

КІБЕРНЕТИКА

CYBERNETICS

УДК 621.391.15:519.7

Алгоритм PQC CSIKE на нециклічних кривих Едвардса / А.В. Бессалов, С.В. Абрамов // Кібернетика та системний аналіз. 2023. Том 59, № 6. С. 3–18.

Анотація. Запропоновано оригінальний алгоритм постквантової криптографії CSIKE як модифікацію CSIDH, але з одним відкритим ключем замість двох. Обґрунтовано умови його імплементації на двох класах нециклічних кривих Едвардса. Розглянуто властивості квадратичних та скручених суперсингулярних кривих Едвардса, що утворюють пари квадратичного кручення порядку $p + 1 \equiv 0 \pmod{8}$ над простим полем F_p . Наведено модифікацію алгоритму CSIDH і алгоритм CSIKE, які побудовані на ізогеніях цих кривих замість традиційної арифметики кривих у формі Монтгомері. Для ізогеній ступенів 3, 5, 7 розраховано і табульовано параметри ізогенних ланцюжків нециклічних суперсингулярних кривих Едвардса, якщо $p = 839$. Розглянуто імплементацію схеми інкапсуляції ключа за умови, що Аліса шифрує його відкритим ключем Боба. Запропоновано новий рандомізований алгоритм CSIKE з випадковим рівномірним вибором кривої з двох класів на кожному кроці ланцюжка ізогеній. Наведено оцінку ймовірності успішної атаки побічного каналу в рандомізованому алгоритмі, у якому запропоновано можливість відмови від обчислення ізогенної функції $\phi(R)$ випадкової точки R , що істотно прискорить алгоритм.

Ключові слова: крива в узагальненій формі Едвардса, повна крива Едвардса, скручена крива Едвардса, квадратична крива Едвардса, порядок кривої, порядок точки, ізоморфізм, ізогенія, w -координати, квадратичний лишок, квадратичний нелишок.

PQC CSIKE algorithm in non-cyclic Edwards curves / A.V. Bessalov, S.V. Abramov // Kibernetika ta Systemnyi Analiz. 2023. Vol. 59, N 6. P. 3–18.

Abstract. The original post-quantum cryptography algorithm CSIKE is proposed as a modification of CSIDH but with one public key instead of two. The conditions for its implementation on two classes of non-cyclic Edwards curves are substantiated. The properties of quadratic and twisted supersingular Edwards curves that form pairs of quadratic twist of order $p + 1 \equiv 0 \pmod{8}$ over a prime field F_p are considered. A modification of the CSIDH algorithm and the CSIKE algorithm are presented, which are generated on the isogenies of these curves instead of the traditional arithmetic of curves in the Montgomery form. For isogenies of degrees 3, 5, and 7, the parameters of isogenic chains of non-cyclic supersingular Edwards curves are calculated and tabulated for $p = 839$. The implementation of the key encapsulation scheme with its encryption by Alice with Bob's public key is considered. A new randomized CSIKE algorithm with random equiprobable selection of a curve from two classes at each step of the isogeny chain is proposed. An estimate of the probability of a successful side-channel attack in a randomized algorithm is given. It is proposed to abandon the calculation of the isogenic function $\phi(R)$ of a random point R , which significantly speeds up the algorithm.

Keywords: curve in generalized Edwards form, complete Edwards curve, twisted Edwards curve, quadratic Edwards curve, curve order, point order, isomorphism, isogeny, w -coordinates, quadratic residue, quadratic nonresidue.

УДК 519.713.1

Побудова для множини $-\omega$ -слів, заданої $-\omega$ -регулярним виразом, її максимальної префіксно-замкнутої підмножини / А.М. Чеботарьов // Кібернетика та системний аналіз. 2023. Том 59, № 6. С. 19–29.

Анотація. Наведено метод побудови для множини $-\omega$ -слів R , заданої $-\omega$ -регулярним виразом, її максимальної префіксно-замкнутої підмножини. Цей метод ґрунтується на побудові розміченого графу, названого графом елементарних продовжень, вершинами якого є деякі $-\omega$ -регулярні підмножини множини R . Кожній вершині цього графу поставлено у відповідність лінійне рівняння над множинами $-\omega$ -слів. Отже, граф елементарних продовжень визначає систему лінійних рівнянь. У результаті розв'язання цієї системи рівнянь для кожної вершини графу отримуємо максимальну префіксно-замкнуту відносно R підмножину множини $-\omega$ -слів, яка відповідає цій вершині графу. Об'єднання цих підмножин для всіх початкових вершин графу, тобто вершин, з яких починають побудову графу, є максимальною префіксно-замкнутою підмножиною заданої множини R . Запропоновано метод побудови такого графу, який названо методом неповних перетинів, та спосіб розв'язання системи рівнянь, яку визначає граф елементарних продовжень.

Ключові слова: $-\omega$ -слово, $-\omega$ -регулярний вираз, префіксно-замкнута підмножина $-\omega$ -слів, граф елементарних продовжень, лінійне рівняння над $-\omega$ -регулярними множинами.

Constructing the maximum prefix-closed subset for a set of $-\omega$ -words defined by a $-\omega$ -regular expression / A.N. Chebotarev // Kibernetika ta Systemnyi Analiz. 2023. Tom 59, No 6. P. 19–29.

Abstract. We present a method for constructing the maximum prefix-closed subset of a set of $-\omega$ -words R defined by a $-\omega$ -regular expression. This method is based on constructing a labeled graph, called a graph of elementary extensions, whose vertices are some $-\omega$ -regular subsets of the set R . We associate every vertex of this graph with a linear equation over sets of $-\omega$ -words. Thus, the graph of elementary extensions determines a system of linear equations. As a result of its solution, for each vertex of the graph, we obtain the maximum prefix-closed (with respect to R) subset of the set of $-\omega$ -words corresponding to this vertex. The union of such

subsets that correspond to all initial vertices of the graph, i.e., the vertices from which constructing the graph starts, is the maximum prefix-closed subset of the given set R . We propose a method for constructing such a graph, called the method of incomplete intersections, and propose how to solve the system of equations determined by the graph of elementary extensions.

Keywords: ω -word, ω -regular expression, prefix-closed set of ω -words, graph of elementary extensions, linear equations over ω -regular sets.

УДК 681.3

Про один підхід до знаходження оцінок достовірності за умов нечіткого моделювання / О.І. Провотар, О.П. Ількун // Кібернетика та системний аналіз. 2023. Том 59, № 6. С. 30–39.

Анотація. Запропоновано підхід до знаходження чисельних оцінок достовірності нечітких знань у системах нечіткого логічного виведення. Модель системи типу «вхід–вихід» побудовано засобами нечіткої логіки. За правилом Мамдані знайдено вихід такої системи у вигляді нечітких знань з подальшим обчисленням їхньої достовірності. Для обчислення достовірності нечітких знань використано елементи теорії ймовірностей нечітких подій. Наведено приклад обчислення достовірності нечітких знань.

Ключові слова: нечітка множина, умовна ймовірність нечіткої події, нечітке правило.

An approach to finding credibility estimates in fuzzy modeling / O.I. Provotar, O.P. Ilkun // Kibernetika ta Systemnyi Analiz. 2023. Vol. 59, N 6. P. 30–39.

Abstract. The author proposes an approach to finding numerical estimates of the credibility of fuzzy knowledge in fuzzy logical inference systems. The “input–output” type system is modeled by means of fuzzy logic. According to Mamdani’s rule, the output of the system is found in the form of fuzzy knowledge with subsequent calculation of its credibility. Elements of the probability theory of fuzzy events are used to calculate the credibility of fuzzy knowledge. An example of calculating the credibility of fuzzy knowledge is given.

Keywords: fuzzy set, conditional probability of a fuzzy event, fuzzy rule.

УДК 336.144.36, 519.216.3, 519.254

Одне узагальнення ARIMA-моделі на нелінійний та неперервний випадки / М.Я. Кушнір, К.А. Токарева // Кібернетика та системний аналіз. 2023. Том 59, № 6. С. 40–50.

Анотація. Наведено один метод розширення класичних ARIMA- та GARCH-моделей на неперервний та нелінійний випадки. Як розширені моделі розглянуто стохастичні диференціально-функціональні рівняння, які є природним узагальненням сум незалежних випадкових величин. Запропоновано нову модель і відповідну оптимізаційну задачу оцінювання параметрів моделі, причому непараметричну задачу зведено до параметричної. Нову модель протестовано на реальних даних та зроблено порівняльний аналіз результатів прогнозування і класичних моделей.

Ключові слова: стохастичні диференціально-функціональні рівняння, генетичний алгоритм, прогнозування фінансових процесів, стохастична оптимізація.

A generalization of the ARIMA model to the nonlinear and continuous cases / M. Kushnir, K. Tokarieva // Kibernetika ta Systemnyi Analiz. 2023. Vol. 59, N 6. P. 40–50.

Abstract. A method of extending the classical ARIMA and GARCH models to the continuous and nonlinear cases is considered. Stochastic functional differential equations, which are a natural generalization of the sums of independent random variables, are considered extended models. Along with the new model, a relevant optimization problem for estimating model parameters is considered, and the non-parametric problem is reduced to a parametric one. The new model was tested on real data, and the forecast results were compared with classical models.

Keywords: stochastic functional differential equations, genetic algorithm, forecasting of financial processes, stochastic optimization.

УДК 004.8, 004.62

Адаптація технології Neural Radiance Fields (NeRF) для задачі 3D-реконструкції сцени в умовах динамічного освітлення / В.В. Савін, О.О. Колодяжна // Кібернетика та системний аналіз. 2023. Том 59, № 6. С. 51–61.

Анотація. Розглянуто проблему синтезу нових зображень сцени з використанням технології Neural Radiance Fields (NeRF) для середовища з динамічним освітленням. Для навчання NeRF моделей використано фотометричну функцію втрат, тобто попіксельну різницю між значеннями інтенсивності зображень сцени та зображень, згенерованих за допомогою NeRF. Для відбивних поверхонь інтенсивність зображення залежить від кута спостереження. Цей ефект враховано шляхом використання напрямку променя як вхідного параметра моделі NeRF. Для сцен зі динамічним освітленням інтенсивність зображення залежить не лише від позиції та напрямку спостереження, а й від часу. Показано, що зміна освітлення впливає на навчання NeRF із стандартною фотометричною функцією втрат і зумовлює зниження якості отриманих зображень та карт глибин. Щоб подолати цю проблему, запропоновано ввести час як додатковий вхідний аргумент до моделі NeRF. Експерименти, проведені на наборі даних ScanNet,

свідчать про те, що NeRF зі змінним входом перевершує оригінальну версію моделі та генерує більш послідовні й цілісні 3D-структури. Результати цього дослідження можна використати для покращення якості аугментації навчальних даних для навчання моделей передбачення відстані (наприклад, моделей depth-from-stereo, які забезпечують передбачення глибини/відстані на основі стереоданих) для сцен з нестатичним освітленням.

Ключові слова: комп'ютерний зір, технологія Neural Radiance Fields, динамічне освітлення, синтез даних, 3D-реконструкція сцени.

Adapting Neural Radiance Fields (NeRF) for 3D scene reconstruction under dynamic illumination conditions / V. Savin, O. Kolodiazhna // Kibernetika ta Systemnyi Analiz. 2023. Vol. 59, N 6. P. 51–61.

Abstract. We address the problem of novel view synthesis using Neural Radiance Fields (NeRF) for scenes with dynamic illumination. NeRF training utilizes photometric consistency loss that is pixel-wise consistency between a set of scene images and intensity values rendered by NeRF. For reflective surfaces, image intensity depends on the viewing angle, and this effect is taken into account by using ray direction as the NeRF input. For scenes with dynamic illumination, image intensity depends not only on the position and viewing direction but also on time. We show that this factor affects NeRF training with standard photometric loss function and decreases the quality of both image and depth rendering. To cope with this problem, we propose to add time as additional NeRF input. Experiments on ScanNet dataset demonstrate that NeRF with modified input outperforms the original model version and renders more consistent 3D structures. The results of this study could be used to improve the quality of training data augmentation for depth prediction models (e.g., depth-from-stereo models) for scenes with non-static illumination.

Keywords: computer vision, neural radiance fields, dynamic illumination, view synthesis, 3D scene reconstruction.

УДК 519.8: 004.934

Методика аналізу бітових потоків на основі використання відстані Дамерау–Левенштейна та інших метрик / А.М. Нищук, С.М. Ніколасв, О.М. Романов // Кібернетика та системний аналіз. 2023. Том 59, № 6. С. 62–71.

Анотація. Проведено аналіз особливостей різних відстаней (метрик) під час розв'язання задач порівняння бітових потоків. На прикладі розглянуто застосування запропонованої методики для розв'язання задачі ідентифікації бітових потоків цифрового кодування мовлення. Показано, що у цьому випадку найбільш ефективною є метрика Дамерау–Левенштейна.

Ключові слова: бітовий потік, відстань, метрика, цифрове кодування мовлення.

Techniques for analyzing bitstreams based on the use of Damerau–Levenshtein distance and other metrics / A. Nyshchuk, S. Nikolaev, O. Romanov // Kibernetika ta Systemnyi Analiz. 2023. Vol. 59, N 6. P. 62–71.

Abstract. The analysis of the features of various distances (metrics) in solving the problems of comparing bitstreams was carried out. The application of the proposed method for solving the problem of identification of bitstreams of digital speech coding is considered as an example. The greatest effectiveness of the Damerau–Levenshtein metric in this case is shown.

Keywords: bitstream, distance, metric, digital speech encoding.

СИСТЕМНИЙ АНАЛІЗ

SYSTEMS ANALYSIS

УДК 519. 21

Деякі багатомовні моделі керування запасами для критерію з переоцінкою / П.С. Кнопов, Т.В. Пепеляєва // Кібернетика та системний аналіз. 2023. Том 59, № 6. С. 72–78.

Анотація. Розглянуто багатомовну модель керування запасами. Досліджено задачу знаходження оптимальних у класі стаціонарних детермінованих марківських стратегій. Доведено твердження, що дає змогу зводити знаходження оптимальних стратегій до задачі знаходження оптимальних параметрів.

Ключові слова: марківські процеси, керування запасами, (s, S) -стратегія, критерій оптимальності, оптимальна стратегія.

Some multi-product inventory control models for criterion with re-evaluation / P.S. Knopov, T.V. Pepelyaeva // Kibernetika ta Systemnyi Analiz. 2023. Vol. 59, N 6. P. 72–78.

Abstract. The multi-task model of the inventory theory is considered. The problem of finding the optimal in the class of deterministic stationary Markov strategies is investigated. The theorems for finding the optimal strategies for the problem of finding optimal parameters are proved.

Keywords: Markov processes, inventory control, (s, S) -strategy, optimality criterion, optimal strategy.

УДК 519.85

Цифрова модель природних кернів із застосуванням методів геометричного проєктування / Ю.Г. Стоян, Т.Є. Романова, О.В. Кравченко, Г.М. Яськов, А.М. Чугай, Д.О. Велігоцький // Кібернетика та системний аналіз. 2023. Том 59, № 6. С. 79–88.

Анотація. Створено цифрову модель кернів порід-колекторів із застосуванням задачі пакування сферичних частинок у циліндричному контейнері. Запропоновано новий підхід до математичного моделювання структури породи-колектора та обчислення її пористості. Побудовано математичну модель задачі розміщення максимальної кількості куль різного діаметру в циліндричному контейнері як задачу змішаного цілочислового програмування. Розроблено алгоритм розв’язання, який ґрунтується на застосуванні методу оптимізації за групами змінних та стратегії ґратчастої декомпозиції. Вихідними даними для моделювання є результати експериментальних петрофізичних досліджень реальних кернів свердловин. Результати моделювання дають гарне наближення абсолютної пористості до природного прототипу. Застосування цього підходу дасть змогу вдосконалити технології видобутку вуглеводнів і збільшити ефективність їхнього впровадження.

Ключові слова: геометричне проєктування, цифрова модель, керн, пакування, кулі, нелінійна оптимізація.

Digital model of natural cores using geometric design / Yu. Stoyan, T. Romanova, O. Kravchenko, G. Yaskov, A. Chuhai, D. Veligotskyi // Kibernetika ta Systemnyi Analiz. 2023. Vol. 59, N 6. P. 79–88.

Abstract. The article aims to create a digital model of rock-collector cores using the problem of packing spherical particles in a cylindrical container. A new approach to the mathematical modeling of the rock-collector structure is proposed. The computation of its porosity is provided. A mathematical model of the problem of placing the maximum number of spheres with different diameters in a cylindrical container is presented. A solution algorithm is developed based on the optimization by groups of variables and a lattice decomposition strategy. The results of experimental petrophysical studies of real well cores are used as input data. The modeling results provide a good approximation of the absolute porosity of the natural prototype. The application of this approach will help improve hydrocarbon extraction technologies and increase their efficiency.

Keywords: geometric design, digital model, kern, packing, spheres, nonlinear optimization.

УДК 519.6

Непокрашувані оцінки швидкості збіжності методу перетворення Келі для наближення операторної експоненти в Гільбертовому просторі / В. Л. Макаров, Н. В. Майко, В. Л. Рябічев // Кібернетика та системний аналіз. 2023. Том 59, № 6. С. 89–95.

Анотація. Одержано інтегральну оцінку точності методу перетворення Келі розв’язування абстрактної задачі Коші для диференціального рівняння 1-го порядку з необмеженим операторним коефіцієнтом у Гільбертовому просторі. Оцінка свідчить, що цей метод має степеневу швидкість збіжності, порядок якої автоматично залежить від гладкості початкового вектора, а отже, він є методом без насичення точності. Доведено також непокрашуваність оцінки за порядком N (параметр дискретизації N характеризує кількість доданків частинної суми в апроксимації наближеного розв’язку).

Ключові слова: диференціальне рівняння, задача Коші, операторна експонента, Гільбертів простір, перетворення Келі, оцінка похибки.

Unimprovable error estimates of the cayley transform method for the operator exponential function in a Hilbert space / V. L. Makarov, N. V. Mayko, V. L. Ryabichev // Kibernetika ta Systemnyi Analiz. 2023. Vol. 59, N 6. P. 89–95.

Abstract. We obtain the error estimate of the Cayley transform method for solving the abstract Cauchy problem for the first-order differential equation with an unbounded operator coefficient in a Hilbert space. The estimate indicates that our method has a power rate of convergence which automatically depends on the smoothness of the initial data (i.e., our method is a method without saturation of accuracy). Moreover, we substantiate that the estimate is unimprovable in the order of N (the discretization parameter N characterizes the number of summands in the partial sum for the approximate solution).

Keywords: differential equation, Cauchy problem, operator exponential function, Hilbert space, Cayley transformation, error estimate.

УДК 519.863

Моделювання впливу кліматичних змін на врожайність сільськогосподарських культур / В.А. Пенеляєв, О.М. Голодніков, Н.О. Голоднікова // Кібернетика та системний аналіз. 2023. Том 59, № 6. С. 96–103.

Анотація. Розглянуто задачу моделювання впливу майбутнього клімату на врожайність сільськогосподарських культур (на прикладі ярої пшениці). Проаналізовано джерела кліматичних даних та значень агрометеорологічних індикаторів для минулих і майбутніх періодів. Розроблено математичну модель залежності медіани функції розподілу врожайності ярої пшениці від кліматичних змін з використанням агрокліматичних індикаторів. Проведено розрахунки за цією моделлю та проаналізовано отримані результати. Аналіз отриманих результатів свідчить про значне зростання рівня врожайності ярої пшениці у 2030–2040 рр. та підвищення ризику втрат її врожайності відносно історичних даних.

Ключові слова: кліматичні параметри, врожайність, квантильна регресія, реаналіз, агрометеорологічні індикатори, статистична вибірка.

Simulating the impact of climate change on the yield of agricultural crops / V.A. Pepelyayev, A.N. Golodnikov, N.A. Golodnikova // Kibernetika ta Systemnyi Analiz. 2023. Vol. 59, N 6. P. 96–103.

Abstract. The problem of modeling the impact of the future climate on the yield of agricultural crops (on the example of spring wheat) is considered. The sources of climatic data and values of agrometeorological indicators for past and future periods were analyzed. A mathematical model of the dependence of the median of the spring wheat yield distribution function on climatic changes was developed using agroclimatic parameters. The calculations were carried out according to this model, and the obtained results were analyzed. The analysis of the results indicates a significant increase in the yield level of spring wheat in 2030–2040 and an increase in the risk of losses of its yield in relation to historical data.

Keywords: climatic parameters, crop capacity, quantile regression, reanalysis, agrometeorological indicators, statistical sampling.

УДК 519.21

М-оцінки: огляд та застосування для прийняття рішень за умов невизначеності / М.С. Дунаєвський // Кібернетика та системний аналіз. 2023. Том 59, № 6. С. 104–115.

Анотація. Розглянуто еволюцію методу робастних оцінок, зокрема основні концепції методів М-оцінок та їхні переваги під час роботи з даними, що містять статистичні викиди. Проведено порівняння методів М-оцінок Хубера, Хампела та методу біквадратних ваг Тьюкі на реальних економічних даних регіонів України. Отримано емпіричне підтвердження ефективності їхнього застосування. Результати порівняння всіх побудованих моделей свідчать про суттєве зміщення оцінок параметрів у разі застосування підходу «наївного» видалення статистичних викидів. На основі побудованих робастних моделей можна з більшою точністю порівняти регіони країни за ефективністю факторів праці та капіталу, та відповідно визначити пріоритетність інвестицій, які більшою мірою стимулюватимуть економічний розвиток регіону.

Ключові слова: децентралізація, прийняття рішень, М-оцінки, регіональний розвиток, робастність, невизначеність.

M-estimates: a review and application for decision-making under uncertainty / M.S. Dunaievskiy // Kibernetika ta Systemnyi Analiz. 2023. Vol. 59, N 6. P. 104–115.

Abstract. A brief overview of the evolution of the robust estimate methods is presented, in particular, the main concepts of m-estimation methods and their advantages when working with data containing statistical outliers. The comparison of the results of the methods of M-estimates by P. Huber, F. Hampel, and the method of biquadratic weights by J. Tukey was held on real economic data of the regions of Ukraine. We have got empirical confirmation of the efficiency of using M-estimates. The comparison of all the generated models indicates a significant shift in parameter estimates, in case, the approach of naive removal of statistical outliers has been applied. Based on the constructed robust models, we can more accurately compare the regions of the country in terms of the labor and capital factors efficiency, and accordingly determine the priority of investments that will stimulate the economic development of the region to a greater extent.

Keywords: decentralization, decision-making, M-estimates, regional development, robustness, uncertainty.

УДК 338.2:338.3:338.4:330.5

Моделювання міжгалузевої економіки як критичної інфраструктури: розроблення сценаріїв розвитку економіки України в умовах війни та післявоєнного відновлення / В.В. Кулик // Кібернетика та системний аналіз. 2023. Том 59, № 6. С. 116–136.

Анотація. Розглянуто схему «витрати–випуск» у застосунку для дослідження міжгалузевого відтворення економіки України як критичної інфраструктури в умовах війни та післявоєнного часу. Розроблено ймовірний сценарій розвитку економіки України в 2022 р. Проаналізовано чутливість елементів кінцевих споживчих витрат до змін на 1 %. Запропоновано методику розроблення сценаріїв економічного розвитку в умовах війни та післявоєнного відновлення з урахуванням лінійності моделі Леонтьєва, чутливості елементів кінцевих споживчих витрат до змін та структури міжгалузових економічних зв'язків в Україні у 2019 р.

Ключові слова: моделювання міжгалузових зв'язків, таблиця «витрати–випуск», економіка України, види економічної діяльності, критична інфраструктура, системний аналіз, формування сценаріїв економічного розвитку, моделювання критичних ситуацій в економіці, кінцеве споживання, випуск.

Modeling the inter-industry economy as a critical infrastructure: generating the scenarios for the development of the economy of Ukraine during the war and in the post-war recovery / V.V. Kulyk // Kibernetika ta Systemnyi Analiz. 2023. Vol. 59, N 6. P. 116–136.

Abstract. The input-output scheme is considered as applied to the analysis of the cross-industry reproduction of the economy of Ukraine as a critical infrastructure in the conditions of war and post-war recovery. A probable scenario of the development of Ukraine's economy in 2022 has been prepared. The

hypothesis of the scenario is that the military economy significantly changes the structure of final consumer spending, which makes it possible to forecast inter-industry relationships, in particular, final spending and output, using the input-output model (Leontief model). An analysis of the sensitivity of elements of final consumer spending was carried out. The methodology for developing scenarios of economic development in the conditions of war and post-war recovery is proposed, taking into account the linearity of the Leontief model, the sensitivity of elements of final consumer spending and the interindustry relationship structure of the Ukraine's economy in 2019. Prepared materials can be used for scientific and educational purposes to generate various scenarios of final consumer spending in the conditions of war and post-war reconstruction.

Keywords: modeling of inter-industry relations, input-output table, economy of Ukraine, types of economic activity, critical infrastructure, system analysis, formation of economic development scenarios, modeling of critical situations in the economy, final consumption, output.

УДК 519.2

Точні оцінки ймовірності попадання випадкової величини в заданий інтервал в одному класі унімодальних розподілів / Л.С. Стойкова, В.Є. Чевардин // Кібернетика та системний аналіз. 2023. Том 59, № 6. С. 137–149.

Анотація. Розглянуто клас A унімодальних функцій розподілу $F_{\mu}(x)$ таких, що відомо лише два їхні перші моменти і мода m , яка співпадає з першим моментом. У класі A знайдено точні оцінки ймовірності попадання випадкової величини μ в інтервал $(0, 2m)$. Визначено додаткові параметри α_{η} і α_{μ} , які, змінюючись від 0 до ∞ , скеровують увесь процес розв'язання задачі: знаходяться екстремальні функції розподілу, що дають точні оцінки відповідному функціоналу; визначаються області існування екстремальних функцій. Задачу розв'язано для кожного фіксованого значення $\sigma_{\mu} \in (0, \infty)$ — середнього квадратичного відхилення випадкової величини μ від моди. Знайдено в явному вигляді унімодальні екстремальні функції розподілу $F_{\mu}(x)$ із класу A , на яких досягаються точні оцінки ймовірності попадання випадкової величини μ в інтервал $(0, 2m)$.

Ключові слова: точні оцінки, лінійні функціонали, класи унімодальних функцій розподілу.

Accurate estimates of the probability of a random variable falling into a given interval in one class of unimodal distributions / L.S. Stoikova, V.E. Chevardin // Kibernetika ta Systemnyi Analiz. 2023. Vol. 59, N 6. P. 137–149.

Abstract. A class A of unimodal distribution functions is considered, for which only the first two moments and the mode m , which coincides with the first moment, are known. In this class, accurate estimates of the probability of a random variable μ falling into the interval $(0, 2m)$ are found. Defined supplemental parameters α_{η} and α_{μ} , changing from 0 to ∞ , guide the entire process of solving the problem: extremal distribution functions are found that give accurate estimates to the corresponding functional; highlighting the areas of existence of these distribution functions with numbers; the problem turns out to be solved for all possible values of the mean square deviations σ_{μ} of the random variable μ . Unimodal extremal distribution functions from class A were found in an explicit form.

Keywords: Exact estimates, linear functionals, classes of unimodal distribution functions.

УДК 519.8

Багатокритерійні задачі оптимізації з векторними неоднорідними згортками критеріїв / А.Ю. Брила // Кібернетика та системний аналіз. 2023. Том 59, № 6. С. 150–157.

Анотація. Розглянуто багатокритерійні задачі прийняття рішень з критерійними порядками надання переваги, що є згортками згорток. Досліджено випадки, коли на множині векторних критеріїв задано субординацію рівної важливості або субординацію строгого ранжування. В обох випадках згортки в межах складових векторних критеріїв можуть бути неоднорідними. Доведено еквівалентність розглядуваних задач відповідним багатокритерійним задачам з однорідним (однаковим) ранжуванням у межах часткових векторних критеріїв.

Ключові слова: багатокритерійна задача оптимізації, згортки критеріїв, згортки згорток, векторні критерії, неоднорідні згортки критеріїв.

Multicriteria optimization problems with vector convolutions of non-homogeneous convolutions of criteria / A.Yu. Bryla // Kibernetika ta Systemnyi Analiz. 2023. Vol. 59, N 6. P. 150–157.

Abstract. Multicriteria decision-making problems are considered. Advantage orders are determined by criterial orders, which are convolutions of convolutions. The cases are analyzed where the subordination of equal importance or strict ranking subordination is specified on the set of vector criteria. In both cases, the convolutions within each of the partial vector criteria can be heterogeneous. The equivalence of the considered problems to the corresponding multicriteria decision-making problems with homogeneous (same) ranking within partial vector criteria is proved.

Keywords: multicriteria optimization problem, convolutions of criteria, convolutions of convolutions, vector criteria, heterogeneous convolutions of criteria.

УДК 519.21

Алгоритм оцінювання невідомого параметра гіббсовського розподілу на основі методу стохастичних квазіградієнтів / О.С. Самосюнок // Кібернетика та системний аналіз. 2023. Том 59, № 6. С. 158–162.

Анотація. Розглянуто практичний алгоритм оцінювання невідомого параметра математичної моделі марковського процесу з локальною взаємодією на основі гіббсовського розподілу. Запропоновано застосувати метод стохастичних квазіградієнтів до функції максимальної вірогідності, що побудована за спостереженнями реалізації гіббсовського поля. Отримано результати, які мають широку прикладну сферу застосування для моделювання стохастичних процесів.

Ключові слова: гіббсовський розподіл, метод максимальної вірогідності, марковські випадкові поля, стохастичний квазіградієнтний метод, оцінювання параметрів.

An algorithm for estimating the unknown parameter of the Gibbs distribution based on the method of stochastic quasi-gradients / O.S. Samosonok // Kibernetika ta Systemnyi Analiz. 2023. Vol. 59, N 6. P. 158–162.

Abstract. The author considers a practical algorithm for estimating an unknown parameter of a mathematical model of a Markov process with local interaction based on the Gibbs distribution. It is proposed to apply the method of stochastic quasi-gradients to the maximum likelihood function, which is constructed from the observations of the implementations of the Gibbs field. The obtained results have a wide application in the modeling of stochastic processes.

Keywords: Gibbs distribution, Maximum Likelihood Estimation, Markov random fields, stochastic quasigradient method, parameter estimation.

ПРОГРАМНО-ТЕХНІЧНІ КОМПЛЕКСИ

SOFTWARE–HARDWARE SYSTEMS

УДК 519.63; 519.64

Високопродуктивні методи моделювання наноадсорбції та дифузії зі зворотними зв'язками в неоднорідних циліндричних багатокомпонентних нанопористих середовищах / М.Р. Петрик, І.В. Бойко, О.М. Хіміч, В.А. Сидорук // Кібернетика та системний аналіз. 2023. Том 59, № 6. С. 163–178.

Анотація. Розроблено нові високопродуктивні аналітичні методи моделювання полів концентрацій дифундованих газів у внутрішньо- та міжчастинковому просторах у неоднорідних циліндричних n -складових нанопористих середовищах з використанням операційного методу Гевісайда та матриць впливу Коші для неоднорідних крайових задач адсорбції для систем рівнянь у частинних похідних зі зворотними зв'язками.

Ключові слова: модель багатокомпонентної наноадсорбції та дифузії, багатокомпонентні неоднорідні нанопористі середовища, операційний метод Гевісайда.

High-performance methods of modeling the nano-adsorption and diffusion with feedback in heterogeneous cylindrical multicomponent nanoporous media / M.R. Petryk, I.V. Boyko, O.M. Khimich, V.A. Sydoruk // Kibernetika ta Systemnyi Analiz. 2023. Vol. 59, N 6. P. 163–178.

Abstract. New high-performance analytical methods are developed for modeling the fields of diffused gas concentrations in intra- and interparticle spaces in inhomogeneous cylindrical n -component nanoporous media. The proposed approach is based on the Heaviside operational method and Cauchy influence matrices for inhomogeneous adsorption boundary-value problems arising from systems of partial differential equations.

Keywords: multicomponent nanoadsorption and diffusion model, heterogeneous nanoporous media, Heaviside operational method.

УДК 621.396, 681.2

Бездротові сенсорні мережі для цифрового землеробства, захисту довкілля та охорони здоров'я / В.О. Романов, І.Б. Галелюка, В.М. Груша, О.В. Вороненко, О.В. Ковирьова, Г.В. Антонова, А.В. Кедич // Кібернетика та системний аналіз. 2023. Том 59, № 6. С. 178–187.

Анотація. Наведено результати розроблення та створення бездротових сенсорних мереж для сільськогосподарства та медицини, отримані колективом авторів протягом останніх п'яти років. Розглянуто сенсорні мережі для оцінювання стану рослин методом індукції флуоресценції хлорофілу на великих площах сільськогосподарських угідь. Мережі мають у своєму складі оригінальні розумні сенсори, побудовані за гнучкою архітектурою, які містять елементи штучного інтелекту на базі нейронних мереж. Це підвищує їхню ефективність під час визначення дії стресових чинників різного походження. На основі бездротової сенсорної мережі побудовано розумну систему дистанційного медичного моніторингу, яка використовує кілька протоколів бездротового обміну даними. Для оцінювання якості життя і спектра симптомів, пов'язаних із захворюванням і/або лікуванням, створено діагностичну систему, яка визначає стан хворого за допомогою міжнародних та національних опитувальників. В основу роботи запропонованих розумних вимірювальних пристроїв та систем покладено базовані на знаннях принципи оброблення та аналізу даних вимірювання для вироблення управлінських рішень та рекомендацій. Більшість отриманих результатів доведено до серійного виробництва.

Ключові слова: бездротова сенсорна мережа, система збору даних, інформаційно-комунікаційна технологія, цифрове сільське господарство, оцінювання якості життя.

Wireless sensor networks for digital agriculture, environmental protection, and healthcare / V.O. Romanov, I.B. Galelyuka, V.M. Hrusha, O.V. Voronenko, O.V. Kovyrova, H.V. Antonova, A.V. Kedych // Kibernetika ta Systemnyi Analiz. 2023. Vol. 59, N 6. P. 178–187.

Abstract. The article presents the results of the development and creation of wireless sensor networks for agriculture and medicine, obtained by the team of authors during the past five years. Wireless sensor networks for estimating the state of plants by the method of chlorophyll fluorescence induction on large areas of agricultural lands are considered. These networks include original smart sensors, built according to flexible architecture and which contain elements of artificial intelligence based on neural networks, which increases their effectiveness in determining the effect of stress factors of different origins. On the basis of the wireless sensor network, a smart remote medical monitoring system has been built, which uses several wireless data exchange protocols. To assess the quality of life and the spectrum of symptoms, associated with the diseases and/or treatment, a diagnostic system was created, which determines the patient's state using international and national questionnaires. The basis of the operation of proposed smart measuring devices and systems is the knowledge-based principles of processing and analyzing the measuring data for making managerial decisions and giving recommendations to users. Most of the obtained results have been brought to serial production.

Keywords: wireless sensor network, data acquisition system, information and communication technology, digital agriculture, quality of life assessment.

УДК 621.317+681.849

Метод побудови системи виявлення та локалізації точок монтажу цифрових відеограм / В.І. Соловйов, О.В. Рибальський, В.В. Журавель, О.М. Шабля, Є.В. Тимко // Кібернетика та системний аналіз. 2023. Том 59, № 6. С. 188–194.

Анотація. Розглянуто та запропоновано базовий підхід до створення системи виявлення монтажу у цифрових відеограмах та відповідний метод. Запропонований підхід ґрунтується на дослідженнях з ідентифікації апаратури запису цифрових зображень за її власними шумами, зафіксованими на цифрових носіях. Встановлено, що основою методу виявлення та локалізації точок монтажу у відеограмах має бути використання функцій, які описують динаміку помилок ідентифікації сусідніх кадрів та динаміку функції модуля різниці рівнів сигналів кольорів двох кадрів перевірюваної відеограми. Для отримання цих функцій запропоновано застосувати декомпозицію сигналів з використанням вейвлета Хаара. Показано, що реалізацію системи слід здійснювати на нейронних мережах глибокого навчання, що забезпечить високу достовірність експертизи.

Ключові слова: апаратура запису цифрових зображень, вейвлети, відеограма, декомпозиція сигналу, ідентифікація, матриця, нейронні мережі глибокого навчання, власні шуми, криміналістика.

A method for constructing a system for detecting and localizing the places for editing digital videograms / V.I. Solovyov, O.V. Rybalskiy, V.V. Zhuravel, A.N. Shablya, Y.V. Tymko // Kibernetika ta Systemnyi Analiz. 2023. Vol. 59, N 6. P. 188–194.

Abstract. The basic approach and method for creating a system for detecting montage in digital videograms are considered and proposed. The proposed approach is based on the identification studies of digital image recording equipment by its own noise recorded on digital media. It has been established that the method for detecting traces and localizing edit points in videograms should be based on the use of the functions of the dynamics of errors in the identification of adjacent frames and the dynamics of the change in the function of the modulus of the difference in the levels of chrominance signals of two frames of the videogram being checked. To obtain these functions, it is proposed to apply signal decomposition using the Haar wavelet. It is shown that the implementation of the system should be carried out on deep learning neural networks, which will ensure high reliability of the examination.

Keywords: digital image recording equipment, wavelets, videogram, signal decomposition, identification, matrix, deep learning neural networks, intrinsic noise, forensics.

**НОВІ ЗАСОБИ КІБЕРНЕТИКИ,
ІНФОРМАТИКИ, ОБЧИСЛЮВАЛЬНОЇ
ТЕХНІКИ І СИСТЕМНОГО АНАЛІЗУ**

**NEW TOOLS IN CYBERNETICS,
COMPUTER SCIENCE, AND SYSTEM
ANALYSIS**

УДК 519.21

Асимптотичні властивості одного класу періодограмних оцінок / Г.Д. Біла, О.П. Кнопов // Кібернетика та системний аналіз. 2023. Том 59, № 6. С. 195–200.

Анотація. Розглянуто клас періодограмних оцінок невідомих параметрів нелінійної моделі регресії «сигнал плюс шум». Доведено їхню асимптотичну нормальність за умови, що функція регресії майже періодична, а шум є функціоналом від Гаусового випадкового процесу із сильною залежністю.

Ключові слова: сильна залежність, Гаусів шум, періодограма оцінка, асимптотична нормальність.

Asymptotic properties of a class of periodogram estimates / G.D. Bila, O.P. Knopov // Kibernetika ta Systemnyi Analiz. 2023. Vol. 59, N 6. P. 195–200.

Abstract. In this article, one class of periodogram estimates of unknown parameters of the nonlinear regression model “signal plus noise” is considered. The asymptotic normality is proved, provided that the regression function is almost periodic, and the noise is a functional of a strongly dependent Gaussian random process.

Keywords: long-range dependence, Gaussian noise, periodogram estimation, asymptotic normality.