# B E C T H H K

## САНКТ-ПЕТЕРБУРГСКОГО УНИВЕРСИТЕТА

Серия 10 Выпуск 4 2011 Декабрь ПРИКЛАДНАЯ МАТЕМАТИКА ИНФОРМАТИКА ПРОЦЕССЫ УПРАВЛЕНИЯ

НАУЧНО-ТЕОРЕТИЧЕСКИЙ ЖУРНАЛ. ИЗДАЕТСЯ С АВГУСТА 1946 ГОДА

## СОДЕРЖАНИЕ

### ПРИКЛАДНАЯ МАТЕМАТИКА

Александров А. Ю. Исследование устойчивости решений одного класса сложных	3
системИванов В. Я. Численное моделирование быстрых фотодетекторов большой пло- щади	3 14
Камачкин А. М. О строении окрестности кусочно-гладкой орбиты	32
Карелин В. В. Точные штрафы в задаче оценки координат динамической системы в условиях неопределенности	40
Костюнин С. Ю., Шевкопляс Е. В. Об упрощении интегрального выигрыша в дифференциальных играх со случайной продолжительностью	47
Мирошин Р. Н. Класс не чебышевских систем функций, допускающий использование теоремы Маркова в конечной проблеме моментов	57
Muxeeв В. С. Шуровская рациональная аппроксимация шуровских функций	63
Новоселов В. С. К имитационному моделированию нервного импульса	73
ИНФОРМАТИКА	
Молдовян Д. Н., Молдовян Н. А. Особенности строения групп векторов и синтез	
криптографических схем на их основе	84
Раба Н. О. Разработка и реализация алгоритма расчета коагуляции в модели облаков со смешанной фазой с использованием технологии CUDA	94



© Авторы статей

© Издательство Санкт-Петербургского университета, 2011

Яхонтов С. В. Эффективное по времени и по памяти вычисление экспоненциальной функции комплексного аргумента на машине Шёнхаге	105
ПРОЦЕССЫ УПРАВЛЕНИЯ	
	119
АННОТАЦИИ	133
SUMMARIES	137
ОТ РЕДАКЦИИ	
Конференция «Процессы управления и устойчивость»	140
ПЕРЕЧЕНЬ СТАТЕЙ	141

#### УДК 517.925.51

Александров А.Ю. Исследование устойчивости решений одного класса сложных систем // Вестн. С.-Петерб. ун-та. Сер. 10. 2011. Вып. 4. С. 3–13.

Рассматривается сложная система, состоящая из двух взаимодействующих подсистем. Предполагается, что одна из подсистем описывается векторным уравнением Льенара и имеет асимптотически устойчивое нулевое решение. Сложная система такого рода может быть получена при анализе устойчивости в критическом случае нескольких нулевых корней или в критическом случае нескольких чисто мнимых корней. Она также может описывать взаимодействие двух механических систем, одна из которых находится под действием существенно нелинейных диссипативных и потенциальных сил. С помощью метода векторных функций Ляпунова найдены достаточные условия асимптотической устойчивости нулевого решения сложной системы относительно части переменных. Полученный результат представляет собой распространение теоремы Ляпунова-Малкина на случай существенно нелинейных подсистем. Далее изучаются условия асимптотической устойчивости нулевого решения по отношению ко всем переменным. Сначала для сложной системы строится семейство функций Ляпунова. Затем решается проблема выбора оптимальной функции Ляпунова из построенного семейства, которая задает наибольшую область асимптотической устойчивости в пространстве параметров рассматриваемой системы. Кроме того, с помощью метода дифференциальных неравенств получены оценки времени переходных процессов в сложной системе. Библиогр. 22 назв.

*Ключевые слова*: сложные системы, устойчивость, функции Ляпунова, дифференциальные неравенства, декомпозиция.

#### УДК 621.317.329; 537.533.79; 519.688

Иванов В. Я. Численное моделирование быстрых фотодетекторов большой площади // Вестн. С.-Петерб. ун-та. Сер. 10. 2011. Вып. 4. С. 14–31.

Дан обзор современных достижений в области моделирования и экспериментальных исследований микроканальных усилителей для различных областей применений. Приведено описание полуаналитических, численных моделей и программы MCS (Monte Carlo Simulator) для расчетов фотодетекторов пикосекундного разрешения в трехмерном приближении. Эти модели включают моделирование свойств микроканальных усилителей, новых перспективных материалов и технологий для многослойных покрытий в микроканальных пластинах. Библиогр. 74 назв. Ил. 17.

Kлючевые слова: фотодетектор, микроканальная пластина, моделирование, методы Монте Карло.

#### УДК 517.925.42

Камачкин А. М. О строении окрестности кусочно-гладкой орбиты // Вестн. С.-Петерб. ун-та. Сер. 10. 2011. Вып. 4. С. 32–39.

Предложена модификация метода В. И. Зубова построения специальной системы координат вдоль гладкой орбиты для случая кусочно-гладкой орбиты. Это позволяет строить непрерывную вдоль траектории функцию Ляпунова для исследования окрестности кусочно-гладкой орбиты. Рассмотрен пример исследования периодического решения системы с релейным гистерезисом. Библиогр. 16 назв.

*Ключевые слова*: устойчивость, кусочно-гладкая орбита, окрестность периодического решения.

#### УДК 539.3

Карелин В.В. Точные штрафы в задаче оценки координат динамической системы в условиях неопределенности // Вестн. С.-Петерб. ун-та. Сер. 10. 2011. Вып. 4. С. 40–46.

Проблеме учета ограничений в задачах математического программирования было уделено много внимания. Во многих случаях ее решали с помощью штрафных функций. В настоящее время идея точных штрафов хорошо разработана и широко используется. Подход, основанный на точном штрафе, наиболее интересен и изящен, но он приводит к необходимости решать негладкую задачу оптимизации, даже если исходная задача является гладкой. Однако прогресс в области численных методов недифференцируемой безусловной оптимизации, достигнутый в последние годы, дает некоторую надежду, что эти трудности будут преодолены. Ранее теория точных штрафов была применена к исследованию одного класса задач управления, в которых управления были просто параметрами системы дифференциальных уравнений, описывающей поведение некоторого управляемого объекта. В статье рассматривается задача наблюдения. Система дифференциальных уравнений считается ограничениями. Показано, как можно их убрать, вводя соответствующую штрафную функцию. Получающийся новый функционал – существенно негладкий, тем не менее он обладает интересными дифференциальными свойствами, и современные методы недифференцируемой оптимизации позволяют решать указанные задачи численно. Библиогр. 4 назв.

*Ключевые слова*: наблюдаемость, дифференциальные уравнения, штрафные функции, недифференцируемая оптимизация, управление.

#### УДК 517.977.8+517.977.5

Костюнин С.Ю., Шевкопляс Е.В. **Об** упрощении интегрального выигрыша в дифференциальных играх со случайной продолжительностью // Вестн. С.-Петерб. vn-та. Сер. 10. 2011. Вып. 4. С. 47–56.

В статье рассматривается класс дифференциальных игр со случайной продолжительностью. Формулируются условия, при выполнении которых интегральный функционал, представляющий собой математическое ожидание выигрыша игрока, может быть упрощен путем перестановки интегралов. Теоретические результаты иллюстрируются на примере дифференциальной игры управления вредными выбросами. Библиогр. 12 назв.

*Ключевые слова*: дифференциальные игры, интегральный выигрыш, случайная продолжительность, дифференциальная игра управления вредными выбросами.

#### УДК 517.5

Мирошин Р.Н. Класс не чебышевских систем функций, допускающий использование теоремы Маркова в конечной проблеме моментов // Вестн. С.-Петерб. ун-та. Сер. 10. 2011. Вып. 4. С. 57–62.

Указанный в заголовке класс образован степенями одновершинной непрерывной функции, несколько последовательных степеней левой ветви которой на соответствующем интервале ее определения есть чебышевская система. Оказывается, максимум и минимум определенного интеграла от некоторой неизвестной функции можно получить с помощью теоремы Маркова, в которой веса и узлы найдены только по этой левой ветви. Необходимость в таких оценках возникает естественным образом из простейшей задачи нелинейной динамики типа итераций одновершинной функции с неизвестным распределением начального значения и известными ее степенными моментами при следующем шаге итерации. Библиогр. 7 назв.

Ключевые слова: проблема моментов, чебышевская система функций, теорема Маркова.

Михеев В.С. **Шуровская рациональная аппроксимация шуровских функций** // Вестн. С.-Петерб. ун-та. Сер. 10. 2011. Вып. 4. С. 63–72.

Исследуется задача аппроксимации элемента из  $H_2^+$  – класса аналитических функций на замкнутом единичном круге U, принимающих только вещественные значения на сегменте [0,1], элементом из  $\mathcal{H}_n^+$  – класса неприводимых вещественных рациональных функций, со степенями числителя и знаменателя, не превосходящих n. Доказано, что если  $f \in H_2^+$  и  $f \notin \mathcal{H}_k^+$ , где k < n, то любой локальный минимайзер нелинейной программы  $\|f - g\|^2 \longrightarrow \min_{n \in \mathcal{H}_k^+}$  не принадлежит

 $\mathcal{H}_m^+$ , где m < n. Этот результат переносится на класс  $S^+$  шуровских функций, выделяемый из  $H_2^+$  условием  $\sup_{z \in U} |f(z)| \leqslant 1$ . Если  $\mathcal{S}_n^+$  есть шуровский подкласс класса  $\mathcal{H}_n^+$ , то доказано, что при  $f \in S^+$  и  $f \notin \mathcal{S}_k^+$ , где k < n, любой локальный минимайзер нелинейной программы  $\|f-g\|^2 \longrightarrow \min_{g \in \mathcal{S}_n^+}$  не принадлежит  $\mathcal{S}_m^+$ , где m < n. Библиогр. 6 назв.

Kлючевые слова: единичный круг, шуровские функции, аппроксимация, рациональные функции, алгоритм Шура.

#### УДК 531:518:577

Новоселов В.С. **К** имитационному моделированию нервного импульса // Вестн. С.-Петерб. ун-та. Сер. 10. 2011. Вып. 4. С. 73–83.

В статье рассматривается соединение ионно-возбудимой мембраны с нелинейным диффузионным процессом, это может производить перемещение нелинейной волны электрического возбуждения. Фундаментальным уравнением при описании распространения нелинейных волн для одномерного случая в слабо дисперсионной среде является уравнение Кортевега-де Фриса (KdV), решения которого имеют структуру стабильных уединенных волн, т. е. солитонов. Бегущий импульс (то же самое солитонный импульс) есть частицеподобное решение определяющих уравнений, сохраняющее от начала до конца свою форму. Мы приходим к уравнению KdV прямо от уравнений нейродинамики (при распространении активного потенциала вдоль аксона нерва). Уравнение KdV показывает, что активный потенциал должен распространяться с фиксированной скоростью, которая должна быть вычислена. При изучении бегущих волн вводится специальная фазовая координата бегущей волны  $\xi = x - vt$ , где  $v = \mathrm{const} > 0$  есть скорость волны. Благодаря применению координаты бегущей волны, дифференциальные уравнения в частных производных становятся обыкновенными дифференциальными уравнениями. Для представления о структуре бегущей импульсной волны полезно рассмотрение решений в виде бегущего импульса простейшего кусочно-линейного уравнения с тремя или четырьмя участками. На каждом участке дифференциальные уравнения являются линейными, и решения строятся аналитически. Решения на участках непрерывно стыкуются в точках  $u=u_{\pi}$  и  $u = u_{\max}$ . Переменная u есть мембранный потенциал. Понимание структуры бегущего импульса для сердечной мышцы дает прежде всего изучение решения в виде бегущей волны кусочнолинейного уравнения модели ФитцХью-Нагумо. Представление о структуре бегущего импульса в немиелинированном нервном волокне можно получить при изучении бегущего импульса решения кусочно-линейного уравнения в модели Ходжкина-Хаксли. В статье рассмотрены три кусочно-линейные модели. Решения кусочно-линейных уравнений дают начальные приближения. После этого бегущие импульсы уравнений ФитцХью-Нагумо и Ходжкина-Хаксли можно получить численным вычислением. Библиогр. 21 назв.

*Ключевые слова*: солитон, длинноволновое уравнение, бегущий нервный импульс, активный потенциал, кусочно-линейная модель.

#### УДК 681.3

Молдовян Д.Н., Молдовян Н.А. **Особенности строения групп векторов и синтез криптографических схем на их основе** // Вестн. С.-Петерб. ун-та. Сер. 10. 2011. Вып. 4. С. 84–93.

Показана перспективность задачи дискретного логарифмирования (ЗДЛ) по многомерному основанию, формулируемой над примарными подгруппами с многомерной цикличностью, и ЗДЛ в скрытой коммутативной подгруппе, формулируемой над конечными некоммутативными группами, для повышения производительности алгоритмов аутентификации информации, коммутативного шифрования и протоколов открытого распределения ключей. Задание конечных групп с требуемыми свойствами выполнено над конечными векторными пространствами. Библиогр. 13 назв. Табл. 2.

*Ключевые слова*: электронная цифровая подпись, задача дискретного логарифмирования, коммутативное шифрование, конечная группа, некоммутативная группа, группа векторов, многомерная цикличность.

#### УДК 004.272.23+519.681.3

Pa6a H. O. Разработка и реализация алгоритма расчета коагуляции в модели облаков со смешанной фазой с использованием технологии CUDA // Вестн. С.-Петерб. ун-та. Сер. 10. 2011. Вып. 4. С. 94–104.

К наиболее эффективным инструментам изучения конвективных облаков относится численное моделирование. Для увеличения точности прогноза желательно использовать модели со спектральным описанием микрофизических процессов со смешанной фазой (жидкой и ледяной). При применении таких моделей основная часть компьютерных ресурсов тратится на вычисление микрофизических процессов и в особенности процесса коагуляции. Одним из способов ускорения расчетов являются параллельные вычисления. Современные процессоры для обычных ПК имеют от 2 до 6 ядер, в отличие от видеокарт с несколькими сотнями ядер. Для распараллеливания на такое большое количество ядер требуются специальные алгоритмы. В настоящей статье описан алгоритм расчета коагуляции для модели со смешанной фазой. Представлен способ распараллеливания этого алгоритма для расчета на видеокарте с помощью технологии CUDA. Охарактеризован метод, позволяющий избежать одновременного (параллельного) обращения к ячейкам памяти из разных потоков. Приведенные результаты тестирования показывают существенное увеличение скорости расчета коагуляции. Библиогр. 7 назв. Ил. 3.

Kлючевые слова: параллельные вычисления, CUDA, GPGPU, коагуляция, спектральная микрофизика.

#### УДК 519.688+510.52

Яхонтов С.В. Эффективное по времени и по памяти вычисление экспоненциальной функции комплексного аргумента на машине Шёнхаге // Вестн. С.-Петерб. ун-та. Сер. 10. 2011. Вып. 4. С. 105–118.

Для построения конструктивного аналога комплексной экспоненциальной функции применяется модель вычислимых функций, основанная на понятии машины Шёнхаге с оракульной функцией. Вычисление комплексной экспоненциальной функции с помощью простых преобразований сводится к расчету вещественной экспоненциальной функции. Далее приближенные значения вещественной экспоненциальной функции рассчитываются на основе разложения в ряд Тейлора с помощью модифицированного алгоритма быстрого вычисления экспоненты ModFEE, который, в свою очередь, использует модифицированный алгоритм двочичного деления ModBinSplit для гипергеометрических рядов. Для алгоритмов ModBinSplit, ModFEE и основного алгоритма ExpValue показывается квазилинейность по времени и линейность по памяти. Библиогр. 7 назв.

Kлючевые слова: экспоненциальная функция, конструктивные вещественные функции, квазилинейная временная сложность, линейная емкостная сложность.

 $\mathbb{H}$ енников А.В. Принцип включения и устойчивоподобные свойства «частичного» положения равновесия динамической системы // Вестн. С.-Петерб. ун-та. Сер. 10. 2011. Вып. 4. С. 119–132.

Во многих приложениях динамические математические модели содержат подсистемы, обладающие общими частями. В указанных случаях прибегают к расширению фазового пространства исходной динамической системы с последующим его сужением до размеров фазового пространства исходной системы. Расширение фазового пространства приводит исходную динамическую систему к системе, у которой у всех подсистем нет общих частей. При этом рассматриваемые динамические системы могут иметь положения равновесия в классическом понимании, а также так называемые «частичные» положения равновесия. Для реализации процесса расширения-сужения необходимо знать условия, при выполнении которых это возможно осуществлять. Указанные условия составляют основу принципа включения. В данной работе найдены условия, при выполнении которых удается проводить изучение устойчивоподобных свойств «частичного» положения равновесия динамической системы, заданной в виде системы нелинейных обыкновенных дифференциальных уравнений, относительно всех и части фазовых переменных с использованием принципа включения. На примере системы дифференциальных уравнений с однородной правой частью порядка  $\mu = 3, 5, \dots$  продемонстрирована техника исследования устойчивоподобных свойств ее движений с применением идей и методов принципа включения. Приведен пример системы, для которой не удается доказать асимптотическую устойчивость без использования принципа включения. Библиогр. 16 назв.

Kлючевые слова: динамические системы, принцип включения, перекрывающиеся декомпозиции, устойчивость, однородные системы.

#### SUMMARIES

Aleksandrov A. Yu. Investigation of sulutions stability for a class of complex systems // Vestnik St. Petersburg University. Ser. 10. 2011. Issue 4. P. 3–13.

A complex system composed of two interacting subsystems is considered. It is assumed that one of subsystems is described by the vector Lienard equation and possesses the asymptotically stable zero solution. Such complex system can be obtained under stability analysis in the critical case of several zero roots or in the critical case of several pure imaginary roots. It can also describe interaction of two mechanical systems one of which is exposed essentially nonlinear dissipative and potential forces. By the use of Lyapunov vector functions method the sufficient conditions of asymptotic stability with respect to a part of variables for zero solution of a complex system are determined. The result obtained is an extension of the Lyapunov–Malkin theorem on the case of essentially nonlinear subsystems. Furthermore, the conditions of asymptotic stability of zero solution with respect to all variables are studied. At first, the family of Lyapunov functions for the complex system is constructed. After that the problem of choosing an optimal function from the family constructed is solved. This optimal Lyapunov function gives us the largest asymptotic stability region in the space of parameters of the system considered. Moreover, using a differential inequalities method, the estimates of transient processes time in the complex system are obtained.

Key words: complex systems, stability, the Lyapunov functions, differential inequalities, decomposition.

Ivanov V. Ya. Numerical simulation of large-area fast photodetectors // Vestnik St. Petersburg University. Ser. 10. 2011. Issue 4. P. 14–31.

Many complex physical effects (fringe fields, saturation, emission properties of compaund materials and space charge relaxation) have been taken into account in modeling a new generation of photodetectors based on micro channel plates. The results of numerical simulations have good agreement with experimental data and publication of other authors.

Key words: photodetector, microchannel plate, modeling, Monte Catlo methods.

Kamachkin A. M. On construction of the piecewise-smooth orbit neighborhood // Vestnik St. Petersburg University. Ser. 10. 2011. Issue 4. P. 32–39.

Under consideration there is the modification of the Zubov's method of construction of special coordinate system along the smooth orbit for the piecewise-smooth case. This modification allows

constructing the Lyapunov smooth function along the trajectory for the research into the periodical solution of the relay hysteresis system.

Key words: stability, piecewise-smooth orbit, neighborhood of periodic solution.

Karelin V. V. Exact penalties functions in the problem of estimating the coordinates of the dynamical system under uncertainty // Vestnik St. Petersburg University. Ser. 10. 2011. Issue 4. P. 40–46.

The problem of reducing a constrained mathematical programming problem to an unconstrained one has been given a great deal of attention. In most cases such a reduction is performed with the help of so-called penalty functions. At present the theory of Penalization is well developed and widely used. The exact penalization approach is most interesting and elegant but it generally requires solving a nonsmooth problem even if the original one was smooth. However, recent developments in Nondifferentiable Optimization give some hope that these difficulties will be overcome. To be able to reduce a constrained optimization problem to an unconstrained one via exact penalization it is suitable to represent the constraining set in the form of equality, where the function describing the set must satisfy some conditions on its directional derivatives (or, in general, on its generalized directional derivatives). In the present paper we show how to describe the constraints – given in the form of differential equations – by a (nonsmooth) functional whose directional derivatives satisfy the required properties. We treat one parametric optimization problem. This problem is reduced to a nonsmooth unconstrained optimization problem. It makes it possible to construct a numerical algorithm for the unconstrained optimization problem. It makes it possible to construct a numerical algorithm for the unconstrained optimization problem just allowing one to solve the original parametric optimization problem. Then, by making use of necessary optimality conditions (for a nonsmooth problem) it is shown that the conditions we obtain are equivalent to the well-known ones.

Key words: observability, the differential equations, penal functions, not differentiated optimization, management.

Kostyunin S. Yu., Shevkoplyas E. V. On simplification of integral payoff in differential games with random duration // Vestnik St. Petersburg University. Ser. 10. 2011. Issue 4. P. 47–56.

A class of differential games with random duration is considered. Conditions for simplification of mathematical expectation of the player's integral payoff are given. Theoretical results are illustrated with the example of a differential game of pollution control.

Key words: differential games, integral payoff, random duration, differential game of pollution control.

Miroshin R. N. On a class of nonChebyshev function systems allowing to use Markov theorem in the finite moment problem // Vestnik St. Petersburg University. Ser. 10. 2011. Issue 4. P. 57-62.

The class indicated in the header is formed by degrees of a unimodal continuous function, whose several successive powers of the left branch on the corresponding interval of its definition is Chebyshev system. It turns out that both maximum and minimum of a specific integral with some unknown function can be obtained using the Markov theorem in which the weights and nodes are found only with the help of the left branch. The need for such estimates naturally arises from the simplest problem of nonlinear dynamics such as iterations of a unimodal function with unknown distribution of the initial value and its known polynomial moments of the next iteration step.

Key words: moment problem, Chebyshev system of function, Markov theorem.

Mikheev V. S. Schur's rational approximation of Schur's functions // Vestnik St. Petersburg University. Ser. 10. 2011. Issue 4. P. 63–72.

The problem of approximating elements from the class  $H_2^+$  of the analytic functions in the closed unit disk U assuming only real values on the segment [0,1] is investigated. As approximant class is taken to be  $\mathcal{H}_n^+$  which is the class of irreducible real rational functions with the degrees of a numerator and a denominator not greater n. It is proved that if  $f \in H_2^+$  and  $f \notin \mathcal{H}_n^+$  where k < n then any local minimizer of nonlinear programme  $\|f - g\|^2 \longrightarrow \min_{g \in \mathcal{H}_n^+}$  does not belong to  $\mathcal{H}_m^+$ , where m < n. The result is expanded to the class

 $S^+$  of Schur's functions selected from  $H_2^+$  by the condition  $\sup_{z \in U} |f(z)| \leq 1$ . If  $\mathcal{S}_n^+$  is a Schur's subclass of  $\mathcal{H}_n^+$  then it is proved that, when  $f \in S^+$  and  $f \notin \mathcal{S}_k^+$ , where k < n, any local minimizer of non linear programme  $\|f - g\|^2 \longrightarrow \min_{g \in \mathcal{S}_n^+}$  does not belong to  $\mathcal{S}_m^+$ , where m < n.

Key words: unit disk, Schur's function, approximation, rational function, Schur's algorithm.

Novoselov V. S. On simulation modelling of nerve impulse // Vestnik St. Petersburg University. Ser. 10, 2011. Issue 4, P. 73–83.

It is shown that when an ionic excitable membrane is incorporated into a nonlinear diffusion process, it can give rise to travelling nonlinear waves of electrical excitation. The fundamental equation describing the propagation of nonlinear waves in a one-dimensional case in medium weakly dispersion is the Kortewegde Vries equation (KdV), with solution as stable solitary wave structures, i. e. solitons. A travelling pulse (often called a solitary pulse) is a travelling wave solution that starts and ends at the same steady state of the governing equations. We derive the KdV equation from the full set of neurodynamic equations (for the propagation of action potential along the axon of a nerve). The showed KdV equation indicated that this action potential should propagate along an axon with fixed velocity, which could be calculated. To study travelling waves define the travelling wave coordinate  $\xi = x - vt$ , where v = const > 0 is the wave velocity. Because of application of the travelling coordinate the partial differential equations become the ordinary differential equations. To understand the structure of a travelling pulse it is helpful to study travelling pulse solution in the partial piecewise linear equation mit three or four regions. In each region the differential equation is linear and can be analytically solved. The regional solutions are then joined at  $u = u_{\pi}$ , and  $u = u_{\text{max}}$  by stipulating. The variable u is a membrane potential. To understand the structure of a travelling pulse for the cardiac muscle it is helpful first to study travelling pulse solution piecewise linear equation in the FitzHugh-Nagumo model. To understand the structure of a travelling pulse for the nonmyelinated nerve fibers it is helpful to study travelling pulse solution of a piecewise linear equation in the Hodgkin-Huxley model. In this article three piecewise linear models are examined. The solutions of piecewise linear equations give initial approximations. Here upon the travelling pulses of the FitzHugh-Nagumo and Hodgkin-Huxley equations can be numerically computed.

Key words: soliton, wave equation of long waves, travelling nerve pulse, action potential, piecewise linear model.

Moldovyan D. N., Moldovyan N. A. Structure peculiarities of the finite vector groups and their use in the cryptoscheme design // Vestnik St. Petersburg University. Ser. 10. 2011. Issue 4. P. 84–93.

Its is shown that problem of finding discrete logarithm to the multi-dimension base is an attractive primitive for designing fast signature schemes using computations in the finite vector groups. Other introduced primitive called problem of finding discrete logarithm in a hidden cyclic subgroup of the finite non-commutative group represents interest for designing fast public key agreement protocols and commutative encryption algorithms. For implementing such cryptoschemes finite non-commutative groups of four dimension vectors are proposed.

Key words: digital signature, discrete logarithm problem, commutative encryption, finite group, non-commutative group, vector group, multidimension cyclicity.

# $\it Raba~N.~O.~$ Development and realization of algorithm of coagulation calculation in mixed-phase cloud model using CUDA technology // Vestnik St. Petersburg University. Ser. 10. 2011. Issue 4. P. 94-104.

Numerical modeling is one of the most effective way to investigate convective clouds. Mixed-phase cloud models with spectral microphysics are usually applied for more accurate forecast. Computer resources are mainly spent on microphysical processes calculations (especially on coagulation process). One of the methods of computations speed-up is parallel computing. Modern central processors have only 2–6 cores in contrast to a few hundreds of cores in video cards. Special parallel algorithms are required for such numbers of cores. In the paper a coagulation calculation algorithm for a mixed-phase cloud model is described. This algorithm is modified version of the algorithm for liquid phase cloud model. A method of parallelization of this algorithm for computation on video card using CUDA technology is also proposed. A way of avoid simultaneous access to memory cells from different threads is demonstrated. The testing shows significant speeding-up of coagulation calculation.

Key words: parallel computing, CUDA, GPGPU, coagulation, coalescence, spectral microphysics.

# $Yakhontov\ S.\ V.$ Time- and space-efficient evaluation of a complex exponential function on machine Schonhage // Vestnik St. Petersburg University. Ser. 10. 2011. Issue 4. P. 105–118.

Quasi-linear time and linear space algorithms for evaluation of a complex exponential function on machine Schonhage are presented. These algorithms are based on a modified method of fast evaluation of an exponential function and on a modified method of binary splitting for hypergeometris series.

Key words: exponential function, constructive real functions, quasi-linear time complexity, linear space complexity.

Shchennicov A. V. Inclusion principle and stability-like properties of "partial" equilibrium position of a dynamical system // Vestnik St. Petersburg University. Ser. 10. 2011. Issue 4. P. 119–132.

In numerous applications, dynamical mathematical models contain subsystems with common parts. In such cases, the extension of phase space of the studied system is used. This extension transforms an initial dynamical system to a system whose subsystems have no common parts. The considered dynamical systems can possess both equilibrium positions in the classical sense and so-called "partial" equilibrium positions. After investigation stability of extended systems equilibrium positions the obtained results are transferred to the initial system by means of phase space constriction. The important problem is that one of determinating conditions under which the realization of the extension-constriction process is possible. These conditions compose the basis of the inclusion principle. In the present paper the stability-like properties with respect to all or to a part of variables of a "partial" equilibrium position of a differential equations system are studied. The conditions are obtained under which these properties can be investigated by the use of the inclusion principle. On the example of the differential equations system with homogeneous right-hand sides of the order  $\mu=3,5,\ldots$  the technique of the inclusion principle application for the analysis of stability-like properties is demonstrated. The example of the system for which we failed to prove the asymptotic stability without using the inclusion principle is given.

 $\label{eq:Keywords} \textit{Key words} : \textit{dynamical systems}, \textit{inclusion principle}, \textit{overlapping decompositions}, \textit{stability}, \textit{homogeneous systems}.$ 

#### ОТ РЕДАКЦИИ

# КОНФЕРЕНЦИЯ «ПРОЦЕССЫ УПРАВЛЕНИЯ И УСТОЙЧИВОСТЬ»

С 4 по 7 апреля 2011 г. на факультете прикладной математики—процессов управления (ПМ–ПУ) Санкт-Петербургского государственного университета состоялась XLII ежегодная Международная научная конференция аспирантов и студентов «Процессы управления и устойчивость», "Control Processes and Stability" (CPS'11).

К участию в конференции было подано 122 заявки от студентов, аспирантов, преподавателей факультета ПМ–ПУ, других факультетов СПбГУ, а также университетов Беларуси, Италии, Китая, России и Японии.

На открытии конференции выступил проф. E.~U.~Bеремей с докладом «Современные компьютерные технологии в процессах управления».

Работа конференции проходила по пяти секциям:

секция № 1: Математическая теория процессов управления (председатель – проф. А. П. Жабко); секция № 2: Математические методы в механике и физике (председатель – проф. О. И. Дривотин);

секция N 3: *Математические модели медико-биологических систем* (председатель - доц. Е. Д. Котина);

секция № 4: Информационные и компьютерные технологии (председатели – доценты С. Л. Сергеев и А. Н. Кривцов);

секция № 5: *Управление социально-экономическими системами* (председатели – профессора А. Ю. Гарнаев и В. Д. Ногин).

По результатам работы конференции издан сборник, в который включены полные тексты докладов, сделанных на конференции и рекомендованных к публикации: **Процессы управления и устойчивость**: Труды 42-й Международной научной конференции аспирантов и студентов. Россия, СПб.: 4–7 апреля 2011 г. / под ред. А. С. Ерёмина, Н. В. Смирнова. СПб.: Издат. Дом С.-Петерб. ун-та, 2011. 588 с.

Со 2 по 5 апреля 2012 г. на факультете ПМ–ПУ СПбГУ состоится 43-я Международная научная конференция аспирантов и студентов «Процессы управления и устойчивость», "Control Processes and Stability" (CPS'12). Информация о конференции будет размещена на сайте факультета http://www.apmath.spbu.ru в феврале 2012 г. Мы будем рады видеть Вас в составе участников нашей научной конференции.

Подробная информация о правилах предоставления статей и порядке их рецензирования приведена в выпусках журнала за 2009 г., в вып. 1 за 2010 г. и на сайте факультета ПМ–ПУ (e-mail: vkarelin@apmath.spbu.ru).

# ПЕРЕЧЕНЬ СТАТЕЙ, ОПУБЛИКОВАННЫХ В ЖУРНАЛЕ «ВЕСТНИК САНКТ-ПЕТЕРБУРГСКОГО УНИВЕРСИТЕТА» В 2011 ГОДУ. СЕРИЯ 10: ПРИКЛАДНАЯ МАТЕМАТИКА,

ИНФОРМАТИКА, ПРОЦЕССЫ УПРАВЛЕНИЯ

#### Прикладная математика

Аббасов М. Э. Условия экстремума в терминах несобственных экзостеров	2	3-8
Александров А. Ю. Исследование устойчивости решений одного класса сложных систем Ананьев К. И., Демьянова В. В., Демьянов В. Ф., Кокорина А. В., Свиступ С. Я., Сте-	4	3-13
галин И. С. Оптимизационные методы в задачах диагностики	3	3-12
Баринов В. А., Басинский К. Ю. Решение нелинейной задачи о волнах на поверхности слабовязкой жидкости	2	9-16
Бедрина М. Е., Егоров Н. В., Куранов Д. Ю., Семенов С. Г. Расчет фталоцианинатов		10.01
цинка на высокопроизводительном вычислительном комплексе	3	13–21
Буре В. М., Сергеева А. А. Конкуренция двух фирм на рынке логистических перевозок	3	22–28
Веремей Е. И. Среднеквадратичный синтез цифровых систем методами <i>Н</i> -теории Ейбожсенко Д. А. Алгоритм <i>k</i> -кластерной оптимизации для задачи Штейнера на ори-	2	17–28
ентированных графах Ехменина И. В., Шешин Е. П., Чадаев Н. Н. Автоэмиссионный источник ультрафиоле-	2	29–39
тового излучения с автокатодом из наноструктурированного углеродного материала Жабко А. П., Зараник У. П. О приближении решений экспоненциально устойчивых	1	3-8
систем дифференциально-разностных уравнений	3	29–38
Жабко А. П., Медведева И. В. Алгебраический подход к анализу устойчивости дифференциально-разностных систем	1	9-20
Золотухин М. А., Гарнаев А. Ю., Захаров В. В. Передача данных при утечке инфор-	0	40.54
мации Иголкин В. Н. Вычисление некоторых характеристик неразорения страховой компании	2	40–54
с помощью модели Лундберга	3	39–46
Иванов В. Я. Численное моделирование быстрых фотодетекторов большой площади Kawata S., Takahashi K., Sato D., Barada D., Andreev A. A., Klimo O., Limpouch J., Ma Y. Y., Sheng Z. M., Wang W. M., Li Y. T., Kong Q., Wang P. X. Efficient ion beam generation in laser foil interaction – toward a controllable laser ion accelerator	1	14–31 21–28
Камачкин А. М. О строении окрестности кусочно-гладкой орбиты	4	32–39
Карелин В. В. Точные штрафы в задаче оценки координат динамической системы в условиях неопределенности	4	40–46
Костюнин С. Ю., Шевкопляс Е. В. Об упрощении интегрального выигрыша в диффе-	4	40 40
ренциальных играх со случайной продолжительностью	4	47–56
ных радионуклидных исследованиях	1	29–36
ных радиопуклидных исследованиях  Курбатова Г. И., Попова Е. А. О различных математических моделях транспортировки газа по трубопроводам	3	47–55
Мальков В. М., Кабриц С. А., Мансурова С. Е. Математическое моделирование нели-		
нейной деформации эластомерного слоя	3	56–63
теоремы Маркова в конечной проблеме моментов	4	57-62
Muxeeв В. С. Шуровская рациональная аппроксимация шуровских функций	4	63 - 72
Новоселов В. С. К имитационному моделированию нервного импульса	4	73–83
ний в среде MapReduce	2	55-66

Полякова Л. Н. Гиподифференциал и $\varepsilon$ -субдифференциал полиэдральной функции Senichev Yu. V., Chechenin A. N., Kostromin S. A. Variable transition energy lattices based	3	64-71
on different periodic cells with various types of dispersion suppressor	1	37–48 49–59
Терешонков Ю. В., Андрианов С. Н., Jakšić Milko, Pastuović Želiko, Tadić Tonči. Математическое моделирование ионных микрозондов с учетом краевых полей	1	60–75
Информатика		
Агеев М. С., Добров Б. В. Метод эффективного расчета матрицы ближайших соседей		
для полнотекстовых документов	3	72-84
$Apcenmьeвa\ E.\ \Pi.$ Об измельчении триангуляции вблизи границы области	1	76–84
граммируемой логической интегральной схемы	3	85–99
для исследования структуры тонких пленок	2	76–80
Кознов Д. В. О спецификации диаграммных преобразований в графических редакторах Кознов Д. В., Смирнов М. Н., Дорохов В. А., Романовский К. Ю. WebMLDoc: подход к автоматизированному отслеживанию изменений в пользовательской документации	3	100–111
Web-приложений	3	112–126
Мишенин А. Н. Тематическая сегментация семантически однородных документов Молдовян Д. Н., Молдовян Н. А. Особенности строения групп векторов и синтез крип-	3	127–133
тографических схем на их основе	4	84–93
ния для разработки Web-приложений в системе Aspect.NET	1	85–105
со смешанной фазой с использованием технологии CUDA $Pa\ddot{u}\kappa$ $A.~B.,~Bedpuna~M.~E.$ Моделирование процесса адсорбции воды на поверхности	4	94–104
кристаллов	2	67–75
функции комплексного аргумента на машине Шёнхаге	4	105–114
Процессы управления		
Aлександров $A$ . $H$ 0., $H$ 0. $H$		
с нелинейными поглотителями энергии	1	106-115
катор в задаче многопрограммной стабилизации	2	81–89
Веремей Е. И., Сотникова М. В. Стабилизация плазмы на базе прогноза с устойчивым линейным приближением	1	116-133
трубками дрейфа на малую энергию	1	134–141
с распределенными и сосредоточенными параметрами в точке соединения <i>Нгуен Динь Хуен</i> . Условия конвергенции некоторых классов нелинейных разностных	1	142–146
систем	2	90–96
ложения равновесия динамической системы	4	119–131
Хроника		
Л. А. Петросян (к 70-летию со дня рождения и 50-летию научной деятельности		
в Ленинградском-Санкт-Петербургском государственном университете)	1	147 - 149
Камачкия А. М. Балакина А. А. Т. Таппыкин (к. 100-летию солия рожления)	1	150-151

Петросян Л. А., Покровский А. Н., Демьянов В. Ф., Зубова А. Ф., Зубов А. В., Зубов С. В., Зубов И. В., Блистанова Л. Д., Жабко А. П., Квитко А. Н., Стрекопытова М. В., Малафеев О. А., Мутлу О. В., Чижова О. Н., Прасолов А. В.,		
Иванов А. И., Вахнина Л. А., Зубов А. И., Зубов В. И., Клемина А. А., Кольцов И. В., Кольцова Н. И., Кудинова В. А., Стрельцова Е. В., Шастин Э. Г., Кондратьева С. И. Памяти Н. В. Зубова	2	97
Рефераты	1	152 - 155
	2	98-100
	3	134-138
	4	133–137
Summaries	1	156-159
	2	101-103
	3	139-141
	4	137–140
От редакции		
Конференция «Процессы управления и устойчивость»	4	140

# CONTENTS

## APPLIED MATHEMATICS

Aleksandrov A. Yu. Investigation of sulutions stability for a class of complex systems	3
Ivanov V. Ya. Numerical simulation of large-area fast photodetectors	14
Kamachkin A. M. On construction of the piecewise-smooth orbit neighborhood  Karelin V. V. Exact penalties functions in the problem of estimating the coordinates	32
of the dynamical system under uncertainty	40
Kostyunin S. Yu., Shevkoplyas E. V. On simplification of integral payoff in differential games with random duration	47
Miroshin R. N. On a class of nonChebyshev function systems allowing to use Markov theorem in the finite moment problem	57
Mikheev V. S. Schur's rational approximation of Schur's functions	63
Novoselov V. S. On simulation modelling of nerve impulse	73
INFORMATICS	
Moldovyan D. N., Moldovyan N. A. Structure peculiarities of the finite vector groups and their use in the cryptoscheme design	84
Raba N. O. Development and realization of algorithm of coagulation calculation in mixed-phase cloud model using CUDA technology	94
Yakhontov S. V. Time- and space-efficient evaluation of a complex exponential function on machine Schonhage	105
CONTROL PROCESSES	
Shchennicov A. V. Inclusion principle and stability-like properties of "partial" equilibrium position of a dynamical system	119
ANNOTATIONS	133
SUMMARIES	137
FROM EDITORIAL STAFF	
Conference "Control Process and Stability"	140
LIST OF ARTICLES	141