

**AZƏRBAYCAN RESPUBLİKASI TƏHSİL NAZİRLİYİ
BAKİ DÖVLƏT UNİVERSİTETİ**

İNFORMATİKANIN NƏZƏRİ ƏSASLARI

fənnindən

PROQRAM

Bakı – 2017

**AZƏRBAYCAN RESPUBLİKASI TƏHSİL NAZİRLİYİ
BAKİ DÖVLƏT UNİVERSİTETİ**

**Tətbiqi riyaziyyat və kibernetika
fakültəsi
“Riyazi kibernetika”
kafedrası**

İxtisas: 050116 – İnformatika müəllimliyi

İPF-B11-İNFORMATİKANIN NƏZƏRİ ƏSASLARI

fənnindən

PROQRAM

Bakı Dövlət Universitetinin Qrif komissiyasının 22.05.18 tarixli 09 sayli iclasının qərarı ilə fənn proqramı kimi təsdiq edilmişdir

Bakı – 2017

Tərtib edənlər:

1. BDU Riyazi kibernetika kafedrasının müdiri, f.r.e.d., prof. K.B.Mənsimov.
2. BDU Riyazi kibernetika kafedrasının dosenti, f.r.e.n,dos S.T.Əliyeva
3. BDU Riyazi kibernetika kafedrasının b/m. N.X.Aslanova

Elmi redaktor:

BDU Riyazi kibernetika kafedrasının müdiri, f.r.e.d., prof. K.B.Mənsimov.

Rəyçilər:

1. SDU-nin “Diferensial tənliklər və optimallaşdırma” kafedrasının müdiri, prof. Feyziyev F.G.
2. BDU-nun “Riyazi kibernetika” kafedrasının dosenti, f.-r.e.n. Əhmədova J.B.

İPF-B11-İNFORMATIKANIN NƏZƏRİ ƏSASLARI

İzahat vərəqi

“İnformatikanın nəzəri əsasları” fənninin informatika müəllimliyi istiqaməti üzrə bakalavr hazırlığında aktuallığı və əhəmiyyəti ondan ibarətdir ki, bu fəndə İnformasiyanın işlənməsində istifadə olunan riyazi modellər və metodlar öyrənilir. “İnformatikanın nəzəri əsasları” fənni aşağıdakı bölmələrdən ibarətdir: sonlu avtomatlar nəzəriyyəsi; requlyar ifadələr və requlyar çoxluqlar ; kodlaşdırma nəzəriyyəsi və əlifba kodlaşdırılması ; informasiya nəzəriyyəsi, ədədlər nəzəriyyəsi və kriptografiyada istifadə edilən bəzi alqoritmlər.

“İnformatikanın nəzəri əsasları” fənninin əsas məqsədi tələbələrə informasiyanın işlənməsində istifadə olunan məsələlərin riyazi modellərini qurmaq, informasiyanın təhlükəsizliyi məsələsində istifadə olunan riyazi metodları öyrənmək, informasiyanın kodlaşması üsullarını (effektiv və kuyədavamlı), informasiyanın etibarlı ötürülməsi şərtlərini təyin etmək, ədədlər nəzəriyyəsinin bəzi üsullarından istifadə etmək, bu üsulların tətbiqinin aşılamaqdır.

“İnformatikanın nəzəri əsasları” fənni sonlu avtomatlar nəzəriyyəsi, riyazi məntiq, informasiya nəzəriyyəsi, kodlaşdırma nəzəriyyəsi, alqoritmlər nəzəriyyəsi, ədədlər nəzəriyyəsi kurslarına əsaslanır.

Fənnin mənimsənilməsi nəticəsində tələbələr

Bilməlidir:

- DSA və onun verilməsi qaydalarını;
- QSA və onun verilməsi qaydalarını;
- eyni bir dil üçün DSA və QSA-nın təyini və onlar arasında ekvivalent keçidi;
- dilin requlyar çoxluqlar, requlyar ifadələr vasitəsilə verilməsini;
- sonlu avtomatlardan requlyar ifadəyə keçidi və əksinə ,requlyar ifadədən sonlu avtomata keçidi;
- informasiyanın miqdarının ölçülməsini;
- kodlaşdırma üsullarını, Fano və Xafman üsullarını, əlifba kodlaşdırılmasının qurulmasını;
- Evklid alqoritmi və onun əsasında genişlənmiş Evklid alqoritmini;
- müqayisələr və müqayisələr sistemini, Qalıq haqqında Çin teoremini.

Bacarmalıdır:

- verilmiş dili tanıyan DSA-ın keçid diaqramını və keçid cədvəlini qurmağı;
- verilmiş dili tanıyan QSA-ın keçid diaqramını və keçid cədvəlini qurmağı;
- QSA-dan DSA-a alt coxluqların asan konstruksiyası əsasında keçidi;
- DSA-dan requlyar ifadəyə keçidi;
- requlyar ifadədən SA-a keçidi;
- qeyri-müəyyənlik ölçüsü –entropiyanın təyin olunmasını;
- Fano və Xafman metodları ilə kodlaşdırma sxeminin qurulmasını;
- Evklid alqoritmi və onun əsasında genişlənmiş Evklid alqoritminin köməyi ilə tənlik və tənliklər sisteminin həll olunmasını.

Yiyələnməlidir:

- eyni dili tanıyan DSA və QSA-nın qurulması qaydalarına;
- SA-dan requlyar ifadəyə və əksinə keçidin qurulması qaydalarına;
- ən sadə kodlarda səhvin düzəldilməsi qaydalarına;
- müqayisə və müqayisə sisteminin həll edilməsi qaydalarına.

Fənnin tədrisində mövzulara uyğun hazırlanmış slaydların nümayişi üçün noutbuk və proyektorun olması məqsədəuyğundur.

MÖVZULARIN SAATLAR ÜZRƏ PAYLANMASI

№	Mövzuların adı	Auditoriya saatlarının miqdarı	
		mühazirə	məşğələ
1.	Avtomatlar nəzəriyyəsinə giriş. Determinik sonlu avtomatlar (DSA). DSA-nın təyini.	2	1
2.	Qeyri-determinik sonlu avtomatlar (QSA). QSA-dan DSA-a ekvivalent keçid.	2	1
3.	Requlyar çoxluqlar, requlyar ifadələr və onların xassələri. Requlyar dillər və ifadələr.	2	1
4.	Qrammatika (əsas anlayışlar). SA ilə requlyar çoxluqlar arasında əlaqə	2	1
5.	Vəziyyətlərin kənarlaşdırılması üsulu ilə DSA-dan requlyar ifadəyə keçid.	2	1
6.	Requlyar ifadədən DSA-a keçid.	2	1
7.	İnformasiya nəzəriyyəsinin elementləri. Entropiya anlayışı.	2	1
8.	Kodlaşdırma nəzəriyyəsinin əsas anlayışları. Rabitə kanalının modeli. Sadə kodlar.	2	1
9.	Qrup, halqa, meydan anlayışları. Vektor fəzası.	2	1
10.	Xətti blok kodları. Xemminq kodları.	2	1
11.	Əlifba kodlaşdırmasının elementləri.	2	1
12.	Genişlənmiş Evklid alqoritmi və onun	2	1

	tərs modul qiymətinin hesablanmasına tətbiqi.		
13.	Müqayisələr və müqayisələr sistemi. Qalıq haqqında Çin teoremi.	2	1
14.	Eyler funksiyası, Eyer teoremi. Ferma teoremi.	2	1
15.	Kriptografiyanın əsas anlayışları. RSA algoritmi.	2	1

Mövzuların qısa məzmunu

Mövzu № 1. Avtomatlar nəzəriyyəsinə giriş. DSA-nın təyini .

Avtomatlar nəzəriyyəsinin tətbiq sahələri, avtomatlar həm riyazi model, həm də qurğu kimi verilir, avtomatlar nəzəriyyəsinin əsas anlayışları verilir, DSA-ın formal təyini, DSA-ın verilmə üsulları, genişlənmiş keçid funksiyası təyin olunur və dili tanıyan DSA-in keçid diaqramının qurulmasına aid məsələlər həll olunur. [1-10].

Mövzu № 2. Qeyri-determinik sonlu avtomatlar. QSA-dan DSA-a ekvivalent keçid.

QSA-ın formal təyini, QSA-ın verilmə üsulları, genişlənmiş keçid funksiyası təyin olunur, alt çoxluqların konstruksiyası üsulu ilə QSA-dan DSA-a ekvivalent keçid verilir, dili tanıyan QSA-ın keçid diaqramının qurulması və alt çoxluqların asan konstruksiyası üsulu

ilə QSA-dan DSA-ya ekvivalent keçidə aid məsələlər həll olunur. [1-10].

Mövzu № 3. *Requlyar çoxluqlar, requlyar ifadələr və onların xassələri. Requlyar dillər və ifadələr.*

Çoxluqlar üzərində bəzi əməllər təyin olunur, requlyar çoxluq və requlyar ifadələr formal olaraq təyin olunur, requlyar dillərə aid nümunələrə baxılır, requlyar ifadələrin xassələri verilir. [1-10].

Mövzu № 4. *Qrammatika (əsas anlayışlar). SA ilə requlyar çoxluqlar arasında əlaqə.*

Dilin tanıyıcı mexanizmi olan qrammatika izah olunur, qaydaların təyin olunmasına əsasən sağxətti qrammatika və requlyar qrammatikalar anlayışları daxil edilir, SA-dan sağxətti qrammatikaya keçid, dili doğuran requlyar qrammatikadan requlyar ifadəyə keçid göstərilir və məsələlər həll olunur. [1-10].

Mövzu № 5. *Vəziyyətlərin istisna üsulu ilə SA-dan requlyar ifadəyə keçid.*

DSA-ın keçid diaqramından istifadə edərək, aralıq vəziyyətlər kənarlaşdırılır, keçid diaqramında başlanğıc və məqbul vəziyyətlər qaldıqda requlyar ifadəyə keçid tətbiq edilir və məsələlər həll olunur. [1-10].

Mövzu № 6. Requlyar ifadədən DSA-a keçid.

Baza requlyar ifadələr üçün SA qurulur, sonra baza ifadələrdən istifadə edərək dillərin birləşməsi, konkatenasiyası və iterasiyasından alınan requlyar ifadələr üçün SA-lar qurulur. [1-10].

Mövzu № 7. *İnformasiya nəzəriyyəsinin elementləri. Entropiya anlayışı.*

İnformasiya nəzəriyyəsinin əsas elementləri haqqında məlumat verilir, kəsilməz və diskret informasiya anlayışları verilir, qeyri-müəyyənlik ölçüsü-entropiya anlayışı daxil edilir, informasiyanın ölçülməsi göstərilir və məsələlər həll olunur. [1-4, 6].

Mövzu № 8. *Kodlaşdırma nəzəriyyəsinin əsas anlayışları. Rabitə kanalının modeli. Sadə kodlar.*

Kodlaşdırma nəzəriyyəsinin əsas məsələsi izah olunur, əsas anlayışlar verilir, rabitə kanalının modeli verilir, komponentlər izah olunur, ən sadə kodlara aid nümunələr göstərilir və məsələlər həll olunur. [1-4, 6].

Mövzu № 9. *Qrup, halq., meydan anlayışları.vektor fəzası.*

Sonlu riyaziyyatda istifadə olunan cəbri strukturlar-qrup, halqa, meydan anlayışları verilir, cəbrin kodlaşdırmada tətbiqlərinə aid məsələlərə baxılır. [1-4, 6].

Mövzu № 10. Xətti blok kodları. Xemminq kodları.

Blok kodlarına baxılır, xətti blok kodlarında Xemminq məsafəsi, Xemminq çəkisi anlayışları daxil edilir, xətti kodların əmələgətirici və yoxlayıcı matrisləri arasında əlaqəyə baxılır, xətti Xemminq kodlarının qurulması üsulları göstərilir. [1-4, 6, 10].

Mövzu № 11. Əlifba kodlaşdırmasının elementləri.

Kodlaşdırma üsulları göstərilir, qarşılıqlı birqiymətli kodlaşdırma üçün teorem verilir, Fano və Xafman üsulları ilə effektiv kodlaşdırmaya baxılır və məsələlər həll olunur.[1-4, 6, 10].

Mövzu № 12. Genişlənmiş Evklid alqoritmi və onun tərs modul qiymətinin hesablanmasına tətbiqi.

Tam ədədlərin xassələri verilir, ƏBOB-un tapılması üçün Evklid alqoritmi izah olunur, onun əsasında genişlənmiş Evklid alqoritmi verilir və tərs modulun hesablanması izah olunur. [1-4, 10].

Mövzu № 13. Müqayisələr və müqayisələr sistemi. Qalıq haqqında Çin teoremi .

Tam ədədlərin m moduluna görə müqayisə olunması anlayışı verilir, müqayisə və müqayisələr sisteminin həllərinə baxılır, müqayisə və müqayisələr sisteminin həll olunması üçün qalıq haqqında Çin teoremi verilir və onun köməyi ilə məsələlər həll olunur. [6, 9].

Mövzu № 14. Eyler funksiyası, Eyler teoremi. Ferma teoremi.

n moduluna görə elementin tərs elementinin tapılması üçün Eyler və Ferma teoremlərinə baxılır, onlara aid nümunələr göstərilir və məsələlər həll olunur.

[1-2, 6, 10].

Mövzu № 15. Kriptografiyanın əsas anlayışları. RSA.

Kriptografiya haqqında məlumat verilir, tətbiq sahələri göstərilir, kriptografiyada istifadə olunan alqoritmlər qeyd olunur, ən məşhur alqoritm olan RSA alqoritm haqqında məlumat verilir və nümunələrə baxılır. [1-4, 6].

Sərbəst işlərin mövzuları.

1. Avtomatlar nəzəriyyəsinə giriş. DSA-nın təyini. Qeyri-determinik sonlu avtomatlar. QSA-dan DSA-a ekvivalent keçid.
2. Requlyar çoxluqlar, requlyar ifadələr və onların xassələri. Requlyar dillər və ifadələr.
3. Qrammatika (əsas anlayışlar). SA-la requlyar çoxluqlar arasında əlaqə.
4. Vəziyyətlərin istisna üsulu ilə SA-dan requlyar ifadəyə keçid. Requlyar ifadədən DSA-a keçid.
5. İnformasiya nəzəriyyəsinin elementləri. Entropiya anlayışı.

6. Kodlaşdırma nəzəriyyəsinin əsas anlayışları. Rabitə kanalının modeli. Sadə kodlar. Qrup, halqa. Meydan anlayışı. Vektor fəzası.
7. Xətti blok kodları. Xemminq kodları. Əlifba kodlaşdırmasının elementləri.
8. Genişlənmiş Evklid alqoritmi və onun tərs modul qiymətinin hesablanmasına tətbiqi.
9. Müqayisələr və müqayisələr sistemi. Qalıq haqqında Çin teoremi. Eylər funksiyası, Eylər teoremi. Ferma teoremi.
10. Kriptografiyanın əsas anlayışları. RSA.

ƏDƏBİYYAT

Əsas

1. Хопкрофт Дж., Мотвани Р., Ульман Дж. Введение в теорию автоматов, языков и вычислений. 2002, 480 с.
2. Коган Д.И., Бабкина Т.С. «Основы теории конечных автоматов и регулярных языков. Учебное пособие» Издательство ННГУ, 2002 г. 283 с.
3. Mənsimov K.B., Feyziyev F.G., Aslanova N.X. Kodlaşdırma nəzəriyyəsi. BDU-nəşriyyatı-2009, 223 s.

4. Блейхут Р. Теория и практика кодов, контролирующих ошибки. Москва-1986, 572 с.
5. Зверева Е.Н., Лебедько Е.Г.Сборник примеров и задач по теории информации и кодирований сообщений. Санкт Петербург 2014,110 с.
6. Виноградов И.М. Основы теории чисел.

Әlavә

7. Гилл А. Линейные последовательные машины:1974. 256 с,
8. Пентус А.Е., Пентус М.Р.. Теория формальных языков. Москва-2004, 80 с.
9. Айерлэнд К., Роузен М. Классическое введение в современную теорию чисел. Москва-1987. 419 с.
10. Кучинский В.Ф., Спирина Т.П. Теоретические основы экономической информатики: учеб. пособие. – СПб: НИУ ИТМО, 2014. – 90 с.