadəsi informasiyanın uyğun koda çevrilməsinə və nəticədə alınan kod sözünün informasiya əvəzinə RK ilə ötürülməsinə əsaslanır. RK -nın sonunda qəbul edilən söz əsasında kanalda ötürmə zamanı təhrifin olmasını aşkarlamaq və düzəltmək üçün müxtəlif alqoritmlər və üsullar yaradılmışdır.

Xətti kodların ötürülməsi zamanı səhvlərin aşkarlanması və düzəldilməsi üçün standart düzüm qaydası (SDQ) üsulu istifadə olunur. Bu üsul qrupların altqruplara nəzərən yanaşı siniflərə ayrılmasına əsaslanır. Xətti kod sözlərinin RK ilə ötürülməsi zamanı təhrifləri müəyyən etmək üçün qəbul edilən sözün sindromu əsasında yanaşı siniflər cədvəlində axtarış aparılır və səhv düzəldilir. Lakin böyük uzunluqlu kodlar halında bu üsul ilə səhvlərin düzəldilməsinə xeyli vaxt sərf olunur.

Dövri kodların RK ilə ötürülməsi zamanı səhvlərin aşkarlanması və düzəldilməsi üçün cədvəl və Meqqitt teoreminə əsaslanan üsullar istifadə olunur. Bu üsulların effektiv reallaşdırılması, yəni daha az vaxtda səhvlərin aşkarlanması və düzəldilməsinin bir yolu bu proseslərin paralelləşdirilməsidir. Odur ki, proseslərin avtomat modellərinin və ya xətti ardıcıllıqlı maşınlar (XAM) sinfində təsvirlərinin qurulmasına ehtiyac vardır.

BÇX kodlarının ötürülməsi zamanı səhvlərin aşkarlanması və düzəldilməsi üçün istifadə olunan üsullardan biri Piterson-Qorensteyn-Çirler (PQÇ) alqoritmidir. Bu alqoritmdə səhvləri tapmaq üçün əlavə olaraq xüsusi xətti cəbri tənliklər sistemi (XCTS) matrisin tərsinin tətbiqi ilə həll edilir. PQÇ alqoritmi sadə şərhə malik alqoritmdir, lakin sistemin matrisinin elementləri sonlu meydan üzərində olan çoxhədlilərdir və bu səbəbdən

PQÇ alqoritminin işində xeyli hesablamalar lazım gəlir. Ona görə də bu alqoritmin istifadəsi böyük uzunluqlu kodlar halında məqsədəuyğun deyildir.

Kodlaşdırma və dekodlaşdırmanın təşkilində sürüşmə registrləri, sonlu ardıcıllıqlı maşınlar (ARM) və s. istifadə olunur. A.Gil, R.H.Fərəcov, F.G.Feyziyev və başqalarının işlərində ARM-ların tədqiqi sahəsində alınan nəticələr geniş şərh olunmuşdur. ARM-ların qəbul edilən sözlərdə səhvlərin aşkarlanması və düzəldilməsi proseslərinin təsviri və sintezi sahəsində tətbiqi effektiv nəticələr alınmasına səbəb ola bilər.

Dissertasiya işində xətti kodlar, dövri kodlar və BÇX kodlarının ötürülməsi zamanı yaranan səhvlərin aşkarlanması və düzəldilməsi üçün yuxarıda adı çəkilən üsullarla bağlı qeyd olunan nöqsanların aradan qaldırılmasına baxılır və tətbiqi nöqteyi-nəzərdən işin mövzusu aktualdır.

İşin məqsədi. Dissertasiya işində aşağıdakı məsələlərə baxılır:

– İkilik xətti blok kodlarında standart düzüm qaydası əsasında səhvlərin aşkarlanması və düzəldilməsi prosesinin effektiv reallaşdırılması;

– Dövri kodların ötürülməsi zamanı yaranan səhvlərin cədvəl üsulu əsasında aşkarlanması, düzəldilməsi və informasiya sözünün ayrılması prosesinin XAM-lar sinfində modelləşdirilməsi;

– Dövri kodların ötürülməsi zamanı yaranan səhvlərin Meqqitt teoremi əsasında aşkarlanması, düzəldilməsi və informasiya sözünün ayrılması prosesinin XAM-lar sinfində modelləşdirilməsi;

– BÇX kodlarının ötürülməsi zamanı səhvlərin aşkarlanaraq düzəldilməsi üçün PQÇ alqoritminin modifikasiyası və effektiv reallaşdırılması.

İşin elmi yeniliyi. İşdə alınan yeni nəticələr aşağıdakılardır:

- İkilik xətti blok kodların ötürülməsi zamanı səhvlərin aşkarlanması və düzəldilməsinin effektiv reallaşdırılması metodikası işlənilmişdir;

- İkilik olmayan dövri kodların ötürülməsi zamanı səhvlərin cədvəl üsulu əsasında aşkarlanması, düzəldilməsi və informasiya sözünün ayrılması prosesinin XAM-lar sinfində təsviri düsturları verilmişdir;

- Dövri kodların ötürülməsi zamanı yaranan səhvlərin Meqqitt teoremi əsasında aşkarlanması, düzəldilməsi və informasiya sözünün ayrılması prosesinin XAM-lar sinfində təsviri düsturları verilmişdir;

- İkilik BÇX kodlarının ötürülməsi zamanı səhvlərin aşkarlanması və düzəldilməsi üçün Piterson alqoritminin Qauss üsulu əsasında modifikasiyası və sonlu meydan elementləri üzərində cəbri əməllərin xassələri və cədvəllərinə əsaslanan effektiv reallaşdırılması metodikası verilmişdir;

- İkilikolmayan BÇX kodlarının ötürülməsi zamanı səhvlərin aşkarlanması və düzəldilməsi üçün PQÇ alqoritminin Qauss üsulu əsasında modifikasiyası və sonlu meydan elementləri üzərində əməllərin xassələrinə və

cədvəllərinə əsaslanan effektiv reallaşdırılması metodikası verilmişdir.

İşin nəzəri və praktik əhəmiyyəti. İnformasiya sözlərinin dövri kodlara çevrilməsi, dövri kodların ötürülməsi zamanı səhvlərin aşkarlanması, düzəldilməsi və informasiya sözünün ayrılması prosesinin XAM-lar sinfində təsvir düsturları koder və dekoderlərin sintezində istifadə oluna bilər. PQÇ üsulunun effektiv reallaşdırılması metodikası BÇX kodları üçün olan digər üsullar halında və ümumiyyətlə başqa tip kodlar halında da uyğun metodikaların işlənilməsində əsas ola bilər. Alınan riyazi təsvir düsturları və təklif olunan effektiv reallaşdırma metodikaları maşın səmtli dillərdə proqram təminatının qurulmasında və s. istifadə oluna bilər.

Tədqiqat üsulları. Qarşıya qoyulan məqsədə çatmaq üçün kodlaşdırma nəzəriyyəsi, sonlu meydanlar nəzəriyyəsi, matrislər nəzəriyyəsi, çoxhədlilər nəzəriyyəsi, ardıcıllıqlı maşınlar nəzəriyyəsi, diskret riyaziyyat, kompüter sistem və şəbəkələri nəzəriyyəsi və s. istifadə olunmuşdur.

Müdafiəyə çıxarılan əsas müddəalar:

- İkilik xətti kodların ötürülməsi zamanı yaranan səhvlərin aşkarlanması, düzəldilməsi prosesinin effektiv reallaşdırılması metodikası;
- Dövri kodların cədvəl və Meqqitt teoremi əsasında səhvlərin aşkarlanması, düzəldilməsi və informasiyanın ayrılması prosesinin XAM sinfində təsviri düsturları;
- BÇX kodlarının ötürülməsi zamanı səhvlərin aşkarlanması və düzəldilməsi üçün Piterson və PQÇ alqoritmlərinin Qauss üsulu əsasında modifikasiyaları və onların effektiv reallaşdırılması metodikaları.

İşin aprobasiyası. İşdə alınan nəticələr BDU-nun "İnformasiya texnologiyaları və proqramlaşdırma", SDU-nun "Diferensial tənliklər və optimallaşdırma" kafedralarının elmi seminarlarında müzakirə olunmuş və "IV International Conference Problems of Cybernetics and Informatics (PSI' 2012, September 12-15,2012, Baku,Azerbaijan)", "Riyaziyyatın tətbiqi məsələləri və yeni informasiya texnologiyaları II Respublika Elmi Konfransı (Sumqayıt, SDU, 27-28 noyabr, 2012)", "Riyaziyyat və Mexanika İnstitutunun 55 illiyinə həsr olunmuş Riyaziyyat və Mexanikanın aktual problemləri Beynəlxalq konfransı (Bakı, 15-16 may 2014)" və "Riyaziyyat və İKT-nin tətbiq sahələri. Yeni tədris texnologiyaları Beynəlxalq Konfransı (Gəncə, GDU, 05-06 iyun 2014)" kimi elmi konfranslarda məruzə edilmişdir.

Nəticələrin nəşri. Dissertasiya işinin əsas məzmunu 13 elmi işdə çap olunmuşdur.

İşin strukturu və həcmi. Dissertasiya işi giriş, üç fəsil, nəticə, ədəbiyyat siyahısından ibarətdir. Dissertasiyanın əsas məzmunu 98 addan ibarət ədəbiyyat siyahısı da daxil olmaqla 154 səhifədə şərh olunmuşdur.

İŞİN ƏSAS MƏZMUNU

Girişdə dissertasiya işinin əsas xarakteristikaları və qısa məzmunu şərh olunur.

Birinci fəsildə səhvlərə nəzarətedici blok kodlarında səhvlərin aşkarlanmasının üsul və vasitələri şərh olunur. Burada **1.1 yarımfəslində** səhvlərə nəzarətedici kodlar nəzəriyyəsinin üsulları haqqında məlumatlar verilir. Sürüşmə registri vasitəsilə kodlaşdırma, səhvlərin aşkarlanması və düzəldilməsinin təşkili məsələləri **1.2 yarımfəslində** şərh olunur. **1.3 yarımfəslində** dövri kodlar halında kodlaşdırma, dekodlaşdırma və səhvlərin aşkarlanması və düzəldilməsi prosesinin ARM sinfində təsvirinə baxılır.

İkinci fəsil ARM-ların kodlaşdırma və dekodlaşdırma proseslərində tətbiqi məsələsinə həsr olunur. **2.1 yarımfəslində** (n,k,d^*) - ikilik xətti kodlar $GF(2)$ meydanı üzərində n-ölçülü vektorların toplama və ədədə vurma əməllərinə görə yaratdığı $GF^n(2)$ fəzasının altfəzası kimi şərh olunur. Burada k informasiya, n isə kodun uzunluqları. n düzəldilə bilən səhvlərin maksimal t sayından asılıdır. d^* kodun minimal məsafəsidir və $d^* \geq 2t+1$. Kodda 2^k sayda kod sözü vardır: $(c)_1,...,(c)_{2^k}$. Bu sözlərin hər birinin t radiuslu dekodlaşma kürəsi vardır. $G=(g_{ij})$ $(i=\overline{1,k}, j=\overline{1,n})$, $H=(h_{\alpha\beta})$ $(\alpha=\overline{1,n-k},\ \beta=\overline{1,n})$ kodun əmələgətirici və yoxlayıcı matrisləri, i informasiya və c kod sözləridirsə, onda $c=i\cdot G$.

Xətti kodlar halında qəbul edilən sözlərdə səhvlərin aşkarlanması və düzəldilməsinin effektiv təşkilinə **2.2 yarımfəslində** baxılır. Xətti kod sözlərinin RK ilə ötürülməsi zamanı təhriflərin baş verməsini müəyyən etmək üçün $\upsilon=(\upsilon_1,...,\upsilon_n)$ qəbul edilən sözün $s=(s_1,...,s_{n-k})$ sindromu

$$s_\alpha=\upsilon_1 h_{\alpha 1}+...+\upsilon_n h_{\alpha n},\quad \alpha=1,...,n-k, \qquad (1)$$

düsturu ilə tapılır. Sindrom sözü sıfır söz olmazsa, onda kod sözünün ötürülməsi zamanı təhrif baş vermişdir. υ sözü və onun s sindromu əsasında ötürülən kod sözünü tez tapmaq üçün SDQ əsasında metodika verilir. SDQ qrupların altqrupa görə yanaşı siniflərə ayrılmasına əsaslanır. Qrup $GF^n(2)$, altqrup isə n- uzunluqlu kodlar çoxluğudur. $(c)_1$, ..., $(c)_{2^k}$ sözlərinin hər birinə cədvəlin bir sütunu uyğun gəlir. Birinci sətirdə $(c)_1,...,(c)_{2^k}$ kod sözləri yazılır. Cədvəlin birinci sütunu qonşuluq sinfinin lideri adlanır. Sadələşdirilmiş SDQ-də cədvəlin ancaq birinci sütunu, yəni qonşuluq sinfinin liderləri sütunu iştirak edir. Təklif olunan metodikaya

görə qonşuluq siniflərinin liderləri M massivində ünvan üsulu ilə yerləşdirilir. M massivi 2^{n-k} sayda sətirdən ibarət olan massivdir. Massivin hər bir sətrində bir qonşuluq sinfinin lideri yerləşdirilir. Tutaq ki, $s=(s_1,...,s_{n-k})$ hər hansı bir sindromdur. Bu sindroma uyğun qonşuluq sinfinin lideri M massivinin $j=s_1+2s_2+...+2^{n-k-1}s_{n-k}$ və ya

$$j=\left(...\left(\left(s_{n-k}\cdot 2+s_{n-k-1}\right)\cdot 2+s_{n-k-2}\right)\cdot 2+s_{n-k-3}\right)\cdot 2+...+s_2\Big)\cdot 2+s_1 \quad (2)$$

kimi təyin olunan j nömrəli sətrində yerləşdirilir. υ qəbul edilən sözü əsasında (1) düsturu ilə s sindromu hesablanır. s sıfırdan fərqli söz olduqda (2) düsturu ilə uyğun qonşuluq sinfinin liderinin M massivində saxlandığı sətir nömrəsi tapılır. M - in tapılan nömrəli sətrindən qonşuluq sinfinin lideri götürülür və onu υ sözü ilə toplamaqla ötürülən c sözü hesablanır.

2.3 yarımfəslində ikilikolmayan dövri kodlar halında qəbul edilən sözlərdə sindromlar cədvəlinə əsaslanan üsulla səhvlərin aşkarlanması və düzəldilməsi prosesinin XAM-lar sinfində təsvirinə baxılır.

İkilik dövri kodlar halında qəbul edilən sözlərdə Meqqitt teoreminə əsaslanan üsulla səhvlərin aşkarlanması və düzəldilməsi prosesinin XAM-lar sinfində təsvirinə **2.4 yarımfəslində** baxılır.

Tutaq ki, B çoxluğu $GF(2)$ üzərində dövri kod əmələ gətirən $c=(c_0,...,c_{n-1})$ vektorlarının çoxluğudur, $GF^n(2)$ fəzasının altfəzasıdır və $B(x)=\{c(x)=c_{n-1}x^{n-1}+...+c_1x+c_0 \,|\, (c_0,c_1,...,c_{n-1})\in B\}$. $B(x)$ çoxluğunda çoxhədlilər $GF(2)$ meydanı üzərində toplanırlar. $B(x)$ -dən olan $p_1(x)$ və $p_2(x)$ çoxhədliləri $p_1(x)p_2(x)=R_{x^n+1}[p_1(x)p_2(x)]$ düsturu ilə vurulurlar, harada ki, $R_{b(x)}[a(x)]$ ilə $a(x)$ -in $b(x)$ -ə bölünməsindən alınan qalıq işarə olunmuşdur. $c(x)$ kodunun dövri sürüşdürülməsi $c'(x)=x\cdot c(x)$ kimi yerinə yetirilir. Tutaq ki, $g(x)$ çoxhədlisi B kodunun əmələgətirici çoxhədlisidir və $g(x)=g_{n-k}x^{n-k}+...+g_0$, $g_{n-k}=1$. Burada $g(x)$ $B(x)$ çoxluğunda ən kiçik dərəcəli sadə çoxhədlidir və x^n+1 çoxhədlisinin bölənidir. Tutaq ki, $i=(i_0,..,i_{k-1})$ vektoru $GF(2)$ meydanı üzərində k - ölçülü vektordur və $i(x)=i_{k-1}x^{k-1}+...+i_0$. Onda k - ölçülü i ikilik informasiya vektoru $c(x)=i(x)g(x)$ düsturu ilə c kod sözünə çevrilir. Tutaq ki, RK ilə $c(x)$ çoxhədlisinin əmsalları ötürülmüş, RK-nın sonunda $\upsilon(x)=\upsilon_{n-1}x^{n-1}+...+\upsilon_0$ çoxhədlisinin əmsalları qəbul edilmişdir və

$e(x) = e_{n-1}x^{n-1} + ... + e_0$ səhv, $s(x) = s_{n-k-1}x^{n-k-1} + ... + s_0$ sindrom çoxhədlilərdir, yəni $e(x) = \upsilon(x) + c(x)$, $s(x) = R_{g(x)}[\upsilon(x)] = R_{g(x)}[e(x)]$. Burada $i(x), c(x), \upsilon(x), e(x), s(x)$ çoxhədlilərinin real dərəcələri uyğun olaraq k-1, n-1, n-1, n-1, $n-k-1$ ədədlərindən kiçik və ya bərabərdirlər.

Meqqitt teoreminə görə $R_{g(x)}[\upsilon(x)] = s(x)$ və $g(x)$ çoxhədlisi $(x^n + 1)$ -in böləni olarsa, onda $R_{g(x)}[x\,\upsilon(x) \,(\mathrm{mod}\, x^n + 1)] = R_{g(x)}[x\,s(x)]$ və

$$R_{g(x)}[x\,e(x) \,(\mathrm{mod}\, x^n + 1)] = R_{g(x)}[x\,s(x)]\ . \qquad (3)$$

(3) görə əgər $s(x)$ çoxhədlisinə $e(x)$ çoxhədlisi uyğun gəlirsə, onda $s'(x) = xs(x)(\mathrm{mod}\, g(x))$ çoxhədlisinə $e'(x) = xe(x)(\mathrm{mod}\, x^n + 1)$ çoxhədlisi uyğun gəlir. $s(x)$ çoxhədlisinin x^{n-k-1} həddinin əmsalı sıfıra bərabər olduqda onun x ilə $GF(2)[x]/g(x)$ halqasında hasili bir addım sağa dövri sürüşməsidir. x və $e(x)$ çoxhədlilərinin $GF(2)[x]/(x^n + 1)$ halqasında hasili həmişə $e(x)$ çoxhədlisinin bir addım sağa dövri sürüşməsidir. (3)-ə görə $s(x)$ çoxhədlisini və ona uyğun $e(x)$ çoxhədlisini cədvəldə saxlamaqla, $s(x)$ sindrom çoxhədlisindən alınan $s'(x) = R_{g(x)}[x\,s(x)]$, $s''(x) = R_{g(x)}[x\,s'(x)]$, … çoxhədlilərinə uyğun $e'(x) = xe(x)(\mathrm{mod}\, x^n + 1)$, $e''(x) = x^2e(x)\,(\mathrm{mod}\, x^n + 1)$,… çoxhədlilərini müəyyən etmək olar. Cədvəldə yüksək həddinin əmsalı vahidə bərabər olan sindrom çoxhədliləri - bazis sindrom çoxhədliləri saxlanılır. Tutaq ki, $s(x)$ hər hansı bir bazis sindrom çoxhədlisidir. Əgər $s'(x)$ sindrom çoxhədlisi bazis olmayan sindrom çoxhədlisidirsə, lakin onun bir neçə addım sağa sürüşməsi nəticəsində $s(x)$ bazis sindrom çoxhədlisi ilə üst-üstə düşən çoxhədli alınırsa, onda bu çoxhədli $s(x)$ bazis sindrom çoxhədlisinə aid olan çoxhədli adlanır. Bazis sindrom çoxhədlisi $s^b(x) = s^b_{n-k-1}x^{n-k-1} + ... + s^b_0$ kimi yazılır.

İnformasiya sözü kodlaşdırıldıqda koder n takt işləyir. İlk k taktda koderin girişinə $i(x)$ – in $i_0, ..., i_{k-1}$ əmsalları, sonrakı taktlarda isə sıfırlar verilir. Koderin çıxışında kod çoxhədlisinin əmsalları $c_0, ..., c_{n-1}$ ardıcıllığı ilə alınmalıdır. Koderin işi aşağıdakı kimi təsvir olunur

$$y[t] = g_0 z[t] + ... + g_{n-k} z[t-(n-k)],\ t = 0,1,...,n-1,\ GF(2). \qquad (4)$$

Burada $z[t]$ və $y[t]$ koderin uyğun olaraq giriş və çıxış ardıcıllıqlarıdır,

g_α, $\alpha = 0,1,...,n-k$, əmsalları isə $g(x)$ çoxhədlisinin əmsallarıdır. Aydındır ki, $z[\alpha] = i_\alpha, \alpha = 0,...,k-1;\ z[\alpha] = 0, \alpha = k,...,n-1$. (4) koderinin girişinə yuxarıdakı kimi təyin olunan $z[\alpha]$, $\alpha = 0,...,n-1$, ardıcıllığı daxil olduqda onun çıxışı $c(x) = i(x)g(x)$ düsturu ilə təyin olunan $c(x)$ çoxhədlisinin əmsalları ilə üst-üstə düşür: $c_o = y[0]$, $c_1 = y[1],...,\ c_{n-1} = y[n-1]$.

Tutaq ki, RK ilə $\upsilon(x)$ çoxhədlisi qəbul olunmuşdur. Səhvləri aşkarlamaq və düzəltmək üçün $s(x)$ sindrom çoxhədlisini hesablamaq lazımdır. Əgər $\upsilon(x)$ çoxhədlisinin real dərəcəsi $n-k$-dan kiçik olarsa, onda $s(x)$ sindrom çoxhədlisi olaraq $\upsilon(x)$ çoxhədlisini götürmək, yəni

$$s_\alpha = \upsilon_\alpha, \alpha = 0,1,..., n-k-1, \tag{5}$$

qəbul etmək lazımdır. Əgər $\upsilon(x)$ çoxhədlisinin real dərəcəsi $(n-k)$-dan kiçik olmazsa, onda onun əmsalları dekoderin girişinə verilir. Aşağıdakı düsturla verilən dekoder $\upsilon(x)$ çoxhədlisini $g(x)$ çoxhədlisinə bölür:

$$\begin{cases} y_\alpha[0] = \upsilon_\alpha, \ \alpha = 0,1,...,n-1; \\ y_{n-\beta-\alpha}[\beta] = y_{n-\beta-\alpha}[\beta-1] + y_{n-\beta}[\beta-1]\, g_{n-k-\alpha}, \ \alpha = 1,...,n-k, \ GF(2), \\ y_{n-\beta-\alpha}[\beta] = y_{n-\beta-\alpha}[\beta-1], \ \alpha = n-k+1,...,n-\beta, \quad \beta = 1,2,...,k-1; \\ y_{n-k-\alpha}[k] = y_{n-k-\alpha}[k-1] + y_{n-k}[k-1]\, g_{n-k-\alpha}, \ \alpha = 1,...,n-k, \ GF(2). \end{cases} \tag{6}$$

(6) XAM-ı k takt işləyir və işin sonunda $\upsilon(x)$ çoxhədlisinin $g(x)$ çoxhədlisinə bölünməsi nəticəsində alınan natamam qismət və qalıq çoxhədlilərinin əmsalları indekslərin azalma ardıcıllığı ilə uyğun olaraq $y_{n-1}[0]$, $y_{n-2}[1]$, … , $y_{n-k}[k-1]$ və $y_{n-k-1}[k]$, $y_{n-k-2}[k],..., y_0[k]$ elementlərinin qiymətləri olur. Beləliklə, (6) XAM-ın işinin sonunda $s(x)$ sindrom çoxhədlisinin əmsallarını aşağıdakı düsturla tapmaq olar:

$$s_{n-k-\alpha} = y_{n-k-\alpha}[k], \ \alpha = 1,2,...,n-k. \tag{7}$$

Dekoder (5) və ya (6), (7) düsturları ilə $s(x)$ çoxhədlisini hesablayır. Əgər $s(x)$ sıfır çoxhədlisidirsə, onda heç bir səhv baş verməmişdir. Əgər $s(x)$ sıfırdan fərqli çoxhədlisidirsə, onda səhv baş vermişdir. Bu halda dekoder səhvi düzəltməlidir. Əgər $s(x)$ sindrom çoxhədlisi bazis çoxhədlisidirsə, onda $\nu = 0$ və $s^b(x) = s(x)$, yəni $s^b_\alpha = s_\alpha$, $\alpha = 0,1,...,n-k-1$,qəbul edilir. $s(x)$ çoxhədlisi bazis olmayan çoxhədli olduğu halda onun hansı bazis çoxhədlisinə aid olmasını müəyyənləşdirmək üçün onu sağa o qədər dəfə sürüşdürmək lazımdır ki, onun yüksək həddinin əmsalı vahidə bərabər olsun. Bu sürüşdürmələrin sayı aşağıdakı düstur əsasında müəyyən edilir:

$$\begin{cases} \nu = 0,\ p = 1; p := p(s_{n-k-\beta} + 1),\ GF(2), \\ \nu := \nu + p,\ \beta = 1,2,...,n-k-1. \end{cases} \tag{8}$$

(8) düsturu ilə tapılan ν -nün qiyməti $s(x)$ çoxhədlisinin sürüşmələrinin lazım olan sayını verir. aydındır ki, $s_{n-k-1} = s_{n-k-2} = ... = s_{n-k-\nu} = 0$.

$s(x)$ sindrom çoxhədlisini və (8) düsturu ilə hesablanan ν -nün qiymətini istifadə etməklə $s(x)$ çoxhədlisinin aid olduğu $s^b(x)$ bazis sindrom çoxhədlisinin əmsalları aşağıdakı rekurrent sxemlə tapılır:

$$s^b_{n-k-1-\gamma} = s_{n-k-1-\gamma-\nu},\ \gamma = 0,1,...,n\text{-}k\text{-}1\text{-}\nu; \qquad s^b_{\gamma-1} = 0,\ \gamma = 1,...,\nu.$$

Tutaq ki, bütün mümkün bazis sindrom çoxhədlilərinin sayı M ədədinə bərabərdir və $S^{(\beta)}_\alpha, \alpha = 0,1,...,n-k-1$, və $e^{(\beta)}_\alpha,\ \alpha = 0,1,...,n-1$, uyğun olaraq β -cı bazis sindrom çoxhədlisinin və β -cı səhv çoxhədlisinin əmsallarıdır. $s^b(x)$ bazis sindrom çoxhədlisinin əmsallarına görə cədvəldən uyğun səhv çoxhədlisinin nömrəsi aşağıdakı rekurrent sxemlə tapılır:

$$\begin{cases} P_\beta = \prod_{\alpha=0}^{n-k-1}\left(s^b_\alpha + S^{(\beta)}_\alpha + 1\right),\quad GF(2),\quad \beta = 1,...,M; \\ \beta = 1,\ p = 1; p := p(P_\gamma + 1),\ GF(2),\quad \beta := \beta + p,\quad \gamma = 1,...,M. \end{cases} \tag{9}$$

Sonda β -nın qiyməti cədvəldə $s^b(x)$ ilə eyni olan bazis sindrom çoxhədlisinin nömrəsi olar. $e^{(\beta)}(x) = e^{(\beta)}_{n-1}x^{n-1} + ... + e^{(\beta)}_0$ isə səhv çoxhədlisi olar. $\nu = 0$ olduqda $e_\alpha = e^{(\beta)}_\alpha,\ \alpha = 0,1,...,n\text{-}1$, qəbul edilir. $\nu \geq 1$ olduqda $s(x)$ -ə uyğun $e(x)$ çoxhədlisinin əmsalları aşağıdakı kimi götürülür:

$$e_\alpha = e^{(\beta)}_{\nu+\alpha},\ \alpha = 0,1,...,n\text{-}1\text{-}\nu;\ e_{n-\nu+\alpha} = e^{(\beta)}_\alpha,\ \alpha = 0,1,...,\nu\text{-}1. \tag{10}$$

$e(x)$ çoxhədlisi tapıldıqdan sonra $\upsilon(x)$ çoxhədlisində $\upsilon_\alpha := \upsilon_\alpha + e_\alpha$, $GF(2),\ \alpha = 0,1,...,n\text{-}1,$ düsturu ilə düzəliş edilir. Sonra, $\upsilon(x)$ çoxhədlisi $g(x)$ çoxhədlisinə aşağıdakı ikilik XAM-ı istifadə etməklə bölünür:

$$\begin{cases} y_\alpha[0] = \upsilon_\alpha,\ \alpha = 0,1,...,n-1; \\ y_{n-\beta-\alpha}[\beta] = y_{n-\beta-\alpha}[\beta-1] + y_{n-\beta}[\beta-1]g_{n-k-\alpha},\ \alpha = 1,...,n-k,\ GF(2), \\ y_{n\text{-}\beta\text{-}\alpha}[\beta] = y_{n\text{-}\beta\text{-}\alpha}[\beta\text{-}1],\ \alpha = n\text{-}k+1,...,n\text{-}\beta, \\ I_{k-\beta}[\beta] = y_{n-\beta}[\beta\text{-}1],\ \beta = 1,2,...,k\text{-}1; \\ y_{n-k-\alpha}[k] = y_{n-k-\alpha}[k-1] + y_{n-k}[k-1]g_{n-k-\alpha},\ \alpha = 1,...,n-k,\ GF(2); \\ I_o[k] = y_{n-k}[k-1]. \end{cases} \tag{11}$$

Beləliklə, $i=(i_0,i_1,...,i_{k-1})$ informasiya vektorunun aşağıdakı kimi tapılır

$$i_{k-\beta}=I_{k-\beta}[\beta],\quad \beta=1,2,...,k. \tag{12}$$

2.5 yarımfəslində ikilik olmayan dövri kodlar halında qəbul edilən sözlərdə Meqqitt teoreminə əsaslanan üsulla səhvlərin aşkarlanması və düzəldilməsi prosesinin XAM-lar sinfində təsvirinə baxılır.

Üçüncü fəsil BÇX kodlarının ötürülməsi zamanı yaranan səhvlərin aşkarlanması və düzəldilməsi üçün PQÇ alqoritminin effektiv reallaşdırılmasına həsr olunur. Burada **3.1 yarımfəslində** BÇX kodlarının qurulması qaydası və bu kodların ötürülməsi zamanı yaranan səhvlərin aşkarlanması və düzəldilməsi üçün PQÇ alqoritmi şərh olunur.

İkilik BÇX kodlarının ötürülməsi zamanı yaranan səhvlərin aşkarlanması və düzəldilməsi üçün Piterson alqoritminin effektiv reallaşdırılmasına **3.2 yarımfəslində** baxılır. 3.2.1 altyarımfəslində Piterson alqoritminin Qauss üsulu əsasında modifikasiyası verilir. Tutaq ki, $GF(2^m)$ meydanında α primitiv elementdir. t sayda səhvi düzəldən n- uzunluqlu BÇX kodu $g(x)=\text{ƏKOB}[f_1(x),...,f_{2t}(x)]$ əmələgətirici çoxhədlili dövri koddur. Burada $f_\beta(x)$ çoxhədlisi $\alpha^\beta\in GF(2^m)$ elementinin minimal çoxhədlisidir, $\beta=\overline{1,2t}$. Tutaq ki, $k=n-\deg g(x)$ və $i=(i_0,...,i_{k-1})$ vektoru $GF(2)$ üzərində k - ölçülü informasiya vektorudur. $i(x)$ informasiya çoxhədlisi $c(x)=i(x)g(x)$ düsturu ilə $c(x)$ kod çoxhədlisinə kodlaşdırılır. Burada n, k və t ədədləri üçün $2t\le n-k$ şərti ödənilməlidir. Tutaq ki, RK ilə $c(x)$ çoxhədlisi ötürülmüş, kanalın digər ucunda $\upsilon(x)$ qəbul edilmişdir. $e(x)=\upsilon(x)+c(x)$, $GF(2)$, səhv çoxhədlisində isə t-dən çox olmayan sayda əmsal sıfırdan fərqlidir. Tutaq ki, baxılan anda ν sayda səhv baş vermişdir ($0\le\nu\le t$, ν ədədi də naməlumdur) və həmin səhvlərə naməlum $p_1,p_2,...,p_\nu$ mövqeləri uyğundur. Bu halda $e(x)$ səhv çoxhədlisi $e(x)=x^{p_1}+...+x^{p_\nu}$ şəklində yazıla bilər. Səhvləri tapmaq üçün naməlum kəmiyyətlər tapılmalıdır. Onları tapmaq üçün Piterson üsuluna görə aşağıdakı kimi hesablanan sindrom komponentləri istifadə olunur:

$$S_\beta=\upsilon(\alpha^\beta)=e(\alpha^\beta)=(\alpha^{p_1})^\beta+(\alpha^{p_2})^\beta+...+(\alpha^{p_\nu})^\beta. \tag{13}$$

$S_\beta=0$, $\beta=\overline{1,2t}$, olarsa, onda $\upsilon(x)$ çoxhədlisində səhv yoxdur. $X_\ell=\alpha^{p_\ell}$ səhvin lokatoru kəmiyyətləri daxil edilir ($\ell=\overline{1,\nu}$). $\beta\in\{1,...,2t\}$ olmaqla $S_\beta=X_1^\beta+X_2^\beta+...+X_\nu^\beta$ -dən $X_1,...,X_\nu$ lokatorlarına nəzərən aşağıdakı

qeyri-xətti cəbri tənliklər sistemi (QXCTS) alınır

$$S_\beta = X_1^\beta + X_2^\beta + ... + X_\nu^\beta , \quad \beta = \overline{1,2t} . \tag{14}$$

(14) QXCTS- ni həll etmək üçün kökləri $X_1^{-1},..,X_\nu^{-1}$ kəmiyyətləri hesab olunan $\Lambda(x) = \Lambda_\nu x^\nu + ... + \Lambda_1 x + 1$ səhvlər lokatoru çoxhədlisi istifadə olunur. Bu çoxhədlinin əmsalları məlum olduqda, səhvlər lokatorunu tapmaq üçün onun köklərini tapmaq lazımdır. Sindrom komponentləri və əmsallar arasında əlaqə aşağıdakı düstur vasitəsilə verilir.

$$A\,col(\Lambda_\nu, \Lambda_{\nu-1},...,\Lambda_1) = col(S_{\nu+1}, S_{\nu+2},...,S_{2\nu}) \tag{15}$$

Burada $A = (a_{\rho,\beta})$, $\rho,\beta = \overline{1,\nu}$, ($a_{\rho,\beta} = S_{\rho-1+\beta}$). A matrisi cırlaşmayandırsa, onda (15) XCTS-nin $\Lambda_1, \Lambda_2,...,\Lambda_\nu$ məchullarına nəzərən yeganə həlli olar.

Piterson alqoritminin Qauss üsulu əsasında modifikasiyası:

Addım 1. $S_\beta = \upsilon(\alpha^\beta)$-nı hesablamalı ($\beta = \overline{1,2t}$). $\nu = t$.

Addım 2. Əgər $A = (a_{\rho,\beta}), \rho,\beta = \overline{1,\nu}$, matrisində, harada ki, $a_{\rho,\beta} = S_{\rho-1+\beta}$, sıfıra bərabər sətir və ya sütun vardırsa, onda addım 4-ə keçməli, əks halda aşağıdakı XCTS-ni üçbucaq şəklinə gətirməli

$$A\,col(\Lambda_\nu, \Lambda_{\nu-1},...,\Lambda_1) = col(S_{\nu+1}, S_{\nu+2},...,S_{2\nu}) . \tag{16}$$

Addım 3. Əgər A matrisi cırlaşandırsa, onda addım 4-ə, əks halda addım 5-ə keçməli.

Addım 4. $\nu := \nu - 1$. Addım 2-yə keçməli.

Addım 5. $A_1 col(\Lambda_\nu, \Lambda_{\nu-1},..., \Lambda_1) = b$ XCTS-ni həll edib $\Lambda_1, \Lambda_2,...$ $,\Lambda_\nu$ əmsallarını tapmalı. Burada b vektoru (16) XCTS-ni üçbucaq şəklinə gətirdikdə $col(S_{\nu+1}, S_{\nu+2},...,S_{2\nu})$ sütun vektorundan alınır , A_1 matrisi isə A matrisinin üçbucaq şəklidir.

Addım 6. $\Lambda(x)$ çoxhədlisinin $x_1,...,x_\nu$ köklərini və $X_\beta = x_\beta^{-1}$, $\beta = 1,...,\nu$, düsturu ilə səhvlər lokatorunu tapmalı.

Addım 7. $p_1,...,p_\nu$ - qüvvət ($\ell = 1,...,\nu$) dərəcələrinin qiymətlərini

$$p_\ell = \begin{cases} -1, & X_\ell = 0, \\ \sigma, & X_\ell = \alpha^\sigma, \ \sigma \in \{0,...,2^m - 2\} \end{cases} \tag{17}$$

düsturu ilə tapmalı və baş verən səhvləri $\upsilon_{p_\ell} := \upsilon_{p_\ell} + 1$, $\ell = 1,...,\nu$, $GF(2)$, düsturu ilə düzəltməli və $i(x) = \upsilon(x) / g(x)$ düsturu ilə $i(x)$-i hesablamalı.

Addım 8. Son.

A matrisinin elementləri $GF(2^m)$ meydanından olan çoxhədlilərdir və sıfırdan fərqliləri α primitiv elementinin qüvvəti şəklində təsvir oluna bilir. $GF(2^m)$ meydanının elementləri üzərində cəbri əməlləri yerinə yetirəndə belə təsvirin qüvvət dərəcəsinə əsaslanan hazır əməllər cədvəlindən istifadə etməklə əməllərin yerinə yetmə vaxtını azaltmaq olar.

3.2.2 altyarımfəsildə yuxarıda verilən alqoritmin effektiv reallaşdırılmasına baxılır və səhvlərin aşkarlanması və düzəldilməsi üçün $GF(2^m)$ meydanının elementləri əvəzinə elementlərin uyğun qüvvət dərəcəsinin və ya -1-in (0 elementi əvəzinə) istifadə edilməsinə əsaslanan metodika işlənilir. Burada $S_1,...,S_{2t}$ komponentləri üçün $N_1,...,N_{2t}$ ədədləri daxil edilir: əgər $S_\beta = \alpha^k$, $k \in \{0,...,2^m - 2\}$, onda $N_\beta = k$, əks halda $N_\beta = -1$. N_β, $\beta = \overline{1,2t}$, ədədlərini tapmaq üçün üçdəyişənli $M1$ və ikidəyişənli $M2$ funksiyaları (massivləri) və $*$ əməli əsasında alqoritm verilir. $M1$ -in $M1(u,\beta,\nu)$ və $M2$ -in $M2(\tau,\nu)$ elementləri və $x*y$ uyğun olaraq $u+\alpha^\beta \nu$, $\alpha^\tau + \nu$ və $\alpha^x \alpha^y$ ifadələrinin α primitiv elementin qüvvəti şəkində təsvirlərindəki qüvvət dərəcələrini göstərir, harada ki, $u,\upsilon \in GF(2)$, $\beta \in \{0,...,2^m - 2\}$, $x,y,\tau \in \{-1,0,...,2^m - 2\}$.

(16) XCTS-nin üçbucaq şəklinə gətirilməsi üçün A matrisi və $b = col(S_{\nu+1},...,S_{2\nu})$ vektoru üzərində çevirmələr aparılır. Hər bir addımda A matrisinin çevrilməsi zamanı alınan matrisdə sıfır sətir (sütun) varsa, onda (16) XCTS-nin üçbucaq şəklinə gətirilməsi dayandırılır, əks halda proses davam etdirilir və i.a. Tutaq ki, $(\nu-1)$ – ci addımda

$$A^{(\nu-1)} = \begin{pmatrix} a_{11} & a_{12} & a_{13} & ... & a_{1\nu} \\ 0 & a'_{22} & a'_{23} & ... & a'_{2\nu} \\ ..... & ..... & ..... & ..... & ..... \\ 0 & 0 & 0 & ... & a^{(\nu-1)}_{\nu\nu} \end{pmatrix}, \; b^{(\nu-1)} = \begin{pmatrix} b_1 \\ b'_2 \\ \vdots \\ b^{(\nu-1)}_\nu \end{pmatrix}$$

matris və vektoru alınır, harada ki,

$$a'_{\rho\beta} = a_{\rho\beta} a_{11} + a_{1\beta} a_{\rho 1}, \quad \beta = 2,...,\nu; \quad \rho = 2,...,\nu, \tag{18}$$

$$b'_\rho = b_\rho a_{11} + b_1 a_{\rho 1}, \quad \rho = 2,...,\nu. \tag{19}$$

$$a^{(\ell)}_{\rho\beta} = a^{(\ell-1)}_{\rho\beta} a^{(\ell-1)}_{\ell\ell} + a^{(\ell-1)}_{\ell\beta} a^{(\ell-1)}_{\rho\ell}, \; \beta = \ell+1,...,\nu; \; \rho = \ell+1,...,\nu;$$

$$b^{(\ell)}_\rho = b^{(\ell-1)}_\rho a^{(\ell-1)}_{\ell\ell} + b^{(\ell-1)}_\ell a^{(\ell-1)}_{\rho\ell}, \; \rho = \ell+1,...,\nu; \; \ell = 2,...,\nu-1. \tag{20}$$

$A^{(\nu-1)}$ matrisində $a_{11} \neq 0$, $a'_{22} \neq 0$,..., $a^{(\nu-2)}_{\nu-1,\nu-1} \neq 0$. Əgər $a^{(\nu-1)}_{\nu,\nu} = 0$ olarsa, onda $A^{(\nu-1)}$ cırlaşandır və ν -nün cari qiymətində (16) məsələsinin həlli yoxdur. $a^{(\nu-1)}_{\nu,\nu} \neq 0$ olduqda isə (16) məsələsinin həllinin tapılması aşağıdakı məsələnin həllinin tapılmasına gəlir:

$$A^{(\nu-1)} \cdot col\left(\Lambda_\nu, \Lambda_{\nu-1},..., \Lambda_1\right) = b^{(\nu-1)}. \qquad (21)$$

(21) XCTS-nin həlli aşağıdakı rekurrent düsturla tapıla bilər:

$$\Lambda_1 = \left(a^{(\nu-1)}_{\nu\nu}\right)^{-1} \cdot b^{(\nu-1)}_\nu \ , \qquad (22)$$

$$\Lambda_\rho = \left(a^{(\nu-\rho)}_{\nu-\rho+1,\nu-\rho+1}\right)^{-1} \left\{ b^{(\nu-\rho)}_{\nu-\rho+1} + \sum_{\sigma=1}^{\rho-1} a^{(\nu-\rho)}_{\nu-\rho+1,\nu-\rho+1+\sigma} \Lambda_{\rho-\sigma} \right\}, \ \rho = 2,3,...,\nu \ . \qquad (23)$$

(18)-(23) düsturlarında çoxhədlilər əvəzinə α primitiv elementinin uyğun qüvvətindəki qüvvət dərəcələrinin istifadəsi üçün A matrisi əsasında $Z = (z_{\rho\beta})$, $\rho, \beta = \overline{1,\nu}$, matrisi, b vektoru əsasında $\eta = col(\eta_1,...,\eta_\nu)$ vektoru daxil edilir. Burada $z_{\rho\beta}, \eta_\rho, z^{(\ell)}_{\rho\beta}$ və $\eta^{(\ell)}_\rho$ kəmiyyətləri (17) düsturuna analoji düsturla uyğun olaraq $a_{\rho\beta}$, b_ρ , $a^{(\ell)}_{\rho\beta}$ və $b^{(\ell)}_\rho$ kəmiyyətləri vasitəsilə təyin olunurlar və $z_{\rho\beta} = N_{\rho\text{-}1+\beta}$, $\eta_\rho = N_{\rho+\nu}$. (21)-(22)-dən alınır:

$$z'_{\rho\beta} = MC(z_{\rho\beta} * z_{11}, z_{1\beta} * z_{\rho 1}) , \ \beta = \overline{2,\nu} , \ \rho = \overline{2,\nu} ,$$

$$\eta'_\rho = MC(\eta_\rho * z_{11}, \eta_1 * z_{\rho 1}) , \ \rho = \overline{2,\nu} ,$$

$$z^{(\ell)}_{\rho\beta} = MC(z^{(\ell-1)}_{\rho\beta} * z^{(\ell-1)}_{\ell\ell}, z^{(\ell-1)}_{\ell\beta} * z^{(\ell-1)}_{\rho\ell}) , \ \beta = \ell+1,...,\nu; \ \rho = \ell+1,...,\nu ,$$

$$\eta^{(\ell)}_\rho = MC(\eta^{(\ell-1)}_\rho * z^{(\ell-1)}_{\ell\ell}, \eta^{(\ell-1)}_\ell * z^{(\ell-1)}_{\rho\ell}) , \ \rho = \ell+1,...,\nu , \ell = 2,...,\nu-1.$$

Burada $MC(x,y)$ ilə $\alpha^x + \alpha^y$ ifadəsinin $GF(2^m)$ meydanının α primitiv elementinin qüvvəti şəklində təsvirindəki qüvvət dərəcəsi göstərilir.

(22), (23) düsturlarından alınır ki, $\lambda_1 = (2^m - 1 - z^{(\nu-1)}_{\nu\nu}) * \eta^{(\nu-1)}_\nu$,

$$\lambda_\rho = (2^m - 1 - z^{(\nu-1)}_{\nu-\rho+1,\nu-\rho+1}) * MC(\eta^{(\nu-\rho)}_{\nu-\rho+1}, \gamma_\rho) , \ \rho = 2,3,...,\nu ,$$

harada ki, λ_ρ ədədi (17) düsturuna analoji düsturla Λ_ρ kəmiyyəti əsasında təyin olunur, γ_ρ isə rekurrent olaraq aşağıdakı kimi hesablanır:

$$\gamma_\rho := -1; \ \gamma_\rho := MC(\gamma_\rho, z^{(\nu-\rho)}_{\nu-\rho+1,\nu-\rho+1+\sigma} * \lambda_{\rho-\sigma}) , \ \sigma = 1,..., \rho\text{-}1.$$

Məlum $\Lambda_1, \Lambda_2,..., \Lambda_\nu$ əmsalları halında $\Lambda(x)$-in köklərini tapmaq üçün hər bir $x \in GF(2^m)$ üçün $\Lambda(x)$- i hesablamaq və $\Lambda(x) = 0$ şərtini ödəyən x -

ləri ayırmaq lazımdır. $x \in GF(2^m)$ üçün $\Lambda(x)$ rekurrent olaraq aşağıdakı ardıcıllıqla hesablanır:

$\Lambda_0 := 1,\ \Lambda(x) := \Lambda_\nu x + \Lambda_{\nu-1};\quad \Lambda(x) := \Lambda(x)\cdot x + \Lambda_\ell,\ \ \ell = \nu-2, \nu-3,...,0.$

Hesablamaları sürətləndirmək üçün x-in əvəzinə onun $x = \alpha^\beta$ şəkilindəki təsvirini istifadə etmək olar. Onda sonuncu sxemi

$$\lambda_0 := 0,\ \lambda(\beta) := MC((\lambda_\nu * \beta), \lambda_{\nu-1}),$$
$$\lambda(\beta) := MC((\lambda(\beta) * \beta), \lambda_\ell),\ \ell = \nu-2, \nu-3,...,0,$$

kimi yazmaq olar, harada ki, $\lambda(\beta)$ kəmiyyəti (17) düsturuna analoji düsturla $\Lambda(\alpha^\beta)$ kəmiyyəti əsasında təyin olunur.

3.2.3 altyarımfəslində təklif olunan metodikaların effektivliyi, yəni səhvlərin daha cəld aşkarlanaraq düzəldilməsi əsaslandırılır. 3.2.4 altyarımfəslində qəbul edilən çoxhədlilərdə səhvlərin aşkarlanması, düzəldilməsi və informasiyanın ayrılması üçün aşağıdakı ətraflı alqoritmi verilir:

Addım 0. $\upsilon_{n-1}, \upsilon_{n-2}, ..., \upsilon_1, \upsilon_0$ -ların daxil edilməsi. $\beta = 1$.

Addım 1. $N_\beta = M1(\upsilon_{n-1}, \beta, \upsilon_{n-2})$, $\gamma = 1$.

Addım 2. $N_\beta := M2((N_\beta * \beta), \upsilon_{n-2-\gamma})$.

Addım 3. $\gamma := \gamma + 1$. Əgər $n - 2 - \gamma \geq 0$ olarsa, onda addım 2-yə, əks halda addım 4-ə keçməli.

Addım 4. $\beta := \beta + 1$. Əgər $\beta \leq 2t$ olarsa, onda addım 1-ə, əks halda addım 5-ə keçməli.

Addım 5. Əgər $N_1, N_2, ..., N_{2t}$ ədədlərinin hamısı -1-ə bərabərdirsə, onda addım 36-ya, əks halda addım 6-ya keçməli.

Addım 6. $\nu = t$.

Addım 7. $D = (z_{\rho\beta})$, $\rho, \beta = \overline{1,\nu}$, və $\eta = (\eta_1, \eta_2, ..., \eta_\nu)$ qəbul etməli, harada ki, $z_{\rho\beta} = N_{\rho\text{-}1+\beta}$, $\rho, \beta = \overline{1,\nu}$; $\eta_\rho = N_{\rho+\nu}$, $\rho = \overline{1,\nu}$.

Addım 8. $\ell = 1$.

Addım 9. Əgər $D_1 = (z_{\rho\beta})$, $\rho = \overline{\ell,\nu}$, $\beta = \overline{\ell,\nu}$, matrisində ancaq sıfırlardan ibarət sətir və ya sütun vardırsa, onda addım 19-a keçməli, əks halda $\sigma = \min\{\xi | \xi \in \{\ell, ..., 1\}, z_{\xi\ell} \neq -1\}$ hesablamalı. Əgər $\sigma \neq \ell$ olarsa, onda addım 10-a, əks halda addım 13-ə keçməli.

Addım 10. $\beta = \ell$.

Addım 11. Ardıcıl olaraq $c = z_{\ell\beta}$, $z_{\ell\beta} = z_{\sigma\beta}$, $z_{\sigma\beta} = c$ qəbul etməli.

Addım 12. $\beta := \beta + 1$. Əgər $\beta \le \nu$ olarsa, onda addım 11-ə, əks halda $c = \eta_\ell$, $\eta_\ell = \eta_\sigma$, $\eta_\sigma = c$ qəbul etməli və sonra addım 13-ə keçməli.

Addım 13. $\rho = \ell + 1$. Əgər $\rho > \nu$ olarsa, onda addım 18-ə, əks halda addım 14-ə keçməli.

Addım 14. $\beta = \ell$, $c = z_{\rho\ell}$.

Addım 15. Qəbul etməli: $z_{\rho\beta} := MC(z_{\rho\beta} * z_{\ell\ell}, z_{\ell\beta} * c)$.

Addım 16. $\beta := \beta + 1$. Əgər $\beta \le \nu$ olarsa, onda addım 15-ə keçməli, əks halda $\eta_\rho := MC(\eta_\rho * z_{\ell\ell}, \eta_\ell * c)$ qəbul etməli və addım 17-yə keçməli.

Addım 17. $\rho := \rho + 1$. Əgər $\rho \le \nu$ olarsa, onda addım 14-ə, əks halda addım 18-ə keçməli.

Addım 18. $\ell := \ell + 1$. Əgər $\ell < \nu$ olarsa, onda addım 9-a keçməli, əks halda $z_{\nu\nu}$ -nün qiymətini yoxlamalı. Əgər $z_{\nu\nu} = -1$ olarsa, onda addım 19-a, əks halda addım 20-yə keçməli.

Addım 19. $\nu := \nu - 1$. Addım 7-yə keçməli.

Addım 20. $\lambda_1 = (2^m - 1 - z_{\nu\nu}) * \eta_\nu$.

Addım 21. $\rho := 2$.

Addım 22. $\gamma := -1$; $\sigma = 1$.

Addım 23. $\gamma := MC(\gamma, z_{\nu-\rho+1,\nu-\rho+1+\sigma} * \lambda_{\rho-\sigma})$.

Addım 24. $\sigma := \sigma + 1$. Əgər $\sigma \le \rho - 1$ olarsa, onda addım 23-ə, əks halda addım 25-ə keçməli.

Addım 25. $\lambda_\rho := (2^m - 1 - z_{\nu-\rho+1,\nu-\rho+1}) * MC(\eta_{\nu-\rho+1}, \gamma)$.

Addım 26. $\rho := \rho + 1$. Əgər $\rho \le \nu$ olarsa, onda addım 23-ə, əks halda addım 27-ə keçməli.

Addım 27. $\beta = -1$, $\lambda_0 = 0$, $\sigma = 0$.

Addım 28. $\lambda(\beta) := MC((\lambda_\nu * \beta), \lambda_{\nu-1})$, $\ell = \nu - 2$.Əgər $\ell < 0$ olarsa, onda addım 31-ə, əks halda addım 29-a keçməli.

Addım 29. $\lambda(\beta) := MC((\lambda(\beta) * \beta), \lambda_\ell)$.

Addım 30. $\ell := \ell - 1$. Əgər $\ell \ge 0$ olarsa, onda addım 29-a, əks halda addım 31-ə keçməli.

Addım 31. Əgər $\lambda(\beta) \ne -1$ olarsa, onda addım 33-ə, əks halda addım 32-yə keçməli.

Addım 32. $\sigma := \sigma + 1$, $x_\sigma = \beta$. Əgər $\sigma \ge \nu$ olarsa, onda addım 34-ə, əks halda addım 33-ə keçməli.

Addım 33. $\beta := \beta + 1$. Əgər $\beta \le 2^m - 2$ olarsa, onda addım 28-ə, əks halda addım 34-ə keçməli.

Addım 34. Hər bir $\ell = 1,...,\nu$ üçün qəbul etməli: $p_\ell = 2^m - 1 - x_\ell$.

Addım 35. Qəbul etməli: $\upsilon_{p_\ell} := \upsilon_{p_\ell} + 1$, $GF(2)$, $\ell = 1,...,\nu$.

Addım 36. İnformasiya vektorunu (11),(12) düsturu ilə tapmalı.

Addım 37. Son.

3.2.5 altyarımfəslində Piterson alqoritminin modifikasiyasının və daha tez hesablamaların təmin edilməsi metodikasının konkret nümunəyə tətbiqi verilir və bu nümunə halında göstərilir ki, səhvlər Piterson alqoritminə nisbətən 9 dəfədən də tez vaxta tapılaraq düzəldilir.

3.3 yarımfəslində ikilik olmayan BÇX kodlarının ötürülməsi zamanı səhvlərin aşkarlanması və düzəldilməsi üçün PQÇ alqoritminin effektiv reallaşdırılması şərh olunur.

Nəticədə işdə alınan əsas nəticələr şərh olunur.

İşdə alınan əsas nəticələr aşağıdakılardan ibarətdir:

- İkilik xətti blok kodların ötürülməsi zamanı baş verən səhvlərin SDQ əsasında aşkarlanaraq düzəldilməsi prosesinin effektiv reallaşdırılması metodikası işlənilmişdir;
- İkilik olmayan dövri kodların ötürülməsi zamanı yaranan səhvlərin cədvəl üsulu əsasında aşkarlanaraq düzəldilməsi və informasiya sözünün ayrılması prosesinin XAM-lar sinfində modeli verilmişdir;
- İkilik və ikilik olmayan dövri kodların ötürülməsi zamanı yaranan səhvlərin Meqqitt teoremi əsasında aşkarlanması, düzəldilməsi və informasiya sözünün ayrılması prosesinin XAM-lar sinfində modeli verilmişdir;
- BÇX kodlarının ötürülməsi zamanı səhvlərin aşkarlanması və düzəldilməsi üçün Piterson və PQÇ alqoritmlərinin Qauss üsulu əsasında modifikasiyası və onun effektiv reallaşdırılması metodikası verilmişdir.

Dissertasiyanın əsas nəticələri aşağıdakı elmi işlərdə dərc olunmuşdur:

1. M.A.Babavənd. p -lik dövri kodlarda Meqqitt teoremi əsasında səhvlərin aşkarlanması və düzəldilməsi prosesinin ardıcıllıqlı maşınlar sinfində təsviri. «Riyaziyyatın tətbiqi məsələləri və yeni informasiya texnologiyaları» II Respublika Elmi Konfransının materialları (Sumqayıt, SDU, 27-28 noyabr, 2012). C. 48-50.

2. M.A.Babavənd. İkilik olmayan Bouz-Çoudxuri-Xokvinqem kodları üçün Piterson-Qorensteyn-Çirler alqoritminin bir effektiv realizasiyası.

Riyaziyyat və Mexanika İnstitutunun 55 illiyinə həsr olunmuş "Riyaziyyat və Mexanikanın aktual problemləri" Beynəlxalq konfransının materialları (Bakı, 15-16 may, 2014). S.100-102.

3. M.A.Babavənd. İkilikolmayan dövri kodlar halında qəbul edilən məlumatlarda səhvlərin aşkarlanması və düzəldilməsi prosesinin ardıcıllıqlı maşınlar sinfində təsviri// Sumqayıt Dövlət Universitetinin Elmi xəbərləri, Təbiət və texniki elmlər bölməsi, C. 14, 2014, № 1, S. 73-77.

4. F.G.Feyziyev, M.A.Babavənd. Verilən sayda təhrifləri aşkarlaya və düzəldə bilən ikilik xətti kodların qurulması və onların tətbiqi// SDU-nun Elmi xəbərləri, Təbiət və texniki elmlər bölməsi, C.11, 2011, №1, S. 15-22.

5. F.G.Feyziyev, L.M.Ramazanova, M.A.Babavənd. Description of Encoding and Decoding of Binary Cyclic Codes in a Class Sequential Machines. Proceedings of IV International Conference "Problems of cybernetics and informatics (PCI`2012, September 12-15, 2012, Baku, Azerbaijan)". V. 1, pp. 249-251.

6. Ф.Г.Фейзиев, М.А.Бабаванд. Описание декодирования циклических кодов в классе последовательностных машин, основанного на теореме Меггитта// г. Рига, Автоматика и вычислительная техника, Т. 46, № 4, 2012. С. 26-33 (F.G.Feyziyev, M.A.Babavənd. Description of Decoding of Cyclic codes in the Class of Sequential Machines Based on the Meggitt Theorem// Automatic Control and Computer Sciences,2012,Vol 46, No 4, Allerton Press, Inc.,2012. pp.164-169).

7. Ф.Г.Фейзиев, М.А.Бабаванд К вопросу увеличения скорости выполнение алгоритма Питерсона-Горенстейна-Цирлера для двоичных кодов Боуза-Чоудхури-Хогвингема. «Riyaziyyatın tətbiqi məsələləri və yeni informasiya texnologiyaları» II Respublika Elmi Konfransının materialları (Sumqayıt, SDU, 27-28 noyabr, 2012). С. 57-59.

8. Ф.Г.Фейзиев, М.А.Бабаванд Араблу. Описание декодирования р-ичных циклических кодов в классе последовательностных машин// Изв. НАНА, Сер. физ.-техн. и мат. наук: Информатика и проблемы управления, 2012, Т. XXXII, № 6. С. 3-9.

9. Ф.Г.Фейзиев, М.А.Бабаванд. Об одной реализации алгоритма Питерсона-Горенстейна-Цирлера для двоичных кодов// SDU-nun Elmi xəbərləri, Təbiət və texniki elmlər bölməsi, C. 13, 2013, № 3, S.22-26.

10. Ф.Г.Фейзиев, М.А.Бабаванд. Об одной реализации алгоритма Питерсона-Горенстейна-Цирлера для q-ичных кодов// Sumqayıt Dövlət Universitetinin Elmi xəbərləri, Təbiət və texniki elmlər bölməsi, C. 13, 2013, № 4, S.3-7.

11. Ф.Г.Фейзиев, М.А.Бабаванд. Об одной эффективной реализации алгоритма Ритерсона-Горенстейна-Цирлера для q - ичных кодов БоузаЧоудхури-Хоквингема// Изв.НАНА, Сер. физ.-техн. и мат. наук: Информатика и проблемы управления, 2013, Т. XXXIII, № 6. С. 39-51.

12. F.G.Feyziyev, M.A.Bababənd. “Riyaziyyat və İKT-nin tətbiq sahələri. Yeni tədris texnologiyaları” Beynəlxalq Konfransının maerialları (Gəncə, GDU, 05-06 iyun 2014). II hissə, S.38-41.

13. Mehrdad A. Babavand Arablou, Fikrat G. Feyziyev. On One Modifica-tion of Algorithm Peterson-Gorenstein-Zierler and its Effective Realization// J. of Univrtsitety Malaysia Pahang, Vol. 3, Issue. 3, Supp. 1, 2015, pp. 483-491.

Müştərək müəlliflərlə yerinə yetirilən işlərdə iddiaçının rolu:

[4-13] işlərində əsas düsturların çıxarışı, alqoritmlərin qurulması, əsaslandırılması və yoxlanması iddiaçıya məxsusdur.

БАБАВАНД АРАБЛОУ МЕГРДАД АСЛАН оглы

ЭФФЕКТИВНЫЕ РЕАЛИЗАЦИИ АЛГОРИТМОВ ОБНАРУЖЕНИЯ И ИСПРАВЛЕНИЯ ОШИБКИ В БЛОКОВЫХ КОДАХ, КОНТРОЛИРУЮЩИХ ОШИБКИ

РЕЗЮМЕ

Диссертационная работа посвящена эффективной реализации правила стандартного расположения для декодирование линейных кодов, разработке модификации алгоритма Ритерсона-Горенстейна-Цирлера (РГЦ), основанной на методе Гаусса и описанию обнаружения и исправления ошибок при передаче циклических кодов в классе последовательностных машин.

Научная новизна работы состоит из предложенных модификаций алгоритма РГЦ, методики для эффективной реализации правила стандартного расположения и модификации алгоритма РГЦ, формулы описания декодирования циклических кодов в классе последовательностных машин. Результаты, полученные в диссертационной работе, опубликованы в 13 научных работах.

Диссертация состоит из введения, трех глав, заключения и списка литературы.

Первая глава посвящена изложению методов и средств обнаружения и исправления ошибок в блоковых кодах, контролирующих ошибки.

Во второй главе излагается эффективная реализация обнаружения и исправления ошибок в принятом слове в случае передачи двоичных линейных кодов. Рассматривается описание в классе последовательностных машин процесса обнаружения и исправления ошибок в принятом слове, в случае передачи циклических кодов, по методу, основанному на синдромной таблице и по методу, основанному на теореме Меггитта.

В третьей главе рассматривается вопрос разработки модификации алгоритма Питерсона и алгоритма РГЦ на основе метода Гаусса для обнаружения и исправления ошибок при передаче двоичных и не двоичных кодов Боуза-Чоудхури-Хоквмнгема соответственно и их эффективной реализации.

В заключении приводятся основные результаты, полученные в диссертации.

BABAVAND ARABLOU MEHRDAD ASLAN oglu

EFFECTIVE REALIZATION OF ALGORITHMS FOR DETECTION AND CORRECTION OF AN ERROR IN BLOCK CODES ERROR CONTROL

SUMMARY

The dissertation work to the effective realization of the rules of the standard locations for decoding linear codes, working of modification of the Ritersona-Gorenstein-Zierler (RGZ) algorithm on the based of the Gauss method and the description of the detection and correction of errors in the transmission of cyclic codes in the class sequential machines is devoted.

Scientific innovation of work consists of the proposed modifications of the RGZ algorithm, techniques for the effective realization of the rules of the standard standard locations and modification the RGZ algorithm , formula describing the decoding of cyclic codes in the class of sequential machines.

The results obtained in the dissertation work, published in 13 scientific papers.

The dissertation consists of introduction, 3 charters, conclusion and references.

The first chapter is devoted to the presentation of methods and tools for detecting and correcting errors in Block Codes Error Control.

The second chapter the construction of binary codes, correction of a given number of errors is considered. The effective realization of detecting and correcting errors in the received word in the case of a transfer of binary linear codes is presentation. Description process detecting and correcting errors in the received word, in the case of transfer of cyclic codes, the method based on syndromic table and a method based on the theorem Meggitts in a class of sequential machines is considered.

The third chapter discusses working modification of the Peterson algorithm based on Gauss method for detecting and correcting errors in the transmission of binary and non-binary codes Bose-Chaudhuri-Hochquenghem codes, respectively, and their effective realization.

In conclusion the main results in dissertation are given.

НАЦИОНАЛЬНАЯ АКАДЕМИЯ НАУК АЗЕРБАЙДЖАНА
ИНСТИТУТ СИСТЕМ УПРАВЛЕНИЯ

На правах рукописи

МЕГРДАД АСЛАН оглы БАБАВАНД АРАБЛУ

ЭФФЕКТИВНЫЕ РЕАЛИЗАЦИИ АЛГОРИТМОВ ОБНАРУЖЕНИЯ И ИСПРАВЛЕНИЯ ОШИБКИ В БЛОКОВЫХ КОДАХ, КОНТРОЛИРУЮЩИХ ОШИБКИ

3338.01 – Системный анализ, управление и обработка информации

АВТОРЕФЕРАТ

диссертации на соискание ученой степени доктора философии по техническом наукам

Баку – 2016