

**Київський національний університет
імені Тараса Шевченка**

**Матеріали XX Міжнародної
науково-практичної конференції**

«Шевченківська весна – 2022»

14 квітня 2022 р., м. Київ, Україна

Taras Shevchenko National University of Kyiv

**Proceeding of XX International
Scientific – Practical Conference**

«Shevchenkivska Vesna – 2022»

14 April 2022, Kyiv, Ukraine

Програмний комітет

Анісімов Анатолій Васильович – доктор фізико-математичних наук, професор, член-кореспондент НАН України, декан факультету комп'ютерних наук та кібернетики

Безущак Оксана Омелянівна – доктор фізико-математичних наук, доцент, декан механіко-математичного факультету

Капустян Олена Анатоліївна – доктор фізико-математичних наук, старший науковий співробітник, заступник декана з наукової та міжнародної роботи факультету комп'ютерних наук та кібернетики

Мішура Юлія Степанівна – доктор фізико-математичних наук, професор, завідувач кафедри теорії ймовірностей, статистики та актуарної математики

Ральченко Костянтин Володимирович – доктор фізико-математичних наук, доцент, заступник декана з наукової роботи механіко-математичного факультету

Харитонов Олексій Михайлович – кандидат фізико-математичних наук, доцент, заступник декана з навчальної роботи механіко-математичного факультету

Організаційний комітет

Александрова Поліна Вадимівна – голова студентського парламенту механіко-математичного факультету

Зубченко Володимир Петрович – кандидат фізико-математичних наук, голова Ради молодих вчених механіко-математичного факультету

Шевчук Юлія Михайлівна – кандидат фізико-математичних наук, голова Ради молодих вчених факультету комп'ютерних наук та кібернетики

Верстка: Бахчеджиоглу О.О., Железняк Г.С.

Секція «Математика, статистика та механіка»

Оцінювання параметрів у змішаному дробовому стохастичному рівнянні теплопровідності

Д. А. Аветісян, К. В. Ральченко

Розглядається стохастичне рівняння теплопровідності, кероване змішаним дробовим броунівським рухом:

$$\left(\frac{\partial u}{\partial t} - \frac{1}{2}\Delta u\right)(t, x) = \sigma \dot{B}_x^H + \kappa \dot{W}_x, \quad t > 0, x \in \mathbb{R}.$$

Тут $B^H = \{B_x^H, x \in \mathbb{R}\}$ — це дробовий броунівський рух з індексом Хюрста H , а $W = \{W_x, x \in \mathbb{R}\}$ — вінерівський процес, що не залежить від B^H .

Вивчається задача оцінювання параметрів σ^2 і κ^2 за дискретними спостереженнями вигляду $\{u(t_i, k\delta), i = 1, 2, k = 1, \dots, N\}$, де $t_1 > 0$, $t_2 > 0$ і $\delta > 0$ — фіксовані. Нехай

$$\hat{V}_N(t) = \frac{1}{N} \sum_{k=1}^N u(t, x_k)^2, \quad c_H = \frac{2^{H+1}(2^H - 1)\Gamma(H + \frac{1}{2})}{\sqrt{\pi}(H + 1)}.$$

Доведено, що для всіх $H \in (0, \frac{1}{2}) \cup (\frac{1}{2}, 1)$ статистики

$$\hat{\sigma}_N^2 = \frac{t_1^{-3/2}\hat{V}_N(t_1) - t_2^{-3/2}\hat{V}_N(t_2)}{c_H \left(t_1^{H-1/2} - t_2^{H-1/2}\right)}, \quad \hat{\kappa}_N^2 = \frac{t_1^{-1-H}\hat{V}_N(t_1) - t_2^{-1-H}\hat{V}_N(t_2)}{c_{\frac{1}{2}} \left(t_1^{1/2-H} - t_2^{1/2-H}\right)}$$

є строго консистентними оцінками параметрів σ^2 і κ^2 відповідно.

Досліджено також задачу оцінювання параметра H за спостереженнями $\{u(t_i, k\delta), i = 1, 2, 3, k = 1, \dots, N\}$. Виведено рівняння для знаходження оцінки та доведено її строго консистентність. В окремому випадку $t_3 = 2t_2 = 4t_1$ цю оцінку знайдено в явному вигляді:

$$\hat{H}_N = \frac{1}{2} + \log_2 \frac{t_2^{-3/2}\hat{V}_N(t_2) - t_3^{-3/2}\hat{V}_N(t_3)}{t_1^{-3/2}\hat{V}_N(t_1) - t_2^{-3/2}\hat{V}_N(t_2)}.$$

Автори

Діана Арутюнівна Аветісян — аспірант 3-го року, механіко-математичний факультет, Київський національний університет імені Тараса Шевченка, Київ, Україна; E-mail: diana.avetisyan2017@gmail.com

Костянтин Володимирович Ральченко — д.ф.-м.н., доцент, механіко-математичний факультет, Київський національний університет імені Тараса Шевченка, Київ, Україна; E-mail: kostiantynralchenko@knu.ua

Кількість, сума та добуток дільників натурального числа

Н. О. Арський, О. Д. Приходько

Для натурального числа n визначають функції

$$\tau(n) = \sum_{d|n} 1, \quad \sigma(n) = \sum_{d|n} d, \quad \sigma_m(n) = \sum_{d|n} d^m, \quad \pi(n) = \prod_{d|n} d$$

як кількість, суму, суму m -тих ($m \in \mathbf{N}$) степенів та добуток дільників числа n відповідно.

Зібрано та систематизовано відомості про властивості даних функцій: формули для обчислення; значення даних функцій від простого числа та від добутку двох чисел; умови, коли функції набувають простих, парних чи непарних значень. Вони доповнені такими власними результатами: розширено деякі відомі властивості для всіх натуральних значень степеня; узагальнено теореми про значення даних функцій від добутку двох чисел; виведено значення кількості, суми, суми m -тих степенів та добутку дільників натурального числа, які кратні деякому числу, і дільників, які є точними l -тими ($l \in \mathbf{N}$) степенями.

Отримано значення кількості, суми m -тих степенів та добутку усіх спільних дільників двох натуральних чисел і знайдено формули для обчислення наступних виразів: $\tau(\text{НСД}(s; t))\tau(\text{НСК}(s; t))$, $\sigma_m(\text{НСД}(s; t))\sigma_m(\text{НСК}(s; t))$, $\pi(\text{НСД}(s; t))\pi(\text{НСК}(s; t))$.

Досліджено середні величини для дільників натурального числа: доповнено статтю Ойстіна Оре [1] результатами для середнього степеневих порядку m і середнього квадратичного від всіх дільників натурального числа та виведено значення добутків середніх величин від НСД та НСК двох натуральних чисел.

Виведено формули сум усіх можливих добутків, кожен з яких містить по два або три різних дільники натурального числа, та рекурентну формулу

$$s_{k+1, m} = \frac{1}{k+1} \left((-1)^k \sigma_{(k+1)m}(n) + \sum_{i=0}^{k-1} (-1)^i s_{k-i, m}(n) \sigma_{(i+1)m}(n) \right),$$

де $d_1, d_2, \dots, d_{\tau(n)}$ — це впорядковані за зростанням дільники числа n , а

$$s_{k, m}(n) = \sum_{1 \leq a_1 < a_2 < \dots < a_k \leq \tau(n)} d_{a_1}^m d_{a_2}^m \dots d_{a_k}^m, \quad k \in \mathbf{N}, \quad k \leq \tau(n) - 1.$$

Список літератури

- [1] Ore O. On the Averages of the Divisors of a Number. The American Mathematical Monthly 1948, **55** (10), 615–619. doi:10.2307/2305616
-

Автори

Нікіта Олексійович Арський — учень 10 класу, Український фізикоматематичний ліцей Київського національного університету імені Тараса Шевченка, Київ, Україна; E-mail: nikita.arskiy.25@gmail.com

Ольга Дмитрівна Приходько — вчителька математики, Український фізикоматематичний ліцей Київського національного університету імені Тараса Шевченка, Київ, Україна; E-mail: prykhodkood@gmail.com

Characterization of minimax identity with robust non-concave utility functions for constrained case of random endowments

O. Bahchedjioglou

We studied the robust utility maximization functional of the terminal wealth in complete market models. This problem is well-known for strictly concave utility functions and we extended existing results for non-concave utility functions while considering an additional upper bound. The basic model as in [1] with the assumption that the discounted price process is locally bounded. Moreover, similarly to [2, Chapter 3] we consider a modified constrained counterpart. Specifically, we assume that there is an upper bound on the endowment, given by a random variable $W : \Omega \rightarrow [0, +\infty)$. The budget set is then given by $\mathcal{X}_x^W := \{X \in L^1(Q^e) \mid 0 \leq X \leq W, E_{Q^e}[X] \leq x\}$, where $x > 0$ is the initial wealth and Q^e is the unique equivalent local martingale measure.

Theorem 1. *Under some natural assumptions on the probability space and value functions as in [1], and additionally assuming that the probability space $(\Omega, \mathcal{F}, \mathbb{P})$ be atomless, the following holds*

$$\begin{aligned}
 \sup_{X \in \mathcal{X}_x^W} \inf_{Q \in \mathcal{Q}^e} E_Q[U_c(X)] &\stackrel{(1\star)}{=} \sup_{X \in \mathcal{X}_x^W} \inf_{Q \in \mathcal{Q}} E_Q[U_c(X)] \stackrel{(2\star)}{=} \inf_{Q \in \mathcal{Q}} \sup_{X \in \mathcal{X}_x^W} E_Q[U_c(X)] \\
 &\stackrel{\vee(4\star)}{\leq} \sup_{X \in \mathcal{X}_x^W} \inf_{Q \in \mathcal{Q}^e} E_Q[U(X)] \stackrel{\parallel(3\star)}{\leq} \inf_{Q \in \mathcal{Q}^e} \sup_{X \in \mathcal{X}_x^W} E_Q[U(X)] \\
 &\stackrel{\parallel(6\star)}{\leq} \sup_{X \in \mathcal{X}_x^W} \inf_{Q \in \mathcal{Q}} E_Q[U(X)] \stackrel{(7\star)}{\leq} \inf_{Q \in \mathcal{Q}} \sup_{X \in \mathcal{X}_x^W} E_Q[U(X)] \stackrel{(8\star)}{\leq} \inf_{Q \in \mathcal{Q}^e} \sup_{X \in \mathcal{X}_x^W} E_Q[U(X)] \stackrel{\parallel(5\star)}{\leq} \sup_{X \in \mathcal{X}_x^W} \inf_{Q \in \mathcal{Q}^e} E_Q[U(X)]
 \end{aligned}$$

References

- [1] SCHIED, ALEXANDER; WU, CHING-TANG. Duality theory for optimal investments under model uncertainty.
- [2] HANS FÖLLMER; ALEXANDER SCHIED "Stochastic Finance"; De Gruyter, 2016.
- [3] REICHLIN, CHRISTIAN ROCHUS AUGUST: "Utility Maximization with a Given Pricing Measure When the Utility Is Not Necessarily Concave"; Mathematics and Financial Economics, Volume 7, Issue 4, pp 531-556, 2013

Authors

Bahchedjioglou Olena Oleksiivna — PHD student, Department of Probability, Statistics and Actuarial Mathematics, Mechanics and Mathematics Faculty, Taras Shevchenko national university of Kyiv, Volodymyrska, 60, 01601 Kyiv, Ukraine; E-mail: olenakharytonova06@gmail.com

Непараметричний двофакторний дисперсійний аналіз

А. М. Буковецька

Непараметричні тести застосовують у випадках, коли дані не задовольняють припущення параметричних критеріїв. Одним з відомих непараметричних аналогів

одно-факторного дисперсійного аналізу є тест Краскела-Уолліса. Першу частину роботи присвячено вивченню особливостей застосування цього тесту та порівнянню його потужності з (параметричним) ANOVA, за допомогою тесту перестановок на даних з різних типових розподілів.

Також в роботі вивчено деякі моделі (з повтореннями та без, з перетином та без) дво-факторного дисперсійного аналізу

$$Y_{i,j,k} = m + a_i + b_j + (ab)_{i,j} + e_{i,j,k}$$

Для пошуку непараметричного аналогу двох-факторного ANOVA в роботі розглянуто теорію методу m ранжувань. Бернард і Ван Елтерен [1] застосували її для побудови тесту для головних факторів дисперсійного аналізу. Мета даної роботи полягає у розширенні цього підходу і на тест перетину двох факторів та дослідженні потужності відповідних тестів.

Список літератури

- [1] A. Bernard and P.H. van Elteren. A generalization of the method of m rankings. *Indagationes Mathematicae* 15, 1953, pp. 358–369.
- [2] J.H. Klotz. A computational approach to statistics. University of Wisconsin at Madison, 2006, 492 p.

Автори

Буковецька Андріяна Миколаївна — студентка 2-го курсу магістратури, механіко-математичний факультет, Київський національний університет імені Тараса Шевченка, Київ, Україна; E-mail: 19odri99@gmail.com

Перевірка однорідності розподілів компонент суміші за цензуrowаними даними

Д. Д. Горбунов

Розглянемо модель суміші зі змінними концентраціями (далі СЗК) з випадковим цензуруванням справа. Спостерігаються деякі об'єкти $O_1, \dots, O_N$, кожен з яких може належати одній з M популяцій (компонент). Номер популяції $\text{ind}(O_j)$ вважається невідомим, однак відомі ймовірності потрапляння кожного об'єкта до відповідної компоненти: $p_j^m = \mathbf{P}(\text{ind}(O_j) = m)$. Кожному об'єкту відповідає його час відмови $T_j = T(O_j)$ та цензор $C_j = C(O_j)$. Припускається, що випадкові вектори (T_j, C_j) є незалежними для різних j , розподіл є неперервним та описується моделлю СЗК, а час та цензор є незалежними при фіксованому $\text{ind}(O_j)$. Досліднику відомі лише величина $\xi_j = \min(T_j, C_j)$ та індикатор відсутності цензурування $\delta_j = \mathbf{1}\{T_j \leq C_j\}$.

Для кожної компоненти нас цікавить умовний розподіл часу відмови. Інколи потрібно перевірити, чи не є дві (або більше) компоненти суміші однорідними, тобто чи не є розподіли спостережуваної характеристики однорідними для цих компонент.

У роботі розроблено узагальнення тесту Колмогорова-Смірнова, що базується на використанні виправленої оцінки Каплана-Мейера для СЗК та бутстреп-техніки зі згладжуванням. Продемонстровано роботу тесту на модельованих даних. Методом імітаційного моделювання визначено ймовірності помилок першого та другого роду для розробленого тесту. Результати показують, що на вибірках помірного обсягу тест працює адекватно.

Результати можуть бути застосовані при оцінюванні функцій виживаності у випадку, коли досліджувані об'єкти належать до різних популяцій. Наприклад, у

медицині можна досліджувати часи виживання пацієнтів після застосування деякого препарату, де пацієнти беруться з різних популяцій: за регіоном проживання, історією хвороби тощо.

Список літератури

- [1] Майборода Р.Є., Сугакова О.В. "Оцінювання та класифікація за спостереженнями із суміші". К.: ВПЦ "Київський університет", 213 р. - 2008
- [2] Майборода Р.Є., Хізанов В.Г. "Модифікація оцінки Каплана-Мейера для моделі сумішей зі змінними концентраціями". Теорія ймов. та матем. статистика, Vol.92, Iss. pp. 103 - 103, - 2015
- [3] Shao J., Tu D. The Jackknife and Bootstrap.- Springer, NY, 1995, 516p.

Автори

Горбунів Даниїл Денисович — студент 1-го курсу магістратури, механіко-математичний факультет, Київський національний університет імені Тараса Шевченка, Київ, Україна; E-mail: danielhorbunov@knu.ua

Конгруенції з біноміальними коефіцієнтами

І. О. Горобець, О. Д. Приходько

Остачею від ділення біноміальних коефіцієнтів на натуральне число цікавилось не одне покоління математиків, і зараз це питання теж є актуальним у науковій спільноті. Це підтверджує наявність значної кількості статей та посібників, у яких піднімається дана тема.

У роботі зібрано та упорядковано відомості про базові властивості конгруенцій з біноміальними коефіцієнтами. До всіх тверджень наведено лаконічні та доступні школяреві доведення.

Підготовча частина дослідження містить інформацію про властивості конгруенцій, біноміальних коефіцієнтів та про p -адичну функцію, формулу Лежандра і теорему Куммера.

Основний результат – це леми, твердження та теореми, в яких сформульовані властивості конгруенцій за модулем простого числа з остачею 0, конгруенцій за модулем натурального числа з остачею 0, конгруенцій за модулем простого числа з довільною остачею. Окремо розглянуто теорему для конгруенцій за модулем 2.

Також приділено увагу використанню сформульованих вище властивостей у доведеннях інших результатів. Отримані твердження доповнено конгруенціями, які виконуються для простого числа $p > 2$ та цілого a :

$$a^p + (p - a)^p \equiv 0 \pmod{p^2},$$
$$\sum_{a=1}^p a^p \equiv 0 \pmod{p^2}.$$

Автори

Ірина Олегівна Горобець — учениця 11 класу, Український фізико-математичний лицей Київського національного університету імені Тараса Шевченка, Київ, Україна; E-mail: igorobets33@gmail.com

Про симетрії систем лінійних звичайних диференціальних рівнянь другого порядку

С. Т. Гурака

У рамках групового аналізу диференціальних рівнянь досліджуємо клас нормальних лінійних систем із n звичайних диференціальних рівнянь другого порядку [1] $\dot{\mathbf{x}}_t = A(t)\mathbf{x}_t + B(t)\mathbf{x} + \mathbf{f}(t)$ із n невідомими функціями $x^1, \dots, x^n$, $\mathbf{x}(t) = (x^1(t), \dots, x^n(t))^T$, $n \geq 2$, $A(t)$ та $B(t)$ — довільні гладкі $n \times n$ матрично-значні функції змінної t , $\mathbf{f}(t)$ — довільна гладка векторнозначна функція змінної t . За допомогою перетворень еквівалентності розглядувану систему завжди можна звести до канонічного вигляду $\ddot{\mathbf{x}} = V(t)\mathbf{x}$, де $V(t)$ — $n \times n$ матричнозначна функція змінної t . Якщо $V(t) \equiv V$ — стала $n \times n$ матриця, то систему зводимо до вигляду $\ddot{\mathbf{x}} = J\mathbf{x}$, де J — жорданова нормальна форма матриці V . Якщо матриця J пропорційна одиничній, то система еквівалентна елементарній системі $\ddot{\mathbf{x}} = \mathbf{0}$, лівійській симетрії якої добре відомі (див., наприклад, [1]). Якщо ж матриця J непропорційна одиничній, то відповідно до [2, теорема 1] для повної групової класифікації необхідно розв'язати задачу Фробеніуса, тобто описати всі матриці, що комутують із фіксованою матрицею J . Використовуючи алгоритм, запропонований в [2], у роботі виконано вичерпну групову класифікацію систем $\ddot{\mathbf{x}} = J\mathbf{x}$ у випадках двох, трьох та чотирьох залежних змінних. Завдяки проведенню дослідженням вдалося уточнити результати робіт [3, 4], що були отримані раніше в рамках класичного інфінітезимального підходу.

Список літератури

- [1] Boyko V.M., Lokaziuk O.V., Popovych R.O., Admissible transformations and Lie symmetries of linear systems of second-order ordinary differential equations, arXiv:2105.05139.
- [2] Boyko V.M., Popovych R.O., Shapoval N.M., Lie symmetries of systems of second-order linear ordinary differential equations with constant coefficients, *J. Math. Anal. Appl.* **397** (2013), 434–440.
- [3] Wafo Soh C., Symmetry breaking of systems of linear second-order ordinary differential equations with constant coefficients, *Commun. Nonlinear Sci. Numer. Simul.* **15** (2010), 139–143.
- [4] Campoamor-Stursberg R., Systems of second-order linear ODE's with constant coefficients and their symmetries, *Commun. Nonlinear Sci. Numer. Simul.* **16** (2011), 3015–3023.

Автори

Софія Тарасівна Гурака — студентка 4-го курсу, механіко-математичний факультет, Київський національний університет імені Тараса Шевченка, Київ, Україна; E-mail: sophiahuraka@gmail.com

Класифікація дій людини з використанням радіосигналів Wi-Fi

В. С. Гусев

Наразі дуже актуальною проблемою є безпека власних будинків. Зазвичай для безпеки ведеться відеоспостереження. У результаті виникає нова проблема з конфіденційністю, оскільки більшість людей хотіли б, щоб те, що відбувається всередині їхніх будинків, було приватним від зовнішнього світу. Легко зрозуміти, чому постійно включені камери та мікрофони змушують нас нервувати. Майже у кожної сучасної людини є вдома WI-FI-адаптер, який забезпечує бездротове мережеве з'єднання для обладнання, яке до нього підключено. Робота цього адаптера заснована на розповсюдженні радіосигналів.

У своїй роботі я збираю та використовую ці сигнали для класифікації дій людини. Коли в будинку є рух, брижі створюються в сигналах Wi-Fi. Різні дії викликають різні коливання у сигналах Wi-Fi. Я досліджую такі активності, як: drink, walk, sleeping, cook, sittdown, standup, washingdishes, nothing, petcat, brushteeth, getintobed. Тому моєю головною задачею є побудова математичної моделі, що дозволить відрізнити та класифікувати різні класи дій людини. Тобто, мінімізую функцію, що виначає типи активностей за наявних відомих значень:

$$\sum_{i=1}^n |F(\bar{w}, \tilde{f}(\bar{x}_i)) - R_i| \rightarrow \min_{\bar{w}, \tilde{f}(\bar{x}_i)}, \text{ де}$$

- $F(\bar{w}, \tilde{f}(\bar{x}_i))$ - модель, яка класифікує вхідні дані, набуває значення від 0 до 11, що вказує на порядковий номер активності;
- n - розмір даних, на яких модель "навчається";
- R_i - відомий тип активності;
- $\bar{w}$ - параметри моделі;
- $\tilde{f}(\bar{x}_i)$ - похідні характеристики, вираховані на вхідних даних;
- $\bar{x}_i$ - дані CSI(Інформація про стан каналу).

Вхідними даними є інформація про стан каналу з плати Raspberry Pi 4, яка підключається до адаптера Wi-Fi. На першому етапі я проаналізував дані, з якими працюю. Оскільки на вхід я отримую сигнали з великою кількістю піднесучих, я перевіряв чи корелюють вони між собою. Як виявилось тільки сусідні піднесучі корелюють між собою, тому для зменшення їх кількості я провів аналіз основних компонент. Потім за допомогою ковзного середнього згладив сигнал і відфільтрував шуми вейвлет перетворенням. Для класифікації за заданими ознаками був використаний алгоритм машинного навчання.

Автори

Гусев Володимир Святославович — студент 4-го курсу, механіко-математичний факультет, Київський національний університет імені Тараса Шевченка, Київ, Україна; E-mail: gusevvovik@gmail.com

Геометричні характеристики скручених правильних призматодів

М. С. Деркач

Многогранники призматичної форми використовуються в архітектурі, мистецтві, техніці та різних галузях науки для моделювання об'єктів. Метою даної ро-

боти є дослідження змін геометричних характеристик скручених правильних призматойдів за допомогою математичного моделювання задачі в прямокутній системі координат. В роботі проведено класифікацію призматойдів; введено поняття прямого призматойда (призматойд, основи якого є вписаними многокутниками, центр описаного кола навколо верхньої основи якого проектується в центр описаного кола навколо нижньої основи), скрученого (призматойд, отриманий з початкового призматойда поворотом однієї з основ навколо деякої осі на деякий кут) та правильного призматойда (прямий призматойд з правильними однойменними многокутниками в основах та рівними бічними гранями). Розглянуто дві математичні моделі зміни геометричних параметрів вихідного правильного призматойда при повороті однієї з основ – зі сталою висотою та зі сталою довжиною бічного ребра. Доведено, що многокутники в перерізах, паралельних основам скрученого правильного призматойда, є на чверть правильними, але за деяких умов можуть ставати рівносторонніми напівправильними. Доведено, що котангенси двограних кутів при ребрі основи правильного призматойда задовольняють рівняння раулика Паскаля з віссю симетрії, повернутою на кут $\frac{\pi}{n}$. На відміну від випадку скрученої правильної призми та відповідної антипризми [1, 2] раулик Паскаля може мати як вузлову точку, так і ізольовану точку або точку повернення. Виявлено, що при застосуванні моделі зі сталим ребром вершина скрученої правильної призми рухається по кривій Вівіані, яка проектується на одну з координатних площин у вигляді лемніскати Жероно.

Список літератури

- [1] Рудик Є.А.О. Деформації кручення правильних призм та скручених антипризм. Матеріали – XVIII Міжнародної науково-практичної конференції студентів, аспірантів та молодих вчених «Шевченківська весна – 2020», квітень 2020 року, Київ, Україна. – С.30 – 31.
 - [2] Деркач М.С. Дослідження геометричних характеристик скручених антипризм з рівностороннім напівправильним многокутником в основі // Матеріали XIX Міжнародної науково-практичної конференції студентів, аспірантів та молодих вчених «Шевченківська весна – 2021», квітень 2021 року, Київ, Україна. – С.13 – 14.
-

Автори

Михайло Сергійович Деркач — учень 10-го класу, гімназія № 283, Київ, Україна; E-mail: mishaderkach7v@ukr.net

Morse-Smale flows in the Boy's surface

Luca Di Beo

Morse-Smale (MS) dynamical systems are amongst the simplest possible dynamical systems, with strong restrictions imposed on its critical points. In this thesis, I present a brief history of the development of the theory, along with the introduction of important definitions, theorems and lemmas. Moreover, I investigate MS systems in the Boy's surface (P^4), with emphasis on optimal ones. A method relying only on topological features has been used in order to classify MS systems in P^4 . A review of some topological properties of this space is presented in order to construct the necessary arguments that allowed the discovery of this type of flow in P^4 .

At the time this thesis was written, there was no current work in the literature regarding the classification of all optimal MS flows in P^4 . Hence, my original contribution to knowledge here is the finding of all 342 optimal MS flows in P^4 , the finding of all 80 optimal Projective MS (PMS) flows (Projective MS flows in P^4 are those MS flows in P^4

that can be extended to MS flow in $\mathbf{R}P^2$). in P^4 , and the exposure of a few non-optimal ones, as a preparatory path for future researchers, all up to symmetry.

Автори

Luca Di Beo — студент 6-го курсу, механіко-математичний факультет, Київський національний університет імені Тараса Шевченка, Київ, Україна; E-mail: dibeoluca@gmail.com

Оцінка параметра зсуву θ в моделі з двома дробовими броунівськими рухами

Ю. С. Мішура, Г. С. Железняк

Розглядається задача оцінки невідомого параметра зсуву θ в моделі

$$X_t = \theta t + B_t^{H_1} + B_t^{H_2}, \quad t \in [0, T],$$

де B^{H_1} та B^{H_2} — два незалежні дробові броунівські рухи з різними індексами Хюрста $1/2 \leq H_1 < H_2 < 1$ та параметри H_1 і H_2 відомі. У [1] було показано, що оцінка максимальної вірогідності (ОМВ) має вигляд

$$\hat{\theta}_T = \frac{\int_0^T h_T(t) dY_t}{\gamma_{H_1}(2 - 2H_1) \int_0^T h_T(t) t^{1-2H_1} dt},$$

де процес $Y_t = c_{H_1} \int_0^t s^{\frac{1}{2}-H_1} (t-s)^{\frac{1}{2}-H_1} dX_s$. Зображення оцінки на $[0, T]$ спирається на розв'язок інтегрального рівняння Фредгольма 2-го роду

$$h_T(u) + \frac{1}{2 - 2H_1} \int_0^T h_T(s) K(s, u) ds = 1, \quad u \in [0, T].$$

зі слабо-сингулярним ядром $K(s, u) = u^{1-2H_1} \int_0^{s \wedge u} \varphi(s, v) \varphi(u, v) dv$, де

$$\varphi(s, v) = \frac{\partial}{\partial s} K_{H_1, H_2}(s, v)$$

та

$$K_{H_1, H_2}(s, v) = \beta_{H_2} c_{H_1} v^{\frac{1}{2}-H_2} \int_s^v (s-z)^{\frac{1}{2}-H_1} z^{H_2-H_1} (z-v)^{H_2-\frac{3}{2}} dz.$$

Оцінки $\hat{\theta}_T^{(1)} = \frac{X_T}{T}$ та $\hat{\theta}_T^{(2)} = \frac{\int_0^T X_t dt}{T}$ було розглянуто в якості альтернативних. Поведінку трьох оцінок параметрів зсуву порівняно за допомогою чисельного моделювання. Як правило, оцінка $\hat{\theta}_T^{(1)}$ збігається трохи повільніше, ніж $\hat{\theta}_T$. Однак, перевага $\hat{\theta}_T^{(1)}$ у простоті формі, тому обчислювати її швидше. Оцінка $\hat{\theta}_T^{(2)}$ працює значно гірше, ніж $\hat{\theta}_T$ та $\hat{\theta}_T^{(1)}$, тому ми не рекомендуємо її використовувати.

Список літератури

- [1] Y. Mishura, *Maximum likelihood drift estimation for the mixing of two fractional Brownian motions*, in Stochastic and Infinite Dimensional Analysis, 2016, pp. 263–280.

Автори

Юлія Степанівна Мішура — д.ф.-м.н., професор, механіко-математичний факультет, Київський національний університет імені Тараса Шевченка, Київ, Україна; E-mail: myus@univ.kiev.ua

Ганна Сергіївна Железняк — аспірант 4-го року навчання, механіко-математичний факультет, Київський національний університет імені Тараса Шевченка, Київ, Україна; E-mail: hanna.zhelezniak@knu.ua

Задачі оптимального керування на півосі для диференціальних включень зі швидкоколивними коефіцієнтами

Т. Ю. Жук

У роботі застосовано метод усереднення до розв’язання задачі оптимального керування зі швидкоколивними змінними, лінійної за керуванням, на скінченному інтервалі. Об’єктом керування при цьому виступає система диференціальних включень з Ліпшицевою за фазовою змінною правою частиною. Розглянемо задачу оптимального керування системи диференціальних включень на півосі з малим параметром і швидко осцилюючими коефіцієнтами

$$\dot{x} \in f\left(\frac{t}{\varepsilon}, x\right) + f_1(x)u(t), x(0) = x_0 \quad (1)$$

із критерієм якості

$$J_\varepsilon[u] = \int_0^\infty \left(e^{-jt} A(t, x_\varepsilon(t)) + u^2(t) \right) dt \rightarrow \inf \quad (2)$$

Тут $\varepsilon > 0$ - малий параметр, $j > 0$ - фіксована стала, що характеризує дисконт, x - фазовий вектор в R^d , $u(t)$ - m -вимірний вектор керування, який приймає значення у деякій множині $U \subset R^m$. Нехай для багатозначної функції f існує рівномірно за $x \in R$ середнє

$$\lim_{s \rightarrow \infty} \frac{1}{s} \int_0^s f(t, x) dt = f_0(x), \quad (3)$$

де інтеграл від багатозначної функції розуміємо в сенсі Аумана, а границя багатозначної функції розуміється в сенсі Хаусдорфа. Задачі оптимального керування на півосі 1, 2 ставиться у відповідність усереднена задача керування:

$$\dot{y} = f_0(y) + f_1(y)u(t), y(0, u(0)) = x_0 \quad (4)$$

із критерієм якості

$$J_0[[, u] = \int_0^{\infty} (e^{-jt} A(t, y(t)) + u^2(t)) dt \rightarrow \inf \quad (5)$$

Автори

Тетяна Юріївна Жук — студентка 2-го курсу магістратури, механіко-математичний факультет, Київський національний університет імені Тараса Шевченка, Київ, Україна; E-mail: zhuktanya18@ukr.net

Дослідження динаміки фінансового ринку в умовах макроекономічної невизначеності

В.П. Зубченко

Введення в Україні з 24 лютого 2022 р. воєнного стану та впровадження обмежень на фінансовому ринку згідно Постанови Національного банку України “Про роботу банківської системи в період запровадження воєнного стану” привело до істотної зміни динаміки ключових макропоказників та фінансових інструментів.

У відповідності до вказаної Постанови зафіксований ряд показників діяльності фінансового ринку: облікова ставка, офіційний курс до дол. США, споживча інфляція, крива дохідності до погашення за облігаціями внутрішньої державної позики, Український індекс міжбанківських ставок овернайт (UONIA). Тимчасові обмеження торкнулись операцій за багатьма класичними фінансовими інструментами, міжбанківський ринок працює здебільшого на забезпечення операцій критичної фінансової інфраструктури. Воєнні дії привели до втрати значної частини ВВП, в той же час починає надходити усі більше фінансової допомоги від міжнародних фінансових інститутів (МВФ, Світовий банк, ЄБРР) та країн-партнерів.

Дослідження прибутковості та ризиковості фінансових операцій, прогнозування майбутньої динаміки здійснюється із використанням сценарного підходу. У зв'язку із обмеженнями на фінансовому ринку та загалом тимчасової відсутності ринкових даних для побудови оцінок використовуються нестандартні моделі.

У роботі досліджено динаміку ключових макроекономічних показників, проведено аналіз їх чутливості до стрес-факторів, оцінено вплив на зміну показників прибутковості та ризиковості основних та похідних фінансових інструментів.

Автори

Володимир Петрович Зубченко — канд. фіз.-мат. наук, асистент кафедри теорії ймовірностей, статистики та актуарної математики, механіко-математичний факультет, Київський національний університет імені Тараса Шевченка, Київ, Україна; E-mail: volodymyr.zubchenko@knu.ua

Around the Euler's constant

M. V. Kachaikin

Euler's constant was discovered by mathematician Leonhard Euler in 1734. It is defined as a limit of difference of sequence of partial sums of the harmonic series and natural logarithm:

$$\gamma = \lim_{n \rightarrow \infty} \left(\sum_{k=1}^n \frac{1}{k} - \ln(n) \right) = 0.5772156..$$

By analogy to Euler's constant, based on results of article [1], we constructed one-parameter family of constants, which defined as a limit of a difference of sequence of partial sums of the generalized harmonic series and related integral which depends on parameter:

$$\nu(\alpha) := \lim_{n \rightarrow \infty} \left[\sum_{k=1}^n \frac{1}{k^\alpha} - \int_1^n \frac{dt}{t^\alpha} \right], \alpha \geq 0$$

We showed that $\nu(\alpha)$ is correctly defined, infinitely differentiable on $(0, +\infty)$, discovered that it discontinuous at zero, found a limit as $\alpha \rightarrow +\infty$, and proved that for every $\alpha \geq 0$ holds inequality: $0 \leq \nu(\alpha) \leq 1$.

Results of research accepted for submission in Scientific Bulletin of Uzhhorod University. Series of mathematics and informatics, Vol. 40, No 1.

References

- [1] Kurchenko O.O. Analog staloi Oylera dlya monotonnoyi, zbizhnoyi do nulya funktsiyi [Analogy of Euler's constant for monotone function, which converges to zero]. Scientific Bulletin of Taras Shevchenko National University of Kyiv, Series: Physics and Mathematics. - 2011. - Issue 4 - p.26-29. [in Ukrainian].
-

Authors

Marko Kachaikin — 3rd year Bachelor's degree student, Faculty of Mechanics and Mathematics, Taras Shevchenko National University of Kyiv, Kyiv, Ukraine; E-mail: kachaikinmarko.sci@gmail.com

Математичне моделювання динаміки страхового сектору економіки України

В. В. Копил, В. П. Зубченко

У той час як наслідки COVID-19 та ймовірна, але примарна, загроза повномасштабного військового вторгнення Росії на територію України були визначені як головні загрози стабільності роботи українського страхового ринку, історія 24 лютого 2022 року внесла свої корективи. На жаль, воєнні дії вже більше не будуть розглядатися у площині ймовірності, бо факт початку війни вже стався і чим більше війна триває, тим гірша настає економічна ситуація в країні. Головною метою роботи є проведення стрес-тестування про діяльність страховика по головним ризикам страхового сектору України. Отже, було проведено стрес-тестування діяльності страховика за державними вимогами, використано у дослідженні кризи 2014 року як приклад періоду початку російської агресії проти України. Як наслідок, визначені ключові фактори впливу найголовніших загроз розвитку та стабільності страхової діяльності у залежності від внутрішніх та зовнішніх факторів впливу такі як відтік іноземних інвестицій, вплив COVID-19, прискіпливий моніторинг страхових компаній Нацбанком та інфляції, але найнагальніший ризик на сьогодні є, безперечно, війна. Дослідження проводилися на основі наведених формул у Законі України [1] та європейських вимог директиви Solvency II, що почала запроваджуватися в українській економіці.

Список літератури

- [1] Розпорядження «Про затвердження Вимог щодо регулярного проведення стрес-тестування страховиками та розкриття інформації щодо ключових ризиків та результатів проведених стрес-тестів» від 13.02.2014 р. <https://zakon.rada.gov.ua>

Автори

Валентина Валеріївна Копил — студентка 2-го курсу магістратури, механіко-математичний факультет, Київський національний університет імені Тараса Шевченка, Київ, Україна; E-mail: valyshakopyl@ukr.net

Володимир Петрович Зубченко — канд. фіз.-мат. наук, асистент кафедри теорії ймовірностей, статистики та актуарної математики, механіко-математичний факультет, Київський національний університет імені Тараса Шевченка, Київ, Україна; E-mail: volodymyr.zubchenko@knu.ua

Small counts in nested Karlin's occupancy scheme generated by discrete Weibull-like distributions

V. Kotelnikova

A nested Karlin's occupancy scheme is a symbiosis of classical Karlin's balls-in-boxes scheme and a weighted branching process. To define it, imagine a deterministic weighted branching process in which weights of the first generation individuals are given by the elements of a discrete probability distribution. For each positive integer j , identify the j th generation individuals with the j th generation boxes. The collection of balls is one and the same for all generations, and each ball starts at the root of the weighted branching process tree and moves along the tree according to the following rule: transition from a mother box to a daughter box occurs with probability given by the ratio of the daughter and mother weights.

Assume that there are n balls and that the discrete probability distribution responsible for the first generation is Weibull-like. Denote by $\mathcal{K}_n^{(j)}(l)$ and $\mathcal{K}_n^{*(j)}(l)$ the number of the j th generation boxes which contain at least l balls and exactly l balls, respectively. We prove functional limit theorems (FLTs) for the matrix-valued processes $(\mathcal{K}_{[e^{T+\cdot}]}^{(j)}(l))_{j,l \in \mathbb{N}}$ and $(\mathcal{K}_{[e^{T+\cdot}]}^{*(j)}(l))_{j,l \in \mathbb{N}}$, properly normalized and centered, as $T \rightarrow \infty$. The present FLTs are an extension of a FLT proved by Iksanov, Kabluchko and Kotelnikova [1] for the vector-valued process $(\mathcal{K}_{[e^{T+\cdot}]}^{(j)}(1))_{j \in \mathbb{N}}$. While the rows of each of the limit matrix-valued processes are independent and identically distributed, the entries within each row are stationary Gaussian processes with explicitly given covariances and cross-covariances. We provide an integral representation for each row. The results obtained are new even for Karlin's occupancy scheme.

The talk is based on a joint work with A. Iksanov (Kyiv) [2].

References

- [1] A. Iksanov, Z. Kabluchko and V. Kotelnikova, *A functional limit theorem for nested Karlin's occupancy scheme generated by discrete Weibull-like distributions*. J. Math. Anal. Appl. **507** (2022), 125798.
- [2] A. Iksanov and V. Kotelnikova, *Small counts in nested Karlin's occupancy scheme generated by discrete Weibull-like distributions*. Preprint (2022) available at <https://arxiv.org/abs/2203.08918>

Valeriya Kotelnikova — 4th year student, Faculty of Computer Science and Cybernetics, Taras Shevchenko National University of Kyiv, Kyiv, Ukraine; E-mail: valeria.kotelnikova@unicyb.kiev.ua

Про обмежені в середньому розв'язки різницевих рівнянь другого порядку

В. П. Кравець, М. Ф. Городній

Отримано оцінку близькості компонент єдиного обмеженого у середньому розв'язку різницевого рівняння другого порядку зі стрибком операторного коефіцієнта до компонент обмеженого у середньому розв'язку різницевого рівняння зі сталим операторним коефіцієнтом.

Нехай $(X, \|\cdot\|)$ — комплексний банахів простір; $\mathcal{L}(X)$ — банахів простір усіх лінійних обмежених операторів, що діють в X ; I, O — відповідно одиничний та нульовий оператори в X . Нехай $(\Omega, \mathcal{F}, P)$ — повний імовірнісний простір.

Розглянемо різницеві рівняння

$$\begin{cases} \xi_{n+1} - 2\xi_n + \xi_{n-1} = A\xi_n + \eta_n, & n \geq 1, \\ \xi_{n+1} - 2\xi_n + \xi_{n-1} = B\xi_n + \eta_n, & n \leq 0, \end{cases} \quad (1)$$

$$\zeta_{n+1} - 2\zeta_n + \zeta_{n-1} = A\zeta_n + \eta_n, \quad n \in \mathbb{Z}. \quad (2)$$

у яких A, B — фіксовані оператори з $\mathcal{L}(X)$, $\{\eta_n, n \in \mathbb{Z}\}$ — задана обмежена в середньому послідовність X -значних випадкових елементів, $\{\xi_n, n \in \mathbb{Z}\}, \{\zeta_n, n \in \mathbb{Z}\}$ — шукані обмежені в середньому послідовності X -значних випадкових елементів простору $(\Omega, \mathcal{F}, P)$.

Отримано достатні умови на оператори A, B , при виконанні яких і різницеve рівняння (1), і різницеve рівняння (2) має для довільної обмеженої в середньому послідовності $\{\eta_n, n \in \mathbb{Z}\}$ єдиний обмежений у середньому розв'язок, а також знайдуться сталі $\rho \in (0, 1)$, $C > 0$, $n_0 \in \mathbb{N}$, які залежать тільки від операторів A, B і такі, що для кожної обмеженої в середньому послідовності $\{\eta_n, n \in \mathbb{Z}\}$ для відповідних до цієї послідовності обмежених у середньому розв'язків $\{\xi_n, n \in \mathbb{Z}\}$ рівняння (1) та $\{\zeta_n, n \in \mathbb{Z}\}$ рівняння (2) виконується оцінка:

$$\forall n \geq n_0 : E\|\xi_n - \zeta_n\|_X \leq C\rho^n \sup_{n \in \mathbb{Z}} E\|\eta_n\|_X.$$

Михайло Федорович Городній — д.ф.-м.н., професор, механіко-математичний факультет, Київський національний університет імені Тараса Шевченка, Київ, Україна; E-mail: horodnii@gmail.com

Вікторія Павлівна Кравець — аспірантка 3-го року навчання, механіко-математичний факультет, Київський національний університет імені Тараса Шевченка, Київ, Україна; E-mail: toriawik@ukr.net

Непараметричні тести для порівняння виживання у двох групах

М. В. Любима

Одним із ключових об'єктів аналізу у клінічних дослідженнях є час до визначеної події, а також порівняння двох груп пацієнтів. Чи є ризики у двох групах однаковими? Якщо ні, то яка має більшу тенденцію до настання події? Виходячи з особливостей даних клінічних досліджень, для відповідей на ці питання потрібна більш потужна методика, аніж порівняння функцій ризику поточною або аналіз середніх часу виживання. Найбільш поширеним є лог-ранк тест [1]. Припускається, що відношення функцій ризику двох груп з часом залишається сталим з параметром β :

$$\frac{h_1(t)}{h_2(t)} = \exp(\beta) \quad (1)$$

Основна статистична гіпотеза $H_0 : \beta = 0$. Іншими словами, що криві виживання двох груп однакові. Дається оцінка кількості подій, які б можна було очікувати після попередньої, припускаючи, що різниці між групами немає. Для цього використовується хі-квадрат статистика [1] або оцінка Мантеля-Гензеля [2], якщо попередньо розділити час на інтервали.

Якісною відмінністю і перевагою такого методу є те, що враховується, коли саме подія відбувається, а не лише факт її настання. Таким чином, є сенс використання даного тесту для більшої гнучкості у часі, якщо, наприклад, періоди нагляду за пацієнтами різняться та (або) маємо справу з цензурованими даними.

Розглянуто застосування представлених підходів для обчислення статистик на ілюстративному датасеті, що викладено у вільний доступ.

Аналогічну статистику можна застосувати і для більш складного завдання, досліджуючи вплив одного з факторів (первинного), параметризуючи інші змінні.

Список літератури

- [1] Clark, T., Bradburn, M., Love, S. et al. Survival Analysis Part I: Basic concepts and first analyses. Br J Cancer 89, 232–238 (2003).
 - [2] B. Rosner, "Introduction to Survival Analysis," in Fundamentals of Biostatistics Seventh Edition, Cengage Learning, Inc..
-

Автори

Михайліна Вікторівна Любима — студентка 4-го курсу, механіко-математичний факультет, Київський національний університет імені Тараса Шевченка, Київ, Україна; E-mail: mishlyu@knu.ua

Асимптотична поведінка розв'язку параболічного рівняння зі стохастичною мірою при $t \rightarrow \infty$

Б. І. Манікін

Нехай X - довільна множина, $\mathcal{B}$ - σ -алгебра підмножин X , $L_0 = L_0(\Omega, \mathcal{F}, P)$ - множина всіх випадкових величин на повному ймовірнісному просторі $(\Omega, \mathcal{F}, P)$. Стохастичною мірою на $\mathcal{B}$ називається σ -адитивне відображення $\mu : \mathcal{B} \rightarrow L_0$.

У роботі [1] розглянуто м'який розв'язок параболічного рівняння:

$$u(t, x) = \int_{\mathbb{R}} p(t, x; 0, y) u_0(y) dy + \int_0^t ds \int_{\mathbb{R}} p(t, x; s, y) f(s, y, u(s, y)) dy + \int_{\mathbb{R}} d\mu(y) \int_0^t p(t, x; s, y) \sigma(s, y) ds, \quad (1)$$

де $(t, x) \in [0, +\infty) \times \mathbb{R}$, $u : [0, +\infty) \times \mathbb{R} \times \Omega \rightarrow \mathbb{R}$, стохастична міра μ визначена на борельовій σ -алгебрі, $p(t, x; s, y)$ - фундаментальний розв'язок параболічного оператора

$$\mathcal{L}u(t, x) = a(t) \frac{\partial^2 u(t, x)}{\partial x^2} + b(t) \frac{\partial u(t, x)}{\partial x} + c(t) u(t, x) - \frac{\partial u(t, x)}{\partial t}. \quad (2)$$

У доповіді сформульовано умови на функції a, b, c з (2), u_0, f, σ з (1), за яких

$$\sup_{x \in \mathbb{R}} |u(t, x)| \rightarrow 0, \quad t \rightarrow \infty,$$

де збіжність розглядається у сенсі м. с.

Список літератури

- [1] І. М. Боднарчук, *Регулярність м'якого розв'язку параболічного рівняння зі стохастичною мірою*, Укр. мат. журн., 2017, т.69, вип. 1.
-

Автори

Манікін Борис Ігорович — аспірант 1-го року навчання, механіко-математичний факультет, Київський національний університет імені Т. Г. Шевченка, Київ, Україна; E-mail: bmanikin@gmail.com

Прогнозування демографічних показників за допомогою сплайнів з урахуванням економічних показників

А. А. Мелекесцева

На підставі даних Держкомстату України за 1979–2019 рр. було спрогнозовано ймовірні зміни чисельності, народжуваності та смертності населення м. Коростеня і 5 районів Житомирської області за допомогою сплайнової моделі спостережень [1]:

$$y_i = S(t_i) + \sigma \varepsilon_i, \quad i = 1, \dots, n, \quad (1)$$

де y_i – спостережувані випадкові величини у відомі моменти часу t_i ; S – невідомо-ма функція регресії, що є поліноміальним сплайном з певною сіткою вузлів; ε_i – незалежні випадкові величини, що мають стандартний нормальний розподіл; σ – невідоме стандартне відхилення похибок спостережень.

Побудовано 95 % довірчі смуги для динаміки показників на 1979–2023 рр., а також довірчі інтервали для прогнозів на 2020–2023 рр.

Планується уточнити отримані прогнози, для чого потрібно брати до уваги динаміку економічних показників. Будемо розглядати дещо змінену модель спостере-

жень:

$$y_i = S(t_i) + \beta U_i + \sigma \varepsilon_i, \quad i = 1, \dots, n, \quad (2)$$

де U_i - вектор із 3-5 економічних показників, котрі найбільше впливають на певний демографічний показник; β - відповідні коефіцієнти, які потрібно оцінити.

З метою визначити, які економічні показники найбільше впливають на досліджувані демографічні показники, було обчислено попарні коефіцієнти кореляції між економічними і демографічними показниками. Виявлено, що найбільше пов'язані з демографічними наступні економічні показники: доходи і витрати населення, середньомісячні заробітна плата й пенсія, валовий регіональний продукт та кількість лікарів.

Планується здійснити прогнозування за описаним методом і порівняти отримані прогнози із прогнозами, зробленими раніше без урахування економічних даних.

Список літератури

- [1] Кукуш А. Г. Кубические одномерные сплайны в статистике: Метод. рекомендації для студентів механіко-математического факультета. Київ : КГУ, 1991. 60 с.

Автори

Аліса Андріївна Мелекесцева — студентка 1-го курсу магістратури, механіко-математичний факультет, Київський національний університет імені Тараса Шевченка, Київ, Україна; E-mail: homtom.alice.2016@gmail.com

Рівняння Беллмана для задачі оптимального керування диференціальними рівняннями з імпульсною дією

П. С. Михайлюк

Розглядається така задача оптимального керування імпульсною системою з нефіксованими моментами імпульсів:

$$\varphi(T, x(T)) \rightarrow \inf, \dot{x} = f(t, x(t), u(t)), t \in [0; T], t \neq \tau_i(x), \tau_i \xrightarrow{i \rightarrow \infty} \infty,$$

$$\Delta|_{t=\tau_i} = I_i(x, v_i), i \in \mathbb{N}, x(0) = x_0, u(t) \in U \subset \mathbb{R}^m, v_i \in V \subset \mathbb{R}^k, \forall t \in [0, T]$$

Задача оптимального керування полягає в тому, щоб серед усіх допустимих керувань, які переводять точку з положення $(0; x_0)$ в деяку замкнену множину M , знайти таке, яке мінімізує функціонал φ . Функцію $B(s, y) = \inf_{(u, v) \in \mathcal{J}_{s, y}} \varphi(T, x(T))$

називають функцією Беллмана початкової задачі, де $\mathcal{J}_{s, y}$ - множина допустимих керувань, що переводять систему з положення (s, y) у множину M . Показано, що функція Беллмана має такі властивості:

1. Функція Беллмана задовольняє крайову умову $B(s, y) = \varphi(s, y)$ при $(s, y) \in M$.
2. Якщо $(u(t), v_i) \in \mathcal{J}_{0, x_0}$ а $x(t)$ — інтегральна крива, яка відповідає даним керуванням, то функція Беллмана $B(t, x(t))$ вздовж неї є неспадною на $[0; T]$.
3. Функція Беллмана вздовж оптимальної кривої стала.

Виходячи з даних властивостей, отримано систему рівнянь Беллмана для даної задачі оптимального керування:

$$\begin{cases} \min_{u \in U} \{ \frac{\delta B(t, x)}{\delta t} \} + \langle \nabla_x B(t, x), f(t, x, u) \rangle = 0, t \neq \tau_i(x) \\ \min_{v \in V} \{ B(\tau_i(x), x + I_i(x, v)) - B(\tau_i(x), x) \} = 0, t = \tau_i(x) \end{cases}$$

Маючи функцію Беллмана, можна розв'язати задачу оптимального керування методом динамічного програмування. Такий підхід застосовано до лінійно-квадратичної задачі з імпульсною дією.

Список літератури

- [1] WENDELL H. FLEMING. Optimal Control of Markov Diffusion Processes / Wendell H. Fleming, Raymond W. Rishel // Deterministic and Stochastic Optimal Control / Wendell H. Fleming, Raymond W. Rishel. – New York: Springer, 1975. – (0172-4568). – С. 151–197.

Authors

Павло Сергійович Михайлюк — студент 4-го курсу, механіко-математичний факультет, Київський національний університет імені Тараса Шевченка, Київ, Україна;; E-mail: pashamxl10@knu.ua

Метод складаного ножа для суміші нелінійних регресій

В.О. Мірошніченко

В даній роботі розглядаються оцінки коефіцієнтів регресії, отримані узагальненим методом найменших квадратів за спостереженнями суміші зі змінними концентраціями. Для цих оцінок параметрів будується консистентна оцінка матриці коваріацій.

Ми розглядаємо відібрані об'єкти із суміші зі змінними концентраціями. У кожного з n об'єктів спостерігаються дві змінні $(X_j, Y_j)_{j=1}^n$, для яких виконується модель нелінійної регресії $Y_j = g(X_j, b^{(\kappa_j)}) + \varepsilon_j^{(\kappa_j)}$. Тут g - відома регресійна функція, $b^{(k)}$ - вектор невідомих коефіцієнтів регресії k -го компонента, $\varepsilon_j^{(k)}$ - похибка регресії, κ_j - номер компонента суміші, якому належить j -тий об'єкт (не спостерігається).

Оцінка $\hat{b}_n^{(k)}$ коефіцієнтів регресії - це розв'язок оціночного рівняння:

$$J_n^k(\gamma) = \sum_{j=1}^n a_{j:n}^k (Y_j - g(X_j, \gamma)) \nabla g(X_j, \gamma) = \bar{0},$$

тут $a_{j:n}^k$ - мінімаксні ваги з [1]. Як показано у [1],

$$\sqrt{n} V_n^{-\frac{1}{2}} (\hat{b}_n^{(k)} - b^{(k)}) \rightarrow^w N_d(0, I_d).$$

Оцінкою матриці V_n методом складаного ножа називається наступна оцінка

$$JK\hat{V}_n^{(k)} = \sum_{i=1}^n \left(\hat{b}_{i-;n}^{(k)} - \hat{b}_n^{(k)} \right) \left(\hat{b}_{i-;n}^{(k)} - \hat{b}_n^{(k)} \right)^T.$$

Тут $\hat{b}_{i-;n}^{(k)}$ - оцінки параметрів $b^{(k)}$, що пораховані із вилученням з вибірки i -м спостереженням. При виконанні певних умов

$$JK\hat{V}_n^{(k)} - V_n \xrightarrow{P} 0, \quad n \rightarrow \infty.$$

Список літератури

- [1] Miroshnychenko V., Maiboroda R. “Asymptotic normality of modified LS estimator for mixture of nonlinear regressions”, Modern Stochastics: Theory and Applications, Vol.7, Iss.7 pp. 435 - 448, - 2020
-

Автори

Мірошниченко Віталій Олегович — аспірант 4-го курсу, механіко-математичний факультет, Київський національний університет імені Тараса Шевченка, Київ, Україна; E-mail: vitaliy.miroshnychenko@gmail.com

Ергодичність процесів типу Леві на прямій

Я. Г. Мокану

Дана робота написана за результатами сумісної праці з В.П. Кноповою. Метою роботи є дослідження ергодичності процесів типу Леві, чий феллерівський генератор, визначений на функціях $f \in C_\infty^2(\mathbb{R})$, має вигляд

$$Lf(x) = \int_{\mathbb{R} \setminus \{0\}} (f(x+u) - f(x) - uf'(x)\mathbb{I}_{|u| \leq 1}) \nu(x, du),$$

де $\nu(x, du)$ — ядро типу Леві.

Будемо припускати, що міра $\nu(x, \cdot)$ є симетричною при кожному значенні x , тобто $\nu(x, A) = \nu(x, -A)$, $A \in \mathcal{B}(\mathbb{R})$, $\{0\} \notin A$, а її хвости $N(x, u) = \nu(x, (-\infty, u])$, $u < 0$, задовольняють наступну умову

$$\lambda^{-\delta(x)} \leq \liminf_{u \rightarrow \infty} \frac{N(x, \lambda u)}{N(x, u)} \leq \limsup_{u \rightarrow \infty} \frac{N(x, \lambda u)}{N(x, u)} \leq \lambda^{-\sigma(x)},$$

$\forall \lambda \geq 1, |x| \geq 1$ та для деяких обмежених $0 < \sigma \leq \sigma(x) \leq \delta(x) \leq \delta$.

Для перевірки ергодичності використовується критерій Фостера-Ляпунова. В якості тестової функції розглядається $V_\gamma(x) = \Phi_\gamma^p(x)$, де $\Phi_\gamma(x) = |x|$ для $|x| > \gamma$ та $\Phi_\gamma(x) = \phi_\gamma(x) \in C^2(\mathbb{R})$ для $|x| < \gamma$.

Теорема 1. Якщо виконуються описані вище припущення, то для $p \in (1, \sigma)$, $\sigma \leq \delta$, $\delta \in (1, 2]$ процес є ергодичним.

Список літератури

- [1] S.P. Meyn and R.L. Tweedie. Markov chains and stochastic stability. Springer, 1993.
 - [2] S.P. Meyn and R.L. Tweedie. Stability of markovian processes III: Foster-Lyapunov criteria for continuous-time processes. Applied Probability Trust 1993.
 - [3] N. Sandric. Long-time behavior of stable-like processes. Stoch. Proc. Appl. 123 (2013), 1276-1300.
-

Автори

Яна Георгіївна Мокану — студентка 2-го курсу магістратури, механіко-математичний факультет, Київський національний університет імені Тараса Шевченка, Київ, Україна; E-mail: yana.mokanu3075@gmail.com

О-сфероїди в метричних та лінійних нормованих просторах

І. А. Овцинов

Дане наукове повідомлення присвячене вивченню відкритих і замкнених О-сфероїдів — множин у метричних просторах, частинним випадком яких є відкриті кулі у відповідних просторах. Такий підхід є цілком логічним з огляду узагальнення випадку кола на ситуацію еліпса в геометрії. Відкритими О-сфероїдами називають множини виду

$$A = \{x \in X \mid \rho(x, x_1) + \dots + \rho(x, x_n) < a\}, \quad (1)$$

де $x_1, \dots, x_n$ — попарно різні фіксовані точки простору (X, ρ) з метрикою ρ , які називаються *фокусами О-сфероїда*, а a — фіксована додатна стала — *радіус О-сфероїда*. В означенні замкненого О-сфероїда в (1) виконуватиметься нестрога нерівність.

Введено поняття багатоцентрового О-сфероїда — О-сфероїда, якому належать усі його фокуси. Пояснено, коли О-сфероїд може бути багатоцентровим. Сформульовано й доведено принцип замкнених О-сфероїдів, що є узагальненням відомого принципу замкнених куль. З'ясовано, в яких випадках фокуси О-сфероїда в евклідовому просторі розмірності 3 можуть бути вершинами правильного тетраедра. Досліджено, які О-сфероїди на евклідовій площині можна вписати в трикутник Рело [1, с. 91], що може бути корисним у прикладних задачах механіки, оскільки трикутник Рело є фігурою сталої ширини [2, с. 196].

Крім того, введено поняття радіуса Вороного О-сфероїда в евклідовому метричному просторі зі стандартною метрикою та встановлено нерівність, яка пов'язує цей радіус з точкою Ферма–Торрічеллі [3, с. 236].

Означення та властивості відкритих і замкнених О-сфероїдів легко розповсюджуються на випадок лінійних нормованих просторів. Це, у свою чергу, дозволяє вивчити можливості застосування цих об'єктів у функціональному аналізі.

Список літератури

- [1] Яглом И. М., Болтянский В. Г. Выпуклые фигуры. — М.—Л.: ГИТТЛ, 1951. — (Библиотека математического кружка; Вып. 4).
- [2] Радемахер Г., Тёплиц О. Числа и фигуры: Опыты математического мышления. — М.: ОНТИ, 1936. — (Библиотека математического кружка; Вып. 10). — [Переиздания: 1938, 1962, 1966, 2020]. — § 25 «Кривые постоянной ширины»].
- [3] Boltyanski, V., Martini, H., Soltan, V. (1999), *Geometric methods and optimization problems*, Kluwer Acad. Publ., Dordrecht, Netherlands.

Автори

Ілля Аркадійович Овцинов — студент 4-го курсу, механіко-математичний факультет, Київський національний університет імені Тараса Шевченка, Київ, Україна; E-mail: iliarkov@gmail.com

Unitary Cayley and total graphs of boolean algebras

D. Oliynyk

Let A be an associative algebra with an identity. The *unitary Cayley graph* of A is the graph in which the vertex set consists of all elements of A and two vertices a and b are connected with an edge if and only if $a - b$ is a unit element of A . Such graphs and their properties were studied for matrix algebras [1] and for rings [2, 3]. Unitary Cayley graphs of boolean algebras are considered in this work, and their properties are described. In particular, the following theorem is proved:

Theorem 1. The unitary Cayley graph of any boolean algebra A with distinct additive and multiplicative identities:

- a) is a regular bipartite graph;
- b) has a diameter of 1;
- c) consists of vertices of degree 1;
- d) has $\frac{|A|}{2}$ connected components if A is finite.

In addition, a notion of *total graph* for boolean algebras is considered [4]. The total graph of algebra A has the same set of vertices as the unitary Cayley graph of A . Two distinct vertices a and b are connected if and only if $a + b$ is a zero divisor.

The following results were obtained for total graphs:

Theorem 2. The total graph of any boolean algebra A with distinct additive and multiplicative identities:

- a) is a regular connected graph;
- b) consists of vertices of degree $|A| - 2$ if A is finite;
- c) is a complement graph of the unitary Cayley graph of A .

References

- [1] Kiani, Dariush, and Mohsen Mollahajaghaei. "On the unitary Cayley graphs of matrix algebras." *Linear Algebra and its Applications* 466 (2015): 421-428.
- [2] Klotz, Walter, and Torsten Sander. "Some properties of unitary Cayley graphs." *the electronic journal of combinatorics* (2007): R45-R45.
- [3] Maimani, H. R., et al. "Graphs attached to rings revisited." *Arabian Journal for Science and Engineering* 36.6 (2011): 997-1011.
- [4] Anderson, David F., and Ayman Badawi. "The total graph of a commutative ring." *Journal of algebra* 320.7 (2008): 2706-2719.

Authors

Daryna Oliynyk — 2nd year Master's student, Faculty of Mechanics and Mathematics, Taras Shevchenko National University of Kyiv, Kyiv, Ukraine; E-mail: daryna.oliiynyk@gmail.com

Про обмежені на $\mathbb{R}$ розв'язки диференціальних рівнянь з кусково-сталими операторними коефіцієнтами

М. Ф. Городній, О. А. Печериця

Нехай X – комплексний банахів простір, $\mathcal{L}(X)$ – банахів простір лінійних обмежених операторів, що діють із X в X . $C_b(\mathbb{R}, X)$ – банахів простір усіх неперервних і обмежених на $\mathbb{R}$ функцій $f : \mathbb{R} \rightarrow X$ з нормою $\|f\|_\infty := \sup_{t \in \mathbb{R}} \|f(t)\|$. Для $T \in \mathcal{L}(X)$

позначимо через $\sigma(T)$ спектр T . Припустимо, що $\sigma(T) \cap i\mathbb{R} = \emptyset$. Нехай $\sigma_-(T)$ і $\sigma_+(T)$ – частини $\sigma(T)$, що лежать відповідно у лівій і правій півплощині $\mathbb{C}$. Нехай $P_-(T)$ та $P_+(T)$ – проєктори, що відповідають спектральним множинам $\sigma_-(T)$ та $\sigma_+(T)$. Як відомо, тоді простір X є прямою сумою $X = X_-(T) \dot{+} X_+(T)$ підпросторів $X_-(T) := P_-(T)X$ та $X_+(T) := P_+(T)X$.

Нехай A, B – фіксовані оператори з $\mathcal{L}(X)$. Відома теорема М.Г. Крейна стверджує, що диференціальне рівняння

$$u'(t) = Au(t) + y(t), \quad t \in \mathbb{R}, \quad (1)$$

має для кожної функції $y \in C_b(\mathbb{R}, X)$ єдиний обмежений розв'язок u тоді і тільки тоді, коли $\sigma(A) \cap i\mathbb{R} = \emptyset$.

Нами доведено такі теореми.

Теорема 2. Диференціальне рівняння

$$\begin{cases} x'(t) = Ax(t) + y(t), & t \geq 0, \\ x'(t) = Bx(t) + y(t), & t < 0, \end{cases} \quad (2)$$

має єдиний обмежений розв'язок x для кожної обмеженої функції $y \in C_b(\mathbb{R}, X)$ тоді і тільки тоді, коли виконуються наступні умови:

$$a) \sigma(A) \cap i\mathbb{R} = \emptyset, \quad \sigma(B) \cap i\mathbb{R} = \emptyset; \quad b) X = X_-(A) \dot{+} X_+(B).$$

Теорема 3. Якщо виконуються умови $a)$, $b)$, то знайдуться такі залежні тільки від операторів A, B сталі $C > 0$, $\gamma > 0$, що для кожної функції $y \in C_b(\mathbb{R}, X)$ для відповідних до неї обмежених розв'язків u рівняння (1) і x рівняння (2) справджується оцінка

$$\forall t \geq 0 : \|x(t) - u(t)\| \leq Ce^{-\gamma t} \|y\|_\infty.$$

Також отримано достатні умови існування єдиного обмеженого розв'язку для нелінійного аналога рівняння (2).

Автори

Михайло Федорович Городній — д.ф.-м.н., професор, механіко-математичний факультет, Київський національний університет імені Тараса Шевченка, Київ, Україна; E-mail: gorodnii@univ.kiev.ua

Олексій Анатолійович Печериця — аспірант 2-го року навчання, механіко-математичний факультет, Київський національний університет імені Тараса Шевченка, Київ, Україна; E-mail: pecheritsa.aleksey@gmail.com

Стохастичні функціонально-диференціальні рівняння з нескінченним запізненням

О. А. Правдивий

Нехай $C = (C((-\infty, 0], \mathbb{R}), \|\cdot\|_\infty)$

Тут $\|\cdot\|_\infty$ - супремумна норма.

Нехай $w(t)$ - вінерівський процес, визначений на повному імовірнісному просторі $(\Omega, \mathcal{F}, \mathbb{P})$ з фільтрацією $\mathcal{F}_t^w = \sigma(w(u), 0 \leq u \leq t) \vee \mathcal{N} \subset \mathcal{F}$, де $\mathcal{N}$ - множина елементів міри 0 в $\mathcal{F}$.

Розглянемо таке стохастичне функціонально-диференціальне рівняння:

$$d(x(t)) = f(x_t)dt + g(x_t)dw(t), t \geq 0 \quad (1)$$

$$x(t) = q(t), t \leq 0 \quad (2)$$

Тут $q \in C$; $f, g : C \rightarrow \mathbb{R}$ - неперервні; $x_t(s) = x(t+s)$, $s \in (-\infty, 0]$

Доведене таке твердження:

Теорема(існування і єдиність розв'язку рівняння (1-2)):

Нехай для функцій $f(x)$ і $g(x)$ виконуються такі умови:

$$2\langle f(x) - f(y), x(0) - y(0) \rangle + \|g(x) - g(y)\|^2 \leq K\|x - y\|_\infty^2, x, y \in C \quad (3)$$

$$\exists \gamma \geq 1, \exists C \geq 0 : |f(x)| \leq C(1 + \|x\|_\infty^\gamma), x \in C \quad (4)$$

(Умова (3) - умова монотонності, а умова (4) - умова степеневого зростання на $f(x)$)

В такому випадку розв'язок рівняння (1-2) існує і єдиний.

Аналогічна задача, але зі скінченним запізненням розглядалась в [1],[3]

Список літератури

- [1] M. Scheutzow (2018). Stochastic Delay Equations.
- [2] M. Scheutzow (2018). Stochastic Processes II, WT3. Lecture Notes.URL:<https://page.math.tu-berlin.de/~scheutzow/>
- [3] M. von Renesse, M. Scheutzow (2010). Existence and uniqueness of solutions of stochastic functional differential equations. Random Operators and Stochastic Equations, 18 267-284.

Автори

Олександр Андрійович Правдивий — студент 2-го курсу магістратури, механіко-математичний факультет, Київський національний університет імені Тараса Шевченка, Київ, Україна; E-mail: awxrvtb@gmail.com

Про наближення періодичних сплайнів тригонометричними многочленами з інтерполяцією деяких похідних

В. І. Прохорович

Нехай $k, n, n_1 \geq n, b, s, l$ - фіксовані натуральні числа, $x_j := \frac{\pi j}{n}$, $I_j := [x_j, x_{j+1}]$, де $j \in \mathbb{Z}$, $Y_s := \{-\pi \leq y_1 < y_2 < \dots < y_{2s} < \pi\}$ - набір із $2s$ точок, і $\forall \nu \in \mathbb{Z} \quad \forall i \in \{1, \dots, 2s\} : y_{i+\nu \cdot 2s} := y_i + \nu \cdot 2\pi$; також ми вважаємо, що

$\forall i \in \mathbb{Z} : y_{i+1} - y_i > \frac{5\pi}{n}$ і $\pi - y_{2s} > \frac{5\pi}{n}$. Через $\Sigma_{k,n}^l$ позначимо множину l разів неперервно-диференційовних $(\Sigma_{k,n} := \Sigma_{k,n}^0)$ сплайнів $S : \mathbb{R} \rightarrow \mathbb{R}$ таких, що $\forall j \in \mathbb{Z} \exists p_j \in \mathbb{P}_k : S|_{I_j} = p_j$ (тут $\mathbb{P}_k$ - множина всіх алгебраїчних многочленів степеня $\leq k-1$), і покладемо $\Sigma_{k,n}^l(Y_s) := \{S \in \Sigma_{k,n}^l \mid y_i \in [x_j, x_{j+1}] \implies p_{j-1} \equiv p_j \equiv p_{j+1}\}$. Крім того, $\forall x_{j*} < x_{j*}$ назвемо власним відрізком множину $A = [x_{j*}, x_{j*}]$. Нарешті, визначимо $\pi(x) := \prod_{i=1}^{2s} \frac{|\sin(x-y_i)/2|}{|\sin(x-y_i)/2|+1/n}$, а для $S \in \Sigma_{k,n}$ та власного відрізка $A = [x_{j*}, x_{j*}]$ розглянемо величини: $b_{i,j}(S) := \frac{\|p_i - p_j\|_{I_i}}{|i-j|^{k+1}}$, $b_{i,j}(S, A) := \max_{i,j: I_i \subset A \supset I_j} b_{i,j}(S)$, $b(S) := \max_{i,j} b_{i,j}(S)$. Основним нашим результатом є така теорема 1.

Теорема 1. Нехай $l \geq 1$. Тоді існує стала $C = C(k, s, l, b)$, що для довільного 2π -періодичного $S \in \Sigma_{k,n}^l(Y_s)$ знайдеться тригонометричний многочлен D_{n_1} степеня $\leq Cn_1$ (розглядається рівномірна норма):

$$\|S - D_{n_1}\| \leq Cb(S) \quad (1)$$

і якщо A - довільний власний відрізок, то $\forall x \in A$:

$$|S^{(l+1)}(x) - D_{n_1}^{(l+1)}(x)| \leq C_0 n^{l+1} \pi(x) \left(b(S, A) + b(S) \left(\frac{1}{1 + n_1 \text{dist}(x, \mathbb{R} \setminus A)} \right)^b \right), \quad (2)$$

де C_0 залежить від тих же величин, що й C , а в довільній вузловій точці x_j $S^{(l+1)}(x_j) := \frac{1}{2} (S_+^{(l+1)}(x_j) + S_-^{(l+1)}(x_j))$.

Це твердження є узагальненням відповідного результату з [1], де нерівність (2) була доведена при $l = 1$.

Список літератури

- [1] I. O. Shevchuk, O. V. Motorna, D. Leviatan. Coconvex approximation of periodic functions (*to be published*)

Автори

В'ячеслав Ігорович Прохорович — студент 2-го курсу магістратури, механіко-математичний факультет, Київський національний університет імені Тараса Шевченка, Київ, Україна; E-mail: p.slava.ih@gmail.com

Рівносторонні $(m-1)n$ -кутники на базі правильного n -кутника

М. Є. О. Рудик

Властивості многокутників достатньо вивчені, але поява нових типів многокутників потребує дослідження їх властивостей. Як відомо, напівправильні [2] та на чверть правильні [1] многокутники утворюються у результаті добудовування до правильного n -кутника n рівних трикутників зовні таким чином, що одна їх сторона співпадає зі стороною правильного многокутника. По аналогії з цими многокутниками можна розглянути новий тип многокутників; рівносторонні многокутники, які утворені добудовуванням до правильного n -кутника n рівних m -кутників, так що

одна їх сторона (назвемо її основою) співпадає зі стороною правильного багатокутника. При цьому m -кутники можуть бути і виродженими, тобто такими, у яких несусідні сторони можуть перетинатися або лежати на одній прямій. Будемо вважати, що всі сторони m -кутників крім основи рівні. В роботі досліджено умови опуклості таких багатокутників, доведено, що багатокутники, що утворюється з'єднанням вершин через $m - 1$ (так звані базові багатокутники), є правильними.

Список літератури

- [1] Басюк Д.К. 1/4-правильні багатокутники // Матеріали XVII Міжнародної науково-практичної конференції студентів, аспірантів та молодих вчених «Шевченківська весна — 2019», квітень 2019 року, Київ, Україна. — С.7.
- [2] Лоповок Л.М. Напівправильні багатокутники // Квант. — 1971, № 3. — С. 25-29.

Автори

Марія Єлизавета Олександрівна Рудик — учениця 7-го класу, гімназія № 283, Київ, Україна; E-mail: rudykob@gmail.com

Спіральне перетворення з довільним коефіцієнтом чотирикутника

А. О. Рудик

В сучасній математиці широко застосовуються геометричні перетворення для побудови графіків функцій, доведення геометричних теорем.

В даній роботі застосовано означення [3] спірального перетворення з довільним коефіцієнтом $k > 0, k \neq 1$ багатокутника: образом багатокутника $A_1A_2A_3...A_N$ є багатокутник $B_1B_2B_3...A_N$, для якого $\overrightarrow{A_nB_n} = k\overrightarrow{A_nA_{n+1}}, n = 1, 2, \dots, N-1$. Тоді спіральне перетворення, застосоване у роботах [1, 2] є частинним випадком спірального перетворення з довільним коефіцієнтом при $k = 2$.

В роботі доведено такі твердження: образом паралелограма при $k > 0, k \neq 1$ є паралелограм; при $k = 1/2$ образом ромба є прямокутник, а образом прямокутника є ромб; при $k = 1/2$ довільний чотирикутник переходить у паралелограм Варіньона, і площа образу в два рази менша за площу вихідного багатокутника; при $k > 1$ площа образу довільного чотирикутника в $(1 + 2m^2 + 2m^4)$ разів більша за площу прообразу ($m = k - 1$).

Список літератури

- [1] Корольова Л.В. Спіральне перетворення правильних багатокутників // Конкурс науково-технічних проектів учнів Intel-TECHNO Україна 2015-2016. Тези робіт. Категорія «Математика». — К: НТУУ «КПІ», 2015. — С. 202-203.
- [2] Рудик А.О. Спіральне перетворення рівнокутних напівправильних багатокутників // Матеріали XVIII Міжнародної науково-практичної конференції студентів, аспірантів та молодих вчених «Шевченківська весна –2020», квітень 2020 року, Київ, Україна. — С.29-30.
- [3] Рудик А.О. Спіральне перетворення з довільним коефіцієнтом частково правильних багатокутників // Матеріали XIX Міжнародної науково-практичної конференції студентів, аспірантів та молодих вчених «Шевченківська весна –2021», квітень 2021 року, Київ, Україна. — С.27.

Криптосистема Гольдвассер-Мікалі

О. Г. Тищенко

У наш час одним із головних ресурсів повсякденного життя людини є інформація і вміння працювати з нею. Робота з інформацією дуже часто включає етап передавання інформації, що у деяких випадках є вкрай важливим. Тому потрібно вміти передавати інформацію без її спотворення і витоку назовні, що інколи може призводити до великих втрат, наприклад, дані розвідки під час військових операцій. Одним з таких способів захисту інформації під час її передачі є криптосистема, що описана в даній роботі.

Основною метою моєї роботи є розгляд криптосистеми Гольдвассер-Мікалі [3, розділ 3.10], дослідження того, чи є дана криптосистема захищеною, тобто чи захищає даний алгоритм дані, що передаються, від шахраїв.

У роботі розглянуто наступні поняття:

- Неапроксимований предикат
- Ймовірна криптосистема з відкритим ключем
- Поліноміальна захищеність
- Семантична захищеність

У результаті написання даної роботи отримано наступні результати (детальніший огляд наведений в статтях [1], [2]):

- а) Розглянута криптосистема є поліноміально захищеною, що означає, якщо ми маємо функцію f , що виконує шифровку повідомлень, то маючи декілька повідомлень і якийсь шифрований текст одного з цих повідомлень, ми не можемо визначити за поліноміальний час з ймовірністю більшою за 0.5, шифром якого повідомленням є зашифрований текст.
- б) Криптосистема є семантично захищена, тобто якщо стався витік даних, наприклад, стало відомим число з ключа, що не є квадратичним лишком, то дані залишаються захищеними і шахрай не може розшифрувати повідомлення.
- в) Даний алгоритм не є ефективним при передачі великого об'єму даних, якщо наявні апаратні ресурси є обмеженими. Наприклад, для символу "М" ми маємо, що в двійковому форматі це число має вигляд 10000011100, звідки випливає, що замість одного символу довжиною 11 (бітів) ми повинні передати 11 чисел, довжиною k бітів. Як результат, довжина даних збільшується у k разів.

Список літератури

- [1] S. Goldwasser and S. Micali, Probabilistic encryption and how to play mental poker, keeping secret all partial information, in Proceeding of 14th STOC Conference, San Francisco, 1982.
- [2] S. Goldwasser and S. Micali, Probabilistic encryption, in Journal of computer and system sciences 28, pp.270-299(1984)
- [3] Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman. An Introduction to Mathematical Cryptography, Springer, 2008, pp. 113-176

Олег Геннадійович Тищенко — студент 4-го курсу, механіко-математичний факультет, Київський національний університет імені Тараса Шевченка, Київ, Україна; E-mail: sokol.wise@gmail.com

Зв'язок між коливністю розв'язків динамічного рівняння на часових шкалах та коливністю розв'язків диференціального рівняння другого порядку

В. Б. Цань

Нехай $\mathbf{T}$ - часова шкала, тобто довільна непорожня замкнута підмножина $\mathbf{R}$. Оскільки об'єктом дослідження є коливність розв'язків динамічних рівнянь, то вважатимемо, що $\sup \mathbf{T} = \infty$. Для кожної підмножини $[a, b] \subset \mathbf{R}$ позначимо $[a, b]_{\mathbf{T}} = [a, b] \cap \mathbf{T}$.

Для кожного $t \in \mathbf{T}$ визначається [1] три функції, що характеризують шкалу. Перші дві функції: оператор стрибка вперед $\sigma(t) := \inf\{s \in \mathbf{T} : s > t\}$ та оператор стрибка назад $\rho(t) := \sup\{s \in \mathbf{T} : s < t\}$. Про точку $t \in \mathbf{T}$, кажуть, що t щільна зліва, якщо $t > \inf \mathbf{T}$ і $\rho(t) = t$ і щільна справа, якщо $t < \sup \mathbf{T}$ і $\sigma(t) = t$. Точки, що є щільними справа і зліва називаються щільними. Крім того, якщо $\sigma(t) > t$, кажуть, що t розсіяна праворуч, а якщо $\rho(t) < t$, то t розсіяна ліворуч. Точки, які розсіяні вправо і зліво називаються ізольованими. І нарешті, третя функція - функція зернистості $\mu : \mathbf{T} \rightarrow [0; 1)$ визначається $\mu(t) := \sigma(t) - t$.

Розглядається задача про знаходження зв'язку між коливністю лінійного диференціального рівняння другого порядку на відрізьку $[0, a]$

$$\ddot{x} + p(t)\dot{x} + q(t)x = 0, \quad (1)$$

де $p, q \in C([0, a])$ та коливністю відповідного йому динамічного рівняння на часовій шкалі $\mathbf{T}$

$$x^{\Delta\Delta} + p(t)x^{\Delta} + q(t)x = 0, \quad (2)$$

де $x^{\Delta}(t)$ - дельта-похідна функції x в точці $t \in \mathbf{T}$, що визначається наступним чином $\forall \varepsilon > 0 \quad \exists \delta > 0 \quad \forall s \in (t - \delta; t + \delta) \cap \mathbf{T} : |[x(\sigma(t)) - x(s)] - x^{\Delta}(t)[\sigma(t) - s]| \leq \varepsilon|\sigma(t) - s|$.

Означення. Розв'язок $x(t)$ рівняння (2) називається *узагальненим нулем* в $t \in \mathbf{T}$, якщо $x(t) = 0$ або якщо t є ізольованою зліва і $x(\rho(t)) \cdot x(t) < 0$. Розв'язки диференціального рівняння (1) і динамічного рівняння (2) називаються *відповідними*, якщо мають однакові початкові дані. Якщо на деякому інтервалі розв'язок $x(t)$ матиме не менше двох узагальнених нулів, то будемо називати його *коливним*.

Отримано дві теореми.

Теорема 1. Якщо розв'язок $x(t)$ диференціального рівняння (1) коливний на $[0, a]$, то при достатньо малих μ відповідний розв'язок $x_{\mathbf{T}}(t)$ динамічного рівняння (2) також коливний.

Теорема 2. Якщо розв'язок $x_{\mathbf{T}}(t)$ динамічного рівняння (2) коливний на $[0, a]_{\mathbf{T}}$ при достатньо малих μ , то відповідний розв'язок $x(t)$ динамічного рівняння (1) також коливний.

Список літератури

- [1] Bohner M, Peterson A. Dynamical equations on time scales. An introduction with applications. Boston, MA, USA: Birkhauser, 2001.
-

Автори

Вікторія Борисівна Цань — аспірантка 1-го року навчання, механіко-математичний факультет, Київський національний університет імені Тараса Шевченка, Київ, Україна; E-mail: fizmatovka@gmail.com

Про комутуючі диференціювання кільця многочленів від двох змінних

С. Р. Ширінова

Вивчаються властивості комутуючих диференціювань кільця многочленів від двох змінних. Отримані результати можуть бути корисними при вивченні централізаторів елементів в алгебрі Лі $W_2(K)$. Такі централізатори мало вивчені, вони зустрічаються в деяких розділах алгебр і теорії диференціальних рівнянь.

Нехай K — алгебраїчно замкнене поле характеристики нуль і $K[x, y]$ — кільце многочленів від двох змінних. Нагадаємо, що лінійне відображення $D : K[x, y] \rightarrow K[x, y]$ називається диференціюванням кільця $K[x, y]$, якщо $D(fg) = D(f)g + fD(g)$ для будь-яких $f, g \in K[x, y]$. Кожне диференціювання D кільця $K[x, y]$ однозначно записується у вигляді $D = P(x, y) \frac{\partial}{\partial x} + Q(x, y) \frac{\partial}{\partial y}$, де P, Q — деякі многочлени і $\frac{\partial}{\partial x}, \frac{\partial}{\partial y}$ — частинні похідні. Всі диференціювання кільця $K[x, y]$ утворюють алгебру Лі $W_2(K)$ над полем K відносно операції $[D_1, D_2] = D_1 D_2 - D_2 D_1$ (взяття дужки Лі). Ця алгебра Лі вивчалася багатьма спеціалістами (див., наприклад, [1], [2]).

Для довільного многочлена $\varphi(x, y) \in K[x, y]$ визначене яacobіанне диференціювання D_φ , яке задане за правилом: $D_\varphi(h) = \det I(\varphi, h)$, для довільного $h(x, y) \in K[x, y]$, де $I(\varphi, h)$ — матриця Якобі для φ, h .

Теорема. Нехай $\varphi(x, y) \in K[x, y]$ — незвідний многочлен і $D_\varphi = P(x, y) \frac{\partial}{\partial x} + Q(x, y) \frac{\partial}{\partial y}$ — відповідне яacobіанне диференціювання. Далі, нехай $T = R(x, y) \frac{\partial}{\partial x} + S(x, y) \frac{\partial}{\partial y}$ — диференціювання таке, що $[T, D_\varphi] = 0$. Тоді визначник $\Delta = \begin{vmatrix} P & Q \\ R & S \end{vmatrix}$ може бути записаний у вигляді $\Delta = F(\varphi)$ для деякого многочлена $F(t) \in K[t]$ і при цьому $\operatorname{div} T = -F'(\varphi)$, де $\operatorname{div} T = \frac{\partial R}{\partial x} + \frac{\partial S}{\partial y}$ — дивергенція диференціювання T .

Список літератури

- [1] Nowicki A., Polynomial Derivations and their Rings of Constants, Uniwersytet Mikolaja Kopernika, Torun, 1994.
[2] J.Nagloo J., Ovchinnikov A. and Thompson P., Commuting planar polynomial vector fields for conservative Newton systems, Communications in Contemporary Mathematics 22, 2020.
-

Автор

Ширінова Сабіна Расим-кизи — студентка 4-го курсу, механіко-математичний факультет, Київський національний університет імені Тараса

Шевченка, Київ, Україна; E-mail: sabinashyrinova@gmail.com

Секція «Прикладна математика, комп'ютерні науки, інженерія програмного забезпечення, системний аналіз»

Практичні обчислення над зашифрованими даними

Н. В. Авраменко

У сучасному світі різні компанії пропонують безліч корисних послуг на основі отриманих даних. Та деяку інформацію, наприклад, біометричну, передавати іншій стороні ризиковано. Гомоморфне шифрування дозволяє проводити обчислення над зашифрованими даними, не розкриваючи їх зміст третій стороні. Перше рішення запропонував Крейг Джентрі у 2009 році [1], де він представив гомоморфну схему шифрування з бутстрапінгом. Згодом з'явилося багато нових досліджень, які зробили запропоновані ідеї більш застосовними, практичними. Серед них була схема BGV [2], яка запропонувала процедуру зміни модуля для зменшення шуму крипто-тексту.

Гомоморфна схема шифрування з публічним ключем $\mathcal{E}$ має три алгоритми $KeyGen_{\mathcal{E}}$, $Encrypt_{\mathcal{E}}$, $Decrypt_{\mathcal{E}}$ та додатковий алгоритм $Evaluate_{\mathcal{E}}$ [1]. Саме $Evaluate_{\mathcal{E}}$ дозволяє проводити обчислення над зашифрованими даними. У схемі BGV реалізовано гомоморфні операції додавання та множення, завдяки яким можна створювати більш складні обчислювальні функції.

За допомогою бібліотеки HELib [3], у якій імплементовано схему BGV, було реалізовано функції обчислення симетричних многочленів Ньютона й елементарного симетричного многочлена e_2 , та перевірено їх роботу на різних параметрах схеми шифрування. Код реалізації розташований за посиланням: <https://github.com/RinLaNir/some-polynomials>.

Список літератури

- [1] Craig Gentry. Fully homomorphic encryption using ideal lattices. In Michael Mitzenmacher, editor, STOC, pages 169–178. ACM, 2009.
- [2] Zvika Brakerski and Craig Gentry and Vinod Vaikuntanathan, Fully Homomorphic Encryption without Bootstrapping, Cryptology ePrint Archive, Report 2011/277, 2011, <https://ia.cr/2011/277>.
- [3] HELib, an open-source software library that implements homomorphic encryption (HE), <https://homenc.github.io/HELib/>.

Автори

Нікіта Васильович Авраменко — студент 4-го курсу, механіко-математичний факультет, Київський національний університет імені Тараса Шевченка, Київ, Україна; E-mail: nikita.avramenko@gmail.com

Скрінкаст як засіб візуалізації навчальних матеріалів з інформатики в умовах дистанційного навчання

І. М. Бабійчук, О. П. Косовець

Реалії сьогодення стали серйозним викликом для України та світу в цілому та особливо загострили проблему цифровізації освіти та пошуку нових технологій організації освітнього процесу у дистанційній формі. Особливо гостро постало питання

візуалізації навчальних матеріалів на уроках інформатики в умовах дистанційного навчання. Насамперед це пов'язано зі специфікою пояснення нового матеріалу на уроках, та візуалізації алгоритмів виконання тих чи інших практичних робіт. Вирішенню цієї проблеми, на наш погляд, можна частково зарадити шляхом інтеграції в освітній процес комплексу навчальних відео уроків, розроблених за технологією скрінкастингу, в спеціальному програмному середовищі, такому, як TechSmith Camtasia 2020.

Дослідження проблеми використання мультимедіа, аудіо- та відеотехнологій у освітньому процесі можна знайти у роботах Ю. Верисокіна, А. Кобисі, М.Кадемії, А. Каптерева, О. Шликова та ін. На основі аналізу праць означених науковців, «скрінкаст» визначаємо як відеозапис інформації, що виводиться вчителем на екран комп'ютера та часто супроводжується голосовими коментарями [1]. В рамках дослідження, нами розглянуто особливості створення та використання на уроках інформатики навчальних скрінкастів, спроектованих у програмі TechSmith Camtasia 2020. Переваги даного програмного забезпечення дозволили нам розробити та інтегрувати в дистанційний освітній процес Обласного наукового ліцею-інтернату комплекс авторських скрінкастів до уроків інформатики та комп'ютерної графіки.

Як показала практика, дана технологія є ефективною не лише в умовах дистанційного навчання, а й гармонійно інтегрується в освітній процес очного навчання і дозволяє учням ефективніше сприймати навчальний матеріал і виробляти навички роботи з ПК. На основі проведеного дослідження, та з власного досвіду, можемо зробити висновок, що технологія скрінкастингу є одним із найбільш рішень для покращення особливостей виконання практичних завдань з інформатики у дистанційному режимі.

Список літератури

- [1] Вембер В. П. Сучасні типи навчального відео та особливості їх використання в освітньому процесі [Електронний ресурс] / В. П. Вембер, Д. Л. Бучинська // ISSN Online: 2312-5829. Освітологічний дискурс. – 2016. – Режим доступу до ресурсу: <http://oaji.net/articles/2016/2923-1457766619.pdf>.
-

Автори

Бабійчук Ірина Михайлівна — студентка 4-го курсу, факультет математики, фізики і комп'ютерних наук, Вінницький державний педагогічний університет імені Михайла Коцюбинського, Вінниця, Україна; E-mail: nikkim2010i@gmail.com

Косовець Олена Павлівна — к.п.н., ст. викл. кафедри математики та інформатики Вінницького державного педагогічного університету імені Михайла Коцюбинського, Вінницький державний педагогічний університет імені Михайла Коцюбинського, Вінниця, Україна; E-mail: kosovets.op@vspu.edu.ua

Математичне моделювання активаційних функцій штучного нейрона з використанням системи комп'ютерної алгебри MathCAD

Д. О. Білоконь

Інтелектуальні системи стрімко поширюються. Основна частина проектується на базі штучних нейронних мереж. При створенні цих систем виникає питання - використовувати існуючі бібліотеки або створювати власні? Ці два методи мають позитивні та негативні характеристики - це відбувається через відсутність універсальності у системах штучного інтелекту. Цю проблему сформулював Джон Маккарті (Jhon McCarty)[1].

Отже, створюючи програмне забезпечення на основі штучних нейронних мереж завжди виникає необхідність для створення окремих функцій та модулів задля збільшення універсальності і пристосуванню власних розробок до бажаних потреб. В цілях уніфікації, формалізації та практичного застосування у роботі розглядаються найбільш поширені функції активації[2]: логістична функція (1), непарна сигмоїдальна функція (2) та непарна сигмоїдальна функція (алгебраїчна сигмоїда) (3).

$$\varphi(v) = \frac{1}{1 + \exp(-av)} \quad (1)$$

$$\varphi(v) = \frac{1 - \exp(-av)}{1 + \exp(-av)} = \tanh\left(\frac{av}{2}\right) \quad (2)$$

$$\varphi(v) = \frac{v}{\sqrt{1 + v^2}} \quad (3)$$

В даній роботі проведено огляд сигмоїдальних функцій, розглянуті особливості їх реалізації у системі MathCAD. Проведені обчислювальні експерименти з різними параметрами та побудовані графіки цих функцій, що ілюструють різні нахили та гладкість цих функцій.

Список літератури

- [1] McCarty, J. Generality in Artificial Intelligence: ACM Turing Award Lectures The First Twenty Years 1966-1985 – ACM Press Anthology Series, Addison Wessley Publishing Company - 1987.
 - [2] Haykin, S. Neural Networks: A Comprehensive Foundation. – Prentice Hall, 1999.
-

Автори

Дар'я Олександрівна Білоконь — студентка 1-го курсу, факультет кібернетики, Київський національний університет імені Тараса Шевченка, Київ, Україна;
E-mail: dasha.bilokon123@gmail.com

Аналіз розв'язків SIR моделі поширення інфекційних захворювань з врахуванням життєвого циклу населення

І.В. Вергунова, М.О. Вертелко, Ю.М. Шевчук

Поширеність інфекційних захворювань у суспільстві здатна значно впливати на рівень показника якості життя людей. Технологічний процес наразі дозволяє ефективно використовувати розроблені відповідні математичні моделі для вирішення нагальних проблем контролювання захворюваності, точніше ідентифікувати параметри моделей та прогнозувати динаміку. На основі теоретичного аналізу розв'язків даних моделей постає можливим більш детальне практичне оцінювання динаміки реальних процесів. Було обрано модель SIR із параметрами смертності та народжуваності з огляду на доступність даних, що потрібні для її використання, та оптимальний рівень складності. Вона дозволяє спостерігати динаміку кількості сирійнятливих до захворювання $S(t)$, кількості інфікованих $I(t)$, кількості осіб, що одужали, $R(t)$, динаміку смертності від ускладнень інфекційного захворювання $M(t)$, $t \in (0, T)$ та має вигляд:

$$\begin{cases} \dot{S}(t) = -\alpha(t)S(t)I(t) - \mu_1(t)S(t) + \gamma(t), \\ \dot{I}(t) = \alpha(t)S(t)I(t) - \beta(t)I(t) - \mu_2(t)I(t), \\ \dot{R}(t) = \beta(t)I(t) - \mu_3(t)R(t), \\ \dot{M}(t) = \mu_2(t)I(t), \end{cases} \quad t \in (0, T), \quad (1)$$

де $\alpha(t)$, $\beta(t)$ — параметр інтенсивності інфікування, одужання, $\mu_1(t)$, $\mu_2(t)$, $\mu_3(t)$, $\gamma(t)$ — параметри рівня смертності у 3 групах та народжуваності. Для даної моделі були знайдені умови, за яких розв'язки будуть додатними. Також знайдені точні розв'язки для окремого випадку моделі (1), коли виконується умова $S(t)+I(t)+R(t)=N$, $t \in (0, T)$, де N — константа.

Список літератури

- [1] Harko T., Lobo F.S.N., Mak M.K. Exact analytical solutions of the Susceptible-Infected-Recovered (SIR) epidemic model and of the SIR model with equal death and birth rates. *Applied Mathematics and Computation*. 2014. No236.
- [2] Kröger M., Schlickeiser R. Analytical solution of the SIR-model for the temporal evolution of epidemics. Part A: time-independent reproduction factor. *Journal of Physics A: Mathematical and Theoretical*. 2020. Vol. 53(50). 505601.

Автори

Ірина Вікторівна Вергунова — студентка 4-го курсу, факультет комп'ютерних наук та кібернетики, Київський національний університет імені Тараса Шевченка, Київ, Україна; E-mail: i_verg@outlook.com

Микита Олексійович Вертелко — студент 2-го курсу, факультет комп'ютерних наук та кібернетики, Київський національний університет імені Тараса Шевченка, Київ, Україна; E-mail: vernik03@gmail.com

Юлія Михайлівна Шевчук — асистент кафедри системного аналізу та теорії прийняття рішень, Київський національний університет імені Тараса Шевченка, Київ, Україна; E-mail: shvchuk.iuliia@knu.ua

Синтез оптимальної структури обробки даних оглядових радіолокаційних систем спостереження

А. О. Глущенко

Система контролю повітряного простору забезпечує безпеку повітряного руху. До основних етапів роботи цієї системи відносяться: аналіз повітряної обстановки в зоні відповідальності та прийняття управлінських рішень. Ці рішення приймаються на основі аналізу інформації про стан повітряної обстановки. Основним джерелом інформації про повітряну обстановку в системі контролю повітряного простору є первинний оглядовий радіолокатор. Обробка даних якого і є основою для прийняття рішень. На якість прийняття рішень, в основному, впливають: повнота даних, своєчасність надходження даних, правильність і точність даних, неперервність даних [1]. В загальному випадку спільна оптимальна обробка даних первинного оглядового радіолокатора може здійснюватися: при об'єднанні рішень на рівні виявлення повітряного об'єкта; при об'єднанні рішень на рівне виявлення трас повітряного об'єкта.

В обох варіантах обробки даних імовірність виявлення трас повітряного об'єкта (ПО) оптимізується за рахунок сумісної оптимізації виявлення сигналів, виявлення ПО та виявлення трас ПО [1, 2]. Тобто здійснюється оптимізація всіх етапів обробки

даних. Для цього повинна бути створена інформаційна база зберігання радіолокаційних даних на необхідну кількість кругових оглядів радіолокатора, в кожному елементі якої повинні зберігатися сигнальні дані з показниками якості їх отримання [3, 4, 5].

При цьому слід зазначити, що для реалізації міжетапної оптимізації обробки даних у відповідності до запропонованих математичних алгоритмів, повинна бути створена інформаційна база сигнальних даних з загальним обсягом пам'яті, що залежить від: кількості елементів дозволу за дальністю, кількості збережених у пам'яті оглядів, розміру пачки прийнятих сигнальних даних та розрядності вагового коефіцієнта.

Метою роботи є синтез оптимальної структури обробки даних повітряного об'єкта та аналіз якості обробки даних запропонованою структурою, яка дозволяє здійснити міжетапну оптимізацію обробки даних.

Список літератури

- [1] Обод І.І., Свид І.В., Мальцев О.С. Обробка даних радіолокаційних систем спостереження повітряного простору : навчальний посібник. – Харків: Друкарня Мадрид, 2021. – 255 с.
- [2] Свид І.В., Обод І.І. Завадостійкість радіолокаційних систем ідентифікації за ознакою «свій-чужий»: монографія. – Харків: Друкарня Мадрид, 2021. 254 с.
- [3] Черних О.П., Обод І.І., Свид І.В. Інформаційне забезпечення на основі мереж спостереження повітряного простору. // Eastern-European Journal of Enterprise Technologies, том 2, вип. 9(50), 2011. – С. 23-25.
- [4] Свид І.В., Обод А.І. Синтез структури інформаційного забезпечення споживачів інформаційними системами спостереження повітряного простору // Збірник наук. праць Харківського університету Повітряних Сил. Вип. 2., 2015. - С. 67-70.
- [5] Обод І.І., Свид І.В., Шевцова В.В. Синтез оптимального виявлювача абонентів запиту несинхронної мережі запитальних систем передачі інформації. // Вісник Національного технічного університету «ХПІ». Збірник наукових праць. – Х.: НТУ «ХПІ». – 2013. – № 27 (1000). – С. 124-129.

Автори

Глушченко Артем Олександрович — аспірант, Харківський національний університет радіоелектроніки, Харків, Україна; E-mail: artem.hlushchenko@nure.ua

Розподілена обробка інформації у мережевих системах спостереження повітряного простору

О. О. Даценко

Згідно з концепцією організації повітряного руху Міжнародної організації цивільної авіації пропонується широке використання інформаційних технологій (ІТ) при отриманні, обробці, збереженні та передачі інформації. Що забезпечить розширення можливостей використання повітряного простору країни для польотів повітряних об'єктів (ПО) [1, 2]. Покращення якості інформаційного забезпечення (ІЗ) можливо досягти зміною алгоритмів та структури обробки сигналів за рахунок використання ІТ. ІЗ повинно включати в себе: просторові координати повітряного об'єкту (ПО); додаткову польотну інформацію ПО; інформацію ідентифікації ПО за ознакою «свій-чужий» [3, 4]. Структура ІЗ користувачів на базі первинної обробки інформації розглядаємої мережі включає канали первинної та запитальної систем. Формуляр ПО у кожному каналі системи повинен містити інформацію про: виявлення та вимірювання параметрів виявлених сигналів; виявлення та вимір координат виявлених ПО [5, 6]. Обчислення додаткових даних для поєднання

інформації у формулярі ПО суттєвим чином зменшує інформаційні можливості систем спостереження. Це в свою чергу обмежує показники якості ІЗ споживачів при видачі споживачам повного формуляру. Проведений аналіз дозволяє зробити наступний висновок: використання розподіленої обробки інформації каналів систем спостереження, з урахуванням можливості використання рівноцінності факту виявлення ПО первинною та запитальною системами спостереження, більш доцільно у порівнянні з існуючою структурою ІЗ, що забезпечується більш енергетичним (вторинним) каналом обробки.

Список літератури

- [1] Обод І.І., Свид І.В., Мальцев О.С. Обробка даних радіолокаційних систем спостереження повітряного простору : навчальний посібник. – Харків: Друкарня Мадрид, 2021. – 255 с.
- [2] Свид І.В., Обод І.І. Завадостійкість радіолокаційних систем ідентифікації за ознакою «свій-чужий»: монографія. – Харків: Друкарня Мадрид, 2021. 254 с.
- [3] І.І. Обод, І.В. Свид. Порівняльний аналіз якості виявлення повітряних об'єктів запитальними системами спостереження. // Системи обробки інформації. Вип. 9 (90) – Харків, видавництво ХУПС, 2010 – С. 74-76.
- [4] I. Obod, I. Svyd, O. Maltsev and B. Bakumenko, Comparative Analysis of Noise Immunity Systems Identification Friend or Foe. // 2020 IEEE 40th International Conference on Electronics and Nanotechnology (ELNANO), Kyiv, Ukraine, 2020, P. 751-756.
- [5] I. Obod, I. Svyd, O. Maltsev, B. Bakumenko. Spatial Methods for Increasing the Bandwidth of a Mobile Information Network. // 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET-2020), Lviv-Slavske, Ukraine, 2020. – P. 50-54.
- [6] I. Svyd, I. Obod, O. Maltsev and A. Hlushchenko. Secondary Surveillance Radar Response Channel Information Security Improvement Method. // 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), 2020, P. 341-345.

Автори

Даценко Олександр Олександрович — аспірант, Харківський національний університет радіоелектроніки, Харків, Україна; E-mail: oleksandr.datsenko@nure.ua

Критерії криптографічної стійкості схем генерування раундових ключів

М.О. Дубовик, С.В. Яковлєв

Блокові шифри досліджуються та використовуються вже більш ніж півстоліття, однак досі не існує усталеного переліку критеріїв, виконання яких забезпечує стійкість схем генерування раундових ключів таких шифрів. У даній роботі, ґрунтуючись на попередніх дослідженнях (наприклад, [1, 2]), запропоновано перелік критеріїв стійкості схеми генерування раундових ключів:

а) **незалежні від структури шифру**: ефективне обчислення; сильні властивості розсіювання та перемішування; нелінійний зв'язок раундових ключів з основним ключем та між собою; відсутність витоку бітів ключа; відсутність передбачуваних змін на рівні схеми генерування; максимальні лавинні ефекти в раундових ключах;

б) **залежні від структури шифру**: стійкість до колізій; стійкість до атак на зв'язаних ключах; відсутність слабких ключів; відсутність нерухомих точок раун-

дових перетворень; стійкість до диференціальних атак; відсутність передбачуваних змін на рівні шифру в цілому.

За цими критеріями проаналізовано деякі популярні блокові шифри (DES, AES тощо) та з'ясовано, що навіть за такої слабкої формалізації багато шифрів не задовольняють наведеним критеріям. Більш того, часто відповідність критеріям, особливо наявність розмішування та перемішування, а також лавинні ефекти, підтверджується лише за допомогою статистичних експериментів.

Для посилення надійності пропонується використовувати у схемах генерування раундових ключів перетворення із доказовими криптографічними властивостями (такі як схема Люби-Ракова та її аналоги), побудовані на основі окремих складових раундових перетворень шифру.

Список літератури

- [1] Kelsey, J., Schneier, B., Wagner, D. *Key-Schedule Cryptanalysis of IDEA, G-DES, GOST, SAFER, and Triple-DES*. // *Advances in Cryptology – CRYPTO'96*. – https://doi.org/10.1007/3-540-68697-5_19
 - [2] Afzal Sh. et al. *Cryptographic Strength Evaluation of Key Schedule Algorithms* // *Security and Communication Networks*, vol. 2020. – <https://doi.org/10.1155/2020/3189601>
-

Автори

Маргарита Олексіївна Дубовик — студентка 4-го курсу, ННФТІ, КПІ ім.Ігоря Сікорського, Київ, Україна; E-mail: margodubovik531@gmail.com

Сергій Володимирович Яковлев — к.т.н, доцент кафедри математичних методів захисту інформації ННФТІ КПІ ім. Ігоря Сікорського, Київ, Україна; E-mail: yasv@rl.kiev.ua

Обчислення частинних похідних за часовими рядами хаотичних систем

С. М. Іванов

Непередбачувана поведінка нелінійних хаотичних систем, таких як рідинні системи, конвекційна система Рейле-Бенарда, система Лоренца, Ресслера, Маккея-Гласа та багатьох інших, привертає увагу у багатьох наукових сферах. Однак не завжди рівняння системи є відомими, а наявні лише експериментально визначені її часові ряди. При дослідженні властивостей динаміки хаотичних систем виникає проблема обчислення частинних похідних (чисельної матриці Якобі) за її часовими рядами, особливо для подальшого знаходження показників (експонент) Ляпунова, горизонту прогнозу та ін. [1] - [5] . У описаних методах оцінювання чисельної матриці Якобі та обчислення показників Ляпунова в [1] - [5] розрахунки відбуваються через пошук достатньої кількості близьких точок на аттракторі. Однак численні експерименти з аттракторами Лоренца, Ресслера та ін. показали, що для збіжності до істинних частинних похідних лише тільки ця кількість точок на аттракторі не є достатньою, необхідне подальше знаходження достатніх умов, виконання яких гарантує отримання необхідної збіжності.

Список літератури

- [1] Sano M., Sawada Y. Measurement of Lyapunov spectrum from a chaotic time series. *Phys. Rev. Lett.* 1985. Vol. 55. Issue 10. pp. 1082-1085. doi: <https://doi.org/10.1103/PhysRevLett.55.1082>

- [2] Wolf A., Swift J. B., Swinney H. L., Vastano J. A. Determining lyapunov exponents from a time series. *Physica D: Nonlinear phenomena*. 1985. Vol. 16. Issue 3. pp. 285 – 317. doi: [https://doi.org/10.1016/0167-2789\(85\)90011-9](https://doi.org/10.1016/0167-2789(85)90011-9)
- [3] Qinglan Li, Pengcheng Xu Estimation of Lyapunov spectrum and model selection for a chaotic time series. *Applied Mathematical Modelling*. 2012. 36. pp. 6090 – 6099.
- [4] Eckmann J.-P., Kamphorst S.O., Ruelle D., Ciliberto S. Liapunov exponents from time series. *Phys. Rev. A*. 1986. Vol. 34. Issue 6. pp. 4971 – 4979. doi: <https://doi.org/10.1103/PhysRevA.34.4971>
- [5] Brown R., Bryant P., Abarbanel Henry D.I. Computing the Lyapunov spectrum of a dynamical system from an observed time series. *Phys. Rev. A*. 1991. Vol. 43. Issue 6. pp. 2787 – 2806. doi: <https://doi.org/10.1103/PhysRevA.43.2787>

Автори

Сергій Миколайович Іванов — канд. фіз.-мат. наук, асистент кафедри системного аналізу та теорії прийняття рішень, факультет комп'ютерних наук та кібернетики, Київський національний університет імені Тараса Шевченка, Київ, Україна; E-mail: smivanov87@knu.ua

Числа Шпрага-Гранді

Д. О. Карпенко, О. Д. Приходько

Теорія ігор – це важливий розділ математики, який є корисним при вирішенні багатьох прикладних питань у різних сферах діяльності. Особливу увагу привертають ігри Нім, оскільки вони є зручними у використанні, а також є велика кількість задач, які зводяться до даної гри.

Зібрано та упорядковано відомості про булеві функції одного та двох аргументів, сформульовано та доведено властивості функції XOR. Дано означення та описані умови Нім-гри і похідних від неї ігор. Наведено формулювання та доведення теорем Бутона і Шпрага-Гранді, описано послідовність дій в алгоритмі Шпрага-Гранді, який є наслідком зібраних теорем та властивостей. Даний алгоритм дає можливість розв'язувати будь-які рівноправні комбінаторні ігри двох гравців. Також за його допомогою можна розв'язувати не лише задачі на купки, а й набагато складніші рівноправні ігри, в тому числі ігри на орієнтовних нециклічних графах. Варто зазначити, що алгоритм дає не лише відповідь, а й саму виграшну стратегію гри.

Практичну корисність та актуальність зібраних теорем і властивостей показано у розв'язаних задачах та написаній програмі. Представлені задачі поділяються на два типи: у першому потрібно з'ясувати, хто переможе при правильній стратегії, а в другому – визначити яку незалежну гру потрібно додати або змінити для того, щоб переміг вибраний гравець. Доведені теореми дали можливість створити швидкий і простий алгоритм для програми, в якій можна зіграти у гру Нім з комп'ютером на двох, трьох та чотирьох купках. Варто зауважити, що без використання результатів дослідження реалізувати алгоритм можна лише повним перебором, який працює за дуже великий машинний час.

Автори

Дарина Олександрівна Карпенко — учениця 10 класу, Хмельницька гімназія № 1 імені Володимира Красицького, Хмельницький, Україна; E-mail: djen2006i@gmail.com

Ольга Дмитрівна Приходько — вчителька математики, Український фізико-математичний лицей Київського національного університету імені Тараса Шевченка, Київ, Україна; E-mail: prykhodkood@gmail.com

Система дистанційного позиціонування з можливістю трьох координатної стабілізації

О. В. Крива

Виклики часу по захисту нашої країни вимагають нестандартних підходів у веденні бойових дій, що було доказано на полях битви по захисту столиці нашої держави. Невеликі мобільні групи оснащені сучасними ПТРК показали свою ефективність, однак існує реальна загроза для оператора в умовах відкритої місцевості від снайперських груп ворога, які прикривають бронетехніку. Таку проблему можна вирішити за допомогою нескладного станка з дистанційним візуальним каналом. Подібні станки з успіхом використовуються для ручних кулеметів. Невеликі удосконалення по зменшенню маси та можливості установки на серійні автомобілі значно розширяють ефективність ПТРК при повній безпеці оператора. Також подібна технологія повністю підходить при застосуванні ПЗРК. В роботі розглядаються дві версії системи бюджетна з оптичним каналом на основі ендоскопа та системи позиціонування з використанням шарової опори автомобіля і тяжок поперечної стабілізації. Медичний ендоскоп (використовуються при фіброгастроскопії чи колоноскопії) має гарний оптичний канал та ручний маніпулятор положення в трьохсистемній площині. Маніпулятор забору тканини для біопсії використовується як для налаштування, так і для активації функції запуску. Довжина ендоскопу може бути більше двох метрів, що достатньо для безпеки оператора, зручний окуляр, надійна механіка відсутність елементів живлення запорука надійності. Другий варіант системи позиціонування розроблено на основі сервоприводів з енкадерами та зворотнім зв'язком по оптичному каналу, або з використанням заготовлених попередньо шаблонів можливих загроз. Система управління також може опрацьовувати сигнали сенсорів положення акселерометрів та гіроскопа. Для скорочення термінів розробки було взято за основу бібліотеку підпрограм, які використовуються для кранів відеокамер на знімальному майданчику. Оптичний канал при такому варіанті може бути як на основі відеокамери, так і на основі ендоскопу.

Authors

Ольга Вікторівна Крива — студент 2-го курсу, механіко-математичний факультет, Київський національний університет імені Тараса Шевченка, Київ, Україна; E-mail: olhakryva@gmail.com

Навчання з підкріпленням для оптимізації параметрів електромеханічних систем

Д. С. Лукашов, Н. П. Лукашова

Однією з найважливіших проблем сучасної електромеханіки є підбір оптимальних параметрів для максимізації корисної дії системи. Через складність системи знайти параметри аналітично не є можливим тому на практиці використовують різні обчислювальні алгоритми. Однак вони мають недоліки, наприклад, можуть бути неточними та швидкими, або ж точними але повільними, цю проблему було зазначено в [1]. Для подолання проблем існуючих алгоритмів пропонується використати навчання з підкріпленням глибоких нейронних мереж.

Запропонований на рисунку (1) спосіб працює наступним чином: випадковим чином генеруються початкові параметри, після чого НМ шукач пропонує нові параметри, НМ Оцінювач дає свою оцінку ефективності, симуляція дає свою, на основі цих оцінок формується помилка оптимізатору, після чого нейронні мережі оновлюються за допомогою зворотного розповсюдження.

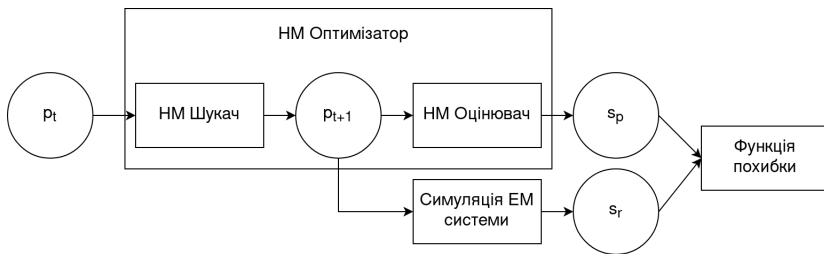


Рис. 1. Схема роботи способу пошуку оптимальних параметрів ЕМ систем

Список літератури

- [1] Лукашова Н. П. Підвищення ефективності роботи ходової частини рейкового міського транспорту з використанням електромеханічних амортизаторів : дис. ... канд. техн. наук.

Автори

Лукашов Дмитро Сергійович — студент 1-го курсу магістратури, факультет інформаційних технологій та менеджменту, Харківський національний університет радіоелектроніки, Київ, Україна; E-mail: dmytro.lukashov@nure.ua

Лукашова Наталя Павлівна — кандидат технічних наук, старший викладач кафедри електричного транспорту Харківського національного університету міського господарства імені О. М. Бекетова, Харків, Україна; E-mail: lukaschova.natalya@gmail.com

Фаззі екстрактори

Г. В. Наumenко

Як відомо, такі криптографічні примітиви, як, наприклад, ключі шифрування та дешифрування, для безпеки повинні бути з рівномірного розподілу. Але не все, що ми використовуємо для, наприклад, авторизацій, має саме такий розподіл. Розглянемо для прикладу біометричні дані: скан лиця, скан сітківки ока, скан відбитку пальця, голос, біоакустичні сигнали нашого тіла тощо - усе це явно не з рівномірного розподілу, але дуже активно використовується для безпеки і ідентифікації користувача. Також, не дуже безпечно такі дані віддавати третім особам для подальшої обробки. Один із варіантів, який можна застосувати для вилучення стійких криптографічних примітивів - Фаззі екстрактори.

Нехай M - деякий метричний простір з визначеною на ньому метрикою d і через n позначимо довжину елементів M .

Означення 1. (m, l, t, ϵ) -Фаззі екстрактором називають пару недетермінованих алгоритмів Gen, Rep з наступними властивостями:

- Алгоритм генерування Gen , що приймає на вхід $w \in M$ і повертає випадковий рядок $r \in \{0, 1\}^l$ і допоміжний рядок $p \in \{0, 1\}^*$. Алгоритм репродукції Rep , що приймає на вхід $w' \in M$ і допоміжний рядок $p \in \{0, 1\}^*$.
- Коректність:** якщо $d(w, w') \leq t$ та $(r, p) \leftarrow Gen(w)$, то тоді $Rep(w', p) = r$.

- в) *Безпека*: Для довільного розподілу W на M з ентропією m , рядок r близький до рівномірно розподіленого навіть якщо має залежність від значення p .

Допоміжний рядок p може бути публічним: це не робить видобутий рядок r ненадійним.

Вимога до такої системи - бути стійкою до наступної атаки: зломисник просить випробувача відновити приватний рядок, використовуючи алгоритм *Rep* на вибраних спотвореннях секрету для довільних публічних рядків (в тому числі з попередніх запитів до *Gen*). Для зломисника повинно бути алгоритмічно складно відновити або відрізнити який-небудь приватний рядок, що не був в запиті.

В даній роботі проведено порівняльний аналіз безпеки та ефективності фаззи екстракторів, запропонованих у роботах [1, 2, 3, 4]

Список літератури

- [1] Yevgeniy Dodis, Leonid Reyzin, and Adam Smith: Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data, NY University, Boston University, MIT, 2004
 - [2] Abhishek Jana, Md Kamruzzaman Sarker, Monireh Ebrahimi, Pascal Hitzler, George T Amariuca: Neural Fuzzy Extractors: A Secure Way to Use Artificial Neural Networks for Biometric User Authentication, Department of Computer Science, Kansas State University, 2020
 - [3] Bhavana Kanukurthi and Leonid Reyzin: An Improved Robust Fuzzy Extractor, Boston University Computer Science, 2018
 - [4] Xavier Boyen: Reusable Cryptographic Fuzzy Extractors, Voltage Security, Palo Alto, 2004
-

Автори

Георгій Вадимович Науменко — студент 4-го курсу, механіко-математичний факультет, Київський національний університет імені Тараса Шевченка, Київ, Україна; E-mail: goga.naumenko.08@gmail.com

Using TDD compared to manual testing

V. Nekriach, V. Kovalenko

Authors of software engineering books considered classic [1, 2] are passionate advocates for the adoption of 'clean' code and XP practices. This paper proposes a hypothesis that one of the pillars of XP - Test Driven Development [3] is a better alternative compared to manual testing.

The experiment has been set up in the following way: we have been writing code for 3 months only using manual testing before handing in the results to the manual QA team, and for 3 months we have been using TDD (mostly writing small unit tests and occasionally writing integration tests) and then passing a new version to the manual QA. Most of the features we worked on were small incremental changes of the project or small bug fixes.

The results of using this technique are quite fascinating as all the 11 features that had been made with the use of TDD made it to the production environment without any bugs noticed by manual QA. Meanwhile, the results for the features for which we used manual testing aren't as good - only 9 did.

	Passed manual QA	Sent back
Follows TDD	11	0
Manual dev testing	9	6

Based on the results of the experiment, authors of this paper propose a hypothesis that TDD is a better and an easier alternative for developers compared to manual testing of code, as it reduces the possibility of human error and simplifies implementation of the code required to pass the test.

References

- [1] Fowler, Martin and Kent Beck. Refactoring, 2nd edition. Addison-Wesley, 2019.
 - [2] Martin, Robert. Clean Code. Pearson, 2008.
 - [3] Fowler M., short article on Test Driven Development and its benefits. <https://martinfowler.com/bliki/TestDrivenDevelopment.html>
-

Authors

Vladyslav Nekriach — 3rd year student, BSc Computer Science, Faculty of Computer Science and Cybernetics, Taras Shevchenko National University of Kyiv; E-mail: nekriach_vv@knu.ua

Victoria Kovalenko — 3rd year student, BSc Computer Science, Faculty of Computer Science and Cybernetics, Taras Shevchenko National University of Kyiv; E-mail: victoria.kovalenko@knu.ua

Протокол обміну повідомленнями на основі лінійних функцій і операторів

С. Л. Кривий, Ю. О. Нортман

Пропонований протокол обміну повідомленнями ґрунтується на властивостях операторів у лінійному просторі і складності алгоритмів розв'язання систем лінійних неоднорідних діофантових рівнянь над множиною натуральних чисел [1, 2]. Використовуючи деяку послідовність таких відображень зі зсувами на деякі задані вектори, дістаємо можливість за результатом значенням оператора знайти його початкове значення. В протоколі всього чотири кроки, які описують взаємодію між абонентами Алісою і Бобом.

Крок 0 Аліса і Боб просять Джона згенерувати для них спільний ключ c - ціле додатне число або вектор таких чисел заданої розмірності.

Крок 1 а) Аліса будує систему лінійних виразів Ax , де A матриця розмірності $p \times q$ ($p < q$), невідроджені матриці розмірності $p \times p$ $B_0, B_1, \dots, B_s$ і вектори $b_0, b_1, \dots, b_s, b_i$, де b, b_i - приватні вектори зсуву з цілими координатами, $i = 1, 2, \dots, s$;

б) Будує систему виразів $D(x) = B_s(B_{s-1}(\dots B_1(B_0(A(x)) + b_0) + b_1)\dots) + b_{s-1}) + b_s + b$;

в) Висилає Бобу вирази Ax , і $D(x)$ відкритим каналом.

Крок 2 а) Боб обирає довільний вектор x розмірності $1 \times q$ і обчислює [1] значення $Ax = v$, яке є приватним;

б) Обчислює значення $D(x) = d$ і висилає Алісі значення $d' = d + c$ відкритим каналом.

Крок 3 Аліса за значенням d' обчислює значення $B_0^{-1}(B_1^{-1}(\dots(B_{s-1}^{-1}(B_s^{-1}(d' - c) - b) - b_s) - b_{s-1}))\dots - b_1) - b_0 = A(x)$ за допомогою обернених матриць до матриць B_i [3].

Надійність наведеного протоколу цілком ґрунтується на таємності ключа c та складності розв'язання системи лінійних діофантових рівнянь в множині натуральних чисел, тобто на криптографічній функції $f_c : Dx + c = d'$.

Для передачі наперед заданих повідомлень використовуються системи лінійних рівнянь над скінченним полем, яке ізоморфне полю лишків за модулем простого числа і над яким такі системи завжди сумісні [1].

Для реалізації протоколу була обрана мова програмування Java 11, для передачі повідомлень між абонентами використовується брокер повідомлень RabbitMQ [4], який працює по протоколу AMQP (Advanced Message Queuing Protocol) [5].

Список літератури

- [1] Кривий С.Л. Лінійні діофантові обмеження та їх застосування. К.: Інтерсервіс. - 2021.-260 с.
 - [2] Hermann M., Juban L., Kolaitis P. G. On the Complexity of Counting the Hilbert Basis of Linear Diophantine System. Springer Verlag. - LNCS. - 1999. - № 1705. - P. 13–32.
 - [3] Кормен Т., Лейзерсон Ч., Ривест Р., Штайн К. Алгоритмы построения и анализа (2-е изд.). Издательский дом «Вильямс». - 2005.-1290 с.
 - [4] Videla A. RabbitMQ in Action / A. Videla, J. Williams. - Shelter Island: Manning Publications Co., 2012. - 288 с.
 - [5] AMQP Advanced Message Queuing Protocol Specification // 0-9-1. - 2008. -<https://www.rabbitmq.com/resources/specs/amqp0-9-1.pdf>.
-

Автори

Юлія Олександрівна Нортман — студентка 1-го курсу магістратури, факультет комп'ютерних наук та кібернетики, Київський національний університет імені Тараса Шевченка, Київ, Україна; E-mail: ynortman@gmail.com

Сергій Лук'янович Кривий — д.ф.-м.н., професор, факультет комп'ютерних наук та кібернетики, Київський національний університет імені Тараса Шевченка, Київ, Україна; E-mail: sl.krivoi@gmail.com

Щодо існування ортоморфізмів над групами, які застосовуються у криптографічних задачах

О. Ю. Паршин, С. В. Яковлев

Для побудови деяких криптографічно стійких примітивів, наприклад, схем шифрування Лая-Мессі та квазі-Фейстеля, схеми гешування Девіса-Мейєра тощо, необхідно використовувати так звані ортоморфізми для запобігання можливим уразливостям.

Нехай $\langle G, + \rangle$ — група порядку n . Відображення $\phi: G \rightarrow G$ називається *орторморфізмом*, якщо $\forall x, y \in G: x - \phi(x) = y - \phi(y) \Rightarrow x = y$. Зокрема, з означення випливає, що відображення $\phi(x)$ та $\phi'(x) = \phi(x) - x$ повинні бути бієктивними.

У частковому випадку, коли G є групою двійкових векторів $\{0, 1\}^m$ відносно побітового додавання, в роботі [1] доведено існування ортоморфізмів та наведено алгоритм їх побудови. Такі ортоморфізми широко використовуються для побудови шифрів на основі схеми Лая-Мессі. Однак в останні роки, у зв'язку із широким розповсюдженням новітніх протоколів доведення з нульовим розголошенням, цікавість становлять такі групи, як Z_p^* , $Z_{p^\alpha}^*$, Z_{pq}^* , Z_n^* , де p та q — прості, n — довільне натуральне.

У даній роботі показано, що ортоморфізми не можна побудувати над адитивними групами Z_n^+ у випадку, коли n є парним, а також над мультиплікативними групами Z_2^* , Z_4^* , $Z_{p^\alpha}^*$ та $Z_{2p^\alpha}^*$. Над адитивними групами Z_n^+ , де n непарне, а також над мультиплікативними групами $Z_{2^n}^*$ при $n \geq 3$ та Z_{pq}^* побудова ортоморфізмів виявляється можливою.

У подальшому планується провести аналіз існування ортоморфізмів над мультиплікативною групою Z_n^* для довільного n , а також створити обчислювально ефективні алгоритми побудови ортоморфізмів над групами, де це можливо.

Список літератури

- [1] L. Mittenhall. *Block Substitutions Using Orthomorphic Mappings*. // Advances in Applied Mathematics, vol. 16, issue 1. – Academic Press, Inc. – 1995. – pp. 59-71. – <https://doi.org/10.1006/aama.1995.1003>

Автори

Олександр Юрійович Паршин — студент 4-го курсу ННФТІ КПІ ім. Ігоря Сікорського, Київ, Україна; E-mail: parshin_o@ukr.net

Сергій Володимирович Яковлев — к.т.н, доцент кафедри ММЗІ ННФТІ КПІ ім. Ігоря Сікорського, Київ, Україна; E-mail: yasv@rl.kiev.ua

The optimal control problem with application to business strategy

O. Kapustian, I. Reznichenko

In this paper, we consider the optimal control problem that describes a business strategy for a plant that produces a unique good [1]:

$$\begin{cases} \int_0^T (1 - u(t))x(t) \cdot p dt \rightarrow \max, \\ \dot{x} = ux, \\ x(0) = a, \quad a > 0, \quad p > 0, \\ U = \{u(t) | 0 \leq u(t) \leq 1, \quad t \in [0, T]\} \subset \mathbb{R}, \end{cases} \quad (1)$$

where $x(t)$ is total amount of produced goods (output), a is an initial productive capacity, $u(t)$ is the fraction of the output $x(t)$ that we reinvest, p is the selling price of goods, U is a set of admissible controls. Functions $u(t)$ are piecewise continuous. At every moment, such production can either be reinvested to expand the productive capacity or sold. The initial productive capacity grows as the reinvestment rate. The main aim of this paper is to show what fraction $u(t)$ of the output $x(t)$ at time t should be reinvested to maximize total sales over the fixed period $[0; T]$ and the fixed selling price (constant). To gain the aim we solve this optimal control problem with two main approaches — the Variational approach (Pontryagin Maximum Principle) and the Dynamic Programming approach [2]. Both approaches show that in a situation where the business strategy is of medium or long time, the best choice is to invest the entire production to increase it up to time $T - 1$ and then sell everything to make profit.

Список літератури

- [1] A. Calogero. Notes on optimal control theory with economic models and exercises. – Dipartimento di Matematica e Applicazioni, Università di Milano-Bicocca. – May 14, 2018. – 152 p. (Preprint).
- [2] W.H. Fleming and P.W. Rishel. Deterministic and stochastic optimal control. Springer-Verlag, 1975.

Authors

Ілона Резніченко — студентка 4-го курсу, факультет комп'ютерних наук та кібернетики, Київський національний університет імені Тараса Шевченка, Київ, Україна; E-mail: barsareznich@gmail.com

Олена Анатоліївна Капустян — доцент кафедри системного аналізу та теорії прийняття рішень, факультет комп'ютерних наук та кібернетики, Київський національний університет імені Тараса Шевченка, Київ, Україна; E-mail: olenakapustian@knu.ua

Аналіз якісних показників обробки даних оглядових радіолокаційних систем спостереження

С. В. Старокожев

Система спостереження повітряного простору (ССПП) виконує функції контролю та безпеки повітряного простору країни. Основним джерелом даних про повітряний простір є оглядові радіолокаційні системи (ОРЛС). Обробка даних ОРЛС є основою для прийняття рішень у ССПП. Якість прийняття рішення визначається як якістю, так і складом інформації (даних), на основі якої приймаються рішення [1].

Обробка даних ОРЛС – це приведення інформації, отриманої від ОРЛС, до виду можливого для використання. Система обробки даних повітряного об'єкта (ПО) безпосередньо пов'язана з джерелами сигналів і забезпечує вирішення наступних інформаційних завдань [1, 2]: виявлення та вимірювання параметрів прийнятих сигналів і відсіювання завад; виявлення та вимірювання координат ПО; «зав'язки» виявлених сигналів у траєкторії та визначення параметрів цих траєкторій; обчислення згладжених та упереджених на деякий відрізок часу координат ПО.

Рішення задач обробки даних ОРЛС призводить до поетапної обробки потоків даних котрі можливо розділити на наступні етапи: обробка сигналів ОРЛС, первинної обробки даних (ПОД) та вторинної обробки даних (ВОД) [3, 4].

Оптимальність рішення задачі виявлення сигналів приймається, як правило, за критерієм Неймана-Пірсона, котрий зводиться до максимізації імовірності правильного виявлення сигналів при обмеженні на імовірність хибного виявлення. Ці дві імовірності і є показниками якості виявлення сигналів. Операції оцінки параметрів сигналів у загальному випадку оптимізується за критерієм мінімуму середнього ризику [5].

Метою роботи є аналіз якісних показників обробки даних оглядових радіолокаційних систем спостереження. Показано, що як показник якості інформаційного забезпечення ССПП можна застосовувати імовірність правильного виявлення траєкторії ПО.

Список літератури

- [1] І.І. Обод, І.В. Свид, О.С. Мальцев, Обробка даних радіолокаційних систем спостереження повітряного простору: навчальний посібник. – Харків: Друкарня Мадрид, 2021. – 255 с.
- [2] Свид І.В., Обод І.І. Завадостійкість радіолокаційних систем ідентифікації за ознакою «свій-чужий»: монографія. – Харків: Друкарня Мадрид, 2021. 254 с.
- [3] І.І. Обод, І.В. Свид, Порівняльний аналіз якості виявлення повітряних об'єктів запитальними системами спостереження. // Системи обробки інформації. Вип. 9 (90) – Харків, видавництво ХУПС, 2010 – С. 74-76.
- [4] I. Obod, I. Syd, O. Maltsev, B. Bakumenko. Spatial Methods for Increasing the Bandwidth of a Mobile Information Network. // 15th International Conference on

- [5] I. Svyd, I. Obod, O. Maltsev, G. Zavolodko, D. Pavlova, H. Maistrenko. Fusion of Airspace Surveillance Systems Data. // 3rd IEEE International Conference on Advanced Information and Communication Technologies (AICT), Lviv, Ukraine, 2019. – P. 430-433.

Автори

Старокожев Святослав Валерійович — аспірант, Харківський національний університет радіоелектроніки, Харків, Україна; E-mail: sviatoslav.starokozhev@nure.ua

Аналіз структури обробки даних первинних радіолокаторів

М. Г. Ткач

Основним джерелом даних про повітряну обстановку в системі контролю використання повітряного простору є первинні радіолокатори. Це визначає вимогу оптимізації обробки даних первинних радіолокаторів (ПРЛ), яка визначає оптимізацію виявлення траси повітряного об'єкта [1, 2]. Зараз обробка інформації ПРЛ неможлива без широкого використання інформаційних технологій. Саме інформаційні технології дозволяють реалізувати автоматичний збір, обробку, зберігання, передачу та видачу даних користувачам, підвищуючи при цьому практично всі показники якості даних первинних радіолокаційних систем [3, 4]. Система обробки даних ПРЛ безпосередньо пов'язана з джерелами сигналів та забезпечує вирішення наступних інформаційних завдань: виявлення та вимірювання параметрів корисних прийнятих сигналів та відсіювання завад; виявлення та вимірювання координат повітряних об'єктів; зіставлення виявлених сигналів у траєкторії та визначення параметрів цих траєкторій; обчислення згладжень та випереджень на деякий відрізок часу координат повітряних об'єктів. Складність структури системи обробки даних ПРЛ не дозволяє проводити формалізацію та аналіз її роботи загалом, що вимагає розбиття системи обробки даних ПРЛ на кілька частин [5]. Розв'язання задач обробки даних ПРЛ призводить до поетапної обробки потоків даних, які можна поділити на такі етапи: обробки сигналів ПРЛ; первинної обробки даних; вторинної обробки даних. Проведені дослідження наочно показують, що етапна реалізація обробки даних ускладнює наскрізну оптимізацію виявлення і вимірювання координат ПО. Так, як стабілізація ймовірності помилкового виявлення ПО повинна здійснюватися аналоговим порогом виявлення сигналу, що складно забезпечити в розглядаємій системі обробки даних первинного радіолокатора.

Список літератури

- [1] І.І. Обод, І.В. Свид, О.С. Мальцев, Обробка даних радіолокаційних систем спостереження повітряного простору: навчальний посібник. – Харків: Друкарня Мадрид, 2021. – 255 с.
- [2] Свид І.В., Обод І.І. Завадостійкість радіолокаційних систем ідентифікації за ознакою «свій-чужий»: монографія. – Харків: Друкарня Мадрид, 2021. 254 с.
- [3] І.І. Обод, І.В. Свид. Порівняльний аналіз якості виявлення повітряних об'єктів запитальними системами спостереження. // Системи обробки інформації. Вип. 9 (90) – Харків, видавництво ХУПС, 2010 – С. 74-76.
- [4] I. Obod, I. Svyd, O. Maltsev and B. Bakumenko, Comparative Analysis of Noise Immunity Systems Identification Friend or Foe. // 2020 IEEE 40th International Conference on Electronics and Nanotechnology (ELNANO), Kyiv, Ukraine, 2020, P. 751-756.

- [5] I. Obod, I. Syvd, O. Maltsev, B. Bakumenko. Spatial Methods for Increasing the Bandwidth of a Mobile Information Network. // 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET-2020), Lviv-Slavske, Ukraine, 2020. – P. 50-54.
-

Автори

Ткач Марія Геннадіївна — аспірант, Харківський національний університет радіоелектроніки, Харків, Україна; E-mail: mariia.zavorotna@nure.ua

**Київський національний університет
імені Тараса Шевченка**

**Матеріали XX Міжнародної
науково-практичної конференції**

«Шевченківська весна – 2022»

14 квітня 2022 р., м. Київ, Україна

Taras Shevchenko National University of Kyiv

**Proceeding of XX International
Scientific – Practical Conference**

«Shevchenkivska Vesna – 2022»

14 April 2022, Kyiv, Ukraine