A.A. TSHATSHAPANYAN

THE IMPACT OF ADI SHAMIR THRESHOLD SCHEME ON COMPUTER NETWORK PRODUCTIVITY

Ensuring the speed and security of computer networks is important during their operation. Adi Shamir (k, n) threshold scheme is among the effective key management methods. On the one hand, it ensures network security, on the other hand, it reduces performance. The artikle includes an estimation of the decrease in the performance of the computer network when applying the of Adi Shamir key management (k,n)threshold scheme.

Keywords: computer network, speed, security.threshold scheme, secret distribution, Lagrange Interpolation,performance.

ՀՏԴ 371.214

Գ.Ա. ՀԱՐՈՒԹՅՈՒՆՅԱՆ, Է.Հ. ՀՈՎՀԱՆՆԻՍՅԱՆ

ԳԻՏԵԼԻՔՆԵՐԻ ՍՏՈՒԳՄԱՆ ԱՎՏՈՄԱՏԱՑՎԱԾ ՀԱՄԱԿԱՐԳՈՒՄ ՊԱՏԱՍԽԱՆՆԵՐԻ ՃՇՏՈՒԹՅԱՆ ԱՍՏԻՃԱՆԻ ՈՐՈՇՈՒՄԸ

Ուսումնասիրվել են ավտոմատացված ուսուցման համակարգերում սովորողների պատասխանների դիֆերենցիալ գնահատման խնդիրները, իրականացվել է տեքստային հարցերի ներկայացման տարբեր ձևերի և համապատասխանաբար պատասխանների վերլուծություն: Առաջարկվում են գործնականում իրագործելի մեթոդներ՝ պատասխանների ճշգրտությունը որոշելու համար, որոնք կախված չեն հարցերի սեմանտիկ կառուցվածքից և թույլ են տալիս կատարել դիֆերենցված գնահատում:

Առանցքային բառեր. ուսուցման ավտոմատացված համակարգ, գիտելիքների վերահսկման համակարգ, թեստավորում, բազմություն, ցուցակ, նմանության աստիճան:

Ներածություն: Կրթական գործընթացի հիմքը ուսումնական համակարգերի օգտագործման ժամանակ սովորողի ինքնավերահսկվող ինքնուրույն աշխատանքն է:

Գիտելիքների վերահսկման ավտոմատացված համակարգերում սովորաբար օգտագործվում են գիտելիքների վերահսկման կազմակերպման 2 հիմնական մոտեցումներ.

1.Սովորողի գործողությունների գնահատում [1]: Այս մեթոդը կիրառվում է փորձագիտական համակարգերում, այսինքն՝ այն համակարգերում, որոնք հիմնված են գիտելիքների վրա: Առարկայական ոլորտի վերաբերյալ գիտելիքները և սովորողի գործողությունների գնահատման կանոնները թույլ են տալիս երկխոսության ընթացքում որոշել սովորողի գիտելիքների մակարդակը [2]:

2. Գիտելիքների ստանդարտացված վերահսկողություն[3]: Սրա էությունն այն է, որ սովորողին առաջարկվում են հատուկ առաջադրանքներ:

Ներկայում առկա ավտոմատացված ուսուցման համակարգերում օգտագործվում է երկմիավոր գնահատման համակարգ. պատասխանը համարվում է բացարձակապես ճիշտ կամ բացարձակապես սխալ: Սա սահմանափակում է, քանի որ չի համապատասխանում իրական դրույթին, երբ պատասխանի ճշգրտությունը որոշում է ուսուցիչը, ով մոտենում է գնահատականին դիֆերենցված: Ուստի նպատակահարմար է գիտելիքների վերահսկման համակարգում ներառել համակարգ, որը հնարավորություն է տալիս որոշել պատասխանի ճշգրտության աստիճանը: Օրինակ՝ (2,3,5) պատասխանն ավելի մոտ է (3,4,5) պատասխանին, քան (1,2) պատասխանին, այդ իսկ պատճառով տվյալ պատասխանը պետք է գնահատվի ավելի բարձր: Այս խնդիրը լուծելու համար պահանջվում է.

▪ վերլուծել տարբեր տեսակի թեստային հարցեր և պատասխաններ,

▪ սահմանել չափորոշիչներ՝ էտալոնային պատասխանների հետ սովորողի պատասխանների համընկնման աստիճանը որոշելու համար:

Տարբեր տեսակի թեստային հարցերի և պատասխանների վերլուծություն:

Սովորողի պատասխանների վերլուծություն: Ներկայիս համակարգերում ամենատարածված պատասխանների տեսակը ընտրանքայինն է: Հարցին ներկայացվում են մի քանի պատրաստի պատասխաններ, որոնցից մեկը ընտրվում է որպես ճիշտ պատասխան: Ապա, ըստ տարածվածության, հաջորդում են թվային կամ տեքստային պատասխանները: Գոյություն ունեցող թեստային համակարգերի վերլուծության հիման վրա կարելի է առանձնացնել.

▪ Հարցի տեսակները (ըստ ներկայացման ձևի).

1. Տեքստ,
2. Նկար,
3. Գործընթաց,
4. Խոսքային հաղորդում (ներառված՝ «տեքստ» և/ կամ «գործընթաց» տեսակներում),

▪ Պատասխանի տեսակները (ըստ մուտքագրման և ներկայացման ձևի).

1. Տարրերի բազմություն,
2. Տարրերի ցուցակ,
3. Արտահայտություններ (թվաբանական),
4. Արտահայտություն (տեքստային),
5. Նկար,
6. Խոսքային հաղորդում (ներառված տեքստային արտահայտություն):

Գործնական տեսանկյունից հարցերի և պատասխանների բազմաթիվ տարբերակներ հեշտությամբ կարող են դասվել հետևյալ տեսակներին.

▪ Հարցերի տեսակներ.

1. ՏԵՔՍՏ – հարց՝ ներկայացված տողերի և սիմվոլների միջոցով:

2. ՀՐԱՄԱՆ – հրամանի տող՝ հարց, որի տրման համար անհրաժեշտ է մեկնարկել արտաքին հրաման (նկարի, ձայնային հաղորդագրության և այլնի մուտք):

3. Պատասխանի տեսակները.

4. ՏԵՔՍՏ – պատասխան՝ ներկայացված տողերի և սիմվոլների միջոցով:

5. ԲԱԶՄՈՒԹՅՈՒՆ – պատասխան՝ ներկայացված անկանոն տարրերի հաջորդականությամբ:

6. ՑՈՒՑԱԿ – պատասխան՝ կազմված տարրերի կանոնավոր բազմությունից:

7. ԱՐՏԱՀԱՅՏՈՒԹՅՈՒՆ – պատասխան՝ ներկայացված թվաբանական արտահայտություններով:

Ընտրանքային պատասխանների տարածվածությունը բացատրվում է ընդհանուր գործածությամբ և վերլուծության պարզությամբ: Ընդհանուր առմամբ ընտրանքային պատասխանը ներկայացնում է տարրերի բազմություն (անկանոն) կամ տարրերի ցուցակ (կանոնավորված): Տարրերը կարող են հանդես գալ բազմության և ցուցակների տեսքով, այդ դեպքում ստացվում են երկաստիճան սխեմաներ՝ բազմության ցուցակ և ցուցակների բազմություն:

Ընտրանքային պատասխանի ճշգրտությունը գնահատվում է էտալոնի հետ համեմատության ճանապարհով: Գոյություն ունեցող համակարգերում ընտրանքային պատասխանի ճշգրտությունը, որպես կանոն, որոշվում է էտալոնին ամբողջական համընկնմամբ, այսինքն տեղի է ունենում երկուական գնահատում: Տարբերակված գնահատման համար առաջարկվում է օգտագործել որոշակի միանմանություն որևէ ֆունկցիալության, որը թույլ կտա որոշել գիտելիքների որոշակի հատվածում էտալոնի հետ նմանության աստիճանը: Պատասխանի ճշգրտությունը կախված է պատասխանի տեսակից, անհրաժեշտ է առանձնացնել 4 տեսակի ընտրանքային պատասխան՝ բազմություն, ցուցակ, ցուցակների բազմություն, բազմությունների ցուցակ:

Բազմությունների տարրերի համեմատում: Այն դեպքում, երբ պատասխանը ներկայացնում է բազմություն, ապա պատասխանի գնահատականը բազմությունների միջև ընկած հեռավորությունն է:

Տրված են երկու բազմություններ Ma, Me, կազմված R բազմության տարրերից: Պահանջվում է որոշել բազմությունների միջև հեռավորությունը:

Հեռավորությունը պետք է բավարարի հետևյալ պահանջները.

1. |aa|=0, ∀a.
2. |ab|=|ba|, ∀a,b.
3. |ab|+|bc| ≤ |ac| ∀a,b,c,

Ընդունենք [0, 1] որպես r հեռավորության փոփոխության միջակայք այնպես, որ՝

- r=0, եթե Ma ≡Me;
- r=1, եթե Ma ∩Me =∅;
- 0<r<1, եթե Ma ∩Me ≠ ∅:

Տրված է կամայական սահմանափակ բազմություն R: A={ai} և B = {bi} Ենթաբազմությունների միջև հեռավորությունը կարելի է հաշվել՝

$$r=1-\frac{K}{L}, \quad (1)$$

որտեղ K-ն A և B ենթաբազմությունների միջև համընկնող տարրերի քանակն է:

L=|A|=|B| - ենթաբազմության հզորություն: Եթե |A|≠|B|, ապա առաջին բանաձևը վերափոխվում է ՝

$$r=1-\frac{K}{L+K_b}, \quad (2)$$

որտեղ K_b = |A| - K B ենթաբազմության այն տարրերի քանակն է, որոնք չկան A-ում:

Բազմությունների նմանության աստիճանը կկոչենք մեծություն, հակառակ հեռավորություն՝

$$\delta=1-r: \quad (3)$$

2-րդ և 3-րդ արտահայտությունների միավորումը կնապաստի՝ գնահատելու սովորողի պատասխանը՝ էտալոն պատասխանի հետ համընկնման աստիճանը հետևյալ բանաձևով՝

$$\delta_1 = \frac{K_a}{L+K_b}, \quad (4)$$

որտեղ L=|S_e|, K_a =| S_e ∩ S_e |, K_b=| S_a|-K_a:

Ցուցակների տարրերի համեմատում: Այն դեպքում, երբ պատասխանը ներկայացված է տարրերի կանոնավոր բազմության՝ ցուցակների տեսքով, պատասխանի գնահատումը կատարվում է աստիճանական համեմատմամբ ցուցակների միջև: Այդ դեպքում կարելի է ընդունել [0, 1] որպես միջակայք r հեռավորության փոփոխությունն, այսպես որ.

- r=0, երբ ցուցակները համընկնում են;

▪ r= 1, երբ տարրերի ենթաբազմությունները չեն հատվում;

▪ 0<r<1, երբ ցուցակները համընկում են մասամբ:

Կիրառենք ցուցակի դասակարգում, որպեսզի որոշենք ցուցակների միջև եղած հեռավորությունը: Հերթականության հարաբերակցությունը բազմության տարրերի վրա ներմուծվում է այնպես, որ ցանկացած երեք a,b,c-ն համապատասխանեն հետևյալ պայմաններին.

▪ Ճշմարիտ է մեկ միայն և մեկ հարաբերակցություն՝ a<b, a=b, a>b:

▪ Եթե a<b և b<c, ապա a<c:

Տարրերի կարգավորումը կատարվում է տեսակավորման միջոցով՝ գտնել տարրերի այնպիսի հաջորդականություն, որից հետո դրանք կգտնվեն չնվազող կարգով:

Հակադարձ աղյուսակը, եզակիորեն տարբերակում է համապատասխան վերադասավորումը, հետևաբար՝ ցանկացած հակադարձ աղյուսակից, որը ստեղծում է պայմանը, կարելի է միանշանակ վերականգնել նախնական վերադասավորումը:

Դրա մեջ մտնող տարրերը դասավորելու համար a1, a2, … an քայլերի մեծագույն քանակ պետք է կատարել միայն այն դեպքում, երբ տվյալ վերադասավորումը գտնվում է հակառակ հերթականությամբ: Եթե դասակարգումը անցկացնենք տարրերի զույգային տեղափոխություններով, ապա n տարրերի վերադասավորումների մեծագույն քանակը հավասար կլինի.

$$Kn=\frac{n(n-1)}{2}: \quad (5)$$

(5) Արտահայտության հիման վրա ցուցակների միջև եղած հեռավորությունը կարելի է հաշվել հետևյալ բանաձևով.

$$r= Ki / Kn: \quad (6)$$

A և B ցուցակների միջև եղած հեռավորության հաշվումը, վերադասավորման ճանապարհով, մուտքագրված մյուս ցուցակի հիման վրա, բավարարում է հեռավորություն հասկացությանը:

Այս սահմանմանը համապատասխան՝ մուտքագրենք մեկ այլ հասկացություն՝ ցուցակների նմանության աստիճանը: Նմանության աստիճանը մեծություն է՝ հավասար ցուցակների միջև հեռավուրությանը:

3 և 7 բանաձևերից ելնելով՝ ունենում ենք մի նոր բանաձև.

$$\delta =1-(Ki / Kn), \quad (7)$$

որտեղ Ki –ն ցույց է տալիս զույգային վերադասավորությունների քանակը, իսկ Kn –ն՝ մեծագույն քանակի վերադասավորումները n երկարությամբ ցուցակի դեպքում:

Բանաձևն ունի հետևյալ սահմանափակումները.

- Եթե Sa ≡ Se , ապա Ki = 0, δ2 =1,
- Եթե Sa ∩ Se =∅ , ապա Ki = Kn , δ2 =0,
- Հակառակ դեպքում՝ 0< δ2 <1:

Ընդհանուր առմամբ, Sa և Se էտալոններ գտնվում են սկզբնական բազմությունում:

Եթե վերլուծենք, որ Sa ցուցակը պարունակում է {bj}, ապա այդ տարրերը չեն կարող որոշվել: Այդ իսկ պատճառով նմանության աստճանի որոշումը տեղի է ունենում 2 փուլով: Առաջին փուլում ցուցակները դիտարկվում են որպես բազմություններ, և որոշվում է նմանությունը 2 բազմությունների միջև (բանաձև 4): Ապա տեղի է ունենում տարրերի փոխարինում: bj տարրերը փոխարինվում են հատուկ տարրերով, որոնք հավասար են համապատասխան տարրին: Այն դեպքում, երբ ցուցակների երկարությունները չեն համապատասխանում, ավելի կարճ ցուցակը լրացվում է տարրերով՝ աջից:

Երկրորդ փուլում որոշվում է Sa′ և Se′ ցուցակների համընկնումը: Դա հաշվվում է Sa ′ ցուցակի վերադասավորմամբ, համապատասխանաբար Se ′ - ի հետ:

Ապա նմանության աստիճանը հաշվվում է բանաձև 8-ի միջոցով:

Ցուցակի վերջնական աստիճանային տարբերությունն իրականացվում է հետևյալ ձևերով.

$$\delta = (\delta 1 + \delta 2)/2, \quad (8)$$

$$\delta = \max(\delta 1, \delta 2), \quad (9)$$

$$\delta = \mathrm{mix}(\delta 1, \delta 2), \quad (10)$$

$$\delta = \delta 1 * \delta 2: \quad (11)$$

Մաքսիմումի ֆունկցիայի կիրառման պարագայում կարող են առաջանալ դեպքեր, երբ սխալ պատասխանը կարող է ճիշտ թվալ: Օրինակ՝ Sa ={1,2,3,4} , իսկ Se ={4,3,2,1} , ապա δ1=1, δ2 =0, δ=max {1,0}=1

Ցուցակների բազմությունների համեմատում: Դիտարկենք դեպք, երբ Se բազմության անդամները rj բազմություններն են կամ si (i=1,..., N) ցուցակները:Այդ պարագայում Se -ի պատասխանի ստացումը կարող է լինել 2 փուլով:

Առաջին փուլում ամեն անդամ (r_j բազմության կամ Si ցուցակի) համեմատվում է Se էտալոն բազմության բոլոր անդամների հետ (ըստ բազմությունների և ցուցակների համեմատության կանոնների):

Այդ անդամի՝ էտալոն բազմությանը նմանության աստիճանի համար ընտրվում է երկու բազմությունների անդամների նմանության առավելագույն

աստիճանը: Այս համեմատության աստիճաններից կազմվում է վեկտոր L-ը, որի երկարությունը հավասար է N-ի ուժին:

Եթե rj (si) անդամին չի համապատասխանում էտալոն Sa բազմության ոչ մի անդամ, ուրեմն L վեկտորի i անդամը հավասար է 0-ի:

Երկրորդ փուլում պատասխանի և էտալոն բազմության նմանության աստիճանը հաշվվում է L վեկտորով, օրինակ՝ ինչպես վեկտոր L-ի միջին թվաբանականի հաշվումը:

Ցուցակների բազմությունների համեմատում: Ցուցակների բազմությունների համեմատումը նույնպես կարելի է իրականացնել 2 փուլով:

Առաջին փուլը Sa և Se ցուցակների համեմատումն է և K համապատասխանության վեկտորի առաջացումը: K վեկտորի k անդամը հավասար է Se ցուցակի ամենամոտ անդամի համարին կամ թվի, որը գերազանցում է էտալոն բազմության անդամների քանակը: Se նմանության աստիճանը կարող է հաշվվել՝ ինչպես ցուցակների աստիճանների թվաբանական միջինը:

Երկրորդ փուլում ստացված ցուցակը դասավորում ենք ըստ զույգային վերադասավորման: Δ2 նմանության աստիճանը հաշվվում է ըստ ցուցակների նմանության կանոնների:

Վերջնական պատասխանի և էտալոն բազմության նմանության աստիճանը հաշվվում է 9-11 բանաձևերից մեկով: Կարող է նաև լինել ավելի պարզ եղանակ իրագործման տեսանկյունից, որի էությունն այն է, որ Sa ցուցակը համարվում է դասավորված, և Sa ցուցակի i անդամ համադրվում է Se ցուցակի i անդամին:

Պատասխանի վերլուծությունը թվաբանական արտահայտության տեսքով: Պետք է որոշված լինի էտալոնը (ճիշտ պատասխանը) և թույլատրվող սխալը: Թույլատրվող սխալի օգտագործման եղանակներից մեկը պատասխանի ստուգումն է էտալոնում:

Եթե դիտարկենք դա որպես 2 մակարդակ ունեցող կառուցվածք, ապա կարելի է ներբեռնել տեքստային դիտարկված տիպերի պատասխան՝ բազմությունների ցուցակ կամ ցուցակների ցուցակ:

Եզրակացություն:

- Դիտարկվում են ավտոմատացման ուսուցման համակարգերում ուսանողների պատասխանների դիֆերենցված գնահատման խնդիրները:
- Բերվում է թեստային հարցերի և պատասխանների ներկայացման տարբեր ձևերի վերլուծությունը:
- Առաջարկվում են պատասխանների ճշտության որոշման գործնականում իրականացնելի մեթոդներ, որոնք կախված չեն հարցերի սեմանտիկ կառուցվածքից և թույլ են տալիս կատարել դիֆերենցված գնահատում:

Առաջարկված մեթոդներով պատասխանի ներկայացման և ճշգրտության վերլուծությունը թույլ է տալիս էականորեն ծավալել տեքստային առաջադրանք-

ների ներկայացման ձևերը: Ստացված արդյունքները կարող են հիմք հանդիսանալ համակարգչային ավտոմատացման միջոցների նախագծման, որը կարող է հանդիսանալ կարևորագույն ավտոմատացման համակարգ՝ հեռավար ուսուցման համար: Ակնհայտ է, որ այս արդյունքները կարող են օգտակար լինել ոչ միայն ամփոփիչ գիտելիքների գնահատման համար, այլ նաև ապահովել հակադարձ կապի մոտիվացիա համակարգչային ուսուցման մակարդակի բարձրացման համար:

ԳՐԱԿԱՆՈՒԹՅԱՆ ՑԱՆԿ

1. **Агеев В.Н.** Электронные учебники и автоматизированные обучающие системы – М., 2001. -79с.
2. **Андерсон Дж.Р., Рейзер Б.Дж.** Учитель Лиспа // В сб.: Реальность и прогнозы искусственного интеллекта / Под ред. В.Л. Стефанюка; Пер. с англ. - М.: Мир, 1987.- С. 27-47.
3. **Свиридов А.П.** Основы статистической теории обучения и контроля знаний: Метод. пособие. – М.: Высшая школа, 1981. – 262 с.

Г.А. АРУТЮНЯН, Э.Г. ОГАНЕСЯН

ОПРЕДЕЛЕНИЕ СТЕПЕНИ ТОЧНОСТИ ОТВЕТОВ В АВТОМАТИЗИРОВАННОЙ СИСТЕМЕ КОНТРОЛЯ ЗНАНИЙ

Рассматриваются проблемы дифференцированной оценки ответов обучаемых в автоматизированных обучающих системах. Проводится анализ различных форм представления тестовых вопросов и соответствующих ответов. Предлагаются практически реализуемые методы определения точности ответов, которые не зависят от семантики вопросов и позволяют проводить оценку дифференцированно.

Ключевые слова: автоматизированная обучающая система, система контроля знаний, тестирование, множество, список, степень сходства.

G.A. HARUTYUNYAN, E.H. HOVHANNISYAN

DETERMINING THE DEGREE OF THE ANSWER ACCURACY IN THE AUTOMATED SYSTEM OF KNOWLEDGE TESTING

Problems of differentiated estimation for the answers of training in automated training systems are considered. The analysis of various forms of test questions and corresponding answer presentation is given. Practically realizable methods of defining the answer accuracy which donot depend on the semantics of questions and allow to carry out differentiated estimation are proposed.

Keywords: automated learning system, knowledge control system, testing, set, list, degree of similarity.