Algorithms. http://www.nbuv.gov.ua/Portal/natural/ VNULP/ISM/ 2008_621/01.pdf 5.Овсяк В. Алгоритми: аналіз методів, алгебра впорядкувань, моделі, моделювання. – Львів: Світ, 1996. – 132 с. 6. Овсяк В. Алгоритми: методи побудови, оптимізації, дослідження вірогідності. – Львів: Світ, 2001. – 160 с. 7. Овсяк О. Модель абстрактної підсистеми комп'ютерної інформаційної системи генерування коду /О. Овсяк //Компютерні науки та інформаційні технології. Вісник національного університету Львівська політехніка. – №686. 2010. – С.127 – 136. 8. Бритковський В.М. Моделювання редактора формул секвенційних алгоритмів: автореф. дис. на здобуття наук. ступеня канд. тех. наук: спец. 01.05.02 "Математичне моделювання та обчислювальні методи" / В.М. Бритковський – Львів, 2003. – 18 с. 9. Василюк А.С. Підвищення ефективності математичного і програмного забезпечення редактора формул алгоритмів: автореф. дис. на здобуття наук. ступеня канд. тех. наук: спец. 01.05.02 "Математичне та програмне забезпечення обчислювальних машин і систем" / А.С. Василюк – Львів, 2008. – 20 с. 10. Petzold C. Programowanie Windows w języku C#. –Warszawa: „RM", 2002. – 1161 s. 11. Мэтью Мак-Дональд. Windows presentation foundation в .NET 3.5 с примерами на C# 2008. – М.–СПб.– К.: "Apress", 2008. – 922 с.

УДК 004.852; 004.94

П. Кравець
Національний університет "Львівська політехніка",
кафедра інформаційних систем та мереж

САМООРГАНІЗАЦІЯ СТРАТЕГІЙ СТОХАСТИЧНОЇ ГРИ НА ПРИКЛАДІ ПОБУДОВИ ЛАТИНСЬКИХ КВАДРАТІВ

Досліджується проблема ігрової самоорганізації розподіленої системи на прикладі розв'язування задачі побудови латинських квадратів. Суть самоорганізації полягає у перетворенні локально скоординованих стратегій гравців у глобальну координацію розв'язків стохастичної гри. Сформульовано ігрову задачу, розроблено метод та алгоритм її розв'язування, виконано комп'ютерне моделювання стохастичної гри для побудови ортогональних та звичайних латинських квадратів. Отримано та проаналізовано характеристики самоорганізації стохастичної гри.

Ключові слова: стохастична гра, координація стратегій, самоорганізація системи, латинський квадрат.

The problem of game self-organizing of the distributed system on an example of the problem solving of Latin squares construction is investigated. The essence of self-organizing consists in transformation of the locally-co-ordinated strategies of players to global coordination of stochastic game solution. The game problem is formulated, the method and algorithm of its solution are developed, computer modelling of stochastic game for construction of orthogonal and normal Latin squares is executed. Characteristics of self-organizing of stochastic game are received and analysed.

Keywords: stochastic game, coordination of strategies, self-organization of system, Latin square.

Вступ

Безкоаліаційна стохастична гра – це повторювальна математична гра в умовах невизначеності матриць виграшів, у якій гравці після незалежного випадкового вибору чистих стратегій на основі побудованого на динамічних змішаних стратегіях імовірнісного механізму отримують випадковий виграш (або програш), який використовують для адаптивної модифікації змішаних стратегій так, щоб максимізувати функції середніх виграшів (або мінімізувати функції середніх програшів).

Стохастична гра задається множиною гравців, множинами чистих стратегій та матрицями розподілів випадкових виграшів (або програшів) [1 – 3].

Стохастична гра є ефективним інструментом дослідження колективних процесів конкуренції, взаємодії, кооперації, навчання, координації та самоорганізації систем в умовах невизначеності. Хід розв'язування стохастичної гри можна зобразити у вигляді пошукових траєкторій змішаних стратегій на системі одиничних симплексів до визначених станів колективної рівноваги: Неша, Слейтера, Парето, Джофріона, Байєса, корельованої рівноваги тощо.

Можливість досягнення точок колективної рівноваги визначається координацією дій гравців. З теоретико-ігрового погляду координація – це узгоджений вибір стратегій, що задовольнять умови, накладені на значення функцій виграшів або програшів, отримані у ході їх оптимізації колективом гравців. Колективні рішення є скоординованими, якщо вони задовольняють вимоги вигідності, стійкості та справедливості для усіх учасників прийняття рішень.

Координація ґрунтується на явній або неявній взаємодії між гравцями. За неявної взаємодії гравці поводятьсянезалежно і впливають на вибір стратегій інших гравців зміною станів спільного середовища. За явної або комунікативної взаємодії гравці додатково здійснюють прямий обмін інформацією між собою. Обмін інформації може бути глобальним або у межах локально визначених коаліцій. Гравці можуть обмінюватися отриманими під час гри даними про стани середовища, значеннями функцій виграшів, чистими або змішаними стратегіями.

Координація дій призводить до виникнення умов самоорганізації системи. Самоорганізація – це цілеспрямований процес створення, відтворення, впорядкування або вдосконалення організації (структури та функцій) складної динамічної системи за рахунок внутрішніх факторів, без відповідного зовнішнього впливу [4–8]. Це – здатність колективу гравців з локально-обумовленими зв'язками і цілями досягати стійких скоординованих стратегій поведінки в умовах невизначеності за рахунок самонавчання, здатність функціонувати як єдине ціле та забезпечувати виконання глобальної мети розвитку системи.

Ігрова координація стратегій гравців, яка призводить до самоорганізації системи, є актуальною науково-практичною проблемою, недостатньо вивченою сьогодні. Самоорганізація та складні форми поведінки системи можуть проявлятися при реалізації найпростіших дій гравців. Зовнішніми проявами самоорганізації можуть бути утворення впорядкованих структур, скоординованих дій агентів та властивість емерджентності – набута системою властивість, якою не володіють її складові елементи. Такі або інші прояви самоорганізації дають можливість розглядати і вивчати розподілену систему як один організм. З пізнавального погляду важливою є візуалізація отриманих у результаті комп'ютерного експерименту скоординованих ігрових стратегій як однієї з ознак самоорганізації системи. Візуалізацію скоординованих стратегій стохастичної гри виконаємо на прикладі розв'язування задачі побудови латинських квадратів. Вибір задачі обумовлений локальним способом формування поточних програшів гравців, зручністю контролю за значеннями фінальних розв'язків гри, які відображають перетворення локально скоординованих стратегій окремих гравців у глобальну координацію (або самоорганізацію) усього колективу гравців та можливістю практичного використання отриманих результатів.

Латинський квадрат – це матриця розміром $N \times N$ з властивістю розміщення N різних елементів (символів, чисел або об'єктів): у кожному рядку та у кожному стовпчику кожен із елементів зустрічається тільки один раз. Два квадрати називаються ортогональними, якщо в результаті їх накладання утворюється квадрат з унікальними, неповторювальними комбінаціями елементів. Вперше задачу побудови ортогональних латинських квадратів 6-го порядку поставив швейцарський математик Л. Ейлер у 1782 році. Він висловив гіпотезу, що не існує ортогональних квадратів порядку $N = 4k + 2$, де $k = 1, 2, \ldots$. У 1901 році французький математик Г. Таррі експериментально підтвердив відсутність ортогональних латинських квадратів порядку $N = 6$. Згодом, у 60-х роках XX століття, використовуючи засоби обчислювальної техніки, американські математики Р. К. Боуз, С. С. Шрикхенд та Е. Т. Паркер побудували ортогональні квадрати від 10-го до 22-го порядків, що спростувало гіпотезу Ейлера для порядків, більших за 6-й [9].

Латинські квадрати використовуються для планування експериментів, розв'язування задач теорії груп, кодування інформації, складання розкладів, розподілу ресурсів, побудови математичних головоломок та ігор.

Планування експериментів на основі латинських квадратів полягає у генеруванні неповторювальної комбінації варіантів дослідження у дискретному просторі незалежних факторів. Латинський квадрат задає план експерименту, у якому рядки відповідають різним значенням одного фактора, стовпці – значенням другого, а елементи на перетині рядків і стовпців – значенням третього фактора. При побудові плану експерименту з використанням латинських квадратів зменшується кількість пошукових варіантів. Так, для трьох факторів з N дискретними значеннями замість N^3 дослідів, що відповідає повному перебору варіантів, з використанням латинського квадрата необхідно лише N^2 варіантів. Зменшення кількості варіантів досягається за рахунок втрати інформації про взаємодію факторів. Для збільшення кількості факторів використовують греколатинські квадрати, які утворюються накладанням ортогональних латинських квадратів.

Латинські квадрати використовуються також для побудови логічних ігор. Відома гра під назвою „судоку" (з японської „су" – цифра, „доку" – розміщена окремо) полягає у заповненні латинського квадрата для заданих початкових значень деяких із його елементів. Задача заповнення латинського квадрата є NP-повною, однак частково заповнений квадрат можна доповнити до латинського за прийнятний час.

Метою роботи є розв'язування задачі побудови латинських квадратів як ілюстративного прикладу процесів координації та самоорганізації стохастичної гри в умовах ситуативної невизначеності. Для досягнення мети необхідно розв'язати такі задачі: визначити критерії самоорганізації розподіленої системи на прикладі побудови латинських квадратів, розробити ігрову модель, метод та алгоритм побудови латинських квадратів, виконати програмне комп'ютерне моделювання для контролю динаміки та візуалізації результатів розв'язування стохастичної гри.

Постановка ігрової задачі

Нехай підбір значень елементів ортогональних латинських квадратів здійснюється двома коаліціями, кожна з яких складається з $N \times N$ гравців з чистими стратегіями $U = (u[1], u[2], ..., u[N])$, де $u[i] \in \{1..N\}$. Після вибору варіанта $u_n^m[i, j]$, де $m = 1,2$, гравці отримують поточний програш, який складається з двох складових:

$$z_n^m[i, j] = l\, x_n^m[i, j] + (1 - l) x_n^{1,2}[i, j], \tag{1}$$

де $l \in [0,1]$ – ваговий коефіцієнт; $i, j = 1..N$.

Перша складова визначає штраф за недотримання структури латинського квадрата:

$$x_n^m[i, j] = \frac{1}{2(N-1)} \left(\sum_{\substack{k=1,\\ k \neq j}}^{N} c\,(u_n^m[i,k] = u_n^m[i, j]) + \sum_{\substack{k=1,\\ k \neq i}}^{N} c\,(u_n^m[k, j] = u_n^m[i, j]) \right),$$

де $c(\,) \in \{0,1\}$ – індикаторна функція події.

Друга складова визначає штраф за порушення умови ортогональності двох латинських квадратів:

$$x_n^{1,2}[i, j] = \frac{1}{N^2 - 1} \sum_{\substack{k=1,\\ k \neq i}}^{N} \sum_{\substack{l=1,\\ l \neq j}}^{N} c\,(u_n^1[k,l] = u_n^2[i, j]).$$

Якість вибору значень чистих стратегій визначається середніми програшами

$$Z_n^m[i, j] = \frac{1}{n} \sum_{t=1}^{n} z_t^m[i, j],\ i, j = 1..N,\ m = 1,2. \tag{2}$$

Мета гри полягає у мінімізації функцій середніх програшів:

$$\lim_{n \to \infty} Z_n^m[i, j] \to \min_{u_n^m[i, j]},\ i, j = 1..N,\ m = 1,2.$$

Метод розв'язування задачі

Пошук чистих стратегій $\{u_n^m[i,j]\}$, які мінімізують систему функцій $Z_n^m[i,j]$, виконаємо на основі випадкового механізму, побудованому на динамічних імовірнісних розподілах:

$$p_{n+1}^m[i,j] = p_{e_{n+1}}^N\left\{p_n^m[i,j] - g_n z_n^m[i,j]\left(e(u_n^m[i,j]) - p_n^m[i,j]\right)\right\},\ i,j=1..N,\ m=1,2, \tag{3}$$

де $p_{e_{n+1}}^N$ – проектор на одиничний e-симплекс $S_{e_{n+1}}^N$ [3]; $p_n^m[i,j] \in S_{e_n}^N$ – змішана стратегія гравця; $g_n > 0$, $e_n > 0$ – монотонно спадні послідовності невід'ємних величин; $z_n^m[i,j] \in R^1$ – поточний програш гравця; $e(u_n^m[i,j])$ – одиничний вектор-індикатор вибору варіанта $u_n^m[i,j] \in U$.

Параметр g_n регулює величину кроку методу (3), а параметр e_n – крок розширення e-симплексу. Ці параметри можуть бути задані так:

$$g_n = g n^{-a},\ e_n = e n^{-b}\ , \tag{4}$$

де $g > 0$; $a > 0$, $e > 0$; $b > 0$.

Значення чистих стратегій визначаються з умови:

$$u_n^m[i,j] = \left\{u^m(l) \,|\, l = \arg\min_l \sum_{k=1}^{l} p_n^m[i,j,k] > w\ (i,j,k,l=1..N)\right\}, \tag{5}$$

де $w \in [0,1]$ – випадкова величина з рівномірним розподілом.

Збіжність змішаних стратегій до оптимальних значень визначається співвідношеннями параметрів g_n та e_n, які повинні задовольняти базові умови стохастичної апроксимації [10]. Враховуючи, що $M\{z_n^m[i,j]\} > 0$, $g_n > 0$; $g_{n+1} < g_n$; $e_n \in (0, N^{-1})$; $e_{n+1} < e_n$, після відповідного оцінювання згенерованих методом (3) послідовностей випадкових величин отримаємо умови середньоквадратичної збіжності:

$$\sum_{n\to\infty} g_n = \infty;\ \lim_{n\to\infty} e_n = 0;\ \lim_{n\to\infty}(|e_n - e_{n-1}|\, g_n^{-1} + g_n) = 0.$$

Для послідовностей величин (4) зазначені умови виконуються при $a \in (0,1]$; $b > 0$. Оптимальні значення параметрів ігрового методу уточнюються під час комп'ютерного експерименту.

Динаміку збіжності ігрового методу спостерігатимемо за значеннями функцій поточних і середніх програшів та коефіцієнта координації.

Функція поточних програшів обчислюється усередненням по усіх гравцях:

$$z_n = \frac{1}{2N^2}\sum_{i=1}^{N}\sum_{j=1}^{N}\sum_{m=1}^{2} z_n^m\ .$$

Функція середніх програшів визначається усередненням поточних програшів у часі:

$$Z_n = \frac{1}{n}\sum_{t=1}^{n} z_t\ . \tag{6}$$

Коефіцієнт координації обчислимо відношенням кількості сприятливих варіантів (для яких виконується умова ортогональності латинських квадратів) до кількості пройдених кроків моделювання:

$$K_n = \frac{1}{n}\sum_{t=1}^{n}\sum_{i=1}^{N}\sum_{j=1}^{N} c\left(K_t^1 + K_t^2 + K_t^{1,2} = 0\right). \tag{7}$$

Складові K_t^m, $m=1,2$ виразу (7) визначають кількість повторень елемента $u_t^m[i,j]$ у рядку з номером i та у стовпчику з номером j для кожного з синтезованих квадратів:

$$K_t^m = \sum_{\substack{k=1,\\ k\neq j}}^{N} c\,(u_t^m[i,k] = u_t^m[i,j]) + \sum_{\substack{k=1,\\ k\neq i}}^{N} c\,(u_t^m[k,j] = u_t^m[i,j])\,.$$

Складова $K_t^{1,2}$ визначає кількість повторень комбінації елементів $\left(u_t^1[i,j], u_t^2[i,j]\right)$ серед поточних значень обох квадратів:

$$K_t^{1,2} = \sum_{\substack{x=1,\\ x\neq i}}^{N}\sum_{\substack{y=1,\\ y\neq j}}^{N} c\left(\left(c(u_t^1[i,j]=u_t^1[x,y])\ and\ c(u_t^2[i,j]=u_t^2[x,y])\right)=1\right).$$

Для методу побудови звичайних латинських квадратів у виразі коефіцієнта координації (7) враховується тільки значення складової K_t^1.

Алгоритм розв'язування задачі

1. Задати початкові значення параметрів:

N – кількість чистих стратегій;

$U=(u[1],u[2],...,u[N])$; $u[i]\in\{1..N\}$ – вектор значень чистих стратегій;

$p[i,j]=(1/N,...,1/N)$; $i,j=1..N$ – змішані стратегії (вектори імовірностей вибору чистих стратегій);

$g>0$ – параметр кроку навчання;

$a\in(0,1]$ – порядок кроку навчання;

$e\in(0,N^{-1})$ – параметр кроку розширення e-симплексу;

$b>0$ – порядок кроку розширення e-симплексу;

$n=0$ – початковий момент часу;

$n_{\max}$ – максимальна кількість кроків методу.

2. Вибрати чисті стратегії гравців $u_n[i,j]\in U$; $i,j=1..N$ згідно з (5).

3. Отримати значення поточних програшів гравців $x_n[i,j]$; $i,j=1..N$ згідно з (1).

4. Обчислити значення параметрів g_n та e_n (4).

5. Обчислити елементи векторів змішаних стратегій $p_n[i,j]$; $i,j=1..N$ згідно з (3).

6. Обчислити характеристики якості вибору варіантів рішень Z_n (6) та K_n (7).

7. Задати наступний момент часу $n:=n+1$.

8. Якщо $n<n_{\max}$, то перейти на крок 2, інакше – кінець.

Результати комп'ютерного моделювання

Виконаємо побудову латинських квадратів за допомогою ігрового методу (3) з параметрами: $l=0.5$, $g=10$, $e=0.999/N$, $a=0.1$, $b=1$. Один із варіантів ортогональних квадратів порядку $N=5$ зображено на рис. 1.

5	1	3	4	2
2	5	1	3	4
3	4	2	5	1
1	3	4	2	5
4	2	5	1	3

3	5	2	4	1
4	1	3	5	2
1	3	5	2	4
2	4	1	3	5
5	2	4	1	3

Рис. 1. Ортогональні латинські квадрати 5-го порядку

При накладанні ортогональних квадратів утворюється греко-латинський квадрат з різними елементами. Так, для зображених на рис. 1 ортогональних квадратів, отримаємо квадрат, зображений на рис. 2.

53	15	32	44	21
24	51	13	35	42
31	43	25	52	14
12	34	41	23	55
45	22	54	11	33

Рис. 2. Суміщені ортогональні латинські квадрати 5-го порядку

Крім унікальних комбінацій елементів, утворений греко-латинський числовий квадрат має ще одну цікаву властивість: суми елементів у кожному рядку та кожному стовпчику є однаковими. Інакше такий квадрат називається магічним.

Якщо поточний програш гравців визначається тільки першою складовою штрафу (1), що існує при $l=1$, то метод (3) забезпечує формування звичайних латинських квадратів. Отриманий ігровим методом приклад латинського квадрата 10-го порядку наведено на рис. 3.

6	7	8	10	4	1	9	2	5	3
3	1	10	8	2	5	6	9	4	7
4	9	1	6	8	3	5	10	7	2
10	5	9	7	6	2	3	4	1	8
7	6	3	2	1	9	8	5	10	4
8	4	5	9	3	7	2	1	6	10
9	8	7	4	5	6	10	3	2	1
5	2	6	3	10	4	1	7	8	9
1	3	2	5	7	10	4	8	9	6
2	10	4	1	9	8	7	6	3	5

Рис. 3. Латинський квадрат 10-го порядку

При повторній реалізації методу (3) для різних послідовностей випадкових величин отримаємо інші варіанти латинських квадратів.

Характеристики збіжності ігрового методу для побудови ортогональних латинських квадратів 5-го порядку зображено на рис. 4, а звичайного латинського квадрата 10-го порядку – на рис. 5.

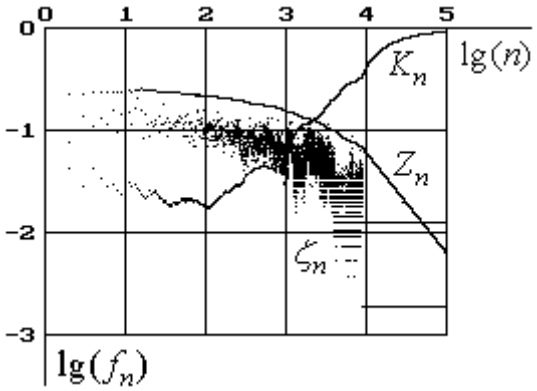

Рис. 4. Характеристики збіжності ігрового методу побудови ортогональних квадратів 5-го порядку

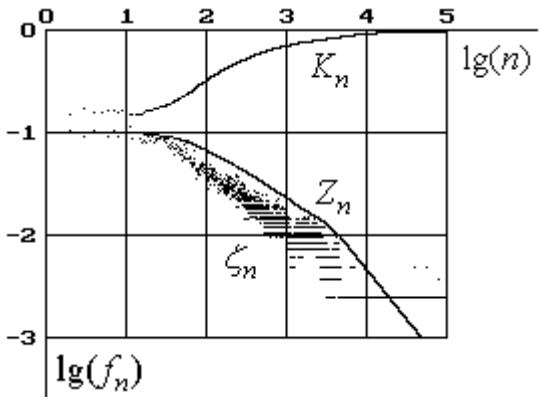

Рис. 5. Характеристики збіжності ігрового методу побудови латинського квадрата 10-го порядку

Зменшення функції середніх програшів Z_n та зростання коефіцієнта координації K_n свідчить про збіжність ігрового методу (3). Порядок швидкості збіжності n^{-q} може бути оцінений тангенсом гострого кута, утвореним графіком лінійної апроксимації функції середніх програшів Z_n з віссю моментів часу n.

Слід зазначити, що ігрова побудова ортогональних квадратів вимагає набагато більшої кількості пошукових кроків, ніж побудова звичайних латинських квадратів. Відповідні графіки залежності середньої кількості кроків стохастичної гри $\overline{n}$ від порядку латинських квадратів N зображено на рис. 6. Графік 1 відповідає звичайним, а графік 2 – ортогональним латинським квадратам.

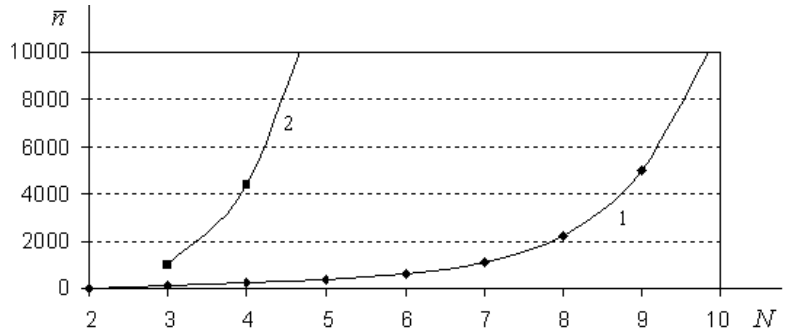

Рис. 6. Залежність середньої кількості пошукових кроків від порядку латинських квадратів

Як видно на рис. 6, із зростанням порядку латинських квадратів середня кількість кроків стохастичної гри зростає за показниковим законом. Ортогональні латинські квадрати не існують для порядків 2 та 6.

Висновки

Розроблений ігровий метод побудови латинських квадратів є добрим ілюстративним прикладом самоорганізації стохастичної гри через локальнообумовлену координацію стратегій гравців. Кожен з гравців здійснює локальне спостереження за діями гравців, розміщеними в одному з ним рядку та стовпчику квадратної матриці. Для побудови ортогональних латинських квадратів гравці однієї коаліції (матриці) додатково спостерігають за діями усіх гравців іншої коаліції. Після обчислення відповідних штрафів за порушення умов ортогональності квадратів гравці отримують поточні програші, які використовуються ними для формування динамічних векторів змішаних стратегій. Побудований на основі стохастичної апроксимації метод перетворення змішаних стратегій (3) забезпечує мінімізацію функцій середніх програшів на вершинах одиничних симплексів. Цілеспрямована динаміка змішаних стратегій перетворює локально скоординовані дії гравців у глобальну координацію (самоорганізацію) стохастичної гри, що виявляється у правильному розміщенні значень елементів латинських квадратів.

Запропонований ігровий метод побудови латинських квадратів грунтується на рекурентному перетворенні векторів змішаних стратегій і має повільну збіжність, оскільки гравці приймають рішення в умовах апріорної невизначеності матриць програшів. Цей недолік успішно долається застосуванням сучасних швидкодіючих засобів обчислювальної техніки та можливістю розпаралелювання ігрового алгоритму.

Розроблені програмні засоби побудови латинських квадратів можуть бути використані для планування експериментів, кодування інформації, складання розкладів, розподілу ресурсів, розв'язування ігрових та комбінаторних задач.

1. Доманский В.К. Стохастические игры / В.К. Доманский // Математические вопросы кибернетики. – 1988. – № 1. – С. 26 – 49. 2. Fudenberg D. The Theory of Learning in Games / D. Fudenberg, D.K. Levine. – Cambridge, MA: MIT Press, 1998. – 292 pp. 3. Назин А.В. Адаптивный выбор вариантов: Рекуррентные алгоритмы / А.В. Назин, А.С. Позняк. – М.: Наука, 1986. – 288 с.

4. Ashby W. R. Principles of the Self-Organizing Dynamic System / W. R. Ashby // Journal of General Psychology. – 1947. – v. 37. — p. 125—128. 5. Хакен Г. Синергетика. Иерархия неустойчивостей в самоорганизующихся системах и устройствах / Г. Хакен. – М.: Мир, 1985. 6. Пригожин И. Порядок из хаоса. Новый диалог человека с природой: Пер. с англ. / И. Пригожин, И. Стенгерс. – М.: Эдиториал УРСС, 2003. – 312 с. 7. Хакен Г. Информация и самоорганизация. Макроскопический подход к сложным системам: Пер. с англ. / Г. Хакен. – М.: КомКнига, 2005. – 248 с. 8. Кравець П.О. Самоорганізація мультиагентної системи з локальними зв'язками / П.О. Кравець // Праці 12-ї науково-технічної конференції «Системний аналіз та інформаційні технології». – 25 – 29 травня 2010 р. – Київ: Навчально-науковий комплекс „Інститут прикладного системного аналізу" Національного технічного університету України „Київський політехнічний інститут". – С. 265. 9. Laywine C.F. Discrete Mathematics Using Latin Squares / C.F. Laywine, G.L. Mullen. – Wiley & sons inc., 1998. – 303 p. 10. Граничин О.Н. Введение в методы стохастической аппроксимации и оценивания: Учеб. пособие / О.Н. Граничин. – СПб.: Издательство С.-Петербургского университета, 2003. – 131 с.

УДК 01.05.02; 05.13.06; 05.13.21

Л. Фабрі, А. Ковальчук, Мар'яна Ступень
Національний університет "Львівська політехніка",
кафедра автоматизованих систем управління

ШИФРУВАННЯ І ДЕШИФРУВАННЯ ЗОБРАЖЕНЬ З ВИКОРИСТАННЯМ КВАДРАТИЧНИХ ФРАКТАЛЬНИХ АЛГОРИТМІВ

Запропоновано застосування квадратичних фрактальних перетворень до шифрування і дешифрування зображень в градаціях сірого кольору.

Ключові слова: шифруваня, дешифрування, фрактальний алгоритм, зображення

The use of quadratic fractal transforms to encryption and decryption of images in grayscale color.

Keywords: shyfruvanya, decoding, fractal algorithm, image

Вступ

Важливою характеристикою зображення є наявність в зображенні контурів. Задача виділення контура вимагає використання операцій над сусідніми елементами, які є чутливими до змін і пригашають області постійних рівнів яскравості, тобто, контури – це ті області, де виникають зміни, стаючи світлими, тоді як інші частини зображення залишаються темними [2].

Математично ідеальний контур – це розрив просторової функції рівнів яскравості в площині зображення. Тому виділення контура означає пошук найбільш різких змін, тобто максимумів модуля вектора градієнта [2]. Це є однією з причин, через що контури залишаються в зображенні при шифруванні в системі RSA, оскільки шифрування тут грунтується на піднесенні до степеня за модулем деякого натурального числа. При цьому на контурі і на сусідніх до контура пікселах піднесеня до степеня значення яскравостей дає ще більший розрив.

Існують різні алгоритми, які виділяють контури, наприклад, відстежуючі алгоритми. Відстежуючі алгоритми грунтуються на тому, що на зображенні відшукується об'єкт (точка об'єкта, яка зустрілася першою) і контур об'єкта відстежується і векторизується. Перевагою цього алгоритму є його простота, до недоліків можна віднести їх послідовну реалізацію і деяку складність при пошуку і обробці внутрішніх контурів. Приклад такаго алгоритму – "алгоритму жука" – наведено на рис.1.