

конференции «Межкультурная коммуникация: лингвистические и лингводидактические аспекты». – Новосибирск: изд-во НГТУ. – 2010. – С. 221-229.

3. Кручинина Г.А. Использование информационных и коммуникационных технологий в модульном обучении в средних специальных учебных заведениях [Текст] / Г.А. Кручинина, С.А. Заливчей // Ярославский педагогический вестник – Том II (Психолого-педагогические науки) – 2010. – № 3. С. 72-77.

4. Садчиков И.А. Возможности и перспективы использования динамических экспертных систем в становлении новой науки эдукологии [Текст] / И.А. Садчиков, И.А. Суслова // Актуальные научно-педагогические проблемы воспитания и образования учащихся и студентов. Сборник научных статей. – СПб.: Изд. БПА, 2010. – 244 с. С. 221 – 227.

5. Суслова И.А. Перспективы интеллектуализации адаптивных методических систем в дистанционных образовательных технологиях [Текст] / И.А. Суслова // Образование и наука: изв. Урал. отд-ния Рос. акад. образования. – 2008. – № 1. С. 95 – 103.

И.А. Трещев, Е.И. Аладинский, А.Л. Григорьева
ОБ АСИМПТОТИЧЕСКИ СТРОГОЙ ОЦЕНКЕ АЛГОРИТМОВ ПЕРЕБОРА В
ЗАДАЧАХ ЗАЩИТЫ ИНФОРМАЦИИ

jan198282@mail.ru

*ФГБОУ ВПО «Комсомольский-на-Амуре государственный технический университет»,
Комсомольск-на-Амуре*

Standard encryption, DES, AES, and other industrial algorithm assumes complete listing of all kinds of key information. With the exhaustive search (bruteforce) an important task is to obtain a priori estimates of the time required for the operation of the algorithm. We propose a new class of asymptotically strict functions to obtain more accurate estimates of the time of search.

Общепринятые асимптотические функции для оценки вычислительной сложности алгоритмов и имеют следующий вид[1]:

$\Theta(g(n)) = \{f(n) \mid \exists c_1, c_2, n_0 \mid \forall n \geq n_0; 0 \leq c_1(g(n)) \leq f(n) \leq c_2(g(n));\}$

$O(g(n)) = \{f(n) \mid \exists c_1, n_0 \mid \forall n \geq n_0; 0 \leq f(n) \leq c_1(g(n));\}$

$\Omega(g(n)) = \{f(n) \mid \exists c_1, n_0 \mid \forall n \geq n_0; 0 \leq c_1(g(n)) \leq f(n);\}$

$o(g(n)) = \{f(n) \mid \exists c_1, n_0 \mid \forall n \geq n_0; 0 < f(n) < c_1(g(n));\}$

$w(g(n)) = \{f(n) \mid \exists c_1, n_0 \mid \forall n \geq n_0; 0 < c_1(g(n)) < f(n);\}$

Сформулируем свойства для приведенных классов функций:

Теорема 1

Функция $f(n)$ принадлежит $\Theta(g(n))$ тогда и только тогда, когда $f(n)$ принадлежит $O(g(n))$ и $f(n)$ принадлежит $\Omega(g(n))$

Доказательство:

Для обозначения принадлежности функции классу будем использовать знак $=$. Покажем, что функция $f(n)$ принадлежит $\Theta(g(n))$ тогда, когда $f(n)$ принадлежит $O(g(n))$ и $f(n)$ принадлежит $\Omega(g(n))$.

$$\left\{ \begin{array}{l} f(n)=O(g(n)), \\ f(n)=\Omega(g(n)). \Rightarrow f(n)=\Theta(g(n)). \end{array} \right.$$

По определению:

$$\left\{ \begin{array}{l} \mathbf{O}(g(n)) = \{f(n) \mid \exists C_1, n_0 \mid \forall n \geq n_0; 0 \leq f(n) \leq C_1(g(n));\}, \\ \mathbf{\Omega}(g(n)) = \{f(n) \mid \exists C_2, n'_0 \mid \forall n \geq n'_0; 0 \leq C_2(g(n)) \leq f(n);\}. \end{array} \right.$$

Следовательно $\forall n \geq n'_0 = \max(n_0, n'_0) \Rightarrow 0 \leq f(n) \leq C_1(g(n))$ и $0 \leq C_2(g(n)) \leq f(n)$, значит $C_2(g(n)) \leq f(n) \leq C_1(g(n)) \Rightarrow f(n) = \mathbf{\Theta}(g(n))$.

Покажем, что из того, что $f(n) = \mathbf{\Theta}(g(n))$ следует, что $f(n) = \mathbf{O}(g(n))$ и $f(n) = \mathbf{\Omega}(g(n))$.

Доказательство:

По определению:

$$\left\{ \begin{array}{l} f(n) = \mathbf{\Theta}(g(n)) \Rightarrow \{\exists c_1, c_2, n_0 \mid \forall n \geq n_0; 0 \leq c_1(g(n)) \leq f(n) \leq c_2(g(n));\}, \text{ следовательно} \\ \forall n \geq n_0 \exists c_1; 0 \leq c_1 g(n) \leq f(n), \Rightarrow f(n) = \mathbf{\Omega}(g(n)), \\ \forall n \geq n_0 \exists c_2; c_2 g(n) \geq f(n) \geq 0. \Rightarrow f(n) = \mathbf{O}(g(n)). \end{array} \right.$$

Теорема доказана.

Мы предлагаем ввести новый класс асимптотической строгой оценки алгоритмов в задачах защиты информации

$$\mathbf{\Sigma}(g(n)) = \{f(n) \mid \exists c_1, c_2, n_0 \mid \forall n \geq n_0; 0 < c_1(g(n)) < f(n) < c_2(g(n));\}$$

Теорема 2

Покажем, что функция $f(n)$ принадлежит $\mathbf{\Sigma}(g(n))$ тогда, когда $f(n)$ принадлежит $\mathbf{o}(g(n))$ и $f(n)$ принадлежит $\mathbf{w}(g(n))$.

Доказательство:

$$\left\{ \begin{array}{l} f(n) = \mathbf{o}(g(n)), \\ f(n) = \mathbf{w}(g(n)). \Rightarrow f(n) = \mathbf{\Sigma}(g(n)); \end{array} \right.$$

По определению:

$$\left\{ \begin{array}{l} \mathbf{o}(g(n)) = \{f(n) \mid \exists c_1, n_0 \mid \forall n \geq n_0; 0 < f(n) < C_1(g(n));\}, \\ \mathbf{w}(g(n)) = \{f(n) \mid \exists c_2, n'_0 \mid \forall n \geq n'_0; 0 \leq C_2(g(n)) < f(n);\}. \end{array} \right.$$

Следовательно $\forall n \geq n'_0 = \max(n_0, n'_0) \Rightarrow 0 < f(n) < C_1(g(n))$ и $0 \leq C_2(g(n)) < f(n)$, значит $C_2(g(n)) < f(n) < C_1(g(n)) \Rightarrow f(n) = \mathbf{\Sigma}(g(n))$;

Покажем, что из того, что $f(n) = \mathbf{\Sigma}(g(n))$ следует, что $f(n) = \mathbf{o}(g(n))$ и $f(n) = \mathbf{w}(g(n))$.

Доказательство:

По определению:

$$f(n) = \mathbf{\Sigma}(g(n)) \Rightarrow \{\exists c_1, c_2, n_0 \mid \forall n \geq n_0; 0 \leq c_1(g(n)) < f(n) < c_2(g(n));\}$$

$$\left\{ \begin{array}{l} \forall n \geq n_0 \exists c_1; 0 \leq c_1 g(n) < f(n), \Rightarrow f(n) = \mathbf{w}(g(n)), \\ \forall n \geq n_0 \exists c_2; c_2 g(n) > f(n) > 0. \Rightarrow f(n) = \mathbf{o}(g(n)). \end{array} \right.$$

Теорема доказана.

Для алгоритмов перебора введенный класс асимптотически строгих оценок позволяет уточнить алгоритмическую сложность и до проведения процедуры перебора всех возможных

вариантов ключевой информации[2], оценить асимптотическую скорость роста времени необходимого для перебора.

Библиографический список

1. Кормен, Т., Лейзерсон, Ч., Ривест, Р., Штайн, К. Алгоритмы: построение и анализ = Introduction to Algorithms / Под ред. И. В. Красикова. — 2-е изд. — М.: Вильямс, 2005. — 1296 с. — ISBN 5-8459-0857-4
2. Трещев И.А. Оценка временных затрат для осуществления распределенного перебора в гетерогенных системах при помощи временных волновых систем // Доклады ТУСУРа 1(25), часть 2, ISSN 1818-0442, С. 141-148.

Н.О. Черняев

АВТОМАТИЗАЦИЯ ПРОЦЕССА УЧЕТА УСПЕВАЕМОСТИ СТУДЕНТОВ УНИВЕРСИТЕТА В РАМКАХ БАЛЛЬНО – РЕЙТИНГОВОЙ СИСТЕМЫ

niwalke@mail.ru

ФГБОУ ВПО «Южно-Уральский государственный университет» (НИУ), Челябинск

The article presents accounting information system student performance in the point-rating system of the University. This information system – a new approach to accounting student performance.

В 2010 Южно-Уральский государственный университете перешел на балльно-рейтинговую систему оценки успеваемости студентов. Под балльно-рейтинговой системой понимается система количественной оценки качества освоения образовательной программы. Основная идея этой системы заключается в том, что студент на протяжении семестра получает баллы, на основании которых формируется итоговая оценка по дисциплине. В течение семестра преподаватели проводят ряд контрольных точек (лабораторные работы, тесты, практические задания, контрольные работы), за каждую из которых студенты получают баллы. В итоге эти баллы складываются и вместе с баллом за посещаемость (выставляется автоматически на основании данных о посещаемости студента) дают итоговый балл.

В ходе семестра студенту можно начислить следующее количество баллов, исходя из формы итогового контроля:

- если семестр завершается зачетом – максимально 80 баллов (с учетом посещаемости);
- если семестр завершается экзаменом – максимально 60 баллов (с учетом посещаемости).

Проект информационной системы автоматизации процесса начисления баллов студентов и составления на их основе рейтинга лучших студентов представляет собой рабочее место преподавателя, который позволяет проводить весь комплекс работ по выставлению, мониторингу успеваемости студентов в электронной форме.

Главная цель проекта – обеспечение реализации учета успеваемости на основании балльно-рейтинговой системы.

Проект включает в себя 2 модуля:

1. Программа «Дневник преподавателя»
2. Веб – версия Учета успеваемости студентов
1. Программа «Дневник Преподавателя»