**КІБЕРНЕТИКА** **CYBERNETICS**

УДК 519.72, 003.26

**Доверительные вычисления с использованием складывающей машины. I / А.В. Анисимов, А.К. Новокшонов** // Кибернетика и системный анализ. 2017. Том 53, № 5. С. 3–13.

Іл.: 0. Табл. 0. Бібліогр.: 16 назв.

**Аннотация.** Предложено решение проблемы целостности арифметических программ, выполняемых на удаленном вычислительном ресурсе. Решение состоит в замене арифметических операций, таких как умножение и деление, процедурами складывающей машины (addition machine), введенной Р. Флойдом и Д. Кнутом. Вычисления и порядок следования команд подписываются динамически изменяемой цифровой подписью, гомоморфной по сложению/вычитанию. Верификация цифровых подписей гарантирует обнаружение любых несанкционированных изменений в исходном тексте программы и результатах вычислений.

**Ключевые слова:** складывающая машина, цифровая подпись, гомоморфная криптография.

**Довірчі обчислення з використанням додавальної машини. I / А.В. Анісімов, А.К. Новокшонов** // Кібернетика та системний аналіз. 2017. Том 53, № 5. С. 3–13.

**Анотація.** Запропоновано розв'язання проблеми цілісності арифметичних програм, які виконуються на віддаленому обчислювальному ресурсі. Підхід до розв'язання полягає у заміні арифметичних операцій, таких як множення і ділення, процедурами додавальної машини (addition machine), введеної Р. Флойдом і Д. Кнутом. Обчислення і послідовність команд підписуються динамічним цифровим підписом, що є гомоморфним за додаванням/відніманням. Верифікація цифрових підписів гарантує виявлення будь-яких несанкціонованих змін у вихідному тексті програми і результатах обчислень.

**Ключові слова:** додавальна машина, цифровий підпис, гомоморфна криптографія.

**Trusted computing with addition machines. I / A.V. Anisimov, A.K. Novokshonov** // Kibernetika i sistemnyi analiz. 2017. Vol. 53, N 3. P. 3–13.

**Abstract.** A solution of the integrity problem for arithmetic programs running on a remote computing resource is proposed. The solution is to replace the arithmetic operations such as multiplication and division by procedures of the addition machine introduced by R. Floyd and D. Knuth. The order of instructions as well as current meanings of variables are signed by dynamic digital signatures, which are homomorphic with respect to addition and subtraction. Verification of digital signatures ensures detection of any unauthorized changes to the source code of the program and to the results of calculations.

**Keywords:** addition machine, digital signature, homomorphic cryptography.

===

УДК 512.548.7+519.713

**Автоматы на абстрактных конечных квазигруппах / В.В. Скобелев, В.Г. Скобелев** // Кибернетика и системный анализ. 2017. Том 53, № 5. С. 14–21.

Іл.: 0. Табл. 0. Бібліогр.: 13 назв.

**Аннотация.** Исследована структура семейств автоматов без выхода, заданных рекуррентными соотношениями на абстрактных конечных квазигруппах. Обоснована целесообразность их использования для построения семейств итерированных хэш-функций с достаточно высокой вычислительной стойкостью. Показано, как на основе этих семейств автоматов без выхода можно построить семейства обратимых автоматов Мили и Мура. Обоснована целесообразность использования предложенных семейств автоматов Мили и Мура для построения математической модели поточных шифров.

**Ключевые слова:** конечные квазигруппы, автоматы без выхода, автоматы Мили и Мура.

**Автомати на абстрактних скінченних квазігрупах / В.В. Скобелєв, В.Г. Скобелєв** // Кібернетика та системний аналіз. 2017. Том 53, № 5. С. 14–21.

**Анотація.** Досліджено структуру сімей автоматів без виходу, які визначено рекурентними співвідношеннями на абстрактних скінченних квазігрупах. Обґрунтовано доцільність їхнього використання для побудови сімей ітерованих геш-функцій з достатньо високою обчислювальною стійкістю. Показано, як на базі цих сімей автоматів без виходу можна побудувати сім'ї оборотних автоматів Мілі та Мура. Обґрунтовано доцільність використання запропонованих сімей автоматів Мілі та Мура для побудови математичних моделей потокових шифрів.

**Ключові слова:** скінченні квазігрупи, автомати без виходу, автомати Мілі та Мура.

**Automata over abstract finite quasigroups / V.V. Skobelev, V.G. Skobelev** // Kibernetika i sistemnyi analiz. 2017. Vol. 53, N 3. P. 14–21.

**Abstract.** The paper analyzes the structure of families of automata without output mapping that are defined by recurrence relations on abstract finite quasigroups. The expediency of their use to design iterated hash functions with sufficiently high security is justified. It is shown how some families of reversible Mealy and Moore automata can be constructed based on these families of automata without output mapping. The expediency of using the proposed families of Mealy and Moore automata as the basis for construction of mathematical models for stream ciphers is justified.

**Keywords:** finite quasigroups, automata without output mapping, Mealy and Moore automata.

===

УДК 519.713.1

**Проблемы синтеза Σ-автоматов, специфицированных в языках LP и LF логики первого порядка / А.Н. Чеботарев** // Кибернетика и системный анализ. 2017. Том 53, № 5. С. 22–33.

Іл.: 0. Табл. 0. Бібліогр.: 13 назв.

**Аннотация.** Для двух фрагментов, LP и LF, логики первого порядка с ограниченными кванторами сформулированы и доказаны соответствующие варианты теоремы о спецификации, позволяющие свести процедуру синтеза Σ-автоматов, специфицированных формулами этих логик, к эквивалентному преобразованию формул.

**Ключевые слова:** логики первого порядка, спецификация, Σ-автомат, LP-формула, LF-формула, автоматная семантика, теорема о спецификации.

**Проблеми синтезу Σ-автоматів, специфікованих мовами LP і LF логіки першого порядку / А.М. Чеботарьов** // Кібернетика та системний аналіз. 2017. Том 53, № 5. С. 22–33.

**Анотація.** Для двох фрагментів, LP і LF, логіки першого порядку з обмеженими кванторами сформульовано і доведено відповідні варіанти теореми про специфікацію, які дають можливість зведення процедури синтезу Σ-автоматів, що специфіковані формулами цих логік, до еквівалентного перетворення формул.

**Ключові слова:** логіки першого порядку, специфікація, Σ-автомат, LP-формула, LF-формула, автоматна семантика, теорема про специфікацію.

**Problems of synthesis of Σ-automata specified in languages LP and LF of first order logic / A.N. Chebotarev** // Kibernetika i sistemnyi analiz. 2017. Vol. 53, N 3. P. 22–33.

**Abstract.** For two fragments LP and LF of monadic first-order logic with bounded quantifiers, the corresponding versions of specification theorem are formulated and proved, which enables the Σ--automata synthesis procedure to be reduced to the equivalent transformation of formulas.

**Keywords:** first order logics, specification, -automaton, LP-formula, LF-formula, automatic semantics, specification theorem.

===

УДК 004.8

**Определение языков XML/RDF Semantic Web в метаязыке нормальных форм знаний / А.Ф. Кургаев, С.Н. Григорьев** // Кибернетика и системный анализ. 2017. Том 53, № 5. С. 34–42.

Іл.: 0. Табл. 0. Бібліогр.: 10 назв.

**Аннотация.** Даны формальные текстовые описания проблемно-ориентированных языков XML/RDF — базовых языков Semantic Web. Наличие таких описаний гарантирует реализуемость языков XML/RDF с использованием интерпретатора метаязыка нормальных форм знаний (НФЗ). Показано, что выразительные возможности метаязыка НФЗ для описания синтаксиса этой пары языков вполне сопоставимы с выразительными возможностями EBNF.

**Ключевые слова:** метаязык нормальных форм знаний, формальное описание метаязыка, eXtensible Markup Language, Resource Description Framework, Semantic Web.

**Визначення мов XML/RDF Semantic Web у метамові нормальних форм знань / О.П. Кургаєв, С.М. Григор'єв** // Кібернетика та системний аналіз. 2017. Том 53, № 5. С. 34–42.

**Анотація.** Наведено формальні текстові описи проблемно-орієнтованих мов XML/RDF — базових мов Semantic Web. Наявність таких описів гарантує реалізовність мов XML/RDF з використанням інтерпретатора метамови нормальних форм знань (НФЗ). Показано, що виразні можливості метамови НФЗ для опису синтаксису цієї пари мов цілком порівнянні з виразними можливостями EBNF.

**Ключові слова:** метамова нормальних форм знань, формальний опис метамови, eXtensible Markup Language, Resource Description Framework, Semantic Web.

**Definition of XML/RDF Semantic Web languages in the normal forms of knowledge metalanguage / A.F. Kurgaev, S.N. Grigoriev** // Kibernetika i sistemnyi analiz. 2017. Vol. 53, N 3. P. 34–42.

Abstract. Provided are the formal text descriptions of the problem-oriented XML/RDF languages, which are the basic Semantic Web languages. The availability of such descriptions guarantees the ability to implement the XML/RDF languages with the implementation of the interpreter of the NFK metalanguage. It is shown that the expressiveness of the NFK metalanguage in describing the syntax of the given pair of languages is quite comparable with EBNF expressiveness.

Keywords: Normal Forms of Knowledge Metalanguage, formal description of Metalanguage, eXtensible Markup Language, Resource Description Framework, Semantic Web.

===

**СИСТЕМНИЙ АНАЛІЗ** **SYSTEMS ANALYSIS**

УДК 519.8

**Теория и программные реализации *r*-алгоритмов Шора / П.И. Стецюк** // Кибернетика и системный анализ. 2017. Том 53, № 5. С. 43–57.

Іл.: 1. Табл. 1. Бібліогр.: 20 назв.

**Аннотация.** Рассмотрены три вычислительные формы *r*-алгоритмов с различным объемом вычислений на одной итерации. Приведены результаты о сходимости предельного варианта *r*-алгоритмов для выпуклых гладких функций и $r_\mu(\alpha)$-алгоритма для выпуклых кусочно-гладких функций. Обсуждены практические аспекты варианта $r(\alpha)$-алгоритмов с постоянным $\alpha$ — коэффициентом растяжения пространства, и адаптивным способом регулировки шага в направлении нормированного антисубградиента в преобразованном пространстве переменных.

**Ключевые слова:** субградиентный метод, наискорейший спуск, разность субградиентов, растяжение пространства, *r*-алгоритм, метод сопряженных градиентов, адаптивный шаг, программная реализация.

**Теорія та програмні реалізації *r*-алгоритмів Шора / П.І. Стецюк** // Кібернетика та системний аналіз. 2017. Том 53, № 5. С. 43–57.

**Анотація.** Розглянуто три обчислювальні форми *r*-алгоритмів з різним обсягом обчислень на одній ітерації. Наведено результати про збіжність граничного варіанта *r*-алгоритмів для опуклих гладких функцій і $r_\mu(\alpha)$-алгоритму для опуклих кусково-гладких функцій. Обговорено практичні аспекти варіанта $r(\alpha)$-алгоритмів з постійним $\alpha$ — коефіцієнтом розтягу простору і адаптивним способом регулювання кроку в напрямку нормованого антисубградієнта в перетвореному просторі змінних.

**Ключові слова:** субградієнтний метод, найшвидший спуск, різниця субградієнтів, розтяг простору, *r*-алгоритм, метод спряжених градієнтів, адаптивний крок, програмна реалізація.

**Theory and software implementations of Shor's *r*-algorithms / P.I. Stetsyuk** // Kibernetika i sistemnyi analiz. 2017. Vol. 53, N 3. P. 43–57.

**Abstract.** Three computational forms of *r*-algorithms with different amount of computation per iteration are considered. The results on the convergence of the limit variant of *r*-algorithms for convex smooth functions and the $r_\mu(\alpha)$-algorithm for convex piecewise smooth functions are presented. Practical aspects of the variant of $r(\alpha)$-algorithms with a constant coefficient of space dilation $\alpha$ and an adaptive method for step adjustment in the direction of the normalized anti-subgradient in the transformed space of variables are discussed.

**Keywords:** subgradient method, steepest descent, difference of subgradients, space dilation, *r*-algorithm, conjugate gradient method, adaptive step, software implementation.

===

УДК 517.977

**О растяжении времени в дифференциальных играх с импульсными управлениями / Г.Ц. Чикрий** // Кибернетика и системный анализ. 2017. Том 53, № 5. С. 58–66.

Іл.: 0. Табл. 0. Бібліогр.: 21 назва.

**Аннотация.** В развитие идей академика Б.Н. Пшеничного рассмотрена линейная дифференциальная игра сближения с импульсными управлениями. Предложена методика исследования, основанная на растяжении времени и ориентированная на ситуацию, когда классическое условие Понтрягина не имеет места. Получены достаточные условия конечности гарантированного времени сближения. Приведен иллюстративный пример.

**Ключевые слова:** функция растяжения времени, дифференциальная игра, импульсное управление, многозначное отображение, геометрическая разность Минковского, условие Понтрягина.

**Про розтягування часу у диференціальних іграх з імпульсними керуваннями / Г.Ц. Чикрій** // Кібернетика та системний аналіз. 2017. Том 53, № 5. С. 58–66.

**Анотація.** У розвиток ідей академіка Б.Н. Пшеничного розглянуто лінійну диференціальну гру з імпульсними керуваннями. Запропоновано методику дослідження, що базується на розтягуванні часу і орієнтована на ситуацію, коли класична умова Понтрягіна не має місця. Отримано достатні умови скінченності гарантованого часу зближення. Наведено ілюстративний приклад.

**Ключові слова:** функція розтягування часу, диференціальна гра, імпульсне керування, багатозначне відображення, геометрична різниця Мінковського, умова Понтрягіна.

**On the time extension in differential games with impulse controls / G.Ts. Chikrii** // Kibernetika i sistemnyi analiz. 2017. Vol. 53, N 3. P. 58–66.

**Abstract.** In the development of ideas of B.N. Pshenichnyi, the paper considers a linear differential game with impulse controls. A research technique is proposed, which is based on time extension and oriented to the case where the classical Pontryagin condition does not hold. Sufficient conditions for the finiteness of the guaranteed approach time are obtained. An illustrative example is given.

**Keywords:** function of the time extension, differential game, impulse control, set-valued mapping, Minkowski' geometric difference, Pontryagin's condition.

===

УДК 519.8

**Использование конической регуляризации при вычислении лагранжевых оценок в задачах квадратичной оптимизации / Ю.П. Лаптин, О.А. Березовский** // Кибернетика и системный анализ. 2017. Том 53, № 5. С. 67–81.

Іл.: 1. Табл. 0. Бібліогр.: 30 назв.

**Аннотация.** Для невыпуклых задач квадратичной оптимизации рассматривается вычисление оценок значений глобальных экстремумов на основе лагранжевых релаксаций исходных задач. На границе допустимой области оценочной задачи ее функции являются разрывными и плохо обусловленными, что накладывает определенные требования на вычислительные алгоритмы. Предложен новый подход, основанный на использовании конических регуляризаций выпуклых задач оптимизации позволяющий учесть указанные особенност, а также построить эквивалентную задачу безусловной оптимизации, целевая функция которой определена на всем пространстве переменных задачи и удовлетворяет условию Липшица.

**Ключевые слова:** задачи квадратичной оптимизации, лагранжева релаксация, условие неотрицательной определенности матрицы, коническая регуляризация.

**Використання конічної регуляризації при обчисленні лагранжевих оцінок у задачах квадратичної оптимізації / Ю.П. Лаптін, О.А. Березовський** // Кібернетика та системний аналіз. 2017. Том 53, № 5. С. 67–81.

**Анотація.** Для неопуклих задач квадратичної оптимізації розглянуто обчислення оцінок значень глобальних екстремумів на основі лагранжевої релаксації початкових задач. На границі допустимої області оціночної задачі її функції розривні та погано обумовлені, що накладає певні вимоги на обчислювальні алгоритми. Запропонован новий підхід для урахування зазначених особливостей, який базується на використанні конічних регуляризацій опуклих задач оптимізації. Він дозволяє побудувати еквівалентну задачу безумовної оптимізації, цільова функція якої визначена на всьому просторі змінних задачі і задовольняє умові Ліпшиця.

**Ключові слова:** задача квадратичної оптимізації, лагранжева релаксація, умова невід'ємної визначеності матриці, конічна регуляризація.

**Using conical regularization in calculating Lagrangian estimates in quadratic optimization problems / Yu.P. Laptin, O.A. Berezovskyi** // Kibernetika i sistemnyi analiz. 2017. Vol. 53, N 3. P. 67–81.

**Abstract.** For nonconvex quadratic optimization problems, calculation of global extreme value estimates on the basis of Lagrangian relaxation of the original problems is considered. On the boundary of the feasible region of the estimation problem, the functions of the problem are discontinuous, ill-conditioned, which imposes certain requirements on the computational algorithms. The paper presents a new approach taking into account these features, based on the use of conical regularizations of convex optimization problems. It makes it possible to construct an equivalent unconditional optimization problem, whose objective function is defined on the entire space of problem variables and satisfies the Lipschitz condition.

**Keywords:** quadratic optimization problem, Lagrangian relaxation, condition of non-negative definiteness of the matrix, conical regularization.

===

УДК 519.85
**Метод искусственного расширения пространства в задачах размещения геометрических объектов / С.В. Яковлев** // Кибернетика и системный анализ. 2017. Том 53, № 5. С. 82–89.

Іл.: 0. Табл. 0. Бібліогр.: 30 назв.

**Аннотация.** Рассматривается задача оптимального размещения геометрических объектов с заданными формой и физико-метрическими параметрами. Выделяется комбинаторная структура задачи. На основе искусственного расширения размерности пространства сформулирована эквивалентная постановка исходной задачи, в которой физико-метрические параметры являются независимыми переменными. Рассмотрен пример построения равновесной модели задачи упаковки кругов в круг минимального радиуса.

**Ключевые слова:** оптимальное размещение, комбинаторное множество, равновесная упаковка.

**Метод штучного розширення простору у задачах розміщення геометричних об'єктів / С.В. Яковлєв** // Кібернетика та системний аналіз. 2017. Том 53, № 5. С. 82–89.

**Анотація.** Розглянуто задачу оптимального розміщення геометричних об'єктів із заданими формою і фізико-метричними параметрами. Виділено комбінаторну структуру задачі. На основі штучного розширення розмірності простору сформульовано еквівалентну постановку вихідної задачі, у якої фізико-метричні параметри є незалежними змінними. Розглянуто приклад побудови рівноважної моделі задачі упаковки кругів у круг мінімального радіусу.

**Ключові слова:** оптимальне розміщення, комбінаторна множина, рівноважне пакування.

**The method of artificial space expansion in problems of optimal placement of geometric objects / S.V. Yakovlev** // Kibernetika i sistemnyi analiz. 2017. Vol. 53, N 3. P. 82–89.

**Abstract.** The problem of optimal placement of geometric objects with specified shape and physical-metric parameters is considered. The combinatorial structure of the problem is defined. An equivalent problem is formulated based on the artificial expansion of space dimension with physical-metric parameters being independent variables. The proposed approach is illustrated by the solution of balanced circular packing problem.

**Keywords:** optimal packing problem, combinatorial set, balanced packing.

===

УДК 517.9:519.6
**Решения некоторых задач дробно-дифференциальной фильтрационной динамики на основе модели с *ABC*-дробной производной / В.М. Булавацкий** // Кибернетика и системный анализ. 2017. Том 53, № 5. С. 90–101.

Іл.: 0. Табл. 0. Бібліогр.: 29 назв.

**Аннотация.** Для геофильтрационной математической модели с дробной производной Атангана–Балеану получены замкнутые решения краевых задач теории фильтрации в однородном и слоистом массивах конечной мощности. Приведены постановки и решения задачи с нелокальными граничными условиями и обратной задачи дробно-дифференциальной фильтрационной динамики.

**Ключевые слова:** математическое моделирование, дробно-дифференциальная динамика фильтрационных процессов, геопористые среды, неклассические модели, уравнение фильтрации с *ABC*-дробной производной, краевые задачи, замкнутые решения.

**Розв'язки деяких задач дробово-диференційної фільтраційної динаміки на основі моделі з *ABC*-дробовою похідною** / В.М. Булавацький // Кібернетика та системний аналіз. 2017. Том 53, № 5. С. 90–101.

**Анотація.** Для геофільтраційної математичної моделі з дробовою похідною Атангана–Балеану одержано замкнені розв'язки крайових задач теорії фільтрації в однорідному та шаруватому масивах скінченної потужності. Наведено постановки і розв'язання задачі з нелокальними граничними умовами та оберненої задачі дробово-диференційної фільтраційної динаміки.

**Ключові слова:** математичне моделювання, дробово-диференційна динаміка фільтраційних процесів, геопористі середовища, некласичні моделі, рівняння фільтрації з *ABC*-дробовою похідною, крайові задачі, замкнені розв'язки.

**Solutions of some problems of fractional-differential filtration dynamics based on models with *ABC*-fractional derivative / V.M. Bulavatsky** // Kibernetika i sistemnyi analiz. 2017. Vol. 53, N 3. P. 90–101.

**Abstract.** For geofiltration mathematical model with Atangana–Baleanu fractional derivative, closed solutions of boundary-value problems of filtration theory in homogeneous and layered arrays of finite size are obtained. Problems with nonlocal boundary conditions and the inverse problem of fractional differential filtration dynamics are formulated and solved.

**Keywords:** mathematical modeling, fractional-differential dynamics of filtration processes, geoporous media, non-classical models, equation of filtration with *ABC*-fractional derivative, boundary-value problems, closed form solutions.

===

УДК 517.95:519.86:539.3
**О задачах управления динамикой неполно определенных трехмерных упругих тел. II. Случай дискретно заданного желаемого состояния / В.А. Стоян** // Кибернетика и системный анализ. 2017. Том 53, № 5. С. 102–112.

Іл.: 0. Табл. 0. Бібліогр.: 7 назв.

**Аннотация.** Решены задачи управления линейно преобразованной вектор-функцией смещений точек трехмерного упругого тела в целях среднеквадратического приближения ее к дискретно заданным значениям. Задачи решаются без ограничений на геометрию тела и при дискретно определенных наблюдениях за его начально-краевым состоянием. В качестве управляющих факторов рассматриваются объемно-, поверхностно- и начально-распределенные внешнединамические возмущения. Выполнена оценка точности и однозначности управления.

**Ключевые слова:** пространственно распределенные динамические системы, пространственные задачи теории упругости, псевдоинверсия, управление.

**Про задачі керування динамікою неповно визначених тривимірних пружних тіл. II. Випадок дискретно заданого бажаного стану / В.А. Стоян** // Кібернетика та системний аналіз. 2017. Том 53, № 5. С. 102–112.

**Анотація.** Розв'язано задачі керування лінійно перетвореною вектор-функцією зміщень точок тривимірного пружного тіла з метою середньоквадратичного наближення її до дискретно заданих значень. Задачі розв'язуються без обмежень на геометрію тіла і при дискретно визначених спостереженнях за його початково-крайовим станом. Як керувальні фактори розглянуто об'ємно-, поверхнево- і початково-розподілені зовнішньодинамічні збурення. Проведено оцінювання точності та однозначності керування.

**Ключові слова:** просторово розподілені динамічні системи, просторові задачі теорії пружності, псевдоінверсія, керування.

**Problems of control of the dynamics of incompletely defined three-dimensional elastic bodies. II. The case of discretely defined desired state / V.A. Stoyan** // Kibernetika i sistemnyi analiz. 2017. Vol. 53, N 3. P. 102–112.

**Abstract.** The author solves the problems of control of linearly transformed vector function of displacement points of three-dimensional elastic body with the purpose of root-mean-square approximation to its discretely defined values. The problems are solved without constraints on the body geometry and under discretely defined observations of its initial-boundary state. Space, superficial, and initially distributed outward perturbations are considered as control factors. The evaluation of accuracy and uniqueness of control is conducted.

**Keywords:** spatially distributed dynamical systems, spatial problems of elasticity theory, pseudoinversion, control.

===

УДК 519.8
**Совершенные паросочетания и полиматроиды / Ф.А. Шарифов** // Кибернетика и системный анализ. 2017. Том 53, № 5. С. 113–119.

Іл.: 2. Табл. 0. Бібліогр.: 7 назв.

**Аннотация.** Показано, что произвольный граф содержит совершенное паросочетание тогда и только тогда, когда специально определенный вектор является базой расширенного полиматроида, описанного субмодулярной функцией, определенной на подмножествах множества вершин. На базе этого факта можно применить различные алгоритмы решения задачи о допустимых потоках на сетях для нахождения совершенного паросочетания в заданном графе.

**Ключевые слова:** совершенное паросочетание, граф, расширенный полиматроид.

**Досконалі парносполуки і поліматроїди / Ф.А. Шаріфов** // Кібернетика та системний аналіз. 2017. Том 53, № 5. С. 113–119.

**Анотація.** Показано, що довільний граф містить досконалу парносполуку тоді і тільки тоді, коли спеціально визначений вектор є базою розширеного поліматроїда, описаного субмодулярною функцією, визначеною на підмножинах множин вершин. На базі цього факту можна застосовувати різні алгоритми розв'язання задачі про допустимі потоки в мережах для знаходження досконалої парносполуки у заданому графі.

**Ключові слова:** досконалі парносполуки, граф, розширений поліматроїд.

**Perfect matching and polymatroids / F.A. Sharifov** // Kibernetika i sistemnyi analiz. 2017. Vol. 53, N 3. P. 113–119.

**Abstract.** It is shown that any graph has a perfect matching if and only if a specially defined vector is the base of the extended polymatroid associated with the submodular function defined on subsets of the vertex set. Based on this fact, different algorithms for testing flow feasibility can be used to find some perfect matching in a given graph.

**Keywords:** perfect matching, graph, extended polymatroid.

===

УДК 519.6+004.02
**Повышение эффективности чебышевской сегментной дробно-рациональной аппроксимации / Л.П. Вакал, А.А. Каленчук-Порханова, Е.С. Вакал** // Кибернетика и системный анализ. 2017. Том 53, № 5. С. 120–128.

Іл.: 0. Табл. 2. Бібліогр.: 21 назва.

**Аннотация.** Представлен алгоритм чебышевской сегментной аппроксимации со свободными узлами. В качестве аппроксимирующих функций на подынтервалах использованы рациональные дроби. Для поиска оптимальных узлов применен алгоритм дифференциальной эволюции. Приведены численные результаты по сегментной аппроксимации функций с оптимальными узлами.

**Ключевые слова:** чебышевская сегментная аппроксимация, задача многомерной нелинейной оптимизации, рациональные дроби, оптимальные узлы, алгоритм дифференциальной эволюции.

**Підвищення ефективності чебишовської сегментної дробово-раціональної апроксимації / Л.П. Вакал, А.О. Каленчук-Порханова, Є.С. Вакал** // Кібернетика та системний аналіз. 2017. Том 53, № 5. С. 120–128.

**Анотація.** Представлено алгоритм чебишовської сегментної апроксимації з вільними вузлами. Як апроксимуючі функції на підінтервалах використовують раціональні дроби. Для пошуку оптимальних вузлів застосовується алгоритм диференціальної еволюції. Наведено чисельні результати щодо сегментної апроксимації функцій з оптимальними вузлами.

**Ключові слова:** чебишовська сегментна апроксимація, задача багатовимірної нелінійної оптимізації, раціональні дроби, оптимальні вузли, алгоритм диференціальної еволюції.

**Increasing the efficiency of Chebyshev segment rational fractional approximation / L.P. Vakal, A.A. Kalenchuk-Porkhanova, E.S. Vakal** // Kibernetika i sistemnyi analiz. 2017. Vol. 53, N 3. P. 120–128..

**Adstract.** An algorithm for Chebyshev segment approximation with free nodes is presented. Rational fractions are used as approximating functions on subintervals. The differential evolution algorithm is used to find optimal nodes. Numerical results concerning segment approximation of functions with optimal nodes are given.

**Keywords:** Chebyshev segment approximation, multidimensional nonlinear optimization problem, rational fractions, optimal node, differential evolution algorithm.

===

УДК 621.396
**Модель работы локального планировщика на основе решения задач нелинейного булевого программирования / Е.С. Листровая, В.А. Брыксин, М.С. Курцев** // Кибернетика и системный анализ. 2017. Том 53, № 5. С. 129–140.

Іл.: 4. Табл. 3. Бібліогр.: 7 назв.

**Аннотация.** Рассмотрена имитационная модель работы грид-системы, позволяющая сравнивать существующие методы планирования выполнения заданий, и дано математическое описание исследуемых в модели характеристик. Приведен пример решения задачи на основе метода групповой выборки. Получены экспериментальные результаты, доказывающие преимущества метода планирования выполнения заданий на основе решения задач булевого нелинейного программирования.

**Ключевые слова:** грид-системы, планирование, ресурс, кластер, пакетная обработка, групповая выборка.

**Модель роботи локального планувальника на основі розв'язання задач нелінійного булевого програмування / О.С. Лістрова, В.О. Бриксін, М.С. Курцев** // Кібернетика та системний аналіз. 2017. Том 53, № 5. С. 129–140.

**Анотація.** Розглянуто імітаційну модель роботи грід-системи, яка дозволяє порівнювати наявні методи планування виконання завдань, та дано математичний опис досліджуваних в моделі характеристик. Наведено приклад розв'язання задачі на основі методу групової вибірки. Отримано експериментальні результати, що доводять переваги методу планування виконання завдань на основі розв'язання задач булевого нелінійного програмування.

**Ключові слова:** грід-системи, планування, ресурс, кластер, пакетне оброблення, групова вибірка.

**Modeling local planner operation based on solution of nonlinear boolean programming problems / E.S. Listrovaya, V.A. Bryksin, M.S. Kurtsev** // Kibernetika i sistemnyi analiz. 2017. Vol. 53, N 3. P. 129–140.

**Abstract.** The simulation model of grid system operation is considered, which allows comparing available job scheduling methods. The mathematical description of the characteristics analyzed in the model is given. An example of problem solution based on cluster sampling method is presented. The experimental results are obtained, which demonstrate the advantages of scheduling method based on the solution of Boolean linear programming problems.

**Keywords:** grid systems, planning, resource, cluster, batch processing, sample group.

===

УДК 519.21
**Определение стационарных характеристик некоторых систем обслуживания с эрланговскими распределениями / Ю.В. Жерновый** // Кибернетика и системный анализ. 2017. Том 53, № 5. С. 141–150.

Іл.: 0. Табл. 3. Бібліогр.: 9 назв.

**Аннотация.** Предложен метод исследования систем обслуживания $M / E_s / 1 / m$, $E_r / E_s / 1 / m$ и $E_r / M / n / m$, включая случай $m = \infty$. Получены рекуррентные соотношения для вычисления стационарного распределения числа заявок в системе и стационарных характеристик. Построенные алгоритмы проверены на примерах с использованием имитационных моделей, созданных с помощью инструментальных средств GPSS World.

**Ключевые слова:** система обслуживания, эрланговские распределения, метод фиктивных фаз, рекуррентные соотношения, стационарные характеристики.

**Визначення стаціонарних характеристик деяких систем обслуговування з ерлангівськими розподілами / Ю.В. Жерновий** // Кібернетика та системний аналіз. 2017. Том 53, № 5. С. 141–150.

**Анотація.** Запропоновано метод дослідження систем обслуговування $M / E_s / 1 / m$ , $E_r / E_s / 1 / m$ та $E_r / M / n / m$ , в тому числі для випадку $m = \infty$. Отримано рекурентні співвідношення для обчислення стаціонарного розподілу кількості замовлень у системі та стаціонарних характеристик. Побудовані алгоритми перевірено на прикладах з використанням імітаційних моделей, створених за допомогою інструментальних засобів GPSS World.

**Ключові слова:** система обслуговування, ерлангівські розподіли, метод фіктивних фаз, рекурентні співвідношення, стаціонарні характеристики.

**Determining steady-state characteristics of certain queueing systems with Erlangian distributions / Yu.V. Zhernovyi** // Kibernetika i sistemnyi analiz. 2017. Vol. 53, N 3. P. 141–150.

**Abstract.** We propose a method to study $M / E_s / 1 / m$, $E_r / E_s / 1 / m$, and $E_r / M / n / m$ queueing systems, including the case of $m = \infty$. Recurrence relations are obtained to compute the stationary distribution of the number of customers in the system and the steady-state characteristics. The developed algorithms are tested on examples using simulation models constructed with the assistance of the GPSS World tools.

**Keywords:** queueing systems, Erlangian distribution, fictitious phase method, recurrence relations, steady-state characteristics.

===

УДК 519.212
**Интенсивность пересечений заданного уровня однородным случайным полем / Д.В. Евграфов** // Кибернетика и системный анализ. 2017. Том 53, № 5. С. 151–159.

Іл.: 3. Табл. 0. Бібліогр.: 16 назв.

**Аннотация.** Дано определение понятия интенсивности пересечений однородным полем заданного уровня как среднего количества попаданий точек поверхности уровня в расширяющееся пространство. Показано, что независимо от положения центра расширяющегося пространства задача отыскания интенсивности сводится к подсчету поверхностей уровня в единице объема. Сформулирована возможность отыскания количества поверхностей уровня как характеристики, зависящей от количества поверхностно порождающих точек. Найдено дифференциальное уравнение, связывающее интенсивности точек локальных максимумов и локальных минимумов с искомой интенсивностью поверхностей уровня. На гауссовом стационарном процессе проверена достоверность полученных результатов, которые полностью совпадают с выражением, впервые найденным Райсом.

**Ключевые слова:** пересечения фиксированного уровня снизу вверх (сверху вниз) случайным полем, ожидаемое количество выбросов случайного поля, распределение абсолютного максимума случайного поля.

**Інтенсивність перетинів заданого рівня однорідним випадковим полем / Д.В. Євграфов** // Кібернетика та системний аналіз. 2017. Том 53, № 5. С. 151–159.

**Анотація.** Наведено визначення поняття інтенсивності перетинів однорідним полем заданого рівня як середньої кількості потрапляння точок поверхні рівня у розширному просторі. Показано, що незалежно від положення центру розширного простору задача відшукування інтенсивності зводиться до підрахунків кількості поверхонь рівня в одиниці об'єму. Сформульовано можливість відшукування кількості поверхонь рівня як характеристики, що залежить від кількості поверхнево породжувальних точок. Знайдено диференційне рівняння, яке зв'язує інтенсивності точок локальних максимумів і локальних мінімумів з шуканою інтенсивністю поверхонь рівня. На гаусівському стаціонарному процесі перевірено достовірність отриманих результатів, які повністю збігаються з виразом, уперше знайденим Райсом.

**Ключові слова:** перетини фіксованого рівня знизу вверх (зверху вниз) випадковим полем, очікувана кількість викидів випадкового поля, розподіл абсолютного максимуму випадкового поля.

**Intensity of crossings of a given level by a homogeneous random field / D.V. Yevgrafov** // Kibernetika i sistemnyi analiz. 2017. Vol. 53, N 3. P. 151–159.

**Abstract.** The author defines the concept of the intensity of crossings of a given level by a homogeneous field as the average number of points of level surface that hit the expanding space. It is shown that irrespective of the position of the center of expanding space, the problem of finding the intensity reduces to counting the level surfaces per unit volume. The author formulates the possibility of finding the number of level surfaces as a characteristic that depends on birth-surface points. A differential equation is found that relates the intensities of points of local maxima and local minima with the desired intensity of level surfaces. The accuracy of the results is verified for the stationary Gaussian process. The results completely coincide with the expression found by Rice for the first time.

**Keywords:** up-crossings (down-crossings) of the fixed level by random field, expected number of excursion sets for the random field, distribution of absolute maximum of random field.

===

УДК: 656.09:519.832.3

**Формирование матрицы выигрышей в формализованной игре между судовладельцем и менеджерской компанией / Е.С. Мелешенко** // Кибернетика и системный анализ. 2017. Том 53, № 5. С. 160–166.

Іл.: 0. Табл. 3. Бібліогр.: 11 назв.

**Аннотация.** Разрешен конфликт между судовладельцем и менеджером по договору судового менеджмента посредством использования методологического аппарата теории игр. Представлены стратегии поведения игроков — судовладельца и менеджера, на основании которых сформированы матрицы выигрышей, способствующие принятию решений по обеспечению устойчивого и эффективного взаимодействия.

**Ключевые слова:** теория игр, матрица выигрышей, судовладелец, менеджерская компания, стратегия.

**Формування матриці виграшів у формалізованій грі між судновласником і менеджерською компанією / К.С. Мелешенко** // Кібернетика та системний аналіз. 2017. Том 53, № 5. С. 160–166.

**Анотація.** Розв'язано конфлікт між судновласником і менеджером за договором суднового менеджменту за допомогою використання методологічного апарату теорії ігор. Представлено стратегії поведінки гравців — судновласника і менеджера, на підставі яких сформовано матриці виграшів, що сприяють прийняттю рішень щодо забезпечення сталої та ефективної взаємодії.

**Ключові слова:** теорія ігор, матриця виграшів, судновласник, менеджерська компанія, стратегія.

**Forming the payoff matrix in the formalized game between shipowner and managing company / K.S. Meleshenko** // Kibernetika i sistemnyi analiz. 2017. Vol. 53, N 3. P. 160–166.

**Abstract.** The settlement of the conflict between the shipowner and manager under a contract of marine management can be realized through the use of methodological apparatus of game theory. The paper presents the strategies of behavior of players (shipowner and manager), on the basis of which the matrixes of wins are formed and decision-making for sustainable and effective interaction.

**Keywords:** game theory, payoff matrix, shipowner, management company, strategy.

===

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

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

УДК 004.22 + 004.93'11

**Индексные структуры для быстрого поиска по сходству бинарных векторов / Д.А. Рачковский** // Кибернетика и системный анализ. 2017. Том 53, № 5. С. 167–192.

Іл.: 0. Табл. 0. Бібліогр.: 134 назв.

**Аннотация.** Дан обзор индексных структур для быстрого поиска по сходству объектов, представленных бинарными векторами (с компонентами 0 или 1). Рассмотрены структуры как для точного, так и для приближенного поиска по расстоянию Хэмминга и другим мерам сходства. Представлены, главным образом, индексные структуры на основе хэш-таблиц, сохраняющего сходство хэширования, а также древовидных структур, графов соседства и нейросетевой распределенной автоассоциативной памяти. Изложены идеи известных и предложенных в последнее время алгоритмов.

**Ключевые слова:** поиск по сходству, расстояние Хэмминга, ближайший сосед, ближний сосед, индексные структуры, мультииндексное хэширование, локально-чувствительное хэширование, древовидные структуры, граф соседства, нейросетевая автоассоциативная память.

**Індексні структури для швидкого пошуку за схожістю бінарних векторів / Д.А. Рачковський** // Кібернетика та системний аналіз. 2017. Том 53, № 5. С. 167–192.

**Анотація.** Наведено огляд індексних структур для швидкого пошуку за схожістю об'єктів, що представлені бінарними векторами (із компонентами 0 або 1). Розглянуто структури як для точного, так і для наближеного пошуку за відстанню Хеммінга та іншими мірами схожості. Описано, головним чином, індексні структури на основі хеш-таблиць, хешування, що зберігає схожість, а також деревовидних структур, графів сусідства та нейромережевої розподіленої автоасоціативної пам'яті. Викладено ідеї конкретних алгоритмів (відомих та нещодавно запропонованих).

**Ключові слова:** пошук за схожістю, відстань Хеммінга, найближчий сусід, ближній сусід, індексні структури, мультиіндексне хешування, локально-чутливе хешування, деревовидні структури, граф сусідства, нейромережева автоасоціативна пам'ять.

**Index structures for fast similarity search of binary vectors / D.A. Rachkovskij** // Kibernetika i sistemnyi analiz. 2017. Vol. 53, N 3. P. 167–192.

**Abstract.** We survey index structures for fast similarity search of objects represented by binary vectors (with components 0 or 1). Structures for both exact and approximate search by Hamming distance and other similarity measures are considered. Mainly, we present index structures based on hash tables, similarity-preserving hashing, as well as tree structures, neighborhood graphs, and neural distributed autoassociative memory. The ideas of specific algorithms, including the recently proposed ones, are outlined.

**Keywords:** similarity search, Hamming distance, nearest neighbor, near neighbor, index structures, multi-index hashing, locally-sensitive hashing, treelike structures, neighborhood graph, neural autoassociative memory.

===