

**Національна академія наук України
Інститут кібернетики імені В.М. Глушкова**

**ПРАЦІ МІЖНАРОДНОЇ
МОЛОДІЖНОЇ МАТЕМАТИЧНОЇ ШКОЛИ**

**ПИТАННЯ ОПТИМІЗАЦІЇ ОБЧИСЛЕНЬ
(ПОО – XXXVII)**

Київ – 2011



***International Youth School of Mathematics
"The Issues of Calculation Optimization
(ISCOPT-XXXVII)"
September 2011, Katsyveli
The Southern Coast of the Crimea (Ukraine)***

Kyiv – 2011

Національна академія наук України
Інститут кібернетики імені В.М. Глушкова

ПРАЦІ МІЖНАРОДНОЇ
МОЛОДІЖНОЇ МАТЕМАТИЧНОЇ ШКОЛИ

ПИТАННЯ ОПТИМІЗАЦІЇ ОБЧИСЛЕНЬ
(ПОО – XXXVII)

Україна, Крим
Велика Ялта, смт. Кацивелі
22–29 вересня 2011 року

Праці школи

Київ – 2011

УДК 517:518:519:533:534

Праці міжнародної молодіжної математичної школи “Питання оптимізації обчислень (ПОО-XXXVII)” – Київ: Інститут кібернетики імені В.М. Глушкова НАН України, 2011. – 214 с.

Розглядаються питання побудови оптимальних за складністю (та близьких до них) алгоритмів розв’язання наступних класів задач обчислювальної та прикладної математики: цифрова обробка сигналів, відновлення функцій і функціоналів, розв’язування різних класів рівнянь, системний аналіз і математичне програмування, методи захисту інформації.

Відмінною рисою праць школи є їх спрямованість на побудову ефективних за різними критеріями алгоритмів, оцінок їх характеристик, порівняльний аналіз за цими характеристиками та розв’язання широкого спектра прикладних задач. Певна увага приділена комп’ютерній технології розв’язання задач прикладної та обчислювальної математики із заданими значеннями характеристик якості.

Збірник праць розрахований на спеціалістів у галузі обчислювальної та прикладної математики.

Редакційна колегія:

академік НАН України І.В. Сергієнко (відповідальний редактор), академік НАН України В.С. Дейнека, академік НАН України Ю.Г. Кривонос, член-кореспондент НАН України В.К. Задірака (заст. відповідального редактора), доктор фізико-математичних наук М.Д. Бабич (відповідальний секретар).

Рецензент: член-кореспондент НАН України А.О. Чикрій

ISBN 978-966-02-5965-2

© Інститут кібернетики
імені В.М. Глушкова НАН України, 2011

Гнатів Л.О. Метод побудови простих цілочисельних косинусних ступінчастих перетворень порядку 16 для високоефективного відеокодування.....	37
Гнатів Л.О., Луц В.К. Просте цілочисельне косинусне ступінчасте перетворення порядку 16 низької складності для високоефективного відеокодування.....	39
Горбенко Ю.І., Горбенко І.Д. Принципи створення, застосування та розвиток інфраструктури відкритих ключів, включаючи системи ЕЦП.....	41
Горбенко І.Д., Шапочка Н.В. Методи генерування псевдовипадкових послідовностей на основі спарювання точок еліптичних кривих та гешування.....	43
Грищенко О.Ю., Марцафей А.С., Федорова В.С. Різницева схема розщеплення, побудована на основі ДС-алгоритму	45
Гусак Д.В. Про наближення ймовірностей банкрутства.....	47
Дейнека В.С., Аралова А.А. Чисельна ідентифікація параметрів осесиметричних задач пружного та термопружного стану товстого циліндра	48
Долгов В.І., Неласа Г.В. Застосування криптографічних перетворень на гіпереліптичних кривих в алгоритмах асиметричної криптографії.....	50
Денисенко П.Н. Инструментальные средства для решения интегральных уравнений в системах компьютерной алгебры.....	52
Дудикевич В.Б., Гарасим Ю.Р. Вибір структури системи захисту інформації за показником її живучості	54
Emmenegger J.-F. Modeling the Prices of Securities on Financial Markets	56
Ємець О.О. Деякі властивості операції суми та лінійного порядку для нечітких чисел з дискретним носієм	58
Ємець О.О., Ємець Є.М., Ольховський Д.М. Модифікація другого методу комбінаторного відсікання	60
Ємець О.О., Ольховська О.В. Про збіжність ітераційного методу для розв'язування задач комбінаторної оптимізації ігрового типу на переставленнях	62
Зинченко С.В., Зинченко В.П., Малишко А.О., Стасюк В.В., Ходанкова О.В. К вопросу разработки оптимального алгоритма работы вычислительной системы микроспутника	64
Ivanov Viktor V., Korzhova Valentina N. On approximate solution of 3D-Navier-Stokes equations	65
Касянчук М.М., Якименко І.З., Івасьєв С.В. Теорія та оптимізація алгоритмів опрацювання великорозрядних чисел у базисі Крестенсона	67

О.О. ЄМЕЦЬ, О.В. ОЛЬХОВСЬКА
 Полтавський університет економіки і торгівлі, Полтава,
 yemetsli@mail.ru, contacts@informatics.org.ua

ПРО ЗБІЖНІСТЬ ІТЕРАЦІЙНОГО МЕТОДУ ДЛЯ РОЗВ'ЯЗУВАННЯ ЗАДАЧ КОМБІНАТОРНОЇ ОПТИМІЗАЦІЇ ІГРОВОГО ТИПУ НА ПЕРЕСТАВЛЕННЯХ

У роботах [1–3] розглянуто новий клас задач – задачі комбінаторної оптимізації ігрового типу на розміщеннях та переставленнях. У цих задачах на стратегії одного з гравців накладаються комбінаторні обмеження. У роботі [3] запропоновано ітераційний метод розв'язку такого класу задач на переставленнях. Розглянемо доведення збіжності цього методу.

Нехай задана платіжна матриця $A' = (a'_{ij})$ вимірності $m \times n$, елемент a'_{ij} якої показує перевищення (різницю) прибутків другого гравця в порівнянні з першим гравцем. На обмеження першого гравця накладаються комбінаторні обмеження, що визначаються переставленнями:

$X = (x_1, \dots, x_m) \in E_m(G)$, де $E_m(G)$ – множина переставлень з елементів множини G .

Складемо нову матрицю $A = (a_{ij})$ розмірністю $\bar{m} \times n$, де $\bar{m} = m!$. У цій матриці

$$a_{ij} = \sum_{t=1}^m a'_{ij} x_{it}, \quad \forall i = \overline{1, \bar{m}}, \quad \forall j = \overline{1, n}.$$

Нехай перший гравець обирає i -й рядок з ймовірністю p_i , а другий гравець вибирає j -й стовпчик з ймовірністю q_j , де $p_i \geq 0$, $\sum_{i=1}^{\bar{m}} p_i = 1$, $q_j \geq 0$, $\sum_{j=1}^n q_j = 1$. Математичне сподівання платежу

першого гравця дорівнює $\sum_{i=1}^{\bar{m}} \sum_{j=1}^n a_{ij} p_i q_j$. Оскільки $\min_j \sum_{i=1}^{\bar{m}} a_{ij} p_i \leq \sum_{i=1}^{\bar{m}} \sum_{j=1}^n a_{ij} p_i q_j \leq \max_i \sum_{j=1}^n a_{ij} q_j$, то

$$\min_j \sum_{i=1}^{\bar{m}} a_{ij} p_i \leq \max_i \sum_{j=1}^n a_{ij} q_j. \quad (1)$$

Основна теорема теорії ігор [4] стверджує, що, при деяких наборах ймовірностей $P = (p_1, \dots, p_m)$ та $Q = (q_1, \dots, q_n)$, у відношенні (1) досягається рівність, а $(P; Q)$ є оптимальним розв'язком матричної гри.

Значення v ціни гри при цьому дорівнює: $v = \min_j \sum_{i=1}^{\bar{m}} a_{ij} p_i = \max_i \sum_{j=1}^n a_{ij} q_j$.

Покладемо A_i – це i -й рядок матриці A , а відповідно A_j – j -й стовпець. Тоді якщо $SUM_1(N)$ – вектор у послідовності $\{SUM_1(0), SUM_1(1), \dots, SUM_1(N), \dots\}$, то позначимо його j -у координату $SUM_{1j}(N)$.

Позначимо $\max_j SUM_1(N) = \max_j SUM_{1j}(N)$, $\min_j SUM_1(N) = \max_j SUM_{1j}(N)$. З цими

позначеннями перепишемо (1): $\min_j \sum_{i=1}^{\bar{m}} A_i p_i \leq \max_i \sum_{j=1}^n A_j q_j$, де $p_i \geq 0$, $\sum_{i=1}^{\bar{m}} p_i = 1$, $q_j \geq 0$, $\sum_{j=1}^n q_j = 1$.

Означення. Послідовність \bar{m} – вимірних векторів $SUM_2(0), SUM_2(1), \dots$, та n вимірних векторів $SUM_1(0), SUM_1(1), \dots$ назвемо векторною системою (SUM_2, SUM_1) для A якщо виконуються наступні умови:

1) вектори $SUM_1(0), SUM_2(0)$ – нульові, тобто $SUM_1(0) = (0, \dots, 0)$, $SUM_2(0) = (0, \dots, 0)$.

Зауважимо, що тоді виконується умова $\min SUM_2(0) = \max SUM_1(0) = 0$, при цьому ці рівності – це рівності нулю;

2) $SUM_2(N+1) = SUM_2(N) + A_i$, $SUM_1(N+1) = SUM_1(N) + A_j$ (2), де i, j задовольняє співвідношенню $SUM_{1i}(t) = \max_j SUM_1(N)$, $SUM_{2j}(t) = \max_i SUM_2(N)$.

Система з такими властивостями утворюється при реалізації методу з [3] алгоритм якого сформульовано та програмно реалізовано в [5].

Векторну систему (SUM_2, SUM_1) для A можна представити рекурентно, якщо задати $SUM_2(0), SUM_1(0)$. У методі з [3] на кожній ітерації рядок таблиці SUM (накопичені суми скалярних добутоків першого гравця) додається до SUM_2 і визначається максимальна компонента SUM_1 (за алгоритмом з [5] – це $N\bar{v}$ – максимальний накопичений виграш), рядок таблиці SUM (накопичені суми скалярних добутоків другого гравця) додається до SUM_1 і визначається мінімальний компонент SUM_2 (за алгоритмом з [5] – це $N\underline{v}$ – мінімальний накопичений виграш).

Якщо $SUM_2(0) = 0, SUM_1(0) = 0$, $\frac{SUM_2(N)}{N}$ є середнім рядків, а $\frac{SUM_1(N')}{N'}$ середнім стовпців, для кожного N, N' (N, N' – кількість ітерацій методу) буде виконуватися:

$$\frac{\min SUM_2(N)}{N} \leq v \leq \frac{\max SUM_1(N')}{N'}$$

Розв'язок гри отримується, коли ці границі рівні при $N, N' \rightarrow \infty$. Наступна теорема встановлює цей факт.

Теорема. Якщо (SUM_2, SUM_1) векторна система для матриці A , утворена в процесі роботи алгоритму ітераційного методу для розв'язування задач комбінаторної оптимізації ігрового типу на переставленнях [3], то $\lim_{N \rightarrow \infty} \frac{\min SUM_2(N)}{N} = \lim_{N \rightarrow \infty} \frac{\max SUM_1(N)}{N} = v$.

Доведення даної теореми здійснено аналогічно доведенню збіжності методу Брауна – Робінсона.

У доповіді представлено обґрунтування збіжності ітераційного методу для розв'язування задач комбінаторної оптимізації ігрового типу на переставленнях.

1. Емец О.А., Устьян Н.Ю. Решение некоторых задач комбинаторной оптимизации на размещениях и перестановках игрового типа // Проблемы управления и информатики. – 2006. – № 3. – С. 37–47.
2. Емец О.А., Устьян Н.Ю. Исследование математических моделей и методов решения задач на перестановках игрового типа // Кибернетика и системный анализ. – 2007. – № 6. – С. 103–114.
3. Ємець О.О., Устьян Н.Ю. Один ітераційний метод розв'язування ігрових задач на переставленнях // Наукові вісті НТУ України “КПІ”. – 2008. – № 3. – С. 5–10.
4. Вентцель Е.С. Элементы теории игр. Изд. 2-е, стереотип. – М.: Физматгиз, 1961. – 67 с.
5. Ємець О.О., Ольховська О.В. Розв'язування задач ігрового типу на множині розміщень // Інформатика та системні науки (ІСН-2010): матеріали Всеукраїнської науково-практичної конференції 18-20 березня 2010. – Полтава: РВВ ПУСКУ, 2010. – С. 61–63.