ВІСНИК
КИЇВСЬКОГО НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ ІМЕНІ ТАРАСА ШЕВЧЕНКА

ISSN 1728-2276

КІБЕРНЕТИКА (1)14/2014

Засновано 1999 року

Наведено результати досліджень з аналізу, оцінки, керування й оптимізації динамічних систем, проблем еколого-економічного аналізу та чисельних методів моделювання процесів.
Для викладачів, наукових співробітників, аспірантів і студентів.

In this issue the results of researches in analysis, estimates, control and optimization of dynamical systems, problems of ecology-economic analysis and numeral methods of processes are presented.
For scientists, professors, aspirants and students.

ЗМІСТ

СОДЕРЖАНИЕ

CONTENTS

УДК 519.87

Д. О. Вадньов, здобувач,
Київський національний університет імені Тараса Шевченка, Київ

ПРО ВИКОРИСТАННЯ ЗАДАЧІ ПРО РЮКЗАК В ЯКОСТІ АЛГОРИТМУ ДЛЯ ШИФРУВАННЯ ДАНИХ

Розглянуто алгоритм шифрування даних на основі задачі про рюкзак. Визначено завдання про підвищення криптостійкості алгоритму. Запропоновано схему шифрування, побудовану з використанням простих чисел та операцій над ними спеціального вигляду. Проілюстровано використання алгоритму та його модифікації на прикладі конкретної текстової послідовності.

Ключові слова: задача про рюкзак, криптостійкість, алгоритм шифрування.

Одним з перших алгоритмів для узагальненого шифрування з відкритим ключем є алгоритм рюкзака, розроблений Ральфом Мерклом та Мартином Хелманом [1]. Даний алгоритм, що отримав назву алгоритму Меркла-Хелмана, спочатку використовувся лише для шифрування, але пізніше Аді Шамір [2] адаптував криптосистему для створення цифрового підпису. Безпека алгоритмів рюкзака зпирається на проблему вирішення задачі про рюкзак, яка є NP-повною проблемою.

Задача про рюкзак нескладна і добре відома. Припускається, що задано множину предметів різної ваги. Необхідно визначити, як можна покласти деякі з цих предметів у рюкзак таким чином, щоб вага рюкзака стала рівною наперед заданому значенню. Більш формально, для заданого набору значень M_1, M_2,….., M_n (n – потужність заданої множини) та величини S потрібно визначити значення b_i, $i = \overline{1,n}$, такі що

$$S = b_1M_1 + b_2M_2 + b_nM_n, \quad (1)$$

де b_i, $i = \overline{1,n}$, може бути або нулем, або одиницею. Одиниця показує, що предмет кладуть в рюкзак, а ноль – що не кладуть.

Наприклад, ваги предметів мають значення 1, 5, 6, 11, 14 та 20. Можна наповнити рюкзак таким чином, щоб його вага стала рівною 22, використавши величини 5, 6 і 11. З іншої сторони, неможливо упакувати рюкзак так, щоб його вага була рівною 24. У загальному випадку час, необхідний для вирішення цієї проблеми, з ростом кількості предметів в наборі росте експоненційно.

В основі алгоритму Меркла-Хелмана лежить ідея шифрувати повідомлення на основі ключа – послідовності ваг задачі про рюкзак (відкритий ключ). Предмети з набору обираються за допомогою блоку відкритого тексту, рівного за довжиною кількості предметів в наборі (біти відкритого тексту відповідають значенням b_i, $i = \overline{1,n}$), а шифротекст є отриманою сумою. Приклад шифротексту, отриманого за допомогою задачі про рюкзак, наведено у табл.1.

***Таблиця* 1**

Відкритий текст	111001	010110	000000	011000
Рюкзак	1 5 6 11 14 20	1 5 6 11 14 20	1 5 6 11 14 20	1 5 6 11 14 20
Шифротекст	1+5+6+20=32	5+11+14=30	0=0	5+6=11

Однак, виявилось, що ця схема є криптографічно нестабільною і, як наслідок, не набула популярності.

В якості суттєвого покращення базового алгоритму Меркла-Хелмана було запропоновано створення закритого ключа, який є перетвореною послідовністю ваг задачі про рюкзак спеціального вигляду. Даний варіант використовувався у двох модифікаціях: однотапній та багатоетапній. Але запропоновані вдосконалення не забезпечили криптостійкості алгоритму. Вперше про його небезпеку було повідомлено у роботі [2]. Більш того, схема алгоритму дозволяє визначити вхідну послідовність без використання будь-якого закритого ключа [3]. Тому зрозуміло, що практично одразу після створення розпочався пошук модифікацій запропонованого алгоритму, що забезпечують підвищений захист від зламу. Для подолання недоліків базової схеми Родні Гудман та Ентоні Маколі [4] розробили процедуру, що базується на модульних рюкзаках. Надалі з'ясувалось, що ця схема також небезпечна. Окрім використання модульних рюкзаків були запропоновані схеми використання інших видів рюкзака. У 1986 році Харальд Нідерайтер [5], опубліковав рюкзачну криптосистему на основі алгебраїчної теорії кодування, яка також була зламана, а у 1988 році Масакацу Морії та Масао Касахара [6] розробили криптосистему з використанням мультиплікативного рюкзака. Ця ідея виявилась вдалою і поки система на мультиплікативних рюкзаках не зламана. Також вдалою виявилась ідея Хусейна Алі Хусейна, Джафара Ваді Абдули Сада та М. Каліфа [7], які у 1991 році запропонували багатоетапну рюкзачну криптосистему. У ній фіксується рюкзачний вектор на кожному етапі, а вихід (зашифроване повідомлення) після кожної стадії алгоритму використовується у якості вхідних даних (тексту) на наступному етапі. Вдалої атаки на дану схему на поточний час невідомо. Продовжилися покращення і класичного алгоритма Меркла-Хелмана.

Підсумовуючи короткий огляд, можна зробити висновок, що, незважаючи на небезпеку алгоритму, варто вивчити його функціонування, тому що на прикладі цього алгоритму можна продемонструвати можливість застосування NP-повної проблеми в криптографії з відкритими та закритими ключами.

Проблеми шифрування на основі задачі про рюкзак. Розглядаючи зміст задачі про рюкзак, можна відмітити, що існує дві різні задачі, одна з яких вирішується за лінійний час, а інша, як вважається, – ні. Просту задачу можна перетворити у складну. Відкритий ключ представляє собою складну (важку) проблему, яку дуже просто можна використати для шифрування, але неможливо для дешифрування повідомлень. Закритий ключ є простою (легкою) проблемою, що надає простий спосіб дешифрування повідомлення. Тим, хто не знає закритий ключ, потрібно спробувати вирішити складну задачу про рюкзак.

Надзростаючі рюкзаки.

Означення. Надзростаючою послідовністю називається послідовність, кожний член якої більше суми усіх попередніх членів.

Наприклад, послідовність {1,3,6,13,27,52} є надзростаючою, а послідовність {1,3,4,9,15,25} – ні. В даному контексті варто згадати і добре відому послідовність чисел Фібоначчі, яка, незважаючи на швидке зростання елементів, не є надзростаючою.

Розглянемо просту проблему рюкзака. Якщо перелік ваг предметів у наборі є надзростаючою послідовністю, то отриману проблему рюкзака можна нескладно вирішити. Розв'язок надзростаючого рюкзака знаходиться наступним чином. Необхідно взяти повну вагу і порівняти його з найбільшим числом послідовності. Якщо повна вага менше цього числа, то його не кладуть у рюкзак. Якщо повна вага більше або рівна цього числа, то воно кладеться у рюкзак. Зменшимо вагу рюкзака на це значення і перейдемо до наступного за величиною числа послідовності. Будемо повторювати ці дії, доки процес не завершиться. Якщо повна вага зменшується до нуля, то розв'язок знайдено. У протилежному випадку – ні.

Покладемо для прикладу, що повна вага рюкзака має бути 70, а надзростаюча послідовність ваг {2,3,6,13,27,52}. Найбільша вага – 52, яка менше 70, тому 52 кладуть у рюкзак. Віднімаючи 52 від 70, отримуємо 18. Наступна вага - 27, більше 18, тому число 27 у рюкзак не кладуть. Наступну вагу 13, яка менше 18, кладуть у рюкзак. Віднімаємо 13 з 18 і отримуємо 5. Чергова вага – 6, більша за 5, не кладеться у рюкзак. Продовжуючи цей процес, отримаємо, що ваги 3 і 2 кладуть у рюкзак, і повна вага зменшується до 0, що свідчить про знайдений розв'язок. Якщо розглядати цю процедуру як блок шифрування методом рюкзака Меркла-Хелмана, відкритий текст, отриманий із значення шифротексту 70, був би рівний 110101.

Пошук заповнення нормальних рюкзаків послідовностями, які не є надзростаючими, представляють собою складну проблему. Швидкого алгоритму для вирішення даної задачі в реальному часу поки не знайдено. Єдиним відомим способом визначити, які предмети упаковано у рюкзаку, є методична перевірка можливих розв'язків до знаходження вірного. Найшвидкіший алгоритм, приймаючи до уваги різні евристики, має експоненційну залежність від кількості можливих предметів. Тому, якщо додати до послідовності ваг лише один елемент, знаходження розв'язку задачі стає вдвічі складніше. Це набагато важче надзростаючого рюкзака, в якому, якщо додати один предмет до послідовності, складність пошуку розв'язку зростає на одну операцію.

Алгоритм Меркла-Хелмана базується на цій властивості. Закритий ключ є послідовністю ваг задачі надзростаючого рюкзака. Відкритий ключ – це послідовність ваг проблеми нормального рюкзака з тим самим розв'язком. Р. Меркл та М. Хелман [1], застосовуючи цілочислову арифметику, розробили спосіб перетворення проблеми надзростаючого рюкзака в проблему нормального рюкзака.

Створення відкритого ключа з закритого. Розглянемо роботу алгоритму, не заглиблюючись в теорію чисел. Для отримання нормальної послідовності рюкзака візьмемо надзростаючу послідовність рюкзака, наприклад наведену раніше $\hat{E}$ ={2,3,6,13,27,52}, і домножимо всі значення на число $\grave{O}$ за модулем N. Значення модуля повинно бути більше суми всіх чисел послідовности, тобто утворювати з заданою послідовністю надзростаючу послідовність. Оберемо, наприклад, N =105. Множник $\grave{O}$ повинен бути взаємно простим числом з модулем N, тобто НСД (N ,T) =1. Покладемо, наприклад, $\grave{O}$ =31. Нормальною послідовністю рюкзака у цьому випадку буде {62,93,81,88,102,37}, де 62=2*31 mod 105; 93=3*31 mod 105; 81=6*31 mod 105; 88=13*31 mod 105 ; 102=27*31 mod 105 ; 37=52*31 mod 105.

Надзростаюча послідовність рюкзака разом з числами N та T {2,3,6,13,27,52; 105, 31} є закритим ключем, а нормальна послідовність рюкзака {62,93,81,88,102,37} – відкритим.

Шифрування. Для шифрування повідомлення розбивається на блоки, що за довжиною дорівнюють кількості елементів послідовності рюкзака. Далі, вважаючи, що одиниця відповідає присутності члена послідовності, а ноль - його відсутності, обчислюємо повні ваги рюкзаків - по одному для кожного блоку повідомлень.

Якщо припустити, що повідомлення у бінарному вигляді подається як 011000110101101110, то шифрування, яке використовує попередню послідовність рюкзака, буде здійснюватися таким чином:

Вхідне повідомлення у блочному вигляді = 011000 110101 101110, звідки

011000 відповідає числу 93 + 81 = 174;

110101 відповідає числу 62 + 93 + 88 + 37 = 280;

101110 відповідає числу 62 + 81 + 88 + 102 = 333.

У результаті шифротекстом повідомлення 011000110101101110 є числова послідовність 174,280,333.

Дешифрування. Законний отримувач даного повідомлення знає закритий ключ: оригінальну надзростаючу послідовність, а також значення N та T , які використовувалися для перетворення її в нормальну послідовність рюкзака. Для дешифрування повідомлення отримувач визначає мультиплікативне обенене T^{-1}, таке що $T*(T^{-1}) \pmod{N}$ = 1. Кожне значення шифротексту домножується на $T^{-1} \bmod N$, а потім розгортається в суму за допомогою закритого ключа, щоб отримати значення відкритого тексту.

У нашому прикладі надзростаюча послідовність {2,3,6,13,27,52}, N = 105, T = 31. Шифротекстом є послідовність 174,280,333. У цьому випадку T^{-1} дорівнює 61 (31*61 mod 105=1891 mod 105=1), тому значення шифротексту домножуються на величину 61 mod 105.

Маємо 174*61 mod 105 = 9 = 3 + 6, що відповідає 011000;

280*61 mod 105 = 70 = 2 + 3 + 13 + 52, що відповідає 110101;

333*61 mod 105 = 48 = 2 + 6 + 13 + 27, що відповідає 101110.

Розшифрованим відкритим текстом є бінарні послідовності 011000 110101 101110, що повністю відповідає вхідному повідомленню.

Підвищення крипостійкості алгоритму шифрування. Сучасні дослідження по вдосконаленню алгоритму здійснюються за двома основними напрямками. Перший з них об'єднує роботи, що спрямовано на використання різних варіантів задачі про рюкзак. Інший напрямок досліджує застосування різних додаткових схем та процедур, що підвищують захищеність алгоритму.

Запропонуємо модифікацію базової схеми на основі нечіткого підходу [8] та послідовностей простих чисел спеціального вигляду.

Позначимо, $P_k(a)$ – k-те просте число, що не менше цілого $a \geq 0$, $k = 0,1,2,...$.

Нескладно перевірити, що

1) $P_0(0)=0$, $P_0(1)=1$, $P_1(0)=1$;

2) $P_k(a)=P_1(P_{k-1}(a))=...=P_{k-1}(P_1(a))$, $k=1,2,3,...$, $a\geq 0$;

3) $P_k(a)\leq P_l(a)$ для будь-яких $k\leq l$, $k=0,1,2,...$, $l=0,1,2,3,...$, $a\geq 0$.

Крім традиційних арифметичних операцій додавання, віднімання, множення та ділення, на послідовності чисел $P_k(a)$, $a\geq 0$, $k=0,1,2,...$, введемо операцію зсуву на m, $m\in N\cup\{0\}$, простих чисел у вигляді

$$P_k(a)\oplus m=P_{k+m}(a)=P_m(P_k(a)), \tag{2}$$

яка не виводить за межі заданої послідовності, та операцію p - кратної композиції ($p\in N$) відношення двох чисел $P_k(a)$ та $P_l(a)$, $k=0,1,2,...$, $l=0,1,2,3,...$, у вигляді

$$P_k(a)\big/P_l(a)\circ p=P_k(a)\oplus p\big/P_l(a)\oplus p=P_{k+p}(a)\big/P_{l+p}(a)=P_p(P_k(a))\big/P_p(P_l(a)). \tag{3}$$

Числа, що входять до відкритого ключа $K=\{r_1,...,r_n\}$, є довільними цілими числами. Традиційне поняття нечіткості [8], яке визначає міру належності конкретного числового значення до нечіткої множини, в даному випадку може інтерпретуватися як рівень складності кодування кожного числа $r_j\in K, j=\overline{1,n}$.

Для визначення величини складності доповнимо відкритий ключ двома довільними значеннями k та l, $k\leq l$, $k=0,1,2,...$, $l=1,2,3,...$, за якими з послідовності простих чисел визначаються величини $s=P_k(a)$, $q=P_l(a)$ для деякого числа $a\geq 0$. За таких умов отримуємо, що $0\leq s/q\leq 1$. Ця величина може служити показником складності кодування, а за допомогою значень s та q можна змінити ваги відкритого ключа K та величини N та T, наприклад, за наступною схемою:

- для чисел T та N, які є взаємно простими числами, обчислюються числа $P_s(T)$ та $P_q(N)$ відповідно, де $s=P_k(a)$, $q=P_l(a)$;
- для цілих чисел $r_j\in K, j=\overline{1,n}$, які входять до ключа K, обчислюються величини $u_j=P_s(r_j)-r_j$ та $v_j=P_q(r_j)$, $j=\overline{1,n}$, $s=P_k(a)$, $q=P_l(a)$;
- формується вектор пар елементів $\bar{K}=\{(u_1,v_1),...,(u_n,v_n)\}$, який буде новим значенням відкритого ключа *K*. Величини $P_s(T)$, $P_q(N)$ та вектор $\bar{K}$ передаються отримувачу разом з зашифрованим за допомогою елементів v_j, $j=\overline{1,n}$, повідомленням.

Зрозуміло, що дана схема допускає різні модифікації. В якості основних можна розглядати:

- схему з кодуванням лише чисел N та T,
- паралельне кодування чисел N, T та чисел ключа K,
- послідовне кодування чисел N та T у числа $P_s(T)$ та $P_q(N)$, відповідно, з подальшим перетворенням елементів ключа $K=\{r_1,...,r_n\}$ за традиційною процедурою $r_j * P_s(T) \bmod P_q(N)$, $j=\overline{1,n}$, $s=P_k(a)$, $q=P_l(a)$ і кодуванням отриманих значень вектором пар елементів $\bar{K}=\{(u_1,v_1),...,(u_n,v_n)\}$.

Іншою важливою рисою запропонованої схеми є можливість динамічно змінювати значення $s=P_k(a)$ і $q=P_l(a)$. Використовуючи операцію зсуву для зміни чисел s та q, у вхідній ключовій послідовності задається величина зсуву m, $m\in N\cup\{0\}$, яка дозволяє обчислити нові прості числа $P_k(a)\oplus m$ та $P_l(a)\oplus m$ за формулою (2). Отримані значення можна розглядати як нові параметри процедур шифрування та дешифрування текстових повідомлень.

Для демонстрації дії розробленої схеми повернемося до наведеного вище прикладу. Покладемо a =1. Припустимо, що k =4, l =7. Відповідні прості числа s =7, q =17. Для елементів відкритого ключа *K*={62,93,81,88,102,37} та величин N =105, T =31 обчислимо відповідні значення u_1 =35, v_1=149, u_2 =34, v_2 =179, u_3 =28, v_3 =167, u_4 =25, v_4 =173, u_5 =35, v_5 =191, u_6 =30, v_6 =109, $P_7(31)$ =61, $P_{17}(105)$ =193. Тоді новим відкритим ключем буде множина пар значень $\bar{K}=\{(35,149),(34,179),(28,167),(25,173),(35,191),(30,109)\}$. Величини $P_s(T)$ =61 та $P_q(N)$ =193 є зашифрованими значеннями T =31, N =105. При цьому необхідно відмітити, що усі отримані значення нескладно дешифруються у попередній стан за допомогою простих чисел s =7, q =17.

Зашифровані елементи вхідного повідомлення 011000 110101 101110 з новим відкритим ключем будуть мати вигляд:

011000 задається числом 179 + 167 = 346;
110101 задається числом 149 + 179 + 173 + 109 = 610;
101110 задається числом 149 + 167 + 173 + 191 = 680,

а шифротекстом повідомлення 011000110101101110 є числова послідовність 346,610,680.

Запропонований підхід дозволяє ускладнити процедуру шифрування вхідних повідомлень, що збільшує криптостійкість алгоритму Меркла-Хелмана.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Ralph Merkle, Martin Hellman. Hiding information and signatures in trapdoor knapsacks // IEEE Trans. Information Theory. – 1978. – V.24(5) – P.525–530.
2. Adi Shamir. A polynomial time algorithm for breaking the basic Merkle-Hellman cryptosystem// CRYPTO-1982. – P.279–288.
3. Ernest F. Brickell. Breaking iterated knapsacks / G. R. Blakley, David C. Chaum. Advances in cryptology// Lecture Notes in Computer Science. CRYPTO-1984. – Springer, Berlin, 1985. – V. 196. – P. 342–358.

4. Rodney M. F. Goodman, A. J. McAuley. New trapdoor-knapsack public-key cryptosystem// IEE Proceedings, 1985. – V. 132, Pt. E. – № 6. – P. 289–292.
5. Harald Niederreiter. Knapsack-type cryptosystems and algebraic coding theory// Problems of Control and Information Theory, 1986. – V. 15. – P. 159–166.
6. Masakatu Morii, Masao Kasahara. New public key cryptosystem using discrete logarithm over GF(p)// IEICE Transactions, 1988. – V. J71-D. – № 02. – P. 448–453.
7. Hussain Ali Hussain, Jafar Wadi Abdul Sada, Saad M. Kalipha. New multistage knapsack public-key cryptosystem// International Journal of Systems Science, 1991. – V. 22. – №11. – P. 2313–2320. 8. Zadeh L.A. Fuzzy sets // Inf. Contr., 1965. – V.8. – P. 338–353.

Надійшла до редколегії 25.08.14

Ваднев Д. А., соискатель,
Киевский национальный университет имени Тараса Шевченко, Киев

ОБ ИСПОЛЬЗОВАНИИ ЗАДАЧИ О РЮКЗАКЕ В КАЧЕСТВЕ АЛГОРИТМА ДЛЯ ШИФРОВАНИЯ ДАННЫХ

Рассмотрен алгоритм шифрования данных на основе задачи о рюкзаке. Сформулирована задача повышения криптоустойчивости алгоритма. Предложена схема шифрования, построенная с использованием простых чисел и операций над ними специального вида. Проиллюстрирована работа алгоритма и его модификации на примере конкретной текстовой последовательности.

Ключевые слова: задача о рюкзаке, криптоустойчивочть, алгоритм шифрования.

Vadnev D.A., researcher,
Taras Shevchenko National University of Kyiv

ON THE USE KNAPSACK PROBLEM AS ALGORITHM FOR DATA ENCRYPTION

In this paper a data encryption algorithm based on the problem of the knapsack is considered. The problem of algorithm's crypto resistance increasing is defined. It is proposed an encryption scheme, based on the use of prime numbers and operations on them by special form. The use of the algorithm and its modifications are illustrated on the test example of a text sequence.

Key words: knapsack problem, algorithm's crypto resistance, encryption algorithm.

УДК 517.929.4

Гаркуша Н. І., канд. екон. наук
Київський університет імені Тараса Шевченка, Київ

ДИНАМІКА ОДНІЄЇ ЕКОЛОГІЧНОЇ МОДЕЛІ "ХИЖАК-ЖЕРТВА" БЕЗ ВРАХУВАННЯ ВІКОВОЇ СТРУКТУРИ

Розглядається математична модель екології, що описує ріст популяції і взаємодії хижак-жертва. Модель представлена системою двох нелінійних диференціальних рівнянь із запізненням, що визначає час статевого дозрівання популяції. Одержано умови, при виконанні яких рівноважний стан кількості хижаків і жертв є стійким.

Ключові слова: система диференціальних рівнянь, положення рівноваги, запізнення, стійкість.

Екологія – це наука, що вивчає умови існування живих організмів у взаємозв'язку між організмами і середовищем, в якому вони мешкають. Спочатку екологія розвивалася як складова частина біологічної науки в тісному зв'язку з іншими природничими науками [1,2]. Головний об'єкт екології – екосистеми, що представляють собою єдині комплекси, утворені живими організмами і середовищем їх проживання. Крім того, в область її досліджень входить вивчення окремих видів організмів, їх популяцій, тобто сукупностей особин одного виду, біотичних співтовариств, тобто сукупностей популяцій і біосфери в цілому. В даний час екологія вийшла за рамки суто біологічної науки і перетворилася на міждисциплінарну науку, що вивчає найскладніші проблеми взаємодії людини з навколишнім середовищем.

Одними із завдань екологічної науки є:

- розробка теорії і методів оцінки стійкості екологічних систем всіх рівнів;
- дослідження проблем популяційної екології, екології біотичних співтовариств, збереження біорізноманіття в природі, регулюючого впливу біоти на навколишнє середовище;
- оцінка стану і динаміки природних ресурсів та екологічних наслідків їх споживання;
- розробка і вдосконалення методів управління якістю навколишнього середовища.

Дана робота присвячена розробці та аналізу математичних моделей динаміки екологічних процесів з використанням різницевих, диференційно-різницевих рівнянь з післядією. Крім того, в ній розглядаються питання дослідження стійкості та одержання оцінок збіжності усталених режимів досліджуваних моделей екології, стабілізації положень рівноваги систем, описуваних рівняннями з післядією [3,4].

1. Модель взаємодії популяцій. В роботі розглядається математична модель росту популяції і взаємодії "хижак-жертва" з наступними припущеннями [5, стор.29].

1. Щільність даного виду, тобто число особин на одиницю площі, може бути повністю описана за допомогою однієї змінної, тобто нехтуємо віковими, статевими та генетичними відмінностями.
2. Зміни щільності можуть бути адекватно описані детерміністськими рівняннями.
3. Результати взаємодії в межах виду і між видами відбуваються миттєво.

Тоді модель може бути представлена системою двох диференціальних рівнянь виду [5, стор.38]

$$\dot{x}(t) = ax(t) - bx^2(t) - cx(t)y(t), \quad \dot{y}(t) = ey(t) - f\frac{y^2(t)}{x(t)}.$$

Або у вигляді "з виділеною квазілінійною частиною"

$$\dot{x}(t) = \left[a - bx(t) - cy(t)\right]x(t), \quad \dot{y}(t) = \left[e - f\frac{y(t)}{x(t)}\right]y(t). \qquad (1.1)$$

Рівняння для жертви ідентично для рівняння В. Вольтера з демпфуючим елементом. Рівняння для "хижака" подібно до логістичного рівняння, але другий член змінений, щоб враховувати щільність "жертви".

Якщо враховувати міжвидове запізнювання (час статевого дозрівання), то модель має вигляд системи із запізненням

$$\dot{x}(t) = ax(t) - bx^2(t) - cx(t-\tau)y(t-\tau),\ \dot{y}(t) = ey(t) - f\frac{y^2(t-\tau)}{x(t-\tau)}.$$

2. Дослідження моделі без післядії. Проведемо якісне дослідження отриманої системи без післядії (1.1). Знайдемо особливі точки. Особливі точки системи визначаються системою рівнянь

$$ax - bx^2 - cxy = 0,\ \ ey - f\frac{y^2}{x} = 0. \tag{2.1}$$

Очевидно, що точку, яка є початком координат $O_1(0,0)$, можна виключити з розгляду. Вона означає відсутність популяцій і нецікава. Система рівнянь

$$a - bx - cy = 0,\ \ ex - fy = 0.$$

визначає особливу точку $O_2(x_2, y_2)$, що лежить в першому квадраті

$$O_2(x_2,y_2).\ x_2 = \frac{af}{bf+ce},\ y_2 = \frac{ae}{bf+ce}. \tag{2.2}$$

Лінеарізуємо систему з запізненням (1.1) в околі особливої точки $O_2(x_2,y_2)$. Загальна схема лінеаризації системи з запізненням в околі особливої точки $O_2(x_2,y_2)$ має наступний вигляд

$$\dot{x}(t) = [a - 2bx - cy]\Big|_{\substack{x=x,\\ y=y_2}}(x(t)-x_2) - c\,x\Big|_{\substack{x=x_2,\\ y=y_2}}(y(t)-y_2),$$

$$\dot{y}(t) = \left[f\frac{y^2}{x^2}\right]_{\substack{x=x_2,\\ y=y_2}}(x(t)-x_2) + \left[e - 2f\frac{y}{x}\right]_{\substack{x=x_2,\\ y=y_2}}(y(t)-y_2).$$

Підставивши значення $x = x_2$, $y = y_2$, отримуємо систему двох лінійних диференціальних рівнянь

$$\dot{x}(t) = A_1(x(t)-x_2) + B_1(y(t)-y_2),\ \ \dot{y}(t) = C_1(x(t)-x_2) + D_1(y(t)-y_2),$$

$$A_1 = a - 2bx_2 - cy_2,\ B_1 = -cx_2,\ C_1 = f\frac{y_2^2}{x_2^2},\ D_1 = e - 2f\frac{y_2}{x_2}. \tag{2.3}$$

Позначивши $x = x_2 + \xi$, $y = y_2 + \eta$, отримуємо, так звану систему "рівнянь збурень"

$$\dot{\xi}(t) = A_1\xi(t) + B_1\eta(t),\ \dot{\eta}(t) = C_1\eta(t) + D_1\eta(t).$$

Її характеристичне рівняння має вигляд

$$\lambda^2 - (A_1 + D_1)\lambda + (A_1D_1 - B_1C_1) = 0.$$

Як випливає з умови Гурвіца, необхідною і достатньою умовою стійкості положення рівноваги для систем на площині є виконання нерівностей

$$(A_1 + D_1) < 0,\ (A_1D_1 - B_1C_1) > 0. \tag{2.4}$$

Підставивши значення параметрів з (2.3), отримаємо наступні нерівності

$$\left(a - 2bx_2 - cy_2 + e - 2f\frac{y_2}{x_2}\right) < 0,\ \left[(a - 2bx_2 - cy_2)\left(e - 2f\frac{y_2}{x_2}\right) + cf\frac{y_2^2}{x_2}\right] > 0. \tag{2.5}$$

Якщо підставити значення точки $\hat{I}_2(x_2,y_2)$, то перше з нерівності (2.5) прийме вигляд

$$-\frac{abf}{bf+ce} - e < 0$$

і завжди виконується. Друга нерівність має вигляд

$$e\left[\frac{abf}{bf+ce} + \frac{ce}{f}\right] > 0$$

і завжди виконується.

Таким чином, ненульове положення рівноваги, розташоване у першому квадраті, завжди є асимптотично стійким.

В роботі [5, стор.38] відзначено, "якщо відношення x/y велике (багато особин "жертви" на одного "хижака"), то чисельність "хижака" зростає; якщо $x/y = f/e$, то чисельність "хижака" досягає рівноваги; якщо ж $x/y < f/e$, то воно знижується. З рівнянь випливає наявність в системі швидко затухаючих коливань".

3. Дослідження моделі з післядією. Якщо враховувати міжвидове запізнювання (час статевого дозрівання), то модель має вигляд системи з запізненням (1.2)

$$\dot{x}(t) = ax(t) - bx^2(t) - cx(t-\tau)y(t-\tau),\ \dot{y}(t) = ey(t) - f\frac{y^2(t-\tau)}{x(t-\tau)}.$$

Проведемо дослідження положення рівноваги $O_2(x_2,y_2)$ цієї моделі. Лінеаризація системи (1.2) в околі точки $O_2(x_2,y_2)$ дає систему

$$\dot{x}(t) = [a - 2bx]_{\substack{x=x_2,\\ y=y_2}}(x(t)-x_2) - c\,y\Big|_{\substack{x=x_2,\\ y=y_2}}(x(t-\tau)-x_2) - c\,x\Big|_{\substack{x=x_2,\\ y=y_2}}(y(t-\tau)-y_2),$$

$$\dot{y}(t) = e\left(y(t) - y_2\right) + f\frac{y^2}{x^2}\Big|_{\substack{x=x_2,\\ y=y_2}} \left(\left(x(t-\tau) - x_2\right)\right) - 2f\frac{y}{y}\Big|_{\substack{xx=x_2,\\ y=y_2}} \left(y(t-\tau) - y_2\right).$$

Її можна записати у вигляді

$$\dot{x}(t) = \left[a - 2bx_2\right]\left(x(t) - x_2\right) - cy_2\left(x(t-\tau) - x_2\right) - cx_2\left(y(t-\tau) - y_2\right),$$

$$\dot{y}(t) = e\left(y(t) - y_2\right) + \frac{y_2^2}{x_2^2}\left(x(t-\tau) - x_2\right) - 2f\frac{y_2}{x_2}\left(y(t-\tau) - y_2\right).$$

Позначивши

$$A_2 = a - 2bx_2,\ A_3 = -cy_2,\ B_3 = -cx_2,\ D_2 = e,\quad ,\ D_3 = -2f\frac{y_2}{x_2},$$

$$x_2 = \frac{af}{bf + ce},\ y_2 = \frac{ae}{bf + ce},$$

отримаємо

$$\dot{x}(t) = A_2\left(x(t) - x_2\right) + A_3\left(x(t-\tau) - x_2\right) + B_3\left(y(t-\tau) - y_2\right),$$

$$\dot{y}(t) = D_2\left(y(t) - y_2\right) + C_3\left(x(t-\tau) - x_2\right) + D_3\left(y(t-\tau) - y_2\right). \tag{3.1}$$

Або у векторно-матричному вигляді

$$\dot{z}(t) = Az(t) + Bz(t-\tau), \tag{3.2}$$

де

$$z(t) = \begin{pmatrix}\xi(t)\\ \eta(t)\end{pmatrix} = \begin{pmatrix}x(t) - x_2\\ y(t) - y_2\end{pmatrix}\ A = \begin{bmatrix}A_2 & 0\\ 0 & D_2\end{bmatrix},\ B = \begin{bmatrix}A_3 & B_3\\ C_3 & D_3\end{bmatrix}. \tag{3.3}$$

Неважко побачити, що

$$A_1 = A_2 + A_3,\ B_1 = B_3,\ C_1 = C_3,\ D_1 = D_2 + D_3. \tag{3.4}$$

Дослідимо вплив запізнювання на стійкість положення рівноваги.

Як відомо, необхідною умовою стійкості системи з запізненням є асимптотична стійкість системи без запізнювання, тобто умови заперечності дійсних частин власних чисел матриці $A + B$ [6,7]. Як випливає з викладеного вище, ця умова виконується. Тоді, в силу безперервності, при достатньо малому запізненні $\tau < \tau_0$ буде асимптотично стійким і положення рівноваги $\hat{I}_2(x_2, y_2)$ системи з запізненням (1.2). Однак, при збільшенні $\tau > 0$ може статися біфуркація, і стале становище рівноваги може стати нестійким. Встановимо значення величин параметрів системи, при яких зберігається стійкість.

Характеристичне рівняння із запізненням (3.1) має вигляд

$$\det\left\{A + e^{-\lambda\tau}B - \lambda E\right\} = 0,$$

або

$$\begin{vmatrix}A_2 + A_3e^{-\lambda\tau} - \lambda & B_3e^{-\lambda\tau}\\ C_3e^{-\lambda\tau} & D_2 + D_3e^{-\lambda_\tau} - \lambda\end{vmatrix} = \left(A_2 + A_3e^{-\lambda\tau} - \lambda\right)\left(D_2 + D_3e^{-\lambda\tau} - \lambda\right) - C_3B_3e^{-2\lambda\tau} = 0.$$

Його можна переписати у вигляді

$$\lambda^2 - \left[\left(A_3 + D_3\right)e^{-\lambda\tau} + \left(A_2 + D_2\right)\right]\lambda + \left[\left(A_3 + D_3\right)e^{-2\lambda\tau} + \left(A_3D_2 + A_2D_3\right)e^{-\lambda\tau} + A_2D_2\right] = 0.$$

Умовою асимптотичної стійкості положення рівноваги є заперечність дійсних частин коренів характеристичного рівняння, тобто $\mathrm{Re}\,\lambda_i < 0$, $i = 1,2,3,...$ Однак, перевірка цієї умови, в загальному випадку, є важкою.

Тому для отримання умов стійкості системи з запізненням скористаємося другим методом Ляпунова. А саме методом функцій Ляпунова з додатковою умовою Б.С. Разумихина при оцінці похідної. Функція Ляпунова береться у вигляді квадратичної форми

$$V(\xi, \eta) = h_{11}\xi^2 + 2h_{12}\xi\eta + h_{22}\eta^2, \tag{3.5}$$

Тобто в вигляді $V(z) = z^THz$, де

$$H = \begin{bmatrix}h_{11} & h_{12}\\ h_{12} & h_{22}\end{bmatrix},\ z = \begin{pmatrix}x - x_2\\ y - y_2\end{pmatrix}. \tag{3.6}$$

Має місце наступне твердження.

Теорема. Нехай існують коефіцієнти c_{11}, c_{12}, c_{22}, які задовольняють нерівностям

$$c_{11} > 0,\ c_{11}c_{22} - c_{12}^2 > 0, \tag{3.7}$$

які задовольняють нерівностям

$$\lambda_{\min}(C) - 2|HB|\left(1 + \sqrt{\frac{\lambda_{\max}(H)}{\lambda_{\min}(H)}}\right) > 0. \tag{3.8}$$

Тут

$$\lambda_{\min}(C) = \frac{1}{2}\left[\left(c_{11} + c_{12}\right) - \sqrt{\left(c_{11} - c_{12}\right)^2 + 4c_{12}^2}\right],\ \lambda_{\min}(H) = \frac{1}{2}\left[\left(h_{11} + h_{12}\right) - \sqrt{\left(h_{11} - h_{12}\right)^2 + 4h_{12}^2}\right],$$

$$\lambda_{\max}(H)=\frac{1}{2}\left[(h_{11}+h_{12})+\sqrt{(h_{11}-h_{12})^2+4h_{12}^2}\right],\quad h_{11}=\frac{\Delta_{11}}{\Delta},\ h_{12}=\frac{\Delta_{12}}{\Delta},\ h_{22}=\frac{\Delta_{22}}{\Delta},\tag{3.8}$$

де

$$\Delta=\begin{vmatrix}A_2+A_3 & C_3 & 0\\ B_3 & A_2+A_3+D_2+D_3 & C_3\\ 0 & B_3 & D_2+D_3\end{vmatrix},\ \Delta_{11}=-\begin{vmatrix}c_{11}/2 & C_3 & 0\\ c_{12} & A_2+A_3+D_2+D_3 & C_3\\ c_{22}/2 & B_3 & D_2+D_3\end{vmatrix},$$

$$\Delta_{12}=-\begin{vmatrix}A_2+A_3 & c_{11}/2 & 0\\ B_3 & c_{12} & C_3\\ 0 & c_{22}/2 & D_2+D_3\end{vmatrix},\ \Delta_{22}=-\begin{vmatrix}A_2+A_3 & C_3 & c_{11}/2\\ B_3 & A_2+A_3+D_2+D_3 & c_{12}\\ 0 & B_3 & c_{22}/2\end{vmatrix}.\tag{3.9}$$

Тоді положення рівноваги $O_2(x_2,y_2)$ є асимптотично стійким при довільному запізненні $\tau>0$.

Доведення. Нехай матриця є позитивно певної матрицею. Обчислимо повну похідну функції (3.5) в силу системи (3.2). Отримуємо наступне

$$\frac{d}{dt}V(z(t))=z'(t)Hz(t)+z(t)Hz'(t)=\left(Az(t)+Bz(t-\tau)\right)^T Hz(t)+z^T(t)H\left(Az(t)+Bz(t-\tau)\right)=$$

$$=z^T(A+B)^T Hz(t)+z^T(t)H(A+B)-2z^T(t-\tau)HBz(t).$$

або

$$\frac{d}{dt}V(z(t))=-z^T(t)\left[-(A+B)^T H-H(A+B)\right]z(t)-2z^T(t-\tau)HBz(t).$$

Як випливає з [8], якщо $A+B$ асимптотично стійка матриця, то при довільній додатно визначеній матриці

$$C=\begin{bmatrix}c_{11} & c_{12}\\ c_{12} & c_{22}\end{bmatrix}\tag{3.7}$$

матричне рівняння Ляпунова

$$(A+B)^T H+H(A+B)=-C\tag{3.7}$$

має єдине рішення – позитивно певну матрицю H. Тому для повної похідної функції Ляпунова отримуємо таку нерівність

$$\frac{d}{dt}V(z(t))\le-\lambda_{\min}(C)|z(t)|^2+2|HB|\left[|z(t)|+|z(t-\tau)|\right].$$

Використовуючи умову Разуміхіна Б.С. про оцінку похідної за умови "підходу до поверхні рівня з внутрішньої сторони", отримуємо

$$\lambda_{\min}(H)|z(t-\tau)|^2\le V(z(t-\tau))<V(z(t))\le\lambda_{\max}(H)|z(t)|^2.$$

Звідси випливає, що $$|z(t-\tau)|\le\sqrt{\frac{\lambda_{\max}(H)}{\lambda_{\min}(H)}}|z(t)|.$$

І для повної похідної отримуємо нерівність

$$\frac{d}{dt}V(z(t))\le-\left[\lambda_{\min}(C)-2|HB|\sqrt{\frac{\lambda_{\max}(H)}{\lambda_{\min}(H)}}\right]|z(t)|^2.$$

Якщо вираз в квадратних дужках позитивний, то похідна є негативно визначеною функцією, і положення рівноваги буде асимптотично стійким.

Розглянемо матричне рівняння Ляпунова (3.7) з матрицями (3.3), записане в матричному вигляді

$$\begin{bmatrix}A_2+A_3 & B_3\\ C_3 & D_2+D_3\end{bmatrix}^T\begin{bmatrix}h_{11} & h_{12}\\ h_{12} & h_{22}\end{bmatrix}+\begin{bmatrix}h_{11} & h_{12}\\ h_{12} & h_{22}\end{bmatrix}\begin{bmatrix}A_2+A_3 & B_3\\ C_3 & D_2+D_3\end{bmatrix}=-\begin{bmatrix}c_{11} & c_{12}\\ c_{12} & c_{22}\end{bmatrix}.\tag{3.8}$$

Як випливає з критерію Сильвестра, щоб матриця була додатно визначеною необхідно і достатньо виконання нерівностей (3.7)

$$c_{11}>0,\qquad c_{11}c_{22}-c_{12}^2>0.$$

Рішенням матричного рівняння (3.8) буде

$$h_{11}=\frac{\Delta_{11}}{\Delta},\ h_{12}=\frac{\Delta_{12}}{\Delta},\ h_{22}=\frac{\Delta_{22}}{\Delta},\tag{(3.9)}$$

Де

$$\Delta=\begin{vmatrix}A_2+A_3 & C_3 & 0\\ B_3 & A_2+A_3+D_2+D_3 & C_3\\ 0 & B_3 & D_2+D_3\end{vmatrix},\quad \Delta_{11}=-\begin{vmatrix}c_{11}/2 & C_3 & 0\\ c_{12} & A_2+A_3+D_2+D_3 & C_3\\ c_{22}/2 & B_3 & D_2+D_3\end{vmatrix},$$

$$\Delta_{12}=-\begin{vmatrix}A_2+A_3 & c_{11}/2 & 0\\ B_3 & c_{12} & C_3\\ 0 & c_{22}/2 & D_2+D_3\end{vmatrix},\ \Delta_{22}=-\begin{vmatrix}A_2+A_3 & C_3 & c_{11}/2\\ B_3 & A_2+A_3+D_2+D_3 & c_{12}\\ 0 & B_3 & c_{22}/2\end{vmatrix}.\tag{3.10}$$

Оскільки, за умовою, матриця $A+B$ асимптотично стійка, то при виконанні умов

$$c_{11}>0,\ c_{11}c_{22}-c_{12}^2>0$$

матриця H (3.6)) з елементами, визначеними в (3.9), (3.10), буде позитивно визначеною. І, якщо виконується нерівність (3.8), то похідна функції Ляпунова є негативно визначеною, і справедливо твердження теореми.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Гринь С.А., Кузнецов П.В., Шапорев П.В., Боглаенко Д.В., Экология. Тексты лекций. Харьков, НТУ "ХПИ", 2007. – 172 с.
2. Арский Ю.М., Данилов-Данильян В.И., Залиханов М.Ч., Кондратьев К.Я., Котляков В.М., Лосев К.С. Экологические проблемы: Кто виноват и что делать. – Москва, Изд.во МНЭПУ, 1997. – 332 с.
3. Гаркуша Н.І. Про близькість моделей динаміки Вольтера та Гудвіна // Вісник Київського національного університету імені Тараса Шевченка. Серія: Фізико-математичні науки, в.2, 2013. – С. 3.
4. Гаркуша Н.І. Динаміка моделі Гудвіна з післядією // Вісник Київського національного університета імені Тараса Шевченка. Серія: Фізико-математичні науки, в.4, 2013. – С.139-142
5. Смит Дж. Модели в экологии. – М., Мир, 1976. – 184 с.
6. Эльсгольц Л.Э., Норкин С.Б. Введение в теорию дифференциальных уравнений с отклоняющимся аргументом. – М., Наука, 1970. – 240 с.
7. Хейл Дж. Теория функционально-дифференциальных уравнений. – М.: Мир, 1984. – 421 с.
8. Барбашин Е.А. Метод функций Ляпунова. – М.: Наука, 1970 . – 240 с.
9. Хусаинов Д.Я., Шатырко А.В. Метод функция Ляпунова в исследовании устойчивости дифференциально-функциональных систем. – Киев, Изд.-во Киевского университета, 1977. – 236 с.

Надійшла до редколегії 25.09.14

Н. И. Гаркуша, канд. экон. наук,
Киевский национальный университет имени Тараса Шевченко, Киев

ДИНАМИКА ОДНОЙ ЭКОЛОГИЧЕСКОЙ МОДЕЛИ "ХИЩНИК-ЖЕРТВА" БЕЗ УЧЕТА ВОЗРАСТНОЙ СТРУКТУРЫ

Рассматривается математическая модель экологии, описывающая рост популяций и взаемодействия хищник-жертва. Модель представлена системой двух нелинейных дифференциальных уравнений с запаздыванием, определяющим время полового созревания популяции. Получены условия, при выполнении которых равновесное состояние количества хищников и жертв является устойчивым.

Ключевые слова: система дифференциальных уравнений, положение равновесия, запаздывание, устойчивость.

Harkusha N.I., PhD,
Taras Shevchenko National University of Kyiv

DYNAMICS OF ONE OF ECOLOGICAL MODELS "PREDATOR-PREY" WITHOUT REGARD TO AGE STRUCTURE

In this paper the mathematical model of the environment, describing the growth of the population and predator-prey interactions. Model represented by a system of two nonlinear differential equations with delay in determining the time of puberty population. We obtain conditions under which the equilibrium state is the number of predators and prey is stable.

Key words: the system of differential equations, the equilibrium position, delay, stability.

УДК 519.83 – Теория игр

С. И. Доценко, канд. физ.-мат. наук, ст. научн. сотр.,
Киевский национальный университет имени Тараса Шевченко, Киев

ВЕКТОР ШЕПЛИ ДЛЯ ИЕРАРХИЧЕСКИХ ИГР

Рассмотрен ряд примеров вычисления вектора Шепли для кооперативной игры в случае. если игроки, образующие коалицию, неравноправны и между ними существует иерархия.

Ключевые слова: теория кооперативных игр, вектор Шепли, иерархические игры.

Введение. Теория кооперативных игр (ТКИ) – это раздел теории игр, в котором игры рассматриваются без учёта стратегических возможностей игроков. В отличии от некооперативных игр, в которых каждый игрок выбирает стратегию, исходя из своих эгоистических мотивов, стремится максимизировать собственный выигрыш и безразличен к выигрышам остальных игроков, в ТКИ игроки (или агенты) действуют сообща, стремясь максимизировать суммарный выигрыш. Конфликт же возникает на этапе дележа полученного суммарного выигрыша. Каждый из игроков может претендовать на определенную часть общего выигрыша, аргументируя свой вклад в общие усилия при его получении. В терминах ТКИ поддаются описанию многие экономические и социальные явления.

Основоположником ТКИ принято считать американского математика и экономиста Ллойда Шепли, лауреата нобелевской премии по экономике за 2012 год. Ключевым понятием ТКИ является вектор Шепли, описывающий способ справедливого дележа, компонентами которого являются доли игроков в общем выигрыше.

Рассмотрим основные понятия ТКИ.

Пусть N – множество игроков , n – их количество .

Определение.Коалиция – подмножество множества игроков. Большая (Гранд) коалиция – это множество всех игроков.

Для кооперативной игры задается отображение $2^N \to R$ из множества всех коалиций в множество действительных чисел, которое носит название характеристической функции игры.

Характеристическая функция каждой коалиции ставит в соответствие совместный заработок ее членов. Характеристическая функция в принципе может быть отрицательной (распределение затрат), но чаще она неотрицательная. При этом всегда предполагается, что пустая коалиция ничего не зарабатывает и никому ничего не должна, т.е. V(ф)=0.

Определение. Вкладом игрока i в коалицию S (где $i \notin S$) называется величина $V(S \cup i) - V(S)$ и обозначается Add(i,S).

Зафиксируем некоторую перестановку игроков. Для данной перестановки заработком каждого игрока назовем его вклад в коалицию, состоящую из предыдущих игроков. Ясно, что заработок может зависеть от порядка игроков в перестановке.

Вектор Шепли (ВШ) – это вектор заработков игроков, усредненный по всем возможным n! Перестановкам

$$Sh(V) = \frac{1}{n!} \sum_{\Pi_j} (add(1, \Pi_j), .., add(n, \Pi_j)) \qquad (1)$$

Более удобная формула вычисления ВШ имеет такой вид: $Sh(V) = (\varphi_1(V),...,\varphi_n(V))$,

где $$\varphi_i(V) = \sum_{S,i\in S} \frac{(|S|-1)!(n-|S|)!}{n!}(V(S)-V(S\setminus i)), \quad (2)$$

а под. символом |S| подразумевается размер коалиции S.

Такая формула иногда приводится в качестве определения ВШ, что является верным с формальной точки зрения, но затрудняет понимание сути.

Другим способом вычисления вектора Шепли является предварительное вычисление функции потенциала, при этом оказывается, что компоненты ВШ могут быть найдены как разности потенциалов на последнем этапе вычислений. Рассмотрим этот способ.

Пусть задано отображение $2^N \to R$ (это отображение зависит от характеристической функции игры и ставит в соответствие каждой коалиции некоторое действительное число).

Для данного отображения введем понятие маргинального вклада игрока i в коалицию S (где i € S).

Di P(S,V)=P(S,V)-P(S\{i},V)

Определение. Отображение $P(2^N,V) \to R$ называется потенциалом, если она для любой коалиции S удовлетворяет условиям

$$P(\varphi) = 0, \sum_i D^i P(S,V) = V(S). \quad (3)$$

Формулу (3) можно переписать в эквивалентном виде

$$P(\varphi) = 0, P(S) = \frac{1}{|S|}\left(V(S) + \sum_{i\in S} P(S/i)\right), \quad (4)$$

что позволяет вычислять потенциал рекуррентно (вначале для 1-элементных коалиций, затем для 2-элементных, и т.д., вплоть до гранд- коалиции).

Тогда оказывается, что компоненты ВШ равны маргинальному вкладу потенциала гранд-коалиции, т.е. $\varphi_i = D^i P(N)$.

ВШ был введен самим Ллойдом Шепли следующим образом. Вначале были введены четыре аксиомы Шепли для вектора распределения (сформулированные аксиомы на самом деле – это свойства, которым должен удовлетворять вектор распределения).

Аксиомы Шепли для вектора распределения $(\phi_1(V),...,\phi_n(V))$.

1. Эффективность. При эффективном распределении должна быть распределена вся доступная сумма (т.е выигрыш гранд-коалиции должен быть равен V(N)), $\sum_{i\in N} \phi_i(V) = V(N)$.

2. Симметрия. Симметричные игроки должны получать равные доли при распределении. Это значит, что если для игроков i и j имеет место

$V(S\cup\{i\}) = V(S\cup\{j\})$ для любой коалиции S, не содержащей игроков i и j, то $\phi_i(V) = \phi_j(V)$.

3. Свойство болванов. Игрок, вносящий нулевой вклад в любую коалицию, при распределении получает ноль. Другими словами, для игрока i такого, что $V(S\cup\{i\}) = V(S)$ для любой коалиции S, не содержащей игрока i, $\phi_i(V) = 0$.

4. Аддитивность. Если V_1 и V_2 – две характеристические функции, то $\phi_i(V_1+V_2) = \phi_i(V_1) + \phi_i(V_2)$.

Теорема. Существует единственный вектор распределения, удовлетворяющий аксиомам 1–4. Этот вектор может быть найден по формулам (1) или (2).

Вектор Шепли для случая иерархической структуры игроков. Пусть как в классической кооперативной игре на множестве игроков задана характеристическая функция $2^N \to R$ – отображение из множества всех коалиций в множество действительных чисел и пусть данная функция принимает неотрицательные значения.

На множестве игроков зададим иерархию как некоторое отношение частичного порядка, (т.е. отношение, удовлетворяющее свойствам антирефлексивности, антисимметричности и транзитивности). Пусть данное отношение описывает отношение субординации начальник-подчиненный. Ориентированный граф, описывающий такое отношение субординации, имеет вид дерева либо леса.

Рассмотрим иерархический аналог вектора Шепли в предположении, что подчиненный может получать причитающийся ему доход лишь в тех коалициях, в которые входят все его начальники, в противном случае начальники, не входящие в данную коалицию, присваивают его доход и делят его между собой, и приведем несколько примеров, для которых такой подход является правомерным.

Предлагаемый механизм расчета доходов игроков будет состоять из двух этапов.

На первом этапе составляется таблица расчета вектора Шепли, как в классическом случае, где для всех возможных перестановок игроков последовательно записываются вклады игроков в коалиции, состоящие из всех игроков, стоящих в данной перестановке левее него.

На втором этапе составляется аналогичная таблица, в которую вносятся штрафы за нарушение субординации. Перед заполнением данной таблицы нужно для каждого игрока выписать множество его начальников. Рассмотрим произвольную перестановку $(\vec{s}_1, A, \vec{s}_2)$ и опишем механизм перераспределения, связанный с некоторым игроком A. Если все начальники A принадлежат $\vec{s}_1$ (или, другими словами, лежат слева от A), либо же A вообще не имеет начальников, то A не нарушает субординации и перераспределения не происходит. Если же один или несколько начальников A принадлежат $\vec{s}_2$ (или, другими словами, лежат справа от A), то в клетку A этой строки пишется (со знаком минус) штраф, который платит A за нарушение субординации, равный вкладу A в коалицию $\vec{s}_1$. Этот штраф перераспределяется поровну между его начальниками, принадлежащими $\vec{s}_2$ (лежащими справа). Однако, можно применить более простую процедуру перераспределения, а именно, отдать штраф начальнику A, стоящему в $\vec{s}_2$ правее всех остальных, что не повлияет на окончательный расчет. Действительно, пусть $\vec{s}_2$ содержит k начальников A. Рассмотрим все

перестановки, в которых начальники А стоят на тех же местах, что и в А, таких перестановок будет k!. Если штраф в каждой перестановке делить поровну, то каждому начальнику пишется дополнительный доход $\frac{Add(A,s_1)}{k}$, а по всем k! перестановкам – $k!\frac{Add(A,s_1)}{k} = (k-1)!Add(A,s_1)$. Если же штраф распределять в пользу того начальника, который стоит правее всех, то он будет получать штраф $Add(A,s_1)$ целиком, и количество перестановок (из рассматриваемых k!) равно (k-1)!, и таким образом сумма доходов каждого начальника составит те же самые $(k-1)!Add(A,s_1)$. Поэтому в дальнейшем для удобства будем записывать штраф в пользу начальника, стоящего правее всех остальных. Затем для каждого находится сумма его штрафов и доходов, делится на число всех перестановок n! и добавляется к соответствующей компоненте вектора Шепли, найденной из 1-й таблицы.

Полученная величина обладает такими свойствами.

1. Нейтральность. Игрок, не имеющий начальников и подчиненных, получает тот же доход, что и в классическом случае.

2. Неотрицательность. Если характеристическая функция игры $2^N \to R_0^+$ неотрицательная, то при любом отношении субординации выигрыши всех игроков неотрицательные.

Действительно, в каждом случае игрока либо штрафуют на величину вклада, вносимого в определенную коалицию, либо не штрафуют. Поэтому, если составить таблицу, элементы которой будут равны сумме соответствующих таблиц.

3. Симметричность. Одинаковые игроки имеют одинаковые доходы.

Игроки являются одинаковыми, если они вносят одинаковый вклад в одинаковые коалиции, а также имеют одинаковый список начальников и подчиненных.

4. Аддитивность. Пусть $V: 2^N \to R_0^+, W: 2^N \to R_0^+$ – две игры. Заданные на одном множестве игроков и пусть для этих двух игр задано одно и то же отношение субординации. Если игре V соответствует вектор выплат $\vec{x}_v$, а игре W – вектор выплат $\vec{x}_w$. Тогда игре V+W соответствует вектор выплат $\vec{x}_v + \vec{x}_w$.

5. Болванизм. В классической кооперативной игре болваном (dummy) назывался игрок, вносивший нулевой вклад в любую коалицию. В векторе Шепли компоненты болванов равны нулю. В кооперативной игре с субординацией для того, чтобы иметь ненулевой доход, нужно обладать по крайней мере одним из двух свойств:

а) Вносить положительный вклад в коалицию, содержащую всех начальников.

б) Иметь по крайней мере одного подчиненного, вносящего положительный вклад в коалицию, не содержащую его (начальника).

Рассмотрим несколько примеров вычисления векторов Шепли для иерархических систем, где задание той или иной иерархии обосновано содержательной постановкой задачи.

Пример 1. Распределение скидки. Пусть есть три покупателя A,B,C, которые закупают однородный товар в количестве 10, 20 и 40 ед. по цене 1 у.е. за единицу. За оптовую закупку товара магазин предоставляет такие скидки: от 50 ед. – 10 %, от 60 ед. –15 %, от 70 ед. – 20 %.

Пусть A,B и C объединяются, делают совместную оптовую закупку в количестве 70 ед. и экономят на этом 14 у.е. Возникает вопрос – как распределить сэкономленную сумму? В реальной жизни скорее всего покупатели распределили бы скидку пропорционально количеству купленного товара, т.е. 2, 4 и 8 у.е. соответственно. Оказывается, это не совсем правильно. Характеристическая функция игры имеет вид:

V(A)=V(B)=V(C)=0, V(A,B)=0, V(A,C)=5, V(B,C)=9, V(A,B,C)=14.

Таблица для вычисления вектора Шепли имеет вид:

***Таблица* 1**

	A	**B**	**C**
ABC	0	0	14
ACB	0	9	5
BAC	0	0	14
BCA	5	0	9
CAB	5	9	0
CBA	5	9	0
$\sum$	15	27	42
Шепли	2.5	4.5	7

Таким образом, справедливое распределение скидки (2.5; 4.5; 7).

Пусть теперь магазин предоставляет скидки на тех же условиях, но к тому же требует наличие дисконтной карты, и такая карта есть только у A. Тогда рассмотрим иерархическое отношение A→B, A→C. Таблица штрафов будет иметь вид:

***Таблица* 2**

	A	**B**	**C**
ABC	0	0	0
ACB	0	0	0
BAC	0	0	0
BCA	+9	0	-9
CAB	0	0	0
CBA	+9	-9	0
$\sum$	+18	-9	-9
Среднее	+3	-1.5	-1.5

Тогда справедливое распределение скидки (5.5; 3; 5.5).

Пример 2. Продажа кроссовок со шнурками. У Пети и Васи есть по одному кроссовку, а у Коли шнурки. Один кроссовок ничего не стоит.

Пара кроссовок без шнурков стоит 300 грн.

Пара кроссовок со шнурками стоит 350 грн.

Шнурки можно продать отдельно за 20 грн.

Тогда характеристическая функция имеет вид:

V(П)=V(В)=0, V(К)=20, V(П,В)=300,

V(П,К)=V(В,К)=20, V(П,В,К)=350.

Таблица для вычисления вектора Шепли имеет вид:

***Таблица* 3**

	П	**В**	**К**
(П,В,К)	0	300	50
(П,К,В)	0	330	20
(В,П,К)	300	0	50
(В,К,П)	330	0	20
(К,П,В)	0	330	20
(К,В,П)	330	0	20
$\sum$	960	960	180
Шепли	160	160	30

Предположим, что Вася и Петя совместно контролируют торговлю обувью и Коля может продать шнурки только с их совместного разрешения. Тогда рассмотрим иерархическое отношение: П→К, В→К. Таблица штрафов будет иметь вид:

***Таблица* 4**

	П	**В**	**К**
(П,В,К)	0	0	0
(П,К,В)	0	+20	-20
(В,П,К)	0	0	0
(В,К,П)	+20	0	-20
(К,П,В)	0	+20	-20
(К,В,П)	+20	0	-20
$\sum$	+40	+40	-80
Среднее	+6 1/3	+6 1/3	-12 2/3

Тогда справедливое распределение доходов от продажи кроссовок со шнурками имеет вид: (166.33; 166.33; 17.33).

Пример 3. Задача о банкротстве. Пусть банкрот имеет некоторую сумму, которую он может вернуть своим кредиторам, однако суммарные претензии кредиторов превышают данную сумму. Если суд признал все претензии кредиторов правомерными, то как должна быть разделена доступная сумма межу кредиторами?

В [3] был проведен анализ данной задачи на оснований текстов Талмуда. В Талмуде была предложена следующая задача. Пусть у человека было три жены, которым он завещал 100, 200 и 300 у.е. После его смерти и распродажи имущества оказалось, что наличной суммы недостаточно, чтобы выплатить завещание всем трем претенденткам. В этом случае Талмуд рекомендует три варианта дележа для случаев, когда наличная сумма составляет 100, 200 и 300 у.е.

Данная задача решается по принципу последовательного удовлетворения претензий, имеющего непосредственное отношение к вектору Шепли. Зафиксируем некоторую перестановку претендентов, и будем выдавать им требуемые суммы до тех пор, пока хватает денег. Последнему претенденту или претендентам денег не хватит. Данную процедуру проделаем для всех n! перестановок претендентов и найдем средние выплаты. Оказалось, что в двух случаях из трех дележ, предложенный в Талмуде совпадает с дележом, найденным на основании построения вектора Шепли, а в третьем случаи предложенные платежи имеют сходную структуру.

***Таблица* 5**

	A (100)	**B (200)**	**C (300)**
100, совпадает	33.33	33.33	33.33
200, Т/Ш	50 /33.33	75/ 83.33	75/83.33
300, совпадает	150	100	50

Рассмотрим пример дележа с подчинением. Пусть доступная сумма банкрота составляет 120 у.е. и на нее есть три претендента A, B и C с претензиями 30, 60 и 90 у.е. соответственно. Кроме того, предположим, что A является дочерним филиалом B, т.е. имеет место отношение B→A, поэтому приоритет в удовлетворении претензий принадлежит A. Расчетные таблицы приведены ниже.

***Таблица* 6**

	A	**B**	**C**
ABC	30	60	30
ACB	30	0	90
BAC	30	60	30
BCA	0	60	60
CAB	30	0	90

Окончание табл. 6

	A	B	C
СВА	0	30	90
$\sum$	120	210	390
Шепли	20	35	65

Таблица 7

	A	B	C
ABC	-30	+30	0
ACB	-30	+30	0
BAC	0	0	0
BCA	0	0	0
CAB	-30	+30	0
CBA	0	0	0
$\sum$	-90	+90	0
Среднее	-15	+15	0

Таким образом, справедливое распределение выплат кредиторам с учетом отношения иерархии имеет вид: (5, 50, 65).

Выводы. Предложенный метод и приведенные примеры расширяют концепцию вектора Шепли на круг игр, в которых игроки могут вступать в иерархические отношения "начальник-подчиненный". Разобранные примеры показывают, что, как и следовало ожидать, в рассматриваемой схеме происходит перераспределение доходов подчиненных в пользу начальников. Другими словами по сравнению с компонентами классического вектора Шепли доходы начальников растут, а доходы починенных уменьшаются.

СПИСОК ИСПОЛЬЗОВАНЫХ ИСТОЧНИКОВ

1. A.Roth, L.Shapley. Scientific background. Stable allocations and the practice of market design. Advanced information on Nobel prize in economics. http://www.nobelprize.org/nobel_prizes/economics/laureates/2012/advanced-economicsciences 2012.pdf
2. С. Доценко. Вектор Шепли как способ справедливого распределения. // Журнал обчислювальної та прикладної математики, 2013, №3 (113), 12 с.
3. R. Aumann, M. Maschler. Game theoretic analysis of a bankruptcy problem from the Talmud. // Journal of economic theory 36 (1985), p. 195–213.

Поступила в редколегию 22.09.14

С. І. Доценко, канд. фіз.-мат. наук, ст. наук. співроб.,
Київський національний університет імені Тараса Шевченка

ВЕКТОР ШЕПЛІ ДЛЯ ІЄРАРХІЧНИХ ІГОР

Розглянуто ряд прикладів обчислення вектора Шеплі для кооперативної гри у випадку, коли гравці, що утворюють коаліцію є нерівноправними та між ними існує ієрархія.

Ключові слова: теорія корпоративних ігор, вектор Шеплі, ієрархічні ігри.

Dotsenko S.I., PhD, phusical and mathematical sciences, senior researcher
Taras Shevchenko National University of Kyiv

SHAPLEY VALUE FOR HIERARCHICAL GAMES

The article considers Shapley value for cooperative games in the case, when players haven't equal rights, and there is some subordination among them.

Key words: theory of cooperative games, the Shapley value, hierarchical games.

УДК 519.87

Є. В. Івохін, д-р фіз.-мат. наук, доцент,
Київський національний університет імені Тараса Шевченка, Київ

ПРО ПІДХІД ДО РОЗВ'ЯЗАННЯ ТРАНСПОРТНОЇ ЗАДАЧІ З НЕЧІТКИМИ РЕСУРСАМИ

В роботі розглянуто метод пошуку оптимального розв'язку нечіткої транспортної задачі, ресурси в якій представлено нечіткими трикутними числами. Проілюстровано використання метода на прикладі реальної транспортної задачі. Розглянуто узагальнення методики вирішення нечіткої транспортної задачі з урахуванням важливості обмежень. Запропоновано залучення розробленого підходу для вирішення нечітких транспортних задач загального вигляду.

Ключові слова: транспортна задача лінійного програмування, множина розв'язків, методи прийняття рішень, нечіткі числа.

Вступ. Зміст транспортної задачі (ТЗ), яка є одним з прикладів задач математичного програмування, полягає у розподілі продукції будь-якої групи "виробників" серед будь-якої групи "споживачів" економічно найбільш оптимальним способом із заданими обмеженнями "пропозиції" та "попиту". В залежності від природи функції вартості перевезень транспортні задачі діляться на лінійні та нелінійні транспортні задачі.

Транспортна задача, що розв'язується на мережі, яка складається з кінцевого числа вузлів і дуг між ними, є задачею лінійного програмування (ЗЛП), якщо загальна вартість перевезень та обмеження на обсяги перевезень задаються лінійними функціями. Типовою проблемою є транспортування продукції від m виробників до n споживачів з потужностями $a_1, a_2, ..., a_m$ та $b_1, b_2, ..., b_n$, відповідно. Для знаходження ефективного плану перевезень задається вартість транспортування одиниці продукції c_{ij} з пункту виробництва $i, i = \overline{1,m}$, до пункту споживання $j, j = \overline{1,n}$, а змінні x_{ij}, $i = \overline{1,m}$, $j = \overline{1,n}$, визначають обсяги перевезень від виробника до місця призначення.

Ефективні алгоритми вирішення транспортної задачі були розроблені для випадків, коли вартість та коефіцієнти споживання відомі апріорі. Однак на практиці досить часто розглядаються приклади, в яких ці параметри не можуть бути задані точно. Наприклад, вартість доставки може змінюватися в процесі транспортування. Запити на обсяги споживання можуть бути невизначеними через специфіку деяких неконтрольованих факторів.

В роботі [1] Bellman та Zadeh запропонували концепцію прийняття рішення в нечітких умовах, яку можна розглядати як один із способів розв'язання транспортної задачі з неточними параметрами. Стаття Lai та Hwang [2] присвячена ситуації, в якій всі параметри моделі ТЗ є нечіткими. У 1979 році Isermann [3] розробив алгоритм для вирішення ТЗ, який визначає її ефективні розв'язки. Ringuest та Rinks [4] запропонували дві ітераційні схеми для вирішення лінійних багатокритеріальних транспортних задач. S.Chanas та D.Kuchta [5] розробили підхід, заснований на інтервальному визначенні неточно заданих коефіцієнтів. Tien Fuling [6] застосував метод інтерактивного нечіткого багатоцільового лінійного програмування для вирішення задачі транспортного планування. Новий підхід, отримав назву нечіткої модифікованої обчислювальної процедури для пошуку оптимального розв'язку ТЗ.

Існують також дослідження, що присвячені зведенню нечітких транспортних задач до традиційних ТЗ [7-14]. R.N.Gasimov і K.Yenilmez [6] досліджували транспортні задачі з нечіткими величинами запитів та пропозицій, вирішуючи їх за допомогою параметричних моделей математичного програмування з урахуванням критерію Белмана та Заде. Цей метод полягає в отриманні розв'язків, які максимально задовольняють обмеженням і цільовій функції на множині варіантів можливих перевезень.

Нові арифметичні операції над трапецієподібними (трикутними) нечіткими числами [11] надали можливість використовувати нечіткі числа для формалізації нечітких ТЗ. Цей підхід спростив формалізацію та вирішення транспортних задач, величини ресурсів в яких визначаються нечіткими трикутними числами. Крім цього, залучення методик порівняння важливості критеріїв в задачах вибору дозволило узагальнити даний підхід на випадок різної важливості обмежень ТЗ. Таким чином, за умов нечіткого визначення ресурсів виробників та/або споживачів продукції можна розглядати ТЗ, розв'язки яких враховують різні рівні можливості відхилень ресурсів від номінальних значень і характеризуються відповідними значеннями важливості заданих обмежень. Одночасне опрацювання даних параметрів дозволило сформулювати новий підхід для вирішення загальної нечіткої транспортної задачі перевезень однотипової продукції від постачальників до споживачів з мінімальною вартістю.

Запропонований підхід може бути розповсюджений на багатокритеріальні нечіткі транспортні задачі з нечітко заданими обмеженнями на ресурси. Це дозволить здійснювати пошук ефективних (оптимальних або компромісних) за сукупністю критеріїв розв'язків нечітких транспортних задач на множинах допустимих варіантів перевезень, що визначаються із урахуванням параметрів неточності та важливості обмежень.

1. Стандартна задача лінійного програмування. Без обмеження загальності математична модель задачі лінійного програмування може бути записана у вигляді

$$max \ \sum_{j=1}^{n} c_j x_j \tag{1}$$

при обмеженнях

$$\sum_{j=1}^{n} a_{ij} x_j \le b_i \ , \quad i = \overline{1,m} \ , \quad x \ge 0; x \in R^n \ . \tag{2}$$

Ця задача при фіксованих відомих значеннях параметрів c_j , a_{ij} , b_i , $j = \overline{1,n}$, $i = \overline{1,m}$, є стандартною задачею лінійного програмування, а коли вони є випадковими величинами з відомими функціями розподілу, її можна вирішити методами стохастичного програмування. Однак на практиці ці параметри часто невідомі і для параметрів можна лише вказати інтервал можливих значень. Задачу такого типу можна назвати ЗЛП з заданою множиною значень коефіцієнтів. У рамках цієї задачі вже недоречно говорити про максимізацію цільової функції (1), оскільки значення цієї функції - не числа, а множини чисел. У цьому випадку необхідно з'ясувати, яке відношення переваги в множині альтернатив породжує ця функція, а потім визначити, вибір яких розв'язків слід вважати більш раціональним у розумінні цього відношення переваги.

Наступним етапом на шляху деталізації та уточнення розглянутої моделі (1), (2) є опис параметрів задачі у вигляді нечітких множин. В модель вводиться додаткова інформація у формі функції приналежності цих нечітких множин. Ці функції можна розглядати як спосіб наближеного відображення експертом наявного у нього неформалізованого уявлення про реальну величину даного параметра. Значення функцій належності - це вагові коефіцієнти, які експерти приписують різним можливим значенням кожного конкретного параметра.

Означення 1. [15] Нечіткою множиною $\tilde{A}$ універсальної множини X , називається сукупність пар $\tilde{A} = \{(\mu_{\tilde{A}}(x), x)\}$, де $\mu_{\tilde{A}} : X \to [0,1]$ – відображення множини X в одиничний відрізок [0,1], яке називається функцією належності нечіткої множини.

Після такого уточнення можна перейти до визначення задачі нечіткого математичного програмування [10]. Розглядається лінійна модель

$$\max Z = \sum_{j=1}^{n} \tilde{c}_j x_j \ , \tag{3}$$

в якій значення коефіцієнтів $\tilde{c}_j$ задано нечітко у формі нечітких підмножин заданих універсальних множин. Крім цього, задано обмеження

$$\sum_{j=1}^{n} \tilde{a}_{ij} x_j \le \tilde{b}_i \ , \quad i = \overline{1,m} \ , \qquad x_j \ge 0, \ j = \overline{1,n} \ , \tag{4}$$

де значення коефіцієнтів $\tilde{a}_{ij}$, $\tilde{b}_i$ також подано у формі відповідних нечітких множин. Необхідно здійснити раціональний вибір рішення $x \in R^n$, яке в деякому розумінні максимізує задану нечітко лінійну форму (3).

2. Постановка транспортної задачі. Нехай $A_1, \ldots, A_m$ – виробники однорідного продукту, причому обсяг виробництва в пункті A_i складає a_i одиниць, $i = \overline{1,m}$. Припустимо, що продукт споживають в пунктах $B_1, \ldots, B_n$, а обсяг споживання в пункті B_j складає b_j одиниць $j = \overline{1,n}$. Транспортні витрати з доставки одиниці продукції з пункту A_i в пункт B_j дорівнюють c_{ij} ($i = \overline{1,m}$, $j = \overline{1,n}$). Задача полягає у визначенні такого плану перевезень, при якому запити усіх споживачів B_j, $j = \overline{1,n}$, повністю задоволено, весь продукт з пунктів виробництва A_i, $i = \overline{1,m}$, вивезено і сумарні транспортні витрати мінімальні.

Необхідно визначити множину змінних $x_{ij} \geq 0$, $i = \overline{1,m}$, $j = \overline{1,n}$, що задовольняють умовам

$$\sum_{j=1}^{n} x_{ij} = a_i, \; i = \overline{1,m} \;, \tag{5}$$

$$\sum_{i=1}^{m} x_{ij} = b_j, \; j = \overline{1,n} \;, \tag{6}$$

і таких, що цільова функція

$$Z = \sum_{i=1}^{m}\sum_{j=1}^{n} c_{ij} x_{ij} \tag{7}$$

досягає мінімального значення.

Таким чином, транспортна задача представляє собою ЗЛП з mn числом змінних і з (m+n) числом обмежень у вигляді рівностей.

Рівняння

$$\sum_{i=1}^{m} a_i = \sum_{j=1}^{n} b_j, \tag{8}$$

яке називають умовою балансу, є необхідною та достатньою умовою розв'язку ТЗ.

Відповідна нечітка транспортна задача (НТЗ) може бути записана у вигляді:

$$\min Z = \sum_{i=1}^{m}\sum_{j=1}^{n} \tilde{c}_{ij} x_{ij} \;, \tag{9}$$

при обмеженнях

$$\sum_{j=1}^{n} x_{ij} = \tilde{a}_i, \quad i = \overline{1,m}, \tag{10}$$

$$\sum_{i=1}^{m} x_{ij} = \tilde{b}_j, \quad j = \overline{1,n}, \tag{11}$$

$$\sum_{i=1}^{m} \tilde{a}_i = \sum_{j=1}^{n} \tilde{b}_j. \tag{12}$$

2. Транспортна задача з нечіткими обмеженнями на ресурси. Розглянемо транспортну задачу нечіткого виробництва та розподілу товарних ресурсів, що задаються нечіткими трикутними числами [12] $\tilde{a}_i, i = \overline{1,m}$, $\tilde{b}_j, j = \overline{1,n}$.

При розв'язанні прикладних задач для формалізації нечіткості використовують інші означення нечіткої множини, що еквівалентні класичному означенню 1.

Означення 2. [12] Нечітким трикутним числом $\tilde{A}$ називається впорядкована трійка чисел *(a, b, c)*, що визначають функцію належності $\mu_{\tilde{A}}(x)$:

1. $\mu_{\tilde{A}}(x) = \dfrac{x-a}{b-a}, x \in [a,b]$;
2. $\mu_{\tilde{A}}(x) = \dfrac{c-x}{c-b}, x \in [b,c]$;
3. $\mu_{\tilde{A}}(x) = 0, x \notin [a,c]$.

Нечітке трикутне число *(a, b, c)* іноді називається триплетом. Крім цього, нечітке трикутне число виду *(a, b, b)*, яке називається лівим нечітким трикутним числом, визначається функцією належності

$$\mu_{\tilde{A}}(x) = 0, x < a \;; \quad \mu_{\tilde{A}}(x) = \frac{x-a}{b-a}, x \in [a,b] \;; \quad \mu_{\tilde{A}}(x) = 1, x > b \;,$$

а нечітке трикутне число виду *(b, b, c)*, яке називається правим нечітким трикутним числом, – функцією належності

$$\mu_{\tilde{A}}(x) = 1, x < b \;; \; \mu_{\tilde{A}}(x) = \frac{c-x}{c-b}, x \in [b,c] \;; \; \mu_{\tilde{A}}(x) = 0, x > c \;.$$

У цьому випадку транспортна задача з нечіткими товарними ресурсами, які задаються нечіткими трикутними числами, може розглядатися як задача лінійного програмування, що записується у вигляді

$$\min Z = \sum_{i=1}^{m}\sum_{j=1}^{n} c_{ij} x_{ij} \;, \tag{13}$$

з обмеженнями

$$\sum_{j=1}^{n} x_{ij} = \tilde{a}_i, \quad i = \overline{1,m}, \tag{14}$$

$$\sum_{i=1}^{m} x_{ij} = \tilde{b}_j, \quad j = \overline{1,n}, \tag{15}$$

$$\sum_{i=1}^{m} \tilde{a}_i = \sum_{j=1}^{n} \tilde{b}_j. \tag{16}$$

Розв'язок НТЗ (13)–(16) знайдемо за допомогою підходу, запропонованого в [12]. Нехай L_1 та U_1 – найменше та найбільше значення цільової функції Z. З урахуванням отриманих рівнів отримаємо нечітку задачу визначення величин $x_{ij} \ge 0$, $i = \overline{1,m}$, $j = \overline{1,n}$, що задовольняють обмеженням

$$Z \ge \tilde{s},\ \tilde{s} = (L_1, U_1, U_1), \tag{17}$$

$$\sum_{j=1}^{n} x_{ij} = \tilde{a}_i,\quad i = \overline{1,m},\qquad \sum_{i=1}^{m} x_{ij} = \tilde{b}_j,\quad j = \overline{1,n},\qquad \sum_{i=1}^{m} \tilde{a}_i = \sum_{j=1}^{n} \tilde{b}_j\ . \tag{18}$$

Функції належності нечітких обмежень (17), (18) визначаються у вигляді:
для першого обмеження (17)

$$\mu^1\left(\sum_{i=1}^{m}\sum_{j=1}^{n} c_{ij}x_{ij}\right) = \begin{cases} 0, & \text{for } \sum_{i=1}^{m}\sum_{j=1}^{n} c_{ij}x_{ij} < L_1, \\ \left(\sum_{i=1}^{m}\sum_{j=1}^{n} c_{ij}x_{ij} - L_1\right) \Big/ (U_1 - L_1), & \text{for } L_1 \le \sum_{i=1}^{m}\sum_{j=1}^{n} c_{ij}x_{ij} < U_1, \\ 1, & \text{for } \sum_{i=1}^{m}\sum_{j=1}^{n} c_{ij}x_{ij} \ge U_1, \end{cases}$$

для i-того обмеження, $i = \overline{1,m}$,

$$\mu_i^2\left(\sum_{j=1}^{n} x_{ij}\right) = \begin{cases} 0, & \text{for } \sum_{j=1}^{n} x_{ij} < a_i - a_i^l, \\ \left(\sum_{j=1}^{n} x_{ij} - a_i + a_i^l\right) \Big/ a_i^l, & \text{for } a_i - a_i^l \le \sum_{j=1}^{n} x_{ij} < a_i, \\ \left(a_i + a_i^l - \sum_{j=1}^{n} x_{ij}\right) \Big/ a_i^r, & \text{for } a_i \le \sum_{j=1}^{n} x_{ij} < a_i + a_i^r, \\ 1, & \text{for } \sum_{j=1}^{n} x_{ij} \ge a_i + a_i^r, \end{cases}$$

для j-того обмеження, $j = \overline{1,n}$,

$$\mu_j^3\left(\sum_{i=1}^{m} x_{ij}\right) = \begin{cases} 0, & \text{for } \sum_{i=1}^{m} x_{ij} < b_j - b_j^l, \\ \left(\sum_{i=1}^{m} x_{ij} - b_j + b_j^l\right) \Big/ b_j^l, & \text{for } b_j - b_j^l \le \sum_{i=1}^{m} x_{ij} < b_i, \\ \left(b_j + b_j^r - \sum_{i=1}^{m} x_{ij}\right) \Big/ b_j^r, & \text{for } b_i \le \sum_{i=1}^{m} x_{ij} < b_j + b_j^r, \\ 1, & \text{for } \sum_{i=1}^{m} x_{ij} \ge b_j + b_j^r. \end{cases}$$

Використовуючи *max-min*-оператор Zimmermann'a [7], задачу (17), (18) можна записати у формі

$$\max\ \lambda \tag{19}$$

з обмеженнями

$$\sum_{i=1}^{m}\sum_{j=1}^{n} c_{ij}x_{ij} - \lambda(U_1 - L_1) \ge L_1\ ,$$

$$\sum_{j=1}^{n} x_{ij} - \lambda a_i^l \ge a_i - a_i^l,\qquad \sum_{j=1}^{n} x_{ij} + \lambda a_i^r \le a_i + a_i^r,$$

$$\sum_{i=1}^{m} x_{ij} - \lambda b_i^l \ge b_j - b_j^l\ ,\qquad \sum_{i=1}^{m} x_{ij} + \lambda b_i^r \ge b_j + b_j^r\ , \tag{20}$$

$$0 \le \lambda \le 1,\ x_{ij} \ge 0\ ,\ i = \overline{1,m},\ \ j = \overline{1,n}\ ,$$

де величини допустимих відхилень $0 \le a_i^l \le a_i$, $a_i^r \ge 0$, $i = \overline{1,m}$, $0 \le b_j^l \le b_j$, $b_j^r \ge 0$, $j = \overline{1,n}$, визначають граничні зміни ресурсів моделі (17), (18).

3. Застосування методів прийняття рішень для розв'язання транспортної задачі з нечіткими обмеженнями на ресурси. При вирішенні задачі нечіткого вибору елементів з заданої множини враховуються величини функції належності окремих елементів, які можуть бути знайдені за допомогою методу парних порівнянь.

Для цього розглянемо множину елементів $X = \{x_i \ge 0,\ i = \overline{1,k}\}$. Ступінь належності елементів нечіткій множині можна отримати, порівнюючи елементи між собою. Оцінку елемента x_i порівняно з елементом x_j позначимо q_{ij}.

Для узгодженості покладемо $q_{ji} = 1/q_{ij}$. Оцінки q_{ij} складають матрицю $Q = \|q_{ij}\|$, $i, j = \overline{1,k}$.

Знайдемо власний вектор $w = (w_1, ..., w_k)$, що відповідає максимальному власному числу матриці Q. Отримані величини $w_i \ge 0$, $i = \overline{1,k}$ приймаються у якості рівнів належності елементів $X = \{x_i,\ i = \overline{1,k}\}$ відповідній нечіткій множині.

Коефіцієнти відносної важливості елементів q_{ij} визначаються на основі шкали оцінок (табл.1, [16]):

Таблиця 1

Відносна важливість елементів	*Елементи матриці A*
Рівна важливість елементів	1
Ненабагато важливіше	3
Важливіше	5
Суттєво важливіше	7
Набагато важливіше	9
Проміжні значення	2,4,6,8

Визначаючи за даною методикою важливість ресурсних обмежень транспортної задачі отримуємо вигляд задачі ЛП з урахуванням важливості обмежень за обсягами виробництва та споживання (w_1,w_2):

знайти значення $\lambda_0 \in [0,1]$, яке є розв'язком задачі лінійного програмування

$$\lambda_0 \to \max \tag{21}$$

з обмеженнями

$$\sum_{i=1}^{m}\sum_{j=1}^{n} c_{ij}x_{ij} - \lambda_0(U_1 - L_1) \ge L_1,$$

$$\sum_{j=1}^{n} x_{ij} - \lambda_1 a_i^l \ge a_i - a_i^l, \qquad \sum_{j=1}^{n} x_{ij} + \lambda_1 a_i^r \le a_i - a_i^r, \tag{22}$$

$$\sum_{i=1}^{m} x_{ij} - \lambda_2 b_j^l \ge b_j - b_j^l, \ \sum_{i=1}^{m} x_{ij} + \lambda_2 b_j^r \le b_j + b_j^r,$$

$$w_1 \le \lambda_1,\ w_2 \le \lambda_2,\ \ x_{ij} \ge 0,\ i = \overline{1,m},\ \ j = \overline{1,n},\ \lambda_p \ge \lambda_0,\ 0 \le \lambda_p \le 1,\ p = \overline{1,2}.$$

4. Приклад розв'язання транспортної задачі з нечіткими обмеженнями на ресурси. В якості прикладу розглянемо транспортну задачу [14] з трьома виробниками та трьома споживачами з цільовою функцією вартості перевезень

$$32x_{11} + 40\,x_{21} + 120\,x_{31} + 60\,x_{12} + 68\,x_{22} + 104\,x_{32} + 200\,x_{13} + 80\,x_{23} + 60\,x_{33} \to \min \tag{23}$$

та обмеженнями

$$x_{11} + x_{21} + x_{31} = \tilde{30}, \quad x_{12} + x_{22} + x_{32} = \tilde{35}, \quad x_{13} + x_{23} + x_{33} = \tilde{30}, \tag{24}$$

$$x_{11} + x_{12} + x_{13} = \tilde{20}, \quad x_{21} + x_{22} + x_{23} = \tilde{30}, \quad x_{31} + x_{32} + x_{33} = \tilde{45},\ x_{ij} \ge 0,\ i = \overline{1,3},\ \ j = \overline{1,3}.$$

У даній моделі праві частини обмежень задано нечіткими числами $\tilde{30} = (28,30,32)$, $\tilde{35} = (34,35,37)$, $\tilde{30} = (29,30,31)$, $\tilde{20} = (18,20,23)$, $\tilde{30} = (28,30,33)$, $\tilde{45} = (44,45,46)$.

Перепишемо задачу у формі ЗЛП (19), (20). Отримуємо $\max \lambda$ при обмеженнях

$$32x_{11} + 40\,x_{21} + 120\,x_{31} + 60\,x_{12} + 68\,x_{22} + 104\,x_{32} + 200\,x_{13} + 80\,x_{23} + 60\,x_{33} - \lambda(5760 - 5560) \ge 5560,$$

$$x_{11} + x_{21} + x_{31} \ge 28 + 2\lambda, \quad x_{11} + x_{12} + x_{13} \ge 18 + 2\lambda,$$

$$x_{11} + x_{21} + x_{31} \le 32 - 2\lambda, \quad x_{11} + x_{12} + x_{13} \le 23 - 3\lambda,$$

$$x_{12} + x_{22} + x_{32} \le 34 + 2\lambda, \quad x_{21} + x_{22} + x_{23} \ge 28 + 2\lambda,$$

$$x_{12} + x_{22} + x_{32} \le 38 - 3\lambda, \quad x_{21} + x_{22} + x_{23} \le 33 - 3\lambda,$$

$$x_{13} + x_{23} + x_{33} \ge 29 + \lambda, \quad x_{31} + x_{32} + x_{33} \ge 44 + \lambda,$$

$$x_{13} + x_{23} + x_{33} \le 31 - \lambda, \quad x_{31} + x_{32} + x_{33} \le 46 - \lambda,$$

$$x_{ij} \ge 0,\ i = \overline{1,3},\ \ j = \overline{1,3},\ 0 \le \lambda \le 1.$$

Оптимальний розв'язок цієї задачі:

$x_{11} = 0, x_{21} = 26, x_{31} = 0, x_{12} = 15.8, x_{22} = 0, x_{32} = 17.17, x_{13} = 2.17, x_{23} = 0, x_{33} = 25.8, \lambda = 1, Z = 5842.8.$

Використовуючи підхід з урахуванням важливості обмежень, припустимо, що матриця Q задана у вигляді

$$Q = \begin{Vmatrix} 1 & 5 \\ 1/5 & 1 \end{Vmatrix}.$$

Максимальне власне число матриці $\lambda(Q)$ =2, а власний вектор, що відповідає цьому власному числу, $w = (5/6, 1/6)$.

Відповідно до підходу, який враховує важливість ресурсних обмежень транспортної задачі, отримуємо ЗЛП наступного вигляду:

$$\max \lambda_0$$

з обмеженнями $32x_{11} + 40\,x_{21} + 120\,x_{31} + 60\,x_{12} + 68\,x_{22} + 104\,x_{32} + 200\,x_{13} + 80\,x_{23} + 60\,x_{33} - \lambda_0(5760 - 5560) \ge 5560,$

$$x_{11} + x_{21} + x_{31} \ge 28 + 2\lambda_1, \quad x_{11} + x_{21} + x_{31} \le 32 - 2\lambda_1,$$

$$x_{12} + x_{22} + x_{32} \le 34 + 2\lambda_1, \quad x_{12} + x_{22} + x_{32} \le 38 - 3\lambda_1,$$

$$x_{13} + x_{23} + x_{33} \ge 29 + \lambda_1, \quad x_{13} + x_{23} + x_{33} \le 31 - \lambda_1,$$

$$x_{11} + x_{12} + x_{13} \ge 18 + 2\lambda_2, \quad x_{11} + x_{12} + x_{13} \le 23 - 3\lambda_2,$$

$$x_{21} + x_{22} + x_{23} \ge 28 + 2\lambda_2, \quad x_{21} + x_{22} + x_{23} \le 33 - 3\lambda_2,$$

$$x_{31} + x_{32} + x_{33} \geq 44 + \lambda_2, \quad x_{31} + x_{32} + x_{33} \leq 46 - \lambda_2,$$
$$5/6 \leq \lambda_1, \; 1/6 \leq \lambda_2, \; \lambda_1 \geq \lambda_0, \; \lambda_2 \geq \lambda_0,$$
$$x_{ij} \geq 0, \; i = \overline{1,3}, \quad j = \overline{1,3}, \; 0 \leq \lambda_p \leq 1, \quad p = 0,1,2.$$

Оптимальний розв'язок у цьому випадку:

$$x_{11} = 0.23, \; x_{21} = 29.42, \; x_{31} = 0, \; x_{12} = 19.78, \; x_{22} = 0, \; x_{32} = 14.8, \; x_{13} = 0, \; x_{23} = 0, \; x_{33} = 29.83,$$
$$\lambda_0 = 0.712, \; \lambda_1 = 0.83, \; \lambda_2 = 0.712, \; Z = 5699.96$$

Як випливає з отриманих результатів, при використанні методики порівняння важливості обмежень транспортної задачі вдалося не лише знизити вартість перевезень, а й визначити допустимі границі ресурсних змін, за рахунок яких досягається це зменшення. Зрозуміло, що остаточний вибір величин обсягів виробництва та споживання визначатиметься особою, що приймає рішення.

Висновки. В роботі розглянуто метод пошуку оптимального розв'язку нечіткої транспортної задачі, ресурси в якій представлено нечіткими трикутними числами. Проілюстровано використання методу на прикладі реальної транспортної задачі. Розглянуто узагальнення методики вирішення нечіткої транспортної задачі з урахуванням важливості обмежень. Наведено приклад застосування розробленого підходу для вирішення нечітких транспортних задач загального вигляду. Запропонований підхід може бути розповсюджений на багатокритеріальні нечіткі транспортні задачі з нечітко заданими обмеженнями на ресурси. Це дозволить здійснювати пошук ефективних за сукупністю критеріїв розв'язків нечітких транспортних задач на множинах допустимих рішень, що визначаються із урахуванням параметрів неточності та важливості обмежень.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Bellman R.E., Zadeh L.A. Decision making in a fuzzy environment //Management Science, 17, 1970. – P.141–164.
2. Lai Y.J., Hawng C.L. Fuzzy Mathematical Programming. Lecture notes in Economics and Mathematical systems // Springer-Verlag, 1992.
3. Isermann H. The numeration of all efficient solutions for a linear multiobjective transportation problems// Naval Research Logistic Quarterly, 26, 1979. – P. 123–139.
4. Ringuest L.,Rinks D.B. Interactive solutions for the linear multiobjective transportation problem // European Journal of Operational Research, 32, 1987. – P. 96–106.
5. Chanas S., Kuchta D. Fuzzy programming in multi-objective linear programming-parametric approach // Fuzzy Set and System, 29, 1989. – P.303–313.
6. Tien Fuling. Applying interactive fuzzy multi-objective Linear programming to transportation planning decisions // Journal of information and optimization sciences. – V.27. – №1. – 2006. – P.107–126.
7. Zimmermann H.J. Fuzzy programming and linear programming with several objective functions // Fuzzy Sets and System, 1, 1978. – P.45–55.
8. Gasimov R.N., Yenilmez K. Soving fuzzy linear programming with linear membership functions // Turk. J.Math., 26, 2002. – P.375–396.
9. Sakawa M., Yano H. Interactive decision making for multi-objective linear fractional programming problems with fuzzy parameters // Cybernetics Systems, 16, 1985. – P.377–394.
10. Dubois D. Linear programming with fuzzy data / D. Dubois // Analysis of Fuzzy Information / J. C. Bezdek (ed.). Boca Raton : CRC Press, 1987. – Vol. 3: Applications in Engineering and Science. – P. 241–263.
11. Tanaka H., Asai K. Fuzzy linear programming problems with fuzzy numbers // Fuzzy Sets and Systems, 13, 1984. – P.1–10.
12. Bablu Jana, Tapan Kumar Roy. Multi-Objective Fuzzy Linear Programming and Its Application in Transportation Model // Tamsui Oxford Journal of Mathematical Sciences. – Vol.21. – №2. – 2005. – P.243–268.
13. Ivokhin E.V., Almodars Barraq Subhi Kaml. Single-Objective Linear Programming Problems With Fuzzy Coefficients and Resources // Computational and Applied Math. – №2. – 2013.
14. Reeb J., Leavengood S. Transportation Problem: A Special Case for Linear Programming Problems // Performance Eexcellence in the Wood Products Industry EM 8779, June 2002.
15. Zadeh L.A. Fuzzy sets // Inf. Contr., 1965. – V.8. – P.338–53.
16. Борисов А.Н. Принятия решений на основе нечетких моделей / А.Н. Борисов. - Рига: Зинатне, 1990. – 184 с.

Надійшла до редколегії 18.01.14

Ивохин Е. В., д-р физ.-мат. наук, доцент,
Киевский национальный университет имени Тараса Шевченко, Киев

О ПОДХОДЕ К РЕШЕНИЮ ТРАНСПОРТНОЙ ЗАДАЧИ С НЕЧЕТКИМИ РЕСУРСАМИ

Рассмотрен метод поиска оптимального решения нечеткой транспортной задачи, ресурсы в которой представлены нечеткими треугольными числами. Проиллюстрировано использование метода на примере реальной транспортной задачи. Рассмотрено обобщение методики решения нечеткой транспортной задачи с учетом важности ограничений. Предложено использование розработанного подхода для решения нечетких транспортных задач общего вида.

Ключевые слова: транспортная задача линейного программирования, множество решений, методы принятия решений, нечеткие числа.

Ivokhin E. V., Dr.Sci., Associate Professor,
Taras Shevchenko National University of Kyiv

ON THE APPROACH TO SOLVING TRANSPORTATION PROBLEM WITH FUZZY RESOURCES

The paper presents a method of finding the optimal solution of fuzzy transportation problem, in which resources are represented by triangular fuzzy numbers. The using of the method is illustrated on the real transportation problem. A generalization of the method of solving the fuzzy transportation problem with regard to the importance of restrictions is considered. The fuzzy approach is proposed for solving the transportation problems of general form.

Key words: transportation task of linear programming problem, solution set, decision support methods, fuzzy numbers.

УДК 519.87

E. V. Ivokhin, D.Sci., ass. prof.,
Almodars Barraq. Subhi Kaml, post-graduate,
Taras Shevchenko National University of Kyiv

USE THREE-INDEX TASK FOR SOLVING A REAL PROBLEM OIL TRANSPORTATION

The paper considers the application of the three-index transportation problem of linear programming to find the optimal solutions of oil transportation from production sites to points of consumption via intermediate points. Selecting waypoints defines by alternative method based on mutual exclusion. For a given real process mathematical problem is formulated taking into account the cost of transportation in various ways to use waypoints. The optimal solution for the three-index transportation problem was numerically obtained. The proposed approach is constructive and can be used to solve various problems of resource distribution based on three dimensions and using real process indicators for problem area.

Key words: classic transportation problem, multi-indexes transportation problem, mixed integer linear programming, constraints choice.

Introduction. The solid transportation problem (STP) may be considered as a special case of linear programming problem. In STP the bounds are given on three items namely, supply, demand and conveyance (modes). In many industrial problems a homogeneous product is delivered from an origin to a destination by means of different modes of transport called conveyances, such as trucks, cargo flights, goods trains, ships, etc. The STP was proposed by Schell [2]. Haley [3] introduced the solution procedure of STP which is an extension of the modified distribution method. Patel and Tripathy [4] developed a computationally superior method for a STP with mixed constraints. Basa M., Pal B. B. and Kundu A. [5] provided an algorithm for finding the optimum solution of a solid fixed charge linear transportation problem.

The transportation problem one of the original applications of linear programming models. A firm produce goods at m different supply centers. Label these $i=\overline{1,m}$. The supply produced at supply center i is S_i, $i=\overline{1,m}$. The demand for the good is spread out at n different demand centers. Label these $j=\overline{1,n}$ . . The demand at the $j-$th demand center is D_j, $j=\overline{1,n}$. Assume that the cost of shipping one unit from supply center i to demand center j is C_{ij}, $i=\overline{1,m}$, $j=\overline{1,n}$. The problem of the firm is to get goods from supply centers to demand centers at minimum cost. The cost of schedule by the linearity assumption is given by

$$Min\ z=\sum_{i=1}^{m}\sum_{j=1}^{n}c_{ij}x_{ij} \tag{1}$$

where x_{ij} is the amount of goods what we ship from center i to center j, $i=\overline{1,m}$, , $j=\overline{1,n}$.

The total amount shipped out of supply center i is $\sum_{j=1}^{n}x_{ij}$. This quantity cannot exceed supply available. Hence we have the constraint

$$\sum_{j=1}^{n}x_{ij}\le S_i\ ,\ i=\overline{1,m} \tag{2}$$

Similarly , the constraint that guarantee that we meet the demand at each of the demand centers look like :

$$\sum_{i=1}^{m}x_{ij}\ge D_j,\ \ j=\overline{1,n}. \tag{3}$$

Consider the feasibility of the transportation problem. The only way that the problem can be feasible is if the total supply exceed total demand $\sum_{i=1}^{m}D_j\le\sum_{j=1}^{n}S_i$. If this inequality did not hold, then there would be exceed demand. There would be no way to meet all demand with available supply. If there is enough supply, then we must be to convince ourselves that we can satisfy the constraints of the problem. That is, the problem is feasible unless there is exceed demand. It is conventional to assume that the total supply is equal to the total demand. If so that is if

$$\sum_{i=1}^{m}D_j=\sum_{j=1}^{n}S_i, \tag{4}$$

transportation problem has an optimal solution. The equality (4) is named by balanced condition. The balanced condition is the necessary and sufficient condition for the existence of a feasible solution of transportation problem.

Then all of the constraints in the problem must be hold as equations (that is when total supply equals total demand then a feasible transportation plan exactly meets demand at each demand center and uses up all of the supply at each supply center). After making the simplification that the total supply equals total demand, we arrive at the standard formulation of transportation problem as follow :

$$Min\ z=\sum_{i=1}^{m}\sum_{j=1}^{n}c_{ij}x_{ij}$$

subject to

$$\sum_{j=1}^{n}x_{ij}=S_i\ ,\ i=\overline{1,m} \tag{5}$$

$$\sum_{i=1}^{m}x_{ij}=D_j,\ \ j=\overline{1,n}. \tag{6}$$

$$x_{ij}\ge 0,\quad j=\overline{1,n},\quad i=\overline{1,m}.$$

1. Solid mathematical transportation model. In the classical transportation problem the cost of transportation is directly proportional to the number of units of the commodity transported. But in real world situations when a commodity is transported, a fixed cost is incurred in the objective function. The fixed cost may represent the cost of renting a vehicle, landing fees in an airport, set up costs for machines in a manufacturing environment etc.

Suppose $i=\overline{1,m}$ are the origins, $j=\overline{1,n}$ are the conveyance, $k=\overline{1,p}$ are the destinations,

x_{ikj} – represent the unknown quantity to transported from origin i to destination k by the conveyance j;

c_{ikj} – the costs transportation of commodity from origin i to destination k by the conveyance j;

A_i – the total quantity of commodity availability in source (origin) i, $i=\overline{1,m}$;

B_j – the total capacity of conveyance j, $j=\overline{1,n}$;

E_k – the total demand of commodity in destination k, $k=\overline{1,p}$.

For this case the solid transportation problem can be written as

$$Min\ z=\sum_{i=1}^{m}\sum_{j=1}^{n}\sum_{k=1}^{p}c_{ijk}x_{ijk} \tag{7}$$

subject to

$$\sum_{j=1}^{n}\sum_{k=1}^{p}x_{ijk}=A_i,\quad i=\overline{1,m},\quad \sum_{i=1}^{m}\sum_{k=1}^{p}x_{ijk}=B_j,\quad j=\overline{1,n},\quad \sum_{i=1}^{m}\sum_{j=1}^{n}x_{ijk}=E_k,\quad k=\overline{1,p}. \tag{8}$$

$$\sum_{i=1}^{m}A_i=\sum_{j=1}^{n}B_j=\sum_{k=1}^{p}E_k. \tag{9}$$

The equality (9) implies that the amount of commodities received by all destinations of different types of commodities is equal to the amount of commodities supplied from all origins to all destinations and to the amount of different types of commodities supplied from all origins. The equality (8) for the transportation problem above is the balanced condition. Otherwise, this transportation problem is called unbalanced.

Let F_{ijk} - the addition cost of commodity from origin i to destination k by the conveyance j. Then we shall consider the solid transportation fixed problem as

$$Min\ z=\sum_{i=1}^{m}\sum_{j=1}^{n}\sum_{k=1}^{p}c_{ijk}x_{ijk}+\sum_{i=1}^{m}\sum_{j=1}^{n}\sum_{k=1}^{p}F_{ijk}x_{ijk} \tag{10}$$

subject to (8) and (9).

2. Formulation possibilities through mixed integer programming. Integer programming formulation of situations in which variables are inherently discrete in nature do not pose any problem. However, there are numerous situations wherein the variables are not discrete.

Nevertheless, these problems fit into linear programming format except for some minor disparity. Fortunately, certain formulation possibilities are available for circumventing some of these disparities. These involve the introduction of one or more artificial variables that are restricted to be integers. This reduces the problem to be a mixed integer programming problem in the desired format. As progress continues in the development of efficient algorithms, this approach is attaining increasing particular importance. Some of the problem handled by this approach are "*Either, Or*" Constraints (when *K* out of *N* adjusted constraints, $K\le N$, must be hold) [6]**.** Let the some optimization problem with *N* constraints be defined by

$$Min\ z=\sum_{j=1}^{n}c_{ij}x_{ij}, \tag{11}$$

subject to

$$\sum_{j=1}^{n}a_{ij}x_j\le(=)b_i,\quad i=\overline{1,N}. \tag{12}$$

Consider a case wherein it is desired that only *K* out of *N* adjusted constraints, ($K\le N$), must be hold. Using the logic of the *K* out of *N* constraints the equivalent formulation is

$$\sum_{j=1}^{n}a_{ij}x_j\le b_i+M(1-y_i),\quad i=\overline{1,N}. \tag{13}$$

$$\sum_{i=1}^{N}y_i=N-K, \tag{14}$$

where $M\ 0$ and $y_i\in\{0,1\}$, $i=\overline{1,N}$ since the constraints on y_i (14) guarantee that *K* of the original constraints will remain unchanged and the rest will in effect be eliminated.

3. Case study in the field of oil. The following data adopted from Bhumik [7]. The Texago Corporation is a large, fully integrated petroleum company based in the U.S.A. The company produces most of its oil in its own oil fields and then imports the rest of what it need from Middle East. An extensive distribution network is used to transport the oil to the company's refineries and then to transport the petroleum products from the refineries to Texago's distribution centers. The locations of these various facilities are given in Table 1.Texago is continuing to increase market share for several of its major products. Therefore management has made the decision to expand output by building an additional refinery and increasing import of crude oil from Middle East. The crucial remaining decision is where to locate the new refinery.

Table **1**

Location of Texago's current facilities

Type of facility	Locations
Oil fields	1.Taxas 2.California 3. Alaska
Refineries	1.Near new Orleans Louisiana. 2.Near Charleston south Carolina. 3.Near seattle ,Washinghington.
Distribution centers	1.Pittsbourgh , Pennsylvania 2.Atalanta , Georgia 3.Kansas city , Mussouri 4.San Francisco,California

The addition of the new refinery will have a great impact on the operation of the entire distribution system, including decisions on how much crude oil to transport from each of its sources to each refinery (including the new one) and how much finished product to ship from each refinery to each distribution center. Therefore, the three key factors for management's decision on the location of the new refinery are:

1. the cost of transporting the oil from its sources to all the refineries including the new one;
2. the cost of transporting finished product from all the refineries including the new one to the distributions centers;
3. the operating costs for the new refinery including labor costs, taxes, the cost of needed supplies (other than crude oil), energy costs, the cost of insurance, the effect of financial incentives provided by the state or city, and so forth. Management has set up a task force to study the issue of where to locate the new refinery. After considerable investigation, the task force has determine that there are three attractive potential sites and the new refinery will built in the one of the three sites that labeled (A,B,C). These sites and the main advantages of each are spelled out in Table 2. Other relevant factors such as standard of living consideration for management and employees are considered reasonably comparable at these sites.

Table **2**

Potential sites for Texago's new refineries and their main advantages

Potential sites	Main advantages
Near los angeles , California	1. Near California oil fields 2. Ready access from Alaska oil fields 3. Fairly near San Francisco distribution center
Near Galveston	1. Near Texas oil fields 2. Ready access from Middle East imports 3. Near corporate headquarters
Near St. Louis, Missour	1. Low operating costs 2. Centrally located for distribution centers 3. Ready access to crude oil via Mississippi River

4. Gathering the necessary data. The task force needs to gather a large amount of data some of which requires considerable digging in order to perform the analysis requested by management.

Management wants all the refineries including the new one to operate at full capacity. Therefore the task force begins by determining how much crude oil each refinery would need to receive annually under these conditions. Using units 1 million barrels these needed amount are shown on the left side of Table 3. The right side of the table shows the current annual output of crude oil from the various oil fields. These quantities are expected to remain stable for some years to come. Since the refineries need a total of 360 million barrels of crude oil and the oil fields will produce a total of 240 million barrels the difference of 120 million barrels will need to be import from the Middle East.

Table **3**

Production data for Texago corp.

Refinery	Crude Oil Needed Annually (million Refinery barrels)	Oil fields	Crude Oil Produced Annually Oil Fields (million barrels)
New Orleans	100	Texas	80
Charleston	60	California	60
Seattle	80	Alaska	100
New one	120		
Total	360	Total	
		Needed imports	360–240 = 120

Since the amounts of crude oil produced or purchased will be the same regardless of which location is chosen for the new refinery the task force concludes that the associated production or purchase costs (exclusive of shipping costs) are not relevant to the site selection decision. On the other hand the costs for transporting the crude oil from its source to a refinery are very relevant. These costs are shown in table 4 for both the three current refineries and the three potential sites for the new refinery. Also very relevant are the costs of shipping the finishing product a refinery to a distribution center.

***Table* 4**

Cost data for shipping crude oil to a Texago refinery

	Cost per Unit Shipped (millions of dollars per million barrels) Refinery or Potential Refinery					
	New Orleans	**Charleston**	**Seattle**	**Los Angeles**	**Galveston**	**St. Louis**
Texas	2	4	5	3	1	1
California	5	5	3	1	3	4
Alaska	5	7	3	4	5	7
Middle East	2	3	5	4	3	4

Letting one unit of finished product corresponding to the production of a refinery from 1 million barrels of crude oil these costs are given in Table 5. The bottom row of the table shows the number of unite of finished product needed by each distribution center.

***Table* 5**

Cost data for shipping finished product to a distribution center

Cost per Unit Shipped (millions of dollars) Distribution Center					
		Pittsburgh	**Atlanta**	**Kansas City**	**San Francisco**
Refinery	New Orleans	6.5	5.5	6	8
	Charleston	7	5	4	7
	Seattle	7	8	4	3
Potential Refinery	Los Angeles	8	6	3	2
	Galveston	5	4	3	6
	St. Louis	4	3	1	5
Number of units needed		100	80	80	100

The final key body of data involves the operating costs for refinery at each potential site. Estimating these costs requires site visits by several member of the task force to collect details information about local labor costs, tasks, and so forth. Comparisons then are made with the operating costs of the current refineries to help refine these data. In addition the task force gathers information on one time site costs for land construction and so forth and amortizes these costs on an equivalent uniform annual cost basis. This process leads to the estimates in Table 6.

***Table* 6**

Estimated operating costs for a Texago refinery at each potential site

Site	**Annual Operating Cost (millions of dollars)**
Los Angeles	620
Galveston	570
St. Louis	530

5. Formulate the model. Let x_{ijk} are the quantities transported of crude oil from the field *i* to the refinery *j*, and the quantities transferred from refinery *j* to distribution centers *k* (annually), where $i=1,2,3,4$, $j=1,2,3,(A\ or\ B\ or\ C)$, $k=1,2,3,4$ for this model.

The objective function is

$$Min\ z=\sum_{i=1}^{4}\sum_{j=1}^{3}\sum_{k=1}^{4}c_{ijk}x_{ijk}+\sum_{i=1}^{4}\sum_{j\in\{A,B,C\}}\sum_{k=1}^{4}c_{ijk}\delta_{ijk}x_{ijk}+F_j\delta_j \tag{15}$$

$$\delta_{ijk}=\begin{cases}1,\ if\ \exists\ x_{ijk}>0\ ,\ j\in\{A,B,C\}\ ,\ i=\overline{1,4}\ ,k=\overline{1,4};\\ 0,\ otherwise\ \text{ó}\ (x_{iAk}>0,\ x_{iBk}>0\ ,x_{iCk}>0),\ i=\overline{1,4}\ ,k=\overline{1,4};\end{cases}$$

$$\delta_j=\begin{cases}1,\ if\ \exists\ \delta_{ijk}=1,\ i=\overline{1,4}\ ,k=\overline{1,4},\ j=1,2,3,\ (A\,or\,B\,or\,C)\\ 0,\ otherwise\end{cases}$$

F_j – additional costs for the case $\delta_j=1,\ j\in\{A,B,C\}$,

subject to

- constraints fields oil production and purchase

$$\sum_{j=1}^{3}\sum_{k=1}^{4}x_{1jk}+\sum_{k=1}^{4}x_{1Ak}+My_1\ge 80,\qquad \sum_{j=1}^{3}\sum_{k=1}^{4}x_{2jk}+\sum_{k=1}^{4}x_{2Ak}+My_1\ge 60, \tag{16}$$

$$\sum_{j=1}^{3}\sum_{k=1}^{4}x_{1jk}+\sum_{k=1}^{4}x_{1Bk}+My_2\ge 80,\qquad \sum_{j=1}^{3}\sum_{k=1}^{4}x_{2jk}+\sum_{k=1}^{4}x_{2Bk}+My_2\ge 60,$$

$$\sum_{j=1}^{3}\sum_{k=1}^{4}x_{1jk}+\sum_{k=1}^{4}x_{1Ck}+My_3\ge 80,\qquad \sum_{j=1}^{3}\sum_{k=1}^{4}x_{2jk}+\sum_{k=1}^{4}x_{2Ck}+My_3\ge 60,$$

$$\sum_{j=1}^{3}\sum_{k=1}^{4}x_{3jk}+\sum_{k=1}^{4}x_{3Ak}+My_1\ge 100,\qquad \sum_{j=1}^{3}\sum_{k=1}^{4}x_{4jk}+\sum_{ik=1}^{4}x_{4Ak}+My_1\ge 120,$$

$$\sum_{j=1}^{3}\sum_{k=1}^{4} x_{3jk} + \sum_{k=1}^{4} x_{3Bk} + My_2 \geq 100, \qquad \sum_{j=1}^{3}\sum_{k=1}^{4} x_{4jk} + \sum_{k=1}^{4} x_{4Bk} + My_2 \geq 120,$$

$$\sum_{j=1}^{3}\sum_{k=1}^{4} x_{3jk} + \sum_{k=1}^{4} x_{3Ck} + My_3 \geq 100, \qquad \sum_{j=1}^{3}\sum_{k=1}^{4} x_{4jk} + \sum_{k=1}^{4} x_{4Ck} + My_3 \geq 120,$$

- constraints refinery capacity

$$\sum_{i=1}^{4}\sum_{k=1}^{4} x_{i1k} = 100, \qquad \sum_{i=1}^{4}\sum_{k=1}^{4} x_{i2k} = 60, \qquad \sum_{i=1}^{4}\sum_{k=1}^{4} x_{i3k} = 80, \tag{17}$$

$$\sum_{i=1}^{4}\sum_{k=1}^{4} x_{iAk} + My_1 \geq 120, \qquad \sum_{i=1}^{4}\sum_{k=1}^{4} x_{iBk} + My_2 \geq 120, \qquad \sum_{i=1}^{4}\sum_{k=1}^{4} x_{iCk} + My_3 \geq 120,$$

- constraints distribution centers

$$\sum_{i=1}^{4}\sum_{j=1}^{3} x_{ij1} + \sum_{i=1}^{4} x_{iA1} - My_1 \leq 100, \qquad \sum_{i=1}^{4}\sum_{j=1}^{3} x_{ij2} + \sum_{i=1}^{4} x_{iA2} - My_1 \leq 80, \tag{18}$$

$$\sum_{i=1}^{4}\sum_{j=1}^{3} x_{ij1} + \sum_{i=1}^{4} x_{iB1} - My_2 \leq 100, \qquad \sum_{i=1}^{4}\sum_{j=1}^{3} x_{ij2} + \sum_{i=1}^{4} x_{iB2} - My_2 \leq 80,$$

$$\sum_{i=1}^{4}\sum_{j=1}^{3} x_{ij1} + \sum_{i=1}^{4} x_{iC1} - My_3 \leq 100, \qquad \sum_{i=1}^{4}\sum_{j=1}^{3} x_{ij2} + \sum_{i=1}^{4} x_{iC2} - My_3 \leq 80,$$

$$\sum_{i=1}^{4}\sum_{j=1}^{3} x_{ij3} + \sum_{i=1}^{4} x_{iA3} - My_1 \leq 80, \qquad \sum_{i=1}^{4}\sum_{j=1}^{3} x_{ij4} + \sum_{i=1}^{4} x_{iA4} - My_1 \leq 100,$$

$$\sum_{i=1}^{4}\sum_{j=1}^{3} x_{ij3} + \sum_{i=1}^{4} x_{iB3} - My_2 \leq 100, \qquad \sum_{i=1}^{4}\sum_{j=1}^{3} x_{ij4} + \sum_{i=1}^{4} x_{iB4} - My_2 \leq 80,$$

$$\sum_{i=1}^{4}\sum_{j=1}^{3} x_{ij3} + \sum_{i=1}^{4} x_{iC3} - My_3 \leq 100, \qquad \sum_{i=1}^{4}\sum_{j=1}^{3} x_{ij4} + \sum_{i=1}^{4} x_{iC4} - My_3 \leq 80,$$

$$y_1 + y_2 + y_3 = 2, \tag{19}$$

$$x_{ijk} \geq 0,\ i = 1,2,3,4,\ \ j = 1,2,3,(A \text{ or } B \text{ or } C),\ \ k = 1,2,3,4,\ y_p \in \{0,1\},\ p = 1,2,3,\ M \gg 0.$$

By using software WINQSB [1] programming we get the optimal solution (annually million barrels): $x_{111} = 34,5455,$ $x_{1C2} = 25,4545,\ x_{234} = 60,\ x_{323} = 5,4545,\ x_{1C3} = 74,5455,\ x_{334} = 20,\ x_{3C4} = 20,\ x_{411} = 65,4545,\ x_{422} = 54,5455,$ and the total cost $z = 2707$ millions of dollars annually.

6. Conclusion. The necessity of solid transportation problems (STP) arises when heterogeneous conveyances are available for shipment of products in public distribution system. This method can help decision makers in the logistics related issues of real life problems by aiding them in the decision making process and providing an optimal solution in a simple and effective manner.

References

1. James, K.H. Computing True Shadow Prices in Linear programming. – INFORMATICA, – V.11, No.4, – 2000. – pp.421–434.
2. Shell E. Distribution of a product by several properties. Directorate of Management Analysis, Proc. 2nd Symp. on Linear Programming, – V. 2, – 1955. – pp. 615–642.
3. Haley K.B. The solid transportation problem. – Oper. Res., No.11, – 1962. – pp.446–448.
4. Patel G. and Tripathy J. The solid transportation problem and its variants. Intern. J. Management and Systems. – No.5. – 1989. – pp.17–36.
5. Basu M., Pal B.B. and Kundu A. An algorithm for finding the optimum solution of solid fixed charge transportation problem. – No. 31. – 1994. – pp.283–291.
6. Gupta P.K., Hira D.S. Operations research. Schand and company LTD, – 2000. – pp. 585–586.
7. Bhumik,http://www.casestudy.com.in/a-case-study-in-many-transportation-problems Highered. McGraw- hill.com //hil61217_ch08_suppleme.qsd 5/12/2004

Надійшла до редколегії 15.02.2014

Івохін Е. В., д-р фіз.-мат. наук, доц.,
Алмодарс Барак Субхі Камл, аспірант,
Київський національний університет імені Тараса Шевченка, Київ

ВИКОРИСТАННЯ ТРЬОХІНДЕКСНОЇ ЗАДАЧІ ДЛЯ ВИРІШЕННЯ ОДНІЄЇ ПРОБЛЕМИ ТРАНСПОРТУВАННЯ НАФТИ

В роботі розглянуто застосування трьохіндексної транспортної задачі лінійного програмування для знаходження оптимального розв'язку транспортування нафти з місць добутку до пунктів споживання через проміжні пункти. Вибір проміжних пунктів визначається альтернативним способом на основі взаємовиключення. Для заданого реального процесу сформульовано задачу, що враховує у вартості транспортування різні способи використання проміжних пунктів. Чисельно отримано оптимальний розв'язок для трьохіндексної транспортної задачі. Запропонований підхід є достатньо конструктивним і може бути використаний при розв'язанні різних проблем розподілу ресурсів на основі трьох вимірів та з застосуванням реальних показників процесів проблемної області.

Ключові слова: класична транспортна задача, багатоіндексна транспортна задача, змішані задачі цілочисельного лінійного програмування, вибір обмежень.

Ивохин Е.В., д-р физ.-мат. наук, доц.,
Алмодарс Барак Субхи Камл, аспирант,
Киевский национальний университет имени Тараса Шевченко, Киев

ИСПОЛЬЗОВАНИЕ ТРЕХИНДЕКСНОЙ ЗАДАЧИ ДЛЯ РЕШЕНИЯ ОДНОЙ ПРОБЛЕМИ ТРАНСПОРТИРОВКИ НЕФТИ

В работе рассмотрено применение трехиндексной транспортной задачи линейного программирования для нахождения оптимального решения транспортировки нефти из мест добычи в пункты потребления через промежуточные пункты. Выбор промежуточных пунктов определяется альтернативным способом на основе взаимоисключения. Для заданного реального процесса сформулирована задача, учитывающая в стоимости транспортировки различные способы использования промежуточных пунктов. Численно получено оптимальное решение для трехиндексной транспортной задачи. Предложенный подход является достаточно конструктивным и может быть использован при решении различных проблем распределения ресурсов на основе трех измерений и с использованием реальных показателей процессов проблемной области.

Ключевые слова: классическая транспортная задача, многоиндексная транспортная задача, смешанные задачи целочисленного линейного программирования, выбор ограничений.

УДК 004.451.642

С. И. Кифоренко, д-р биол. наук, В. В. Кравченко, асп.,
Международный научно-учебный центр информационных технологий и систем НАН Украины и МОН Украины, Киев

ИНФОРМАЦИОННО-ТЕХНОЛОГИЧЕСКИЕ АСПЕКТЫ КОНТРОЛЯ И КОРРЕКЦИИ ФИЗИЧЕСКОГО ЗДОРОВЬЯ

Описаны принципы и подходы к оценке физического здоровья. Проведена структуризация информационного поля исследования, представлена информационно-структурная модель оценивания физического здоровья. Обоснована целесообразность его количественного донозологического оценивания. Приведена информационно-структурная схема алгоритма оценивания физического статуса и поддержки принятия решений при выборе оздоровительных мероприятий для контроля, коррекции и поддержания здоровья.

Ключевые слова: методы оценки физического здоровья, иерархическая свертка, метод инфотомирования, метод нормированной унификации разнокачественной информации (МНУРИ), поддержка принятия решений.

Введение. Низкий уровень состояния здоровья населения, усугубившийся в связи с социально-экономическим, экологическим кризисом, создает много проблем для оказания своевременной медицинской помощи. Анализ сложившейся ситуации показал актуальность смены парадигм: с увеличения средств на лечение болезней – на затраты, связанные с их предупреждением и профилактикой. Экономически выгоднее тратить средства на оздоровление, на увеличение резервов здоровья, чем на лечение болезней и их осложнений. Особенно дорого стоит лечение хронических заболеваний. Гораздо дешевле быть здоровым и тратить средства на поддержание здоровья на протяжении всей жизни, чем на лечение болезней. Акцентирование внимания на самоконтроле состояния своего здоровья, ориентация на ведение здорового образа жизни – необходимая составляющая культуры современного человека, адекватно ориентирующегося в современных жизненных условиях.

Своим здоровьем нужно управлять. Здоровье как объект управления рассматривается в работах [1, 2, 3 и др.]. Но для того, чтобы грамотно управлять, необходимо знать уровень здоровья и уметь оценивать возможности своего организма, чтобы постоянно находиться в адекватно-активном взаимодействии с внешней средой. Для этого нужно самому себе уметь ответить на вопросы: "Насколько я здоров?", "Каковы мои резервы здоровья?", "Каковы мои возможности для его поддержания?". Другими словами, не только пропустить через сознание эти качественно-принципиальные мысли, но и уметь измерить здоровье, оценить не только его наличие, но и возможности его регулирования с использованием методик количественного оценивания.

Введение количественных оценок позволяет увеличить разрешающую способность качественного самооценивания, которое в основном содержится в словах: "Хорошо", "Не очень хорошо", "Удовлетворительно" и т.д.

Наряду с традиционными методами анализа и оценивания отдельных физиологических систем внутренней сферы организма в контексте идеологии – "Здоровье на протяжении всей жизни" – на современном этапе рассматривается концептуальный взгляд на структуру здоровья, позволяющий ее представить в виде совокупности отдельных составляющих: физической, психической, социальной. Каждая из составляющих имеет определенную информационную ценность и как самостоятельный элемент, и как взаимосвязанный с остальными в целостном неразделимом комплексе. Тем не менее, процедура декомпозиции в научных исследованиях почти всегда является этапом предшествующим и дополняющим впоследствии системное представление об изучаемом объекте – здоровье человека в целом.

Диагностика определения уровня физического здоровья, как составной части здоровья человека – чрезвычайно трудоемкий процесс. Анализ используемых при этом методов и приемов способствуют улучшению понимания процессов оценивания в исследуемой предметной области – оценивания физической составляющей здоровья. Стремительные темпы развития информационных технологий расширяют возможности повышения эффективности оценивания здоровья, в том числе и физического, за счет создания компьютерных диагностических систем, поддерживающих, организующих и уточняющих принятие соответствующих решений для внедрения в жизнь оздоровительных мероприятий. В этом контексте можно сформулировать постановку задачи исследования.

Постановка задачи – провести анализ существующих методов, способов и алгоритмов оценки физического здоровья человека, как необходимых этапов разработки информационной технологии поддержки принятия решений при коррекции состояния физического статуса организма человека с целью формирования информационного поля необходимых знаний при обеспечении возможности адекватного индивидуального выбора оздоровительных мероприятий для поддержания физического здоровья, как составляющей здоровья в целом.

Методы: метод инфотомирования, информационно-структурное моделирование, метод МНУРИ, многомерное шкалирование, синтез диагностических моделей.

Здоровье и его оценивание. Взгляд на здоровье сквозь призму иерархичности позволил коллективу авторов [2,4,5] разработать информационно-структурное представление о здоровье как триединстве физического, психического и социального статусов, которое послужило основой для разработки методологии многомерного количественного оценивания здоровья и его составляющих.

Определение понятия здоровья. В настоящее время существует много определений понятия здоровья. Так, по трактовке ВОЗ: ***Здоровье*** – это состояние физического, душевного и социального благополучия, а не только отсутствие болезней [6]. В работе [7] здоровье определяется как нормальное психосоматическое состояние человека, способного реализовать потенциал своих телесных и духовных сил и оптимально удовлетворить систему своих материальных, духовных и социальных потребностей. Согласно [5], здоровье это – нормальное внутрисистемное функционирование статусов (физического, психического, социального) как потенциального базиса индивидуума и адекватное внутрисистемное и системно-средовое их проявление в социальном поведении личности. Большинство *авторов едины в* основном понимании структуры здоровья, как сложного системного образования, включающего также психосоматические компоненты, безусловно зависящие от социальных условий, в которых организм пребывает.

Физическое здоровье (ФЗ) – важнейший компонент в сложной структуре состояния здоровья человека. В рамках принятой концепции триединства *физический статус* есть эволюционно базисный статус общего здоровья человека и ему принадлежит ответственная роль в материально-энергетическом обеспечении функционирования физиологических систем организма. Физическое здоровье (ФЗ) [5] определяется как состояние организма, при котором интегральные показатели его физиологических систем лежат в пределах физиологической нормы и адекватно изменяются при взаимодействии человека со средой.

Согласно принятым в учебной литературе [7,8] определениям ФЗ – это состояние организма человека, характеризующееся достаточным *уровнем физического развития, физической и функциональной подготовленностью* организма к выполнению физических нагрузок и возможностями *адаптироваться* к различным факторам среды.

Оценивание здоровья. Отметим, что существует достаточно широкий набор *способов, методов, методик оценивания здоровья* в целом и отдельных его составляющих, базирующихся на введении *количественных мер,* относящихся к разным граням функционирования организма. При этом для *оценки физического развития* используются антропометрические показатели, включающие длину тела и отдельных его частей, на основе которых рассчитываются различные индексы, наиболее простой из них – индекс Брока (росто-весовое отношение). *Функциональное состояние* организма, его физическая и функциональная подготовленность к выполнению загрузок, чаще всего оценивают по состоянию сердечно-сосудистой и дыхательной систем, основными показателями состояния которых являются частота сердечных сокращений и время ее восстановления, артериальное давление (систолическое, диастолическое), жизненная емкость легких, а также коэффициент ее отношения к массе тела и др. [9–11]. Согласно Н. М. Амосову, который ввел понятие "количество здоровья", количество здоровья определяется суммой *резервных* мощностей основных *функциональных систем* организма и рассчитывается с помощью резервных коэффициентов [12] – отношений величин максимального потребления кислорода (мл на 1 кг массы тела в 1 мин), сердечного выброса (литров в 1 мин.) при различных нагрузках к тем же показателям в состоянии покоя [13]. В работе [10] Г. Л. Апанасенко также считает, что наиболее точно количество физического здоровья можно определить, включая в оценочный алгоритм величину максимального потребления кислорода организмом, являющуюся важнейшим физиологическим показателем жизнедеятельности организма.

Индикатором резервных возможностей организма является способность увеличения при необходимости поглощения кислорода. Резервные мощности – это есть функциональные ресурсы органов и систем, которыми определяются *адаптационные* возможности организма – способность адаптироваться к новым условиям, своевременно мобилизовать эти ресурсы, чтобы предотвратить истощение регуляторных физиологических механизмов, обеспечивающих гомеостатические свойства физиологических систем и гомеостатичность организма в целом [14,15].

Адаптивность – это фундаментальное свойство живой системы. Адаптационные возможности организма – это показатель уровня здоровья, базирующегося на понятии гомеостаза, который можно рассматривать как целевую функцию многоуровневого иерархического управления в организме [16].

Существенно расширило возможности экспрессоценивания здоровья использование диагностических методик, основанных на использовании *компьютерных технологий*, информация о которых содержится в научных публикациях и на многочисленных сайтах в интернете.

Известна *компьютерная* программа донозологической экспресс-оценки уровня физического здоровья, в основе которой методика Г. Л. Апанасенко, включающая оценку физического развития по антропометрическим данным, оценку функциональных возможностей органов дыхания и кровообращения, оценку двигательных качеств, а также адаптационных резервов сердечно-сосудистой и дыхательной систем [17].

Диагностический комплекс "Здоровье-Экспресс" [18] предназначен для скрининг-оценки уровня психофизиологического и соматического здоровья, резервов организма, параметров физического развития и выдаче индивидуальных рекомендаций по коррекции состояния и выбору образа жизни.

Известен комплекс компьютерных систем для учебных работ в области диагностики и профилактики старения, а также для задач общего оздоровления и биоактивации [19].

Программа "Мониторинг здоровья" [20] представляет собой многопользовательскую систему, работающую по технологии "клиент-сервер". Это позволяет выполнять работу с программой (вводить данные мониторинга, осуществлять их систематизацию, анализ и другие функции) одновременно на большом числе персональных компьютеров. Хранение и обработку данных осуществляет SQL сервер Firebird. Программа создана в среде программирования Delphi. Блок вычисления индексов и интегральных показателей позволяет рассчитать уровень физического здоровья (по Г. Л. Апанасенко), адаптационный потенциал (по Р. М. Баевскому), индекс физического состояния, ударный объем крови, максимальное потребление кислорода и ряд других показателей, характеризующих индивидуальное и популяционное здоровье.

Диагностическая программа "Здоров'я" [21], базируется на создании формализованной экспресс-оценки (в баллах) уровня здоровья индивида по физиологическим показателям таких как маса тела, рост, ЧСС, САД, ДАД, жизненная емкость легких (ЖЕЛ) и др.).

Несмотря на востребованность и широкое использование различных способов и программ оценивания физического здоровья при массовом скрининге различных контингентов и групп населения, вопрос об уровне адекватности конкретных подходов рассматриваемой проблеме, о необходимости и методологии модификации их структуры и совершенствования способов реализации разработанных диагностических систем остается открытым.

Для решения поставленной *задачи:* разработка информационной технологии поддержки принятия решений при оценке и коррекции состояния физического статуса, – используется технология *информационно-структурного моделирования,* предложенная в работах [4,5].

Информационно-структурная модель физического статуса здоровья. Авторы работ [4,5], опираясь на основное положение о структуре здоровья как о триединстве основополагающих структурных составляющих – физического, психического и социального статусов, базируясь на методологии *инфотомирования,* предложили комплексную систему количественного оценивания здоровья на всех его уровнях, начиная от конкретных показателей, до основных физиологических систем, идентификаторами состояния которых является совокупность этих показателей. На следующем этапе оцениваются вышележащие уровни *системно-иерархических структур.* Разработанный при этом алгоритм позволяет оценивать количественно физическое, психическое, социальное здоровье и здоровье в целом. Каждая из описанных составляющих здоровья представляет самостоятельный интерес для исследования, безусловно являясь неотъемлемой частью, вносящей существенный вклад в формирование здоровья целостного организма.

Инфотомирование – реализация принципа декомпозиции знаний об объекте и представление их в виде структуры иерархически и послойно организованных информационных модулей. Опираясь на эту методологию, разработана информационно-структурная модель здоровья, обеспечивающая возможность многомерного количественного оценивания здоровья как триединства 3-х статусов: физического, психического и социального с учетом иерархичности всех нижеследующих вложений. Анализ литературных данных показал, что экспрессоценивание физического здоровья при массовых обследованиях различных категорий населения – студентов, школьников, военнослужащих, водителей транспорта, при профотборе спортсменов – широко используются методы оценивания *физического развития* организма, его *физической и функциональной подготовленности*, запаса *адаптационных резервов* и т.д. Эти методы легко доступны в связи с их неинвазивностью и поэтому востребованы при массовом контроле состояния индивидуального здоровья. Перечисленные особенности оценивания не учтены в схемах, описанных в работах [4,5]. Поэтому целесообразно *расширить* ранее предложенное информационно-структурное представление физического здоровья путем включения в его структуру *дополнительного модуля*, отвечающего за готовность организма к физическим нагрузкам, информирующего об уровне физического развития, подготовленности, а также о его резервных и адаптационных возможностях. Целью этого включения является совершенствование методологии оценивания физического статуса здоровья.

Информационно-структурная схема такого представления физического статуса здоровья, основанная на методологии инфотомирования, изображена на рис.1. Древовидная информационная структура представлена следующими уровнями (слоями):

Рис.1. Информационно-структурная модель физического статуса здоровья

Первый уровень иерархии – физический статус здоровья (ФЗ);

Второй уровень иерархии – компоненты физического статуса здоровья – представлен тремя модулями. К имеющимся ранее в разработанной структуре [2,4,5] модулям – внутренних физиологических систем (ВФС), координирующих систем организма (КСО) – (нейро-эндокринно-иммунный комплекс) – добавлен дополнительный модуль, – исполнительные физические возможности (ИФВ).

Третий уровень – составляющие компонент статусов. Для компоненты – внутренняя физиологическая сфера – это отдельные физиологические системы организма – сердечно-сосудистая система (ССС), система дыхания – (СД), система крови (СК), система углеводного обмена (СУО) и др. Для компоненты – координирующие системы организма (КСО) – составляющими являются нервная, эндокринная и иммунная системы.

Составляющими исполнительных физических возможностей (ИФВ) в этой новой ветви иерархической структуры – есть физическое развитие (ФР), физическая и функциональная подготовленность (ФФП), адаптационные резервы (АР).

Четвертый уровень структуры физического здоровья формируют отдельные показатели составляющих компонент физического статуса. Отметим, что состояние внутренних физиологических систем организма, как правило, основывается на измерениях конкретных показателей. Для сердечно-сосудистой системы – это частота сердечных сокращений (ЧСС), систолическое артериальное давление (САД), диастолическое артериальное давление (ДАД), минутный и ударный объем сердца (МОС) и др.; для системы углеводного обмена (СУО) – это концентрация глюкозы в крови, в моче, данные глюкозотолерантного теста, концентрация гликированного гемоглобина и др.; для системы крови (СК) – СОЭ (скорость оседания эритроцитов), L – количество лейкоцитов, эритроцитов, pH и ряд других информативных данных.

Выделить опорные показатели для каждой из *координирующих* систем (нервной, эндокринной и иммунной) с учетом того, что они взаимосвязаны, сложно. Для оценки состояния этих систем авторы работы [5] разработали *систематизированный вопросник*, дающий возможность оценить качество функционирования этих систем в комплексе, как возможность противостоять неблагоприятным факторам внутренней и внешней сред. Оценка состояния в этом случае проводится в *баллах*.

В ветви *исполнительных физических возможностей, четвертый уровень* иерархии, представлен внутренними вложениями, представляющими *совокупность показателей*, характеризующих готовность организма к выполнению физических нагрузок. Это – показатели, характеризующие развитие мышечной системы; показатели, характеризующие готовность организма к нагрузкам – состояние сердечно-сосудистой системы, функциональные возможности органов дыхания, кровообращения, устойчивость к гипоксии, сила, выносливость, быстрота; показатели, характеризующие адаптационные резервы организма – состояние кардиореспираторной системы, возраст и д.р.

Заметим, что состояние внутренней сферы организма в большой мере определяется состоянием исполнительных физиологических механизмов, способностью их к реализации двигательной активности, а также внешних управляющих воздействий, обеспечивающих и поддерживающих гомеостатичность параметров физиологических систем, которые обеспечиваются также согласованностью взаимодействия координирующих (нервной, эндокринной, иммунной) систем. Они могут выступать либо в качестве средства для достижения цели, либо быть самой целью, если требуется усовершенствовать двигательные акты и навыки. Заметим, что количественная информация о состоянии исполнительных механизмов в структуре жизнедеятельности является индикатором состояния физического здоровья и здоровья в целом.

Взгляд на структуру здоровья с позиций *теории управления* дает возможность информационные блоки (рис.1) представить в виде схемы (рис.2).

Рис. 2. Структура здоровья с позиций *теории управления*

Объектом управления здесь служит внутренняя сфера организма (блок 1). В блоке 2 отражена информация об исполнительных возможностях организма. В блоке 3 представлены технологические этапы выполнения идентификации состояния как внутренней сферы, так и исполнительных возможностей. Результаты оценивания формируются в диагностических выводах о состоянии указанных блоков 1 и 2. Сопоставление полученных выводов с использованием баз данных о видах деятельности и оздоровительных методиках позволяет оценивать степень необходимости выполнения коррекции состояния организма и проводить выбор способов корректирующих воздействий. Таким образом, замыкается обратная связь влияний корректирующих процедур на организм.

Иформационно-алгоритмическая технология оценивания.

Алгоритмическая последовательность количественного оценивания физического здоровья – донозологической диагностики состояния, согласно разработанной технологии [2,4,5], включает следующие этапы:

- синтез информационно-структурной модели оценивания с новым информационным модулем ИФВ в структуре здоровья, позволяющим оценить готовность организма к различным физическим нагрузкам (рис.1);
- оценка идентификационной оснащенности структурных модулей и выбор наиболее информативных из них в контексте предметной направленности процедур оценивания (с соответствующими внутренними вложениями, включая выбор физиологических систем и натурных показателей, характеризующих их состояние);
- разработка локальных диагностических моделей с учетом их соподчиненности согласно выбранной иерархичности;
- использование в процессе обработки результатов оценивания метода нормированной унификации разнокачественной информации (МНУРИ) для приведения выбранных показателей к безразмерному виду: разработка шкал изменения натурных показателей, перевод натурных показателей в информационные (нормирование), позволяющие сравнивать показатели, имеющие разные единицы измерения;
- свертка полученных локальных оценок в единую обобщенную диагностическую оценку;
- разработка локальных шкал для всех оцениваемых внутренних вложенных модулей и обобщенной шкалы для оценки физического здоровья в целом, сопровождаемых текстовой интерпретацией.

Унификация и нормирование показателей в зависимости от положения на шкале его изменений. Согласно разработанной методологии оценивания [5], количественная диагностика состояния физического статуса здоровья и всех его внутренних вложений (компонент, составляющих и показателей) должно лежать в интервале [0,1]. Равенство нулю всех указанных оценок соответствует наилучшему состоянию, а равенство единице – наихудшему. Для построения диагностических оценок по всем информационно значимым структурно-иерархическим элементам необходимо знать диапазон изменений, на котором выделяются граничные значения (максимум – $x_{\max}$ и минимум – $x_{\min}$) и границы нормы $x^H_{\min}$ и $x^H_{\max}$, которые находятся внутри всего диапазона. В зависимости от расположения на шкале измерений расчетные формулы для нормирования будут иметь различный вид.

Если натурный показатель X находится в интервале

$$x_{\min} \le x \le x^H_{\min}, \quad \text{то} \quad x_{OTH} = \frac{x^H_{\min} - x}{x^H_{\min} - x_{\min}}, \tag{1}$$

если $$x_{\min} \le x \le x^H_{\max}, \quad \text{то} \quad x_{OTH} = 0, , \tag{2}$$

если $$x^H_{\max} \le x \le x_{\max}, \quad \text{то} \quad x_{OTH} = \frac{x - x^H_{\max}}{x_{\max} - x^H_{\max}}, \tag{3}$$

Если показатели выражены в баллах, то принимается, что максимально возможное значение – это значение верхней границы нормы, т.е. $x_{\max} = x^H_{\min}$. В этом случае перевод значений в баллах в относительные показатели проводится по формуле (1).

Натурные измерения, нормированные по формулам (1)–(3), называются информационными показателями и составляют нижний уровень иерархической структуры, в нашем случае – физического здоровья, на которых дальше строятся обобщенные унифицированные оценки состояния на уровне составляющих, уровне компонент в виде линейно взвешенных сумм. Следующий уровень восхождения, согласно [5] представляет в нашем случае уровень физического статуса. Оценка его состояния, базирующаяся на оценках состояния составляющих – ВФС (внутренняя физиологическая сфера), КСО (координирующие системы организма), ИФВ (исполнительные физические возможности) есть линейно взвешенная сумма, по которой индексируется физическое здоровье:

$$\Delta_{фз} = \gamma_1 \Delta\ (ВФС) + \gamma_2 \Delta\ (КСС) + \gamma_3 \Delta\ (ИФВ) \tag{4}$$

Весовые коэффициенты γ_1, γ_2, γ_3, выбранные на основе экспертных оценок, нормируются так, чтобы сумма весов при всех членах равнялась единице; $\Delta(ВФС)$, $\Delta(КСО)$, $\Delta(ИФВ)$ - оценки состояния модулей.

Вербальная интерпретация количественного оценивания базируется на единой количественной классификационной шкале:

Отклонение от нормы:	Норма, нормальное состояние	оценка =0;
	Практическая норма	0,<оценка≤0,033;
	Малое	0, 033<оценка≤0,33;
	Среднее	0,33<оценка≤0,666;
	Значительное	0,666<оценка<1
	Максимальное	оценка =1

Разработанная технология позволяет совокупность оценок на различных уровнях иерархии разработанной структуры физического здоровья интегрировать в одно число (см. (4)) – индекс физического здоровья. Характеристики и оценки, полученные в ходе использования разработанной информационной технологии, могут быть инструментом сравнения, анализа, прогнозирования состояния физического здоровья и основой для принятия решений по его сохранению и укреплению. Достоинством таких индексов является простота интерпретации, удобство в применении для массовых обследований, недостатком – потеря части информации при свертке признаков.

Выводы. Анализ публикаций по исследуемой теме показал, что для оценки физического здоровья существуют различные подходы и методы. Не все предложенные системы дают комплексную оценку компонентов физического здоровья как целостности. Расширение информационной структуры физического здоровья путем включения дополнительного модуля (ИФВ – исполнительные физические возможности) позволяет повысить разрешающую способность оценивания состояния физического статуса за счет разработки дополнительных шкал, применения дополнительных процедур количественного оценивания и более детального вербального трактования полученных результатов. Разработанная технология может служить информационным базисом для разработки компьютерной системы поддержки принятия решений при валеологической экспресс-диагностике и при выборе оздоровительных мероприятий для контроля, коррекции и поддержания здоровья.

СПИСОК ИСПОЛЬЗОВАНЫХ ИСТОЧНИКОВ

1. Дартау Л .А., Мизерницкий Ю .Л., Стефанюк А.Р. Здоровье человека и качество жизни: проблемы и особенности управления М.: СИНТЕГ, 2009. 400 с.
2. Биоэкомедицина / В.И. Гриценко, М.И. Вовк, А.Б. Котова и др. – К.: Наук. думка, 2001.– 318 с.
3. Пустовойт О.Г., Котова А.Б., Кифоренко С.И. Информационные технологии исследования и управления физическим здоровьем человека.// Управляющие системы и машины.– К., 2010.– №3 С.70–77.
4. Открытая концепция здоровья / Ю.Г. Антомонов, В.М. Белов, В.И. Гриценко, А.Б. Котова и др. – К., 1993. – 27 с. – (Препр.) НАН Украины. Ин-т кибернетики им. В.М. Глушкова).
5. Гриценко В.І., Котова А.Б., Вовк М.І., Кіфоренко С.І., Бєлов В.М. Інформаційні технології в біології і медицині: Курс лекцій: Навчальний посібник. – Київ: Наук. думка, 2007. – 382 с.
6. Устав (конституция) Всемирной Организации Здравоохранения принят Международной конференцией (подписан 22 июля 1946 г). Официальный сайт Всемирной организации здоровья/ Информационный бюллетень №220, сентябрь 2010 г. URL: http://www.who.int/mediacentre/factsheets/fs220/ru/index.html
7. Петленко. В.П. Основы валеологии. Книга первая. 1998. – 433 с.
8. Никифоров Г.С. Психология здоровья: Учебник для вузов / Под ред. Г. С. Никифорова. – СПб.: Питер, 2006.– 607 л: ил. – (Серия "Учебник для вузов").
9. Апанасенко Г.Л., Науменко Р.Г. Физическое здоровье и максимальная аэробная способность индивида // Теория и практика физической культуры. – 1988. – №4. – С.2.
10. Апанасенко Г. Л. О возможности количественной оценки здоровья человека // Гигиена и санитария. 1985. № 6. – С. 55–58.
11. Клапчук В. В. Кількісна оцінка рівня фізичного здоров'я та превентивна фізична реабілітація курсантів і студентів вищих навчальних закладів МВС України: навч. посібник / В. В. Клапчук, В. В. Самошкін. – Дніпропетровськ юрид. акад. МВД України, 2005. – 52 с.
12. Амосов Н.М. Моя система здоровья – К.: Здоров'я, 1997. – 56 с.
13. Купер К. Аэробика для хорошего самочувствия / К. Купер // [2-е изд. доп., перераб.]. – М. : Физкультура и спорт, 1989. – 224 с.).
14. Баевский Р.М. Оценка и классификация уровней здоровья с точки зрения теории адаптации // Вестн. АМН СССР. – 1989. – No 8. – С. 73–78.
15.Баевский Р.М. Оценка адаптационных возможностей организма и риск развития заболеваний / Р.М. Баевский, А.П. Берсенева – М.: Медицина, 1997. – 236 с.
16. Баевский Р.М. Теоретические и прикладные аспекты оценки и прогнозирования функционального состояния организма при действии факторов длительного космического полета http://www.imbp.ru/WebPages/win1251/Science/UchSov/Docl/2005/Baevski_speach.html
17. Хрущев СВ., Поляков С.Д., Соболев А.М. Компьютерные технологи мониторинга физического здоровья школьников // Физкультура в профилактике, лечении и реабилитации. – 2004. – № 4 (8). С. 4–9.
18. Аппаратно-программный комплекс ЗДОРОВЬЕ-ЭКСПРЕСС. http://www.mks.ru/dev/functionaltest/healthexpress/].
19. Компьютерные системы для диагностики и профилактики старения.http://www.ngcrussia.org/evm.pdf].
20. Компьютерная программа "МОНИТОРИНГ ЗДОРОВЬЯ" http://healthmonito-ru.1gb.ru/index.php?page=10
21. Салук І. Рівень фізичного здоров'я студентів технічного вищого навчального закладу // Проблеми активації рекреаційно-оздоровчої діяльності населення: Матеріали IV Всеукраїнської науково-практичної конференції. – Львів:ЛДІФК, – 2004. – С.123–125.

Поступила в редколегию 20.09.2014

Кифоренко С. И., д-р биол. наук, Кравченко В. В., асп.,
Международный научно-учебный центр информационных технологий
и систем НАН Украины и МОН Украины, Киев

ІНФОРМАЦІЙНО-ТЕХНОЛОГІЧНІ АСПЕКТИ КОНТРОЛЮ ТА КОРЕКЦІЇ ФІЗИЧНОГО ЗДОРОВ'Я

Описані принципи та підходи до оцінки фізичного здоров'я. проведена структуризація інформаційного поля дослідження, представлена інформаційно-структурна модель оцінювання фізичного здоров'я. Обґрунтовано доцільність його кількісного до нозологічного оцінювання. Приведена інформаційно-структурна схема алгоритму оцінювання фізичного статусу та підтримки прийняття рішень при виборі оздоровчих заходів для контролю, корекції та підтримки здоров'я.

Ключові слова: методи оцінки фізичного здоров'я, ієрархічна згортка, метод інфотомування, метод нормованої уніфікації різноякісної інформації (МНУРИ), підтримка прийняття рішень.

Kiforenko S. I., Doctor of Biological Sciences, Kravchenko V. V., graduate student
International Research and Training Center for Information Technologies
and Systems of the National Academy of Sciences (NAS) of Ukraine
and Ministry of Education and Science (MES) of Ukraine

INFORMATION AND TECHNOLOGICAL ASPECTS OF CONTROL AND CORRECTION OF PHYSICAL HEALTH

The paper describes the principles and approaches to the assessment of physical health. Held structuring information field studies presented information and structural model estimation of physical health. The expediency of its quantitative estimation prenosological. Shows a block diagram of information and the physical status of the estimation algorithm and decision support in the selection of health measures for the control, correction and maintenance of health.

Keywords: methods of assessing physical health, hierarchical convolution method infotomirovaniya method normalized unification of different quality information (MNURI), decision support.

УДК 517.929.4

А. Т. Кожаметов, канд. физ.-мат. наук, доц.,
Нукусский университет, Каракалпакстан, Узбекистан,
А. В. Шатырко, канд. физ.-мат. наук, Д. Я. Хусаинов, д-р физ.-мат. наук,
Киевский национальный університет имени Тараса Шевченко, Киев

ОБ ОДНОМ ЧИСЛЕННОМ МЕТОДЕ ПОЛУЧЕНИЯ ОПТИМАЛЬНОЙ ФУНКЦИИ ЛЯПУНОВА

Рассматривается, ставшая уже классической, задача исследования глобальной устойчивости тривиального положения равновесия системы автоматического регулирования с одной нелинейностью, расположенной в заданном линейном секторе. Т.е. так называемая проблема абсолютной устойчивости. Аппаратом исследования выбран прямой метод Ляпунова, с функциями из заданного класса – квадратичная форма плюс интеграл от нелинейности. Предложен оптимизационный подход практического построения функции Ляпунова для заданного класса, основанный на применении обобщенной градиентной процедуры.

Ключевые слова: система регулирования, функция Ляпунова, абсолютная устойчивость, оптимизация, обобщенный градиент

Введение. Одним из универсальных методов исследования динамики систем различного вида является второй метод Ляпунова. Основные формулировки утверждений метода гласят, что если существует положительно определенная функция, полная производная которой в силу системы является отрицательно определенной функцией, то нулевое решение системы устойчиво (асимптотически устойчиво). Основные теоремы JЛяпунова про устойчивость и асимптотическую устойчивость носят необходимый и достаточный характер. Доказано, если нулевое решение системы асимптотически устойчиво, то функция Ляпунова существует [1]. Однако несмотря на теоретическую завершенность метода неразрешимой проблемой является собственно построение требуемой функции. В каком-то смысле, задача нахождения функции Ляпунова похожа на задачу нахождения интеграла системы. В основном, функция Ляпунова ищется в заранее заданном классе функций, например в классе квадратичных функций [2]. В этом случае задача нахождения функции Ляпунова облегчается.

В работах [3-12] было показано, что проблему нахождения функции Ляпунова можно свести к решению задачи выпуклого программирования с целевой функцией, имеющей вид минимального собственного числа. Были сформулированы условия существования решения поставленных задач. Известно, что одним из эффективных численных методов решения задач оптимизации является градиентный метод [13-15]. Однако в задачах оптимизации функции Ляпунова целевые функции являются недифференцируемыми. Кроме того, встает проблема получения градиента в явном виде. В настоящей работе предлагается использовать понятие «производной по направлению». И, если брать производную по каждой координате положительно определенной матрицы, входящей в функцию Ляпунова, то можно сформулировать понятие «градиента».

Численный метод, основанный на градиентной процедуре. Рассмотрим систему прямого регулирования, описаную системой

$$\dot{x}(t) = Ax(t) + bf(\sigma(t)), \quad \sigma(t) = c^T x(t), \quad A \in R^{n\times n}, \quad x(t), c, b \in R^n \tag{1}$$

Матрица A линейной части системы (1) асимптотически устойчивая, а нелинейная функция $f(\sigma)$, $\sigma(t) = c^T x(t)$ удовлетворяет, так называемому "условию сектора"

$$0 \le \sigma f(\tau) \le k\sigma^2, \; k = const.$$

Система называется абсолютно устойчивой, если ее нулевое решение асимптотически устойчиво в целом, т.е. во всем пространстве, при произвольной функции $f(\sigma)$, удовлетворяющей "условию сектора".

Одним из методов исследования задач абсолютной устойчивости является использование второго метода Ляпунова. Рассмотрим задачу получения гарантированного условия абсолютной устойчивости в заданном классе функций Ляпунова

$$V(x) = x^T Hx + \beta\int_0^{\sigma} f(\sigma)d\sigma\,. \tag{2}$$

с некоторой положительно определенной матрицей H и скаляром $\beta \ge 0$.

Используя "условие сектора", оценку полной производной функции (2) в силу системы (1) можно записать в виде квадратичной формы

$$\frac{d}{dt}V(x(t) \le -x^T(t)C(H,\beta,\nu)x(t),$$

где

$$C(H,\beta,\nu) = \begin{bmatrix} -A^T H - HA & -\left[Hb + \frac{1}{2}(\beta A^T + I\nu)c\right] \\ -\left[Hb + \frac{1}{2}(\beta A^T + I\nu)c\right]^T & \frac{\nu}{k} + \beta b^T c \end{bmatrix},$$

Или в виде

$$\frac{d}{dt}V(x(t)) \le -\lambda_{\min}[C(H,\beta,\nu)]x(t)|^2,$$

где I – единичная матрица, $\nu \ge 0$ - некоторая постоянная (множитель Лагранжа).

И задача исследования абсолютной устойчивости сводится к оптимизационной задаче нахождения положительно определенной матрицы H^0 и величин $\beta^0 \ge 0$, $\nu^0 \ge 0$, при которых минимальное собственное число

симметричной матрицы $C\left(H^0,\beta^0,\nu^0\right)$, которая определяет производную функции Ляпунова в силу системы (1), будет максимальным.

Оптимизационная задача рассматривается на множестве троек $L=\left\{(H,\beta,\nu): H\geq 0,\beta\geq 0,\nu\geq 0\right\}$, где под $H\geq 0$ понимается положительная полуопределенность матриц H. Выберем в качестве нормы

$$\left|(H,\beta,\nu)\right|=\sqrt{\left|H\right|^2+\beta^2+\nu^2},\ \left|H\right|=\lambda_{\max}(H).$$

Тут и далее будем обозначать $\lambda_{\max}(\bullet)$, $\lambda_{\min}(\bullet)$ – экстремальные собственные числа соответствующих симметричных положительно определенных матриц.

Как известно, симметричная матрица $C(H,\beta,\nu)$ положительно определена тогда и только тогда, когда $\lambda_{\min}\left[C(H,\beta,\nu)\right]>0$. И задачу нахождения гарантированного условия абсолютной устойчивости системы (1) в классе функций (2) можно рассматривать как оптимизационную задачу

$$\phi(H,\beta,\nu)\rightarrow\min_{(H,\beta,\nu)\in L} \tag{3}$$

при ограничениях

$$\lambda_{\min}(H)\geq 0,\ \ \beta\geq 0\ \ \nu\geq 0,\qquad \phi(H,\beta,\nu)=-\lambda_{\min}\left[C(H,\beta,\nu)\right]. \tag{4}$$

Нетрудно показать, что множество L - является линейным пространством, которое представляет собой выпуклый конус [3]. И, если оптимизационная задача (3), (4) имеет решением тройку (H^0,β^0,ν^0), для которой будет выполняться

$$\phi(H^0,\beta^0,\nu^0)<0,$$

то система регулирования (1) будет абсолютно устойчивой. Если

$$\phi(H^0,\beta^0,\nu^0)>0,$$

то задача исследования абсолютной устойчивости в классе функций вида (1) за счет выбора H, β, ν не решается.

Обозначим через L_1 подмножество L которое состоит из троек (H,β,ν), находящихся внутри единичной сферы, т.е. удовлетворяющих условию

$$\lambda^2_{\max}(H)+\beta^2+\nu^2\leq 1. \tag{5}$$

Приведенная задача оптимизации является задачей динамического программирования с ограничениями. Наиболее часто используемым методом решения задач такого типа есть градиентный метод и его модификации [13].

Поскольку вычислить градиент от целевой функции, представляющей собой экстремальное собственное число в общем случае затруднительно, для решения задачи оптимизации будем использовать понятие производной по направлению.

Определение. 1. Пусть для двух троек $(H_0,\beta_0,\nu_0),\in L_1$, $(M,\alpha,\gamma),\in L_1$ и $0\leq t\leq t_1$ выполняется $(H_0+tM,\beta_0+t\alpha,\nu_0+t\gamma)\in L_1$. Если существует предел

$$\frac{d\varphi(H_0,\beta_0,\nu_0)}{d(M,\alpha,\gamma)}=\lim_{t\rightarrow+0}\frac{1}{t}\{\varphi(H_0+tM,\beta_0+t\alpha,\nu_0+t\gamma)-\varphi(H_0,\beta_0,\nu_0)\}, \tag{6}$$

то выражение $d\varphi(H_0,\beta_0,\nu_0)/d(M,\alpha,\gamma)$ называется производной функции $\phi(H,\beta,\nu)$ по направлению (M,α,γ) в точке (H_0,β_0,ν_0).

Лемма 1. Производная функции $\varphi(H,\beta,\nu)=-\lambda_{\min}\left[C(H,\beta,\nu)\right]$ по направлению (M,α,γ) в точке $(H_0,\beta_0,\nu_0)\in L_1$ имеет вид

$$\frac{d\varphi(H_0,\beta_0,\nu_0)}{d(M,\alpha,\gamma)}=-(y^0_{\min})^T C(M,\alpha,\gamma)y^0_{\min}. \tag{7}$$

Здесь $y^0_{\min}$ – граничный единичный собственный вектор матрицы $C(H_0,\beta_0,\nu_0)$ по направлению (M,α,γ) т.е.

$$y^0_{\min}=\lim_{t\rightarrow+0}y_{\min}(t),\ \ y_{\min}(t)=y_{\min}\left[C(H_0+tM,\beta_0+t\alpha,\nu_0+\gamma t)\right]. \tag{8}$$

Доказательство. Рассмотрим возмущенную матрицу $C\left[(H_0+tM,\beta_0+t\alpha,\nu_0+t\gamma)\right]$, $0\leq t\leq t_1$ и, соответственно, ее минимальное собственное число $\lambda_{\min}\left[C(H_0+tM,\beta_0+t\alpha,\nu_0+t\gamma)\right]$ и минимальный нормированный собственный вектор $y_{\min}(t)$. В силу непрерывности, при $t\rightarrow+0$ будет выполняться

$$\lambda_{\min}\left[C(H_0+tM,\beta_0+t\alpha,\nu_0+t\gamma)\right]\rightarrow\lambda_{\min}\left[C(H_0,\beta_0,\nu_0)\right],\ y_{\min}(t)\rightarrow y^0_{\min}.$$

Поскольку $y_{\min}(t)$ нормированный вектор, то, по определению, для $0\leq t\leq t_1$ тождественно выполняются соотношения

$$y^T_{\min}(t)y_{\min}(t)\equiv 1,$$

$$\lambda_{\min}\left[C(H_0+tM,\beta_0+t\alpha,\nu_0+t\gamma)\right]\equiv y^T_{\min}(t)C(H_0+tM,\beta_0+t\alpha,\nu_0+t\gamma)y_{\min}(t).$$

Собственное число и собственные векторы симметричных матриц являются кусочно непрерывно дифференцируемыми функциями (кроме случая кратных корней). И в некотором промежутке $0\leq t\leq t_1$ функции $y_{\min}(t)$ и $\lambda_{\min}\left[C(H_0+tM,\beta_0+t\alpha,\nu_0+t\gamma)\right]$ будут иметь производные.

Продифференцировав приведенные тождества по t, получим

$$\left(y'_{\min}(t)\right)^T y_{\min}(t) + y^T_{\min}(t) y'_{\min}(t) \equiv 0, \tag{9}$$

$$\frac{d}{dt}\lambda_{\min}\left[C\left(H_0+tM,\beta_0+t\alpha,\nu_0+t\gamma\right)\right] = \left(y'_{\min}(t)\right)^T C\left(H_0+tM,\beta_0+t\alpha,\nu_0+t\gamma\right) y_{\min}(t) +$$

$$+\left(y_{\min}(t)\right)^T \frac{d}{dt} C\left(H_0+tM,\beta_0+t\alpha,\nu_0+t\gamma\right) y_{\min}(t) +$$

$$+\left(y_{\min}(t)\right)^T C\left(H_0+tM,\beta_0+t\alpha,\nu_0+t\gamma\right) y'_{\min}(t) \tag{10}$$

Первое тождество дает

$$\left(y'_{\min}(t)\right)^T y_{\min}(t) = -y^T_{\min}(t) y'_{\min}(t)$$

Имеют место тождественные соотношения

$$C\left(H_0+tM,\beta_0+t\alpha,\nu_0+t\gamma\right) y_{\min}(t) \equiv \lambda_{\min}\left[C\left(H_0+tM,\beta_0+t\alpha,\nu_0+t\gamma\right)\right] y_{\min}(t)$$

где

$$C\left(H_0+tM,\beta_0+t\alpha,\nu_0+t\gamma\right) = \begin{bmatrix} -A^T H_0 - H_0 A & -\left[H_0 b + \frac{1}{2}\left(\beta_0 A^T + I\nu_0\right)c\right] \\ -\left[H_0 b + \frac{1}{2}\left(\beta_0 A^T + I\nu_0\right)c\right]^T & \frac{\nu_0}{k} - \beta_0 b^T c \end{bmatrix} +$$

$$+t\begin{bmatrix} -A^T M - MA & -\left[Mb + \frac{1}{2}\left(\alpha A^T + I\gamma\right)c\right] \\ -\left[Mb + \frac{1}{2}\left(\alpha A^T + I\gamma\right)c\right]^T & \frac{\gamma}{k} - \alpha b^T c \end{bmatrix}.$$

Отсюда следует, что

$$\lim_{t\to 0}\frac{d}{dt}\lambda_{\min}\left[C(H_0+tM,\beta_0+t\alpha,\nu_0+t\gamma)\right] = \lim_{t\to 0}\left(y_{\min}(t)\right)^T C(M,\alpha,\gamma) y_{\min}(t) =$$

$$= \left(y^0_{\min}\right)^T C(M,\alpha,\gamma) y^0_{\min}$$

$$C(M,\alpha,\gamma) = \begin{bmatrix} -A^T M - MA & -\left[Mb + \frac{1}{2}\left(\alpha A^T + I\gamma\right)c\right] \\ -\left[Mb + \frac{1}{2}\left(\alpha A^T + I\gamma\right)c\right]^T & \frac{\gamma}{k} - \alpha b^T c \end{bmatrix}.$$

И получаем, что

$$\frac{d}{dt}\lambda_{\min}\left[C\left(H_0+tM,\beta_0+t\alpha,\nu_0+t\gamma\right)\right] =$$

$$= \lambda_{\min}\left[C(H_0+tM,\beta_0+t\alpha,\nu_0+t\gamma)\right]\left(y'_{\min}(t)\right)^T y_{\min}(t) - \left(y_{\min}(t)\right)^T C(M,\alpha,\gamma) y_{\min}(t) +$$

$$+\lambda_{\min}\left[C(H_0+tM,\beta_0+t\alpha,\nu_0+t\gamma)\right]\left(y_{\min}(t)\right)^T y'_{\min}(t) = \left(y_{\min}(t)\right)^T C(M,\alpha,\gamma) y_{\min}(t).$$

Переходя к пределу при $t\to 0$, получаем утверждение (7) леммы 1, что и необходимо было доказать.

Приведем условия решения задачи оптимизации (3) - (5) в терминах обобщенного градиента.

Определение 2. Пусть $U \subseteq L_1$ некоторое множество и $(H_0,\beta_0,\nu_0)\in U$. Направление (M,α,γ) назовем возможным в точке (H_0,β_0,ν_0) если существует $t_0>0$ такое, что при всех $0\le t\le t_0$ будет выполняться $(H_0+tN,\beta_0+t\alpha,\nu_0+t\gamma)\in U$.

Приведем необходимые условия решения задачи (3) - (5).

Теорема 1. Пусть U_* – множество точек минимума функции $\phi(H,\lambda,\nu)$ в L_1 и в точке (H_*,λ_*,ν_*) функция $\varphi(H,\beta,\nu)$ имеет производные по всем возможным направлениям. Тогда, если в точке (H_*,β_*,ν_*) функция достигает минимума, то по произвольному возможному направлению (M,α,γ) выполняется условие

$$\frac{d\varphi(H_*,\beta_*,\nu_*)}{d(M,\alpha,\gamma)} \ge 0. \tag{11}$$

Доказательство. Пусть $(H,\beta,\nu)\in L_1$ и (M,α,γ) – возможное направление в этой точке. Тогда, по условию

$$\varphi(H_*+tM,\ \beta_*+t\alpha,\nu_*+t\gamma) - \varphi(H_*,\beta_*,\nu_*) \ge 0.$$

Разделив на $t\ge 0$ и направив $t\to +0$, получим

$$\frac{d\varphi(H_*,\beta_*,\nu_*)}{d(M,\alpha,\gamma)} = \lim_{t\to+0}\frac{\varphi(H_*+tM,\ \beta_*+t\alpha,\nu_*+t\gamma)-\varphi(H_*,\beta_*,\nu_*)}{t} \ge 0,$$

то есть получаем утверждения теоремы.

Возьмем за возможные направления базисные векторы, которые построенные следующим образом. Выберем в пространстве симметричных матриц в качестве базиса матрицы Δ_{sk}, у которых на месте (s,k) – го и (k,s)-го элементов стоит одна вторая, а другие элементы нули (если $s=k$, т.е. это диагональный элемент, то стоит единица), Θ – нулевая матрица. Тогда произвольную симметричную матрицу

$$H = \{h_{ij}\},\ 1\le i\le j\le n$$

можно представить в виде

$$H = \sum_{1 \le k \le sn} h_{ij} \Delta_{ij}$$

Возьмем за базисные направления тройки $(\Delta_{sk},1,1),\ 1 \le i \le j \le n,\ 1 \le i \le j \le n.$ И в качестве производных по направлениям (M,α,γ) функции $\varphi(H,\beta,\nu)$ будем брать производные по этим базисным направлениям. Образуем тройки, первым элементом которых является набор $n(n+1)/2$ квадратичных форм матриц $C(\Delta_{ij},0,0)$, $1 \le i \le j \le n$, а вторым и третим элементами квадратичные формы от матриц $C(\Theta,1,0)$, $C(\Theta,0,1)$

$$\nabla(H,\beta,\gamma) = \left\{\left(y^1_{\min}(s,k)\right)^T C(\Delta_{ij},0,0) y^1_{\min}(s,k), \left(y^2_{\min}\right)^T C(\Theta,1,0) y^2_{\min}, \left(y^3_{\min}\right)^T C(\Theta,0,1) y^3_{\min}\right\}, \quad (12)$$

где

$$C(\Delta_{ij},0,0) = \begin{bmatrix} -A^T\Delta_{ij} - \Delta_{ij}A & -\Delta_{ij}b \\ -b^T\Delta_{ij} & 0 \end{bmatrix} \quad C(\Theta,1,0) = \begin{bmatrix} \Theta & -\frac{1}{2}A^T c \\ -\frac{1}{2}c^T A & -b^T c \end{bmatrix}, \quad C(\Theta,0,1) = \begin{bmatrix} \Theta & -\nu c \\ -c^T\nu & \frac{1}{k} \end{bmatrix}.$$

Здесь $y^1_{\min}(s,k)$ — предельный единичный минимальный собственный вектор матрицы $C(\Delta_{ij},0,0)$, который отвечает направлению $(\Delta_{ij},0,0)$, $y^2_{\min}$ — предельный единичный минимальный собственный вектор матрицы $C(\Theta,1,0)$, который отвечает $(\Theta,1,0)$., $y^3_{\min}$ — предельный единичный минимальный собственный вектор матрицы $C(\Theta,0,1)$, который отвечает $(\Theta,0,1)$.

Определение 3. Назовем тройку

$$\nabla(H,\beta,\gamma) = \left\{\left(y^1_{\min}(s,k)\right)^T C(\Delta_{ij},0,0) y^1_{\min}(s,k), \left(y^2_{\min}\right)^T C(\Theta,1,0) y^2_{\min}, \left(y^3_{\min}\right)^T C(\Theta,0,1) y^3_{\min}\right\},$$

которая составлена из производных по базисным направлениям $(\Delta_{ij},0,0)$ (12) градиентом функции $\varphi(H,\beta,\gamma)$.

Имеет место следующее утверждение.

Теорема 2. Если (H_0,β_0,γ_0) есть решение задачи оптимизации (3) - (5), то градиент $\nabla\varphi(H_0,\beta_0,\gamma_0)$ по направлениям базиса $(\Delta_{sk},0,0),\ (\Theta,1,0),\ (\Theta,0,1),\ 1 \le i \le j \le n$ в точке (H_0,β_0,γ_0) состоит из неотрицательных элементов.

Доказательство. Утверждение теоремы основано на утверждении предшествующей теоремы и выборе производных по направлениям..

СПИСОК ИСПОЛЬЗОВАНЫХ ИСТОЧНИКОВ

1. Красовский Н.Н. Некоторые задачи теории устойчивости движения, М., Физматгиз. – 211 с.
2. Валеев К.Г., Финин Г.С. Построение функций Ляпунова, Киев, Наукова думка, 1981. – 412 с.
3. Хусаинов Д.Я., Кожаметов А.Т., Утебаев Д., Хусаинов Д.Я., Кожаметов А.Т., Утебаев Д. Оптимизация оценок характеристик решений в динамике систем. – Нукус, Изд.-во МВ и ССО Республики Узбекистан, 1992. – 139 с.
4. Хусаинов Д.Я. Об оптимизации оценивания времени переходного процесса в линейных системах с использованием функции Ляпунова. – В сб.: Кибернетика и вычислительная техника. Сложные системы управления, в.69, К.: Изд.-во Института кибернетики АН УССР, 1986. – С.33–37.
5. Жуйкова А.Г., Хусаинов Д.Я. Оптимизация оценки области изменения параметров в системах непрямого регулирования // Вестник Киевского университета. Моделирование и оптимизация сложных систем, в.6, К.: Изд.-во "Наукова думка" при КГУ, 1987. – С.93–97.
6. Хусаинов Д.Я. Оптимизация оценки времени переходного процесса в задачах регулирования.- В сб.: Вычислительная и прикладная математика, в.61, К.: Изд.-во "Наукова думка" при КГУ, 1987. – С.106–112.
7. Хусаинов Д.Я., Кожаметов А.Т. Оптимизация оценок начальных возмущений в линейных стохастических системах.- Вестник Киевского университета. Моделирование и оптимизация сложных систем, в.7, К.: Изд.-во "Наукова думка" при КГУ, 1988. – С.40–45.
8. Хусаінов Д.Я., Давидов В.Ф. Оптимізація оцінки області стійкості квадратичних систем градієнтним методом // Вісник Київського університету. Серія: Фізико-математичні науки, в.4, 1992. – С.27–33.
9. Бычков А.С., Лобок А.П., Нечаева И.Г., Хусаинов Д.Я. Оптимизация оценок устойчивости систем стохастических дифференциально-разностных уравнений // Кибернетика и системный анализ, – №4, – 1992. – С.38–43.
10. Хусаинов Д.Я., Марценюк В.П. Оптмизационный метод исследования устойчивости линейных систем с запаздыванием // Кибернетика и системный анализ, N4, 1996. – С.88–93.
11. Хусаинов Д.Я., Марценюк В.П. Оптимизационный метод построения функционалов Ляпунова-Красовского в стационарных системах с запаздыванием. – В сб. Вычислительная и прикладная математика, – В.80, – 1996. – С.142–151.
12. Хусаинов Д.Я., Стадник О.И., Давыдов В.Ф. Оптимизация оценок характеристик динамических систем // Журнал обчислювальної та прикладної математики, – N1 (84), – 1999, – С.128–136.
13. Бейко І.В., Зінько П.М. Наконечний О.Г. Задачі, методи та алгоритми оптимізації. – К., ВПЦ Київського національного університета імені Тараса Шевченка, – 2012. – 799 с.
14. Васильев Ф.П. Численные методы решения экстремальных задач. – М., Наука, 1988. – 552 с.
15. Пшеничный Б.Н., Данилин Ю.М. Численные методы в экстремальных задачах. – М., Наука, 1975. – 320 с.

Поступила в редколлегию 20.09.14

Кожаметов А. Т. канд. фіз.-мат. наук, доц.,
Нукуського університета, Каракалпакстан, Узбекістан,
Шатирко А. В., канд. фіз.-мат. наук,
Хусаїнов Д. Я., д-р фіз.-мат. наук,
Київський національний університет імені Тараса Шевченка, Київ

ПРО ОДИН ЧИСЕЛЬНИЙ МЕТОД ОТРИМАННЯ ОПТИМАЛЬНОЇ ФУНКЦІЇ ЛЯПУНОВА

Розглядається задача, що стала вже класичною, дослідження глобальної стійкості тривіального положення рівноваги системи автоматичного регулювання з однією нелінійністю, що розташована в заданому лінійному секторі. Т.е. так звана проблема абсолютної стійкості. Апаратом дослідження обрано прямий метод Ляпунова, з функціями із заданого класу – квадратична форма плюс інтеграл від нелінійності. Запропоновано оптимізаційний підхід практичної побудови функції Ляпунова для заданого класу, заснований на застосуванні узагальненої градієнтної процедури.

Ключові слова: система регулювання, функція Ляпунова, абсолютна стійкість, оптимізація, узагальнений градієнт

Kozhametov A. T. Ph.D. in Math.,
Universiteta Nukus, Karakalpakstan, Uzbekistan,
Shatyrko A. V., Ph.D. . in Math.,
Khusainov D. Ya., Dr. Sc. Prof.,
Faculty of Cybernetics, Taras Shevchenko National University of Kyiv

ON A NUMERICAL METHOD FOR OBTAINING THE OPTIMAL LYAPUNOV FUNCTION

The problem of studying the global stability of the trivial equilibrium position of the automatic control system with a non-linearity, which is located at a predetermined linear sector, is considered. This is so-called absolute stability problem (or Lur'e problem), which has already become a classic. Lyapunov's direct method, with the functions of a given class – quadratic form plus integral of the nonlinearity is selected as apparatus for studying. We propose an optimization approach practical construction of Lyapunov function for a given class, based on the application of the generalized gradient procedure.

Key words: Lur'e type control system, Lyapunov function, absolute stability, optimization, generalized gradient.

УДК 517.929

А. В. Нікітін, канд. фіз.-мат. наук, доц.
Чернівецький національний університет, Чернівці

МОМЕНТНІ РІВНЯННЯ ДЛЯ ЛІНІЙНИХ СТОХАСТИЧНИХ РІВНЯНЬ ІЗ ВИПАДКОВИМИ КОЕФІЦІЄНТАМИ У ГІЛЬБЕРТОВИХ ПРОСТОРАХ

Робота присвячена дослідженню стійкості розв'язків лінійних стохастичних диференціальних рівнянь у гільбертових просторах з допомогою моментних рівнянь.

Ключові слова: Гільбертовий простір, стійкість, диференціальні рівняння

Нехай H – гільбертів простір і $X(t)$ – векторний випадковий процес із H, що є розв'язком рівняння

$$dX(t) = A(t,\xi(t))X(t)dt + \sum_{j=1}^{\infty} B_j(t,\xi(t))X(t)dW_j(t), \quad X(0) = \zeta, \tag{1}$$

де $\xi(t)$ – неперервний справа марковський процес, що набуває зліченну кількість значень $\theta_1,...,\theta_q,...$; $A(t,\theta_s), B_j(t,\theta_s), s = \overline{1,q},$ – неперервні на відрізку $[0,T]$ функції, $W_1(t),...,W_r(t),...$ – незалежні між собою скалярні вінерові процеси, причому величини $(W_1(t),...,W_r(t),...,\xi(t),\zeta)$ також є незалежними. Позначимо $P_s(t) \equiv P\{\xi(t) = \theta_s\}$. Вважатимемо, що існують неперервні на відрізку $[0,T]$ функції $\alpha_{kj}(t)$ такі, що

$$P_{kj}(t+h,t) = \delta_{kj} + \alpha_{kj}(t)h + o(h), \tag{2}$$

де δ_{kj} – символ Кронекера, $h > 0$, $\frac{o(h)}{h} \to 0, h \to 0$.

Нехай

$$F_k(t,x) = P\{X(t) < x, \xi(t) = \theta_k\},$$
$$m_k(t) = \int_{R^m} x dF_k(t,x),$$
$$D_k(t) = \int_{R^m} xx^* dF_k(t,x).$$

Означення 1. *Функції $m_k(t), D_k(t)$ називаються частковими середніми та частковими матрицями других моментів відповідно.*

Теорема 1. *Нехай $X(t)$ є розв'язком рівняння (1), $\left\langle |\zeta|^2 \right\rangle < \infty$, а перехідні ймовірності марковського процесу $\xi(t)$ задовольняють умові (2). Тоді справедливими є рівняння*

$$\frac{dm_k(t)}{dt} = A_k(t)m(t) + \sum_{s=1}^{\infty} \alpha_{ks} m_s(t), \quad m_k(0) = \langle \zeta \rangle P_k(0), \quad k = \overline{1,q}, \tag{3}$$

$$\frac{dD_k(t)}{dt} = A_k(t)D_k(t) + D_k(t)A_k^*(t) + \sum_{j=1}^{\infty} B_{jk}(t)D_k(t)B_{jk}^*(t) +$$
$$+ \sum_{s=1}^{\infty} \alpha_{ks} D_s(t), \quad D_k(0) = \left\langle \zeta\zeta^* \right\rangle P_k(0), \quad k = \overline{1,q}, \tag{4}$$

де $A_k(t) = A(t,\theta_k), B_{jk}(t) = B_j(t,\theta_k)$.

Доведення. Розіб'ємо інтервал $(0,T)$ точками $0 < t_1 < t < ... < t_N < T$ з кроком t_{k+1}, $t_k = h$, $t_n = nh$. Позначимо через $X(n) = X(t_n)$, $\xi_n = \xi(t_n)$, $A(n,\xi_n) = A(t_n,\xi(t_n))$, $B_j(n,\xi_n) = B_j(t_n,\xi(t_n))$. Поставимо у відповідність рівнянню (1) різницеве рівняння

$$X(n+1) = X(n) + hA(n,\xi_n)X(n) + \sum_{j=1}^{\infty} B_j(n,\xi_n)\Delta W_j(t_n)X(n), \quad X(0) = \zeta, \tag{5}$$
$$\Delta W_j(t_n) = W_j(t_{n+1}) - W_j(t_n).$$

Для часткових моментів вектора $X(n)$ запишемо рівняння

$$m_k(n+1) = \sum_{s=1}^{\infty} P_{ks}(n)[E + hA_s(n)]m_s(n) =$$

$$= P_{kk}(n)[E + hA_k(n)]m_k(n) + \sum_{s\neq k} P_{ks}(n)\left[E + hA_s(n)\right]m_s(n) =$$

$$= (1+\alpha_{kk}(n)h)[E + hA_k(n)]m_k(n) + h\sum_{s\neq k}\alpha_{ks}(n)\left[E + hA_s(n)\right]m_s(n) =$$

$$= m_k(n) + hA_k(n)m_k(n) + h\sum_{s=1}^{\infty}\alpha_{ks}(n)m_s(n) + o(h)$$

або

$$\frac{m_k(n+1) - m_k(n)}{h} = A_k(n)m_k(n) + \sum_{s=1}^{\infty}\alpha_{ks}(n)\,m_s(n) + \frac{o(h)}{h}.$$

Спрямуємо h до нуля. Тоді одержимо рівняння (3). Запишемо далі рівняння для часткових матриць $D_k(n)$ вектора $X(n)$. Із рівнянь (5) випливає, що матриця $D_k(n)$ задовольняє рівняння

$$D_k(n+1) = \sum_{s=1}^{\infty}[E + hA_s(n)]D_s(n)[E + hA_s(n)]^* + \sum_{s=1}^{\infty}\sum_{s=1}^{\infty}P_{ks}(n)B_{js}(n)D_s(n)B^*_{js}(n)h.$$

При виведенні цього рівняння ми скористалися тим, що $\left\langle \Delta W_j(t_n)\Delta W_k(t_n)\right\rangle = \delta_{jk}$. Перепишемо рівняння для $D_k(n)$ у наступному вигляді

$$D_k(n+1) = P_{kk}(n)[E + hA_k(n)]D_k(n)[E + hA_k(n)]^* +$$

$$+\sum_{s\neq k}[E + hA_s(n)]D_s(n)[E + hA_s(n)]^*P_{ks}(n) +$$

$$+\sum_{j=1}^{\infty}P_{kk}(n)B_{jk}(n)D_k(n)B^*_{jk}h + \sum_{s\neq k}\sum_{j=1}^{\infty}P_{ks}(n)B_{js}(n)D_s(n)B^*_{js}h =$$

$$= D_k(n) + hA_k(n)D_k(n)A^*_k(n) + h\sum_{j=1}^{\infty}B_{jk}(n)D_k(n)B^*_{jk}(n) + h\sum_{s=1}^{\infty}\alpha_{ks}(n)D_s(n) + o(h),$$

або поділивши на h та спрямувавши h до нуля одержимо рівняння (3).

Припустимо далі, що $0 \le \tau_1 < \tau_2 < \ldots < \tau_N \le T$ є стрибки процесу $\xi(t)$ на проміжку $[0,T]$.

$X(t)$ – розв'язок стохастичного рівняння (1) з умовами

$$X(\tau_j) = C(\xi(\tau_j), \xi(\tau_j - 0))X(\tau_j - 0), \tag{6}$$

де $C_{ks} = C(\theta_k, \theta_s)$ – деякі матриці.

Нехай $0 \le t_1 < t_2 < \ldots < t_N \le T$ точки розбиття відрізку $[0,T]$ з кроком h, так що $t_n = nh$, $t_{k+1} - t_k = h$. Поставимо у відповідність рівнянню (1) з умовами (6) різницеве рівняння

$$X_{n+1} = X_n + [hA(t_n, \xi_{n+1}, \xi_n) + \sum_{j=1}^{\infty}B_j(t_n, \xi_{n+1}, \xi_n)\Delta W(t_n)]X_n, \quad X(0) = \zeta, \tag{7}$$

де

$\xi_n = \xi(t_n)$, $X_n = X(t_n)$, $A(t_n, \theta_s, \theta_s) = A(t_n, \theta_s)$, $B_j(t_n, \theta_s, \theta_s) = B_j(t_n, \theta_s)$, $B_j(t_n, \theta_k, \theta_s) = 0, k \neq s$, $E + hA(t_n, \theta_k, \theta_s) = C(\theta_k, \theta_s), k \neq s$.

Запишемо рівняння для часткових моментів вектора X_n.

$$m_k(n+1) = \sum_{s=1}^{\infty}P_{ks}(n)[E + hA(t_n, \theta_k, \theta_s)]m_s(n) =$$

$$= P_{kk}(n)[E + hA(t_n, \theta_k)]m_k(n) + \sum_{s\neq k}P_{ks}(n)C(\theta_k, \theta_s)m_s(n) =$$

$$= (1+\alpha_{kk}(n)h)[E + A(t_n, \theta_k)h]m_k(n) + h\sum_{s\neq k}\alpha_{ks}(n)C(\theta_k, \theta_s)m_s(n) =$$

$$= m_k(n) + h\alpha_{kk}(n)m_k(n) + hA(t_n, \theta_k)m_k(n) + h\sum_{s\neq k}\alpha_{ks}(n)C(\theta_k, \theta_s)m_s(n) + o(h).$$

При $h \to 0$ одержимо рівняння

$$\frac{dm_k(t)}{dt} = A_k(t)m_k(t) + \sum_{s=1}^{\infty}\alpha_{ks}C_{ks}m_s(t),$$
$$m_k(0) = \left\langle \zeta \right\rangle P\{\xi(0) = \theta_k\}, \tag{8}$$

де $A_k(t) = A(t, \theta_k), C_{ks} = C(\theta_k, \theta_s)$ при $k \neq s$, $C_{kk} = E$.

Одержимо рівняння для часткових других моментних матриць. Зауважимо, що $D_k(n)$ задовольняють рівняння

$$D_k(n+1) = \sum_{s=1}^{\infty}P_{ks}(n)\bar{A}_{ks}D_s(n)\bar{A}^*_{ks} + \sum_{s=1}^{\infty}P_{ks}(n)\sum_{j=1}^{\infty}B_{jks}D_s(n)B^*_{jks}h,$$

де $\bar{A}_{ks} = E + hA(t_n, \theta_k, \theta_s)$, $B_{jks} = B_j(t_n, \theta_k, \theta_s)$.

Далі перепишемо рівняння $D_k(n)$ у вигляді

$$D_k(n+1) = P_{kk}(n)\bar{A}_{kk}D_k(n)\bar{A}^*_{kk} + \sum_{s\neq k}P_{ks}(n)C_{ks}D_s(n)C^*_{ks} +$$

$$+P_{kk}(n)\sum_{j=1}^{\infty}B_{jkk}D_k(n)B^*_{jkk}h + \sum_{s\neq k}P_{ks}(n)\sum_{j=1}^{\infty}B_{jks}D_s(n)B^*_{jks}h =$$

$$= D_k(n) + hA(t_n, \theta_k)D_k(n)A^*(t_n, \theta_k) + h\sum_{s\neq k}\alpha_{ks}(n)C_{ks}D_s(n)C^*_{ks} +$$

$$+\alpha_{kk}D_k(n)h + h\sum_{j=1}^{\infty}B_{jkk}D_s(n)B_{jkk}^* + o(h).$$

При $h \to 0$ одержимо рівняння

$$\frac{dD_k(t)}{dt} = A_k(t)D_k(t) + D_k(t)A_k^*(t) +$$
$$+\sum_{s=1}^{\infty}\alpha_{ks}C_{ks}D_k(t)C_{ks}^* + \sum_{j=1}^{\infty}B_j(t,\theta_k)D_k(t)B_j^*(t,\theta_k), \quad (9)$$
$$D_k(0) = \langle\zeta\zeta^*\rangle P\{\xi(t) = \theta_k\},$$

де $C_{kk} = E$.

Таким чином, ми показали, що має місце наступне твердження.

Твердження 1. *Нехай* $X(t)$ *є розв'язком рівняння (1) з умовами (6). Тоді функції* $m_k(t), D_k(t), k = \overline{1,q}$, *є розв'язками рівнянь (8) та (9) відповідно.*

Припустимо далі, що стрибки процесу $X(t)$ задовольняють умові

$$X(\tau_j) = C(\xi(\tau_j),\xi(\tau_j - 0))X(\tau_j - 0) + H(\tau_j,\xi(\tau_j),\xi(\tau_j - 0)).$$

Введемо позначення: $H_{ks}(t) = H(t,\theta_k,\theta_s)$ при $k \neq s$ та $H_{ss}(t) = 0$. Нехай вектор функція $H_{ks}(t)$ є неперервною на відрізку $[0,T]$.

Твердження 2. *Функції* $m_k(t)$ *та* $D_k(t), k = \overline{1,q}$, *є розв'язками лінійних диференціальних рівнянь*

$$\frac{dm_k(t)}{dt} = A_k(t)m_k(t) + \sum_{s=1}^{\infty}\alpha_{ks}(t)(C_{ks}m_s(t) + H_{ks}(t)P_s(t)),$$
$$m_k(0) = \langle\zeta\rangle P\{\xi(0) = \theta_k\}, \quad (10)$$
$$\frac{dD_k(t)}{dt} = A_k(t)D_k(t) + D_k(t)A_k^*(t) +$$
$$+\sum_{s=1}^{\infty}\alpha_{ks}(t)[C_{ks}D_s(t)C_{ks}^* + C_{ks}m_k(t)H_{ks}^*(t) + H_{ks}(t)m_k^*(t)C_{ks}^*] +$$
$$+\sum_{s=1}^{\infty}\alpha_{ks}H_{ks}(t)H_{ks}^*(t)P_k(t).$$
$$D_k(0) = \langle\zeta\zeta^*\rangle P\{\xi(t) = \theta_k\},$$

де $P_k(t) = P\{\xi(t) = \theta_k\}, k = \overline{1,q}$.

Доведення. Нехай $t_k, k = \overline{1,n}$, – точки розбиття відрізку $[0,T]$ з кроком h, $0 \le t_1 < t_2 < \ldots < t_N = T$, $t_{k+1} - t_k = h$, $k = \overline{1,N-1}$. Покладемо $t_n = nh$, $n = \overline{1,N}$. Поставимо у відповідність рівнянню з умовами різницеве рівняння

$$X_{n+1} = f(X_n,\xi_{n+1},\xi_n,t_n), \quad X(0) = \zeta, \quad n = 0,1,2,\ldots,$$

де

$$X_n = X(t_n),$$
$$f(X,\theta_s,\theta_s,t_n) = X + hA_s(t_n)X + \sum_{j=1}^{\infty}B_{js}(t_n)\Delta W_j(t_n),$$
$$f(X,\theta_k,\theta_s,t_n) = C_{ks}X + H_{ks}(t_n), \ k \neq s.$$

Тоді рівняння для частинних середніх вектора X_n буде мати вигляд

$$m_k(n+1) = P_{kk}(n)(E + hA_k(t_n))m_k(n) + \sum_{s\neq k}P_{ks}(n)C_{ks}m_s(n) + \sum_{s\neq k}P_{ks}(n)H_{ks}(t_n)P_s(t_n),$$

або враховуючи рівності

$$P_{kk}(n) = \alpha_{kk}(n)h + o(h), \ \ P_{ks}(n) = \alpha_{ks}(n)h + o(h),$$

матимемо

$$m_k(n+1) = m_k(n) + hA_k(t_n)m_k(n) + \alpha_{kk}(n)m_k(n)h +$$
$$+h\sum_{s\neq k}\alpha_{ks}(n)C_{ks}m_s(n) + h\sum_{s\neq k}\alpha_{ks}(n)H_{ks}(t_n)P_s(t_n) + o(h).$$

При $h \to 0$ одержимо рівняння для функцій $m_k(t)$. Аналогічно доводиться, що справедливим є рівняння для $D_k(t)$.

Зауваження. Функції $P_k(t)$ є розв'язком диференціального рівняння

$$\frac{dP_k(t)}{dt} = \sum_{k=1}^{\infty}\alpha_{ks}(t)P_s(t), \quad P_k(0) = P\{\xi(0) = \theta_k\}.$$

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Беллман Р., Кук К. Дифференциально-разностные уравнения. – М.: Мир, 1967. – 548 с.
2. Валеев К.Г., Карелова О.Л., Горелов В.И. Оптимизация линейных систем со случайными коэффициентами. Монография. – М.: Изд-во РУДН, 1996. – 258 с.
3. Биллингсли П. Сходимость вероятностных мер. – М.: Наука, 1977. – 352 с.
4. Боголюбов Н.Н., Митропольский Ю.А. Асимптотические методы в теории нелинейных колебаний. – М.: Физматгиз, 1962. – 412 с.
5. Гихман И.И., Скороход А.В. Стохастические дифференциальные уравнения и их приложения. – Киев: Наукова думка, 1982. – 612 с.

6. Гихман И.И., Скороход А.В. Стохастические дифференциальные уравнения. – Киев: Наукова думка, 1968. – 354 с.
7. Далецкий Ю.Л., Крейн М.Г. Устойчивость решений дифференциальных уравнений в банаховом пространстве. – М.: Наука, 1970. – 536 с.
8. Данфорд Н., Шварц Дж.Т. Линейные операторы. 1. Общая теория. – М.: НЛ, 1962. – 895 с.
9. Дуб Дж.Л. Вероятностные процессы. – М.: НЛ, 1965. – 605 с.
10. Дынкин Е.Б. Марковские процессы. – М.: Физматгиз, 1963. – 859 с.
11. Жакод Ж., Ширяев А.Н. Предельные теоремы для случайных процессов. – Т.1. – М.: Наука, 1994. – 544 с.
12. Жакод Ж., Ширяев А.Н. Предельные теоремы для случайных процессов. – Т.2. – М.: Наука, 1996. – 628 с.
13. Кац И.Я. Метод функций Ляпунова в задачах устойчивости и стабилизации систем случайной структуры. – Екатеринбург: Изд-во Уральской госакадемии путей сообщения, 1998. – 222 с.
14. Колмановский В.Б., Носов В.Р. Устойчивость и периодические режимы регулируемых систем с последействием. – М. Наука, 1981. – 448 с.
15. Скороход А.В. Асимптотические методы теории стохастических дифференциальных уравнений. – Киев.: Наукова думка, 1987. – 328 с.
16. Хасьминский Р.З. Устойчивость систем дифференциальных уравнений при случайных возмущениях их параметров. – М.: Наука, 1969. – 367 с.
17. Хейл Дж . Теория функционально-дифференциальных уравнений. – М.: Мир, 1984. – 421 с.
18. Царьков Е.Ф. Случайные возмущения дифференциально-функциональных уравнений. – Рига: Зинатне, 1989. – 429 с.
19. Korolyuk V.S., Limnions W. Stochastic systems in merging Phase Space. – London: World Scientific, 2006. – 331 p.

Надійшла до редколегії 15.05.14

Никитин А. В. канд. физ.-мат. наук
Черновицкий национальный университет, Черновцы

МОМЕНТНЫЕ УРАВНЕНИЯ ДЛЯ ЛИНЕЙНЫХ СТОХАСТИЧЕСКИХ УРАВНЕНИЙ СО СЛУЧАЙНЫМИ КОЭФФИЦИЕНТАМИ В ГИЛЬБЕРТОВОМ ПРОСТРАНСТВЕ

Посвящена исследованию устойчивости решений линейных стохастических дифференциальных уравнений в гильбертовом пространстве с помощью моментных уравнений.
Ключевые слова: Гильбертовое пространство, устойчивость, дифференциальные уравнения

Nikitin A. V. Ph.D. Physics and Mathematics
Chernivtsi National University, Chernivtsi

MOMENT EQUATION FOR LINEAR STOCHASTIC DIFFERENTIAL EQUATIONS WITH RANDOM COEFFICIENTS IN A HILBERT SPACE

This article is devoted to research of stability of decisions of linear stochastic differential equations in Hilbert Space with the help of moment equations.
Keywords: Hilbert space, stability, differential equations

УДК 512.7+519.7+681.3

В. В. Скобелев, канд. физ.-мат. наук,
В. Г. Скобелев, д-р физ.-мат. наук, д-р техн. наук, проф.,
ИПММ НАН Украины, Донецк

МЕТОДЫ АНАЛИЗА АВТОМАТНО-АЛГЕБРАИЧЕСКИХ МОДЕЛЕЙ

В работе рассмотрены методы анализа автоматных моделей, определенных над конечными кольцами. Для управляемых логических операций исследована сложность обнаружения и локализации неисправностей в процессе off-line контроля их аппаратных реализаций, а также вычислительная стойкость семейств легко-вычислимых перестановок. Исследована задача построения имитационной модели для семейства автоматов, определенных системами уравнений над конечными кольцами, а также вычислительная стойкость семейства хэш-функций, определяемых автоматом без выхода. Исследованы автоматы, определенные на многообразии над конечным кольцом, в том числе, автоматы, определенные на эллиптической кривой над конечным полем.

Ключевые слова: конечные автоматы, конечные кольца, многообразия, эллиптические кривые.

Введение. Развитие информационных технологий на современном этапе, их проникновение практически во все сферы деятельности человечества выдвинули защиту информации в число одной из наиболее актуальных проблем. От ее успешного решения зависит не только благополучие индивидуумов, организаций и государств, но часто и их существование. Именно по этой причине в течение последних тридцати лет всем мире прилагаются значительные усилия в области разработки математических основ криптографии (достаточно полный анализ используемых в криптографии моделей и методов содержится в [1–3]). Последняя, в свою очередь, оказывает существенное влияние на переосмысление задач, решаемых в классических областях математики (теория чисел, теория конечных алгебраических систем, алгебраическая геометрия и т.д.) и компьютерных наук (теория булевых функций, теория автоматов, теория алгоритмов и т.д.). В частности, на первый план выходит анализ вычислительной стойкости алгоритмов преобразования информации [4].

Переход криптографии от комбинаторных моделей к комбинаторно-алгебраическим моделям стимулировал создание нового раздела алгебраической теории автоматов, объект исследования которого – автоматы, определенные на конечных алгебраических структурах, а предмет исследования – анализ вычислительной стойкости отображений, реализуемых исследуемыми инициальными автоматами. Отметим, что такой анализ включает в себя в качестве основных задачи идентификации начального состояния автомата и параметрической идентификации автомата, принадлежащего заданному семейству, а также исследование множества неподвижных точек автоматных отображений.

В настоящей работе дан обзор результатов исследований автоматно-алгебраических моделей, полученных в ИПММ НАН Украины.

1. Управляемые логические операции. Эти операции являются основой построения скоростных блочных шифров [5]. Формальная модель управляемой перестановочной (соответственно, подстановочной) операции – такое отображение $\mathbf{y}=\mathbf{f}(\mathbf{x},\mathbf{v})$, ($\mathbf{x}\in\mathbf{E}^n$, $\mathbf{v}\in\mathbf{E}^m$, $\mathbf{y}\in\mathbf{E}^l$, $\mathbf{E}=\{0,1\}$), что $n=l$ (соответственно, $n\le l$) и для каждого $\mathbf{v}_0\in\mathbf{E}^m$ отображение $\mathbf{g}_{\mathbf{v}_0}:\mathbf{E}^n\to\mathbf{E}^l$, где $\mathbf{g}_{\mathbf{v}_0}(\mathbf{x})=\mathbf{f}(\mathbf{x},\mathbf{v}_0)$ – перестановка компонент вектора $\mathbf{x}\in\mathbf{E}^n$ (соответственно, инъекция). Вектор $\mathbf{x}\in\mathbf{E}^n$ – информационный, а вектор $\mathbf{v}\in\mathbf{E}^m$ – управляющий.

Так как управляемые логические операции могут быть реализованы аппаратно, то естественно возникают задачи off-line обнаружения и локализации неисправностей комбинационной схемы C, реализующей ту или иную управляемую логическую операцию. Эти задачи исследованы в [6–12]. Основные результаты состоят в следующем.

Пусть C – комбинационная схема, реализующая управляемую логическую операцию. Сложность $\mu(\tilde{N})$ схемы C определим как общее число ножек всех ее элементов, неисправность схемы C – как одиночную константную неисправность ножки или как короткое замыкание двух соседних ножек элемента, сложность $\mu_a(C)$ теста, обнаруживающего $(a = dt)$, либо локализирующего $(a = lc)$ исследуемые неисправности – как количество элементов матрицы, строки которой – вход-выходные пары эталона, а относительную асимптотическую сложность теста по отношению к сложности схемы C – как величину $O(\mu_a(C)\cdot\mu^{-1}(\tilde{N}))$ при условии, что длина информационного вектора неограниченно возрастает.

Обозначим через $\mathbf{M}_{n,m}^{(1)}$ (соответственно, $\mathbf{M}_{n,m}^{(2)}$) блок управляемых перестановок (БУП) в котором элементы, реализующие перестановку, соединены последовательно (соответственно, параллельно), а через $\mathbf{M}_{n,m}^{(3)}$ – БУП, в котором отсутствует дешифратор, а управляющие символы подаются непосредственно на управляющие входы последовательно соединенных элементов, реализующих управляемые перестановки. Доказаны следующие теоремы.

Теорема 1. Для всех чисел $m,n \in \mathbf{N}$ $(m \le \lceil \log n! \rceil)$ истинны неравенства

$$\mu_{dt}(\mathbf{M}_{n,m}^{(1)}) \le (m+2n+2)(2^m + \lceil 0{,}5m \rceil + 1),$$

$$\mu_{lc}(\mathbf{M}_{n,m}^{(1)}) \le (m+2n+2)(2^m(n+1) + \lceil 0{,}5m \rceil - 2n + 1),$$

$$\mu_a(\mathbf{M}_{n,m}^{(2)}) \le (m+2n+2)(2^m(n+1) + \lceil 0{,}5m \rceil - 2n + 1) \quad (a \in \{dt, lc\}).$$

Теорема 2. Для всех чисел $m,n \in \mathbf{N}$ $(m \le \lceil \log n! \rceil)$ истинны неравенства

$$\mu_{dt}(\mathbf{M}_{n,m}^{(3)}) \le 2n(2n+m),\ \mu_{lc}(\mathbf{M}_{n,m}^{(3)}) \le (2n+m)(2n+m+nm).$$

Из этих теорем вытекает, что:

1. Если $2^m = O(n!)$ $(n \to \infty)$, то:

1) относительная асимптотическая сложность обнаружения неисправностей БУП $\mathbf{M}_{n,m}^{(1)}$ по отношению к сложности БУП $\mathbf{M}_{n,m}^{(1)}$ не превосходит величины $O(\log n)$ $(n \to \infty)$;

2) относительная асимптотическая сложность локализации неисправностей БУП $\mathbf{M}_{n,m}^{(1)}$ по отношению к сложности БУП $\mathbf{M}_{n,m}^{(1)}$, а также относительная асимптотическая сложность обнаружения либо локализации неисправностей БУП $\mathbf{M}_{n,m}^{(2)}$ по отношению к сложности БУП $\mathbf{M}_{n,m}^{(2)}$ не превосходит величины $O(n\log n)$ $(n \to \infty)$.

2. Если $m = O(n\log n)$ $(n \to \infty)$, то:

1) относительная асимптотическая сложность обнаружения неисправностей БУП $\mathbf{M}_{n,m}^{(3)}$ по отношению к сложности БУП $\mathbf{M}_{n,m}^{(3)}$ не превосходит величины $O(\log n)$ $(n \to \infty)$;

2) относительная асимптотическая сложность локализации неисправностей БУП $\mathbf{M}_{n,m}^{(3)}$ по отношению к сложности БУП $\mathbf{M}_{n,m}^{(3)}$ не превосходит величины $O(n\log n)$ $(n \to \infty)$.

Послойный БУП $\mathbf{P}_{n,m}$ содержит элементы, реализующие перестановки компонент n-битовой последовательности, которые последовательно соединены с помощью элементов $\mathbf{P}_{2,1}$, реализующих такое отображение $\mathbf{g}: \mathbf{E}^2 \times \mathbf{E} \to \mathbf{E}^2$, что

$$\mathbf{g}(\mathbf{x}, v) = \begin{cases} (x_2, x_1), \text{ åñëè } v = 1 \\ (x_1, x_2), \text{ åñëè } v = 0 \end{cases} \quad (\mathbf{x} = (x_1, x_2) \in \mathbf{E}^2).$$

Доказана следующая теорема.

Теорема 3. Для всех чисел $n,l \in \mathbf{N}$ (n – четное число) и $m = 0{,}5n(l-1)$ истинны неравенства $\mu_{dt}(\mathbf{P}_{n,m}) \le n^2(l+3)$ и $\mu_{lc}(\mathbf{P}_{n,m}) \le n^2(l+3)(l-1)$.

Из теоремы 3 вытекает, что если $n \to \infty$ и $l \to \infty$, то:

1) относительная асимптотическая сложность обнаружения неисправностей БУП $\mathbf{P}_{n,m}$ по отношению к сложности БУП $\mathbf{P}_{n,m}$ не превосходит величины $O(n)$ $(n \to \infty)$;

2) относительная асимптотическая сложность локализации неисправностей БУП $\mathbf{P}_{n,m}$ по отношению к сложности БУП $\mathbf{P}_{n,m}$ не превосходит величины $O(\mu^2(\mathbf{P}_{n,m}))$ $(n \to \infty)$.

Пусть $\mathbf{C}_{(r,s),m}$ и $\mathbf{C}_{(r,s,r),m}$ (где $rs = n$) – соответственно, 2-х и 3-х уровневая сеть Клоса.

Доказана следующая теорема.

Теорема 4. Для $a \in \{dt, lc\}$ истинны следующие неравенства

$$\mu_a(\mathbf{C}_{(r,s,r),m}) \le 2s(2r + 2m' + m'')(2s\mu_a(\mathbf{P}_{n,m'}) + r\mu_a(\mathbf{P}_{s,m''})),$$

$$\mu_a(\mathbf{C}_{(r,s),m}) \le 2s(2r + m' + m'')(s\mu_a(\mathbf{P}_{n,m'}) + r\mu_a(\mathbf{P}_{s,m''})).$$

На основе анализа сетей Клоса построена рекурсивная процедура построения тестов для рекурсивных БУП. Показано, что эта процедура применима также для достаточно широкого класса управляемых подстановочных операций.

В [13] исследована структура такого множества F_π семейств перестановок компонент n-битовых векторов $H(\mathbf{h}_1,\ldots,\mathbf{h}_k)=\{\mathbf{h}_1^{\alpha_1}\circ\ldots\circ\mathbf{h}_k^{\alpha_k}\mid\alpha_1,\ldots,\alpha_k\in\mathbf{E}\}$ (где $\circ$ – операция суперпозиции, а $\mathbf{h}_i^{\alpha_i}$ $(\alpha_i\in\mathbf{E})$ определено следующим образом: $\mathbf{h}_i^1=\mathbf{h}_i$, а $\mathbf{h}_i^0$ - тождественная перестановка), что для фиксированных чисел $k,n\in\mathbf{N}$ $(1<k<\lfloor 0{,}5n\rfloor)$ перестановка $\mathbf{h}_i$ $(i=1,\ldots,k)$ определена в терминах фиксированного разбиения $\pi=\{B_1,\ldots,B_k\}$ ($|B_i|\geq 2$ $(i=1,\ldots,k)$) множества $\mathbf{N}_n$. Доказана следующая теорема.

Теорема 5. Для всех чисел $k,n\in\mathbf{N}$ $(1<k<\lfloor 0{,}5n\rfloor)$ и каждого разбиения $\pi=\{B_1,\ldots,B_k\}$ ($|B_i|\geq 2$ $(i=1,\ldots,k)$) множества $\mathbf{N}_n$ элементы каждого семейства $H(\mathbf{h}_1,\ldots,\mathbf{h}_k)\in F_\pi$ являются попарно различными перестановками множества n-битовых векторов.

Из теоремы 5 вытекает, что для всех чисел $k,n\in\mathbf{N}$ $(1<k<\lfloor 0{,}5n\rfloor)$ и каждого разбиения $\pi=\{B_1,\ldots,B_k\}$ ($|B_i|\geq 2$ $(i=1,\ldots,k)$) множества $\mathbf{N}_n$ истинно равенство $|F_\pi|=\prod_{i=1}^{k}(|B_i|-1)!$. Из этого равенства, в свою очередь, вытекает, что:

1) для каждого числа $n=kl$ $(k,l\in\mathbf{N},k\geq 2,l\geq 2)$ и каждого разбиения $\pi=\{B_1,\ldots,B_k\}$ ($|B_i|=l$ $(i=1,\ldots,k)$) множества $\mathbf{N}_n$ истинно равенство $|F_\pi|=((nk^{-1}-1)!)^k$;

2) для каждого числа $n=k^2$ $(k\in\mathbf{N},k\geq 2)$ и каждого разбиения $\pi=\{B_1,\ldots,B_k\}$ (p_i $(i=1,\ldots,k)$) множества $\mathbf{N}_n$ истинно равенство $|F_\pi|=((\sqrt{n}-1)!)^k$.

Пусть $T_\pi=\{\tilde{H}(\mathbf{h}_1,\ldots,\mathbf{h}_k)\mid\mathbf{h}_i\in S(B_i)\ (i=1,\ldots,k)\}$, где $S(U)$ – симметрическая группа на множестве U, а $\tilde{H}(\mathbf{h}_1,\ldots,\mathbf{h}_k)=\{\mathbf{h}_1\}\cup\{\mathbf{h}_2^{\alpha_2}\circ\ldots\circ\mathbf{h}_k^{\alpha_k}\mid\alpha_2,\ldots,\alpha_k\in\mathbf{E},\ \sum_{i=2}^{k}\alpha_i\geq 1\}$. Обозначим через $S_{fxd}(\tilde{H}(\mathbf{h}_1,\ldots,\mathbf{h}_k))$ множество всех неподвижных точек перестановок, принадлежащих семейству $\tilde{H}(\mathbf{h}_1,\ldots,\mathbf{h}_k)$. Доказана следующая теорема.

Теорема 6. Если $n=\sum_{i=1}^{k}p_i$, где p_i $(i=1,\ldots,k)$ – простые числа, а $\pi=\{B_1,\ldots,B_k\}$ – такое разбиение множества $\mathbf{N}_n$, что $|B_i|=p_i$ $(i=1,\ldots,k)$, то для каждого семейства перестановок $\tilde{H}(\mathbf{h}_1,\ldots,\mathbf{h}_k)\in T_\pi$ истинно равенство $|S_{fxd}(\tilde{H}(\mathbf{h}_1,\ldots,\mathbf{h}_k))|=|\mathbf{E}^n|(1-\prod_{i=1}^{k}(1-2^{1-p_i}))$.

Следствие 1. Пусть $n=\sum_{i=1}^{k}p_i$, где p_i $(i=1,\ldots,k)$ – простые числа, а $\pi=\{B_1,\ldots,B_k\}$ – такое разбиение множества $\mathbf{N}_n$, что $|B_i|=p_i$ $(i=1,\ldots,k)$. Если $p_i\to\infty$ для всех $i\in\mathbf{N}_k$, то для каждого семейства $\tilde{H}(\mathbf{h}_1,\ldots,\mathbf{h}_k)\in T_\pi$ почти все векторы $\mathbf{x}\in\mathbf{E}^n$ не являются неподвижными точками.

В [14] исследован класс семейств легко вычислимых подстановок, определенных системой уравнений над кольцом вычетов $Z_{p^k}=(\mathbf{Z}_{p^k},\oplus,\circ)$, где p – простое число, а $k\in\mathbf{N}$. Такие семейства подстановок, управляемые изображением псевдофрактала, могут быть использованы в поточном шифре для преобразования информационных последовательностей. Основные результаты состоят в следующем.

Рассмотрим такие семейства подстановок $F^{(i)}=\{f_n^{(i)}:\mathbf{Z}_{p^k}\to\mathbf{Z}_{p^k}\mid n\in\mathbf{N}\}$ $(i\in\mathbf{N}_l)$, что $f_n^{(i)}(x)=\beta_i^n\circ x\oplus(n\ (\mathrm{mod}\ p^k))\circ A_i(n)$ $(x\in\mathbf{Z}_{p^k},n\in\mathbf{N})$, а $A_i(n)=\bigoplus_{j=1}^{l}a_j\circ\alpha_j^n\ominus 2\circ a_i\circ\alpha_i^n$ $(i\in\mathbf{N}_l;\ n\in\mathbf{N};\ \alpha_j,\beta_j,a_j\in\mathbf{Z}_{p^k}^{inv}\ (j\in\mathbf{N}_l))$. Доказаны следующие утверждения.

Утверждение 1. Если $\alpha_1=\ldots=\alpha_l=\alpha$ и $a_1=\ldots=a_l=a$, где $\alpha,a\in\mathbf{Z}_{p^k}^{inv}$, то:

1) $f_n^{(i)}=f_n^{(j)}$ $(i,j\in\mathbf{N}_l)$ тогда и только тогда, когда $\beta_i^n=\beta_j^n$;

2) для каждого $n\in\mathbf{N}$ множество неподвижных точек подстановки $f_n^{(i)}\in F^{(i)}$ $(i\in\mathbf{N}_l)$ совпадает с множеством решений уравнения $(1\ominus\beta_i^n)\circ x=(n\ (\mathrm{mod}\ p^k))\circ(l-2)\circ a\circ\alpha^n$.

Следствие 2. Пусть $\alpha_1=\ldots=\alpha_l=\alpha$ и $a_1=\ldots=a_l=a$, где $\alpha,a\in\mathbf{Z}_{p^k}^{inv}$, $1\ominus\beta_i^n\neq 0$, $n\ (\mathrm{mod}\ p^k)\neq 0$ и r_1,r_2 – такие максимальные натуральные числа, что $1\ominus\beta_i^n\equiv 0\ (\mathrm{mod}\ p^{r_1})$ и $(n\ (\mathrm{mod}\ p^k))\circ(l-2)\equiv 0\ (\mathrm{mod}\ p^{r_2})$. Если $r_1>r_2$, то подстановка $f_n^{(i)}\in F^{(i)}$ $(i\in\mathbf{N}_l)$ не имеет неподвижных точек.

Утверждение 2. Если $\alpha_1=\ldots=\alpha_l=\alpha$, то подстановка $f_{\phi(p^k)}^{(i)}\in F^{(i)}$ $(i\in\mathbf{N}_l)$ (где ϕ – функция Эйлера) имеет неподвижные точки тогда и только тогда, когда $l-2\equiv 0\ (\mathrm{mod}\ p)$.

Рассмотрим такое множество $\boldsymbol{K}$ семейств подстановок $\mathbf{F}(\mathbf{u},\mathbf{v},\mathbf{a},h)=\{\mathbf{f}_n\mid n\in\mathbf{N}\}$, предназначенное для преобразования информационных векторов фиксированной длины l, что $h\in S(\mathbf{N}_l)$, $\mathbf{u}=(\alpha_1,\ldots,\alpha_l)\in(\mathbf{Z}_{p^k}^{inv})^l$,

$\mathbf{v}=(\beta_1,\ldots,\beta_l)\in(\mathbf{Z}_{p^k}^{inv})^l$, $\mathbf{a}=(a_1,\ldots,a_l)\in(\mathbf{Z}_{p^k}^{inv})^l$, а отображения $\mathbf{f}_n:(\mathbf{Z}_{p^k})^l\to(\mathbf{Z}_{p^k})^l$ определены равенством $\mathbf{f}_n(\mathbf{x})=(f_n^{(1)}(x_{h^n(1)}),\ldots,f_n^{(l)}(x_{h^n(l)}))^{\mathrm{T}}$ $(\mathbf{x}=(x_1,\ldots,x_l)\in(\mathbf{Z}_{p^k})^l)$, где $f_n^{(i)}\in F^{(i)}$ $(i\in\mathbf{N}_l)$. Доказаны следующие теоремы.

Теорема 7. Пусть p – нечетное простое число. Тогда для всех $\mathbf{F}(\mathbf{u},\mathbf{v},\mathbf{a},h)\in\boldsymbol{K}$ поиск семейства $\mathbf{F}_{n_0,n_1}(\mathbf{u},\mathbf{v},\mathbf{a},h)=\{\mathbf{f}_n\}_{n\in\mathbf{N}_{n_1}\setminus\mathbf{N}_{n_0}}$ $(n_0,n_1\in\mathbf{N};\ n_1>n_0)$, обладающего заданной неподвижной точкой $\mathbf{x}_0\in(\mathbf{Z}_{p^k})^l$, при условии, что n_0 и n_1 не являются показателями (по модулю p^k) ни одного из чисел $\alpha_i,\beta_i\in\mathbf{Z}_{p^k}^{inv}$ $(i\in\mathbf{N}_l)$, сводится к решению системы многостепенных диофантовых уравнений с $2l$ неизвестными с последующей проверкой для каждого ее решения разрешимости $2l$ задач дискретного логарифмирования.

Теорема 8. Пусть $p=2$, $\beta_i=1$ $(i\in\mathbf{N}_l)$, l – нечетное число и $k\geq 3$. Тогда для любого семейства подстановок $\mathbf{F}(\mathbf{u},\mathbf{v},\mathbf{a},e)\in\boldsymbol{K}$ (где $e\in S(\mathbf{N}_l)$ – тождественная подстановка) ни одно семейство подстановок $\mathbf{F}_{n_0,n_1}(\mathbf{u},\mathbf{v},\mathbf{a},e)$ $(1\leq n_0<n_1<2^k)$ не имеет неподвижных точек.

Теорема 9. Пусть известны значения векторов параметров $\mathbf{a}$ и $\mathbf{u}$. Если в момент $n_0\in\mathbf{N}$ экспериментатор может управлять алгоритмом, реализующим подстановку $\mathbf{f}_{n_0}$, и наблюдать соответствующий выход, то идентификация вектора параметров $\mathbf{v}$ сводится к независимому решению l задач дискретного логарифмирования.

Теорема 10. Пусть p – нечетное простое число и известны значения векторов параметров $\mathbf{a}$ и $\mathbf{v}$. Если в момент $n_0\in\mathbf{N}$, где $(n_0 \pmod{p^k})\in\mathbf{Z}_{p^k}^{inv}$, экспериментатор может наблюдать вход и соответствующий выход алгоритма, реализующего подстановку $\mathbf{f}_{n_0}$, то идентификация вектора параметров $\mathbf{u}$ сводится к независимому решению l задач дискретного логарифмирования.

2. Автоматы над конечными кольцами. Исследования поточных шифров, построенных на аддитивном внесении информационной переменной в хаотическую динамическую систему, показывают, что возникают ошибки из-за погрешностей округления. Для того чтобы нивелировать эти ошибки естественно перейти к вычислениям в конечной алгебраической системе. В качестве такой алгебраической системы целесообразно выбрать конечное кольцо, так как при наличии делителей нуля в кольце существенно возрастает сложность действий криптоаналитика в процессе его атаки на соответствующий шифр. Исходя из этого, были исследованы над кольцом Z_{p^k} (p – простое число, $k\in\mathbf{N}$) автоматы, построенные как аналоги хаотических динамических систем Эно [15], Спротта [16], Лоренца [17], free-running system и Guckenheimer and Holmes cycle [18]. Развитые при этом методы послужили основой для системного анализа над кольцом Z_{p^k} множества линейных автоматов [11,19,20], и множества нелинейных автоматов, определенных системами уравнений 2-й степени от состояния автомата [11]. В [21] эти результаты были следующим образом обобщены для автоматов над произвольным конечным ассоциативно-коммутативным кольцом $K=(K,+,\cdot)$ с единицей.

Пусть $A_{n,1}$ – множество автоматов Мили M_1, а $A_{n,2}$ – множество автоматов Мура M_2, определенных, соответственно, системами уравнений

$$M_1:\begin{cases}\mathbf{q}_{t+1}=\mathbf{f}_1(\mathbf{q}_t)+\mathbf{f}_3(\mathbf{x}_{t+1})\\ \mathbf{y}_{t+1}=\mathbf{f}_2(\mathbf{q}_t)+\mathbf{f}_4(\mathbf{x}_{t+1})\end{cases}\quad(t\in\mathbf{Z}_+),$$

$$M_2:\begin{cases}\mathbf{q}_{t+1}=\mathbf{f}_1(\mathbf{q}_t)+\mathbf{f}_3(\mathbf{x}_{t+1})\\ \mathbf{y}_{t+1}=\mathbf{f}_2(\mathbf{q}_{t+1})\end{cases}\quad(t\in\mathbf{Z}_+),$$

где $\mathbf{f}_i:K^n\to K^n$ $(i=1,\ldots,4)$, а $\mathbf{q}_t,\mathbf{x}_t,\mathbf{y}_t\in K^n$ – соответственно, состояние автомата, входной и выходной символ в момент $t\in\mathbf{Z}_+$. Следующим образом охарактеризованы подмножества $A_{n,1}^{inv}$ и $A_{n,2}^{inv}$ обратимых автоматов.

Теорема 11. Равенство $A_{n,1}^{inv}=\{M_1\in A_{n,1}\mid\mathbf{f}_4:K^n\to K^n$ – áèåêòèâ$\}$ истинно для любых отображений $\mathbf{f}_i:K^n\to K^n$ $(i=1,2,3)$.

Теорема 12. Равенство $A_{n,2}^{inv}=\{M_2\in A_{n,2}\mid\mathbf{f}_2:K^n\to K^n,\mathbf{f}_3:K^n\to K^n-$ áèåêòèâ$\}$ истинно для любого отображения $\mathbf{f}_1:K^n\to K^n$.

Из этих теорем вытекает, что истинны следующие три следствия.

Следствие 3. Для любого поточного шифра $((M,\mathbf{q}_0),(M^{-1},\mathbf{q}_0))$ $(M\in A_{n,1}^{inv}\cup A_{n,2}^{inv})$ в процессе "шифрование-расшифрование" автоматы M и M^{-1} движутся в пространстве состояний по одной и той же траектории в одном и том же направлении.

Следствие 4. Для любого автомата $M_1\in A_{n,1}^{inv}$ функции переходов и выходов автомата M_1^{-1} разделимы по переменным $\mathbf{q}$ и $\mathbf{x}$ тогда и только тогда, когда по этим переменным разделимы отображения $\mathbf{g}_1(\mathbf{q},\mathbf{x})=\mathbf{f}_3(\mathbf{f}_4^{-1}(\mathbf{x}-\mathbf{f}_2(\mathbf{q})))$ и $\mathbf{g}_2(\mathbf{q},\mathbf{x})=\mathbf{f}_4^{-1}(\mathbf{x}-\mathbf{f}_2(\mathbf{q}))$.

Следствие 5. Для любого автомата $M_2\in A_{n,2}^{inv}$ функции переходов и выходов автомата M_2^{-1} разделимы по переменным $\mathbf{q}$ и $\mathbf{x}$ тогда и только тогда, когда по этим переменным разделимо отображение $\mathbf{g}_3(\mathbf{q},\mathbf{x})=\mathbf{f}_3^{-1}(\mathbf{f}_2^{-1}(\mathbf{x})-\mathbf{f}_1(\mathbf{q}))$.

Построена общая схема анализа конечно-автоматных характеристик исследуемых моделей. В рамках этой схемы охарактеризованы качественные и количественные характеристики основных нетривиальных подмножеств исследуемых автоматов. В частности доказаны следующие утверждения.

Утверждение 3. Автомат $M \in A_{n,1} \cup A_{n,2}$ – сильно-связный автомат с диаметром графа переходов равным 1 тогда и только тогда, когда $\mathbf{f}_3 : K^n \to K^n$ биекция.

Следствие 6. Автомат $M \in A_{n,1} \cup A_{n,2}$ – перестановочный автомат тогда и только тогда, когда $\mathbf{f}_3 : K^n \to K^n$ – биекция.

Следствие 7. Если отображение $\mathbf{f}_3 : K^n \to K^n$ не является биекцией, то диаметр графа переходов автомата $M \in A_{n,1} \cup A_{n,2}$ больше, чем 1.

Утверждение 4. Если $\mathbf{f}_2 : K^n \to K^n$ - биекция, то $M \in A_{n,1}$ – приведенный автомат, любые два состояния которого различимы любым входным символом.

Утверждение 5. Если $\mathbf{f}_1 : K^n \to K^n$ и $\mathbf{f}_2 : K^n \to K^n$ – биекции, то $M \in A_{n,2}$ – приведенный автомат, любые два состояния которого различимы любым входным символом.

Утверждение 6. Состояния $\mathbf{q}, \tilde{\mathbf{q}} \in K^n$ $(\mathbf{q} \neq \tilde{\mathbf{q}})$ автомата $M \in A_{n,1} \cup A_{n,2}$ являются близнецами тогда и только тогда, когда они принадлежат одному и тому же классу разбиения K^n / ε, где $\varepsilon = \ker \mathbf{f}_1 \cap \ker \mathbf{f}_2$, если $M \in A_{n,1}$ и $\varepsilon = \ker \mathbf{f}_1$, если $M \in A_{n,2}$.

На основании этих и аналогичных утверждений оценены мощности подмножеств обратимых автоматов, сильно связных автоматов, перестановочных и приведенных автоматов, а также автоматов, имеющих состояния-близнецы. Кроме того, оценены вероятности того, что при равномерном распределении параметров случайно выбранный автомат принадлежит указанным подмножествам.

Пусть $\tilde{A}_{n,1}$ и $\tilde{A}_{n,2}$ – подмножества множеств $A_{n,1}$ и $A_{n,2}$, состоящие из автоматов, имеющих, соответственно, вид

$$M_1 : \begin{cases} \mathbf{q}_{t+1} = A\mathbf{q}_t\mathbf{q}_t^{\mathrm{T}}\mathbf{b} + C\mathbf{q}_t + \mathbf{d} + E\mathbf{x}_{t+1} \\ \mathbf{y}_{t+1} = G\mathbf{q}_{t+1} + F\mathbf{x}_{t+1} \end{cases} \quad (t \in \mathbf{Z}_+),$$

$$M_2 : \begin{cases} \mathbf{q}_{t+1} = A\mathbf{q}_t\mathbf{q}_t^{\mathrm{T}}\mathbf{b} + C\mathbf{q}_t + \mathbf{d} + E\mathbf{x}_{t+1} \\ \mathbf{y}_{t+1} = G\mathbf{q}_{t+1} \end{cases} \quad (t \in \mathbf{Z}_+),$$

где $\mathbf{q}_t = (q_t^{(1)}, \ldots, q_t^{(n)})^{\mathrm{T}}$, $\mathbf{x}_t = (x_t^{(1)}, \ldots, x_t^{(n)})^{\mathrm{T}}$ и $\mathbf{y}_t = (y_t^{(1)}, \ldots, y_t^{(n)})^{\mathrm{T}}$ – соответственно, состояние автомата, входной и выходной символ в момент t, $A, C, E, G, F \in M_n$ – фиксированные матрицы (M_n – множество всех $n \times n$-матриц над кольцом K), а $\mathbf{b} = (b^{(1)}, \ldots, b^{(n)})^{\mathrm{T}} \in K^n$ и $\mathbf{d} = (d^{(1)}, \ldots, d^{(n)})^{\mathrm{T}} \in K^n$ – фиксированные векторы.

В [22,23] для автомата $M \in \tilde{A}_{n,1} \cup \tilde{A}_{n,2}$ решены задачи параметрической идентификации и идентификации начального состояния. Получены следующие результаты.

Доказано, что для любого автомата $M_1 \in \tilde{A}_{n,1}$ идентификация матриц G и F осуществляется достаточно легко. Сложность идентификации вектора $\mathbf{d}$ и матрицы E существенно зависит от того, является ли матрица G обратимой матрицей. При положительном ответе идентификация вектора $\mathbf{d}$ и матрицы E также осуществляется достаточно легко. Однако если матрица G не является обратимой, то приходится осуществлять перебор по множествам решений систем уравнений. Для идентификации матриц A, C и вектора $\mathbf{b}$ приходится формировать и решать системы нелинейных уравнений над кольцом K (известно, что даже над полями Галуа $GF(2^k)$ решение системы уравнений 2-й степени от многих переменных – NP-полная задача). Показано, что, для любого автомата $M_2 \in \tilde{A}_{n,2}$ идентификация вектора $G\mathbf{d}$ и матрицы GE осуществляется достаточно легко. Однако трудной задачей является идентификация матриц GA, GC и вектора $\mathbf{b}$. Отсюда вытекает, что переход к обратимым автоматам не упрощает решение задачи параметрической идентификации для исследуемых моделей. Поэтому при использовании автомата $M \in \tilde{A}_{n,1}^{inv} \cup \tilde{A}_{n,2}^{inv}$ в качестве поточного шифра (в этом случае параметры играют роль долговременного секретного ключа) особое внимание следует уделить обеспечению секретности параметров A, C и $\mathbf{b}$. Показано, что идентификация начального состояния автомата $M_1 \in \tilde{A}_{n,1}$ (при условии, что $G \in M_n^{non-inv}$) и идентификация начального состояния автомата $M_2 \in \tilde{A}_{n,2}$ сводится к решению системы нелинейных уравнений над кольцом K. Отсюда вытекает, что переход к обратимым автоматам не упрощает решение задачи идентификация начального состояния исследуемых моделей. Это обосновывает целесообразность выбора начального состояния автомата $M \in \tilde{A}_{n,1}^{inv} \cup \tilde{A}_{n,2}^{inv}$ в качестве секретного сеансового ключа соответствующего поточного шифра.

В [24,25] следующим образом решена задача построения имитационной модели для семейства автоматов $M_{\mathbf{A}} = \{M_{\mathbf{a}}\}_{\mathbf{a} \in \mathbf{A}}$ $(\varnothing \neq \mathbf{A} \subseteq K^l)$, заданного над конечным кольцом $K = (K, +, \cdot)$ системой рекуррентных соотношений с параметрами

$$M_{\mathbf{a}} : \begin{cases} \mathbf{q}_{t+1} = \mathbf{f}_1(\mathbf{q}_t, \mathbf{x}_{t+1}, \mathbf{a}) \\ \mathbf{y}_{t+1} = \mathbf{f}_1(\mathbf{q}_t, \mathbf{x}_{t+1}, \mathbf{a}) \end{cases} \quad (t \in \mathbf{Z}_+),$$

где $\mathbf{f}_1 : K^{n_1} \times K^{n_2} \times \mathbf{A} \to K^{n_1}$ и $\mathbf{f}_2 : K^{n_1} \times K^{n_2} \times \mathbf{A} \to K^{n_3}$, либо

$$M_{\mathbf{a}} : \begin{cases} \mathbf{q}_{t+1} = \mathbf{f}_1(\mathbf{q}_t, \mathbf{x}_{t+1}, \mathbf{a}) \\ \mathbf{y}_{t+1} = \mathbf{f}_1(\mathbf{q}_{t+1}, \mathbf{a}) \end{cases} \quad (t \in \mathbf{Z}_+),$$

где $\mathbf{f}_1 : K^{n_1} \times K^{n_2} \times \mathbf{A} \to K^{n_1}$ и $\mathbf{f}_2 : K^{n_1} \times \mathbf{A} \to K^{n_3}$. Зафиксируем числа $r, l_1 \in \mathbf{N}$, множество $\mathbf{B}$ $(\varnothing \neq \mathbf{B} \subseteq K^{l_1})$ и семейства $\{\phi_{\mathbf{b}}^{(1)} : K^{n_1} \times K^{n_2} \to K^{n_3}\}_{\mathbf{b}\in\mathbf{B}}$, $\{\phi_{\mathbf{b}}^{(2)} : K^{n_1} \times \bigcup_{j=1}^{r-1} (K^{n_3})^j \times K^{n_2} \to K^{n_3}\}_{\mathbf{b}\in\mathbf{B}}$ и $\{\phi_{\mathbf{b}}^{(3)} : K^{n_1} \times (K^{n_3})^r \times K^{n_2} \to K^{n_3}\}_{\mathbf{b}\in\mathbf{B}}$. Пусть $G_{\mathbf{B}} = \{G_{\mathbf{b}} : K^{n_1} \times (K^{n_2})^+ \to (K^{n_3})^+\}_{\mathbf{b}\in\mathbf{B}}$ – такое семейство, что $G_{\mathbf{b}}(\mathbf{q}_0, \mathbf{x}_1 \dots \mathbf{x}_m) = \mathbf{y}_1 \dots \mathbf{y}_m$ $(\mathbf{b} \in \mathbf{B}, m \in \mathbf{N})$, где

$$\mathbf{y}_i = \begin{cases} \phi_{\mathbf{b}}^{(1)}(\mathbf{q}_0, \mathbf{x}_1), \text{ åñëè } i = 1 \\ \phi_{\mathbf{b}}^{(2)}(\mathbf{q}_0, \mathbf{y}_1 \dots \mathbf{y}_{i-1}, \mathbf{x}_i), \text{ åñëè } i = 2, \dots, r \\ \phi_{\mathbf{b}}^{(3)}(\mathbf{q}_0, \mathbf{y}_{i-r} \dots \mathbf{y}_{i-1}, \mathbf{x}_i), \text{ åñëè } r < i \le m \end{cases}.$$

Определим отображение $H_{\mathbf{b},\mathbf{q}_0} : (K^{n_2})^+ \to (K^{n_3})^+$ $(\mathbf{b} \in \mathbf{B}, \mathbf{q}_0 \in K^{n_1})$ равенством $H_{\mathbf{b},\mathbf{q}_0}(\mathbf{x}_1 \dots \mathbf{x}_m) = G_{\mathbf{b}}(\mathbf{q}_0, \mathbf{x}_1 \dots \mathbf{x}_m)$ $(\mathbf{b} \in \mathbf{B}, \mathbf{q}_0 \in K^{n_1})$ и зафиксируем такую сюръекцию $h : \mathbf{B} \to \mathbf{A}$, что $H_{h(\mathbf{a}),\mathbf{q}_0}|_{\bigcup_{i=1}^{r}(K^{n_2})^i} = F_{\mathbf{a},\mathbf{q}_0}|_{\bigcup_{i=1}^{r}(K^{n_2})^i}$ $(\mathbf{a} \in \mathbf{A}, \mathbf{q}_0 \in K^{n_1})$, где $F_{\mathbf{a},\mathbf{q}_0}$ – о.-д.- функция, реализуемая инициальным автоматом $(M_{\mathbf{a}}, \mathbf{q}_0)$.

Упорядоченную пару $(G_{\mathbf{B}}, h)$ назовем имитационной моделью семейства автоматов $M_{\mathbf{A}} = \{M_{\mathbf{a}}\}_{\mathbf{a}\in\mathbf{A}}$. На основе стандартного подхода теории алгоритмов формально определено понятие ν -точная $(\nu \in \{\nu_1, \dots, \nu_4\})$ имитационная модель $(G_{\mathbf{B}}, h)$, где числа $\nu_1, \dots, \nu_4 \in [0,1]$ охватывают все комбинации понятий "в наихудшем случае" и "в среднем". ν -точная имитационная модель определяется как асимптотически точная, если $\nu = 1$. Доказана следующая теорема ($\gamma_{\mathbf{a},\mathbf{q}_0,m}$ – среднее количество букв в выходных словах, приходящихся на одну букву входного слова, на которых отображения $F_{\mathbf{a},\mathbf{q}_0}$ и $H_{h(\mathbf{a}),\mathbf{q}_0}$ совпадают на множестве всех входных слов длины, не превосходящей число m).

Теорема 13. Пусть $(G_{\mathbf{B}}, h)$ – такая имитационная модель семейства автоматов $M_{\mathbf{A}} = \{M_{\mathbf{a}}\}_{\mathbf{a}\in\mathbf{A}}$ $(\mathbf{A} \subseteq K^l, |\mathbf{A}| \ge 1)$ над кольцом K, что: 1) существует предел $\gamma_{\mathbf{a},\mathbf{q}_0} = \lim_{m\to\infty} \gamma_{\mathbf{a},\mathbf{q}_0,m}$; 2) существует такое число $r_0 \in \mathbf{N}$ $(r_0 \ge r)$, что при всех $\mathbf{q}_0 \in K^{n_1}$, $\mathbf{a} \in \mathbf{A}$ и $\mathbf{x}_1 \dots \mathbf{x}_m \in (K^{n_2})^m$ $(m > r_0)$ для выходных слов $F_{\mathbf{a},\mathbf{q}_0}(\mathbf{x}_1 \dots \mathbf{x}_m) = \mathbf{y}_1 \dots \mathbf{y}_m$ и $H_{h(\mathbf{a}),\mathbf{q}_0}(\mathbf{x}_1 \dots \mathbf{x}_m) = \tilde{\mathbf{y}}_1 \dots \tilde{\mathbf{y}}_m$ равенства $\mathbf{y}_i = \tilde{\mathbf{y}}_i$ имеют место для всех $i = r_0 + 1, \dots, m$. Тогда $\nu_1 = \nu_2 = \nu_3 = \nu_4 = 1$, т.е. $(G_{\mathbf{B}}, h)$ - асимптотически точная имитационная модель семейства автоматов $M_{\mathbf{A}} = \{M_{\mathbf{a}}\}_{\mathbf{a}\in\mathbf{A}}$ для всех $\nu \in \{\nu_1, \dots, \nu_4\}$.

В [25,26] исследуется задача использования в качестве семейства хеш-функций семейства автоматов без выхода, заданного системой рекуррентных соотношений с параметрами над конечным кольцом $K = (K, +, \cdot)$. Получены следующие результаты.

Пусть $F_{k,m}$ $(k, m \in \mathbf{N}, k \le m)$ – множество всех таких отображений $\mathbf{f} : K^k \times K^m \to K^k$, что $|\{\mathbf{x} \in K^m \mid \mathbf{f}(\mathbf{q}, \mathbf{x}) = \mathbf{q}'\}| = |K|^{m-k}$ $(\mathbf{q}, \mathbf{q}' \in K^k)$ и $\{\mathbf{x} \in K^m \mid \mathbf{f}(\mathbf{q}, \mathbf{x}) = \mathbf{q}''\} \cap \{\mathbf{x} \in K^m \mid \mathbf{f}(\mathbf{q}', \mathbf{x}) = \mathbf{q}''\} = \varnothing$ $(\mathbf{q}, \mathbf{q}', \mathbf{q}'' \in K^k; \mathbf{q} \neq \mathbf{q}')$. Рассмотрим семейство $M_{F_{k,m}} = \{M_{\mathbf{f}}\}_{\mathbf{f}\in F_{k,m}}$ сильно связных автоматов без выхода $M_{\mathbf{f}} : \mathbf{q}_{t+1} = \mathbf{f}(\mathbf{q}_t, \mathbf{x}_{t+1})$ $(t \in \mathbf{Z}_+)$. Каждый автомат $M_{\mathbf{f}}$ определяет семейство хэш-функций $H_{\mathbf{f}} = \{H_{\mathbf{f},\mathbf{q}_0}\}_{\mathbf{q}_0\in K^k}$, где $H_{\mathbf{f},\mathbf{q}_0}(\mathbf{x}_1 \dots \mathbf{x}_t) = \mathbf{f}(\mathbf{q}_0, \mathbf{x}_1 \dots \mathbf{x}_t)$. Доказаны следующие теоремы.

Теорема 14. Для каждого отображения $\mathbf{f} \in F_{k,m}$ при любых таких состояниях $\mathbf{q}_0, \mathbf{q}_0' \in K^k$ автомата $M_{\mathbf{f}} \in M_{F_{k,m}}$, что $\mathbf{q}_0 \neq \mathbf{q}_0'$ неравенство $H_{\mathbf{f},\mathbf{q}_0}(\mathbf{u}) \neq H_{\mathbf{f},\mathbf{q}_0'}(\mathbf{u})$ истинно для каждого входного слова $\mathbf{u} \in (K^m)^+$.

Следствие 8. Для каждого отображения $\mathbf{f} \in F_{k,m}$, если $\mathbf{q}_0 \neq \mathbf{q}_0'$ $(\mathbf{q}_0, \mathbf{q}_0' \in K^k)$, то $H_{\mathbf{f},\mathbf{q}_0}^{-1}(\mathbf{q}) \cap H_{\mathbf{f},\mathbf{q}_0'}^{-1}(\mathbf{q}) = \varnothing$ для любого состояния $\mathbf{q} \in K^k$ автомата $M_{\mathbf{f}} \in M_{F_{k,m}}$.

Теорема 15. Для каждого отображения $\mathbf{f} \in F_{k,m}$ и каждого начального состояния $\mathbf{q}_0 \in K^k$ автомата $M_{\mathbf{f}} \in M_{F_{k,m}}$ равенство $|H_{\mathbf{f},\mathbf{q}_0}^{-1}(\mathbf{q}_t) \cap (K^m)^t| = |K|^{tm-k}$ $(\mathbf{q}_t \in K^k)$ истинно для всех чисел $t \in \mathbf{N}$.

Пусть $P_{\mathbf{f},\mathbf{q}_0,t}^{(1)}(\mathbf{q})$ $(\mathbf{f} \in F_{k,m}; \mathbf{q}_0, \mathbf{q} \in K^k, t \in \mathbf{N})$ – вероятность того, что случайно выбранное из множества $(K^m)^t$ входное слово $\mathbf{u}$ является решением уравнения $H_{\mathbf{f},\mathbf{q}_0}(\mathbf{u}) = \mathbf{q}$, а $P_{\mathbf{f},\mathbf{q}_0,t}^{(2)}$ $(\mathbf{f} \in F_{k,m}; \mathbf{q}_0 \in K^k, t \in \mathbf{N})$ – вероятность того, что для двух различных входных слов $\mathbf{u}$ и $\mathbf{u}'$, случайно выбранных из множества $(K^m)^t$, истинно равенство $H_{\mathbf{f},\mathbf{q}_0}(\mathbf{u}) = H_{\mathbf{f},\mathbf{q}_0}(\mathbf{u}')$. Из теоремы 15 вытекает, что истинны следующие два следствия.

Следствие 9. Для каждого отображения $\mathbf{f} \in F_{k,m}$ при любых состояниях $\mathbf{q}_0, \mathbf{q} \in K^k$ автомата $M_{\mathbf{f}} \in M_{F_{k,m}}$ равенство $|P_{\mathbf{f},\mathbf{q}_0,t}^{(1)}(\mathbf{q})| = |K|^{-k}$ истинно для всех $t \in \mathbf{N}$.

Следствие 10. Для каждого отображения $\mathbf{f} \in F_{k,m}$ и каждого начального состояния $\mathbf{q}_0 \in K^k$ автомата $M_{\mathbf{f}} \in M_{F_{k,m}}$ равенство $P_{\mathbf{f},\mathbf{q}_0,t}^{(2)} = |K|^{-k}\left(1 - \frac{|K|^k - 1}{|K|^{mt} - 1}\right)$ истинно для всех $t \in \mathbf{N}$.

На основе полученных результатов охарактеризована сложность решения задач идентификации для семейства хэш-функций $H_{\mathbf{f}} = \{H_{\mathbf{f},\mathbf{q}_0}\}_{\mathbf{q}_0\in K^k}$.

3. Автоматы на многообразиях над конечными кольцами. Успешное применение эллиптических кривых при решении задач защиты информации [27,28] обосновывают актуальность исследования автоматов, определенных на многообразиях (так как эллиптическая кривая, как и любая алгебраическая кривая, представляет собой специальный случай многообразия). Исследованию семейств автоматов, определенных на многообразиях над конечными кольцами, посвящены работы [25,29–34]. Основные результаты состоят в следующем.

Выделены следующие 2 множества многообразий над кольцом $K=(K,+,\cdot)$:

1) множество $V_{1,n}(K)$ $(n\in\mathbf{N})$ всех таких многообразий $\mathbf{V}\subseteq K^n$, что задана алгебра $A_{\mathbf{V}}=(\mathbf{V},F_{1,\mathbf{V}},F_{2,\mathbf{V}})$, где $F_{1,\mathbf{V}}=\{\alpha_0,\alpha_1,\ldots,\alpha_{k_1}\}$ $(k_1\in\mathbf{Z}_+)$ и $F_{2,\mathbf{V}}=\{\beta_1,\ldots,\beta_{k_2}\}$ $(k_2\in\mathbf{N})$ есть множество, соответственно, унарных и бинарных операций, определенных на множестве $\mathbf{V}$;

2) множество $V_{2,n}(K)$ $(n\in\mathbf{N})$ всех многообразий $\mathbf{V}\subseteq K^n$ $(n\in\mathbf{N})$, для которых существует параметризация $\mathbf{v}=\mathbf{h}(\mathbf{t})$, где $\mathbf{t}\in K^m$ $(m<n)$, а $\mathbf{h}$ – набор из n многочленов от m переменных, а также задано семейство отображений $\Theta=\{\theta_i\}_{i\in\mathbf{N}_k}$, где $\theta_i:K^m\to K^m$ $(i\in\mathbf{N}_k)$ (отображение θ_i $(i\in\mathbf{N}_k)$ и параметризация $\mathbf{v}=\mathbf{h}(\mathbf{t})$ определяют на многообразии $\mathbf{V}\in V_{2,n}(K)$ множество траекторий $\mathbf{h}(\mathbf{t}),\mathbf{h}(\theta_i(\mathbf{t})),\mathbf{h}(\theta_i^2(\mathbf{t})),\ldots$ $(\mathbf{t}\in K^m)$).

Многообразие $\mathbf{V}_2\in V_{1,n_2}(K_2)$ назовем гомоморфным образом многообразия $\mathbf{V}_1\in V_{1,n_1}(K_1)$, если алгебра $A_{\mathbf{V}_2}$ – гомоморфный образ алгебры $A_{\mathbf{V}_1}$ (соответственно, многообразия $\mathbf{V}_1\in V_{1,n_1}(K_1)$ и $\mathbf{V}_2\in V_{1,n_2}(K_2)$ изоморфны, если алгебры $A_{\mathbf{V}_1}$ и $A_{\mathbf{V}_2}$ изоморфны). Если $\mathbf{V}_j\in V_{2,n_j}(K_j)$ $(j=1,2)$ и существует такая пара сюръекций $\phi_1:\mathbf{V}_1\to\mathbf{V}_2$ и $\phi_2:K^{m_1}\to K^{m_2}$, что равенства $\phi_1(\mathbf{h}_1(\mathbf{t}))=\mathbf{h}_2(\phi_2(\mathbf{t}))$ и $\phi_2(\theta_i^{(1)}(\mathbf{t}))=\theta_i^{(2)}(\phi_2(\mathbf{t}))$ истинны для всех $\mathbf{t}\in K^{m_1}$ и $i\in\mathbf{N}_k$, то будем говорить, что: 1) упорядоченная пара $(\mathbf{V}_2,\Theta_2)$ – гомоморфный образ упорядоченной пары $(\mathbf{V}_1,\Theta_1)$; 2) упорядоченные пары $(\mathbf{V}_1,\Theta_1)$ и $(\mathbf{V}_2,\Theta_2)$ изоморфны, если ϕ_1 и ϕ_2 – биекции.

Упорядоченная пара $(\mathbf{V},A_{\mathbf{V}})$ (где $\mathbf{V}\in V_{1,n}(K)$ и $A_{\mathbf{V}}=(\mathbf{V},F_{1,\mathbf{V}},F_{2,\mathbf{V}})$) дает возможность определить семейство $M^{(1)}(\mathbf{V},A_{\mathbf{V}})$ автоматов Мили

$$\begin{cases}\mathbf{q}_{t+1}=\beta_{j_1}(\alpha_{i_1}(\mathbf{q}_t),\alpha_{x_{t+1}}(\mathbf{v}_1))\\ \mathbf{y}_{t+1}=\beta_{j_2}(\alpha_{i_2}(\mathbf{q}_t),\alpha_{x_{t+1}}(\mathbf{v}_2))\end{cases}\quad(t\in\mathbf{Z}_+)$$

и семейство $M^{(2)}(\mathbf{V},A_{\mathbf{V}})$ автоматов Мура

$$\begin{cases}\mathbf{q}_{t+1}=\beta_{j_1}(\alpha_{i_1}(\mathbf{q}_t),\alpha_{x_{t+1}}(\mathbf{v}_1))\\ \mathbf{y}_{t+1}=\beta_{j_2}(\alpha_{i_2}(\mathbf{q}_{t+1}),\mathbf{v}_2)\end{cases}\quad(t\in\mathbf{Z}_+).$$

Охарактеризованы основные нетривиальные с позиции теории автоматов подсемейства исследуемых моделей (семейство групповых автоматов, семейство автоматов с состояниями-источниками, семейство автоматов с состояниями-стоками, семейство явно-приведенных автоматов). Доказана следующая теорема о гомоморфизмах.

Теорема 16. Если упорядоченная пара $(\mathbf{V}_2,A_{\mathbf{V}_2})$ $(\mathbf{V}_2\in V_{1,n_2}(K_2))$ - гомоморфный образ упорядоченной пары $(\mathbf{V}_1,A_{\mathbf{V}_1})$ $(\mathbf{V}_1\in V_{1,n_1}(K_1))$, то существуют такие отображения

$$\Psi_r:M^{(r)}(\mathbf{V}_1,A_{\mathbf{V}_1})\to M^{(r)}(\mathbf{V}_2,A_{\mathbf{V}_2})\quad(r=1,2),$$

что автомат $\Psi_r(M_r)$ $(M_r\in M^{(r)}(\mathbf{V}_1,A_{\mathbf{V}_1}))$ является гомоморфным образом автомата M_r.

Следствие 11. Если упорядоченные пары $(\mathbf{V}_1,A_{\mathbf{V}_1})$ $(\mathbf{V}_1\in V_{1,n_1}(K_1))$ и $(\mathbf{V}_2,A_{\mathbf{V}_2})$ $(\mathbf{V}_2\in V_{1,n_2}(K_2))$ изоморфны, то существуют такие отображения

$$\Psi_r:M^{(r)}(\mathbf{V}_1,A_{\mathbf{V}_1})\to M^{(r)}(\mathbf{V}_2,A_{\mathbf{V}_2})\quad(r=1,2),$$

что автоматы $M_r\in M^{(r)}(\mathbf{V}_1,A_{\mathbf{V}_1})$ и $\Psi_r(M_r)$ изоморфны.

Упорядоченная пара $(\mathbf{V},\Theta)$ (где $\mathbf{V}\in V_{2,n}(K)$ и $\Theta=\{\theta_i\}_{i\in\mathbf{N}_k}$) дает возможность определить семейство $M^{(1)}_{n,k,l}(\mathbf{V},\Theta)$ автоматов Мили

$$\begin{cases}\mathbf{q}_{t+1}=\mathbf{h}(\theta_{x_{t+1}}(\mathbf{t}_t))\\ \mathbf{y}_{t+1}=\mathbf{g}_{x_{t+1}}(\mathbf{q}_t)\end{cases}\quad(t\in\mathbf{Z}_+)$$

и семейство $M^{(2)}_{n,k,l}(\mathbf{V},\Theta)$ автоматов Мура

$$\begin{cases}\mathbf{q}_{t+1}=\mathbf{h}(\theta_{x_{t+1}}(\mathbf{t}_t))\\ \mathbf{y}_{t+1}=\mathbf{g}(\mathbf{q}_{t+1})\end{cases}\quad(t\in\mathbf{Z}_+),$$

где $\mathbf{t}_0\in K^m$, $\mathbf{q}_0=\mathbf{h}(\mathbf{t}_0)$, $\mathbf{t}_{t+1}=\theta_{x_{t+1}}(\mathbf{t}_t)$ $(t\in\mathbf{Z}_+)$, $\mathbf{g}_i:K^n\to K^l$ $(i\in\mathbf{N}_k)$, $\mathbf{g}:K^n\to K^l$ и $x_{t+1}\in\mathbf{N}_k$.

Пусть $M^{(r)}_{n,k}(\mathbf{V},\Theta)=\bigcup_{l=1}^{\infty}M^{(r)}_{n,k,l}(\mathbf{V},\Theta)$ $(r=1,2)$, $F_m(K)$ – множество всех отображений $f:K^m\to K^m$, $T_{\mathbf{V},f}$ $(f\in F_m(K))$ – множество всех траекторий $\mathbf{h}(\mathbf{t}_0),\mathbf{h}(\mathbf{t}_1),\ldots\mathbf{h}(\mathbf{t}_j),\ldots$ $(\mathbf{t}_0\in K^m)$, а $F_{m,\mathbf{h}}(K)$ – множество всех отображений $f\in F_m(K)$, удовлетворяющих условию $(\forall\mathbf{t},\mathbf{t}'\in K^m)(\mathbf{t}\equiv\mathbf{t}'(\ker\mathbf{h})\Rightarrow\mathbf{t}\equiv\mathbf{t}'(\ker(\mathbf{h}\circ f)))$. Доказана следующая теорема.

Теорема 17. Пусть $\mathbf{v}=\mathbf{h}(\mathbf{t})$ $(\mathbf{t}\in K^m)$ – параметризация многообразия $\mathbf{V}\in V_{2,n}(K)$, а $f\in F_m(K)$. Любые две различные траектории, принадлежащие множеству $T_{\mathbf{V},f}$, исходят из различных точек многообразия $\mathbf{V}$ тогда и только тогда, когда не существуют такие точки $\mathbf{t}_0^{(1)},\mathbf{t}_0^{(2)}\in K^m$, что $\mathbf{t}_0^{(1)}\equiv\mathbf{t}_0^{(2)}(\ker\mathbf{h})$ и $\mathbf{t}_0^{(1)}\not\equiv\mathbf{t}_0^{(2)}(\ker(\mathbf{h}\circ f))$.

Следствие 12. Пусть $\mathbf{v}=\mathbf{h}(\mathbf{t})$ $(\mathbf{t}\in K^m)$ – параметризация многообразия $\mathbf{V}\in V_{2,n}(K)$. Тогда:

1) семейство $M_{n,k}^{(r)}(\mathbf{V},\Theta)$ $(r=1,2)$ состоит из детерминированных автоматов тогда и только тогда, когда Θ состоит только из элементов, принадлежащих множеству $F_{m,\mathbf{h}}(K)$;

2) семейство $M_{n,k}^{(r)}(\mathbf{V},\Theta)$ $(r=1,2)$ состоит из недетерминированных автоматов тогда и только тогда, когда Θ содержит хотя бы один элемент из множества $F_m(K)\setminus F_{m,\mathbf{h}}(K)$.

В дальнейшем рассматриваются только семейства детерминированных автоматов.

Охарактеризованы основные нетривиальные с позиции теории автоматов подсемейства исследуемых моделей (семейство групповых автоматов, семейство автоматов с состояниями-источниками, семейство автоматов с состояниями-стоками, семейство явно-приведенных автоматов). Доказана следующая теорема о гомоморфизмах.

Теорема 18. Если упорядоченная пара $(\mathbf{V}_2,\Theta_2)$ $(\mathbf{V}_2\in V_{2,n_2}(K_2))$ – гомоморфный образ упорядоченной пары $(\mathbf{V}_1,A_{\mathbf{V}_1})$ $(\mathbf{V}_1\in V_{2,n_1}(K_1))$, то существуют такие отображения

$$\Psi_r: M_{n_1,k}^{(r)}(\mathbf{V}_1,\Theta_1)\to M_{n_2,k}^{(r)}(\mathbf{V}_2,\Theta_2)\quad (r=1,2),$$

что автомат $\Psi_r(M_r)$ $(M_r\in M_{n_1,k}^{(r)}(\mathbf{V}_1,\Theta_1))$ является гомоморфным образом автомата M_r.

Пусть Γ_{F} – множество всех эллиптических кривых над полем $\mathrm{F}=\mathbf{GF}(q)$ (где $q=p^k$ (p – простое число, $k\in\mathbf{N}$)), G_γ – множество всех точек (включая бесконечно удаленную точку O) эллиптической кривой $\gamma\in\Gamma_{\mathrm{F}}$, а $G_\gamma=(G_\gamma,+_\gamma)$ – абелева группа, определяемая эллиптической кривой γ. Для точки $P\in G_\gamma$ и числа $a\in\mathbf{N}$ положим $aP=\underbrace{P+\ldots+P}_{a\ \text{ðàç}}$.

Для любой эллиптической кривой $\gamma\in\Gamma_{\mathrm{F}}$, любых фиксированных чисел $n,m,l\in\mathbf{N}_{|G_\gamma|}$ и любых фиксированных точек $P_1,P_2\in G_\gamma$ рекуррентные соотношения

$$\begin{cases} q_{t+1}=nq_t+_\gamma x_{t+1}P_1 \\ y_{t+1}=mq_t+_\gamma x_{t+1}P_2 \end{cases}\quad (t\in\mathbf{Z}_+)$$

и

$$\begin{cases} q_{t+1}=nq_t+_\gamma x_{t+1}P_1 \\ y_{t+1}=mq_{t+1} \end{cases}\quad (t\in\mathbf{Z}_+),$$

где $x_{t+1}\in\mathbf{N}_l$, определяют семейство, соответственно, автоматов Мили $M_{1,\gamma,l}$ и автоматов Мура $M_{2,\gamma,l}$.

Охарактеризованы основные нетривиальные с позиции теории автоматов подсемейства исследуемых моделей (семейство групповых автоматов, семейство приведенных автоматов, семейство автоматов с состояниями-близнецами, семейство не сильно связанных автоматов). Решена задача идентификации начального состояния и задача построения асимптотически точной имитационной модели для исследуемых семейств автоматов в предположении, что $n,m\in\mathbf{N}_{|G_\gamma|-1}$ и $P_1,P_2\in G_\gamma\setminus\{O\}$. Доказаны следующие теоремы.

Теорема 19. Для каждого автомата $M_1\in M_{1,\gamma,l}$ идентификация начального состояния (с точностью до множества эквивалентных состояний) сводится к поиску любого решения $v\in G_\gamma$ уравнения $mu=a_0$, где элемент $a_0\in G_\gamma$ определяется в результате простого эксперимента длины 1 с автоматом M_1.

Теорема 20. Для каждого автомата $M_2\in M_{2,\gamma,l}$ идентификация начального состояния (с точностью до множества эквивалентных состояний) сводится к поиску любого решения $u\in G_\gamma$ уравнения $mnv=b_0$, где элемент $b_0\in G_\gamma$ определяется в результате простого эксперимента длины 1 с автоматом M_2.

Теорема 21. Построение точной имитационной модели для семейства автоматов $M_{1,\gamma,l}$ может быть осуществлено в результате кратного эксперимента, кратность которого равна 3, а высота которого не превосходит число $|G_\gamma|+1$. При этом суммарная длина всех входных слов, подаваемых на исследуемый автомат в процессе этого эксперимента, не превосходит число $|G_\gamma|+1+0.5|G_\gamma|(|G_\gamma|+3)$.

Теорема 22. Построение точной имитационной модели для семейства автоматов $M_{2,\gamma,l}$ может быть осуществлено в результате кратного эксперимента, кратность которого равна 2, а высота которого не превосходит число $|G_\gamma|$. При этом суммарная длина всех входных слов, подаваемых на исследуемый автомат в процессе этого эксперимента, не превосходит число $|G_\gamma|+0.5|G_\gamma|(|G_\gamma|+1)$.

Заключение. Приведенные в настоящей работе результаты были получены на основе синтеза моделей и методов современной алгебры, теории систем, теории алгоритмов, теории автоматов и алгебраической геометрии. Новым моментом явилась необходимость разработки методов решения над конечными кольцами систем уравнений с параметрами и разработки методов анализа выполнимости формул над конечными кольцами. В [35] разработана

схема представления в виде теоретико – множественной формулы множества решений над конечным ассоциативным кольцом (с односторонними единицами, либо с двусторонней единицей) систем уравнений с параметрами. Эта схема основана на использовании (односторонних для некоммутативных колец, либо двусторонних для коммутативных колец) классов ассоциированных элементов. В [36] построена схема решателя, предназначенного для проверки выполнимости формул линейной арифметики над любым конечным ассоциативным кольцом с ненулевым умножением. Эта схема основана на использовании (односторонних для некоммутативных колец, либо двусторонних для коммутативных колец) классов ассоциированных элементов, а также на использовании (односторонних для некоммутативных колец, либо двусторонних для коммутативных колец) делителей нуля.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Menezis A., van Oorschot P., Vanstone S. Handbook of applied cryptography. − CRC Press, 1997. − 780 p.
2. Шнайер Б. Прикладная криптология. Протоколы, алгоритмы, исходные тексты на языке СИ. – М.: Триумф, 2003. – 816 с.
3. Харин Ю. С., Берник В.И., Матвеев Г.В., Агиевич С.Г. Математические и компьютерные основы криптологии: – Минск: Новое знание, 2003. – 382 с.
4. Диффи У., Хеллмен М.Е. Защищенность и имитостойкость: Введение в криптографию // ТИИЭР. – 1979. – Т.67. – № 3. – С. 71–109.
5. Молдовян А.А., Молдовян Н.А., Гуц Н.Д., Изотов Б.В. Криптография. Скоростные шифры. – СПб.: БХВ-Петербург, 2002. – 496 с.
6. Анисимова Е.Н., Скобелев В.Г. Сложность идентификации неисправностей блоков управляемых перестановок // Искусственный интеллект. – 2004. – № 4. – С. 794–803.
7. Анисимова Е.Н., Скобелев В.Г. Анализ послойных блоков управляемых перестановок // Искусственный интеллект. – 2005. – № 1. – С. 146–152.
8. Анисимова Е.Н., Скобелев В.Г. Сложность тестирования матричных и послойных БУП // Вестник Томского государственного университета. Приложение. – 2005. – № 14. – С. 139–143.
9. Анисимова Е.Н., Скобелев В.Г. Сложность идентификации неисправностей блока управляемых перестановок // Труды V международной конференции "Идентификация систем и задачи управления (SICPRO 06)". – М.: ИПУ РАН, 2006. – С. 1241–1258.
10. Скобелев В.Г. Контроль неисправностей блоков управляемых перестановок // Надежность. – 2006. – № 4. – С. 41–45.
11. Скобелев В.В., Скобелев В.Г. Анализ шифрсистем. – Донецк: ИПММ НАН Украины, 2009. – 479 с.
12. Скобелев В.Г. Оценки сложности экспериментов с блоками управляемых перестановок // Доповіді НАНУ. – 2011. – № 4. – С. 41–43.
13. Скобелев В.Г. Об одном семействе суперпозиций подстановок // Компьютерная математика. – 2011. – № 1. – С. 116–121.
14. Скобелев В.Г., Зайцева Э.Е. Анализ класса легко вычислимых перестановок // Кибернетика и системный анализ. – 2008. – № 5. – С. 12–24.
15. Скобелев В.Г., Тубольцева О.В. Шифр на основе отображения Эно // Вестник Томского государственного университета. Приложение. − 2004. − № 9(1). − С. 77–82.
16. Скобелев В.Г., Сухинин В.А. Шифры на основе систем Спротта // Вестник Томского государственного университета. Приложение. – 2007. – № 23. – С. 122–126.
17. Скобелев В.Г. Анализ системы Лоренца над кольцом Z_{p^k} // Вестник Томского государственного университета. Приложение. – 2006. – № 17. – С. 134–139.
18. Скобелев В.В. Симметрические динамические системы над конечным кольцом: свойства и сложность идентификации // Труды ИПММ НАНУ. − Т.10. − 2005. − С. 184–189.
19. Скобелев В.В. Исследование структуры множества линейных БПИ-автоматов над кольцом $\mathbf{Z}_{p^k}$ // Доповіді НАНУ. − 2007. − № 10. − С. 44–49.
20. Скобелев В.В. Анализ структуры класса линейных автоматов над кольцом $\mathbf{Z}_{p^k}$ // Кибернетика и системный анализ. − 2008. − № 3. − С. 60–74.
21. Скобелев В.В., Глазунов Н.М., Скобелев В.Г. Многообразия над кольцами. Теория и приложения. − Донецк: ИПММ НАНУ. − 2011. − 323 с.
22. Скобелев В.Г. Анализ задачи параметрической идентификации нелинейных автоматов над конечным кольцом // Проблемы управления и информатики. – 2010. – № 5. – С. 37–41.
23. Скобелев В.Г. Восстановление вектора начального состояния нелинейных автоматов над конечным кольцом // Проблемы управления и информатики. – 2010. – № 6. – С. 31–34.
24. Скобелев В.В. Моделирование автоматов над кольцом автоматами с конечной памятью // Проблемы управления и информатики. – 2012. – № 3. – С. 114–122.
25. Скобелев В.В. Автоматы на алгебраических структурах. Модели и методы их исследования. – Донецк: ИПММ НАНУ, 2013. – 307 с.
26. Скобелев В.В. Анализ семейств хэш-функций, определяемых автоматами над конечным кольцом // Кибернетика и системный анализ. – 2013. – № 2. – С. 46–55.
27. Черемушкин А.В. Лекции по арифметическим алгоритмам в криптографии. – М.: МЦНМО, 2002. – 104 с.
28. Василенко О.Н. Теоретико-числовые алгоритмы в криптографии. – М.: МЦНМО, 2003. − 326 с.
29. Скобелєв В.В. Аналіз автоматів, які визначено на еліптичних кривих // Вісник Київського університету. Сер.: фіз.-мат. науки. – 2012. – Вип. 1. – С. 223–230.
30. Скобелев В.В. Об автоматах на многообразиях над кольцом // Труды ИПММ НАНУ. – 2012. – Т. 24. – С. 190–201.
31. Скобелєв В.В. Автомати на многовидах з алгеброю // Вісник Київського університету. Сер.: фіз.-мат. науки. – 2012. – Вип. 2. – С. 234–238.
32. Скобелев В.В. Об автоматах на полиномиально параметризованном многообразии над конечным кольцом // Труды ИПММ НАНУ. – 2012. – Т. 25. – С. 185–195.
33. Skobelev V.V. Analysis of automata determined over parametric varieties over an associative ring // Вісник Київського університету. Сер.: фіз.-мат. науки. – 2012. – Вип. 3. – С. 239–244.
34. Скобелев В.В. О гомоморфизмах автоматов на многообразиях над кольцом // Доповіді НАНУ. – 2013. – № 1. – С. 42–46.
35. Skobelev V.V. On systems of polynomial equations over finite rings // Наукові записки НаУКМА. Серія: Комп'ютерні науки. – 2012. – Т. 138. – С. 15–19.
36. Skobelev V.V. Satisfiability modulo linear arithmetic over a finite ring // Вісник Київського університету. Сер.: фіз.-мат. науки. – 2013. – Вип. 2. – С. 95–106.

Надійшла до редколегії 15.09.14

Скобелєв В. В., канд. фіз.-мат. наук,
Скобелєв В. Г., д-р фіз.-мат. наук, д-р техн. наук, проф.
ІПММ НАН України, Донецьк

МЕТОДИ АНАЛІЗУ АВТОМАТНО-АЛГЕБРАЇЧНИХ МОДЕЛЕЙ

В роботі розглянуто методи аналізу автоматних моделей, які визначено над скінченними кільцями. Для керованих логічних операцій досліджено складність виявлення та локалізації дефектів у процесі off-line контролю їх апаратних реалізацій, а також обчислювальна стійкість сімей легко-обчислюваних переставлень. Досліджено задачу побудови імітаційної моделі для сім'ї автоматів, які визначено системами рівнянь над скінченними кільцями, а також обчислювальну стійкість сім'ї гэш-функцій, які визначено автоматом без вихідної функції. Досліджено автомати, які визначено на многовиді над скінченним кільцем, у тому числі, автомати, які визначено на еліптичній кривій над скінченним полем.

Ключові слова: скінченні автомати, скінченні кільця, многовиди, еліптичні криві.

Skobelev V. V., PHD, Phys.-math. Sci.
Skobelev V. G., Dr. Phys. Math. Sci., Dr. Tech. Sci., Professor
IAMM of NAS of Ukraine, Donetsk

METHODS FOR ANALYSIS OF AUTOMATA-ALGEBRAIC MODELS

In the given paper there are presented methods for analysis of automata models defined over finite rings. For controlled logic operations there are investigated complexity of checking and localization of faults in the process off-line analysis of their hardware realizations, and computational security of families of easy-computable permutations. There are investigated the problem of design of simulation model for a family of automata defined via a system of equations over a finite ring, and computational security of a family of hash-functions determined by an automaton without output function. There are investigated automata defined on a variety over a finite ring, and automata defined on elliptic curve over a finite field.

Keywords: finite automata, finite rings, varieties, elliptic curves.

УДК 519.852:519.876

Б. Д. Тодоріко, асп.,
В. І. Кудін, д-р техн. наук, пров. наук. співроб.,
Ю. А. Григор'єва, студ.
Київський національний університет імені Тараса Шевченка, Київ

МЕТОД БАЗИСНИХ МАТРИЦЬ ТА РІВНОВАЖНІ СТАНИ МАТРИЧНОЇ ГРИ У ЗМІШАНИХ СТРАТЕГІЯХ

Проаналізовано зв'язки елементів методу базисних матриць для задачі лінійного програмування знаходження оптимальних стратегій гравців матричної гри у змішаних стратегіях. Досліджено умови рівноважності станів матричної гри у змішаних стратегіях (оптимальні стратегії гравців) на основі положень методу базисних матриць для двоїстої пари задач лінійного програмування.

Ключові слова: двоїстна задача, матрична гра, метод Лагранжа, лінійне програмування.

Вступ. Для багатьох практичних задач прийняття рішень математична модель описуються як певний конфлікт (двох гравців). Знаходження оптимальних, вигідних стратегій гравців описується як розв'язання задачі лінійного програмування (матричної гри). В загальному випадку, така задача є лише однією із задач дослідження. Виникає ряд інших задач, наприклад, дослідження властивостей математичної моделі та характер її розв'язків. Ці проблеми вцілому недостатньо досліджені. Наведені нижче умови єдиності розв'язків (стратегій гравців) направлені організувати більш розширений аналіз властивостей матричної гри, як прямої та двоїстої задач лінійного програмування.

Встановлено [1–4], як побудувати пару двоїстих задач лінійного програмування, розв'язок яких визначає оптимальні стратегії заданої матричної гри. Параметри задач лінійного програмування, що відповідають заданій матричній грі, вибираються в процесі конструктивного доведення основної теореми теорії ігор [1,2,4].

Можлива також побудова матричної гри за заданою задачею лінійного програмування. Введення одного з найважливіших понять теорії ігор – поняття *стратегії* - дозволяє звести найрізноманітніші розгорнуті ігри до єдиної стандартної форми, яка називається *нормальною* формою гри.

Стратегією гри [1–3] називається система правил, що однозначно визначають вибір поведінки гравця на кожному ході в залежності від ситуації, що склалася в процесі гри. Гравець, який вибрав стратегію, може не брати участь в грі. За складеною ним інструкцією гру може проводити нейтральна особа.

Кожна фіксована стратегія, яку може обрати гравець, називається його *чистою стратегією*. Чисті стратегії не вичерпують усіх можливостей гравців. Як ми побачимо далі, *платіжною матрицею* або *матрицею виграшів*.

Зауважимо, що складання платіжної матриці при формалізації реальних конфліктних ситуацій є складною задачею. Підстави для побудови платіжної матриці лежать, взагалі кажучи, поза теорією ігор і відносяться до певного застосування, з яким пов'язана постановка задачі.

Постановка та базові означення задачі. Нехай перший гравець має m стратегій, а другий – n. При цьому вважається відомим, що якщо перший гравець вибере i -у стратегію, а другий – j -у, виграш першого (і отже програш другого) дорівнює $\|a_{ij}\|$. Матриця $A=\|a_i\|$ $A=\|a_{ij}\|_{i=1,j=1}^{m,n}$ називається *платіжною матрицею* або *матрицею виграшів*.

Зауважимо, що складання платіжної матриці при формалізації реальних конфліктних ситуацій є складною задачею. Підстави для побудови платіжної матриці лежать, взагалі кажучи, поза теорією ігор і відносяться до певного застосування, з яким пов'язана постановка задачі.

Означення 1. Вектор $u=(u_1,u_2,...,u_m)$, кожна компонента якого вказує відносну частоту (ймовірність), з якою відповідна чиста стратегія використовується в грі, називається *змішаної стратегією* першого гравця.

Набір чисел $w=(w_1,w_2,...,w_n)$ – змішана стратегія другого гравця. Ясно, що $u_i \geq 0,\ i=\overline{1,m},\ \sum_{i=1}^{m} u_i = 1,$ $w_j \geq 0,\ j=\overline{1,n},\ \sum_{j=1}^{n} w_j = 1$. Чиста стратегія може бути визначена як змішана стратегія, в якій всі складові, крім однієї, рівні нулю. Надалі будемо позначати чисті стратегії обох противників у вигляді одиничних векторів $e_i=(\underbrace{0,0,...,0,1,0,...,0}_{i})$ та $e_j=(\underbrace{0,0,...,0,1,0,...,0}_{j})$ відповідно.

Означення 2. Оптимальна стратегія гравця – це стратегія, що забезпечує йому максимально можливий гарантований середній виграш.

Властивості оптимальних стратегій матричної гри випливають з відповідність пари двоїстих задач лінійного програмування типу (1)–(3) та (4)–(6) з однотипними обмеженнями, які наведені нижче.

Пряма задача:

$$\max \sum_{j=1}^{n} c_j x_j, \tag{1}$$

за умов:

$$A=\|a_{ij}\|_{i=1,j=1}^{m,n}\ (a_{ij}>0)\begin{cases} a_{11}x_1+a_{12}x_2+...+a_{1n}x_n \leq b_1; \\ a_{21}x_1+a_{22}x_2+...+a_{2n}x_n \leq b_2; \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{m1}x_1+a_{m2}x_2+...+a_{mn}x_n \leq b_m; \end{cases} \tag{2}$$

$$x_j \geq 0,\quad j=\overline{1,n}\ . \tag{3}$$

де $C=(c_1,c_2,...,c_n)$, $x=(x_1,x_2,...,x_n)^T$, $B=(b_1,b_2,...,b_m)$. Вважаємо, що модель виду (1)−(3) має матрицю обмежень А в якій кількість стовпців більша ніж рядків (“довга”).

Двоїста задача:

$$\min \sum_{i=1}^{m} b_i u_i \tag{4}$$

за умов:

$$\begin{cases} a_{11}u_1 + a_{21}u_2 + a_{31}u_3 + ... + a_{m1}u_m \ge c_1; \\ a_{12}u_1 + a_{22}u_2 + a_{32}u_3 + ... + a_{m2}u_m \ge c_2; \\ ..... \\ a_{1n}u_1 + a_{2n}u_2 + a_{3n}u_3 + ... + a_{mn}u_m \ge c_n; \end{cases} \tag{5}$$

$$u_i \ge 0, \quad (i=\overline{1,m}). \tag{6}$$

Матрична гра у змішаних стратегіях подається як двоїста пара задач лінійного програмування [2–4] (1)–(3) та (4)–(6), де $b_i=1,\ j=\overline{1,m}$, $c_j=1,\ j=\overline{1,n}$.

Задача (4)-(6) є двоїстою або спряженою до задачі (1)–(3), яку називають прямою (основною, початковою).

Оскільки оптимальні стратегії матричної гри визначаються через компоненти розв'язків задач (1)–(3) та (4)–(6) [1–3], то складові оптимальних стратегій $u_i^{'}$ та $w_i^{'}$ ігри пов'язані з компонентами u_i та x_j оптимальних планів двоїстих задач лінійного програмування формулами $w_j^{'}=x_j/\sum_{j=1}^{n}x_j$, $u_i^{'}=u_i/\sum_{i=1}^{m}u_i$.

Мета роботи. Ставиться завдання дослідити властивості векторів оптимальних стратегій гравців у матричній грі, що подається у еквівалентному вигляді (1)–(3) та (4)–(6). Встановити структурні властивості вектору рівноважних станів (сідлових точок), який формується компонентами оптимальних стратегій гравців.

Теорія двоїстості. В дослідженнях зв'язків лінійного програмування з математичним, як більш загального та, зокрема, з методом множників Лагранжа, розглядають постановки задач у канонічному вигляді [5] (обмеження на "="). В теорії лінійного програмування теорія двоїстості та основні методи розв'язування задачі подані з формою запису для задач зі змішаними обмеженнями, однотипними та канонічними. Слід зазначити, що для різних форм запису встановлені положення про зв'язок поміж ними. Перетворення задачі до канонічного вигляду проводиться введенням додаткових змінних (зведення обмеження до “=”) для кожної із задач. А саме, для (2)-(3):

$$A_x^{'}x^{'}=B^T,\ x^{'}\ge 0,\ \text{де}\ x^{'}=(\underbrace{x_1,x_2,...,x_n}_{x},x_{n+1},...,x_{n+m})^T.$$

Аналогічно для (5)-(6):

$$A_u^{'T}u^{'}=C^T,\ u^{'}\ge 0,\ u^{'}=(\underbrace{u_1,u_2,...,u_m}_{x},u_{m+1},...,u_{n+m})^T.$$

Теорема 2. (друга теорема двоїстості для канонічної задачі [5]). Для того, щоб плани x^* та u^* відповідних спряжених задач були оптимальними, необхідно і достатньо, щоб виконувалися умови доповнюючої нежорсткості:

$$x_j^*\left(\sum_{i=1}^{m}a_{ij}u_i^*-c_j\right)=0,\quad j=\overline{1,n},\quad u_i^*\left(\sum_{j=1}^{n}a_{ij}x_j^*-b_i\right)=0,\quad i=\overline{1,m}.$$

Очевидніший взаємозв'язок між оптимальними планами прямої та двоїстої задач встановлює наслідок другої теореми двоїстості.

Наслідок 1. Якщо в результаті підстановки оптимального плану однієї із задач (прямої чи двоїстої) в систему обмежень цієї задачі i-е обмеження виконується як строга нерівність, то відповідна i-а компонента оптимального плану (відповідна стовпцю A_i) спряженої задачі дорівнює нулю.

Якщо i-а компонента оптимального плану однієї із задач додатна (при стовпцю A_i), то відповідне i-е обмеження спряженої задачі виконується для оптимального плану як рівняння.

Оскільки оптимальні стратегії матричної гри визначаються через компоненти розв'язків задач (1)–(3) та (4)–(6) [1], саме складові оптимальних стратегій $u_i^{'}$ та $w_i^{'}$ ігри пов'язані з компонентами u_i та x_j оптимальних планів двоїстих задач лінійного програмування формулами, а саме $w_j^{'}=x_j/\sum_{j=1}^{n}x_j$, $u_i^{'}=u_i/\sum_{i=1}^{m}u_i$.

Метод Лагранжа у лінійному програмуванні. Метод Лагранжа ґрунтується на наступному твердженні [5]: Якщо функція $F(X)=F(x_1,x_2,\dots,x_n)$ досягає свого максимуму або мінімуму при умовах

$$G_i(X)=G_i(x_1,x_2,\dots,x_n)=0,\qquad i=1,2,\dots,m\quad (m<n)$$

у точці $\overline{X}$ (система регулярна в цій точці), то існують такі числа λ_1, λ_1, ..., λ_m, що для функції

$$F_\Lambda(X)=F(X)+\sum_{i=1}^{m}\lambda_i G_i(X)$$

у точці $\overline{X}$ виконуються необхідні умови безумовного екстремума, тобто $\dfrac{\partial F_\Lambda(\overline{X})}{\partial x_i}=0$ при $i=1,2,\dots,n$.

Числа λ_1, λ_1, ..., λ_m прийнято називати множниками Лагранжа, функцію $F_\Lambda(X)$ – функцією Лагранжа. Таким чином, обчислення умовного екстремуму $F(X)=F(x_1,x_2,\dots,x_n)$, «зводиться» до відшукання безумовного екстремуму функції Лагранжа.

Загальна схема методу Лагранжа полягає в наступному.

Складається функція Лагранжа з невизначеними множниками λ_i. Потім вирішується система рівнянь $\frac{\partial F_\Lambda(X)}{\partial x_i} = 0$, $i = 1, 2, \ldots, n$.

Рішення цієї системи залежить від значень невідомих параметрів λ_i, $i = 1, 2, \ldots, m$, які визначаються за допомогою системи.

Задача математичного програмування відрізняється від класичної задачі на умовний екстремум наявністю умов, що мають вид нерівностей. Тому наведений тут метод Лагранжа ("напряму") до неї не застосовний. Однак після деякої видозміни (приведення до канонічного вигляду) цей метод може бути розповсюджений також і на досить широкий клас задач математичного програмування.

Нехай задача лінійного програмування (1)–(3) записана в канонічній формі. Покладемо

$$F(X) = \sum_{j=1}^{n} c_j x_j$$

$$G_i(X) = -\sum_{j=1}^{n} a_{ij} x_j + b_i, \; i = \overline{1,m}$$

Теорема 3. Для оптимальності плану X задачі (1)–(3) необхідно та достатньо, щоб функція Лагранжа

$$F_\Lambda(X) = F(X) + \sum_{i=1}^{m} \lambda_i G_i$$

при деяких значеннях множників λ_i, $i = \overline{1,m}$ досягала в точці $\bar{X}$ максимуму за умови

$$x_j \geq 0, j = \overline{1,n}$$

Твердження дає підставу називати компоненти вектора *Л = (л1, л2, … лm),* що бере участь в формуванні функції $F_\Lambda(X)$ для задачі (1)–(3), множниками Лагранжа задачі.

Встановлено [5], що сукупність розв'язнуючих векторів задачі лінійного програмування (розв'язків (4)-(6)) збігається із системою векторів, складених із множників Лагранжа даної задачі. Тобто, розв'язанні вектори та множники Лагранжа задачі лінійного програмування - поняття еквівалентні.

У формулюванні теореми 3 вектор $\bar{X}$ передбачався планом розглянутої задачі. Тому ця теорема ще не звільняє нас повністю від необхідності враховувати умови (2), що зв'язують змінні задачі (1)–(3).

Задача про відшукання сідлової точки для функції Лагранжа.

Нехай $R(X,Y)$ – функція, що залежить від вектора X, що належить множині T_x, та вектора Y, що змінюється в межах множини T_Y Згідно [5], точку $(X_0, Y_0) \in T_X \times T_Y$ назвемо *сідловою точкою* функції *R(X,Y)* за умови $(X,Y) \in T_X \times T_Y$, якщо співвідношення

$$R(X,Y_0) \leq R(X_0,Y_0) \leq R(X_0,Y)$$

мають місце для всіх точок $(X,Y) \in T_X \times T_Y$. Нерівності показують, що найбільше значення функції $R(X,Y_0)$ на множині T_x досягається в точці X_0, а найменше значення функції $R(X_0,Y)$ на T_y досягається в точці Y_0.

Для задачі лінійного програмування (1)-(3) запишемо:

$$F_\Lambda(X) = F(X,\Lambda) = \sum_{j=1}^{n} c_j x_j + \sum_{i=1}^{m} \lambda_i (b_i - \sum_{j=1}^{n} a_{ij} x_j) =$$

$$= \sum_{j=1}^{n} c_j x_j + \sum_{i=1}^{m} \lambda_i b_i - \sum_{i=1}^{m} \sum_{j=1}^{n} \lambda_i a_{ij} x_j$$

Наслідок теореми [5] Вектори $X^* = (x_1^*, x_2^*, \ldots x_n^*)$ і $\Lambda^* = (\lambda_1^*, \lambda_2^*, \ldots \lambda_n^*)$ є відповідно рішенням задачі (1)-(3) і її розв'язним вектором у тім і тільки в тому випадку, якщо (X^*, Λ^*) – сідлова точка функції $F(X,\Lambda)$ при умовах

$$x_j \geq 0, \; j = \overline{1,n_1}, \qquad \lambda_j \geq 0, \; i = \overline{1,m_1}.$$

Відповідно до теореми 6 пари взаимосопряжених задач (1)–(3) і (4)–(6) еквівалентні задачі про відшукання сідлової точки функції Лагранжа $F(X,\Lambda)$ при умовах $x_j \geq 0, \; j = \overline{1,n_1}, \quad \lambda_j \geq 0, \quad i = \overline{1,m_1}$.

Ставиться завдання дослідити властивості оптимальних стратегій ігроків у матричній грі, що подається у еквівалентному вигляді (1)–(3) та (4)–(6).

Положення методу базисних матриць (МБМ). МБМ [6] може бути застосований як до прямої так і до двоїстої задачі, причому розв'язання кожної з задач буде давати інформацію про властивості стратегій відповідно першого та другого гравців.

Без обмеження загальності, при викладенні положень методу будемо розглядати задачу лінійного програмування у вигляді (4)–(6), а саме:

$$(\max Bu, \; A^T u \leq C^T, \; u \geq 0).$$

Для визначеності, будемо вважати, що задача (1)−(3) має n>>m, матриця A обмежень «витягнута» горизонтально, ранг системи рівним m. Задача виду (4),(5) має n обмежень та m змінних, матриця A^T обмежень «витягнута» вертикально.

Визначення 4. Підматрицю $A_б$ матриці A^T, складену із m лінійно незалежних нормалей $J_b = (i_1, i_2, \ldots, i_m)$ обмежень (5), будемо називати базисною (БМ), а розв'язок $u_0 = (u_{01}, u_{02}, \ldots, u_{0m})^T$ відповідної їм системи рівнянь $A_б u_0 = C^0$, де $C^0 = (c_{i_1}, c_{i_2}, \ldots, c_{i_m})$ – підвектор С базисним (БР).

Дві базисні матриці з відмінним одним рядком будемо називати суміжними.

Нехай: β_{ij}, $i,j \in I = \{1,2,...,m\}$ – елементи $A_б$; e_{rs} та $(\grave{A}_б^{-1})_i$ елементи та i -й стовпець $\grave{A}_б^{-1}$, оберненої до $\grave{A}_б$; $\alpha_r = (\alpha_{r1}, \alpha_{r2}, ..., \alpha_{rm})$ - вектор розвинення нормалі обмеження $a_r u_1 \le c_r$ за рядками $A_б$,

$\alpha_0 = (\alpha_{01}, \alpha_{02}, ..., \alpha_{0m})$ вектор розвинення нормалі цільової функції (4) за рядками $A_б$; $\Delta_r = a_r u_0 - c_r$ - нев'язка r -о обмеження (5), а $\Delta_0 = Bu_0$ – значення цільової функції в вершині u_0, які утворюють вектор $\Delta = (\Delta_0, \Delta_1, ..., \Delta_n)$; $J_б, J_н$ – множини індексів, відповідно базисних і небазисних обмежень (5).

Всі означені елементи при переході до суміжної $\bar{A}_б$, яка утворюється із A_b заміною її рядка a_k на a_l, що не входить в $A_б$, будемо позначати рискою зверху, тобто $\bar{\beta}_{ij}$, $\bar{\alpha}_r$, $\bar{L}_i$, $\bar{\Delta}_k$, $\bar{e}_{ri}$, $(\bar{A}_b^{-1})_i$ $\bar{\alpha}_0$.

Нехай $a_{i1}, a_{i2}, ..., a_{im}$ – нормалі, $a_j u \le c_j, j \in J_б$, де $J_б = \{i_1, i_2, ..., i_m\}$ – індекси обмежень, нормалі яких утворюють $A_б$, $\grave{a}_l$ – вектор-нормалі $a_l u \le c_l$, $\alpha_l = (\alpha_{l1}, \alpha_{l2}, ..., \alpha_{lm})$ – вектор розвинення a_l за рядками $A_б$.

Теорема 4. [6] Між коефіцієнтами розвинення нормалей обмежень (5) та цільової функції (4) за рядками базисної матриці, елементами обернених матриць, базисними розв'язками, нев'язками обмежень (5) та значеннями цільової функції в двох суміжних базисних розв'язках мають місце такі співвідношення

$$\bar{\alpha}_{rk} = \frac{\alpha_{rk}}{\alpha_{lk}}, \quad \bar{\alpha}_{ri} = \alpha_{rs} - \frac{\alpha_{rk}}{\alpha_{lk}}\alpha_{ls}, \qquad r = \overline{0,n}; \quad i = \overline{1,m}; \quad s \ne k; \tag{7}$$

$$\bar{e}_{rk} = \frac{e_{rk}}{\alpha_{lk}}, \quad \bar{e}_{ri} = e_{rs} - \frac{e_{rk}}{\alpha_{lk}}\alpha_{ls}, \qquad r = \overline{1,m}; \quad i = \overline{1,m}; \quad s \ne k; \tag{8}$$

$$\bar{u}_{0j} = u_{0j} - \frac{e_{jk}}{\alpha_{lk}}\Delta_l, \qquad j = \overline{1,m}, \tag{9}$$

$$\bar{\Delta}_k = -\frac{\Delta_l}{\alpha_{lk}}, \qquad \bar{\Delta}_r = \Delta_r - \frac{\alpha_{rk}}{\alpha_{lk}}\Delta_l, \qquad r = \overline{1,n}; \qquad r \ne k; \tag{10}$$

$$B\bar{u}_0 = Bu_0 - \frac{\alpha_{0k}}{\alpha_{lk}}\Delta_l, \tag{11}$$

причому умовою невирожденості є $\alpha_{lk} \ne 0$, умовою допустимості опорного базисного розв'язку – $\alpha_{lk} < 0$, а умовою зростання цільової функції – $\alpha_{0k} < 0$.

Встановлено [6], що якщо існує базисна матриця $A_б$ така, що $\alpha_{0k} \ge 0, k = \overline{1,m}$, то базисна матриця та відповідний їй розв'язок u_0 оптимальні, причому при $\alpha_{ok} > 0, \quad k = \overline{1,m}$, розв'язок єдиний, при $\exists i_0 \in I, \alpha_{0i0} = 0$, розв'язок неєдиний.

Нехай $S_1^c, S_2^c, ..., S_m^c$ – суми елементів стовпців, а $S_1^r, S_2^r, ..., S_m^r$ – суми елементів рядків оберненої матриці A_b^{-1}.

Про дослідження розв'язків матричної гри у змішаних стратегіях методом базисних матриць.

Твердження 1. Компоненти вектора розкладу цільової функції (4) задачі лінійного програмування (двоїстої задачі матричної гри) в ході ітерацій методу базисних матриць обчислюються за формулами $\alpha_{0i} = \sum_{j=1}^{m} e_{ji}, i = \overline{1,m}$, тобто $S_i^c = \alpha_{0i} = \sum_{j=1}^{m} e_{ji}, i = \overline{1,m}$, де $S_1^c, S_2^c, ..., S_m^c$ – суми елементів стовпців оберненої матриці, причому співпадають з невід'ємними компонентами вектора опорного розв'язку прямої задачі.

Наслідок 2. Якщо існує базисна матриця $A_б$ така, що $S_k^c \ge 0$, $k = \overline{1,m}$, то базисна матриця та відповідний їй розв'язок u_0 оптимальні, причому при $S_k^c > 0$, $k = \overline{1,m}$, розв'язок єдиний, при $\exists i_0 \in I, S_{i_0}^c = 0$, розв'язок неєдиний.

Наслідок 3. Компоненти вектору розкладу цільової функції (4) співпадають із невідємними компонентами опорного розв'язку задачі (1)–(3).

Твердження 2. Компоненти вектора розв'язків задачі лінійного програмування (двоїстої задачі матричної гри) в ході ітерацій методу базисних матриць обчислюються за формулами $u_{0i} = \sum_{j=1}^{m} e_{ij}, i = \overline{1,m}$, тобто $S_i^r = u_{0i} = \sum_{j=1}^{m} e_{ij}, i = \overline{1,m}$, де $S_1^r, S_2^r, ..., S_m^r$ – суми елементів рядків оберненої матриці).

Доведення. Неважко переконатись, що вектор обмежень відповідний рядкам, що утворюють базисну матрицю на ітераціях методу базисних матриць буде одиничним (як під вектор одиничного). Розрахунок компонент базисного розв'язку на ітераціях методу буде знаходитись множенням справа оберненої матриці (до базисної) на одиничний вектор-стовпець і буде справедлим $u_{0i} = \sum_{j=1}^{m} e_{ij}, i = \overline{1,m}$.

Наслідок 3. Сума елементів векторів стовпців оберненої матриці співпадають із значенням відповідної компоненти вектору розкладу цільової функції (1) за рядками базисної матриці.

Наслідок 4. Сума елементів рядків оберненої матриці співпадають із значенням відповідної компоненти вектору проміжного розв'язку на ітераціях методу базисних матриць.

Доведення. Оскільки вектор цільової функції задачі (4)–(6) є вектором обмеження двоїстої задачі (в даному випадку задачі (1)–(3)), а оптимальна базисна матриця (рядкова) задачі (4)–(6) при транспонуванні буде утворювати оптимальні стовпці, що відповідають невід'ємним компонентам опорного розв'язку задачі (1)–(3) – умова доповнюю-

чої не жорсткості (тобто для того, щоб плани X^* та U^* відповідних спряжених задач були оптимальними, необхідно і достатньо, щоб виконувалися умови:

$$x_j^*\left(\sum_{i=1}^{m} a_{ij}u_i^* - c_j\right) = 0, \quad j = \overline{1,n}, \qquad u_i^*\left(\sum_{j=1}^{n} a_{ij}x_j^* - b_i\right) = 0, \quad i = \overline{1,m}).$$

Тоді справедливість тверджень 1,2 та наслідків витікає із властивостей розкладу елементів методу базисних матриць за рядками базисної матриці та співвідношень (7) та (9).

$$A_\delta u_0 = C_\delta,\ C_\delta = (\underbrace{1,1,\ldots,1}_{m})^T, \qquad u_0 = A_\delta^{-1} \times C_\delta,\ C_\delta = (\underbrace{1,1,\ldots,1}_{m})^T,$$

$$\alpha_0 \times A_\delta = B,\ B = (\underbrace{1,1,\ldots,1}_{m}), \qquad \alpha_0 = B \times A_\delta^{-1},\ B = (\underbrace{1,1,\ldots,1}_{m}).$$

Висновок. Розв'язання двоїстої пари задач лінійного програмування (матричної гри у змішаних стратегіях) (1)–(3) та (4)–(6) на основі методу базисних матриць встановлює властивості оптимальних розв'язків прямої та двоїстої задачі, зокрема вказує на властивості єдності та неєдиності.

Після встановлення властивостей розв'язків прямої та двоїстої задач можна зробити висновки про рівноважні стани матричної гри (про сідлові точки задачі та їх властивості).

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Golshteyn E.G., Yudin D.B. New directions in linear programming. − M. − Sovetskoe radio, − 1969, − 524p. (in Russian).
2. Dantzig G.B Linear programming and application. M.: Progress, − 1966. (in Russian).
3. Dantzig G.B., Thapa M.N. Linear Programming 1: introduction, Springer, − 1997, − 435p.
4. Dantzig G.B. Dikin's Interior Method for solving LP manuscript, Department of Operations Research, Stanford University, Stanford, − 1988.
5. Golshteyn E.G., Yudin D.B. Linear programming/.Theory and methods. −M.: Nauka, − 1963. – 776p. (in Russian).
6. Kudin V. I., Lyashko S.I., Khritonenko N.V., Yatsenko Yu.P. Analysis of the properties of a linear system using the method of artificial basis matrices // Kibernetika i sistemny analiz. – 2007. – N 4. –.P. 119–127 (in Ukrainian).

Надійшла до редколегії 28.05.14

Тодорико Б. Д., асп.,
Кудин В. И., д-р техн. наук, вед. науч. сотр., Григорьева Ю. А., студ.,
Киевский национальный университет имени Тараса Шевченко, Киев

МЕТОД БАЗИСНЫХ МАТРИЦ И РАВНОВЕСНЫЕ СОСТОЯНИЯ МАТРИЧНОЙ ИГРЫ В СМЕШАННЫХ СТРАТЕГІЯХ

Проанализированы связи элементов метода базисных матриц для задачи линейного программирования нахождения оптимальных стратегий игроков матричной игры в смешанных стратегиях. Исследованы условия равновесности состояний матричной игры в смешанных стратегиях (оптимальные стратегии игроков) на основе положений метода базисных матриц для двойственной пары задач линейного программирования.

Ключевые слова: двоиста задача, матричная игра, метод Лангранжа, линейное программирование.

Todoriko B. D., postgraduate
Kudyn V. I., Dr. Sc. Science
Grigorieva Y. A., a student
Taras Shevchenko National University of Kyiv

THE METHOD OF BASIS MATRICES AND THE EQUILIBRIUM STATE OF THE MATRIX GAME IN MIXED STRATEGIYAH

Analysis of communications elements method basis matrix for the linear programming problem of finding optimal strategies of players in the game matrix mixed strategies. The conditions of equilibrium states of a matrix game in mixed strategies (optimal strategies of players) on the basis of the method of basis matrices for the dual pair of linear programming problems.

Keywords: duol task matrix game, the Lagrangian method, linear programming.

УДК 517.929.4

Д. Я. Хусаинов, д-р физ.-мат. наук, А. С. Сиренко, асп.,
Киевский национальный университет имени Тараса Шевченко, Киев

ОБ УСТОЙЧИВОСТИ ЛИНЕЙНЫХ СИСТЕМ С ПЕРЕКЛЮЧЕНИЯМИ

В настоящей работе будут рассматриваться линейные дифференциальные системы с линейными законами переключения. Получены условия устойчивости их решений.

Ключевые слова: устойчивость, разностные системы, переключение, метод Ляпунова.

Введение. Исследованию устойчивости дифференциальных и разностных систем в отдельности посвящено достаточно много работ. Например, можно указать [1–4]. В последнее время появился интерес к исследованию систем, описываемых одновременно и дифференциальными, и разностными системами (гибридными системами, системами с переключениями, логико-динамическими системами).

Как правило, понятие устойчивости касается только решений систем дифференциальных и разностных уравнений. В нелинейных системах решения бывают как устойчивыми, так и неустойчивыми. Поэтому понятие "устойчивая система" относится только к линейным системам.

1. Устойчивость линейных систем с линейными переключениями. Рассмотрим динамическую систему, описываемую совокупностью дифференциальных и разностных уравнений. А именно, в моменты $t_i \le t < t_{i+1}$, $i = 0,1,2,3,\ldots$ система описывается линейными стационарными дифференциальными уравнениями

$$x'(t) = A_i x(t), \tag{1.1}$$

а в моменты $t = t_i$ происходят переключения, которые описываются линейными разностными уравнениями

$$x(t_i + 0) = B_i x(t_i - 0),\ i = 0,1,2,3,... \tag{1.2}$$

Под решением системы с переключениями (1.1), (1.2) будем понимать непрерывно дифференцируемую на промежутках $t_i \le t < t_{i+1}$, $i = 0,1,2,3,...$ функцию, которая при $i = 0,1,2,3,...$ скачкообразно изменяется согласно зависимости (1.2).

Интерес представляет получение условий асимптотической устойчивости решений динамических систем (1.1) с переключениями (1.2).

Определение 1.1. Нулевое решение системы с переключениями (1.1), (1.2) называется устойчивым по Ляпунову, если для любого решения $x(t)$ при произвольно заданных моментах переключения $t_0 < t_1 < t_2 < ... < t_k < ...$ с систем (1.1) на системы (1.2) и с (1.2) на (1.1) для произвольного $\varepsilon > 0$ существует $\delta(\varepsilon) > 0$ такое, что для любого решения $x(t)$ будет выполняться $|x(t)| < \varepsilon$, $t > t_0$, лишь только $|x(t_0)| < \delta(\varepsilon)$.

Предварительно получим условия устойчивости системы с переключениями (1.1), (1.2), основанные на представлении решений систем дифференциальных (1.1) и разностных (1.2) уравнений.

Теорема 1.1. Для асимптотической устойчивости системы с переключениями (1.1), (1.2) необходимо и достаточно, чтобы для произвольного $\varepsilon > 0$, произвольных моментов переключения $t_0 < t_1 < t_2 < ... < t_k < ...$ и $t > t_k$, $k = 1,2,3,...$ выполнялись неравенства

$$\delta(\varepsilon) < \varepsilon \min\left\{ \frac{1}{\prod_{j=0}^{k-1} B_{k-i} e^{A_{k-i}(t_{k-i} - t_{k-i-1})}}, \frac{1}{e^{A_{k+1}(t-t_k)} \prod_{i=0}^{k-1} B_{k-i} e^{A(t_{k-i} - t_{k-i-1})}} \right\}. \tag{1.3}$$

Доказательство. Вычислим решение системы с переключениями, методом шагов.

1.1. Рассмотрим первый шаг, состоящий из движения по непрерывной траектории системы дифференциальных уравнений

$$x'(t) = A_1 x(t),\ t_0 \le t \le t_1. \tag{1.3}$$

и переключения

$$x(t_1 + 0) = B_1 x(t_1). \tag{1.4}$$

Движение по закону дифференциального уравнения (1.3) описывается решением вида

$$x(t) = e^{A_1(t-t_0)} x(0),\ t_0 \le t \le t_1.$$

И в момент $t = t_1$ оно имеет вид

$$x(t_1) = e^{A_1(t_1 - t_0)} x(0).$$

Далее идет переключение по закону (1.3) и в момент $t = t_1 + 0$ оно равно

$$x(t_1 + 0) = B_1 e^{A_1(t_1 - t_0)} x(0).$$

1.2.Рассмотрим второй шаг, также состоящий из движения по непрерывной траектории системы

$$x'(t) = A_2 x(t),\ t_1 < t \le t_2 \tag{1.5}$$

и переключения

$$x(t_2 + 0) = B_2 x(t_2). \tag{1.6}$$

Движение по закону (1.5) описывается в виде

$$x(t) = e^{A_2(t-t_1)} x(t_1 + 0),\ t_1 < t \le t_2.$$

И в момент $t = t_2$ оно имеет вид

$$x(t_2) = e^{A_2(t_2 - t_1)} x(t_1 + 0) = e^{A_2(t_2 - t_1)} B_1 e^{A_1(t_1 - t_0)} x(0).$$

Далее идет переключение по закону (1.6) и в момент $t = t_2 + 0$ оно имеет вид

$$x(t_2 + 0) = B_2 e^{A_2(t_2 - t_1)} B_1 e^{A_1(t_1 - t_0)} x(0).$$

Продолжая процесс дальше, получаем, что в момент $t = t_k + 0$ решение системы с переключениями имеет вид

$$x(t_k + 0) = \prod_{i=0}^{k-1} B_k e^{A_k(t_{k-i} - t_{k-i-1})} x(0).$$

Если рассматривать момент времени $t_k < t \le t_{k+1}$, то решение имеет вид

$$x(t) = e^{A_{k+1}(t-t_k)} \prod_{i=0}^{k-1} B_{k-i} e^{A_{k-i}(t_{k-i} - t_{k-i-1})} x(0).$$

Таким образом, чтобы выполнялось условие устойчивости, сформулированное в определении 1.1, необходимо и достаточно, чтобы для произвольного $\varepsilon > 0$, произвольных моментов переключения $t_0 < t_1 < t_2 < ... < t_k < ...$ и $t > t_k$, $k = 1,2,3,...$ выполнялись неравенства

$$\delta(\varepsilon) < \frac{\varepsilon}{\left| \prod_{i=0}^{k-1} B_{k-i} e^{A_{k-i}(t_{k-i} - t_{k-i-1})} \right|},\ \delta(\varepsilon) < \frac{\varepsilon}{\left| e^{A_{k+1}(t-t_k)} \prod_{i=0}^{k-1} B_{k-i} e^{A_{k-i}(t_{k-i} - t_{k-i-1})} \right|}.$$

Отсюда следует утверждение теоремы 1.1.

2. Использование второго метода Ляпунова. К сожалению, условия асимптотической устойчивости, сформулированные в теореме 1.1, проверяются тяжело. Они требуют явного представления решений дифференциальных и разностных систем и их "склейки".

Одним из основных методов исследования устойчивости дифференциальных и разностных систем в отдельности является второй метод Ляпунова [1–4]. Он состоит в поиске положительно определенной функции $V(x)$, полная производная которой в силу системы (для разностных систем – первая разность в силу системы) будет отрицательно определенной. Для линейных систем функция Ляпунова, как правило, ищется в виде квадратичной формы $V(x) = x^T Hx$.

Очевидно, достаточным условием асимптотической устойчивости системы с переключениями (1.1), (1.2) будет существование единой функции Ляпунова для системы в целом. Как известно, асимптотическая устойчивость для каждой из дифференциальных систем (1) гарантируется наличием положительно определенной квадратичной формы $V(x) = x^T Hx$, полная производная которой в силу каждой из систем является отрицательно определенной квадратичной формой. Поскольку

$$\frac{d}{dt}V(x) = x^T\left(A^T H + HA\right)x,$$

то асимптотическая устойчивость каждой из подсистем гарантируется существованием положительно определенных матриц C_i, при которых матричные уравнения Ляпунова

$$A_i^T H_i + H_i A_i = -C_i,\ i = 1,2,3,... \tag{4}$$

имеют решениями положительно определенные матрицы H_i, $i = 1,2,3,...$.

Для разностных систем (2), аналогично, асимптотическая устойчивость каждой из подсистем гарантируется существованием положительно определенных матриц C_i, при которых матричные уравнения Ляпунова

$$B_i^T H_i B_i - H_i = -C_i,\ i = 1,2,3,...$$

имеют решениями положительно определенные матрицы H_i.

И, естественно, встает вопрос, при каких условиях существует единая матрица H, при которой соответствующие матрицы $C_i(A_i)$, $C_i(B_i)$ также будут отрицательно определенными [5,6].

2.1. Общая функция Ляпунова для дифференциальных систем.

Приведем некоторые вспомогательные утверждения [7].

Лемма 2.1. Пусть матрица A асимптотически устойчива (в смысле линейного дифференциального уравнения, т.е. все ее собственные числа имеют отрицательную действительную часть $\mathrm{Re}\,\lambda_i(A) < 0$, $i = \overline{1,n}$). Тогда множество $G_A(H)$ положительно определенных матриц H, для которых матрицы $C = -A^T H - HA$ также положительно определенные, образуют выпуклый конус в пространстве $R^{n\times n}$.

Доказательство. Пусть H_1 и H_2 две положительно определенные матрицы, при которых матрицы $C_1 = -A^T H_1 - H_1 A$, $C_2 = -A^T H_2 - H_2 A$ также положительно определены. А тогда при произвольном $0 \le \alpha \le 1$ матрица $\alpha H_1 + (1-\alpha)H_2$ также будет положительно определенной. Кроме того, матрица

$$-A^T\left(\alpha H_1 + (1-\alpha H_2)\right) - \left(\alpha H_1 + (1-\alpha)H_2\right)A =$$
$$= -\alpha\left(A^T H_1 + H_1 A\right) - (1-\alpha)\left(A^T H_2 - H_2 A\right) = \alpha C_1 + (1-\alpha)C_2$$

также будет положительно определенной. Таким образом, множество положительно определенных матриц H образует выпуклое множество. Кроме того, в силу однородности, при произвольном $0 < \beta < \infty$ матрицы βH также будут положительно определенными и такими, что

$$C(\beta) = -A^T(\beta H) - (\beta H)A = -\beta\left(A^T H + HA\right)$$

будут положительно определенными. Следовательно, множество $G_A(H)$ образует выпуклый конус.

Предварительно получим достаточные условия, при выполнении которых существует единая функция Ляпунова для подсистем дифференциальных уравнений.

Рассмотрим линейные стационарные дифференциальные уравнения (1.1)

$$x'(t) = A_i x(t),\ i = \overline{1,n}.$$

Если матрицы A_i, $i = \overline{1,n}$ асимптотически устойчивые, то для произвольных положительно определенных матриц C_i, $i = \overline{1,n}$ матричные уравнения

$$A_i^T H + HA_i = -C_i \tag{2.1}$$

имеют единственными решениями – положительно определенные матрицы H_i, $i = \overline{1,n}$. Рассмотрим алгоритм построения общей функции Ляпунова, т.е. нахождения положительно определенной матрицы H_0, при которой все матрицы C_i^0 также будут положительно определенными.

Обозначим

$$C_{ij} = A_i^T H_j + H_j A_i,\ i \ne j. \tag{2.2}$$

Теорема 2.1. Пусть C_i, $i=\overline{1,n}$ положительно определенные матрицы и H_i соответствующие решения уравнений Ляпунова. Если существуют постоянные $0\le\alpha_i\le 1$, $i=\overline{1,n-1}$, при которых матрицы

$$C_1(\alpha_1,\alpha_2,...\alpha_{n-1})=\alpha_1\alpha_2\alpha_3...\alpha_{n-1}C_1-(1-\alpha_1)\alpha_2\alpha_3...\alpha_{n-1}C_{12}-(1-\alpha_2)\alpha_3\alpha_4...\alpha_{n-1}C_{13}-...$$
$$-(1-\alpha_{n-2})\alpha_{n-1}C_{1,n-1}-(1-\alpha_{n-1})C_{1,n},$$
$$C_2(\alpha_1,\alpha_2,...\alpha_{n-1})=-\alpha_1\alpha_2\alpha_3...\alpha_{n-1}C_{21}+(1-\alpha_1)\alpha_2\alpha_3...\alpha_{n-1}C_2-(1-\alpha_2)\alpha_3\alpha_4...\alpha_{n-1}C_{23}-...$$
$$-(1-\alpha_{n-2})\alpha_{n-1}C_{2,n-1}-(1-\alpha_{n-1})C_{2,n}.$$
$$C_n(\alpha_1,\alpha_2,...\alpha_{n-1})=-\alpha_1\alpha_2\alpha_3...\alpha_{n-1}C_{n,1}-(1-\alpha_1)\alpha_2\alpha_3...\alpha_{n-1}C_{n,2}-(1-\alpha_2)\alpha_3\alpha_4...\alpha_{n-1}C_{n3}-...$$
$$-(1-\alpha_{n-2})\alpha_{n-1}C_{n,n-1}+(1-\alpha_{n-1})C_n. \qquad (2.3)$$

также положительно определены, то для систем (1.1) существует единая функция Ляпунова и она имеет вид $V(x)=x^TH(\alpha_1,\alpha_2,...\alpha_{n-1})x$, где

$$H(\alpha_1,\alpha_2,\alpha_3,...,\alpha_{n-1})=$$
$$=\alpha_1\alpha_2\alpha_3...\alpha_{n-1}H_1+(1-\alpha_1)\alpha_2\alpha_3...\alpha_{n-1}H_2+...+(1-\alpha_2)\alpha_3\alpha_4...\alpha_{n-1}H_3+....$$
$$+(1-\alpha_{n-2})\alpha_{n-1}H_{n-1}+(1-\alpha_{n-1})H_n. \qquad (2.4)$$

Доказательство. Как следует из леммы 2.1, для асимптотически устойчивых матриц A_i множество положительно определенных матриц H_i, при которых линейные комбинации $C_i=-A_i^TH-HA_i$ также положительно определены, образуют выпуклые конусы $G_{A_i}(H)$, $i=\overline{1,n}$. И общая функция Ляпунова существует тогда и только тогда, когда эти конуса имеют непустое пересечение.

Рассмотрим первые две матрицы H_1 и H_2 входящие в конусы $G_{A_1}(H)$, $G_{A_2}(H)$ и построим третью матрицу, расположенную на прямой, соединяющей эти две матрицы.

$$H(\alpha_1)=\alpha_1H_1+(1-\alpha_1)H_2. \qquad (2.5)$$

Если общая функция Ляпунова для первой и второй подсистем существует, то, в силу выпуклости конусов, всегда имеются матрицы H_1 и H_2 и параметр $0\le\alpha_1\le 1$, такие, что общая функция Ляпунова может быть представленной в виде (2.5).

Рассмотрим третью подсистему. Если она асимптотически устойчива, то существует матица H_3, входящая в конус положительно определенных матриц $G_{A_3}(H)$. Построим матрицу $H(\alpha_1,\alpha_2)$ расположенную на отрезке прямой, соединяющей $H(\alpha_1)$ и H_3:

$$H(\alpha_1,\alpha_2)=\alpha_2H(\alpha_1)+(1-\alpha_2)H_3=$$
$$=\alpha_2\left[\alpha_1H_1+(1-\alpha_1)H_2\right]+(1-\alpha_2)H_3=\alpha_1\alpha_2H_1+(1-\alpha_1)\alpha_2H_2+(1-\alpha_2)H_3,\ 0\le\alpha_2\le 1.$$

Рассмотрим четвертую подсистему. Если она асимптотически устойчива, то существует матица H_4, входящая в $G_{A_4}(H)$. Построим матрицу $H(\alpha_1,\alpha_2)$ расположенную на отрезке прямой, соединяющей $H(\alpha_1)$ и H_3:

$$H(\alpha_1,\alpha_2,\alpha_3)=\alpha_3H(\alpha_1,\alpha_2)+(1-\alpha_3)H_4=$$
$$=\alpha_3\left[\alpha_1\alpha_2H_1+(1-\alpha_1)\alpha_2H_2+(1-\alpha_2)H_3\right]+(1-\alpha_3)H_4=$$
$$=\alpha_1\alpha_2\alpha_3H_1+(1-\alpha_1)\alpha_2\alpha_3H_2+(1-\alpha_2)\alpha_3H_3+(1-\alpha_3)H_4.$$

Рассмотрим последнюю n – подсистему. Аналогично получим

$$H(\alpha_1,\alpha_2,\alpha_3,...,\alpha_{n-1})=$$
$$=\alpha_1\alpha_2\alpha_3...\alpha_{n-1}H_1+(1-\alpha_1)\alpha_2\alpha_3...\alpha_{n-1}H_2+...+(1-\alpha_2)\alpha_3\alpha_4...\alpha_{n-1}H_3+....$$
$$+(1-\alpha_{n-2})\alpha_{n-1}H_{n-1}+(1-\alpha_{n-1})H_n.$$

Получим условия, при выполнении которых полученная матрица будет общей для всех подсистем.

Условием того, что полученная таким образом матрица будет матрицей функции Ляпунова для первой подсистемы, есть положительная определенность матрицы

$$C_1(\alpha_1,\alpha_2,...\alpha_{n-1})=-A_1^TH(\alpha_1,\alpha_2,...,\alpha_{n-1})-H(\alpha_1,\alpha_2,...,\alpha_{n-1})A_1=$$
$$=-\alpha_1\alpha_2\alpha_3...\alpha_{n-1}\left(A_1^TH_1+H_1A_1\right)-(1-\alpha_1)\alpha_2\alpha_3...\alpha_{n-1}\left(A_1^TH_2+HA_1\right)-$$
$$-(1-\alpha_2)\alpha_3\alpha_4...\alpha_{n-1}\left(A_1^TH_3+H_3A_1\right)+...$$
$$-(1-\alpha_{n-2})\alpha_{n-1}\left(A_1^TH_{n-1}-H_{n-1}A_1\right)-(1-\alpha_{n-1})\left(A_1^TH_n+H_nA_1\right).$$

Поскольку первое выражение определяется уравнением Ляпунова для первой подсистемы, то

$$C_1(\alpha_1,\alpha_2,...\alpha_{n-1})=\alpha_1\alpha_2\alpha_3...\alpha_{n-1}C_1-(1-\alpha_1)\alpha_2\alpha_3...\alpha_{n-1}\left(A_1^TH_2+H_2A_1\right)-$$
$$-(1-\alpha_2)\alpha_3\alpha_4...\alpha_{n-1}\left(A_1^TH_3+H_3A_1\right)+...$$
$$-(1-\alpha_{n-2})\alpha_{n-1}\left(A_1^TH_{n-1}-H_{n-1}A_1\right)-(1-\alpha_{n-1})\left(A_1^TH_n+H_nA_1\right).$$

Аналогично, можно получить, что условием того, что полученная матрица будет матрицей функции Ляпунова для второй подсистемы, будет положительная определенность матрицы

$$C_2(\alpha_1,\alpha_2,...\alpha_{n-1}) = -A_2^T H(\alpha_1,\alpha_2,...,\alpha_{n-1}) - H(\alpha_1,\alpha_2,...,\alpha_{n-1})A_2 =$$
$$= -\alpha_1\alpha_2\alpha_3...\alpha_{n-1}\left(A_2^T H_1 + H_1 A_2\right) - (1-\alpha_1)\alpha_2\alpha_3...\alpha_{n-1}\left(A_2^T H_2 + H_2 A_2\right) -$$
$$-(1-\alpha_2)\alpha_3\alpha_4...\alpha_{n-1}\left(A_2^T H_3 + H_3 A_2\right) + ...$$
$$-(1-\alpha_{n-2})\alpha_{n-1}\left(A_2^T H_{n-1} - H_{n-1}A_2\right) - (1-\alpha_{n-1})\left(A_2^T H_n + H_n A_2\right).$$

Или

$$C_2(\alpha_1,\alpha_2,...\alpha_{n-1}) = -\alpha_1\alpha_2\alpha_3...\alpha_{n-1}\left(A_2^T H_1 + H_1 A_2\right) + (1-\alpha_1)\alpha_2\alpha_3...\alpha_{n-1}C_2 -$$
$$-(1-\alpha_2)\alpha_3\alpha_4...\alpha_{n-1}\left(A_2^T H_3 + H_3 A_2\right) - ...$$
$$-(1-\alpha_{n-2})\alpha_{n-1}\left(A_2^T H_{n-1} - H_{n-1}A_2\right) - (1-\alpha_{n-1})\left(A_2^T H_n + H_n A_2\right).$$

Для последней подсистемы получаем

$$C_n(\alpha_1,\alpha_2,...\alpha_{n-1}) = -\alpha_1\alpha_2\alpha_3...\alpha_{n-1}\left(A_n^T H_1 + H_1 A_n\right) - (1-\alpha_1)\alpha_2\alpha_3...\alpha_{n-1}\left(A_n^T H_2 + HA_n\right) -$$
$$-(1-\alpha_2)\alpha_3\alpha_4...\alpha_{n-1}\left(A_n^T H_3 + H_3 A_n\right) - ... -(1-\alpha_{n-2})\alpha_{n-1}\left(A_n^T H_{n-1} - H_{n-1}A_n\right) + (1-\alpha_{n-1})C_n.$$

Обозначим

$$C_{ij} = A_i^T H_j + H_j A_i, \quad i \neq j.$$

Тогда

$$C_1(\alpha_1,\alpha_2,...\alpha_{n-1}) = \alpha_1\alpha_2\alpha_3...\alpha_{n-1}C_1 - (1-\alpha_1)\alpha_2\alpha_3...\alpha_{n-1}C_{12} - (1-\alpha_2)\alpha_3\alpha_4...\alpha_{n-1}C_{13} - ...$$
$$-(1-\alpha_{n-2})\alpha_{n-1}C_{1,n-1} - (1-\alpha_{n-1})C_{1,n},$$
$$C_2(\alpha_1,\alpha_2,...\alpha_{n-1}) = -\alpha_1\alpha_2\alpha_3...\alpha_{n-1}C_{21} + (1-\alpha_1)\alpha_2\alpha_3...\alpha_{n-1}C_2 - (1-\alpha_2)\alpha_3\alpha_4...\alpha_{n-1}C_{23} - ...$$
$$-(1-\alpha_{n-2})\alpha_{n-1}C_{2,n-1} - (1-\alpha_{n-1})C_{2,n}.$$

……………………………………………………………………………..

$$C_n(\alpha_1,\alpha_2,...\alpha_{n-1}) = -\alpha_1\alpha_2\alpha_3...\alpha_{n-1}C_{n,1} - (1-\alpha_1)\alpha_2\alpha_3...\alpha_{n-1}C_{n,2} - (1-\alpha_2)\alpha_3\alpha_4...\alpha_{n-1}C_{n3} - ...$$
$$-(1-\alpha_{n-2})\alpha_{n-1}C_{n,n-1} + (1-\alpha_{n-1})C_n.$$

Отсюда следует утверждение теоремы 2.1.

2.2. Единая функция Ляпунова для разностных подсистем. Получим достаточные условия, при выполнении которых существует единая функция Ляпунова для подсистем разностных уравнений. Рассмотрим уравнения (1.2)

$$x(k+1) = B_i x(k), \quad k = 0,1,2,3,..., \quad i = \overline{1,n}.$$

Если матрицы B_i, $i = \overline{1,n}$ асимптотически устойчивые, т.е. $\left|\lambda_i(B_j)\right| < 1$, $i = \overline{1,n}$, $j = \overline{1,n}$ то для произвольных положительно определенных матриц C_i, $i = \overline{1,n}$ матричные уравнения

$$B_i^T H B_i - H = -C_i \tag{2.6}$$

имеют единственными решениями – положительно определенные матрицы H_i, $i = \overline{1,n}$. Рассмотрим алгоритм построения общей функции Ляпунова,

Лемма 2.2. Пусть матрица B асимптотически устойчива (в смысле линейного разностного уравнения, т.е. все ее собственные числа матрицы B по модулю меньше единицы, или $\left|\lambda_i(A)\right| < 1$, $i = \overline{1,n}$). Тогда множество $S_B(H)$ положительно определенных матриц H, для которых матрицы $H - B^T HB$ также положительно определенные, образуют выпуклый конус в пространстве $R^{n\times n}$.

Доказательство. Пусть H_1 и H_2 две положительно определенные матрицы, при которых матрицы $C_1 = H_1 - B^T H_1 B$, $C_2 = H_2 - B^T H_2 B$ также положительно определены. А тогда при произвольном $0 \le \alpha \le 1$ матрицы $\alpha H_1 + (1-\alpha)H_2$ также будут положительно определенными. Кроме того, матрица

$$\left(\alpha H_1 + (1-\alpha H_2)\right) - B^T\left(\alpha H_1 + (1-\alpha)H_2\right)B =$$
$$= \alpha\left(H_1 - B^T H_1 B\right) + (1-\alpha)\left(H_2 - B^T H_2 B\right) = \alpha C_1 + (1-\alpha)C_2$$

также будет положительно определенной. Таким образом, множество положительно определенных матриц H образует выпуклое множество. Кроме того, в силу однородности, при $0 < \beta < \infty$ матрицы βH также будут положительно определенными и такими, что

$$C(\beta) = (\beta H) - B^T(\beta H)B = \beta\left(H - B^T HB\right)$$

также положительно определены. Следовательно, как и в лемме 2.1., множество $S_B(H)$ образует выпуклый конус.

Обозначим

$$C_{ij} = H_j - B_i H_j B_i, \quad i \neq j. \tag{2.7}$$

Теорема 2.2. Пусть C_i, $i = \overline{1,n}$ положительно определенные матрицы и H_i соответствующие решения уравнений Ляпунова. Если существуют постоянные $0 \le \alpha_i \le 1$, $i = \overline{1,n}$, при которых матрицы

$$C_1(\alpha_1,\alpha_2,...\alpha_{n-1}) = \alpha_1\alpha_2\alpha_3...\alpha_{n-1}C_1 - (1-\alpha_1)\alpha_2\alpha_3...\alpha_{n-1}C_{12} - (1-\alpha_2)\alpha_3\alpha_4...\alpha_{n-1}C_{13} - ...$$
$$-(1-\alpha_{n-2})\alpha_{n-1}C_{1n-1} - (1-\alpha_{n-1})C_{1n},$$
$$C_2(\alpha_1,\alpha_2,...\alpha_{n-1}) = -\alpha_1\alpha_2\alpha_3...\alpha_{n-1}C_{21} + (1-\alpha_1)\alpha_2\alpha_3...\alpha_{n-1}C_2 - (1-\alpha_2)\alpha_3\alpha_4...\alpha_{n-1}C_{23} - ...$$
$$-(1-\alpha_{n-2})\alpha_{n-1}C_{2,n-1} - (1-\alpha_{n-1})C_{2,n}.$$
$$C_n(\alpha_1,\alpha_2,...\alpha_{n-1}) = -\alpha_1\alpha_2\alpha_3...\alpha_{n-1}C_{n,1} - (1-\alpha_1)\alpha_2\alpha_3...\alpha_{n-1}C_{n,2} - (1-\alpha_2)\alpha_3\alpha_4...\alpha_{n-1}C_{n3} - ...$$
$$-(1-\alpha_{n-2})\alpha_{n-1}C_{n,n-1} + (1-\alpha_{n-1})C_n. \quad (2.8)$$

также положительно определены, то для систем (1) существует единая функция Ляпунова и она имеет вид $V(x) = x^T H(\alpha_1,\alpha_2,...\alpha_{n-1})x$, где

$$H(\alpha_1,\alpha_2,\alpha_3,...,\alpha_n) =$$
$$= \alpha_1\alpha_2\alpha_3...\alpha_{n-1}H_1 + (1-\alpha_1)\alpha_2\alpha_3...\alpha_{n-1}H_2 + ... + (1-\alpha_2)\alpha_3\alpha_4...\alpha_{n-1}H_3 + ...$$
$$+(1-\alpha_{n-2})\alpha_{n-1}H_{n-1} + (1-\alpha_{n-1})H_n. \quad (2.9)$$

Доказательство. Схема доказательства теоремы 3 аналогична схеме доказательства предыдущей теоремы. Как следует из леммы 2.2, для асимптотически устойчивых матриц B_i множество положительно определенных матриц H_i, при которых линейные комбинации $C_i = H - B_i^T H B_i$ также положительно определены, образуют выпуклые конусы $G_{B_i}(H)$, $i = \overline{1,n}$. И общая функция Ляпунова существует тогда и только тогда, когда эти конуса имеют непустое пересечение.

Рассмотрим матрицы H_1 и H_2 водящие в первые два конуса $S_{B_1}(H)$, $S_{B_2}(H)$ и построим третью матрицу, расположенную на прямой, соединяющей эти две матрицы.

$$H(\alpha_1) = \alpha_1 H_1 + (1-\alpha_1)H_2. \quad (3)$$

Если общая функция Ляпунова для первой и второй подсистем существует, то, в силу выпуклости конусов, всегда имеются матрицы H_1 и H_2 и параметр $0 \le \alpha_1 \le 1$, такие, что общая функция Ляпунова может быть представленной в виде (3).

Рассмотрим третью подсистему. Если она асимптотически устойчива, то существует матица H_3, входящая в конус положительно определенных матриц $G_{A_3}(H)$. Построим матрицу $H(\alpha_1,\alpha_2)$ расположенную на отрезке прямой, соединяющей $H(\alpha_1)$ и H_3:

$$H(\alpha_1,\alpha_2) = \alpha_2 H(\alpha_1) + (1-\alpha_2)H_3 =$$
$$= \alpha_2\left[\alpha_1 H_1 + (1-\alpha_1)H_2\right] + (1-\alpha_2)H_3 = \alpha_1\alpha_2 H_1 + (1-\alpha_1)\alpha_2 H_2 + (1-\alpha_2)H_3,\ 0 \le \alpha_2 \le 1.$$

Рассмотрим последнюю n – подсистему. Аналогично случаю дифференциальных систем получим

$$H(\alpha_1,\alpha_2,\alpha_3,...,\alpha_{n-1}) =$$
$$= \alpha_1\alpha_2\alpha_3...\alpha_{n-1}H_1 + (1-\alpha_1)\alpha_2\alpha_3...\alpha_{n-1}H_2 + ... + (1-\alpha_2)\alpha_3\alpha_4...\alpha_{n-1}H_3 + ...$$
$$+(1-\alpha_{n-2})\alpha_{n-1}H_{n-1} + (1-\alpha_{n-1})H_n.$$

Получим условия, при выполнении которых полученная матрица будет общей для всех подсистем.

Условием того, что полученная матрица будет матрицей функции Ляпунова для первой подсистемы, есть положительная определенность матрицы

$$C_1(\alpha_1,\alpha_2,...\alpha_{n-1}) = H(\alpha_1,\alpha_2,...,\alpha_{n-1}) - B_1^T H(\alpha_1,\alpha_2,...,\alpha_{n-1})B_1 =$$
$$= \alpha_1\alpha_2\alpha_3...\alpha_{n-1}(H_1 - B_1^T H_1 B_1) + (1-\alpha_1)\alpha_2\alpha_3...\alpha_{n-1}(H_2 - B_1 H_2 B_1) -$$
$$-(1-\alpha_2)\alpha_3\alpha_4...\alpha_{n-1}(H_3 - B_1^T H_3 B_1) + ...$$
$$-(1-\alpha_{n-2})\alpha_{n-1}(H_{n-1} - B_1 H_{n-1} B_1) - (1-\alpha_{n-1})(H_n - B_1 H_n B_1).$$

Поскольку первое выражение определяется уравнением Ляпунова для первой подсистемы, то

$$C_1(\alpha_1,\alpha_2,...\alpha_{n-1}) = \alpha_1\alpha_2\alpha_3...\alpha_{n-1}C_1 - (1-\alpha_1)\alpha_2\alpha_3...\alpha_{n-1}(H_2 - B_1 H_2 B_1) -$$
$$-(1-\alpha_2)\alpha_3\alpha_4...\alpha_{n-1}(H_3 - B_1^T H_3 B_1) + ...$$
$$+(1-\alpha_{n-2})\alpha_{n-1}(H_{n-1} - B_1 H_{n-1} B_1) + (1-\alpha_{n-1})(H_n - B_1^T H_n B_1).$$

Далее, условием того, что полученная матрица будет матрицей функции Ляпунова для второй подсистемы, будет положительная определенность матрицы

$$C_2(\alpha_1,\alpha_2,...\alpha_{n-1}) = H(\alpha_1,\alpha_2,...,\alpha_{n-1}) - B_2^T H(\alpha_1,\alpha_2,...,\alpha_{n-1})B_2 =$$
$$= \alpha_1\alpha_2\alpha_3...\alpha_{n-1}(H_1 - B_2^T H_1 B_2) + (1-\alpha_1)\alpha_2\alpha_3...\alpha_{n-1}(H_2 - B_2^T H_2 B_2) +$$
$$-(1-\alpha_2)\alpha_3\alpha_4...\alpha_{n-1}(H_3 - B_2^T H_3 B_2) + ...$$
$$-(1-\alpha_{n-2})\alpha_{n-1}(H_{n-1} - B_2^T H_{n-1} B_2) - (1-\alpha_{n-1})(H_n - B_2^T H_n B_2).$$

Или

$$C_2(\alpha_1,\alpha_2,...\alpha_{n-1}) = -\alpha_1\alpha_2\alpha_3...\alpha_{n-1}(A_2^T H_1 + H_1 A_2) + (1-\alpha_1)\alpha_2\alpha_3...\alpha_{n-1}C_2 -$$

$$-\left(1-\alpha_2\right)\alpha_3\alpha_4...\alpha_{n-1}\left(A_2^T H_3 + H_3 A_2\right)-...$$
$$-\left(1-\alpha_{n-2}\right)\alpha_{n-1}\left(A_2^T H_{n-1} - H_{n-1}A_2\right)-\left(1-\alpha_{n-1}\right)\left(A_2^T H_n + H_n A_2\right).$$

Для последней подсистемы получаем

$$C_n\left(\alpha_1,\alpha_2,...\alpha_{n-1}\right) = -\alpha_1\alpha_2\alpha_3...\alpha_{n-1}\left(A_n^T H_1 + H_1 A_n\right)-\left(1-\alpha_1\right)\alpha_2\alpha_3...\alpha_{n-1}\left(A_n^T H_2 + HA_n\right)-$$
$$-\left(1-\alpha_2\right)\alpha_3\alpha_4...\alpha_{n-1}\left(A_n^T H_3 + H_3 A_n\right)-...-\left(1-\alpha_{n-2}\right)\alpha_{n-1}\left(A_n^T H_{n-1} - H_{n-1}A_n\right)+\left(1-\alpha_{n-1}\right)C_n.$$

Обозначим

$$C_{ij} = H_j - B_i^T H_j B_i, \quad i \neq j.$$

Тогда

$$C_1\left(\alpha_1,\alpha_2,...\alpha_{n-1}\right) = \alpha_1\alpha_2\alpha_3...\alpha_{n-1}C_1 - \left(1-\alpha_1\right)\alpha_2\alpha_3...\alpha_{n-1}C_{12} - \left(1-\alpha_2\right)\alpha_3\alpha_4...\alpha_{n-1}C_{13}-...$$
$$-\left(1-\alpha_{n-2}\right)\alpha_{n-1}C_{1,n-1} - \left(1-\alpha_{n-1}\right)C_{1,n},$$
$$C_2\left(\alpha_1,\alpha_2,...\alpha_{n-1}\right) = -\alpha_1\alpha_2\alpha_3...\alpha_{n-1}C_{21} + \left(1-\alpha_1\right)\alpha_2\alpha_3...\alpha_{n-1}C_2 - \left(1-\alpha_2\right)\alpha_3\alpha_4...\alpha_{n-1}C_{23}-...$$
$$-\left(1-\alpha_{n-2}\right)\alpha_{n-1}C_{2,n-1} - \left(1-\alpha_{n-1}\right)C_{2,n}.$$

……………………………………………………………………………..

$$C_n\left(\alpha_1,\alpha_2,...\alpha_{n-1}\right) = -\alpha_1\alpha_2\alpha_3...\alpha_{n-1}C_{n,1} - \left(1-\alpha_1\right)\alpha_2\alpha_3...\alpha_{n-1}C_{n,2} - \left(1-\alpha_2\right)\alpha_3\alpha_4...\alpha_{n-1}C_{n3}-...$$
$$-\left(1-\alpha_{n-2}\right)\alpha_{n-1}C_{n,n-1} + \left(1-\alpha_{n-1}\right)C_n.$$

И получаем утверждение теоремы 2.2.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Малкин И.Г. Теория устойчивости движения. М., Наука, 1965. – 530 с.
2. Демидович Б.П. Лекции по математической теории устойчивости. – М., Наука, 1967. –
3. Халанай А., Векслер Д. Качественная теория импульсных систем. – М., Мир, 1971. – 309 с.
4. Мартынюк Д.И. Лекции по качественной теории разностных уравнений. – Киев, Наукова думка, 1972. – 246 с.
5. Сиренко А.С. Об одном алгоритме нахождения единой функции Ляпунова двух линейных разностных систем // Вісник Київського національного університету імені Тараса Шевченка. Серія: Фізико-математичні науки, в.1, 2014. – С 107-113.
6. Сиренко А.С., Хусаинов Д. Я. О существовании единой функции Ляпунова для линейных стационарных систем // Вісник Київського національного університету імені Тараса Шевченка. Серія: Кібернетика, в.13, 2013. – С 46-51.
7. Хусаинов Д.Я., Кожаметов А.Т., Утебаев Д. Оптимизация оценок характеристик решений в линамике систем. – Нукус, МВ и ССО Республики Узбекистан, 1992. – 138 с.

Надійшла до редколегії 15.09.14

Хусаїнов Д. Я., д-р фіз.-мат. наук,
Сіренко А. С., асп.,
Київський національний університет імені Тараса Шевченка, Київ

ПРО СТІЙКІСТЬ ЛІНІЙНИХ СИСТЕМ З ПЕРЕМИКАННЯМ

У даний роботі будуть розглядатися лінійні диференціальні системи з лінійними законами перемикання. Одержано умови стійкості їх рішень.
Ключові слова: стійкість, різницеві системи, перемикання, метод Ляпунова.

Khusainov D. Ya., Dr. Sc. phys. math. Professor,
Sirenko A. S., graduate,
Taras Shevchenko National University of Kiev

STABILITY OF LINEAR SYSTEMS WITH SWITCHING

In this paper we consider linear differential systems with linear laws change. Stability conditions of their decisions.
Keywords: stability, difference systems, switching, Lyapunov method.

УДК 517.929

V.O. Yatsenko, Professor, O. I. Kochkodan, PhD student
M. V. Makarychev, , PhD student,O. A. Turovsky student
Space Research Institute NASU-SSAU, Kyiv

ADAPTIVE CONTROL OF LYAPUNOV EXPONENTS

A new approach to adaptive control of local Lyapunov exponents is considered. A numerical optimization algorithm to determine the spectrum of Lyapunov exponents from the observed noise time series of a single variable is proposed. The approach is tested on non-linear lattice with known Lyapunov spectra.

Keywords: adaptive control, Lyapunov exponent, optimization, modeling

1. Optimization approach to estimation of Lyapunov exponents

Let us consider an observed trajectory $x(t)$, which can be considered as a solution of a certain dynamical system:

$$\dot{x} = F(x), \tag{1}$$

where $u \in U \subset R^n$, $x \in M$ – smooth manifold, and is defined in a *d*-dimensional space. On the other hand, the evolution of the tangent vector γ in a tangent space at $x(t)$ is represented by linearizing Eq. (1),

$$\dot{\gamma} = S\left(x(t)\right)\cdot\gamma\,, \tag{2}$$

where $S = DF = \partial F \partial x$ is the Jacobian matrix of F. The solution of the linear nonautonomous Eq. (2) can be obtained as

$$\gamma(t) = A^t \cdot \gamma(0)\,, \tag{3}$$

where A^t is the linear operator which maps tangent vector $\gamma(0)$ to $\gamma(t)$. The mean exponential rate of divergence of the tangent vector γ is defined as follows:

$$\lambda\left(x(0),\gamma(0)\right) = \lim_{t\to\infty}\frac{1}{t}\ln\frac{\left\|\gamma(t)\right\|}{\left\|\gamma(0)\right\|}\,, \tag{4}$$

where $\|...\|$ denotes a norm with respect to some Riemannian metric. Furthermore, there is a *d*-dimensional basis $\{e_i\}$ of $\gamma(0)$, for which λ takes values $\lambda_i\left(x(0)\right) = \lambda\left(x(0), e_i\right)$. These can be ordered by their magnitudes $\lambda_1 \ge \lambda_2 \ge ... \ge \lambda_d$, and are the spectrum of Lyapunov characteristic exponents. These exponents are independent of $x(0)$ if the system is ergodic [1].

We often have no knowledge of the nonlinear equations of the system which produces the observed time series. Moreover, even if we know the equations of motion, such as the Navier-Stokes equations for fluid systems, it is a hard task to derive the mode-truncated equations with finite degrees of freedom from partial differential equations (which is the infinite-dimensional system) and reproduce the same phenomena as the experiment from them. However, there is a possibility of estimating a linearized flow map A^t of tangent space from the observed data.

Let $\{x_j\}$ $(j = 1,2,...)$ denote a time series of some geomagnetic index measured at the discrete time interval Δt, i.e., $x_j = x\left(t_0 + (j-1)\Delta t\right)$. Consider a small ball of radius *r* is centered at the orbital point x_j, and find any set of points $\{x_{k_i}\}$ $(i = 1,2,...,N)$, included in this ball, i.e.,

$$\{y^i\} = \left\{x_{k_i} - x_j \,|\, \left\|x_{k_i} - x_j\right\| \le r\right\}\,, \tag{5}$$

where y_i is the displacement vector between x_{k_i} and x_j. We used a usual Euclidean norm defined as follows: $\|w\| = \left(w_1^2 + w_2^2 + ... + w_d^2\right)^{1/2}$ for some vector $w = (w_1, w_2, ..., w_d)$. After the evolution of a time interval $\tau = m\Delta t$, the orbital point x_j will proceed to x_{j+m} and neighboring points $\{x_{k_i}\}$ to $\{x_{k_i+m}\}$. The displacement vector $y^i = x_{k_i} - x_j$ is mapped to

$$\{z^i\} = \left\{x_{k_i+m} - x_{j+m} \,|\, \left\|x_{k_i} - x_j\right\| \le \varepsilon\right\}\,, \tag{6}$$

If the radius *r* is small enough for the displacement vector y^i and regarded as a good approximation of tangent vectors in the tangent space, evolution of y^i to z^i can be represented by some matrix A_j, as

$$z^i = A_j y^i\,, \tag{7}$$

The matrix A_j is an approximation of the flow map A^τ at x_j in Eq. (3). Let us proceed to the optimal estimation of the linearized flow map A_j from the data sets $\{y^i\}$ and $\{z^i\}$. A plausible procedure for optimal estimation is the least-square-error algorithm, which minimized the average of the squared error norm between z^i and $A_j y^i$ with respect to all components of the matrix A_j as follows [1]:

$$\min_{A_j} S = \min_{A_j}\frac{1}{N}\sum_{i=1}^{N}\left\|z^i - A_j y^i\right\|^2\,. \tag{8}$$

Denoting (k,l) component of matrix A_j by $a_{kl}(j)$ and applying condition (8), one obtains $d\times d$ equations to solve $\partial S / \partial a_{kl}(j) = 0$. One will easily obtain the following expression for A_j:

$$A_j V = C, \quad (V)_{kl} = \frac{1}{N}\sum_{i=1}^{N} y^{ik} y^{il}\,, \tag{9}$$

$$(C)_{kl} = \frac{1}{N}\sum_{i=1}^{N} z^{ik} y^{il}\,,$$

where *V* and *C* are $d\times d$ matrices, called covariance matrices, and y^{ik} and z^{ik} are the *k* **.**

Let us consider a stochastic optimization problem for custom function

$$F(A_i) = E\{S(A_i,\omega\},$$

where ω is an uncertain quantity element of a probability space, and $E\{\bullet\}$ denotes the expectation operations. The problem of minimizing the cost functional *F* subject to constraints on matrix A_j can be viewed as a deterministic optimization problem. In the case where the function F $F(\cdot,\omega)$ is a differentiable function of A_j for each ω, it can be shown under quite general assumption that the gradient of the function *F* exists for each *x* and is given by

$$\nabla F(A_i) = F\left\{\nabla f(A_i,\omega)\right\}\,. \tag{10}$$

To conclude, by using the method we could obtain good estimates of the Lyapunov spectrum from the observed time series in a very systematic way. Because of the ability of the method to measure several Lyapunov exponents, positive, zero, and

even negative ones, other important characteristic invariants such as fractal dimension of attractors of Kolmogorov entropy are obtainable with great ease. It is hoped that the method has wide applicability to systems whose dynamical equations are not available. By definition, chaotic systems display sensitive dependence on initial conditions: two initially close trajectories can diverge exponentially in the phase space with a rate given by the largest Lyapunov exponent [3].

2. Control of Lyapunov exponents. Let us consider the system

$$\dot{x} = f(x, u(t))$$

where $x = (x_1, x_2, ..., x_n)$ are the state variables and $u(t)$ is the parameter, whose value determines the nature of the dynamics

$$\dot{u} = \gamma(S^* - S),$$

where S^* is the target value of some variable S, and the value of γ indicates the stiffness of control.

For the maintenance of a stable fixed point in a discrete dynamical system, the procedure is as follows. The nonlinear system evolves according to the appropriate equation

$$x_{n+1} = f(u, x_n),$$

where u is the parameter to be controlled. If x^* is the required value of x, then the additional equation (for $S \equiv x$)

$$u_{t+1} = u_t + \gamma(x^* - x_t)$$

has the desired effect of tuning the value of u in the way, the dynamics of the combined equation gives $x \to x^*$ over a wide range of initial conditions.

For a one-dimensional discrete dynamical system, the Lyapunov exponent is defined through

$$\lambda = \lim_{N\to\infty} \sum_{i=0}^{N-1} \ln\left|f'(u, x_i)\right|$$

The control equation takes the form

$$u_{t+1} = u_t + \gamma(\lambda^* - \lambda_t)$$

where $\lambda_t = \ln\left|f'(u, x_t)\right|$ is the instantaneous value of the Lyapunov exponent implementation of the methodology in, say, the logistic equation, is direct and the relevant equation are

$$x_{t+1} = u_t x_t (1 - x_t),$$
$$\lambda_t = \ln\left|u_t (1 - 2x_t)\right|,$$
$$u_{t+1} = u_t + \gamma(\lambda^* - \lambda_t)$$

The presented adaptive algorithm, can be used to achieve desired chaotic behavior in nonlinear controlled dynamical systems.

3. Control of Lyapunov exponents in nonlinear lattice. A coupled map lattice is a *N*-dimensional network of interconnected units where each unit evolves in time through a map (or recurrence equation) of the discrete form [3–5]:

$$X^{k+1} = F(X^k), \quad (11)$$

where X^k denotes the field value (*N*-dimensional vector) at the indicated time *k*. In the case of a globally coupled map, with a global (mean field) coupling factor ***e***, the dynamics can be rewritten as:

$$x_n^{k+1} = (1 - \varepsilon) f_n\left[x_n^k\right] + \frac{\varepsilon}{L} \sum_{j=1}^{L} f_j\left[x_j^k\right], \quad (12)$$

where *n* and *j* are the labels of lattice sites ($j \neq n$). The term *L* indicates over how many neighbors we are averaging and it is sometimes referred to as *coordination number*. The local *N*-dimensional map is assumed to be chaotic. Completely synchronous chaotic states are possible with this model when corresponding *N*-dimensional manifolds are attracting or stable. The criterion for stability of this synchronization manifold has been derived in [4]. Further stability analysis of synchronized periodic orbits in coupled map lattices can be found in [5]. Varying ***e*** and *L* we can change the extent of spatial correlations, from systems with local interactions to systems with long-range interactions. These systems typically exhibit spatially and/or temporally chaotic behavior, the control of which is very desirable because of its potential real-life applications. Several strategies have been proposed to control the collective spatiotemporal dynamics of such systems. In this paper we first describe adaptive feedback control strategies for coupled map lattice systems and then describe an optimization technique for choosing optimal feedback parameters.

Experimental studies in rodent models of epilepsy have used EEG recordings from four to six electrodes placed in frontal and temporal regions of the animal brain. We have therefore chosen a CML model with five non-identical logistic maps. The system parameters $б_1 \ldots б_5$ were chosen randomly as 3.9, 3.97, 3.95, 3.965 and 3.96. The coupling term ***e*** was varied from a value of 0.10 to 0.14 to study the dynamical behavior in both the spatial and temporal regimes. Figure 1 shows the changes in spatiotemporal patterns as we increase the value of the parameter ***e***. For illustration purposes we have only shown the amplitude and Lyapunov exponent profiles of the single cell (cell 1). The remaining cells exhibit a similar pattern. As we increase the value of ***e*** gradually as shown in Figure 1D, the amplitude plot, shown in Figure 1A becomes more ordered and we can also see a drop in the Lyapunov exponents (calculated as a running mean) from the same time series, suggesting a more ordered state as illustrated in Figure 1B. Figure 1C shows the mean Lyapunov exponent profile calculated over all 5 cells in the CML [5]. We can observe a gradual fall in the values of this global measure with increasing values of coupling.

Figure 2 illustrates the feedback control strategy also referred to as 'dynamic feedback control' in literature described, for a target $л^* = 0.3$. Since there can be several values of the controlled parameter *б* (corresponding to several different attractors) which gives the desired value of the Lyapunov exponent, the actual value of the controlled parameter takes depends on the stiffness of control, and initial conditions. The fluctuations in the controlled parameter are proportional to the value of the stiffness, converging to a single value for small stiffness while exhibiting large variations for higher values of stiffness.

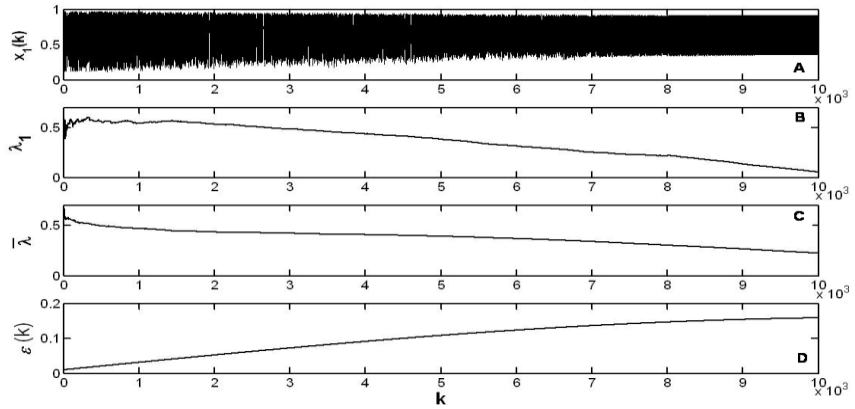

Figure 1. (A) Amplitude spectrum as a function of time; (B) Lyapunov exponent profile of the single cell; (C) Mean Lyapunov exponent profile (L=5) estimated from a five cell CML; (D) parameter e as a function of time

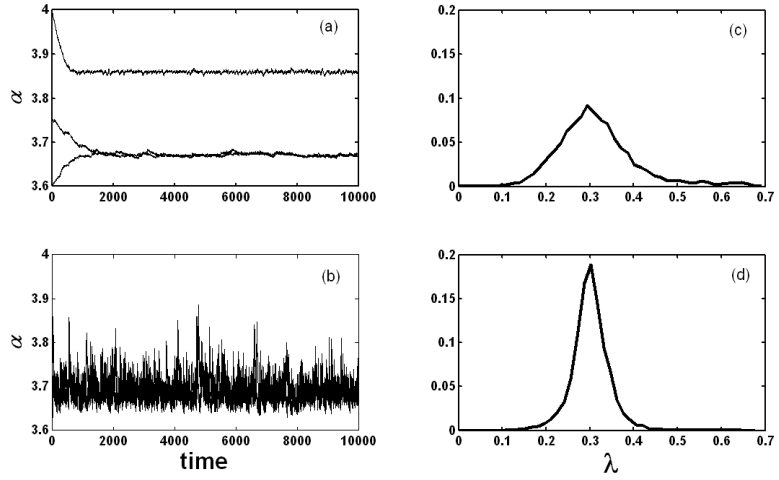

Figure 2. Multiplicative control: of the parameter б as a function of iteration step for л* = 0.3, and stiffness: a) g = 0.001, and b) g = 0.02. The different curves correspond to different initial б. Probability distributions of finite step Lyapunov exponents for б0 = 4.0 and stiffness (c) g = 0.001, and d) g = 0.01

A coupled map lattice system can be used to model the dynamical evolution of Lyapunov exponents in a complex system (Figure 3). The algorithm involves generating an error function between the target Lyapunov exponent profile of the complex system and some nonlinear transformation of estimated lattice Lyapunov exponent values. The error is used to generate an optimized feedback input to the lattice. Such a learning algorithm can be used in developing realistic model of complex system dynamics and hence make the models more useful in the study and control of such complex systems.

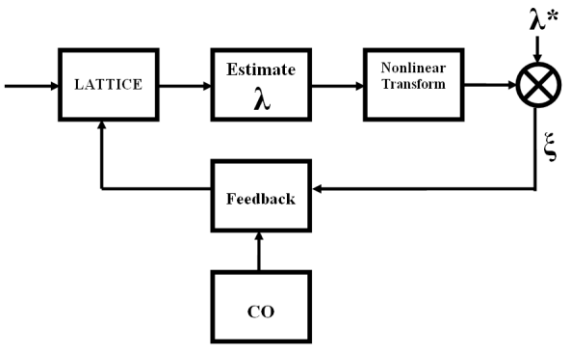

Figure 3. Proposed adaptive learning algorithm for a coupled map lattice via optimized feedback control to emulate the target dynamics of any complex network. CO refers to the constrained optimization block. o refers to error generated from nonlinearly transformed estimates of local Lyapunov exponents and target Lyapunov exponents

References

1. Sano, M., Sawada, Y. Measurement of the Lyapunov Spectrum from a Chaotic Time Series // Physical Review Letter, Vol. 55 (10). 1985 – pp. 1082–1085.
2. Ramaswamy, R., Sinha , Gupte, S. Targeting Chaos through Adaptive Control // Physical Review E, Vol. 57. 1998 – pp. 2507–2510.
3. Yatsenko, V.O., Kochkodan, O.I., Makarychev, M.V., Pashenkovska, I.S, Cheremnikh, S.O. Linear and nonlinear analysis of time series: correlation dimension, Lyapunov exponents, and prediction // Bulletin of Taras Shevchenko National University of Kyiv. Series: Physics & Mathematics, Vol. 4, 2013 – pp. 84–89.
4. Ding, M., Yang., W. Stability of Synchronous Chaos and On-Off Intermittency in Coupled Map Lattice // Physical Review E, Vol. 56. 1997 – pp. 4009–4016.
5. Yatsenko, V.O., Kochkodan, O.I. Modeling and control Lyapunov Exponents in a coupled map lattice // Information Theories and Applications, Vol. 19 (3). 2012 – pp. 216–223.

Надійшла до редколегії 05.09.14

В. О. Яценко, д-р тех. Наук, О. І. Кочкодан, асп., М. В. Макаричев, асп., О. А. Туровський студ.,
Інститут Космічних Досліджень НАНУ-ДКАУ, Київ

АДАПТИВНЕ КЕРУВАННЯ ПОКАЗНИКАМИ ЛЯПУНОВА

Запропоновано підхід до адаптивного керування локальними показниками Ляпунова. Запропоновано чисельний алгоритм визначення спектра показників Ляпунова по спостережуваному зашумленому часовому ряду. Підхід протестовано на прикладі нелінійної гратки з відомим спектром показників Ляпунова.

Ключові слова: адаптивне керування, показники Ляпунова, оптимізація, моделювання.

В. А. Яценко, д-р тех. наук, А. И. Кочкодан, асп., М. В. Макарычев, асп., А. А. Туровский студ.,
Институт Космических Исследований НАНУ-ГКАУ, Киев

АДАПТИВНОЕ УПРАВЛЕНИЕ ПОКАЗАТЕЛЯМИ ЛЯПУНОВА

Предложен подход к адаптивному управлению локальными показателями Ляпунова. Предложен численный алгоритм определения спектра показателей Ляпунова по наблюдаемому зашумленному временному ряду. Подход протестирован на примере нелинейной решетки с известным спектром показателей Ляпунова.

Ключевые слова: адаптивное управление, показатели Ляпунова, оптимизация, моделирование.

Наукове видання

ВІСНИК

КИЇВСЬКОГО НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ ІМЕНІ ТАРАСА ШЕВЧЕНКА

КІБЕРНЕТИКА

Випуск (1)14

Друкується за авторською редакцією

Оригінал-макет виготовлено Видавничо-поліграфічним центром "Київський університет"

Автори опублікованих матеріалів несуть повну відповідальність за підбір, точність наведених фактів, цитат, економіко-статистичних даних, власних імен та інших відомостей. Редколегія залишає за собою право скорочувати та редагувати подані матеріали. Рукописи та дискети не повертаються.

Формат 60x84$^{1/8}$. Ум. друк. арк. 7,4. Наклад 300. Зам. № 214-7214.
Гарнітура Arial. Папір офсетний. Друк офсетний. Вид. № К 1*.
Підписано до друку 30.12.14

Видавець і виготовлювач
Видавничо-поліграфічний центр "Київський університет"
01601, Київ, б-р Т. Шевченка, 14, кімн. 43
☎ (38044) 239 3222; (38044) 239 3172; тел./факс (38044) 239 3128
e-mail: vpc@univ.kiev.ua
http: vpc.univ.kiev.ua
Свідоцтво суб'єкта видавничої справи ДК № 1103 від 31.10.02