

Министерство образования Республики Беларусь

Учреждение образования

«Брестский государственный технический университет»

**«СОВРЕМЕННЫЕ ПРОБЛЕМЫ
МАТЕМАТИКИ И
ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ»**

**Материалы II региональной конференции молодых
ученых и студентов 28-30 ноября 2001 г.**

Брест 2001

УДК 681.3
ББК 32.973

Редакционная коллегия:

В.И. Драган, БГТУ, проректор по научной работе, профессор, председатель
Р.Х. Садыхов, БГУИР, д.т.н., зав. кафедрой ЭВМ,
Н.В. Лазакович, БГУ, д.ф.-м.н., профессор,
А.И. Калинин, БГУ, д.ф.-м.н., зав. кафедрой методов оптимального управления,
Б.А. Железко, БГЭУ, к.т.н., профессор,
В.А. Головкин, БГТУ, к.т.н., профессор,
С.С. Дереченник, БГТУ, к.т.н., зав. кафедрой ЭВМ и Систем,
В.М. Ракетский, БГТУ, к.ф.-м.н., зав. кафедрой информатики и прикладной математики,
В.С. Рубанов, БГТУ, к.ф.-м.н., зав. кафедрой высшей математики,
Л.П. Махнист, БГТУ, к.т.н., доцент,
Ю.В. Савицкий, БГТУ, к.т.н., доцент.

Современные проблемы математики и вычислительной техники: Материалы
II региональной конференции молодых ученых и студентов 28-30 ноября 2001 г.-Брест:
БГТУ, 2001, 174 с.

Представлены материалы по современным проблемам математики, информатики,
вычислительной техники и их приложениям.

ISBN 985-6584-36-1.

АНАЛИТИЧЕСКИЕ И ЧИСЛЕННЫЕ МЕТОДЫ ИССЛЕДОВАНИЙ В МАТЕМАТИКЕ

ЧИСЛЕННЫЙ АНАЛИЗ ХАРАКТЕРИСТИК СГЛАЖЕННОЙ ПЕРИОДОГРАММЫ БАРТЛЕТТА

М.А. Акинфина

(БГУ, г. Минск)

Рассмотрим дискретный устойчивый симметричный стационарный случайный процесс $X(t)$, $t \in Z = \{0, \pm 1, \dots\}$ с характеристическим показателем α , $0 < \alpha < 2$.

Пусть $x(1), x(2), \dots, x(T)$ — $T = L \times M$ — последовательных наблюдений за процессом $X(t)$, $t \in Z$, которые разбиты на L равных непересекающихся отрезков, содержащих по $M = 2k(n-1) + 1$ наблюдений (L не зависит от T), где $n \in N$, $k \in N \cup \left\{ \frac{1}{2} \right\}$, причем при $k = \frac{1}{2}$ будем предполагать, что $n = 2n' + 1$, $n' \in N$.

В качестве оценки спектральной плотности $f(\lambda)$ исследуем статистику

$$\tilde{f}_T(\lambda) = \int_{\Pi} W_T(\nu) \bar{f}_T(\lambda + \nu) d\nu, \quad (1)$$

где $\bar{f}_T(\lambda) = \frac{1}{L} \sum_{l=1}^L I_M^l(\lambda)$, $\lambda \in \Pi$, является периодограммой Бартлетта, а $I_M^l(\lambda)$ и $W_T(\lambda)$, $\lambda \in \Pi$ соответственно — модифицированная периодограмма, построенная по наблюдениям l -го интервала, $l = \overline{1, L}$ и спектральное окно определенные в [1].

Пусть $H_M(\nu) = A_M H^{(M)}(\nu)$,

$$A_M = \left[\int_{\Pi} |H^{(M)}(\nu)|^\alpha d\nu \right]^{-1/\alpha},$$

$$H^{(M)}(\nu) = \operatorname{Re} \sum_{m=-k(n-1)}^{k(n-1)} e^{-i\nu m} h_k(m, n),$$

где $h_k(m, n)$ — окно просмотра данных, позволяющее представить $H^{(M)}(\nu)$ в виде

$$H^{(M)}(\nu) = \frac{2\pi}{B'_{\alpha,T}} \left(\frac{\sin \frac{n\nu}{2}}{\sin \frac{\nu}{2}} \right)^{2k}, \quad B'_{\alpha,T} = \int_{\Pi} \left(\frac{\sin \frac{n\nu}{2}}{\sin \frac{\nu}{2}} \right)^{2k} d\nu.$$

Функции типа $H^{(M)}(\nu)$ называют полиномиальными ядрами типа Джексона.

Статистика $\tilde{f}_T(\lambda)$, $\lambda \in \Pi$ называется вспомогательной, оценкой спектральной плотности. Она была исследована в работах [1], [2]. Показано, что смещение и среднее квадратическое отклонение данной оценки стремится к нулю при $T \rightarrow \infty$.

Теорема [2]. Пусть спектральная плотность $f(\lambda)$ случайного процесса $X(t)$, $t \in Z$ в точке $\lambda_0 \in \Pi$ положительна, удовлетворяет условиям Гельдера (3) и ограничена на множестве Π т.е. $|f(\lambda)| \leq D_0$, $\lambda \in \Pi$, а $|H_M(\lambda)|^\alpha$ является положительным ядром на Π , для которого выполняется условие

$$\int_{\Pi} \left| H_M \left(\lambda_0 - \frac{x_1}{M_T} - \nu \right) H_M \left(\lambda_0 - \frac{x_2}{M_T} - \nu \right) \right|^{\frac{\alpha}{2}} d\nu \xrightarrow{T \rightarrow \infty} 0,$$

$x_1, x_2 \in [-1, 1]$, $|x_1 - x_2| > \varepsilon_T > 0$, $\varepsilon_T \xrightarrow{T \rightarrow \infty} 0$, $\varepsilon_T T \xrightarrow{T \rightarrow \infty} \infty$. Тогда для статистики $\tilde{f}_T(\lambda)$, $\lambda \in \Pi$, заданной равенством (1), справедливы соотношения:

$$1) \quad \tilde{\Delta} = \left| M \tilde{f}_T(\lambda_0) - [f(\lambda_0)]^{p/\alpha} \right| \leq S_1 \frac{1}{M_T^\gamma} \xrightarrow{T \rightarrow \infty} 0,$$

где

$$S_1 = \frac{p}{\alpha} D_0^{p/\alpha - 1} \left(B_1(\lambda_0) \int_{-1}^1 |W(\lambda)|^\gamma d\lambda + B_1(\lambda_0) \frac{\alpha \pi^{\gamma+2k\alpha}}{2^{2k\alpha} (\gamma+1)(2k\alpha-1)} + 2D_0 \frac{(\pi-\rho)\pi^{4k\alpha-1}}{|\rho|^{2k\alpha}} \right)$$

$$2) \quad |D \tilde{f}_T(\lambda_0)| \leq \frac{D_1}{L} \frac{1}{n^t} = \frac{1}{L} \left\{ V_{p,\alpha} \{f(\lambda_0)\}^{2p/\alpha} \int_{-1}^1 W^2(x) dx + C_f C_2 \right\} \frac{1}{n^t} \xrightarrow{T \rightarrow \infty} 0,$$

где $t = \frac{2k^2\alpha^2 - 1 - 2k^2\alpha^2s}{2k\alpha + 1 + 2k^2\alpha^2}$, $V_{p,\alpha} = \frac{\Gamma(2p)\Gamma\left(\frac{1}{2} - \frac{p}{\alpha}\right)\pi \sin p\pi}{2\Gamma^2(p)\Gamma^2\left(1 - \frac{p}{\alpha}\right)\sin^2 \frac{p\pi}{2}} - 1,$

$$3) \tilde{V} = M \left| \tilde{f}_T(\lambda_0) - \{f(\lambda_0)\}^2 \right|^2 \leq \left\{ \frac{D_1}{L} + S_1^2 \right\} n^{-\frac{2\gamma}{k\alpha+1}} \xrightarrow{T \rightarrow \infty} 0,$$

$$C_f = \frac{2p^2 e^{\max_{v \in \Pi} f(v)} \Gamma^2\left(\frac{1-p}{2}\right)}{\alpha^2 \left\{ f\left(\lambda_0 - \frac{x_1}{M_T}\right) f\left(\lambda_0 - \frac{x_2}{M_T}\right) \right\}^{\frac{1-p}{2}} \Gamma^2\left(1 - \frac{p}{\alpha}\right)}, \quad C_2 = \frac{1}{\pi} \left(\frac{\pi}{2}\right)^{2k\alpha} \left(\pi^{2k\alpha+1} + 2(\pi)^{k\alpha} \right),$$

$V_1(\lambda_0)$, M_T , $H_M(\lambda)$ и $W(\lambda)$ определены выше, $\Gamma(x)$ – гамма-функция числа x , $0 < s \leq \frac{1}{k\alpha+1}$, $k \geq \frac{2\gamma+1}{\alpha}$, $0 < p < \frac{\alpha}{2}$, $0 < \alpha < 2$, $\lambda_0 \in \Pi$.

Следствие. Пусть выполнены условия теоремы и спектральная плотность $f(\lambda)=1$. Тогда для статистики $\tilde{f}_T(\lambda)$, $\lambda \in \Pi$, заданной равенством (1), справедливы соотношения:

$$1) \tilde{\Delta} \leq S \frac{1}{M_T^\gamma} = \frac{p}{\alpha} \frac{(\pi - \rho) \pi^{4k\alpha-1}}{\rho^{2k\alpha}} \frac{1}{M_T^\gamma} \xrightarrow{T \rightarrow \infty} 0, \quad (7)$$

$$2) \left| D\tilde{f}_T(\lambda_0) \right| \leq \frac{D}{L} \frac{1}{n^t} = \frac{1}{L} \left\{ V_{p,\alpha} \int_{-1}^1 W^2(x) dx + C_1 C_2 \right\} \frac{1}{n^t} \xrightarrow{T \rightarrow \infty} 0 \quad (8)$$

$$3) \tilde{V} \leq \left\{ \frac{D}{L} + S^2 \right\} n^{-\frac{2\gamma}{k\alpha+1}} \xrightarrow{T \rightarrow \infty} 0, \quad (9)$$

$$C_1 = \frac{2p^2 e \Gamma^2\left(\frac{1-p}{2}\right)}{\alpha^2 \Gamma^2\left(1 - \frac{p}{\alpha}\right)}, \quad M_T, W(\lambda), t, V_{p,\alpha} \text{ и } C_2 \text{ определены выше, } \Gamma(x) - \text{гамма-}$$

функция числа x , $0 < s \leq \frac{1}{k\alpha+1}$, $k \geq \frac{2\gamma+1}{\alpha}$, $0 < p < \frac{\alpha}{2}$, $0 < \alpha < 2$, $\lambda_0 \in \Pi$.

Доказательство. Используя теорему получаем требуемые соотношения.

Проведен анализ констант C_1 , C_2 и D_1 , построены графики S и D при

$\alpha=0,5$, $k=3$, $\alpha=1,5$, $k=1$, и построим их графики в зависимости от p , где $p = \frac{\alpha}{b}$,

$b \in \mathbb{N}$, что минимальное значение p равняется $p=0,001$.

Рассмотрели среднеквадратическое отклонение $\bar{\nu}$. Взяв различное количество наблюдений и варьируя различным числом разбиений, получили следующие результаты.

$\alpha=0,5$	$p=1/500$	$\gamma=0,1, k=3$
T	L	$\bar{\nu}$
100	2	1,105
300	5	$9,71 \times 10^{-1}$
1200	10	$2,04 \times 10^{-1}$
7500	25	$1,16 \times 10^{-1}$
30000	50	$7,5 \times 10^{-2}$
50000	40	$7,91 \times 10^{-2}$
150000	25	$9,1 \times 10^{-2}$
10^6	10^5	$1,9 \times 10^{-2}$

$\alpha=1,5$	$p=1/1500$	$\gamma=0,1, k=1$
T	L	$\bar{\nu}$
40	2	1,062
100	5	$4,28 \times 10^{-1}$
400	2	$8,4 \times 10^{-2}$
2000	25	$7,9 \times 10^{-2}$
8000	20	$8,7 \times 10^{-2}$
10000	50	$3,96 \times 10^{-2}$
5×10^5	250	$9,535 \times 10^{-3}$
4×10^6	10^5	$2,1 \times 10^{-3}$

Из таблицы следует: 1) для того, чтобы $\bar{\nu}$ имело порядок 10^{-1} надо взять 300 наблюдений и $L=5$ при $\alpha=0,5$; и 100 наблюдений, $L=5$ при $\alpha=1,5$; 2) для того, чтобы $\bar{\nu}$ имело порядок 10^{-2} нужно брать 30000 наблюдений и 50 разбиений в случае $0 < \alpha < 1$ и 400 наблюдений, 2 разбиений в случае $1 < \alpha < 2$; 3) для того, чтобы $\bar{\nu}$ имело порядок 10^{-3} необходимо брать не менее 5×10^5 наблюдений и не менее 250 разбиений в случае $1 < \alpha < 2$, а в случае $0 < \alpha < 1$ $\bar{\nu}$ такого порядка не достигает даже при количестве наблюдений равном 10^6 и числе разбиений 10^5 .

Литература.

1. Демеш Н.Н., Акинфина М.А. // Вестник БГУ. Серия физ. мат. инф. - 2001, №1. - С. 75-79.
 2. Акинфина. - Минск, 1999. - 26 с. - Деп. В БелИСА. 16.06.99, № Д199971.

**О КАНОНИЧЕСКОМ ЛИФТЕ ПОДМНОГООБРАЗИЯ
 ОДНОРОДНОГО ПРОСТРАНСТВА**

А.С. Андреев

(БрГУ, г. Брест)

Пусть G – группа Ли, H – её замкнутая подгруппа Ли, $M=G/H$ – однородное G -пространство,

$$\pi : G \rightarrow G/H : a \mapsto aH$$

— каноническая проекция.

Группа G действует в M с помощью левых сдвигов:

$$G \times M \rightarrow M : (a, bH) \mapsto abH = a \cdot bH = T_a(bH).$$

Определение: Подмногообразием размерности n однородного пространства M будем называть пару (\mathcal{D}_0, f) , где \mathcal{D}_0 — окрестность нуля евклидова пространства R_n , f — аналитическое вложение \mathcal{D}_0 в M .

Подмногообразия однородного пространства изучаются локально.

Результат действия на канонический лифт подмногообразия внутренних автоморфизмов описывается следующей теоремой.

Теорема 1. Если канонический лифт подмногообразия (\mathcal{D}_0, f) по системе подпространств $\mathcal{K}_1, \mathcal{K}_2, \dots, \mathcal{K}_{p+1}$ подвергнуть преобразованию

$$J(h) : G \rightarrow G : a \mapsto hah^{-1},$$

то получим канонический лифт подмногообразия $(\mathcal{D}_0, T_h \circ f)$, построенный по системе подпространств

$$h \circ \mathcal{K}_1, h \circ \mathcal{K}_2, \dots, h \circ \mathcal{K}_{p+1}. \quad (1)$$

Справедлива формула:

$$\exp \operatorname{Ad}(\sigma)X = J(\sigma)(\exp X). \quad (2)$$

Рассмотрим $\check{f} = \exp^{-1} \circ \hat{f}$. Отсюда: $\hat{f} = \exp \circ \check{f}$. В силу (2) имеем:

$$J(h) \left(\exp \check{f}(x_0) \right) = \exp \operatorname{Ad} h \left(\check{f}(x_0) \right) = J(h) \left(\hat{f}(x_0) \right), \quad x_0 \in \mathcal{D}_0. \quad (3)$$

Отсюда следует, что $\operatorname{Ad}(h)\check{f}$ есть образ при отображении \exp^{-1} канонического лифта подмногообразия $(\mathcal{D}_0, T_h \circ f)$ по совокупности подпространств (1).

Поскольку в однородном пространстве G/H проблема G - эквивалентности подмногообразий сводится к проблеме H - эквивалентности, то доказанные в работе теоремы сводят проблему G - эквивалентности подмногообразий в однородном пространстве $M=G/H$ к проблеме H - эквивалентности подмногообразий в алгебре Ли \mathcal{J} структурной группы Ли G .

РЕКУРРЕНТНЫЕ МЕТОДЫ АНАЛИЗА СРЕДНИХ ЗНАЧЕНИЙ

А.М. Астахов

(ГрГУ, г. Гродно)

Рассматривается замкнутая сеть массового обслуживания (МО), в которой обслуживаются r типов заявок. Системы обслуживания (СМО) сети являются многолинейными. Дисциплины обслуживания в системах – FIFO. Обслуживание в СМО – произвольное. В докладе рассмотрен случай, когда времена обслуживания заявок одного типа в каждой линии СМО распределены по одинаковым законам, а заявки после обслуживания в СМО могут изменить свой тип. Такие сети являются математическими моделями различных объектов в экономике, страховании.

Для исследования таких сетей строятся приближенные рекуррентные по числу заявок и по моментам времени методы. Методы позволяют находить средние характеристики функционирования сети, такие как среднее время обслуживания заявок различных типов в системах сети, среднюю длину очередей, среднее число занятых линий обслуживания. Кроме того, данные методы позволяют определить среднее число заявок каждого типа в сети.

Разобьем множество возможных пар (i, c) , где i – номер СМО, c – тип заявки, на взаимно непересекающиеся классы по следующему правилу: пары (i, c) и (j, s) принадлежат одному классу, если вероятность того, что после некоторого числа переходов заявка типа c из i -й СМО станет заявкой типа s в j -й СМО, не равна 0. Заметим, что число заявок внутри класса постоянно.

Пусть μ_{ic} – интенсивность обслуживания заявок типа c в каждой линии i -й СМО, $i = \overline{1, n}$, $c = \overline{1, r}$. Обозначим через K^g – число заявок в g -м классе, $g = \overline{1, q}$, $\sum_{g=1}^q K^g = K$, $\bar{K} = (K^1, K^2, \dots, K^q)$; J_i^g – множество всех типов заявок,

входящих в i -ю СМО класса g , I^g – множество индексов всех СМО, обслуживающих заявки g -го класса, G_i – множество всех классов заявок, обслуживающихся в i -й СМО; τ_{ic} – среднее время обслуживания заявки типа c в i -й СМО; p_{icjs} – вероятность того, что после обслуживания в i -й СМО заявка типа c перейдет на обслуживание в j -ю СМО как заявка типа s ,

типа c перейдет на обслуживание в j -ю СМО как заявка типа s , $\sum_{s=1}^r p_{icjs} = 1$,

$i = \overline{1, n}$, $c \in J_i^{G_i}$, $j = \overline{1, n}$; $\sum_{j=1}^n p_{icjs} = 1$, $i = \overline{1, n}$, $c \in J_i^{G_i}$, $s = \overline{1, r}$; $\rho_i(\bar{K})$ - среднее

число занятых линий в i -й СМО, когда в сети обслуживается K^g заявок g -го класса, $g = \overline{1, q}$. И пусть также $N_{ic}(\bar{K})$, $T_{ic}(\bar{K})$ - соответственно среднее число заявок типа c (ожидающих и обслуживающихся) и среднее время пребывания заявок типа c (включая ожидание) в i -й системе в стационарном режиме, когда в ней обслуживается K^g заявок g -го класса, $g = \overline{1, q}$.

Метод, рекуррентный по числу заявок.

Для нахождения средних характеристик сети можно составить следующие рекуррентные по числу заявок в сети соотношения:

1. Полагаем $k^g = 0$, $g = \overline{1, q}$, $N_i(E_0) = 0$, $\rho_i(E_0) = \rho_i^*$, $i = \overline{1, n}$, в качестве ρ_i^* можно взять, например, 1.

2. Выбираем класс заявки g^* , пользуясь правилом получения дискретной случайной величины, которая принимает значение g^* с вероятностью

$$p_{g^*} = \frac{K - k^*}{K - k^*}, \quad g^* = \overline{1, q}, \quad \sum_{g=1}^q p_g = 1.$$

3. Вводим в сеть новую заявку класса g^* и полагаем $k^* = k^* + 1$.

4. Вычисляем $\rho_i(\bar{k}) = \min\{N_i(\bar{k}), m_i\}$, $\rho_{ic}(\bar{k}) = N_{ic}(\bar{k}) \frac{\rho_i(\bar{k})}{\sum_{s=1}^r N_{is}(\bar{k})}$, $i \in I^{g^*}$.

5. Находим $T_{ic}(\bar{k}) = \tau_{ic}(\bar{k}) +$

$$+ \frac{\sum_{s=1}^r \tau_{is}(\bar{k})(N_{is}(\bar{k}) - \rho_{is}(\bar{k})) + \sum_{s=1}^r \rho_{is}(\bar{k}) \frac{M_{is}[t^2]}{2\tau_{is}(\bar{k})}}{\rho_i(\bar{k})}, \quad i \in I^{g^*}.$$

6. Вычисляем
$$N_{ic}(\bar{k}) = \frac{K^g T_{ic}(\bar{k})}{\sum_{j=1}^n \sum_{s \in J_j^{Gj}} T_{js}(\bar{k}) e_{jsic}}, i \in I^g.$$

7. Находим
$$N_i(\bar{k}) = \sum_{c=1}^r N_{ic}(\bar{k}), i \in I^g.$$

8. Средние характеристики СМО с номерами $i \notin I^g$ на данном шаге итерации не меняются.

9. Переходим к пункту 2.

Метод, рекуррентный по моментам времени.

Рассмотрим метод, рекуррентный по моментам времени. Предположим, что сеть функционирует на большом промежутке времени $[0, T]$. Пусть $M_i(t)$ - средняя интенсивность потока заявок из i -й СМО на интервале времени $[0, t]$, а $N_{ic}(\bar{K}, t)$, $N_i(t)$, $T_{ic}(t)$, $\rho_i(t)$ - соответственно среднее число заявок типа c , среднее число заявок, среднее время пребывания заявок, среднее число занятых линий заявками типа c и всеми заявками в i -й СМО сети на интервале времени $[0, t]$, $t < T$, когда в ней обслуживаются \bar{K} заявок.

Для нахождения средних характеристик можно составить следующие, рекуррентные по t соотношения:

1. Вычисляем
$$\rho_i(t) = \min\{N_i(t), m_i\}, \rho_{ic}(t) = N_{ic}(t) \frac{\rho_i(t)}{\sum_{s=1}^r N_{is}(t)}, i = \overline{1, n}.$$

2. Находим
$$T_{ic}(t) = \tau_{ic} + \frac{\sum_{s=1}^r \tau_{is} (N_{is}(t) - \rho_{is}(t)) + \sum_{s=1}^r \rho_{is}(t) \frac{M_{is}[t^2]}{2\tau_{is}}}{\rho_i(t)}, i = \overline{1, n}.$$

3. Вычисляем
$$N_{ic}(t+1) = \frac{K^g T_{ic}(t)}{\sum_{j=1}^n \sum_{s \in J_j^{Gj}} T_{js}(t) e_{jsic}}, g = \overline{1, q}, i \in I^g.$$

4. Находим
$$N_i(t+1) = \sum_{c=1}^r N_{ic}(t+1), i = \overline{1, n}.$$

5. Переходим к шагу 1.

За начальные распределение заявок по системам сети можно взять любые значения $N_{ic}(0) \neq 0$ таким образом, чтобы $\sum_{i=1}^n \sum_{c=1}^r N_{ic}(0) = K$, где

$$K = \sum_{g=1}^q K^g \text{ - число заявок в сети.}$$

Если надо найти, например, среднее число заявок типа c в стационарном режиме, то правилом остановки будет выполнение неравенства $\max_i |N_{ic}(t) - N_{ic}(t-1)| < \epsilon$, где ϵ -заданная точность, $N_{ic}(t-1)$ - число заявок типа c в i -й СМО на предыдущей итерации метода.

Рассмотренные методы применялись для исследования сетей с центральной системой обслуживания и 10-ю периферийными СМО. Результаты расчетов средних характеристик функционирования сети сравнивались с результатами имитационного моделирования. Эксперименты показали, что методы обладают достаточно высокой точностью.

ЧИСЛЕННЫЙ МЕТОД НАХОЖДЕНИЯ КОЭФФИЦИЕНТОВ ХАРАКТЕРИСТИЧЕСКОГО ПОЛИНОМА

Н.Г. Бородулина, А.В. Морской

(ГрГУ, г. Гродно)

Часто на практике возникает задача о нахождении характеристических значений некоторой наперед заданной матрицы численными методами.

Пусть задана некоторая матрица $A = [a_{ij}] \in M_n$, где M_n - пространство квадратных матриц порядка n над полем P , $E_k(A)$ - сумма различных главных миноров порядка k матрицы A , причём $E_0(A) = 1$.

Как известно, для произвольной матрицы $A \in M_n$ определитель находится по формуле

$$\det A = \sum_{\sigma} \operatorname{sgn} \sigma \prod_{i=1}^n a_{i\sigma(i)},$$

где σ пробегает множество всех $n!$ перестановок из n чисел $\{1, 2, \dots, n\}$ и $\operatorname{sgn} \sigma$ есть знак перестановки σ .

Характеристический полином матрицы $A \in M_n$ имеет вид

$$p_A(\lambda) = \det(A - \lambda I).$$

Теорема. Справедливо следующее тождество

$$p_A(\lambda) = \sum_{i=0}^n E_i(A)(-\lambda)^{n-i},$$

где

$$E_k(A) = \sum_{1 \leq i_1 < \dots < i_k \leq n} \sum_{\bar{\sigma}} \operatorname{sgn} \bar{\sigma} \prod_{j=1}^k a_{i_j, \bar{\sigma}(j)}, \quad (1)$$

где $\bar{\sigma}$ пробегает множество всех $k!$ перестановок из k чисел $\{i_1, \dots, i_k\}$ и $\operatorname{sgn} \bar{\sigma}$ есть знак перестановки, $E_k(A)$ – сумма C_n^k различных главных миноров порядка k .

Выражение (1) можно использовать в качестве численного метода нахождения коэффициентов характеристического полинома.

Итак, сумма главных миноров матрицы $A \in M_n$, $E_k(A)$ составлена из произведений k элементов матрицы A , причём у этих элементов индексы составлены из всевозможных сочетаний k элементов из n таким образом, что первые индексы у произведения идут в порядке возрастания, а вторые индексы являются всевозможными перестановками этих k индексов. Знак перед произведением-слагаемым равен знаку перестановки вторых индексов.

Поэтому создан двоичный счётчик из n разрядов, каждый разряд которого будет отвечать за присутствие индекса (номера разряда) в произведении элементов матрицы.

Пусть k – количество единиц в бинарном счётчике, тогда количество элементов в произведении равно k и это произведение является слагаемым суммы $E_k(A)$, причём количество произведений слагаемых равно C_n^k .

ОДИН ИЗ СПОСОБОВ ПРЕДСТАВЛЕНИЯ РЕШЕНИЯ НЕЛИНЕЙНОГО РАЗНОСТНОГО УРАВНЕНИЯ P -ГО ПОРЯДКА

Н.А. Брызгалова

(БГУ, г. Минск)

Будем искать решение уравнения

$$x(n+p) = f(n, x(n), x(n+1), \dots, x(n+p-1)). \quad (1)$$

в виде

$$x(n) = \sum_{j=1}^p c_j(n) x_j(n), \quad (2)$$

где $c_1(n), \dots, c_p(n)$ - линейно-независимые решения уравнения (1).

Предположим, что функции $x_i(n)$ определяются системой

$$\Delta x_i(n) = f_i(n, x_1(n), \dots, x_p(n), c_1(n), \dots, c_p(n)), \quad (i = \overline{1, p}) \quad (3)$$

где функции f_i будут определены системой

$$\begin{aligned} \sum_{j=1}^p c_j(n+1) f_j(n, x_1(n), \dots, x_p(n), c_1(n), \dots, c_p(n)) &= 0, \\ \sum_{j=1}^p c_j(n+2) f_j(n, x_1(n), \dots, x_p(n), c_1(n), \dots, c_p(n)) &= 0, \\ \sum_{j=1}^p c_j(n+3) f_j(n, x_1(n), \dots, x_p(n), c_1(n), \dots, c_p(n)) &= 0, \\ \dots & \\ \sum_{j=1}^p c_j(n+p-1) f_j(n, x_1(n), \dots, x_p(n), c_1(n), \dots, c_p(n)) &= 0, \\ \sum_{j=1}^p c_j(n+p) f_j(n, x_1(n), \dots, x_p(n), c_1(n), \dots, c_p(n)) &= F(n), \end{aligned} \quad (4)$$

где $F(n) = f(n, \sum_{j=1}^p c_j(n) x_j(n), \sum_{j=1}^p c_j(n+1) x_j(n), \dots, \sum_{j=1}^p c_j(n+p-1) x_j(n)) -$
 $-\sum_{j=1}^p x_j(n) f(n, c_j(n), c_j(n+1), \dots, c_j(n+p-1)).$

Если известны функции $c_j(n)$, то мы можем найти функции f_j из системы р линейных уравнений (4). Решая эту систему получим

$$f_j(n, x_1(n), \dots, x_p(n), c_1(n), \dots, c_p(n)) = (-1)^{i+1} \frac{W_j}{W} F(n),$$

где $W = \begin{vmatrix} c_1(n+1) & \dots & c_p(n+1) \\ \dots & \dots & \dots \\ c_1(n+p) & \dots & c_p(n+p) \end{vmatrix}$, а W_j получается из W вычеркиванием j -го столбца и последней строки.

Пример 1. Рассмотрим следующее разностное уравнение второго порядка

$$x(n+2) + \frac{2}{n} x^2(n+1) + f(n)x(n) = 0. \quad (5)$$

Если $c_1(n), c_2(n)$ – линейно-независимые решения уравнения (5), то решение уравнения (5) имеет вид

$$x(n) = c_1(n)x_1(n) + c_2(n)x_2(n),$$

где $\Delta x_i(n)$ ($i=1,2$) находятся из системы уравнений

$$\Delta x_1(n) = \frac{2c_2(n+1)P(n)}{nW},$$

$$\Delta x_2(n) = -\frac{2c_1(n+1)P(n)}{nW},$$

где

$$P(n) = [c_1(n+1)x_1(n) + c_2(n+1)x_2(n)]^2 - x_1(n)(c_1(n+1))^2 - x_2(n)(c_2(n+1))^2,$$

$$W = c_1(n+1)c_2(n+2) - c_1(n+2)c_2(n+1).$$

Пример 2. $x(n+3) + x(n)x(n+2) - x^2(n+1) + 1 = 0.$ (6)

Если $c_1(n), c_2(n), c_3(n)$ – линейно-независимые решения уравнения (6), то решение имеет вид

$$x(n) = c_1(n)x_1(n) + c_2(n)x_2(n) + c_3(n)x_3(n),$$

где $\Delta x_i(n)$ ($i=1,3$) находятся из системы уравнений

$$\Delta x_1(n) = \frac{W_1}{W} G(n),$$

$$\Delta x_2(n) = -\frac{W_2}{W} G(n),$$

$$\Delta x_3(n) = \frac{W_3}{W} G(n),$$

$$G(n) = -(c_1(n)x_1(n) + c_2(n)x_2(n) + c_3(n)x_3(n)) \cdot (c_1(n+2)x_1(n) + c_2(n+2)x_2(n) + c_3(n+2)x_3(n)) -$$

$$-(c_1(n+1)x_1(n) + c_2(n+1)x_2(n) + c_3(n+1)x_3(n))^2 + x_1(n)[c_1(n)c_2(n+2) - (c_1(n+1))^2 + 1] +$$

$$+ x_2(n)[c_2(n)c_2(n+2) - (c_2(n+1))^2 + 1] + x_3(n)[c_3(n)c_3(n+2) - (c_3(n+1))^2 + 1]$$

ОБ ОДНОМ СПОСОБЕ ВЫБОРА ПАРАМЕТРА РЕГУЛЯРИЗАЦИИ ПРИ РЕШЕНИИ ОБРАТНОЙ ЗАДАЧИ В ОПТИКО- ЭЛЕКТРОННОЙ СИСТЕМЕ ДИСТАНЦИОННОГО ЗОНДИРОВАНИЯ

Л.В. Дорошева

(МГПИ, г. Мозырь)

В математическом моделировании систем дистанционного зондирования [1-3] особый интерес представляет обратная задача: "восстановление" исходного изображения по результатам регистрации излучения бортовыми приборами космического аппарата. Математическая формулировка этой задачи сводится к интегральному уравнению первого рода

$$Au = f, u \in U, f \in F, \quad (1)$$

где u - искомая функция; f - известная функция (входные данные, т.е. регистрируемое излучение); A - линейный оператор преобразования $U \rightarrow F$; U и F - метрические пространства. Поскольку f - результат эксперимента и известен приближенно, задача (1) оказывается некорректной [4] и необходима регуляризация ее решения. Обычно полагают $F \subset L_2$; принадлежность U к конкретному функциональному пространству определяется порядком регуляризации [4].

Метод преобразований Фурье позволяет получить регуляризованное решение обратной задачи (1) в виде [4]

$$u_\alpha(x) = \frac{1}{(2\pi)^2} \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} \frac{\check{f}(\omega)\check{K}(\omega) \exp[i(\omega, x)]}{L(\omega) + \alpha M(\omega)} d\omega \quad (2)$$

где $L(\omega) = \check{K}(\omega)\check{K}(-\omega)$, $M(\omega) = M(-\omega)$, $M(\omega) > 0$ при $\omega \neq 0$; $\check{f}(\omega)$ и $\check{K}(\omega)$ - двумерные фурье-образы входной функции $f(x)$, $x = (x_1, x_2)$; $\omega = (\omega_1, \omega_2)$ и функции влияния (в оптике - рассеяния) точечного источника $K(x_1 - s_1, x_2 - s_2)$; $M(\omega)$ - регуляризирующая функция; $\alpha > 0$ - параметр регуляризации.

Данная работа посвящена разработке способа выбора параметра регуляризации и регуляризирующей функции на основе учета предельных "изобразительных" возможностей оптического звена ОЭС.

Пусть входные данные $\check{f}(x)$, описывающие некоторый ландшафт земной поверхности, имеет детерминированную и случайную составляющие. Будем полагать, что детерминированная составляющая $\check{f}(x)$ задана дискретно и аппроксимируется кусочно-постоянными функциями. Пусть составляющая $\check{f}(x)$ имеет резкий скачок в альbedo в направлении оси x_1 : $q(x_1) = \bar{q}$, если $x_1 < 0$, и $\bar{q}(x_1) = \bar{q} + \Delta q$, если $x_1 \geq 0$.

В силу разных причин возникают временные вариации альbedo и интенсивности света, попадающего на приемник излучения при $x_1 > 0$. Вдали от границы раздела областей с разными альbedo угловые отклонения направлений отраженного потока (строго говоря, - максимума индикатрисы отражения) во времени и в пределах апертурного угла усредняются. Вблизи границы скачка в поле зрения объектива будут попадать одновременно точки поверх-

ности с разными альбедами (\bar{q} и \tilde{q}); картина резкого перехода при $x_1 = 0$ окажется несколько размытой (аналогичные явления имеют место при учете статистических факторов зернистости фотоматериалов [7]). Для учета процесса размытия границы перехода без привлечения автокорреляционной функции и энергетического спектра случайной функции, введем "эффективную" функцию размытия линии $q(s)$. Это позволяет рассматривать результирующую функцию как свертку "эффективной" функции рассеяния с детерминированным сигналом $\tilde{f}(x)$:

$$\tilde{f}(x) = (q * \bar{f})(x) \quad (3)$$

Положим, следуя [8], $\tilde{q}(\omega) = F[q(s)]$ в виде $\tilde{q}(\omega) = \exp(-\alpha|\omega|)$.

Здесь в общем случае двумерного скачка $|\omega| = |\omega_1| + |\omega_2|$, а для аппроксимации функции "размытия точки" принята зависимость

$$q(s_1, s_2) = \left[\pi^2 \alpha^2 \left(1 + \frac{s_1^2}{\alpha^2} \right) \left(1 + \frac{s_2^2}{\alpha^2} \right) \right]^{-1}, \quad (4)$$

где параметр $\alpha > 0$ характеризует размер пятна рассеяния оптического звена.

В интерпретации (3) функции $\tilde{f}(x)$ задача (1) оказывается поставленной корректно, а ее решение может быть представлено в виде

$$\tilde{u}(x) = F^{-1} \left[\frac{\tilde{f}(\omega) \exp(-\alpha|\omega|)}{\bar{K}(\omega)} \right] \quad (5)$$

где F^{-1} - оператор обратного преобразования Фурье и учтено, что реальная ОЭС передает ограниченный спектр пространственных частот $|\omega| \in [0, \omega_n]$ (ω_n - предельная передаваемая частота) и в силу этого $1/|\bar{K}(\omega)| < \infty$. Как известно [4], регуляризирующая функция $\varphi(\alpha, \omega)$, в частности $\alpha M(\omega)$, должна удовлетворять определенным условиям. Нетрудно доказать, что $\exp(-\alpha|\omega|)$ удовлетворяет всем условиям, кроме $\forall \alpha > 0 \frac{\varphi(\alpha, \omega)}{\bar{K}(\omega)} \in L_2(-\infty, +\infty)$.

Рассмотрим это требование. Функция принадлежит пространству Лебега, если

$$\int_{-\infty}^{+\infty} \left| \frac{\varphi(\alpha, \omega)}{\tilde{K}(\omega)} \right|^2 d\omega < \infty \quad (6)$$

В [2] и [8, 9] предложены аппроксимации

$$|\tilde{K}(\omega)| = \sum_{k=1}^n a_k \exp(-b_k |\omega|), \quad (7)$$

где $b_k > 0$ для $\forall k$, а коэффициенты a_k и b_k в (7) выбираются такими, что $b_k \rightarrow \infty, a_k \rightarrow 0$ при $k \rightarrow \infty$. При $\omega \rightarrow \omega_n$ в (7) остается только одно слагаемое $a_1 \exp(-b_1 |\omega_n|)$. Условие (6) дает оценку параметра α при $\omega = \omega_n$

$$\alpha > 2b_1. \quad (8)$$

При условии (8) $\exp(-\alpha|\omega|)$ удовлетворяет всем требованиям к регуляризирующим функциям и, следовательно, (5) - регуляризирующий функционал. Функционал (5), как и (2), дает приближенное решение задачи (1) и, в общем случае, $u_\alpha(x) \neq \tilde{u}(x)$. Наложив условие $u_\alpha(x) = \tilde{u}(x)$ и, сравнивая (2) и (5), получим выражение для регуляризирующей функции:

$$M(\omega) = |\tilde{K}(\omega)|^2 \sum_{n=1}^{\infty} \alpha^{n-1} \frac{|\omega|^n}{n!} \approx |\tilde{K}(\omega)|^2 \sum_{m=0}^p \alpha^m \frac{|\omega|^{m+1}}{(m+1)!}, \quad (9)$$

где p - порядок регуляризации.

Функционалы (2) и (5) дают сглаженные решения задачи (1). Для ОЭС физически это означает потерю в решении информации о высших гармониках изображения, что эквивалентно расфокусировке оптической системы и потере разрешающей способности. Во избежание излишнего сглаживания в (9) целесообразно ограничиться регуляризацией, например, первого порядка. Тогда решение $\tilde{u} \in U$, а $U \subset W_2^1$ и $\tilde{u}(x)$ равномерно сходится к $u_\alpha(x)$ при $\alpha \rightarrow 0$.

При аппроксимации (7) для вычисления коэффициентов a_1 и b_1 удобно воспользоваться двумя опорными частотами: верхней $\omega^h = \omega_n$ и нижней $\omega^h = \omega_n/2$, что дает

$$b_1 \approx \frac{2}{\omega_n} \ln \left| \frac{\tilde{K}(\omega_n/2)}{\tilde{K}(\omega_n)} \right|.$$

Тогда для значения параметра α , согласованного с функцией $\tilde{K}(\omega)$, получаем оценочную зависимость

$$\alpha \approx \frac{4}{\omega_n} \ln \left| \frac{\check{K}(\omega_n/2)}{\check{K}(\omega_n)} \right|. \quad (10)$$

В ряде случаев известна не $\check{K}(\omega)$, а функция влияния $K(s)$. Аппроксимируя $K(s)$ функцией $q(x)$ из (5) и рассматривая $K(s)$ на уровне полуширины функции влияния, т.е. $K(s_0) = 1/2K(0)$, находим $\alpha = s_0$, где $2s_0$ - размер пятна рассеяния оптического звена на уровне $1/2$ высоты функции влияния.

Полученные зависимости для $M(\omega)$ и α позволяют уменьшить поле искомых значений параметра и, тем самым, сократить объем вычислений.

Литература.

1. Креков Г.М., Орлов В.М., Белов В.В., и др. Имитационное моделирование в задачах оптического дистанционного зондирования. Новосибирск: Наука, 1988. 185 с.
2. Сушкевич Т.А., Стрелков С.А., Иолтуховский А.А., Метод характеристик в задачах атмосферной оптики. М.: Наука, 1990. 296 с.
3. Росс Ю.К., Князихин Ю.В., Кууск А.Э. и др. Математическое моделирование переноса радиации в растительных средах. С.-П.: Гидрометеониздат, 1990. 198 с.
4. Тихонов А.Н., Арсенин В.Я. Методы решения некорректных задач. М.: Наука, 1974. 223 с.
5. Грынъ В.И. О двухшаговых итерационных методах регуляризации// Журн. вычисл. матем. и матем. физики, 1992. Т. 32. №11. С. 1821-1824.
6. Семенчева О.П., Смолик Ч.К. Решение одномерных интегральных уравнений первого рода типа свертки совместным применением метода регуляризации А.Н. Тихонова и метода экстраполяции// Весці АН БССР. 1990. №6. С. 117.
7. О'Нейл Э. Введение в статистическую оптику. М.: Мир, 1966. 254 с.

МЕТОД ПРОГОНКИ ДЛЯ ПЯТИДИАГОНАЛЬНОЙ МАТРИЦЫ

Н.А. Илючик, В. М. Мадорский

(БрГУ, г. Брест)

Рассмотрим краевую периодическую задачу Дуффинга:

$$x'' + \alpha x' + \beta x^m + \gamma x = F(\sin t, \cos t) \quad (1)$$

$$\alpha_1 x(a) + \beta_1 x'(a) = A_1, \quad (2)$$

$$\alpha_2 x(b) + \beta_2 x'(b) = A_2.$$

Заменив дифференциальную краевую задачу ее разностной аппроксимацией на сетке, получим систему нелинейных уравнений. При решении нелинейной системы квазиньютоновскими методами на каждой итерации необ-

ходимо решать линейную систему, матрица которой представляет собой матрицу Якоби системы нелинейных уравнений и является диагональной, причем количество диагоналей матрицы равно количеству точек, по которым были аппроксимированы производные. Если исходная матрица содержит n диагоналей, то при применении регуляризованных алгоритмов [1] используют матрицу, которая содержит $(2n-1)$ диагоналей.

Так как производная функции, как правило, изменяется более плавно, чем сама функция, то для расчетов мы можем использовать матрицу Якоби, которая бы получалась при аппроксимации производных по трём точкам, а функцию и производные, участвующие в задаче, будем аппроксимировать по большему количеству точек. Данный подход, насколько известно автору, на практике применяется впервые. При таком подходе мы практически не проигрываем в точности, но при этом можем очень значительно (на порядки) сократить количество операций, а значит и время решения задачи. Эта экономия возможна вследствие того, что матрица Якоби при таком подходе будет трехдиагональной, а матрица $\overline{f'(x_n)}f'(x_n)$ пятидиагональной, следовательно, при решении линейной системы мы можем использовать вместо метода Гаусса метод матричной прогонки, который учитывает специфику таких систем и является очень быстрым.

Метод трёхдиагональной прогонки достаточно широко освещен в литературе [2]. Гораздо больший интерес представляет метод пятидиагональной прогонки, которого нет в известной автору литературе.

Метод прогонки для пяти-диагональной матрицы

Пусть необходимо найти решение системы n линейных уравнений с n неизвестными, причем матрица системы имеет пяти-диагональный вид:

$$\left\{ \begin{array}{l} c_1x_1 + d_1x_2 + e_1x_3 = g_1, \\ b_2x_1 + c_2x_2 + d_2x_3 + e_2x_4 = g_2, \\ a_3x_1 + b_3x_2 + c_3x_3 + d_3x_4 + e_3x_5 = g_3, \\ \quad a_4x_2 + b_4x_3 + c_4x_4 + d_4x_5 + e_4x_6 = g_4, \\ \quad \quad a_5x_3 + b_5x_4 + c_5x_5 + d_5x_6 + e_5x_7 = g_5, \\ \dots \quad \dots \quad \dots \quad \dots \quad \dots \quad \dots \\ \quad \quad \quad a_{n-2}x_{n-4} + b_{n-2}x_{n-3} + c_{n-2}x_{n-2} + d_{n-2}x_{n-1} + e_{n-2}x_n = g_{n-2}, \\ \quad \quad \quad \quad a_{n-1}x_{n-3} + b_{n-1}x_{n-2} + c_{n-1}x_{n-1} + d_{n-1}x_n = g_{n-1}, \\ \quad \quad \quad \quad \quad a_nx_{n-2} + b_nx_{n-1} + c_nx_n = g_n. \end{array} \right. \quad (3)$$

Метод прогонки состоит из двух этапов – прямой прогонки и обратной.

1 этап: прямая прогонка

Прямая прогонка состоит в том, что каждое неизвестное x_i выражается через x_{i+1} и x_{i+2} с помощью прогоночных коэффициентов A_i, B_i, C_i :

$$x_i = A_i x_{i+1} + B_i x_{i+2} + C_i, \quad i=1, 2, \dots, n-2. \quad (4)$$

Из первого уравнения системы (3) найдём: $x_1 = -\frac{d_1}{c_1} x_2 - \frac{e_1}{c_1} x_3 + \frac{g_1}{c_1}$.

С другой стороны, в силу (4) $x_1 = A_1 x_2 + B_1 x_3 + C_1$. Приравняв коэффициенты в обоих выражениях для x_1 , имеем, $A_1 = -d_1/c_1, B_1 = -e_1/c_1, C_1 = g_1/c_1$.

Выразим из второго уравнения системы (3) x_2 , заменяя x_1 по формуле (4):

$$\begin{aligned} x_2 &= -\frac{b_2}{c_2} x_1 - \frac{d_2}{c_2} x_3 - \frac{e_2}{c_2} x_4 + \frac{g_2}{c_2} = -\frac{b_2}{c_2} (A_1 x_2 + B_1 x_3 + C_1) - \frac{d_2}{c_2} x_3 - \frac{e_2}{c_2} x_4 + \frac{g_2}{c_2} = \\ &= -\frac{b_2}{c_2} A_1 x_2 - \frac{b_2}{c_2} B_1 x_3 - \frac{b_2}{c_2} C_1 - \frac{d_2}{c_2} x_3 - \frac{e_2}{c_2} x_4 + \frac{g_2}{c_2}. \end{aligned}$$

Приводя подобные слагаемые, имеем выражение для x_2 :

$$x_2 = -\frac{b_2 B_1 + d_2}{(c_2 + b_2 A_1)} x_3 + \frac{g_2 - b_2 C_1}{(c_2 + b_2 A_1)}.$$

Отсюда получаем прогоночные коэффициенты для x_2 :

$$A_2 = -\frac{b_2 B_1 + d_2}{(c_2 + b_2 A_1)}, \quad B_2 = -\frac{e_2}{(c_2 + b_2 A_1)}, \quad C_2 = \frac{g_2 - b_2 C_1}{(c_2 + b_2 A_1)}.$$

Аналогично можно вычислить прогоночные коэффициенты для любого номера i : $A_i = \frac{-a_i A_{i-2} B_{i-1} - b_i B_{i-1} - d_i}{p_i}, B_i = -\frac{e_i}{p_i}, C_i = \frac{-a_i (A_{i-2} C_{i-1} + C_{i-2}) - b_i C_{i-1} + g_i}{p_i}$, где

$$p_i = c_i + a_i (A_{i-2} A_{i-1} + B_{i-2}) + b_i A_{i-1}, \quad i=3, 4, \dots, n-2.$$

2 этап: обратная прогонка

Обратная прогонка состоит в последовательном вычислении неизвестных x_i . Воспользуемся формулой (4) при $i=n-2$ и последним уравнением системы (3).

$$\begin{aligned} x_{n-2} &= A_{n-2} x_{n-1} + B_{n-2} x_n + C_{n-2} \\ a_n x_{n-2} + b_n x_{n-1} + c_n x_n &= g_n. \end{aligned}$$

Подставив первое уравнение во второе, получим:

$$(a_n A_{n-2} + b_n) x_{n-1} + (a_n B_{n-2} + c_n) x_n = g_n - a_n C_{n-2} \quad (5)$$

Рассмотрим предпоследнее уравнение системы:

$$a_{n-1}x_{n-3} + b_{n-1}x_{n-2} + c_{n-1}x_{n-1} + d_{n-1}x_n = g_{n-1}$$

Заменяя в этом уравнении x_{n-3} , x_{n-2} по формуле (4), имеем:

$$(a_{n-1}A_{n-3} + b_{n-1})(A_{n-2}x_{n-1} + B_{n-2}x_n + C_{n-2}) + (a_{n-1}B_{n-3} + c_{n-1})x_{n-1} + d_{n-1}x_n = g_{n-1} - a_{n-1}C_{n-3}$$

Обозначим $s = a_{n-1}A_{n-3} + b_{n-1}$, тогда последнее равенство переписется в

$$\text{виде: } s(A_{n-2}x_{n-1} + B_{n-2}x_n + C_{n-2}) + (a_{n-1}B_{n-3} + c_{n-1})x_{n-1} + d_{n-1}x_n = g_{n-1} - a_{n-1}C_{n-3}$$

$$(sA_{n-2} + a_{n-1}B_{n-3} + c_{n-1})x_{n-1} + (sB_{n-2} + d_{n-1})x_n = g_{n-1} - a_{n-1}C_{n-3} - sC_{n-2} \quad (6)$$

Таким образом, используя (5) и (6), получили систему из двух уравнений с двумя неизвестными:

$$\begin{cases} (a_n A_{n-2} + b_n)x_{n-1} + (a_n B_{n-2} + c_n)x_n = g_n - a_n C_{n-2} \\ (sA_{n-2} + a_{n-1}B_{n-3} + c_{n-1})x_{n-1} + (sB_{n-2} + d_{n-1})x_n = g_{n-1} - a_{n-1}C_{n-3} - sC_{n-2} \end{cases}$$

Вводя обозначения: $A_{n-1} = a_n A_{n-2} + b_n$, $B_{n-1} = a_n B_{n-2} + c_n$, $C_{n-1} = g_n - a_n C_{n-2}$

$$A_n = sA_{n-2} + a_{n-1}B_{n-3} + c_{n-1}, \quad B_n = sB_{n-2} + d_{n-1}, \quad C_n = g_{n-1} - a_{n-1}C_{n-3} - sC_{n-2}$$

получим, что последняя система запишется в виде:

$$\begin{cases} A_{n-1}x_{n-1} + B_{n-1}x_n = C_{n-1} \\ A_n x_{n-1} + B_n x_n = C_n \end{cases}$$

$$\text{Найдём отсюда } x_{n-1}, x_n: x_{n-1} = \frac{C_{n-1} - B_{n-1}x_n}{A_{n-1}}, x_n = \frac{C_n A_{n-1} - A_n C_{n-1}}{B_n A_{n-1} - B_{n-1} A_n}$$

Далее, используя формулу (4) и найденные на первом этапе значения прогоночных коэффициентов, последовательно вычисляем все неизвестные $x_{n-2}, x_{n-3}, \dots, x_1$.

Подсчёт числа операций умножения и деления.

Нетрудно подсчитать число действий умножения и деления, необходимых для решения системы (3) с помощью метода прогонки. Получим, что при реализации метода прогонки для пяти-диагональной матрицы выполняется $14n$ операций умножения и деления. Для сравнения отметим, что при использовании метода Гаусса число действий умножения и деления близко к $2n^3/3$. Естественно, если матрица системы позволяет использовать метод прогонки, то следует использовать именно его.

Литература.

1. Ермаков В.В., Калиткин Н.Н. Оптимальный шаг и регуляризация в методе Ньютона. // Журнал «Вычисл. матем. и матем. физ.», 1981, Т.21, №2, с.491—497.
2. Самарский А.А., Гулин А.В. Численные методы.—М.: Наука, 1989.—432с.

СТОХАСТИЧЕСКИЕ УРАВНЕНИЯ В θ -ИНТЕГРАЛАХ В АЛГЕБРЕ ОБОБЩЕННЫХ СЛУЧАЙНЫХ ПРОЦЕССОВ.

А.Н. Ковальчук

(БГПУ г. Минск)

Современная теория стохастических дифференциальных уравнений базируется на понятиях стохастических интегралов. Наиболее общий среди них — стохастический θ -интеграл, где параметр θ принадлежит отрезку $[0; 1]$ ([1], с.192). Для исследования решений таких уравнений разработана специальная теория (см., напр., [2]).

Аппроксимациями решений стохастических дифференциальных уравнений занимались многие авторы. Как правило, решения уравнений Ито приближаются решениями соответствующих конечно-разностных уравнений, а решения уравнений Стратоновича — решениями обыкновенных дифференциальных уравнений. В работе [3] установлено, что решения стохастических уравнений в θ -интегралах могут быть приближены решениями конечно-разностных уравнений с осреднением.

В сообщении [4] введен новый класс стохастических θ -интегралов, в котором параметр θ принадлежит всей вещественной прямой \mathbf{R} . Данная статья посвящена задаче аппроксимации стохастических интегралов и решений стохастических уравнений в θ -интегралах именно для такого случая. В ней дается полное описание предельного поведения конечных сумм с осреднением для процесса броуновского движения, приводятся необходимые и достаточные условия сходимости решений конечно-разностных уравнений с осреднением к решениям стохастических уравнений в θ -интегралах, $\theta \in \mathbf{R}$. Найдены также оценки скорости сходимости.

Пусть $(\Omega, \mathcal{A}, \mathcal{P})$ — полное вероятностное пространство, $T = [0, a] \subset \mathbf{R}$, $\{F_t\}_{t \in T}$ — стандартный, непрерывный справа поток σ -алгебр и $B(t)$ — стандартный одномерный процесс F_t -броуновского движения ([5], с.48). В качестве представителя обобщенного случайного процесса броуновского движения будем рассматривать

$$B_n(t) = (B^* \rho_n)(t) = \int_0^{1/n} B(t+s) \rho_n(s) ds, \quad (1)$$

где $\rho_n(t) \in D(\mathbf{R})$, $\text{supp } \rho_n(t) \subset [0, 1/n]$, $\int_0^{1/n} \rho_n(s) ds = 1$ и существует $A \in \mathbf{R}$ такое, что $\int_0^{1/n} |\rho_n(s)| ds \leq A$, для любого $n=1, 2, 3, \dots$

Лемма 1. Пусть $t \geq 0$, $h_n > 0$, $n \in \mathbf{N}$, тогда имеет место следующее равенство $E(B_n(t+h_n) - B_n(t))^2 = h_n \iint_{\substack{0 \leq s, \tau \leq 1/n \\ |s-\tau| \leq h_n}} (1 - \frac{|s-\tau|}{h_n}) \rho_n(s) \rho_n(\tau) ds d\tau = h_n K(n, h_n)$.

В качестве представителя обобщенной функции \tilde{f} , ассоциирующей функцию $f: \mathbf{R} \rightarrow \mathbf{R}$, рассмотрим следующую последовательность $f_n = f * \rho_n$, где ρ_n из выражения (1).

Следующие теоремы дают полную классификацию способов аппроксимации стохастических θ -интегралов, где $\theta \in \mathbf{R}$ по броуновскому движению в сверточной алгебре.

Теорема 1. Пусть $f \in C_B^1(\mathbf{R})$, $f \neq 0$ и точка $\bar{B}_n(\tau_i + (k-1)h_n)$ лежит на отрезке, соединяющем точки $B_n(\tau_i + kh_n)$ и $B_n(\tau_i + (k-1)h_n)$, $k=1 \dots m_i$. Тогда конечная сумма $\sum_{k=1}^{m_i} f_n(\bar{B}_n(\tau_i + (k-1)h_n)) [B_n(\tau_i + kh_n) - B_n(\tau_i + (k-1)h_n)]^2$ сходится в $L^2(\Omega, A, P)$ и равно-мерно по $t \in T$ при $n \rightarrow \infty$, $h_n \rightarrow 0$ тогда, и только тогда, когда числовая последовательность $K(n, h_n)$ сходится при $n \rightarrow \infty$, $h_n \rightarrow 0$.

Теорема 2. Пусть $f \in C_B^2(\mathbf{R})$, $f \neq \text{const}$. Конечная сумма $\sum_{k=1}^{m_i} f_n(B_n(\tau_i + (k-1)h_n)) \times [B_n(\tau_i + kh_n) - B_n(\tau_i + (k-1)h_n)]$ сходится в $L^2(\Omega, A, P)$ и равномерно по $t \in T$ при $n \rightarrow \infty$, $h_n \rightarrow 0$ тогда, и только тогда, когда числовая последовательность $K(n, h_n)$ сходится при $n \rightarrow \infty$, $h_n \rightarrow 0$.

Теорема 3. Пусть $f \in C_B^2(\mathbf{R})$ и $\theta \in (-\infty; 1/2]$. Тогда выполняется следующее неравенство $\sup_{t \in T} E(\sum_{k=1}^{m_i} f_n(B_n(\tau_i + (k-1)h_n)) [B_n(\tau_i + kh_n) - B_n(\tau_i + (k-1)h_n)] - (\theta) \int_{\tau_i}^t f(B(s)) dB(s))^2 \leq Ch_n + C/n + C((1-K(n, h_n))/2 - \theta)^2$

Теорема 4. Пусть $f \in C_B^2(\mathbf{R})$, $f \neq \text{const}$. Конечная сумма $\sum_{k=1}^{m_i} f_n(B_n(\tau_i + kh_n)) \times [B_n(\tau_i + kh_n) - B_n(\tau_i + (k-1)h_n)]$ сходится в $L^2(\Omega, A, P)$ и равномерно по $t \in T$ при

$n \rightarrow \infty, h_n \rightarrow 0$ тогда, и только тогда, когда числовая последовательность $K(n, h_n)$ сходится при $n \rightarrow \infty, h_n \rightarrow 0$.

Рассмотрим стохастическое уравнение в θ -интегралах

$$X(t) = x + (\theta) \int_0^t f(X(s)) dB(s) + \int_0^t g(X(s)) ds, \quad t \in T, \quad (2)$$

где $f \in C_B^2(\mathbf{R}), g \in C_B^1(\mathbf{R})$, интеграл в правой части (2) стохастический θ -интеграл, $\theta \in \mathbf{R}$.

Решение данного уравнения будем аппроксимировать решением следующей задачи Коши:

$$\begin{cases} X_n(t+h_n) - X_n(t) = f_n(X_n(t))[B_n(t+h_n) - B_n(t)] + g_n(X_n(t))h_n, \\ X_n(t)|_{[0, h_n]} = X_{n0}(t), \quad t \in T, \end{cases} \quad (3)$$

где случайный процесс $X_{n0}(t), t \in [0; h_n]$ является $F_{t+1/n}$ -измеримым и лежит в $L^2(\Omega, A, P)$

Теорема 5. Пусть $\theta \in (-\infty; 1/2]$, $f \in C_B^2(\mathbf{R})$ и $g \in C_B^1(\mathbf{R})$, "начальное условие" задачи Коши (3) $X_{n0}(t)$ принадлежит $L^2(\Omega, A, P)$ и является $F_{t+1/n}$ измеримым для любых $t \in [0; h_n]$. Тогда для решения задачи Коши (3) $X_n(t)$ и решения уравнения (2) $X(t)$ справедливы следующие неравенства:

$$\sup_{t \in T} E[X_n(t) - X(t)]^2 \leq C \sup_{t \in [0, h_n]} E[X_{n0}(t) - x]^2 + C/(n^{2/3} h_n^{1/3}) + C(K(n, h_n) - (1 - 2\theta))^2$$

Теорема 6. Пусть $\theta \in (-\infty; 1/2]$, $f \in C_B^2(\mathbf{R})$ и $g \in C_B^1(\mathbf{R})$. Если $n \rightarrow \infty, h_n \rightarrow 0$ так, что $1/n^2 = o(h_n)$, причем $\sup_{t \in [0, h_n]} E[X_{n0}(t) - x]^2 \rightarrow 0$, то для сходимости последовательности $X_n(t)$ решений задачи Коши (3) в $L^2(\Omega, A, P)$ и равномерно по $t \in T$ необходимо и достаточно, чтобы сходилась числовая последовательность $K(n, h_n)$.

Чтобы получить аналогичные теоремы для уравнения (2) в случае, когда $\theta \in [1/2; +\infty)$ рассмотрим следующую задачу Коши с опережением

$$\begin{cases} X_n(t+h_n) - X_n(t) = f_n(X_n(t+h_n))[B_n(t+h_n) - B_n(t)] + g_n(X_n(t))h_n, \\ X_n(t)|_{[0, h_n]} = X_{n0}(t), \quad t \in T, \end{cases} \quad (4)$$

Теорема 7. Пусть $\theta \in [1/2; \infty)$, $f \in C_B^2(\mathbf{R})$ и $g \in C_B^1(\mathbf{R})$, "начальное условие" задачи Коши (4) $X_{n0}(t)$ принадлежит $L^2(\Omega, A, P)$ и является $F_{t+1/n}$ измеримым

для любых $t \in [0; h_n]$. Тогда для решений задачи Коши (4) $X_n(t)$ и решения уравнения (2) $X(t)$ справедливы следующие неравенства:

$$\sup_{t \in T} E[X_n(t) - X(t)]^2 \leq C \sup_{t \in (0, h_n)} E[X_{n0}(t) - x]^2 + C/(n^{2/3} h_n^{1/3}) + C(K(n, h_n) - (2\theta - 1))^2$$

Теорема 8. Пусть $\theta \in [1/2; \infty)$, $f \in C_B^2(\mathbf{R})$ и $g \in C_B^1(\mathbf{R})$. Если $n \rightarrow \infty$, $h_n \rightarrow 0$ так, что $1/n^2 = o(h_n)$, причем $\sup_{t \in (0, h_n)} E[X_{n0}(t) - x]^2 \rightarrow 0$, то для сходимости последовательности $X_n(t)$ решений задачи Коши (4) в $L^2(\Omega, A, P)$ и равномерно по $t \in T$ необходимо и достаточно, чтобы сходилась числовая последовательность $K(n, h_n)$.

Литература

1. В.С. Пугачев, И.Н. Синицын. Стохастические дифференциальные системы. Анализ и фильтрация. М.: Наука, 1990. 630 с.
2. И.И. Гихман, А.В. Скороход. Стохастические дифференциальные уравнения и их приложения. Киев. Наукова думка, 1982. 611 с.
3. Лазакевич Н.В., Яблонский О.Л. О приближении решений одного класса стохастических уравнений // Сиб. матем. журнал – 2001. – Т. 42, №1. – С.87-102
4. Ковальчук А.Н., Лазакевич Н.В., Лаппо Д.П. Новые классы стохастических интегралов. // AMADE-2001: Тез. докл. межд. мат. конф., Минск, 15 – 20 февраля 2001 г. – Минск, 2001. – С. 84-85.
5. С. Ваганабз, Н. Икзда. Стохастические дифференциальные уравнения и диффузионные процессы. М.: Наука, 1986. 448 с.

СРАВНИТЕЛЬНАЯ ХАРАКТЕРИСТИКА СПОСОБОВ АППРОКСИМАЦИИ РАЗНОСТНЫХ РЕШЕНИЙ ЗАДАЧИ ДУФФИНГА

А.В. Кот

(БрГУ, г. Брест)

Рассмотрим уравнение Дуффинга

$$\ddot{x}(t) + \alpha \dot{x}(t) + \beta x(t) + \gamma x^3(t) = F(\sin t, \cos t) \quad (1)$$

с краевыми условиями

$$x(0) = x(2\pi), \quad x'(0) = x'(2\pi), \quad (2)$$

где $x(t) - 2\pi$ - периодическая дважды дифференцируемая по t функция.

Разобьем отрезок $[0, 2\pi]$ на N частичных отрезков точками t_i ($i = \overline{0, N}$). Аппроксимируем первую и вторую производную в дифференциальном уравнении (1) линейными комбинациями значений $x(t_i)$ ($i = \overline{0, N}$) следующим образом

$$\dot{x}(t_i) = \sum_{j=0}^{N_A} c_j^1 x(t_{i+j-1}), \quad (3)$$

$$\ddot{x}(t_i) = \sum_{j=0}^{N_A} c_j^2 x(t_{i+j-1}), \quad (4)$$

где N_A – количество точек аппроксимации функции, а l – номер точки, по которой производится аппроксимация. Заметим, что наиболее точно производная будет аппроксимирована в случае, когда $l = \left[\frac{N_A}{2} \right]$.

Значения коэффициентов c_j^1 и c_j^2 ($j = \overline{0, N}$) определяем с помощью метода неопределенных коэффициентов, как показано в [1]. При этом решается следующая система линейных уравнений:

$$\begin{cases} c_0 + c_1 + \dots + c_n = 0, \\ c_0 t_0 + c_1 t_1 + \dots + c_n t_n = 0, \\ \dots \\ c_0 t_0^{k-1} + c_1 t_1^{k-1} + \dots + c_n t_n^{k-1} = 0, \\ c_0 t_0^k + c_1 t_1^k + \dots + c_n t_n^k = k!, \\ c_0 t_0^{k+1} + c_1 t_1^{k+1} + \dots + c_n t_n^{k+1} = \frac{(k+1)!}{2!} t_i, \\ c_0 t_0^{k+2} + c_1 t_1^{k+2} + \dots + c_n t_n^{k+2} = \frac{(k+2)!}{2!} t_i^2, \\ \dots \\ c_0 t_0^n + c_1 t_1^n + \dots + c_n t_n^n = \frac{n!}{(n-k)!} t_i^{n-k}, \end{cases}$$

где n – количество точек аппроксимации производной, а k – порядок производной.

Осуществляя, таким образом, дискретизацию задачи (1) – (2), получим систему нелинейных уравнений вида

$$\begin{cases} \sum_{j=0}^n c_j^2 x_{i+j} + \alpha \sum_{j=0}^n c_j^1 x_{i+j} + \beta x_i + \gamma x_i^3 - F(\sin t_i, \cos t_i) = 0, \quad i = \overline{0, N-1}, \\ x_0 - x_N = 0. \end{cases} \quad (5)$$

Решив полученную систему нелинейных уравнений (5) одним из методов, рассмотренных в [2], получим значения x_i , которые являются численным решением дифференциальной задачи (1) – (2) в системе точек t_i ($i = \overline{0, N}$).

Часто вместо решения в численном виде выгоднее иметь его представление в аналитическом виде. Для этого можно воспользоваться следующими способами аппроксимации решения:

1. С помощью полинома Ньютона

$$x(t) = x_0 + (t-t_0)x(t_0, t_1) + \dots + (t-t_0)(t-t_1)\dots(t-t_{n-1})x(t_0, t_1, \dots, t_n),$$

где $x(t_0, t_1, \dots, t_n)$ – разностное отношение n -го порядка функции $x(t)$.

2. С помощью ряда Фурье

$$x(t) = \frac{a_0}{2} + \sum_{n=1}^{N_G} \left(a_n \cos \frac{\pi n t}{l} + b_n \sin \frac{\pi n t}{l} \right),$$

где N_G – количество гармоник ряда Фурье, а $l = \frac{\pi}{\omega}$ – полупериод функции $x(t)$.

Коэффициенты a_n и b_n можно вычислить, используя, например, квадратурные формулы трапеций:

$$a_0 = \frac{2}{N} \sum_{i=0}^{N-1} (x_i + x_{i+1}),$$

$$a_n = \frac{2}{N} \sum_{i=0}^{N-1} \left(x_i \cos \frac{4\pi n i}{N} + x_{i+1} \cos \frac{4\pi n (i+1)}{N} \right),$$

$$b_n = \frac{2}{N} \sum_{i=0}^{N-1} \left(x_i \sin \frac{4\pi n i}{N} + x_{i+1} \sin \frac{4\pi n (i+1)}{N} \right).$$

3. С помощью кубического сплайна [3]

$$s(t) = x_i + \left(\frac{x_{i+1} - x_i}{h} - \frac{h}{6}(2m_i + m_{i+1}) \right) (t - t_i) + \frac{m_i}{2} (t - t_i)^2 + \frac{m_{i+1} - m_i}{6h} (t - t_i)^3,$$

где $m_i = \ddot{x}(t_i)$ – коэффициенты сплайна, которые можно вычислять стандартным способом, решая следующую систему линейных уравнений:

$$m_{i-1} + 4m_i + m_{i+1} = 12x(t_{i-1}, t_i, t_{i+1}), \quad i = \overline{1, N-1}, \quad (6)$$

где $x(t_{i-1}, t_i, t_{i+1})$ – вторая разделенная разность функции $x(t)$.

Система уравнений (6) – это система $N-1$ линейных алгебраических уравнений относительно $N+1$ неизвестных m_i , $i = \overline{1, N-1}$. Недостающие два уравнения можно получить из следующих соображений:

Так как функция $x(t)$ – периодическая, то $m_0 = m_N$ и $m_{N+1} = m_1$. В этом случае систему (6) удобно решать методом прогонки.

Предположим, что на концах отрезка функция $x(t)$ имеет нулевую кривизну, т.е. $\ddot{x}(t_0) = m_0 = 0$ и $\ddot{x}(t_N) = m_N = 0$. В этом случае система (6) также решается методом прогонки.

Заметим, что коэффициенты m_i ($i = \overline{1, N-1}$) можно вычислять, используя формулы (4). При этом нет необходимости в решении системы линейных уравнений (6), т.к. все коэффициенты вычисляются напрямую.

Как показал опыт, лучшим методом для определения коэффициентов m_i является именно последний метод.

4. С помощью естественного периодического сплайна n -ой степени [4]

$$S(t) = x_0 + \sum_{k=0}^m a_k (t - t_0)^k + \sum_{n=1}^{N-1} b_n (t - t_n)_+^m, \quad (7)$$

$$\text{где } \varphi_+ = \frac{1}{2}(\varphi + |\varphi|) = \begin{cases} \varphi, & \text{если } \varphi > 0, \\ 0, & \text{если } \varphi \leq 0. \end{cases}$$

Коэффициенты a_k и b_k сплайна получаем, решая следующую систему линейных уравнений

$$\begin{cases} \sum_{k=0}^m a_k (t_p - t_0)^k + \sum_{n=1}^{p-1} b_n (t_p - t_n)^m = x_p - x_0, & p = \overline{1, N}, \\ \sum_{k=p}^m \frac{k!}{(k-p)!} a_k (t_N - t_0)^{k-p} + \frac{m!}{(m-p)!} \sum_{n=1}^{N-1} b_n (t_N - t_n)^{m-p} = p! a_p, \\ p = \overline{0, m-1}. \end{cases} \quad (8)$$

Заметим, что система (8) плохо обусловлена. В связи с этим вместо системы (8) вида $AX = B$ на практике лучше решать систему вида $(\alpha E + A^T A)X = A^T B$, $\alpha > 0$, $\alpha \ll 1$.

После того, как решение записано в аналитическом виде, его можно подставить в дифференциальную задачу (1) – (2) и оценить полученную погрешность.

При этом погрешность можно оценить либо только в узлах исходной сетки, либо на всем отрезке $[0, 2\pi]$ в норме L_2 . Очевидно, что второй способ предпочтительнее в связи с его большей строгостью.

Как показал вычислительный эксперимент, лучшими оказались методы аппроксимации решения с помощью кубического сплайна и естественного периодического сплайна невысокой степени.

Литература.

1. И.С. Березин, Н.П. Житков. Методы вычислений, т. 1. — М.: Наука, 1966.
2. В.Л. Макаров, В.В. Хлобыстов. Сплайн-аппроксимация функций: Учеб. пособие для студентов вузов. — М.: Высш. шк., 1983.

О ГЕОМЕТРИЧЕСКИХ ХАРАКТЕРИСТИКАХ ОДНОМЕРНЫХ ПОДГРУПП ГРУППЫ G ВРАЩЕНИЙ ПРОСТРАНСТВА 2R_4 .

О.Н. Курочка
(БрГУ, г.Брест)

Классификация связных подгрупп Ли группы G имеется. При классификации применялся метод линеаризации, т.е. классифицировались подалгебры алгебры \mathfrak{g} с точностью до сопряженности. Поэтому задача состоит в выделении из подгрупп группы G таких, которые имеют образ стационарности из обобщенных флагов. Следовательно, надо уметь находить плоскости и векторные подпространства, инвариантные относительно данной подгруппы, а затем выделить те, которые образуют образ стационарности. Для решения этой задачи опять применим метод линеаризации.

Для нахождения одномерных инвариантных подпространств получаем следующее матричное уравнение $X \cdot C = \lambda X$, где X -произвольный элемент из 2E_4 , а C - произвольный элемент из алгебры Ли исследуемой подгруппы.

Для нахождения двумерных инвариантных подпространств получаем систему: $X \cdot C = \lambda X + \mu Y$, $Y \cdot C = \nu X + \sigma Y$.

Получили следующие результаты. Подпространства, инвариантные относительно G_1 с алгеброй $\mathfrak{g}_1 = \{i_{10}\}$, имеют вид: $\{i_1\}$, $\{i_1, i_2\}$, $\{i_3, i_4\}$, $\{i_1, i_3, i_4\}$, 2E_4 . Относительно G_2 с алгеброй $\mathfrak{g}_2 = \{i_5\}$: $\{\lambda i_3 + \mu i_4\}$, $\{i_1, i_2\}$, $\{i_3, i_4\}$, $\{i_1, i_2, \lambda i_3 + \mu i_4\}$, 2E_4 . Относительно G_3 с алгеброй $\mathfrak{g}_3 = \{i_6\}$: $\{i_1 \pm i_3\}$, $\{\lambda i_2 + \mu i_4\}$, $\{i_1 \pm i_3, \lambda i_2 + \mu i_4\}$, $\{i_1, i_3\}$, $\{i_2, i_4\}$, $\{i_1 \pm i_3, i_2, i_4\}$, $\{\lambda i_2 + \mu i_4, i_1, i_3\}$, 2E_4 . Относительно G_4 с алгеброй $\mathfrak{g}_4 = \{i_8 - i_{10}\}$: $\{\lambda i_1 + \mu(i_2 - i_4)\}$, $\{i_2 - i_4, \lambda i_1 + \mu i_3\}$, $\{\lambda i_1 + \mu(i_2 - i_4)\}^\perp$, 2E_4 . Относительно G_5 с алгеброй $\mathfrak{g}_5 = \{i_5 - i_7\}$: $\{\lambda(i_2 - i_4) + \mu i_3\}$, $\{i_2 - i_4, \lambda i_1 + \mu i_3\}$, $\{\lambda(i_2 - i_4) + \mu i_3\}^\perp$, 2E_4 . Относительно G_6 с алгеброй $\mathfrak{g}_6 = \{i_5 - i_7 - i_8 + i_{10}\}$: $\{\lambda(i_1 + i_3) + \mu(i_2 - i_4)\}$, $\{\nu(i_1 + i_3) - \lambda(i_2 - i_4), \lambda i_1 - (1 + \nu)i_2 + i_4\}$, $\{i_1 - \lambda i_2, i_2 - i_4 + \lambda(i_1 + i_3)\}$, $\{i_2 - i_4, \lambda i_1 + \mu i_3\}$, $\{i_1 + i_3, \lambda i_2 + \mu i_4\}$, $\{\lambda(i_1 + i_3) + \mu(i_2 - i_4)\}^\perp$, 2E_4 . Относительно G_7 с алгеброй $\mathfrak{g}_7 = \{i_5 + i_{10}\}$: $\{i_1 + i_2\}$, $\{i_3 - \lambda i_1 - \mu i_2, i_4 + \mu i_1 + \lambda i_3\}$, 2E_4 . Относительно G_8 с алгеброй $\mathfrak{g}_8 = \{i_6 - i_9\}$:

$\{\lambda(i_1 \pm i_3) + \mu(i_2 \mp i_4)\}$, $\{i_4 + \lambda i_1 + \mu i_2, i_2 - \lambda i_3 + \mu i_4\}$, $\{i_2 \pm i_4, \pm i_1 + \lambda i_2 + i_3\}$, $\{i_2 - i_4, i_1 \pm i_3\}$, $\{i_2 + i_4, i_1 \pm i_3\}$, $\{i_4 + \lambda i_3, i_2 - \lambda i_1\}$, $\{\lambda(i_1 \pm i_3) + \mu(i_2 \mp i_4)\}^\perp$, $\{i_1, i_3\}$, $\{i_2, i_4\}$, 2E_4 . Относительно G_9 с алгеброй $\mathfrak{g}_9 = \{i_5 + \lambda i_{10}, \lambda \neq 0, \pm 1: \{i_1, i_2\}, \{i_3, i_4\}, {}^2E_4$. Относительно G_{10} с алгеброй $\mathfrak{g}_{10} = \{i_6 + \lambda i_9, \lambda \neq 0, \pm 1: \{i_1 \pm i_3\}, \{i_2 \pm i_4\}, \{i_1, i_3\}, \{i_2, i_4\}, \{i_1 + i_3, i_2 \pm i_4\}, \{i_1 - i_3, i_2 \pm i_4\}, \{i_1 \pm i_3, i_2, i_4\}, \{i_2 \pm i_4, i_1, i_3\}, {}^2E_4$. Относительно G_{11} с алгеброй $\mathfrak{g}_{11} = \{i_5 - i_7 + i_8 - i_{10} + 2i_6 - 2i_9\}: \{i_1 - i_3\}, \{i_2 - i_4\}, \{i_1 \pm i_3, i_2 - i_4\}, \{i_1 - i_3, i_2, i_4\}, \{i_2 - i_4, i_1, i_3\}, {}^2E_4$. Относительно G_{12} с алгеброй $\mathfrak{g}_{12} = \{i_6 - i_9 + \lambda(i_5 - i_7)\}, \lambda \neq 0: \{i_2 - i_4\}, \{i_1 \pm i_3, i_2 - i_4\}, {}^2E_4$. Относительно G_{13} с алгеброй $\mathfrak{g}_{13} = \{i_5 + i_7 + i_8 - 3i_{10}\}: \{i_1 + i_3, i_2 - i_4\}, {}^2E_4$.

ОДНОКРАТНО ЗАМЫКАЕМЫЕ ОПТИМАЛЬНЫЕ

ОБРАТНЫЕ СВЯЗИ

Л.И. Лавринович

(БГУ, г. Минск)

Пусть $T = [t_*, t^*]$, $t_* < t^* < +\infty$, — промежуток управления, N — натуральное число, $h = (t^* - t_*)/N$ — промежуток квантования, $T_h = \{t_*, t_* + h, \dots, t^* - h\}$ — квантованный промежуток управления. Скалярную функцию $u(t)$, $t \in T$, назовем дискретным управлением с периодом квантования h , если $u(t) = u(t_* + kh)$, $t \in [t_* + kh, t_* + (k+1)h]$, $k = \overline{0, N-1}$.

В классе дискретных управлений рассмотрим линейную задачу оптимального управления

$$c'x(t^*) \rightarrow \max,$$

$$x = A(t)x + b(t)u + w(t), \quad x(t_*) = x_0,$$

$$x(t^*) \in X^* = \{x \in R^n: g_* \leq Hx \leq g^*\}, \quad (1)$$

$$w(t) \in W = \{w \in R^n: w_* \leq w \leq w^*\},$$

$$u(t) \in U = \{u \in R: |u| \leq 1\}, \quad t \in T.$$

Здесь $x = x(t)$ — n -вектор состояния системы управления в момент времени t , $u = u(t)$ — значение скалярного управляющего воздействия, $w(t)$ — n -вектор возмущения, $A(t)$, $b(t)$, $t \in T$, — $n \times n$ -матричная и n -векторная кусочно-непрерывные функции соответственно, $H \in R^{m \times n}$.

Будем предполагать, что 1) в процессе управления может реализоваться любое кусочно-непрерывное возмущение $w(t) \in W$, $t \in T$; 2) в каждый текущий

момент $t \in T_h$ будет известно состояние системы $x(t)$; 3) до начала процесса управления известно, что в некоторый наперед заданный момент замыкания t^1 , будут доступны значения $x(t^1)$.

Требуется построить такое управление, чтобы 1) система в момент времени t^1 попала на множество X^* , независимо от реализовавшегося возмущения; 2) гарантированное значение критерия качества задачи (1) было наибольшим.

Для простоты обозначений положим $t^* = t^0$, $t^1 = t^2$, $X^2 = X^*$. Определим множество X^1 (множество замыкания) по множеству X^2 следующим образом: $z \in X^1$ тогда и только тогда, когда система с помощью допустимого управления $u(t) \in U$, $t \in [t^1, t^2[$, из состояния $x(t^1) = z$ переводится в момент t^2 на множество X^2 , независимо от реализовавшегося возмущения $w(t) \in W$, $t \in [t^1, t^2[$. Аналогичным образом по множеству X^1 определим множество X^0 , как множество всех начальных состояний, из которых система в момент времени t^1 может быть переведена на множество X^1 . Очевидно, задача (1) имеет допустимые управления в том и только том случае, если $x_0 \in X^0$.

Пусть τ — произвольный текущий момент. Обозначим $u^0(t | \tau, z)$, $t \in [\tau, t^1]$, — оптимальное программное управление в задаче

$$\begin{aligned} c'x(t^2) &\rightarrow \max, \\ x &= A(t)x + b(t)u + w(t), \quad x(\tau) = z, \\ x(t^j) &\in X^j, \quad t^j > \tau, \\ w(t) &\in W, \quad u(t) \in U, \quad t \in [\tau, t^2]. \end{aligned} \tag{2}$$

Пусть X_τ — множество всех $z \in R^n$, для которых задача (2) имеет решения. Функцию

$$u^0(\tau, z) = u^0(\tau | \tau, z), \quad z \in X_\tau, \quad \tau \in T_h, \tag{3}$$

назовем оптимальным дискретным управлением типа замыкаемой обратной связи.

Под траекторией замкнутой системы

$$\dot{x} = A(t)x + b(t)u^0(t, x(t)) + w(t), \quad x(t^0) = x_0,$$

будем понимать решение линейного уравнения

$$\dot{x} = A(t)x + b(t)u + w(t), \quad x(t^0) = x_0,$$

с управлением

$$u^*(t) = u^0(t^0 + kh, x(t^0 + kh)), t \in [t^0 + kh, t^0 + (k+1)h], k = \overline{0, N-1}. \quad (4)$$

Функцию (4) назовем реализацией обратной связи (3) в конкретном процессе управления. Устройство, способное в режиме реального времени вычислять текущие значения оптимальной обратной связи, называется оптимальным регулятором.

Опишем подробнее процедуру построения множеств в точках замыкания. Предположим, что множество X^* можно описать следующим образом:

$$x = \sum_{i=1}^s z_i \beta_i, \quad (5)$$

где $z_i \in \mathbb{R}^n$, $i = \overline{1, s}$, - некоторые фиксированные векторы, а скаляры β_i удовлетворяют следующему условию $d_i \leq \beta_i \leq d_i^*$, $i = \overline{1, s}$.

Рассмотрим отрезок $[t^1, t^2]$. Формула Коши для уравнения (1) на этом отрезке имеет вид

$$x(t^2) = F(t^2)F^{-1}(t^1)x(t^1) + \int_{t^1}^{t^2} F(t^2)F^{-1}(\tau)(bu(\tau) + w(\tau))d\tau \quad (6)$$

Из (6) видно, что для того чтобы гарантировать переход системы на терминальное множество, необходимо выполнение следующих условий:

$$h_i x(t^2) \leq \alpha_i - \max_{w \in W} h_i \int_{t^1}^{t^2} F(t^2)F^{-1}(\tau)w(\tau)d\tau, i = \overline{1, m}. \quad (7)$$

Таким образом, вместо множества X^2 определено некоторое вписанное в него множество \underline{X}^2 . Из формулы (6) можно получить уравнение, описывающее множество X^1 :

$$x(t^1) = F(t^1)F^{-1}(t^2)x(t^2) - \int_{t^1}^{t^2} F(t^1)F^{-1}(\tau)bu(\tau)d\tau \quad (8)$$

Поскольку управление строится в классе дискретных функций и выполняется условие (5), то множество X^p можно записать следующим образом:

$$x(t^p) = \sum_{i=1}^s F(t^p)F^{-1}(t^*)z_i \beta_i + \sum_{j=1}^q l_j u_j, \quad (9)$$

где q - число точек переключения на интервале $[t^p, t^*]$, l_j - соответствующие интегралы (8). Таким образом, множество X^1 представимо в виде (5).

Применив описанную процедуру, можно построить множество X^0 . Построив данные множества, можно сформулировать задачу оптимального управления для нахождения замыкаемой обратной связи. Оптимальные программное и позиционное гарантирующие управления с учетом замыкания являются решениями следующей экстремальной задачи

$$J(u) = \max_w c'x(t^*) \rightarrow \min_u$$

$$x = Ax + bu, x(t^0) = x_0, \quad (11)$$

$$x(t^k) \in X^k, k = \overline{1, 2}$$

$$|u(t)| \leq 1, t \in T.$$

Поскольку решение ищется в классе дискретных функций, то для решения данной задачи применимы методы линейного программирования, что позволяет значительно упростить вычислительный процесс.

При исследовании данной задачи было отмечено, что при росте числа точек замыкания целевая функция уменьшается, однако при этом значительно возрастает размерность задачи линейного программирования. Кроме того, в ходе численных экспериментов было выяснено, что для построения хорошей аппроксимации замкнутой обратной связи достаточно небольшого числа точек замыкания, поскольку, начиная с некоторого числа, добавление еще одного замыкания незначительно улучшает критерий качества.

Литература

1. Габасов Р., Кириллова Ф. М., Костина Е. А. Замыкаемые обратные связи по состоянию для оптимизации неопределенных систем управления. I. Однократное замыкание // Автоматика и телемеханика, 1996. № 7. С. 121-130. II. Многократно замыкаемые обратные связи // Автоматика и телемеханика, 1996. № 8. С. 90-99.

ПОСТРОЕНИЕ И АНАЛИЗ АНАЛИТИЧЕСКИХ РЕШЕНИЙ ЗАДАЧ О МГНОВЕННОМ ТОЧЕЧНОМ ВЗРЫВЕ

А.В. Маковский

(БГУ, г. Минск)

1. Постановка задачи

Рассмотрим идеализированное представление о мгновенном точечном взрыве как о движении газа, которое вызвано мгновенным выделением конечной энергии в некоторой точке.

2. Математическая постановка

Примем точку, где произошло выделение энергии, за начало системы координат и будем считать движение газа симметричным. Внутри области, ограниченной ударной волной, движение будем предполагать непрерывным, так что должны иметь место дифференциальные уравнения газовой динамики. На ударной волне задаются условия Ренкина-Гюгонио. Ещё одно условие вводится исходя из закона сохранения энергии.

3. Система обыкновенных дифференциальных уравнений

Вышеупомянутая система уравнений в частных производных может быть сведена к следующей системе (см., например, [1]):

$$R[\lambda] \left(\frac{(\nu-1)U'[\lambda]}{\lambda} + U[\lambda] \right) + \left(U[\lambda] - \frac{1+\gamma}{2} \lambda \right) R'[\lambda] = 0, \quad (3.1)$$

$$-\frac{\nu}{4}(1+\gamma)R[\lambda]U[\lambda] + \frac{(-1+\gamma)}{2}P'[\lambda] + R[\lambda] \left(-\frac{(1+\gamma)}{2} \lambda + U[\lambda] \right) U'[\lambda] = 0, \quad (3.2)$$

$$-\frac{\nu}{2}(1+\gamma)P[\lambda] + \left(-\frac{(1+\gamma)}{2} \lambda + U[\lambda] \right) P'[\lambda] + \gamma P[\lambda] \left(\frac{\nu-1}{\lambda} U[\lambda] + U'[\lambda] \right) = 0, \quad (3.3)$$

$$\lambda = r/r_2; U(\lambda) = u(r)/u(r_2); P(\lambda) = p(r)/p(r_2); R(\lambda) = \rho(r)/\rho(r_2), \quad (3.4)$$

где r_2 - расстояние от центра до ударной волны, λ - относительная Эйлера координата, ν - размерность задачи, а $U(\lambda)$, $P(\lambda)$, $R(\lambda)$ - относительные величины скорости, давления и плотности.

4. Первые интегралы и нахождение решения

Для системы (3.1-3.3) можно найти два первых интеграла [1], с использованием которых, можно получить из (3.1) однородное дифференциальное уравнение:

$$\partial_\lambda U[\lambda] = -\frac{U[\lambda](\nu-1)(\gamma-1)\gamma V[\lambda]^2/(\gamma+1) - \nu(2\gamma-1)V[\gamma]/2 + \nu(\gamma+1)/4}{\gamma V[\lambda]^2 - (\gamma+1)V[\lambda] + (\gamma+1)/2}, \quad (4.3)$$

где $V[\lambda] = U[\lambda]/\lambda$.

Осуществляя подстановку

$$U[\lambda] = \lambda \Phi[\lambda], \quad (4.4)$$

в равенство (4.3) и интегрируя полученное соотношение, получим:

$$\lambda[\Phi] = \Phi^{-2/(2+\nu)} C[\gamma, \nu, \Phi]^{4[\gamma, \nu]} \left(\frac{-1 + \gamma(-1 + 2\Phi)}{-1 + \gamma} \right)^{-(1-\gamma)/(-2+2\gamma+\nu)} \quad (4.5)$$

где
$$A[\gamma, \nu] = \frac{4(-2 + \nu)\nu + \gamma(-4 + 8\nu - 3\nu^2) + \gamma^2(4 + \nu^2)}{(-2 + \gamma)(2 + \nu)(2 + (-1 + \gamma)\nu)},$$

$$C[\gamma, \nu, \Phi] = \frac{-(1 + \gamma)(2 + \nu) + 2(2 + (-1 + \gamma)\nu)\Phi}{2 + \gamma(-2 + \nu) - 3\nu}$$

$U(\Phi)$ выражается из соотношения (4.4).

Выражения для $P(\Phi)$ и $R(\Phi)$ находятся, используя первые интегралы (4.1) - (4.2) и условие (4.4):

$$P[\Phi] = -(-1 + \gamma)^{\gamma/(2-\gamma)} C[\gamma, \nu, \Phi]^{-A[\gamma, \nu]} \Phi^{2\nu/(2+\nu)} (-1 - \gamma + 2\Phi)^{\gamma/(-2+\gamma)},$$

$$R[\Phi] = (-1 + \gamma)^{D[\gamma, \nu]} (2 + \gamma(-2 + \nu) - 3\nu)^{B[\gamma, \nu]} (-1 - \gamma + 2\Phi)^{2/(-2+\gamma)} \times \\ \times (-1 + \gamma)(2 + \nu) + 2(2 + (-1 + \gamma)\nu)\Phi)^{-B[\gamma, \nu]},$$

$$A[\gamma, \nu] = \frac{4(-2 + \nu)\nu + \gamma(-4 + 8\nu - 3\nu^2) + \gamma^2(4 + \nu^2)}{(-2 + \gamma)(2 + \nu)(2 + (-1 + \gamma)\nu)},$$

где
$$B[\gamma, \nu] = \frac{4(-1 + \gamma)\gamma + 8(-1 + \gamma)\nu + (4 + (-3 + \gamma)\nu)\gamma^2}{(-2 + \gamma)(-2 + 2\gamma + \nu)(2 + (-1 + \gamma)\nu)},$$

$$D[\gamma, \nu] = \frac{(4 - \gamma(4 + \nu))}{(-2 + \gamma)(-2 + 2\gamma + \nu)}.$$

5. Переход к новому параметру.

Использование полученного выше решения на практике сопряжено с некоторыми трудностями вычислительного характера. Во многом это связано с наличием множителя

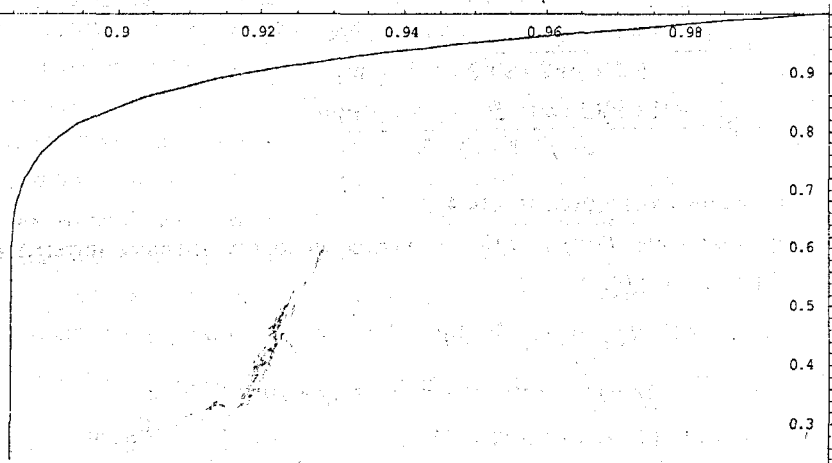
$$\left(\frac{-1 + \gamma(-1 + 2\Phi)}{-1 + \gamma} \right)^{E[\gamma, \nu]}, \text{ где } E[\gamma, \nu] = \frac{\gamma - 1}{-2 + 2\gamma + \nu}$$

в выражениях для λ . Значение показателя в нём очень мало ($E(1.3, 3) = 1/12$), что ведёт к необходимости использования вычислений с повышенной точностью.

График зависимости λ от Φ выглядит следующим образом (см. рис. 1)

Попытаемся получить найденные зависимости в более удобной для практического использования форме, перейдя к новому параметру ξ , исходя из условия:

$$\frac{1 + \gamma - 2\gamma\Phi}{1 - \gamma} = \xi^{E[\gamma, \nu]^{-1}}$$


 Рис. 1. График $\lambda(\Phi)$: при $\gamma=1.3$, $\nu=3$

Выражения для λ , U , P и R запишутся следующим образом:

$$\lambda[\xi] = \xi K[\gamma, \nu, \xi]^{-2/(2+\nu)} L[\gamma, \nu, \xi]^{N[\gamma, \nu]}, \quad U[\xi] = \xi K[\gamma, \nu, \xi]^{\nu/(2+\nu)} L[\gamma, \nu, \xi]^{N[\gamma, \nu]},$$

$$P[\xi] = K[\gamma, \nu, \xi]^{2\nu/(2+\nu)} M[\gamma, \nu, \xi]^{\gamma/(-2+\gamma)} L[\gamma, \nu, \xi]^{\wedge} \left(\frac{-4(-2+\nu)\nu + \gamma(-2+\nu)(-2+3\nu) - \gamma^2(4+\nu^2)}{(-2+\gamma)(2+\nu)(2+(-1+\gamma)\nu)} \right),$$

$$R[\xi] = \xi^{\nu/(-1+\gamma)} M[\gamma, \nu, \xi]^{2/(-2+\gamma)} L[\gamma, \nu, \xi]^{\wedge} \left(\frac{4(-2+\nu)\nu + \gamma(-4+8\nu-3\nu^2) + \gamma^2(4+\nu^2)}{(-2+\gamma)(-2+2\gamma+\nu)(2+(-1+\gamma)\nu)} \right),$$

$$K[\gamma, \nu, \xi] = \frac{1+\gamma+(-1+\gamma)\xi^{2+\nu/(\gamma-1)}}{2\gamma}$$

$$L[\gamma, \nu, \xi] = \frac{-(1+\gamma)(-2+2\lambda+\nu) + (-1+\gamma)(2+(-1+\gamma)\nu)\xi^{2+\nu/(\gamma-1)}}{\gamma(2+\gamma(-2+\nu)-3\nu)},$$

$$M[\gamma, \nu, \xi] = \frac{1+\gamma-\xi^{2+\nu/(\gamma-1)}}{\gamma}, \quad N[\gamma, \nu] = \frac{2}{2+\nu} + \frac{1-\gamma}{-2+2\gamma+\nu} + \frac{1+\gamma}{-2+\nu-\gamma\nu}.$$

Полученные результаты легко использовать на практике, поскольку зависимость Эйлеровой координаты λ от параметра ξ близка к линейной, что облегчает её численное обращение.

Проведение достаточно громоздких промежуточных преобразований стало возможным благодаря использованию пакета Mathematica® 4.0.

Литература:

1. Чудов Л.А., Росляков Г.С., Кестенбойм Х.С. Точечный взрыв. Методы расчета. Таблицы. - М.: Наука, 1974.
2. Wolfram S. The Mathematica Book. - Electronic Version.

РЕГУЛЯРИЗАЦИЯ НЕКОРРЕКТНЫХ ЗАДАЧ МЕТОДОМ ИТЕРАЦИЙ НЕЯВНОГО ТИПА

О.В. Матысик
(БрГУ, г. Брест)

Работа посвящена актуальной проблеме построения регуляризаторов при решении некорректных задач, поскольку такие задачи в большом количестве возникают в многочисленных приложениях современной математики. В работе строится регуляризатор для уравнения

$$Ax = y \quad (1)$$

в виде неявного итеративного метода

$$(E + \alpha A)x_{n+1} = (E - \alpha A)x_n + 2\alpha y, \quad x_0 = 0. \quad (2)$$

Здесь A - ограниченный положительный самосопряженный оператор, действующий в гильбертовом пространстве, для которого нуль не является собственным значением, следовательно, задача некорректна. Предполагается, что при точной правой части y уравнения (1) существует точное решение x . В случае приближенной правой части y_δ , $\|y - y_\delta\| \leq \delta$, метод (2) примет вид:

$$(E + \alpha A)x_{n+1,\delta} = (E - \alpha A)x_{n,\delta} + 2\alpha y_\delta, \quad x_{0,\delta} = 0. \quad (3)$$

Доказана сходимость метода (3) при точной и приближенной правых частях уравнения (1) и в случае истокообразной представимости точного решения $x = A^s z$, $s > 0$ получены оценки погрешности, которые оптимизированы. Доказаны теоремы.

Теорема 1. Итерационный процесс (2) сходится при условии $\alpha > 0$.

Теорема 2. Итерационный процесс (3) сходится при условии $\alpha > 0$, если число итераций n выбирать в зависимости от δ так, чтобы $n(\delta)\delta \rightarrow 0$ при $\delta \rightarrow 0$.

Теорема 3. Если выполняется условие $x = A^s z$, $s > 0$, то общая оценка погрешности метода (3) имеет вид

$$\|x - x_{n,\delta}\| \leq s^s (2n\alpha e)^{-s} \|z\| + 2n\alpha\delta.$$

Теорема 4. Оптимальная оценка погрешности для метода (3) имеет вид

$$\|x - x_{n,\delta}\|_{opt} \leq (1+s) \|z\| \frac{1}{s+1} \delta^{\frac{s}{s+1}} e^{\frac{s}{s+1}}$$

и достигается при

$$n_{opt} = s(2\alpha)^{-1} e^{\frac{s}{s+1}} \|z\| \frac{1}{s+1} \delta^{\frac{1}{s+1}}.$$

Оптимальная оценка погрешности не зависит от α , но от α зависит n_{opt} и, следовательно, объем вычислительной работы, поэтому для уменьшения объема вычислительной работы следует брать α возможно большим из условия $\alpha > 0$ и так, чтобы n_{opt} было целым. Вычислительный процесс необходимо остановить на n_{opt} шаге. Приближение $x_{n,\delta}$, полученное на этом шаге, будет ближе всего к точному решению уравнения. Поскольку на α нет ограничения сверху ($\alpha > 0$), то за счет выбора α можно добиться того, что оптимальная оценка погрешности будет достигаться уже на первых шагах итераций. В этом состоит преимущество неявного метода (3) перед явными методами итераций решения некорректных задач.

Доказана сходимость метода (2) в случае, когда $\lambda = 0$ является собственным значением оператора A , т.е. в случае неединственного решения. Показано, что тогда метод (2) сходится к решению с минимальной нормой.

Если сведения об истокопредставимости решения отсутствуют, то метод (3) можно сделать эффективным, если воспользоваться следующим правилом останова по соседним приближениям.

Определим момент останова итерационной процедуры условием

$$\|z_{n,\delta} - z_{n+1,\delta}\| > \varepsilon, \quad (n < m), \quad \|z_{m,\delta} - z_{m+1,\delta}\| \leq \varepsilon,$$

где ε - заданное до начала вычислений положительное число (уровень останова).

Доказана сходимость метода (3) с указанным правилом останова по соседним приближениям в случае, когда оператор A - несамосопряженный ограниченный положительный, получена оценка для момента останова. Число итераций, нужное для получения решения выбирается автоматически. При этом не требуется знание истокопредставимости точного решения.

Метод (3) также становится эффективным, если воспользоваться правилом останова по невязке

$$\|Ax_{n,\delta} - y_\delta\| > \varepsilon, \quad (n < m), \quad \|Ax_{m,\delta} - y_\delta\| \leq \varepsilon, \quad (4)$$

где ε - заданное до начала вычислений положительное число (уровень останова), $\varepsilon = b\delta$, $b > 1$.

Доказана сходимость метода (3) с правилом останова (4), получена оценка погрешности метода и оценка для момента останова. При решении уравнения (1) методом (3) с правилом останова (4) также не требуется знание истокорпредставимости точного решения. И тем не менее будет автоматически выбрано число итераций m , обеспечивающее оптимальный порядок погрешности. Но даже если истокорпредставимость точного решения отсутствует, останав по невязке (4) обеспечивает сходимость метода, т.е. его регуляризующие свойства.

ЛИНЕЙНЫЕ ОДНОРОДНЫЕ НАГРУЖЕННЫЕ ДИФФЕРЕНЦИАЛЬНЫЕ УРАВНЕНИЯ ВТОРОГО ПОРЯДКА

Н.К. Млыгчик

(БГТУ, Брест)

Линейное однородное нагруженное дифференциальное уравнение (ЛОНДУ) второго порядка имеет вид:

$$y'' + p(x)y' + q(x)y + \alpha_1(x)y(a) + \alpha_2(x)y'(a) + \beta_1(x)y(b) + \beta_2(x)y'(b) = 0, \quad (1)$$

где $p(x)$, $q(x)$, $\alpha_1(x)$, $\alpha_2(x)$, $\beta_1(x)$, $\beta_2(x)$ - заданные функции.

В отличие от линейного однородного дифференциального уравнения $y'' + p(x)y' + q(x)y = 0$, имеющего при «хороших» коэффициентах только два линейно независимых решения, уравнение (1) может иметь до шести линейно независимых решений.

Приведем схему построения ЛОНДУ типа (1) с различным количеством линейно независимых решений.

1). Пусть ЛОНДУ имеет только два линейно независимых решения y_1 и y_2 ; тогда оно может быть представлено в виде

$$\begin{vmatrix} y_1 & y_2 & y \\ y_1' & y_2' & y' \\ y_1'' & y_2'' & y'' \end{vmatrix} + \begin{vmatrix} y_1(a) & y_2(a) & y_1 & y(a) \\ y_1'(a) & y_2'(a) & y_1' & y'(a) \\ y_1(b) & y_2(b) & y_2 & y(b) \\ y_1'(b) & y_2'(b) & y_2' & y'(b) \end{vmatrix} = 0$$

2). Пусть ЛОНДУ имеет три линейно независимых решения y_1, y_2, y_3 ; тогда его можно записать в виде

$$\begin{vmatrix} y_1 & y_2 & y_3 \\ y_1' & y_2' & y_3' \\ y_1'' & y_2'' & y_3'' \end{vmatrix} + \begin{vmatrix} y_1(a) & y_2(a) & y_3(a) & y(a) \\ y_1'(a) & y_2'(a) & y_3'(a) & y'(a) \\ y_1(b) & y_2(b) & y_3(b) & y(b) \\ y_1'(b) & y_2'(b) & y_3'(b) & y'(b) \end{vmatrix} = 0$$

3). Пусть ЛОНДУ имеет четыре линейно независимых решения y_1, y_2, y_3, y_4 ; тогда оно может быть записано так

$$\begin{vmatrix} y_1 & y_2 & y_3 \\ y_1' & y_2' & y_3' \\ y_1'' & y_2'' & y_3'' \end{vmatrix} + \begin{vmatrix} y_1(a) & y_2(a) & y_3(a) & y_4(a) & y(a) \\ y_1'(a) & y_2'(a) & y_3'(a) & y_4'(a) & y'(a) \\ y_1(b) & y_2(b) & y_3(b) & y_4(b) & y(b) \\ y_1'(b) & y_2'(b) & y_3'(b) & y_4'(b) & y'(b) \\ y_1 & y_2 & y_3 & y_4 & y \end{vmatrix} = 0$$

4). Пусть ЛОНДУ имеет пять линейно независимых решения y_1, y_2, y_3, y_4, y_5 ; тогда оно может быть представлено в виде

$$\begin{vmatrix} y_1 & y_2 & y_3 \\ y_1' & y_2' & y_3' \\ y_1'' & y_2'' & y_3'' \end{vmatrix} + \begin{vmatrix} y_1(a) & y_2(a) & y_3(a) & y_4(a) & y_5(a) & y(a) \\ y_1'(a) & y_2'(a) & y_3'(a) & y_4'(a) & y_5'(a) & y'(a) \\ y_1(b) & y_2(b) & y_3(b) & y_4(b) & y_5(b) & y(b) \\ y_1'(b) & y_2'(b) & y_3'(b) & y_4'(b) & y_5'(b) & y'(b) \\ y_1 & y_2 & y_3 & y_4 & y_5 & y \\ y_1' & y_2' & y_3' & y_4' & y_5' & y' \end{vmatrix} = 0$$

5). Пусть ЛОНДУ имеет шесть линейно независимых решения $y_1, y_2, y_3, y_4, y_5, y_6$; тогда оно может быть записано в виде

$$\begin{vmatrix} y_1 & y_2 & y_3 \\ y_1' & y_2' & y_3' \\ y_1'' & y_2'' & y_3'' \end{vmatrix} + \begin{vmatrix} y_1(a) & y_2(a) & y_3(a) & y_4(a) & y_5(a) & y_6(a) & y(a) \\ y_1'(a) & y_2'(a) & y_3'(a) & y_4'(a) & y_5'(a) & y_6'(a) & y'(a) \\ y_1(b) & y_2(b) & y_3(b) & y_4(b) & y_5(b) & y_6(b) & y(b) \\ y_1'(b) & y_2'(b) & y_3'(b) & y_4'(b) & y_5'(b) & y_6'(b) & y'(b) \\ y_1 & y_2 & y_3 & y_4 & y_5 & y_6 & y \\ y_1' & y_2' & y_3' & y_4' & y_5' & y_6' & y' \\ y_1'' & y_2'' & y_3'' & y_4'' & y_5'' & y_6'' & y'' \end{vmatrix} = 0$$

СИСТЕМЫ С ОТРАЖАЮЩЕЙ МАТРИЦЕЙ ПРЕДСТАВЛЯЮЩЕЙ СОБОЙ
ПРОИЗВЕДЕНИЕ ДВУХ МАТРИЧНЫХ ЭКСПОНЕНТ

Э. В. Мусафиров

(ГГУ, г. Гомель)

Данная работа посвящена исследованию периодических дифференциальных систем на наличие периодических решений и их устойчивость с помощью отражающей функции (ОФ) [1].

Рассмотрим систему

$$\dot{x} = P(t)x, \quad t \in \mathbf{R}, \quad x \in \mathbf{R}^n, \quad (1)$$

где $P(t)$ – непрерывно дифференцируемая необходимая число раз матрица.

Известно [2], что отражающую матрицу (ОМ) любой системы (1) можно представить в виде $F(t) \equiv e^{S(t)}$, где $S(t)$ – нечетная $n \times n$ -матрица.

Значит, ОМ любой системы (1) можно представить в виде

$$F(t) \equiv e^{\sum_{i=0}^{\infty} A_i \alpha_i(t)}, \quad (2)$$

где A_i – некоторые постоянные $n \times n$ -матрицы, $\alpha_i(t)$ – некоторые нечетные непрерывно дифференцируемые необходимая число раз скалярные функции (например, функции $t, \sin t, \sin 2t, \dots$, которые целесообразно использовать при изучении 2π -периодических систем (1)).

Задача отыскания для системы (1) ОМ в виде (2) достаточно сложна. Поэтому, целесообразно среди систем (1) выделить те системы, ОМ которых

представима в виде $F(t) \equiv \prod_{i=0}^m e^{A_i \alpha_i(t)}$, где $A_i, i = \overline{0, m}$ – постоянные $n \times n$ -

матрицы, $\alpha_i(t), i = \overline{0, m}$ – нечетные непрерывно дифференцируемые необходимая число раз скалярные функции. Производная такой матрицы достаточно проста и это облегчает нахождение самой матрицы $F(t)$ и основного соотношения (ОС) [1].

Введем обозначения: $K := -2P(0), L := 4(P(0)\dot{P}(0) - \dot{P}(0)P(0)) - 2\ddot{P}(0)$.

Лемма 1. Матрица $F(t) \equiv e^{A\alpha(t)}e^{B\beta(t)}$, где A, B – постоянные $n \times n$ -матрицы; $\alpha(t), \beta(t)$ – скалярные нечетные трижды непрерывно диффе-

реницируемые на \mathbf{R} функции, причем $\dot{\alpha}(0) \neq 0$, $\dot{\beta}(0) \neq 0$, $\dot{\alpha}(0)\ddot{\beta}(0) \neq \dot{\beta}(0)\ddot{\alpha}(0)$, является ОМ системы (1) тогда и только тогда, когда $KL = LK$,

$$F(t)(A\dot{\alpha}(t) + B\dot{\beta}(t) + P(t)) \equiv -P(-t)F(t), \quad A = \frac{K - \dot{\beta}(0)B}{\dot{\alpha}(0)},$$

$$B = \frac{\dot{\alpha}(0)L - \ddot{\alpha}(0)K}{\dot{\alpha}(0)\dot{\beta}(0) - \dot{\beta}(0)\ddot{\alpha}(0)}$$

Теорема 1. Матрица

$$F(t) \equiv e^{A \sin t} e^{B \sin 2t}, \quad (3)$$

где A, B — постоянные $n \times n$ -матрицы, является ОМ системы (1) тогда и только тогда, когда $KL = LK$, $A = \frac{L + 4K}{3}$, $B = -\frac{L + K}{6}$,

$F(t)(A \cos t + 2B \cos 2t + P(t)) \equiv -P(-t)F(t)$. Причем, если $2\pi \frac{p}{q}$ -периодическая

система (1) ($p, q \in \mathbf{N}$, $\frac{p}{q}$ — несократимая дробь) имеет ОМ (3), то все решения этой системы $2\pi p$ -периодические.

Теорема 2. Матрица

$$F(t) \equiv e^{At} e^{B \sin t}, \quad (4)$$

где A, B — постоянные $n \times n$ -матрицы, является ОМ системы (1) тогда и только тогда, когда $KL = LK$, $A = L + K$, $B = -L$,

$F(t)(A + B \cos t + P(t)) \equiv -P(-t)F(t)$. Причем, если $2\pi p$ -периодическая система (1) ($p \in \mathbf{N}$) имеет ОМ (4), то матрица монодромии на периоде $[-\pi p, \pi p]$

есть $F(-\pi p) = e^{-A \pi p}$, и ее мультипликаторы μ_i находятся из уравнения

$$\det(e^{-A \pi p} - \mu E) = 0.$$

Пример 1. Рассмотрим систему $\dot{x} = \begin{pmatrix} a(t) & b(t) \\ c(t) & d(t) \end{pmatrix} x$. Если

$$a(t) \equiv -\frac{1}{2}(l \cos t + 2q \cos 2t) + 2k_1 \sin(s_1 t) \cos(k \sin t + r \sin 2t) + (k_2 \sin(s_2 t) + k_3 \sin(s_3 t)) \sin(k \sin t + r \sin 2t),$$

$$b(t) \equiv \frac{1}{2}(k \cos t + 2r \cos 2t) + 2k_2 \sin(s_2 t) \cos(k \sin t + r \sin 2t) + (k_4 \sin(s_4 t) - k_1 \sin(s_1 t)) \sin(k \sin t + r \sin 2t),$$

$$c(t) \equiv -\frac{1}{2}(k \cos t + 2r \cos 2t) + 2k_3 \sin(s_3 t) \cos(k \sin t + r \sin 2t) + \\ + (k_4 \sin(s_4 t) - k_1 \sin(s_1 t)) \sin(k \sin t + r \sin 2t),$$

$$d(t) \equiv -\frac{1}{2}(l \cos t + 2q \cos 2t) + 2k_4 \sin(s_4 t) \cos(k \sin t + r \sin 2t) - \\ - (k_2 \sin(s_2 t) + k_3 \sin(s_3 t)) \sin(k \sin t + r \sin 2t),$$

где $k, l, q, r, k_i, s_i \in \mathbf{R}$, $i = \overline{1,4}$, то по теореме 1 система имеет ОМ вида (3), где

$$A = \begin{pmatrix} l & -k \\ k & l \end{pmatrix}, \quad B = \begin{pmatrix} q & -r \\ r & q \end{pmatrix}. \quad \text{Причем в этом случае}$$

$$F(t) \equiv e^{l \sin t + q \sin 2t} \begin{pmatrix} \cos(k \sin t + r \sin 2t) & -\sin(k \sin t + r \sin 2t) \\ \sin(k \sin t + r \sin 2t) & \cos(k \sin t + r \sin 2t) \end{pmatrix}. \quad \text{В случае, ко-}$$

гда $s_i \in \mathbf{Z}$, $i = \overline{1,4}$, рассматриваемая система будет 2π -периодической с 2π -периодической ОМ. Тогда по теореме 1 все решения такой системы будут 2π -периодическими.

Полученные результаты для линейных дифференциальных систем можно распространить на нелинейные системы следующим образом.

Рассмотрим $2\pi \frac{p}{q}$ -периодическую ($p, q \in \mathbf{N}$, $\frac{p}{q}$ — несократимая дробь)

по t систему

$$\dot{x} = X(t, x), \quad t \in \mathbf{R}, \quad x \in \mathbf{R}^n, \quad (5)$$

с непрерывно дифференцируемой по всем своим переменным функцией $X(t, x)$, для которой $X(t, 0) = 0$. Согласно [3], если ОФ системы (5) линейна,

то она является ОФ системы (1), где $P(t) \equiv \frac{\partial X}{\partial x}(t, 0)$.

Теорема 3. Пусть матрица $F(t)$ вида (3), где A, B , — постоянные $n \times n$ -матрицы, является ОМ системы (1), где $P(t) \equiv \frac{\partial X}{\partial x}(t, 0)$ и выполнено тождество

$$F(t)X(t, x) + X(-t, F(t)x) \equiv (F(t)P(t) + P(-t)F(t))x. \quad (6)$$

Тогда все решения системы (5) $2\pi p$ -периодические.

Теорема 4. Пусть матрица $F(t)$ вида (4), где A, B — постоянные $n \times n$ -матрицы, является ОМ системы (1), где $P(t) \equiv \frac{\partial X}{\partial x}(t, 0)$. Тогда, 1) если

$$\forall i = \overline{1, n} \quad |\mu_i| < 1, \text{ где } \mu_i, i = \overline{1, n} \text{ решения уравнения } \det \begin{pmatrix} -A \pi^{\frac{p}{q}} & \\ & -\mu E \end{pmatrix} = 0, \text{ то}$$

решение $x \equiv 0$ системы (5) асимптотически устойчиво; 2) если $\exists i: |\mu_i| > 1$, то решение $x \equiv 0$ системы (5) неустойчиво; 3) если верно тождество (6) и $\exists i: \mu_i = 1$, то у системы (5) существует хотя бы одно однопараметрическое семейство $2\pi \frac{p}{q}$ -периодических решений.

Литература.

1. Мироненко В.И. Отражающая функция и периодические решения дифференциальных уравнений. Минск, Университетское, 1986. 86 с.
 2. Вересович П.П. // Дифференц. уравнения. 1998. Т.34, №12. С. 2257 – 2259.

НЕКОТОРЫЕ ПРИЛОЖЕНИЯ ТЕОРЕМЫ СИЛОВА

Т.Ф. Новик
 (БрГУ, г. Брест)

В работе рассматривается возможность описать строение конечных групп при помощи теоремы Силова.

Определение 1. Если все элементы G имеют конечные порядки, являющиеся степенями одного и того же простого числа p , то говорят, что G является p -группой.

Определение 2. Если порядок конечной группы G делится на p^k ($k > 0$, p — простое число) и не делится на p^{k+1} , то всякая подгруппа группы G , имеющая порядок p^k , называется силовской подгруппой группы G относительно простого числа p или силовской p -подгруппой.

Если G -группа порядка pq , где $p < q$ — простые числа, то

1. силовские p -подгруппы и q -подгруппы циклические;
2. число силовских q -подгрупп равно $1 + kq$ (при некотором k) и делит pq ; число силовских p -подгрупп равно $1 + lp$ (при некотором l) и делит pq ;

3. силовская q -подгруппа $\langle b \rangle$ единственная; она нормальна в G ;
4. силовских p -подгрупп одна или q ;
5. если $\langle a \rangle$ силовская p -подгруппа, то $a^{-1}ba = b^r$ ($1 \leq r < q$), причем если $r = 1$, то $G = \langle ab \rangle$.

Пусть p и q - простые числа, $p < q$, а r удовлетворяет сравнению $x^p \equiv 1 \pmod{q}$ и H_r - группа с образующими a и b и определяющими соотношениями:

$$a^p = b^q = e, \quad a^s b^t \cdot a^u b^v = a^{s+u} b^{t+v}.$$

Тогда H_r - абелева группа порядка pq и отображение, заданное формулой $f(a^s b^t) = a^{ms} b^t$ изоморфно.

Таким образом, возможны следующие типы групп порядка pq ($p < q$):

1. при $q \not\equiv 1 \pmod{p}$ существует лишь один тип групп порядка pq - циклические;
2. при $q \equiv 1 \pmod{p}$ существует два типа групп порядка pq :
а) циклические; б) неабелевы.

Отсюда следует, что существуют только две неизоморфные группы 6-го порядка - циклическая и симметрическая и существует лишь одна группа 15-го порядка - циклическая.

Литература.

1. Кострикин А.И. Введение в алгебру. - М.: Наука, 1977.

РЯДЫ ФУРЬЕ УСИЛЕННОЙ СХОДИМОСТИ

Р. Ю. Плотников

(БГТУ, г. Брест)

Часто при решении прикладных задач, в которых функция представляется рядом Фурье, приходится тратить много времени на вычисление большого количества членов ряда Фурье для достижения требуемой точности. Однако, существуют методы, позволяющие уменьшить объем вычислений за счет замены функции быстро сходящимся рядом Фурье или путем усиления сходимости ряда Фурье.

Применение рядов Фурье с быстро убывающими коэффициентами удобно, так как для вычисления суммы ряда достаточно вычислить только не-

сколько первых членов ряда Фурье. При этом чем быстрее убывают коэффициенты, тем меньше членов ряда нужно удержать для отыскания его суммы с требуемой степенью точности.

Однако, несколько большее время затрачивается на приведение функции к быстро сходящемуся ряду Фурье или усиление сходимости ряда, чем в случае с медленно сходящимся рядом Фурье, полученным стандартными методами. Тем не менее эти затраты времени компенсируются упомянутым выше отсутствием необходимости вычислять большое количество членов ряда.

Важность быстроты сходимости рядов Фурье.

Как было отмечено, в приложениях наиболее удобны ряды Фурье с быстро убывающими коэффициентами, так как в этом случае несколько первых членов достаточно точно определяют его сумму.

Кроме этого, в конкретных задачах часто возникает необходимость в почленном дифференцировании ряда Фурье. Каждое такое дифференцирование понижает порядок убывания коэффициентов Фурье на одну единицу.

Следует отметить, что почленное интегрирование ряда Фурье всегда допустимо, при этом получается ряд, коэффициенты которого имеют порядок убывания на одну единицу более высокий, чем порядок убывания коэффициентов исходного ряда.

Быстрота убывания коэффициентов Фурье периодической функции $f(t)$ определяется дифференциальными свойствами этой функции. А именно, если $f(t)$ непрерывна и имеет непрерывные производные до $(m - 1)$ -го порядка включительно, то коэффициенты Фурье функции $f(t)$ имеют порядок убывания не ниже, чем $\frac{1}{k^{m+1}}$. Следовательно, для того, чтобы иметь быстро сходящийся ряд Фурье для функции $f(t)$, нужно добиться непрерывности как функции $f(t)$, так и ее первых производных.

Метод А.С. Малиева разложения функций в быстро сходящийся ряд Фурье.

Предположим, что функция $f(t)$ задана на интервале $\left[0, \frac{T}{2}\right]$ и имеет в нем непрерывные производные до $(m - 1)$ -го порядка и m -ую производную, удовлетворяющую условиям Дирихле. Такой выбор интервала задания функции не ограничивает общности, так как если $f(t)$ задана на любом интервале

$[\alpha, \beta]$, то, совершив замену аргумента t на θ по формуле $t = \frac{2(\beta - \alpha)}{T}\theta + \alpha$, придем к функции $\psi(\theta)$, заданной уже на интервале $\left[0, \frac{T}{2}\right]$.

Для того, чтобы разложить в ряд Фурье функцию $f(t)$, заданную на интервале $\left[0, \frac{T}{2}\right]$, нужно эту функцию с помощью некоторой функции $g(t)$ продолжить в отрицательный интервал $\left[-\frac{T}{2}, 0\right]$, в результате чего получится функция

$$F(t) = \begin{cases} g(t), & -\frac{T}{2} \leq t < 0, \\ f(t), & 0 \leq t \leq \frac{T}{2}, \end{cases}$$

заданная на интервале $\left[-\frac{T}{2}, \frac{T}{2}\right]$. Если нет заинтересованности в каком-либо специальном характере ряда Фурье, с помощью которого требуется представить функцию $f(t)$ (может, например, встретиться необходимость разложить $f(t)$ в ряд Фурье только по косинусам или только по синусам, что предполагает соответственно четное или нечетное продолжение $g(t)$ функции $f(t)$), то можно продолжить ее на интервал $\left[-\frac{T}{2}, 0\right]$ с помощью любой функции $g(t)$.

Положим, что функция $g(t)$ на интервале $\left[-\frac{T}{2}, 0\right]$ имеет непрерывные производные до $(m - 1)$ -го порядка и m -ую производную, удовлетворяющую условиям Дирихле. Однако теперь, несмотря на то, что функции $f(t)$ и $g(t)$ обладают каждая в своем интервале задания "хорошими" дифференциальными свойствами, периодическая функция $\varphi(t)$, получающаяся при периодическом продолжении $f(t)$ с интервала $\left[-\frac{T}{2}, \frac{T}{2}\right]$ на всю ось t , может такими свойствами не обладать. В точках $t = v\frac{T}{2}$, ($v = 0, \pm 1, \pm 2, \dots$) функция $\varphi(t)$ может иметь разрывы; если $\varphi(t)$ непрерывна в этих точках, то в них могут иметь разрывы производные $\varphi(t)$ порядка ниже, чем $(m - 1)$, что не позволит получить для $\varphi(t)$ достаточно быстро сходящийся ряд Фурье.

Потребовав теперь дополнительно, во-первых, чтобы $g(t)$ и $f(t)$ и их производные до $(m-1)$ -го порядка имели одинаковые значения соответственно в точках $t = -\frac{T}{2}$ и $t = +\frac{T}{2}$, т.е. потребовав выполнения $2m$ условий

$$g(0) = f(0), \quad g\left(-\frac{T}{2}\right) = f\left(\frac{T}{2}\right),$$

$$g'(0) = f'(0), \quad g'\left(-\frac{T}{2}\right) = f'\left(\frac{T}{2}\right),$$

$$g''(0) = f''(0), \quad g''\left(-\frac{T}{2}\right) = f''\left(\frac{T}{2}\right),$$

$$\dots\dots\dots$$

$$g^{(m-1)}(0) = f^{(m-1)}(0), \quad g^{(m-1)}\left(-\frac{T}{2}\right) = f^{(m-1)}\left(\frac{T}{2}\right).$$

добьемся того, что периодическая функция $\varphi(t)$ будет иметь непрерывные производные до $(m-1)$ -го порядка и m -ую производную, удовлетворяющую условиям Дирихле.

Коэффициенты Фурье функции $\varphi(t)$ будут иметь в этом случае порядок убывания не ниже, чем $\frac{1}{k^{m+1}}$, а так как ряд Фурье $\varphi(t)$ в интервале $\left[0, \frac{T}{2}\right]$ сходится к функции $f(t)$, то для последней получим ряд Фурье усиленной сходимости [1].

Из изложенного следует, что "улучшающая" функция $g(t)$, ограниченная поставленными условиями, остается достаточно произвольной в отношении своего вида. В частности, независимо от вида $f(t)$, можно брать в качестве $g(t)$ алгебраический многочлен. Удовлетворение $2m$ условиям требует лишь, чтобы многочлен $g(t)$ содержал $2m$ подлежащих определению коэффициентов, т.е. был бы $(2m-1)$ -ой степени

$$g(t) = A_0 t^{2m-1} + A_1 t^{2m-2} + \dots + A_{2m-2} t + A_{2m-1}.$$

Для упрощения процесса преобразования функции в быстро сходящийся ряд Фурье автором разработана программа для вычисления на ЭВМ коэффициентов «улучшающего» многочлена.

Работа выполнена под руководством профессора кафедры высшей математики А. И. Тузика.

Литература.

1. Жевержеев В.Ф., Кальницкий Л.А., Сапогов Н.А. Специальный курс высшей математики для ВТУЗов – М.: Высшая школа, 1970. – 416 с.

О НЕКОТОРЫХ МЕТОДАХ МОДЕЛИРОВАНИЯ УСТОЙЧИВЫХ СЛУЧАЙНЫХ РАСПРЕДЕЛЕНИЙ И ПРОЦЕССОВ

Т. В. Соболева

(БГУ, г. Минск)

В последние годы начал интенсивно расширяться круг практических задач, в которых стали естественным образом появляться устойчивые распределения. В некоторых областях техники, физики, астрономии, экономики и социологии появляются практические задачи использующие устойчивые распределения.

Представляет большой интерес рассмотрение методов и алгоритмов моделирования устойчивых процессов. Оперирование с распределениями устойчивых процессов сильно затруднено, поскольку явный вид устойчивых плотностей известен всего лишь в трёх случаях. Однако, в ряде случаев можно указать, как получать устойчивые процессы, например, из броуновского движения с помощью случайной замены времени.

В данной статье рассматривается алгоритм моделирования устойчивых случайных распределений и процессов предложенный в [1], [2].

Определение 1. Случайный процесс $Z_t, t \geq 0$ называется строго α -устойчивым процессом Леви, если:

$$Law(Z_{at}, t \geq 0) = Law(a^{1/\alpha} Z_t, t \geq 0)^1,$$

где $a \geq 0$.

Приведём один из примеров, который даёт возможность моделирования симметричных α -устойчивых распределений с помощью трёх независимых случайных величин: равномерно распределённой, гауссовской и экспоненциально распределённой.

Пусть $Z_t, t \geq 0$ – симметричный α -устойчивый процесс Леви с характеристической функцией

$$\varphi_t(\theta) = E \exp\{i\theta Z_t\} = \exp\{-t|\theta|^\alpha\},$$

где $0 < \alpha < 2$.

¹ Запись $Law(X) = Law(Y)$ означает совпадение распределений X и Y.

Из изложенного ниже будет следовать, что процесс $Z_t, t \geq 0$ может быть реализован в виде

$$Z_t = B_{T_t}, t \geq 0, \quad (1)$$

где $B_t, t \geq 0$ – броуновское движение с $EB_t = 0, EB_t^2 = 2t$ и $T_t, t \geq 0$ – некоторый неотрицательный неубывающий $\alpha/2$ -устойчивый случайный процесс. О процессе $Z_t, t \geq 0$, получаемом посредством преобразования (1), говорят, что он образован из броуновского движения с помощью случайной замены времени на $T_t, t \geq 0$.

Необходимый для представления (1) процесс $T_t, t \geq 0$ строится таким образом, что $\text{Law}(T_t) = \text{Law}(U^{(\alpha/2)})$, где $U^{(\alpha)}$ – неотрицательная устойчивая случайная величина с параметром $0 < \alpha < 1$. В силу определения 1, получим:

$$\text{Law}(T_t) = \text{Law}\left(t^{\alpha/2} U^{(\alpha/2)}\right) \quad (2)$$

Пусть $p(x, \alpha), x \geq 0, 0 < \alpha < 1$ – плотность распределения вероятностей случайной величины $U = U^{(\alpha)}$, с индексом $0 < \alpha < 1$. Для этой плотности, сосредоточенной на $x \geq 0$, известно следующее представление:

$$p(x, \alpha) = \frac{1}{\pi} \left(\frac{\alpha}{1-\alpha} \right) \left(\frac{1}{x} \right)^{1-\alpha} \int_0^{\pi} a(z, \alpha) \exp \left\{ - \left(\frac{1}{x} \right)^{1-\alpha} a(z, \alpha) \right\} dz,$$

где

$$a(z, \alpha) = \left(\frac{\sin \alpha z}{\sin z} \right)^{1-\alpha} \frac{\sin(1-\alpha)z}{\sin \alpha z}. \quad (3)$$

Плотность $p(x, \alpha)$ является плотностью распределения случайной величины

$$\zeta = \left(\frac{a(\xi, \alpha)}{\eta} \right)^{\frac{1-\alpha}{\alpha}},$$

где $a(z, \alpha)$ задается формулой (3), ξ, η – независимые случайные величины, ξ имеет равномерное распределение на $[0, \pi]$, а η – экспоненциальное распределение с единичным параметром.

Заметим, что:

$$Law(T_t) = Law\left(t^{\alpha/2} U(\alpha/2)\right) = Law\left(\left(\frac{a(\xi, \alpha/2)}{\eta}\right)^{\frac{2-\alpha}{\alpha}}\right) \quad (4)$$

Таким образом, из (2) и (4), обозначая $\gamma(0,2)$ гауссовскую случайную величину с нулевым средним и дисперсией, равной 2, получаем:

$$Law(Z_t - Z_s) = Law\left((t-s)^{1/\alpha} \left(\frac{a(\xi, \alpha/2)}{\eta}\right)^{\frac{2-\alpha}{2\alpha}} \gamma(0,2)\right).$$

Это представление для $Law(Z_t - Z_s)$ показывает, как с помощью моделирования трёх независимых случайных величин ξ , η , $\gamma = \gamma(0,2)$ можно смоделировать данные наблюдений за приращениями $Z_t - Z_s$ симметричного α -устойчивого случайного процесса.

В качестве оценивания качества моделей был использован метод моментов, а также проведено сравнение графиков аналитической и эмпирической функций распределения.

ВЫЧИСЛИТЕЛЬНЫЕ ЗАТРАТЫ ПРИ ЧИСЛЕННОМ РЕШЕНИИ ПЕРИОДИЧЕСКИХ УРАВНЕНИЙ ДУФФИНГА И ВАН-ДЕР-ПОЛЯ

Н.Н. Стрилец, В.М. Мадорский

(БрГУ, г. Брест)

1. Уравнение Дуффинга имеет вид:

$$\ddot{x}(t) + ax(t) + bx(t) + cx^p(t) = F(\sin wt, \cos wt),$$

где $F(\sin wt, \cos wt) = A \sin wt + B \cos wt + C(D \sin wt + E \cos wt)^p + G$,
 $w > 0$; $p \in \mathbb{N}$; a, b, c, A, B, C, D, G — числовые параметры.

2. Уравнение Ван-дер-Поля имеет вид:

$$\ddot{x}(t) - \varepsilon(1 - x^p(t))\dot{x}(t) + x^q(t) = F(\sin wt, \cos wt), \text{ где } \varepsilon > 0; p, q \in \mathbb{N}.$$

Часто приходится решать данные уравнения численно, производя дискретизацию и сведение их к системам нелинейных алгебраических уравнений, которые решаются одним из итерационных процессов [1]:

Шаг 1.

$$\left(\sigma \beta_{n-1} \|f(x_n)\|^2 E + f'^*(x_n) f'(x_n) \right) \Delta x_n = -f'^*(x_n) f(x_n), \quad 0 < \sigma \ll 1, \quad \beta_{-1} = 1. \quad (2)$$

Шаг 2.

$$\beta_{n+1} = \min \left(1, \frac{\nu_n}{\alpha \beta_n \|f(x_{n+1})\|} \right), \quad \alpha > 1, \quad \beta_0 \in (10^{-4}; 10^{-1}),$$

$$\nu_{n+1} = (1 - \beta_{n+1}) \nu_n + \beta_n \beta_{n+1}^2 \|f(x_{n+1})\|, \quad \nu_0 = \gamma \|f(x_0)\|, \quad 0 < \gamma \ll 1.$$

$$x_{n+1} = x_n + \beta_n \Delta x_n, \quad x_0 - \text{начальный вектор.}$$

Шаг 3. Если $\|f(x_n)\| \leq \varepsilon$ и (или) $\|\Delta x_n\| \leq \varepsilon$ – конец просчётов, иначе – шаг 1.

Здесь $f'^*(x)$ – оператор, сопряжённый оператору $f'(x)$ – производной Фреше оператора $f(x)$.

Очевидно, что значительная часть вычислительных затрат связана с решением системы (2) на каждом шаге итерационного процесса.

Приближенные значения производных функции $x(t)$ в точке вычисляем по методу неопределенных коэффициентов (НК) [2]. Для аппроксимации используем нечетное число точек, а сами производные вычисляем в средней точке. Тогда матрица в левой части системы (2), имеет вид

$$S = \begin{bmatrix} A & U \\ V & W \end{bmatrix}, \quad (3)$$

где A – диагональная матрица, в которой число диагоналей нечетно, и по обе стороны от главной находится одинаковое количество диагоналей.

Возможны 3 случая :

I. Если количество точек разбиения отрезка не превышает 128, то для определения вектора Δx_n можно воспользоваться методом квадратных корней.

II. Если же количество точек разбиения находится в пределах от 128 до 1024, то предыдущий вариант не является оптимальным. В этом случае воспользуемся описанным ниже приемом.

Пусть нужно решить систему n линейных уравнений вида $SX = F$, (4)

$$\text{где} \quad S = \begin{bmatrix} A_{n-s, n-s} & U_{n-s, s} \\ V_{s, n-s} & W_{s, s} \end{bmatrix}, \quad X = \begin{bmatrix} X_{n-s, r} \\ X_{s, r} \end{bmatrix}, \quad F = \begin{bmatrix} F_{n-s, r} \\ F_{s, r} \end{bmatrix}.$$

Индексы обозначают соответствующие размерности матриц. Матрица S имеет вид (3). Воспользовавшись для нахождения обратной матрицы формулой Фробениуса [3], аналогично как в [4] получим :

$$X = \begin{bmatrix} X_{n-s,r} \\ 0 \end{bmatrix} + \begin{bmatrix} Y_{n-s,s} (R_{s,s} (F_{s,r} - V_{s,n-s} X_{n-s,r})) \\ R_{s,s} (F_{s,r} - V_{s,n-s} X_{n-s,r}) \end{bmatrix}, \quad (5)$$

$$(W_{s,s} + V_{s,n-s} Y_{n-s,s}) R_{s,s} = E_{s,s}, \quad (6)$$

$$A_{n-s,n-s} Y_{n-s,s} = -U_{n-s,s}, \quad A_{n-s,n-s} X_{n-s,r} = F_{n-s,r}, \quad (7)$$

где $E_{s,s}$ - единичная матрица размерности $[s \times s]$.

Совокупность действий (5)-(7) назовем методом *матричного окаймления*.

Таким образом, если известны решения систем (7) (в которых матрица

$A_{n-s,n-s}$ является диагональной), то в результате выполнения совокупности действий (5)-(6) получим решение исходной системы (4).

Пусть в общем случае каждая из систем (7) имеет вид $S_d X_d = F_d$, (8)

где S_d - диагональная матрица, удовлетворяющая указанным выше условиям.

Если q - количество диагоналей матрицы S_d и $k = \left[\frac{q}{2} \right]$, то выберем

ближайшее к n натуральное число n' ($n' \geq n$), которое делится на k без остатка. Дополним матрицу S_d до матрицы S'_d размерности $[n' \times n']$ добавлением нулевых строк и столбцов. Тогда матрицу S'_d можно разбить на блоки размерности $[k \times k]$. Зная решение системы $S'_d X'_d = F'_d$ (9)

$$S'_d = \begin{bmatrix} A_1 & B_1 & \dots & 0 & 0 \\ A_2 & B_2 & C_2 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & A_{m-1} & B_{m-1} & C_{m-1} \\ 0 & 0 & \dots & B_m & C_m \end{bmatrix}, \quad X'_d = \begin{bmatrix} X_1 \\ X_2 \\ \dots \\ X_m \end{bmatrix}, \quad F'_d = \begin{bmatrix} F_1 \\ F_2 \\ \dots \\ F_m \end{bmatrix}.$$

легко найдем решение системы (8).

Можно показать, что как и в случае трехдиагональной прогонки для решения системы (9) необходимо выполнить совокупность двух действий (назовем их методом *трехдиагональной матричной прогонки*):

♦ Прямой ход:

$$(A_i u_{i-1} + B_i) u_i = -C_i, \quad (A_i v_{i-1} + B_i) v_i = F_i - A_i v_{i-1}, \quad i = \overline{1, m}, \quad u_0 = v_0 = 0$$

♦ Обратный ход: $x_i = u_i x_{i+1} + v_i$, $x_{m+1} = 0$.

III. Если количество точек разбиения превышает 1024, то предыдущий вариант становится неэффективным. В этом случае можно воспользоваться следующим соображением: как правило, производная не столь чувствительна к изменению аргумента как функция, то для аппроксимации якобиана $f'(x)$ производные функции $x(t)$ можно вычислять по методу НК, используя меньшее количество точек, чем при аппроксимации функции $f(x)$. На конечный результат такое допущение (и это подтверждается на практике) при большом количестве точек влияния практически не оказывает. Если для вычисления производной функции $x(t)$ при аппроксимации якобиана $f'(x)$ использовать 3 точки, то матрица A в (3) будет пятидиагональной. Тогда, зная решение систем (7), методом *матричного окаймления* получим решение системы (4). Каждую из систем (7) можно решить методом *пятидиагональной прогонки*.

Пусть дана пятидиагональная система вида

$$a_i x_{i-2} + b_i x_{i-1} + c_i x_i + d_i x_{i+1} + e_i x_{i+2} = g_i, \quad i = \overline{1, l}$$

По аналогии с методом трехдиагональной прогонки можно показать, что для решения этой системы нужно выполнить совокупность двух действий:

– Прямой ход:

$$z_i = a_i(u_{i-2}u_{i-1} + v_{i-2}) + b_i u_{i-1} + c_i, \quad u_i = -\frac{a_i u_{i-2} v_{i-1} + b_i v_{i-1} + d_i}{z_i}, \quad v_i = -\frac{e_i}{z_i},$$

$$w_i = -\frac{a_i(u_{i-2}w_{i-1} + w_{i-2}) + b_i w_{i-1} - g_i}{z_i}, \quad u_{-2} = u_{-1} = v_{-2} = v_{-1} = w_{-2} = w_{-1} = 0.$$

– Обратный ход: $x_i = u_i x_{i+1} + v_i x_{i+2} + w_i$, $x_{n+1} = x_{n+2} = 0$.

Изложенные выше приемы позволяют значительно увеличить число точек разбиения без существенного изменения вычислительных затрат.

Литература.

1. Мадорский В.М. О регуляризованных итерационных методах с обратной связью для решения уравнений. //Труды института математики НАН Беларуси. 2000. Т.5. С. 89-91.
2. Березин И.С., Жидков Н.П. Методы вычислений. М., 1966. Т.1.
3. Гантмахер Ф.Р. Теория матриц. М.: «Наука», 1988.
4. Фадеева В.Н. Вычислительные методы линейной алгебры. М, 1950.

ПРИМЕНЕНИЕ M – ОЦЕНКИ ХЬЮБЕРА ДЛЯ ВАРИОГРАММЫ СТАЦИОНАРНОГО СЛУЧАЙНОГО ПРОЦЕССА

Т.В. Цеховая

(БГУ, г. Минск)

Рассмотрим стационарный в широком смысле случайный процесс $X(s)$, $s \in Z$, с нулевым математическим ожиданием и неизвестной вариограммой [1]

$$2\gamma(h) = D(X(s+h) - X(s)), h \in Z.$$

Некоторые вопросы исследования оценок вариограммы можно найти, например, в статьях [1-4]. В данной работе обсуждается вопрос оценивания вариограммы стационарного случайного процесса с применением m – оценки хьюбера и изучаются статистические свойства построенных оценок.

Обозначим $U(h) = (X(s+h) - X(s))^2$, $s, h \in Z$. Тогда $2\gamma(h) = MU(h)$, то есть оценивание вариограммы сводится к построению оценки математического ожидания процесса $U(h)$, $h \in Z$. Пусть $X(1), X(2), \dots, X(n)$ – n последовательных, полученных через равные промежутки времени наблюдений за процессом $X(s)$, $s \in Z$, и, следовательно, имеем $U(h)$, $h = \overline{0, n-1}$.

В качестве оценок вариограммы $2\gamma(h)$ рассмотрим M -оценки Хьюбера T_n , которые являются решением уравнения

$$\sum_{j=0}^{n-1} \varphi(U(j) - T_n) = 0,$$

где

$$\varphi(x) = \begin{cases} x, & |x| \leq k, \\ \text{sgn}(x), & |x| > k, \end{cases}$$

$0 < k < \infty$. Отметим, что предельные случаи $k \downarrow 0$ и $k \downarrow \infty$ приводят, соответственно, к выборочным медиане \tilde{U} и среднему \bar{U} . Тогда семейство рассматриваемых оценок можно представить в виде $T_n = t_n(F_n) = t_n(U_0, U_1, \dots, U_{n-1})$, где U_0, U_1, \dots, U_{n-1} – порядковые статистики для независимых одинаково распределенных значений $U(0), U(1), \dots, U(n-1)$ с эмпирической функцией распределения $F_n = F_n(u)$. Для среднего, например, функциональная форма не зависит от n и $\bar{U} = t(F_n)$. В других случаях можно выбрать подходящий функционал $t(F_n)$ так, что для больших n разность $t_n(F_n) - t(F_n)$ становится пре-

небрежительно малой. Так, для выборочной медианы \tilde{U} соответствующий выбор приводит к функционалу вида $t(F_n) = F_n^{-1}(1/2)$.

Известно, что если $t(\cdot)$ – непрерывный функционал, то оценка $t(F_n)$ состоятельна для $t(F)$, где $F = F(u)$ – истинное распределение $U(0), U(1), \dots, U(n-1)$. Далее, следуя работе [5], можно показать, что статистика

$$\frac{\{T_n - t(F)\}\sqrt{n}}{\sigma_{t,F}},$$

где

$$\sigma_{t,F}^2 = \int d_{t,F}^2(u) dF(u), \quad (1)$$

$$d_{t,F}(y) = \varphi(y) / \int \varphi'(u) dF(u),$$

имеет асимптотически нормальное распределение с нулевым математическим ожиданием и дисперсией, равной единице.

Чтобы проиллюстрировать свойства M – оценок Хьюбера, приведем некоторые численные результаты, полученные для больших выборок при помощи асимптотической теории [5]. Численные результаты относятся к шести различным порождающим распределениям, а именно

А. Стандартное нормальное $N(0,1)$ - распределение;

В. Смесь нормальных $N(0,1)$ - и $N(0,9)$ - распределений с весами 0,998 и 0,002 соответственно;

С. Смесь нормальных $N(0,1)$ - и $N(0,9)$ - распределений с весами 0,95 и 0,05 соответственно;

Д. Смесь нормальных $N(0,1)$ - и $N(0,9)$ - распределений с весами 0,8 и 0,2 соответственно;

Е. Распределение Лапласа с плотностью $f(x) = 0,5e^{-|x|}$;

Ф. Распределение Коши с плотностью $f(x) = \{\pi(1+x^2)\}^{-1}$.

Для каждой комбинации порождающего распределения и M – оценки Хьюбера при известном ряде значений k и симметричного загрязнения ε в таблице приводится значение дисперсии $\sigma_{t,F}^2$ предельного нормального распределения статистики $\sqrt{n}(T_n - t(F))$, вычисленной по формуле (1). Для сравнения в таблицу включены выборочные медиана и среднее. Выбор оценки математического ожидания с меньшей асимптотической дисперсией будет

эквивалентен получению лучшей оценки. Столбец ε_{min} содержит значения симметричного загрязнения ε , которые для соответствующего k будут приводить к минимальной асимптотической дисперсии.

Таблица

Асимптотическая дисперсия статистики $\sqrt{n}(T_n - t(F))$ для M -оценок Хьюбера T_n и шести порождающих распределений.

k	ε_{min}	A	B	C	D	E	F
		$\varepsilon=0$	$\varepsilon=0.002$	$\varepsilon=0.05$	$\varepsilon=0.2$		
0.0	1.00000	1.5708	1.5750	1.6810	2.0913	1.0000	2.4674
0.1	0.87529	1.4923	1.4964	1.5999	2.0012	1.0333	2.3786
0.5	0.44171	1.2625	1.2664	1.3650	1.7486	1.1653	2.2881
1.0	0.14283	1.1073	1.1113	1.2142	1.61366	1.3226	2.5465
1.5	0.03761	1.0371	1.0418	1.1601	1.6137	1.4653	2.9927
2.0	0.00842	1.0104	1.0161	1.1600	1.7000	1.5890	3.5208
2.5	0.00160	1.0023	1.0094	1.1864	1.8315	1.6917	4.0888
3.0	0.00025	1.0004	1.0090	1.2221	1.9757	1.7740	4.6785
∞		1.0000	1.0160	1.4000	2.6000	2	∞

Как видно из таблицы, выборочное среднее приемлемо при стандартном $N(0,1)$ – порождающем распределении, но совершенно не пригодно в любой ситуации, где возможно появление резко выделяющихся наблюдений. В случае выборочной медианы, резко выделяющиеся наблюдения оказывают известное влияние. Из полученных результатов следует, что M – оценки Хьюбера являются наиболее стабильными для всех распределений и остаются лучшими при распределениях с относительно небольшим загрязнением. Но при распределениях, порождающих большие доли резко выделяющихся наблюдений, и при распределении Коши их дисперсия существенно возрастает.

Описанный выше метод оценивания вариограммы стационарного случайного процесса является дальнейшим развитием некоторых результатов, приведенных в книге Ф. Хампеля, Э. Рончетти, П. Рауссеу, В. Штаэля [5].

Литература.

1. N. Cressie, D. M. Hawkins. Robust Estimation of the Variogram: I // Mathematical Geology, Vol. 12, No. 2, 1980. – p. 115 – 125.
2. N. Cressie. Fitting Variogram Models by Weighted Least Squares // Mathematical Geology, Vol. 17, No. 5, 1985. – p. 563 – 586.

3. Н.Н. Труш, Т.В. Цеховая. Исследование статистических свойств оценок вариограммы и ковариационной функции // Весці НАН Беларусі. Сер. фіз.-мат. навук.- 2001.- №2.- С.24-29.
4. Т.В. Цеховая Асимптотическое поведение семинвариантов высших порядков оценки вариограммы. // Тезисы докл. VIII международной математической конференции Ч. 2, с. 178.- 2000г.
5. Ф. Хампель, Э. Рончетти, П. Рауссеу, В. Штаэль. Робастность в статистике. М.: Мир, 1989.

ИДЕНТИФИКАЦИЯ ОБЪЕКТОВ И ПРОЦЕССОВ ПО КОРРЕЛЯЦИОННОМУ ОБРАЗУ

В.Н. Шуть, И.Г. Прожерин

(БГТУ, Брест)

1. Введение

Объектом исследования является группа случайных точек на плоскости отражающая не жестко, неявно некоторый объект либо физический процесс. Такую группу не жестко связанных точек на плоскости назовем дискретной системой. Определим ее следующим образом. Пусть d и D - произвольные положительные числа. Систему точек на плоскости назовем простой (d, D) -системой, если выполняются следующие два условия:

1. расстояние между любыми двумя точками системы не меньше d (d -условие);
2. где бы на плоскости ни нарисовать окружность радиуса D , внутри или на ней самой лежит хотя бы одна точка системы (D -условие).

Непересекающиеся между собой круги одного и того же радиуса D на плоскости можно располагать бесконечно. Поскольку по D -условию в каждом из них должна содержаться, по крайней мере одна точка (d, D) -системы, то такая система точек бесконечна.

С другой стороны в любой ограниченной области может содержаться лишь конечное число точек d, D -системы. Это непосредственно вытекает из d -условия. Таким образом, в нашей системе нет ни больших разрежений точек, ни чересчур плотных скоплений. D -условие является притягивающей (собирающей) силой, а d -условие действует как отталкивающая сила. Плотность распределения точек колеблется в некоторых пределах, зависящих, разумеется, от параметров d и D . Введение параметров посредством условий 1 и 2 неоднозначно связывает с ними данную систему. В самом деле, если сис-

тема удовлетворяет приведенным условиям при некоторых значениях d и D , то она будет удовлетворять тем же условиям и при других значениях d' и D' , для которых выполняются неравенства $d' < d$, $D' < D$.

Избавиться от неоднозначности можно, выбрав для данной системы в качестве параметра d наибольшее число, при котором она еще удовлетворяет условию 1, а в качестве параметра D - соответственно наименьшее число среди тех, для которых выполняется условие 2. В дальнейшем, несмотря конкретную (d, D) -систему точек, под d и D будем понимать именно экстремальное для этой системы значение параметров, которое может быть практически получено с самой системы.

2. Алгоритм получения контура

Алгоритм построения кругов регрессии основывается на построении контуров. Эти контура строятся следующим образом:

1. выбор минимального значения из строки или столбца и соединяем точки;
2. переходим к следующей строке и соединяем следующие точки;
3. выполняем шаги 1 и 2 для всех строк и столбцов.

Т.о., в результате выполнения алгоритма получим контура различной длины, по которым строятся круги регрессии.

Для определения параметров кругов регрессии необходимо знать координаты центра и радиус. Определим формулы, по которым строятся круги регрессии [1,2]:

$$x_c = \sum_{i=1}^n x_i; \quad y_c = \sum_{i=1}^n y_i \quad (1)$$

где $(x_c; y_c)$ - координаты центра круга регрессии;

$(x_i; y_i)$ - координаты точек контура;

n - количество точек входящих в контур,

$$R = \frac{1}{n} \sum_{i=1}^n \sqrt{(x_i - x_c)^2 + (y_i - y_c)^2} \quad (2)$$

где R - радиус круга регрессии.

Затем по каждому контуру строятся круг регрессии.

3. Статистика

По полученным радиусам кругов регрессии строится гистограмма. Для этого определяется минимальное и максимальное значение радиуса круга регрессии. Затем определяется шаг приращения:

$$\Delta = \frac{1}{n} (R_{\max} - R_{\min}) \quad (3)$$

где n – количество точек облака;

R_{\min} – минимальное значение радиуса круга регрессии;

R_{\max} – максимальное значение радиуса круга регрессии;

Δ – шаг приращения.

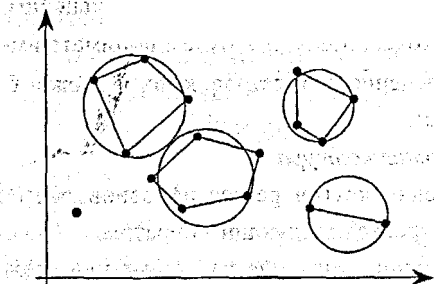


Рис.1 – Пример описания облака кругами регрессии.

По полученным результатам строится таблица, в которой определяют-ся диапазон радиусов и количество таких кругов.

Таблица 1.

Радиус	$r_1 - r_2$...	$r_{n-1} - r_n$
Кол-во	m_1	...	m_n

По таблице строится гистограмма, форма которой описывает объект или процесс, идентифицируя его.

4. Выводы

Т.о., в работе показан новый подход к идентификации случайных объектов или процессов. Случайный объект или процесс можно описать не только с помощью линии регрессии, которая характеризуется углом наклона и отсекаемым отрезком на оси ординат, не только с помощью линий высшего порядка, таких как парабола, гипербола и т.д., но и с помощью кругов регрессии. Круги регрессии наиболее полно представляют случайный объект или процесс, т.к. имеют более сильную связь с объектом.

Литература:

1. Основные математические формулы: Справочник/ В. Т. Воднев, А. Ф. Наумович, Н. Ф. Наумович; Под ред. Ю. С. Богданова. – 3-е изд., перераб. и доп. – Мн.: Выш. шк., 1995.-380 с.:ил.
2. Ефимова М.Р., Петрова Е.В., Румянцев В.Н. Общая теория статистики. – М.: ИНФРА-М, 1997.

СОВРЕМЕННЫЕ ТЕХНОЛОГИИ ПРОГРАММИРОВАНИЯ, ИНФОРМАЦИОННЫЕ СЕТИ И СИСТЕМЫ

ИНФОРМАЦИОННАЯ СОСТАВЛЯЮЩАЯ ЭКСПЕРТНЫХ ОЦЕНОК

В.Л. Бусько, В.Ю. Винкевич

(БУИР, г. Минск)

Пусть рассматривается объект, описываемый суммой параметров, составляющей множество оценок X . Оценки X_{ji} образуют алфавит в подмножестве $A = \{X_{ji}\}$ множества оценок X , которое полностью описывает J -ый объект, т.е. является носителем информации. Непосредственное соотнесение этой информации с алфавитом невозможно, т.к. она никак не связана с ним, поэтому о применении информации к алфавиту можно говорить с позиций теории формирования весовых коэффициентов, отношений, нечетких множеств и т.п.

Одним из возможных путей формирования весовых коэффициентов является понятие "количество информации" одной величины относительно другой.

$$I(v/\eta) = H(v) - MH(v/\eta) \quad (1)$$

где v, η - дискретные величины;

$I(v/\eta)$ - количество информации о величине v относительно величины η ;

$H(v)$ - неопределенность величины v ;

$MH(v/\eta)$ - средняя условная неопределенность величины v при условии η .

Примем, что v - информационные характеристики алфавита $\{X_{ji}\}$, а η - информационные характеристики подмножества A . Тогда $I(v/\eta)$ будет определять количество информации в каждой экспертной оценке при условии, что величина η определяется характеристиками

$$\begin{aligned} &F(N_N); F(H_i), \\ &F(N); F(I), \\ &F(\xi_N); F(\xi_i) \end{aligned} \quad (2)$$

В этом случае

$$H_{ji} = -\sum_{j=1}^2 P_{ji}^* \log_2 P_{ji}^* = [P_{ji}^* \log_2 P_{ji}^* + (1 - P_{ji}^*) \log_2 (1 - P_{ji}^*)] \quad (3)$$

где $P_{ji}^* = P_{ji}(1 - P_{ji}^*)$ - вероятность назначения безошибочной и непротиворечивой оценки.

H_{ji} - уровень неопределенности элемента алфавита.

Для нахождения величины $H(v)$ нужно из уровня H_{ji} вычесть остаточную неопределенность $H_{ji \text{ ост}}$, а оставшегося поля выборки выделить неопределенность, относящуюся непосредственно к элементу алфавита (экспертной оценке).

Если воспользоваться моделью в виде формулы

$$I + H_1 = 1 \quad (4)$$

а для этого есть условия, т.к. уровень H_{ji} получен для двухальтернативного исхода (см. формулу 3), то

$$H_{ji \text{ ост}} = 2 H_{ji} - 1 \quad (5)$$

Оставшееся поле выборки составляет величину

$$H_{ji}^0 - H_{ji} - (2H_{ji} - 1) = -H_{ji} - 1 \quad (6)$$

В соответствие с моделью (см. формулу 4) общее поле выборки между неопределенностью и информацией определяется как

$$I_{ji} + N_{ji} \epsilon_{ji} = H_{ji}$$

Информация составляет часть H_{ji} вида

$$\frac{I_{ji}}{I_{ji} + N_{ji} \epsilon_{ji}} H_{ji} \quad (7)$$

Неопределенность составляет часть H_{ji} вида

$$\frac{N_{ji} \epsilon_{ji}}{I_{ji} + N_{ji} \epsilon_{ji}} H_{ji} \quad (8)$$

На основании формул (6), (7), (8)

$$H(9) = -\frac{N_{ji} \epsilon_{ji}}{I_{ji} + N_{ji} \epsilon_{ji}} H_{ji} + 1 \quad (9)$$

Аналогично устанавливается зависимость для неопределенности $MN(v/\eta)$ на основе характеристик (2)

$$MN(v/\eta) = \frac{N \epsilon_N}{J + N \epsilon_N} H_N \quad (10)$$

Таким образом, количество информации

$$I(v/\eta) = 1 - \frac{N_{ji} \epsilon_{ji}}{I_{ji} + N_{ji} \epsilon_{ji}} H_{ji} - \frac{N \epsilon_N}{I_j + N \epsilon_N} H_N \quad (11)$$

На основании модели (4) можно по информационному признаку построить модель элемента алфавита $\{X_{ji}\}$

$$X_{ji} = X_{ji}^{Iji} + X_{ji}^{Nji} \quad (12)$$

где X_{ji}^I - информационная часть экспертной оценки;

X_{ji}^N - неопределенная часть экспертной оценки.

Представим

$$X_{ji}^{Iji} = K_{ji}^{Iji} \text{ и } X_{ji}^{Nji} = K_{ji}^{Nji} \quad (13)$$

где K_{ji}^{Iji} , K_{ji}^{Nji} - соответственно весовые коэффициенты по информации и неопределенности.

Тогда формулу (12) на основании формулы (13) можно привести к виду

$$K_{ji}^{Iji} = 1 - K_{ji}^{Nji} \quad (14)$$

По определению - модель неопределенности (правая часть формулы (1)) состоит из двух составляющих $H(v)$ и $MH(v/\eta)$. Поэтому, используя эту модель для весового коэффициента неопределенности, получим

$$K_{ji}^{Nji} = K_{ji}^N + K^N \quad (15)$$

Перепишем формулу (12) с учетом формулы (15)

$$K_{ji}^{Iji} = 1 - K_{ji}^N - K^N \quad (16)$$

Сравнивая почленно правые части формул (11) и (16) находим

$$K_{ji}^{Iji} = \frac{N_{ji} * \epsilon_{ji}}{I_{ji} + N_{ji} * \epsilon_{ji}}, K_{ji}^N = \frac{N * \epsilon_N}{I + N * \epsilon_N} \quad (17)$$

Относительно H_{ji} и H_N можно на основании определений (формула (1)) считать

$$H_{ji} \sim X_{ji}, H_N \sim X_{cp}$$

где X_{cp} - среднее значение экспертной оценки в матрице оценок $A = \|X_{ji}\|$.

$$X_{cp} = \frac{1}{N \times S} \sum_{j=1}^N \sum_{i=1}^S X_{ji}$$

Общее выражение для информационной части экспертной оценки:

$$X_{ji}^{Iji} = \left[1 - \frac{N_{ji} * \epsilon_{ji}}{I_{ji} + N_{ji} * \epsilon_{ji}} \right] X_{ji} - \frac{\epsilon_N * N}{I + \epsilon_N * N} X_{cp} \quad (18)$$

Преобразуем формулу (18) к более удобному виду и опустим индексации (j,i) в степенях, тогда формула для определения информационной части экспертных оценок примет вид:

$$X_{ji}^I = \frac{I_{ji}}{I_{ji} + N_{ji} * \epsilon_{ji}} X_{ji} - \frac{\epsilon_N * N}{I + \epsilon_N * N} X_{cp} \quad (19)$$

Поскольку суммы, стоящие в знаменателях в правой части формулы (14) равны одному бит то формально, приняв I_{ji} , N безразмерными коэффициентами, формулу (19) можно упростить для использования:

$$X_{ji}^I = I_{ji} * X_{ji} - \epsilon_N * N * X_{cp} \quad (20)$$

На основании формулы (20) осуществляется коррекция экспертных оценок по информационному признаку, с ограничениями

$$0 < X_{ji}^I \leq X_{ji} \quad (21)$$

Для выполнения неравенства (формула (21)) нужно, чтобы эксперт обладал определенными информативными характеристиками. Примем, что под информативной характеристикой будем понимать функцию $F(I, \epsilon)$, которая включает весь набор функций (2). Верхняя и нижняя границы оценочной функции $F(I, \epsilon)$ могут быть установлены на основании формулы (21)

$$1) \sup F(I, \epsilon) = X_{ji}, \quad (22)$$

$$2) \inf F(I, \epsilon) = 0$$

Верхнее граничное значение функция $F(I, \epsilon)$ достигает, когда весовой коэффициент по информации $I_{ji}=1$ и число квант неопределенности $\epsilon_N = 0$. Это означает, что эксперт дает одноточечные оценки, и они содержат только один квант информации.

$$\sup F(I, \epsilon) = X_{ji} \sim \epsilon_N = 0$$

Нижнее граничное значение $F(I, \epsilon)$ найдем в предположении: если подмножество $A(X_{ji})$ обладает свойствами $F(I, \epsilon)$, то и каждый элемент X_{ji} этого подмножества также обладает этими свойствами. Это предположение позволяет записать

$$F(I_{ji}, \epsilon_{ji}) = F(I, \epsilon_N)$$

Применим это равенство к формуле (20)

$$X_{ji}^J = I X_{ji} - \epsilon_N N X_{cp} \quad (23)$$

Из формулы (21) следует $X_{ji}^J > 0$, что одновременно требует выполнения условия

$$I X_{ji} - \varepsilon_N N X_{\text{ср}} > 0; \text{ или } \frac{X_{ji}}{X_{\text{ср}}} > \frac{\varepsilon_N N}{I}$$

Добавим и вычтем в числителе левой части неравенства член $X_{\text{ср}}$, тогда неравенство примет вид

$$\frac{\Delta X_{ji}}{X_{\text{ср}}} > \frac{\varepsilon_N N}{I} - 1 \quad (24)$$

где $\Delta X_{ji} = X_{ji} - X_{\text{ср}}$ - отклонение экспертной оценки от ее среднего значения.

Выберем наихудший случай, когда

$$\Delta X_{ji} - X_{\text{ср}} \quad (25)$$

Анализ формулы (24) при условии формулы (25) дает

$$\varepsilon_N < 4 \quad (26)$$

Нижняя граница функции $F(I, \varepsilon_N)$ при условии формулы (26)

$$\inf F(I, \varepsilon_N) = 0 \sim \varepsilon_N < 4$$

Оценки эксперта, у которого в информативных характеристиках количество квант неопределенности больше трех ($\varepsilon_N > 3$) не должны использоваться в дальнейшем для принятия решения.

Заключение.

На основе анализа информационной части экспертной оценки установлено, что при числе квант неопределенности $\varepsilon_N \leq 3$ оценки эксперта могут быть использованы для выработки решения по поставленной задаче. При числе квант неопределенности $\varepsilon_N > 3$ в информативных характеристиках эксперта его оценки не могут быть использованы, поскольку отклонения экспертных оценок от их среднего значения достигают 100%-го уровня.

Литература.

1. Бешелев С.Д., Гурвич Ф.Г. Математико-статистические методы экспертных оценок. 2-изд. М.Ж. «Статистика», 1980.-263с.ил.
2. Автоматизация проектно-конструкторских работ и технологической подготовки производства в машиностроении. Т1/Под ред. И.О. Семенкова. Минск, «Высэйшая школа», 1979.-352с.ил.

АЛГОРИТМ PBSP-ДЕРЕВЬЕВ И ЕГО ПРИМЕНЕНИЕ

А.А. Врублевский

(ГрГУ, г. Гродно)

В последнее время роль компьютерной графики резко возросла; особенно повысился спрос на использование интерактивной компьютерной графики. Интерактивная компьютерная графика находит свое применение от визуализации простых объектов (например, на web-страницах) до моделирования сложных физических и математических моделей.

Обычно вся сцена представляется большим набором выпуклых полигонов (многоугольников). Количество полигонов в интерактивной сцене может достигать нескольких десятков или даже сотен тысяч. Такое количество многоугольников практически невозможно обрабатывать в реальное время. Поэтому для представления всей сцены целиком используются различные алгоритмы представления сцен.

Одним из самых прогрессивных алгоритмов является алгоритм BSP-деревьев (Binary Space Partition). Семейство этих алгоритмов рассматривает всю сцену целиком, и для их применения практически нет никаких ограничений по построению сцены. Задача алгоритма BSP-деревьев одна – удаление невидимых поверхностей.

Алгоритм BSP-деревьев является препроцессорным алгоритмом, т.е. для его использования необходимы предварительные расчеты. Этот алгоритм наиболее элегантным способом представляет данные общего характера, тем самым, решая большинство задач компьютерной графики. Однако существенным недостатком этого метода является огромное число перерисовок при отображении графических данных. К этому алгоритму был разработан дополнительный алгоритм (PVS – Potentially Visible Set), оптимизирующий количество выводимой информации, не искажая при этом окончательную картину. Алгоритм PVS в свою очередь не лишен недостатков, самым главным его недостатком является время предварительных расчетов: даже для небольших сцен этот процесс может затягиваться на часы.

Альтернативой алгоритма BSP-деревьев стал разработанный автором алгоритм PBSP (Portal Binary Space Partition – двоичное разбиение пространства, с использованием порталов). Этот алгоритм сочетает в себе все качества алгоритма BSP и лишен основного недостатка PVS. Единственным недостатком PBSP является чисто техническая сторона – задание (создание модели) сцены.

Алгоритм PBSP, как и BSP, оперирует произвольными данными. Но есть небольшие отличия. Алгоритм BSP-деревьев является общим алгоритмом удаления невидимых поверхностей. А алгоритм PBSP является частью алгоритмов теории твердого тела, т.е. исходит из того предположения, что вся сцена высекает собой часть пространства, а не как в BSP – заключает в себе часть пространства. Эти принципы очень близки по восприятию, но существенно влияют на процесс обработки поступающей графической информации. Как правило, на практике гораздо удобнее пользоваться концепцией твердого тела при построения сцен для PBSP-деревьев.

Таким образом, алгоритм PBSP является преемником алгоритма BSP, лишенным практически всех его недостатков – та же элегантность представления графической информации и отсутствие необходимости рассчитывать PVS - данные.

Литература:

1. <http://www.sgi.com>,
2. <http://www.cs.unc.edu/~geom/SSV>,
3. <ftp://ftp.sgi.com/other/bspfaq/>,
4. <http://www.flipcode.com>.

РАЗРАБОТКА ПРОГРАММНОГО КОМПЛЕКСА ДЛЯ ОБЕСПЕЧЕНИЯ ЖИВУЧЕСТИ ОДНОРОДНЫХ ПРОГРАММИРУЕМЫХ ДРЕВОВИДНЫХ СТРУКТУР НА СБИС ПЛМ

М.М. Высоцкий

(БГУ, г. Минск)

В последнее время, разрабатывая новые системы, стали уделять повышенное внимание обеспечению таких свойств, как надежность, отказоустойчивость, живучесть.

Программируемые логические матрицы (ПЛМ) – это один хорошо известный класс структурированных логических схем, которые нашли свое широкое использование в системах СБИС. Задача обеспечения живучести СБИС ПЛМ состоит в том, чтобы в любой момент времени в СБИС ПЛМ существовала подсистема аппаратурно-программных средств (функциональная подсистема) для выполнения цели функционирования. Создание соответствующей

щей подсистемы при нарушении условий функционирования обеспечивается средствами самой СБИС ПЛМ.

Структура, построенная на СБИС ПЛМ, должна нормально реагировать на такие типы неисправностей, как:

- константные;
- неисправности пересечения линий;
- короткие замыкания;

Восстановление функционирования после возникновения неисправности — одна из наиболее трудно реализуемых функций вычислительной системы, так как при эксплуатации могут возникнуть непредвиденные ситуации, а в существующих системах ограничена способность программных и аппаратных средств к обнаружению, диагностике, локализации неисправностей, к созданию работоспособных конфигураций.

Восстановление определяется как совокупность действий, которые осуществляются системой по получению сигнала о неисправности (при наличии системы восстановления). Так, например, восстановление — это реконфигурация структуры системы при элементарных отказах ЭВМ или процессоров с целью перераспределения решаемых системой задач между работоспособными модулями.

Различают восстановление после трех видов неисправностей (ошибок): физических; ошибок программного обеспечения; при управлении вычислительным процессом. Соответственно выделяют три принципиально различных уровня восстановления: аппаратный (физический), программный и уровень управления. Имеющийся опыт проектирования позволяет сформулировать ряд общих положений /1/, лежащих в основе построения систем, обладающих свойством живучести:

- 1) выбор базовой архитектуры, допускающей и облегчающей применение средств повышения живучести;
- 2) последовательное применение принципа параллельности (параллелизм алгоритмов, программ, устройств, данных, маршрутов передачи информации);
- 3) использование и разумное сочетание всех видов избыточности (временной, структурной, энергетической, информационной);
- 4) многофункциональность программного и аппаратного обеспечения;
- 5) автономность и модульность построения устройств, блоков, подсистем;
- 6) частичная децентрализация процессов управления;

7) наличие и обеспечение работы процедур контроля, диагностики и восстановления;

8) введение специальных механизмов и подсистем обеспечения живучести (реконфигурации, перераспределения ресурсов, постепенной функциональной деградации).

Как правило, живучесть системы достигается при использовании всех или части перечисленных принципов, реализованных в виде средств аппаратно-программной поддержки процессов в однородных программируемых древовидных структурах [2].

Для обеспечения живучести однородных древовидных структур на СБИС ПЛМ предлагаются следующие алгоритмы:

- Алгоритм оценки параметров;
- Алгоритм реконфигурации;
- Алгоритм восстановления;

В данной работе используются все три алгоритма, реализованные на языке Delphi 4.0. Программный продукт, представляет собой проект, состоящий из нескольких модулей. Каждый модуль имеет свой набор функций и процедур и предназначен для выполнения конкретных задач.

При помощи программного продукта, реализующего алгоритмы оценки параметров, реконфигурации и восстановления, приведенные в данной работе, были проведены некоторые эксперименты с двумя видами древовидной структуры (бинарное дерево с одной резервной вершиной на каждом уровне и бинарное дерево с дополнительным резервом на каждом уровне), причем каждая из них тестировалась по несколько раз с различными параметрами живучести узлов, связей, количеством резервных узлов и резервных связей.

Анализы проводились на древовидных структурах с 4 уровнями. Созданный удобный и простой интерфейс позволяет легко создавать и редактировать любую древовидную структуру. Быстро произвести анализ и расчёт живучести, удобно и доступно отобразить расчётные характеристики, как в цифровом, так и графическом формате. Все результаты представлены в виде таблиц и графиков, что позволяет более наглядно изучить полученные результаты исследования.

Литература.

1. IEEE Trans. Comput. Отказоустойчивость в архитектуре двоичного дерева, 1984, V. 33, №6.
2. IEEE Trans. Comput. Перестраиваемые программируемые логические матрицы с высоким выходом годных схем, 1990, V. 39, №4, p. 480-489.

ЗАЩИТА ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СЕТЯХ

А.И. Галабурда

(БГТУ, г. Минск)

Развитие средств шифрования стимулируется распространением электронной коммерции, виртуальных частных сетей и растущим числом мобильных сотрудников.

Особую роль в вопросе унификации и стандартизации играют различные стандарты и протоколы, а также продукты на их основе.

Универсальный протокол, основанный на использовании цифровых сертификатов, являющийся в настоящее время стандартом де-факто для решения проблемы безопасности для Web технологий был разработан компанией Netscape Communications, Inc. Этот протокол получил название SSL (Secure Sockets Layer). В настоящее время SSL используется наиболее распространенными программными продуктами для World-Wide-Web (в том числе браузерами Netscape и Microsoft Explorer) для работы в защищенном режиме HTTPS (HTTP Secure).

Он позволяет решить следующие задачи:

- Обеспечить сокрытие передаваемой информации
- Обеспечить целостность этой информации, т.е. защиту от модификации
- Обеспечить аутентификацию сервера и клиентов

Протокол SSL обеспечивает безопасную передачу данных:

- Закрытое соединение. Для шифрования данных используются симметричные алгоритмы (DES[DES], RC4[RC4])
- Аутентификация узлов производится с использованием асимметричных алгоритмов (RSA[RSA], DSS[DSS]).
- Используется надежное соединение. При передаче используется проверка целостности данных с использованием ключевого MAC. Для вычисления MAC используются надежные хеш функции (SHA, MD5).

Защита подразумевает систему распределения сертификатов. Сертификационный центр обеспечивает персональными сертификатами администраторов виртуальных компьютеров и сайт сертификатами - сервера ресурсов. При создании специальных защищенных ресурсов внутри виртуальных компьютеров возможно предоставление персональных сертификатов и пользователям. Все управление подсистемами осуществляется администраторами по защищенному протоколу SSL/TLS. Использование СУБД во многом упроща-

ет схему взаимодействия подсистем и обеспечивает гибкость. В качестве системы защиты от несанкционированного доступа возможно использование FireWall, Ip filter или специализированных, типа Kweb. Пополнение перечня используемых в портале подсистем осуществляется созданием нового программного обеспечения, реализующего новые функции, единого на все виртуальные компьютеры с общей системой пополнения и выбора информации.

Для унификации средств защиты, а также для обеспечения поддержки разработчикам фирма "Микрософт" заложила в свою операционную систему Windows Crypto Api- интерфейс для обеспечения приватности данных.

Программный интерфейс CryptoAPI фирмы Microsoft предоставляет возможности для добавления в приложение, основанное на базе Win32, функций аутентификации, шифрования, расшифрования и электронной подписи. Для написания программы использующей CryptoAPI не надо знать конкретных реализаций алгоритмов шифрования, как не надо знать, например, процедур управления графической картой при использовании графической библиотеки.

Задачами CryptoAPI являются:

- Аутентификация сетевых пользователей
- Шифрование и дешифрование сетевых сообщений
- Шифрование и дешифрование данных
- Создание цифровой подписи и ее подтверждение

CryptoAPI состоит из пяти различных функциональных областей, взаимодействующих с приложением.

В корне иерархии находится криптопровайдер. Напрямую к провайдеру (CSP) приложение обратиться не может.

Функции кодирования сертификатов – эти функции управляют сертификатами и сопутствующими данными через сеть OSI (соединение открытых систем, семиуровневая модель) как описано в CCITT X.200. Методы OSI, описывающие абстрактные объекты, используют абстрактную синтаксическую нотацию один (ASN.1), как описано в CCITT X.209.

Функции базы сертификатов – используются для хранения сертификатов и управления ими. Пользователь со временем может собрать весьма много сертификатов. Обычно это сертификаты описывающие самого пользователя и сертификаты сущностей с которыми он взаимодействует. Обычно для каждой сущности есть несколько сертификатов - связей, используемых для проверки отслеживания существующих сертификатов у авторитета сертифи-

катов (обычно это сайт с сертификатами, отвечающий своим авторитетом за их верность).

Базовые криптографические функции – используются для наиболее полного использования криптографических возможностей в приложении. Это функции взаимодействующие с провайдером. Все криптографические операции выполняются независимыми модулями называемыми Cryptographic Service Providers (CSP). Каждый CSP предлагает различные реализации криптографической поддержки используемой через CryptoAPI. Некоторые провайдеры несут более сильные алгоритмы, некоторые содержат физические компоненты (смарткарты, криптоускорители). В дополнение, некоторые CSP могут напрямую работать с пользователем при использовании личного ключа или подписи.

Однако, версии операционной системы Windows отличаются по функциональным возможностям. Наиболее полно Crypto Api реализован в Windows 2000.

Такие инструментальные средства, как CryptoAPI, и новые, получившие поддержку в отрасли API-интерфейсы, разработанные компаниями RSA Data Security, IBM, JavaSoft, Netscape Communications и др., способны дать толчок широкому применению шифрования, поскольку превращают подобные алгоритмы в стандартные средства операционных систем. Шифрование может быть реализовано на разных уровнях. Самый нижний – это микросхемы и адаптеры, кодирующие, к примеру, данные, передаваемые по сетевому кабелю или отправляемые с рабочей станции. В то же время одной из наиболее привлекательных новых технологий является разработанный Рабочей группой инженеров Internet (IETF) протокол IPsec, предусматривающий стандартный способ шифрования трафика на уровне IP. Он может заменить патентованные решения, предлагаемые производителями брандмауэров и маршрутизаторов. Протокол IPsec включен в некоторые инструментальные средства шифрования и ПО маршрутизаторов.

Вот одно из применений CryptoApi. Одним из нововведений Windows 2000 и NTFS 5.0 является Encrypted File System (EFS), которая используется для шифрования файлов. NTFS по сути является защищенной файловой системой, однако в связи со все более широким распространением таких утилит, как NTFS-Dos, позволяющих обойти систему защиты NTFS, требуется дополнительный уровень защиты файловой системы. Система EFS использует

шифрование с открытым и закрытым ключом и архитектуру CryptoAPI. EFS может использовать любой симметричный алгоритм шифрования файлов, однако первоначальная версия использует только DES. В Северной Америке используются 128-битные ключи, а за ее пределами - 40-битные ключи.

В настоящее время закладываются предпосылки для унификации и стандартизации средств шифрования, что в свою очередь позволяет встраивать криптографическую защиту в программы и операционные системы на более высоком уровне.

Литература:

1. Schneier, Bruce. Applied Cryptography. John Wiley & Sons, 1996.
2. <http://www.bdv.newmail.ru/>
3. RSA Laboratories, a division of RSA Data Security, Inc., RSA Data Security, Inc. Public-Key Cryptography Standards (PKCS), Copyrightc 1991-1993.

СИСТЕМА АУТЕНТИФИКАЦИИ KERBEROS.

А.И. Галабурда

(БГТУ, г. Минск)

Используемые некогда лишь в правительственных учреждениях, таких как Агентство национальной безопасности и военные организации, алгоритмы шифрования сегодня нашли применение в коммерческом ПО брандмауэров. Этот процесс в значительной степени стимулируется распространением электронной коммерции, виртуальных частных сетей и растущим числом мобильных сотрудников. Сейчас улучшению защиты данных, передаваемых между узлами Internet, уделяется самое пристальное внимание.

Особую роль в вопросе унификации и стандартизации играют различные стандарты и протоколы, а также продукты на их основе.

Одним из нововведений Windows 2000 является система распределения ключей Kerberos 5.0. Kerberos – протокол аутентификации, основанный на распределении секретной информации, т.е. пользователь и ЦРК знают пароль пользователя. Кроме клиента и сервера применяется третий участник системы обмена ключевой информацией – ЦРК, которому «доверяют» и клиент и сервер. Протокол предполагает серию передач информации между клиентами, ЦРК, и серверами для получения и использования «билетов» kerberos.

Процесс аутентификации происходит следующим образом: клиент посылает запрос на сервер аутентификации (ЦРК) на предмет получения подключения к определенному серверу. Сервер аутентификации зашифровывает информацию, необходимую для подключения, клиентским ключом и передает клиенту. Информация по подключению содержит «билет» для сервера и временный ключ шифрования, называемый сессионным ключом. Клиент передает «билет», содержащий информацию уникальную для данного клиента, и однозначно идентифицирующую его, и копию сессионного ключа, зашифрованные ключом сервера, на сервер. Сессионный ключ с этого момента разделяем между клиентом и сервером и служит для аутентификации клиента, и может использоваться для аутентификации сервера. Он также может использоваться для шифрования передаваемой информации и для обмена новыми сессионными ключами.

Когда пользователь производит операцию входа в Windows, сервиспровайдер Kerberos получает первоначальный «билет» из зашифрованного значения хеш функции, для которой данными служит пароль пользователя. Операционная система сохраняет «билет» на компьютере пользователя. Когда пользовательская программа пытается получить доступ к сетевым ресурсам, kerberos проверяет хранилище ключей на предмет подходящего сессионного ключа для сервера. Если такого не оказалось «билет» отправляется по запросу на ЦРК для получения сессионного ключа, который бы позволил получить доступ к серверу. В свою очередь этот «билет» также сохраняется для последующего использования с этим сервером. Срок действия ключа может истечь, тогда процедура аутентификации повторяется. Срок действия ключа определяется доменной полиикой.

Windows 2000 реализует ЦРК, как сервис аутентификации, в каждом контроллере домена. Клиент kerberos реализован как провайдер безопасности, основанный на SSP. Первоначальная аутентификация kerberos интегрирована в загрузку системы, реализованную как архитектура единичной подписи. Сервер kerberos ЦРК интегрирован в существующие сервисы безопасности Windows, работающие на контроллере домена. Он использует службу каталога Active Directory как хранилище информации о аккаунтах пользователей.

Протокол аутентификации kerberos улучшает базовые сервисы безопасности Windows:

- Быстрая процедура аутентификации во время установления соединения.
- Делегирование прав при мультисерверной архитектуре.
- Поддержка политика доверия прав при междоменной аутентификации.

Литература:

1. RFC1510
2. <http://msdn.microsoft.com/>

ВЫЧИСЛЕНИЕ ХАРАКТЕРИСТИК ХАОТИЧЕСКОЙ ДИССИПАТИВНОЙ ДИНАМИЧЕСКОЙ СИСТЕМЫ

Н.В. Маньяков

(БГТУ, Брест)

Диссипативные динамические системы характеризуются притяжением всех траекторий, проходящих через некоторую область фазового пространства, к геометрическому объекту, называемому аттрактором. В то же время хаотические динамические системы обладают чувствительностью к заданию начальных условий. Т.е. две близкие в некоторый момент времени траектории через небольшой промежуток времени будут значительно отставать одна от другой. Значит в одних направлениях происходит притяжение, а в других разбегание траекторий. Но учитывая диссипацию весь n -мерный объем необходимо должен сокращаться.

Характеристиками изменения этого объема служат показатели Ляпунова, положительные в некоторых направлениях в случае расходимости траекторий, что характеризует хаотичность системы. Причем сумма всего спектра показателей должна быть отрицательна, что необходимо для диссипации.

Метод вычисления всех показателей Ляпунова основан на вычислении логарифма изменения n -мерного объема в направлениях собственных векторов матрицы Якоби фазового потока динамической системы [1]. В случае, если известны только временные ряды изменения фазовых переменных системы на небольшом промежутке времени, а не система уравнений этой системы, это сделать очень сложно.

Для преодоления этого предлагается использовать нейронную сеть (многослойный персептрон) [2]. Использование ее основано на предложенном

Колмогоровым и Арнольдом решению 13-ой проблемы Гильберта об аппроксимации любой непрерывной функции суперпозицией нелинейных функций.

Тогда имея n временных рядов, характеризующих изменение всех фазовых переменных, построим трехслойную нейронную сеть с одним скрытым слоем с нелинейной функцией активации и с количеством равным n нейронам во входном и выходном слоях. Обучаем сеть, подавая на вход значения временных рядов в момент времени t и ставя за цель получение точек соответствующих временных рядов в момент времени $(t+1)$. Тем самым обученная нейронная сеть будет способна предсказывать временные ряды на один шаг вперёд и полностью аппроксимировать хаотическую диссипативную динамическую систему.

Выбирая теперь в касательном пространстве к многообразию (к аттрактору) ортонормированный базис подаем координаты его концов на нейронную сеть. Как итог получаем образы этих векторов \overline{w}_i ($i = \overline{1, n}$) (задаваемых своими конечными точками). Проводя ортогонализацию этих векторов по методу Грама-Шмитта, получаем новые n ортонормированных векторов \overline{w}_i^0 ($i = \overline{1, n}$), которые в свою очередь подаем на вход сети. И так далее продолжаем итерировать процесс. На k -ом шаге имеем:

$$d_i^k = \left| \overline{w}_i \right|,$$

$$\overline{w}_i^0 = \frac{\overline{w}_i}{d_i^k},$$

.....

$$\overline{v}_j = \overline{w}_j - \sum_{i=1}^{j-1} (\overline{w}_j \cdot \overline{w}_i^0) \cdot \overline{w}_i^0,$$

$$d_j^k = \left| \overline{v}_j \right|,$$

$$\overline{w}_j^0 = \frac{\overline{v}_j}{d_j^k},$$

.....

где ряды ряды чисел d_i^k характеризуют сокращение n -мерного объема.

Тогда показатели Ляпунова вычисляются по формуле $\lambda_i = \lim_{k \rightarrow \infty} \frac{1}{k} \sum_{n=1}^k \ln d_i^n$.

Таким образом были вычислены показатели Ляпунова для временных рядов отображения Энона:

$$\begin{cases} X_{k+1} = Y_k + 1 - \alpha \cdot X_k^2 \\ Y_{k+1} = \beta \cdot X_k \end{cases}$$

Данная система была просчитана для 500 точек, начиная с точки (0,0). В соответствии с этим были получены временные ряды для координат X и Y соответственно на Рис.1 и 2.

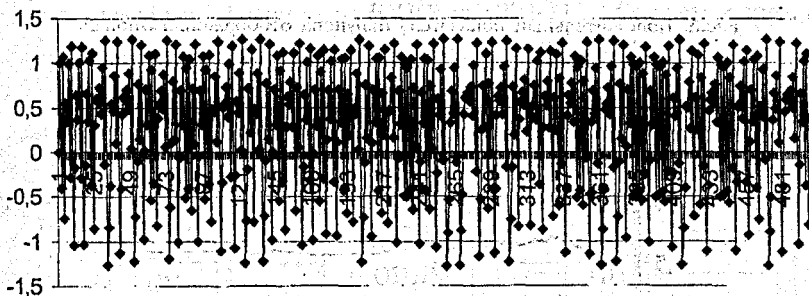


Рис.1 Координата X отображения Энона.

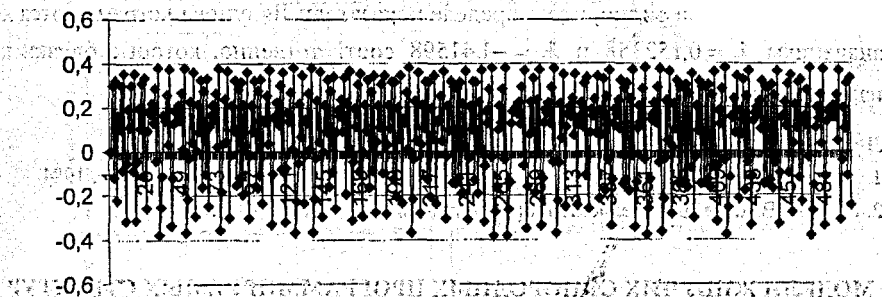


Рис.2 Координата Y отображения Энона.

На этих временных рядах была обучена нейронная сеть (MLP) 2-5-2 с гиперболическим тангенсом в качестве функции активации элементов внутреннего слоя. Среднеквадратичная ошибка обучения после 500 итераций составила $6,76565 \cdot 10^{-9}$.

При вычислении показателей Ляпунова были получены следующие графики (Рис. 3 и 4), характеризующие показатели Ляпунова от количества итераций используемых при их вычислении.

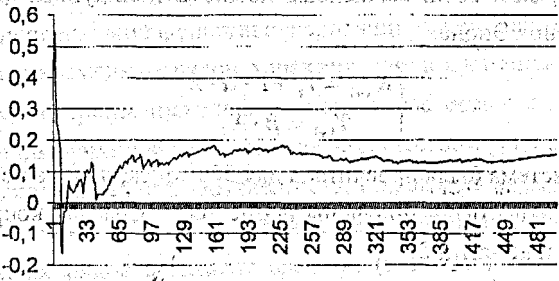


Рис.3. Положительный показатель Ляпунова отображения Энона.

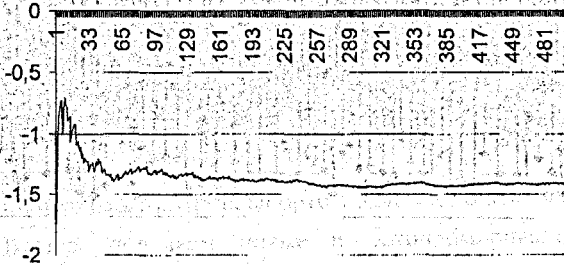


Рис.4. Отрицательный показатель Ляпунова отображения Энона.

Из рисунков видно, что в пределе показатели Ляпунова устремляются к значениям $\lambda_1 = 0,152358$ и $\lambda_2 = -1,41598$ соответственно, которые близки к известным показателям Ляпунова отображения Энона.

Литература.

1. Лихтенберг А., Либман М. Регулярная и стохастическая динамика – М.: Мир, 1984.
2. Головки В.А. Нейроинтеллект: теория и применение, книга 1 – Брест, 1999.

МОДЕЛИ ЖИВУЧИХ ОДНОРОДНЫХ ПРОГРАММИРУЕМЫХ СТРУКТУР

И.К. Мирончиков

(БГСХА, г. Горки)

В настоящее время заслуживает внимания подход к проектированию различных средств цифровой техники, блоков устройств вычислительных систем на базе однородных программируемых структур на СБИС. Обладая регулярной структурой и хорошими эксплуатационными характеристиками однородные программируемые среды (матричные или древовидные) на СБИС занимают передовые позиции в проектировании живучих кристаллов [1].

Для обеспечения живучести таких структур в условиях отказов необходимо следующее: 1) контроль за состоянием ресурсов; 2) самодиагностирование отказов; 3) средство локализации отказавшего вычислительного элемента; 4) реконфигурация ресурсов; 5) создание информационной подсистемы, содержащей данные о ресурсах и их функциональных возможностях; 6) процедуры самовосстановления; 7) периодическая запись текущего состояния структуры.

На рис. 1 приведена обобщенная модель функционирования однородной программируемой структуры (ОПС) на СБИС ПЛМ с учетом средств самодиагностирования, реконфигурации и самовосстановления.

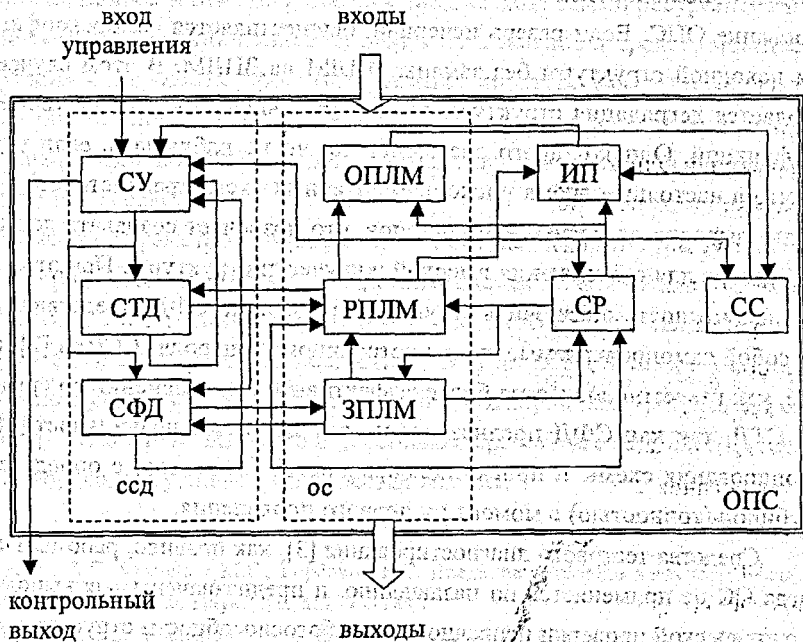


Рис. 1 Модель функционирования живой однородной программируемой структуры на СБИС ПЛМ.

Модель содержит: средства управления (СУ) процессами самодиагностирования, реконфигурации и самовосстановления, а также информационной подсистемой; средства самодиагностирования (ССД), состоящие из средств тестового диагностирования (СТД) и средств функционального диагностирования (СФД); объект самовосстановления (ОС), включающий работо-

способные ПЛМ (РПЛМ), запасные ПЛМ (ЗПЛМ) и отказавшие ПЛМ (ОПЛМ) со средствами функционального диагностирования; средства самореконфигурации (СР) с функциональным диагностированием; средства самовосстановления (СС) и информационную подсистему (ИП).

РПЛМ со средствами функционального диагностирования, выполняющие все рабочие функции программируемой структуры, составляют исходную структуру. В случае отказа, что фиксируется СФД, неисправная ПЛМ исключается (средствами реконфигурации) из исходной структуры и заменяется на ЗПЛМ. Отказавшая ПЛМ включается в число ПЛМ, подлежащих восстановлению. Средства самовосстановления, восстанавливая ОПЛМ, пополняют число ЗПЛМ и восстанавливают правильное функционирование ОПС. Если резерв исчерпан, осуществляется самореконфигурация исходной структуры без замены ОПЛМ на ЗПЛМ. В этом случае наблюдается деградация структуры за счет уменьшения числа выполняемых ею функций. Однако такого состояния можно не наблюдать, если учесть, что в настоящее время число элементарных схем (транзисторов) в кристалле выросло до десятков миллионов, что позволяет создавать достаточный резерв для обеспечения высокой живучести структуры. При этом имеется возможность обеспечить структуру средствами СФД, представляющими собой самопроверяемые схемы встроенного контроля (ССВК) [2], которые, как известно, являются более эффективными в сравнении со средствами СТД, так как СФД предназначены для проверки правильности функционирования схемы и поиска неисправностей (дефектов) с определенной глубиной (точностью) в момент их первого проявления.

Средства тестового диагностирования [3], как правило, работают тогда, когда ОС не применяется по назначению, и предназначены для выполнения периодической проверки исправности и работоспособности структуры, а также поиска дефектов с более высокой точностью в сравнении с функциональным диагностированием. При этом для анализа результатов тестовых воздействий СТД должны иметь определенную информацию о поведении исправного ОС, а также о его поведении в неисправных состояниях, которая хранится в ИП. СТД осуществляют сравнение информации об ОС, хранящейся в ИП и поступающей в СТД через СУ, с фактическими результатами тестовых воздействий и выдают в СУ результаты сравнения, результаты самодиагностиро-

вания через СУ используются СР, выбор которых зависит от количественного и качественного состава ресурсов структуры и принципов их распределения в СБИС. Если рассматриваемая структура имеет вид матрицы из ПЛМ, то в этом случае подсчитывается заранее несколько вариантов эффективных работоспособных конфигураций, ресурсами которых могли бы выполняться все заданные функции или их часть, и это число вариантов запоминается в ИП структуры для использования средствами реконфигурации, осуществляющими выбор соответствующего неисправности варианта конфигурации и оптимальное уменьшение времени реконфигурации. Таким образом реконфигурация как избыточной, так и минимальной структуры с целью устранения последствий ошибок и отказов и обеспечения необходимыми ресурсами выполнение заданных функций является одним из важнейших средств повышения живучести однородных программируемых структур. Кроме того, важную роль в обеспечении живучести таких структур играют средства самовосстановления, среди которых наиболее эффективными являются аппаратурно-программные средства [4].

Анализ параметров отказоустойчивости СБИС ПЛМ, полученных на основе предложенных структурных, аналитических и программных моделей [5], а также рассмотренные средства обеспечения живучести свидетельствуют о том, что решение проблемы построения живучих средств цифровой техники возможно путем проектирования на базе однородных программируемых структур (типа СБИС ПЛМ) со встроенными средствами самодиагностирования, самореконфигурации и самовосстановления.

Литература:

1. Додонов А.Г. Кузнецов М.Г., Горбачик Е.С. Введение в теорию живучести вычислительных систем. -- Киев: Наук. думка, 1990.-184 с.
2. Согомонян Е.С., Слабаков Е.В. Самопроверяемые устройства и отказоустойчивые системы. - М.: Радио и связь, 1989.
3. Коротаев Н.А., Мирончиков. И.К. Обеспечение живучести компьютерных сетей //Сетевые компьютерные технологии: Сб. трудов Междунар. науч. конф. 25-29 октября 2000 г., Минск. - Мн.: БГУ, 2000.-с.132-135.
4. Коротаев Н.А., Высоцкий М.М. Выбор и исследование средств самовосстановления отказоустойчивых СБИС ПЛМ//Актуальные проблемы информатики...Материалы V межгосударственной науч. Конф., 14-18 мая 1996 г.- Минск - с. 29-36.
5. Коваль В.Н. Самодиагностирование программируемых СБИС//Диссертация канд. техн. наук, БГУ. - Минск, 1992. - 197 с.

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ РАСПРЕДЕЛЕНИЯ И ИСПРАВЛЕНИЯ ОШИБОК В ЭЛЕМЕНТАХ ПАМЯТИ

А.В. Орлов

(БГТУ, г. Минск)

Компьютерная модель памяти предназначена для рассмотрения алгоритмов распределения отказов в элементах памяти, оптимизации нахождения ошибок, расчета и определения эффективности исправляющих корректирующих кодов.

Анализ методом имитационного моделирования заключается в определении происходящих в системе памяти событий и их привязки к моментам дискретного времени и элементам системы.

Время, в котором функционирует моделируемый объект, называется *модельным*. Дискретизация модельного времени производится путем разбиения заданного для имитации интервала $[0, T_k]$ на участки. Любое событие, происшедшее на участке с границами t_i и t_{i+1} , считается происшедшим в момент времени t_{i+1} .

Математическая модель, готовая к имитации прохождения заявок, представляет собой программу, включающую ряд операторов. Операторы, относящиеся к группе основных, вызывают действия над заявками. Это операторы генерирования заявок, направления заявок к определенным узлам (микросхема памяти, строка, столбец, ячейка), постановки в очередь на обслуживание, занятия узла, освобождения и др. Исполнение такой программы по отношению к конкретной заявке выявляет ее маршрут и времена прохождения этапов маршрута. Однако поведение заявки в системе не является независимым, оно обуславливается событиями, в которых фигурируют также другие заявки. Поэтому процесс имитации на ЭВМ должен отображать хронологию событий в последовательности, имеющей место в реальной работе микросхем памяти. В связи с этим исполнение программы имитации по отношению к конкретной заявке, например заявке A , должно прерываться, когда заявка задерживается в очереди или в обслуживающем аппарате, и программа должна переходить к имитации более ранних событий, чем события, связанные с дальнейшим продвижением по маршруту заявки A .

Для соблюдения при имитации правильной хронологии событий все события, которые в данный момент модельного времени уже можно предвидеть,

упорядочиваются по времени наступления и оформляются в виде списка. Элементами списка являются имена (ссылки) заявок, с которыми связаны рассматриваемые события. В списке событий можно выделить его начало – *список текущих событий*, т. е. событий, которые должны произойти в текущий момент времени t_i . Остальная часть списка называется *списком будущих событий*.

После того как программа прерывает имитацию прохождения заявкой A своего маршрута, она переходит к обработке очередного события из списка текущих событий. Пусть это событие связано с заявкой B . Программа исполняется, начиная с того оператора, который ранее определил задержку заявки B , и доходит до такого оператора, который означает новую задержку заявки B . Если эта задержка происходит в связи с обслуживанием в некотором устройстве, то при этом определяется, длительность обслуживания, и, следовательно, момент времени $t_i + \tau$, в который, обслуживание закончится. Далее ссылка на заявку B включается в список будущих событий на место, определяемое значением $t_i + \tau$. После этого программа выбирает очередной элемент из списка текущих событий и имитирует продвижение новой заявки. Сведения о том месте, в котором была задержана заявка и с которого, следовательно, нужно возобновлять продвижение, фиксируются в специальном массиве параметров заявок.

После того как все события текущего момента времени t_i исчерпаны, модельное время увеличивается до значения времени t_{i+1} ближайшего события, список событий в момент времени t_{i+1} становится списком текущих событий. Процесс имитации продолжается по тому же алгоритму. Окончание процесса имитации связывается с исчерпанием всего списка событий или с прохождением всего заданного интервала времени T_k .

Следовательно, имитационное моделирование осуществляется путем многократного просмотра операторов имитационной модели и выполнения предписываемых ими действий. Просмотр операторов относится только к тем моментам времени, в которые произошли какие-либо события. При просмотре происходят обращения к математическим моделям тех элементов памяти, с которыми связаны происходящие события. Такое моделирование, избирательное по времени и месту событий, называется *событийным*. Использование принципа событийности позволяет выполнять только те действия, которые действительно необходимы для получения результата, и, следовательно, приводит к сокращению затрат машинного времени.

Программная реализация алгоритмов событийного моделирования представляет собой пакет подпрограмм, реализующий математические модели элементов, программы, осуществляющие процедуры выработки случайных чисел, статистической обработки результатов моделирования и др. Управляющая программа пакета содержит обращения к подпрограммам устройств, источников, памятей, с ее помощью реализуются ввод исходных данных, упорядочение списков событий, изменение модельного времени, продвижение заявок.

В базе данных (БД), с которой работает программа имитации, имеются следующие основные массивы данных:

Массив очередей и списков. Массив очередей упорядочен по устройствам, массив списков — по моментам наступления событий. Элементами этих массивов являются ссылки на заявки. Поэтому при обработке списков по этим элементам могут быть найдены адреса, по которым хранятся сведения о самих заявках.

Массив заявок. Здесь хранятся сведения о каждой заявке: имя заявки, ее тип, значения приоритетов, время очередного события, связанного с заявкой, текущее место нахождения заявки. Доступ к этому массиву осуществляется по ссылкам заявок, содержащимся в массивах очередей и списков.

Массив параметров элементов. В нем содержатся значения таких параметров, как числовые характеристики законов распределения интервалов обслуживания, данные о дисциплинах обслуживания, накопленные суммы, характеризующие на текущий момент время занятого состояния каждого устройства, количество обслуженных заявок, длины очередей, средние времена ожидания в очередях и т. п.

Процесс исполнения программы имитации и ее взаимодействия с БД показан на рис. 1. Каждый этап вычислений, начинается с выборки очередного элемента из списка текущих событий. Этот элемент представляет собой имя заявки (ее адрес в массиве заявок). Обозначим имя обрабатываемой заявки A . По извлеченным из массива заявок сведениям определяется имя освобождающегося OA и номер оператора в программе имитации, с которого будет прослеживаться продвижение заявки A . Сначала программа имитации проверяет наличие очереди на входе освободившегося OA и, если очередь имеется, OA начинает обслуживать некоторую заявку B из очереди в соответствии с заданной дисциплиной обслуживания. При этом происходит обращение к подпрограмме рассматриваемого OA , определяется время обслуживания и тем са-

мым становится предвидимым новое событие – окончание обслуживания заявки *B* в этом *OA*. Ссылка на это событие помещается в список будущих событий, и производятся изменения сведений о заявке *B* в массиве заявок. Далее имитируется продвижение в системе заявки *A*. Это продвижение прерывается, когда в соответствии с заданной программой производится запрос на обслуживание заявки *A* в некотором *OA*. При этом происходит обращение к массиву очередей по имени этого *OA* и либо поступление заявки *A* на обслуживание, либо ее постановка в очередь. Изменения, произошедшие в состояниях очередей, обслуживающих аппаратов и заявок, отражаются в изменении соответствующих данных в массиве параметров.

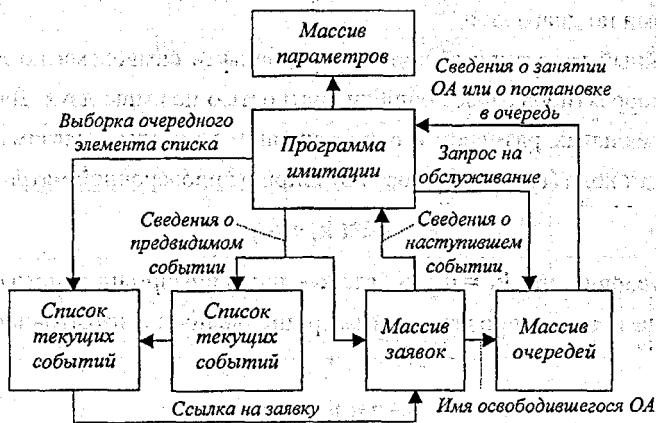


Рис. 1: Взаимодействие программы имитации с массивами БД

Литература.

1. Норенков И.П., Маничев В.Б. Системы автоматического проектирования электронной и вычислительной аппаратуры. – М.: Высшая школа, 1983, 272 с.
2. Северцев Н.А. Надежность сложных систем в эксплуатации и отработке. – М.: Высшая школа, 1989, 432 с.

ОПТИМИЗАЦИЯ ПАРАМЕТРОВ ПРОВЕРОЧНЫХ МАТРИЦ ДЛЯ ЛИНЕЙНОГО И ТРЕХМЕРНОГО ИТЕРАТИВНОГО КОДОВ С ПРОВЕРОЧНЫМИ СИМВОЛАМИ ПО ДИАГОНАЛИ

Д.М. Романенко
(БГТУ, г. Минск)

Наблюдаемое в последние годы резкое увеличение информационных потоков и связанное с этим ужесточение требований к целостности обрабаты-

ваемой информации резко обострили проблему надежного хранения и передачи двоичной информации. Один из способов решения такой проблемы заключается в использовании помехоустойчивого кодирования данных с помощью избыточных кодов.

Одним из этапов как разработки новых, так и совершенствования старых избыточных кодов является определение оптимальных размеров их проверочных матриц. Так как код должен корректировать все ошибки заданной кратности, то основным критерием оптимизации будет выступать величина избыточности, которая должна быть минимальна. В [1] описаны два новых избыточных кода: линейный и трехмерный итеративные коды с проверочными символами по диагонали.

Линейный итеративный код с проверочными символами по диагонали позволяет корректировать все ошибки кратностью не выше двух. Для определения оптимальных размеров его проверочной матрицы выразим величину избыточности кода (r) в зависимости от ширины проверочной матрицы k_1 .

$$r = 2 * (k_1 + k_2). \quad (1)$$

При условии, что $k_1 = k / k_2$, где k – длина информационного слова, k_1 , k_2 – ширина и длина проверочной матрицы, величина избыточности будет равна

$$r = 2 * (k_1 + k / k_1). \quad (2)$$

Оптимальные размеры матрицы будут достигаться при минимуме величины избыточности r . Для определения оптимального k_1 про дифференцируем зависимость $r = f(k_1)$ по k_1 , приравняем полученное выражение к нулю. Решая данное уравнение, получим, что минимум величины избыточности достигается при $k_1 = k / 2$. Следовательно, квадратная матрица является оптимальной с точки зрения избыточности для линейного итеративного кода с проверочными символами по диагонали.

Трехмерный итеративный код с проверочными символами по диагонали, описанный в [1], может использоваться в двух видах: со стандартной и урезанной проверочными матрицами. Для определения оптимальных размеров данных матриц была разработана специальная программа на языке Delphi. Полученные результаты представлены в таблицах 1 и 2 (для стандартной матрицы – табл. 1, для урезанной матрицы – табл. 2).

Таблица 1

Длина информационного слова, k	Размерность матрицы $k_1 \times k_2 \times k_3$	Величина избыточности, r	Относительная избыточность $G_{отн}$, %
8	$2 \times 2 \times 2$	28	350
16	$2 \times 2 \times 4$ $4 \times 2 \times 2$	44	275.0
32	$4 \times 4 \times 2$	64	200.0
64	$4 \times 4 \times 4$	96	150.0
128	$8 \times 4 \times 4$	152	118.7
256	$8 \times 8 \times 4$	224	87.5
512	$8 \times 8 \times 8$	352	68.7
1024	$16 \times 8 \times 8$	560	54.7
4096	$16 \times 16 \times 16$	1344	32.8

Таблица 2

Длина информационного слова, k	Размерность матрицы $k_1 \times k_2 \times k_3$	Величина избыточности, r	Относительная избыточность $G_{отн}$, %
8	$2 \times 2 \times 2$ $4 \times 2 \times 1$	21	262.5
16	$4 \times 4 \times 1$ $4 \times 2 \times 2$	33	206.2
32	$4 \times 4 \times 2$	49	153.1
64	$4 \times 4 \times 4$ $8 \times 4 \times 2$	81	126.6
128	$8 \times 8 \times 2$ $8 \times 4 \times 2$	129	100.8
256	$8 \times 8 \times 4$	193	75.4
512	$8 \times 8 \times 8$ $16 \times 8 \times 4$	321	62.7
1024	$16 \times 8 \times 8$ $16 \times 16 \times 4$	513	50.1
4096	$16 \times 16 \times 16$ $32 \times 16 \times 8$	1281	31.3

Как видно из табл.1 и табл.2, в обоих случаях оптимальной является проверочная матрица, близкая к кубической, либо кубическая (если при заданной длине информационного слова такую матрицу можно построить). При использовании урезанной проверочной матрицы, как правило, существует две оптимальные матрицы. С точки зрения аппаратной реализации и построения

алгоритма коррекции целесообразно использовать проверочную матрицу с $k_1=k_2$, т.е. с квадратной проверочной матрицей для линейного итеративного кода в плоскости.

Литература.

1. Урбанович П.П., Романенко Д.М. Свойства и алгоритмы аппаратной реализации нового вида итеративных кодов для систем памяти // Новые информационные технологии: третья международная конференция NITE'2000, т. 2 – Мн.: БГЭУ, 2000. – с. 159–164.

АЛГОРИТМЫ КОРРЕКЦИИ МНОГОКРАТНЫХ ОШИБОК ТРЕХМЕРНЫМ ИТЕРАТИВНЫМ КОДОМ С ПРОВЕРОЧНЫМИ СИМВОЛАМИ ПО ДИАГОНАЛИ

Д.М. Романенко

(БГТУ, г. Минск)

Поступательное и все ускоряющееся улучшение основных эксплуатационных параметров (быстродействие, емкость ОЗУ – оперативных запоминающих устройств – и др.) персональных компьютеров и других средств вычислительной техники, продиктованное необходимостью внедрения новых информационных технологий, базируется на улучшении адекватных параметров, прежде всего, полупроводниковых устройств хранения и выдачи информации (ОЗУ, ПЗУ, ППЗУ). Принятое за рубежом направление усовершенствования таких ЗУ основывается на создании систем памяти, интегрированных на целой полупроводниковой пластине (WSI – wafer scale integration).

При использовании WSI в качестве ЗУ естественным представляется обобщение итеративных кодов на трехмерный случай. Возможность такого обобщения появляется благодаря тому, что в WSI суммарная емкость системы набирается из однотипных элементов – блоков. Физически такой способ кодирования можно представить в виде куба или параллелепипеда, состоящего из n одинаковых накопителей (отдельных блоков кристалла), "наложенных" друг на друга. Боковые стенки этого куба образуются совокупностью элементов четности n матриц. Верхняя грань является совокупностью элементов четности всех элементов, содержащихся в каждой матрице. В дальнейшем на основе общих характеристик кодов прямого произведения получим основные характеристики кода и рассмотрим его техническую реализацию применительно к WSI.

В [1] описан метод получения трехмерного итеративного кода, а также подробно описаны его свойства. Так трехмерный итеративный код с проверочными символами по диагонали характеризуется следующими параметрами: избыточность (r), минимальное кодовое расстояние (d), скорость (R), эффективность коррекции ошибок.

Величина избыточности равна

$$r = 2*(k_1+k_2)*k_3 + 2*(k_1+k_2), \quad (1)$$

где k_1 и k_2 – количество строк и столбцов в линейном итеративном коде с проверочными символами по диагонали;

k_3 – количество плоскостей в трехмерном итеративном коде.

Если $k_1 = k_2 = k_3$, то

$$r = 6*k_m^2, \quad (2)$$

следовательно,

$$n = k + r = k_m^3 + 5*k_m^2. \quad (3)$$

Тогда скорость (R) определяется следующим соотношением:

$$R = k/n = k_m/(k_m + 5). \quad (4)$$

Величина относительной избыточности ($r_{отн}$) равна

$$r_{отн} = r/k = 5/k_m. \quad (5)$$

Минимальное кодовое расстояние трехмерного итеративного кода, согласно теореме 3 [1], будет $d=10$, а это значит, что код исправляет до четырех ошибок включительно.

Теорема [1] задает способ построения кода, но не дает алгоритмов декодирования, в то же время известно, что декодирование любого кода является наиболее трудоемкой операцией. Поскольку кодирование информации производится тривиальным перемножением проверочной матрицы на транспонированный вектор передаваемого сообщения (можно использовать алгоритмы построения проверочных матриц для дополненного итеративного кода), в дальнейшем сосредоточимся именно на декодировании. Сложности реализации декодеров особенно возрастают при коррекции ошибок, число которых больше единицы. При этом иногда возникают ситуации, когда сложность декодера приводит к таким значительным временным и аппаратным затратам, что сводит на нет корректирующие способности кода. Поэтому более подробно остановимся на различных алгоритмах коррекции многократных ошибок.

В докладе представляется разработанный специальный алгоритм коррекции ошибок кратностью не выше четырех. Данный алгоритм строится на принципах, аналогичных положенным в основу коррекции многократных ошибок дополненным линейным итеративным кодом [1], т. е. с использование hvd классификации с учетом проверок z -рядов (т.е. проверок на четность вдоль оси OZ) [1].

Если ограничить кратность ошибок, которые должны быть исправлены до $(d-1)/2+1$, если d – нечетное, и $(d-2)/2+1$, если d – четное, где d – минимальное кодовое расстояние трехмерного итеративного кода с проверочными символами по диагонали, то для коррекции ошибок можно использовать следующий алгоритм: в случае возникновения ошибки кратностью $(d-1)/2+1$ или $(d-2)/2+1$ координаты ошибки определяются по Z – рядам, “показавшим” о наличии ошибки; в случае возникновения ошибок кратностью меньше $(d-1)/2+1$ или $(d-2)/2+1$ ошибки исправляются силами линейных итеративных кодов с проверочными символами по диагонали. Для реализации данного алгоритма можно использовать урезанную проверочную матрицу, т.е. из проверочной матрицы исключаются паритеты паритетов. В данном случае, хотя и происходит уменьшение кратности корректируемых ошибок, одновременно снижается избыточность кода, а также существенно упрощается алгоритм коррекции. Так избыточность стандартной проверочной матрицы трехмерного итеративного кода с проверочными символами по диагонали при $k = 1024$ равна $r = 560$; при той же длине информационного слова для усеченной проверочной матрицы $r = 513$. Избыточность уменьшилась на 8.4%. Для усеченной проверочной матрицы величина избыточности будет определяться по следующей зависимости:

$$r = 2 * (k_1 + k_2) * k_3 + k_1 * k_2 + 1. \quad (6)$$

При $k_1 = k_2 = k_3$ величина избыточности будет равна

$$r = 5 * k_m^2 + 1, \quad (7)$$

следовательно,

$$n = k + r = k_m^3 + 5 * k_m^2 + 1. \quad (8)$$

Тогда скорость (R) определяется следующим соотношением:

$$R = k/n = 5 * k_m^2 + 1 / (k_m^3 + 5 * k_m^2 + 1). \quad (9)$$

Величина относительной избыточности ($r_{отн}$) равна

$$r_{отн} = r/k = k_m^5 * k_m^2 + 1 / k_m^3. \quad (10)$$

Данный алгоритм является общим для всех трехмерных кодов, полученных путем прямого (кронекеровского) произведения двух кодов, при условии, что одним из кодов сомножителей является свертка по модулю два. Вторым сомножителем может быть любой код, например код Хемминга.

Литература.

1. Урбанович П.П., Романенко Д.М. Свойства и алгоритмы аппаратной реализации нового вида итеративных кодов для систем памяти // Новые информационные технологии: третья международная конференция NITE'2000, т. 2 – Мн.: БГЭУ, 2000. – с. 159–164.

2. Мак-Вильямс Ф., Слоэн Н. Теория кодов, исправляющих ошибки / пер. с англ. под ред. Л.А. Басальго. – М.:Связь, 1979, –746с.

ИСПОЛЬЗОВАНИЕ ГИПЕРБОЛИЧЕСКИХ БРАУЗЕРОВ ДЛЯ ВИЗУАЛИЗАЦИИ БОЛЬШИХ ИЕРАРХИЧЕСКИХ СТРУКТУР

В.С. Скращук, В.М. Волчкевич, Д.Н.Кортелев

(ГрГУ, г. Гродно)

В работе предлагается метод создания динамически настраиваемых эффективных средств для графического представления иерархических структур, основанный на технологии “фокус+контекст”.

Рост объема информации, производимой обществом, заставил обратить внимание на факт отсутствия эффективных средств для ее визуального представления, исследования и поиска. В связи с этим вырос интерес к аспектам информационного исследования средств и методов визуализации, цель которого состоит в том, чтобы обнаружить и развить пути усиления человеческого познания.

Один из способов усиления познания видится в том, чтобы увеличить количество информации, которая может быть помещена в центр внимания пользователей.

Среди новых подходов в области создания средств поиска для систем управления данными выделяется метод визуальных моделей, основанный на технологии «фокус+контекст»[1]. Метод «фокус+контекст» - один из информационных методов визуализации, направленных на увеличение количества информации, которая может быть показана пользователю за счет того, что интересующие его данные выводятся на передний план и в то же время сохраняется структура даже очень больших наборов данных.

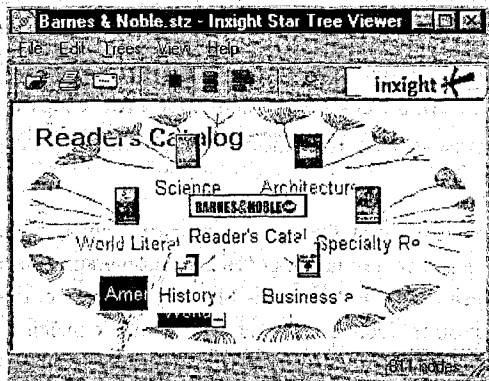


Рис. 1. Окно гиперболического браузера, построенного по технологии "фокус+контекст" (811 узлов)

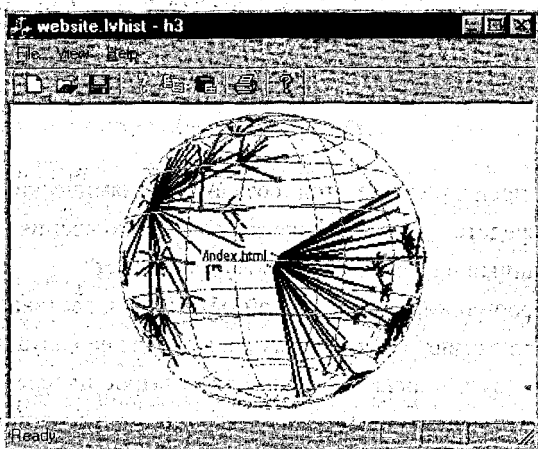


Рис. 2. 3D- гиперболический браузер, построенный по H3-технологии (11000 узлов)

К примеру, компания InXight Software, отделившаяся от Xerox PARC, выпустила собственное средство визуализации Star Tree Viewer [2]. В его основу положен гиперболический браузер (или «рыбий глаз»), использующий гиперболическую геометрию для расширения информационного пространства при работе с иерархическими структурами, которые расширяются экспоненциально с увеличением глубины. Гиперболический браузер может показать порядка 1000 узлов в окне размером 600x600 пикселей, в центре которого высвечивается текст довольно большого объема. Для сравнения, стандартный 2D-браузер (например, программа «Проводник» ОС семейства Windows) может показать на экране не больше 100 узлов). Пользователь может перемещаться

по информационному пространству; щелкая мышью на интересующих его узлах или передвигая их указателем мыши по гиперболической плоскости.

В работе [3] предложен H3-метод изображения больших направленных графов в виде диаграмм связи узлов в 3D-гиперболическом пространстве. Метод позволяет показать намного большие структуры, чем это позволяют сделать традиционные методы изображения графов. Используя проблемно-зависимые знания об отображаемой структуре, строится остовное дерево. Дуги, которые не входят в остовное дерево, могут быть выборочно показаны по запросу пользователя. H3-метод позволяет отображать графы, содержащие больше 20000 узлов.

Среди недостатков реализации указанных выше методов можно отметить их "статичность" – отображаемые иерархические структуры должны быть заранее сформированы и представлены гиперболическому браузеру в необходимом формате. Т.е. отсутствуют средства для оперативной, настройки их на конкретную среду применения и динамической перестройки графовой структуры, отображаемой в окне браузера.

Предлагаемая в докладе реализация гиперболического браузера ориентирована на использование его в качестве навигатора по структуре каталогов файловой системы. Очевидно, что структура каталогов, расположение файлов данных и их типы заранее не известны. Работа начинается с показа графовой структуры, состоящей из единственной вершины, соответствующей корневому каталогу диска. При выборе такой вершины "мышью" считывается и отображается в окне браузера реальная структура каталогов первого уровня и информация о файлах, хранящихся в корневом каталоге. Далее, при выборе одной из вновь изображенных вершин графа, соответствующей каталогу диска, в реальном режиме времени считывается и отображается структура и содержание такого каталога. При выборе вершины, соответствующей файлу данных, можно либо получить информацию о свойствах файла (имя, тип, размер, дата создания и т.п.) или открыть его, используя возможности документо-ориентированного интерфейса Windows.

Для улучшения наглядности и повышения информационных качеств отображаемой структуры, в программе предусмотрена возможность перемещения вершин графа с помощью "мыши", что позволяет плавно перетаскивать их в центр гиперболической плоскости. Кроме того, разработанный гиперболический навигатор допускает несколько режимов просмотра и снабжен

удобной системой контекстных меню. Реализована также функция приближения/удаления гиперболической плоскости, что позволяет изменять масштаб изображения.

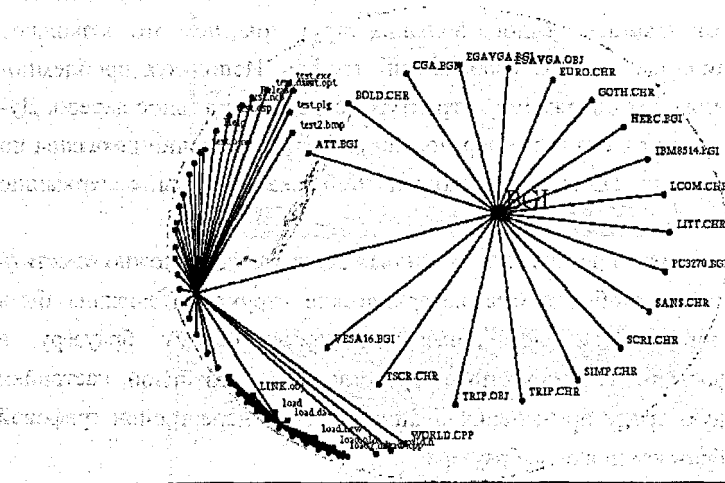


Рис. 3. Гиперболический навигатор для визуализации структуры файловой системы

Для решения традиционно сложной задачи “укладки графа” используются методы моделирования физических систем: взаимодействие вершин подчиняется закону всемирного тяготения, длина дуг графа – законам упругости, перемещения вершин – условиям сопротивления среды. Расположение вершин графа на гиперболической плоскости определяется как результат решения соответствующих систем уравнений.

Гиперболический навигатор реализован на языке C++. Для отображения графовой структуры использована среда OpenGL. Для взаимодействия с ресурсами операционной системы – библиотека GLUT.

Литература:

1. J. Lamping, R. Rao, and P. Pirolly, «A Focus+Context Technique Based on Hiperbolic Geometry for visualizing Large Hierarchies,» Proc. SigChi, ACM Press, New York, 1995.
2. http://www.inxight.com/products_wb/tree_studio/index.html
3. T.Munzner. PhD Thesis Defense: Interactive Visualization of Large Graphs and Networks. Stanford CA, 4/00.

ОЦЕНКИ АЛГОРИТМОВ ЦИФРОВОЙ ПОДПИСИ

А.М. Суходольский., Д.П. Урбанович

(БГУИР, г. Минск)

Введение

Большинство методов аутентификации электронных сообщений базируются на тех или иных криптографических алгоритмах. Такие методы аутентификации электронных сообщений существуют давно, но только с появлением нового направления в криптографии [1] они стали выполнять все требования, которые предъявляются к цифровой подписи.

Новое направление в криптографии связано с введением понятия *системы с открытыми ключами*. Одна из таких систем появилась в 1978 году, как результат работы трёх её авторов R. Rivest, A. Shamir, L. Adleman, и сейчас носит название RSA [2].

Такие криптосистемы с самого начала были ориентированны на обеспечение возможности выполнения с помощью них *цифровой подписи* электронных документов. Для полноты картины здесь необходимо упомянуть ещё одну систему с открытыми ключами, автором которой является Т. El Gamal [3] и которая стала основой для создания государственных стандартов на цифровую подпись США (Digital Signature Standard - DSS).

В статье анализируются сравнительные оценки некоторых алгоритмов формирования и использования электронной подписи.

Особенности использования цифровой подписи

Приведём сравнительную оценку обычной подписи (под обычной подписью мы здесь понимаем подпись и печать) с цифровой подписью с точки зрения выполняемых ими защитных функций.

Защита целостности документа. В случае применения обычной подписи и печати после подписания документ может быть изменён (например, допечатано пару нулей). Изменить же электронный документ, подписанный цифровой подписью, невозможно, поскольку содержание документа через его дайджест "включается" в саму подпись.

Подделка подписи. Чтобы подделать обычную подпись достаточно иметь компьютер, цветные сканер и принтер, а также образец подписи и печати. Стоимость перечисленного оборудования в настоящее время не превышает \$2000. Далее дело техники. Для подделки цифровой подписи, при рекомендуемой специалистами на настоящее время длине ключей, необходимо

иметь специальный суперкомпьютер стоимостью несколько сот миллионов долларов и запас по времени приблизительно в 300 – 500 лет. Если длину ключей увеличить в два раза, то стоимость оборудования и время вычисления подписи резко возрастают.

Конфиденциальность. Документ, подписанный обычной подписью, может быть прочитан любым лицом, к которому он попал в руки. В случае цифровой подписи предусматривается режим, когда документ может быть прочитан только лицом, которому он адресован.

Оценка некоторых алгоритмов цифровой подписи

Проведем теперь сопоставление некоторых конкретных алгоритмов цифровой подписи с целью выявления их преимуществ и недостатков в различных ситуациях. Для удобства оценки основных свойств того или иного алгоритма мы будем сравнивать его основные характеристики: длину ключей, длину цифровой подписи, сложность (время) вычисления и сложность (время) проверки подлинности цифровой подписи при условии, что уровень стойкости подписи по отношению к любым методам фальсификации не ниже, чем 10^{21} (или 30 лет непрерывной работы сети из 1000 суперкомпьютеров). В качестве "базовой" длины ключей и длины самой цифровой подписи мы будем рассматривать длину в 64 байта.

RSA. Первым по времени изобретения конкретным алгоритмом цифровой подписи был разработанный в 1977 году в Массачусетском технологическом институте алгоритм RSA. Алгоритм RSA основывается на том математическом факте, что задача дискретного логарифмирования при выборе целого параметра n в виде произведения двух различных простых чисел примерно равных по порядку величины, т.е. $n = p * q$ становится не менее сложной, чем разложение n на эти простые множители, а последняя задача давно (еще со времен Архимеда и Евклида) известна в математике как сложная.

По современным оценкам сложность задачи разложения на простые множители при целых числах n из 64 байт составляет порядка $10^{17} - 10^{18}$ операций, т.е. находится где-то на грани досягаемости для серьезного "взломщика". Поэтому обычно в системах цифровой подписи на основе алгоритма RSA применяют более длинные целые числа n (обычно от 75 до 128 байт).

Это соответственно приводит к увеличению длины самой цифровой подписи относительно 64-байтного варианта примерно на 20% - 100% (в данном случае ее длина совпадает с длиной записи числа n), а также от 70% до 800% увеличивает время вычислений при подписывании и проверке.

Кроме того, при генерации и вычислении ключей в системе RSA необходимо проверять большое количество довольно сложных дополнительных условий на простые числа p и q (что сделать достаточно трудно и чего обычно не делают, пренебрегая вероятностью неблагоприятного исхода - возможной подделки цифровых подписей), а невыполнение любого из них может сделать возможным фальсификацию подписи со стороны того, кто обнаружит невыполнение хотя бы одного из этих условий (при подписывании важных документов допускать, даже теоретически, такую возможность нежелательно).

DSA. Национальным институтом стандартов и технологий США в 1991 году на основе алгоритма Эль-Гамала [3] был разработан и представлен на рассмотрение Конгресса США новый алгоритм цифровой подписи, получивший название DSA (сокращение от Digital Signature Algorithm). Алгоритм DSA, ставший в дальнейшем основой национального стандарта США на цифровую подпись, имеет по сравнению с алгоритмом RSA целый ряд преимуществ: во-первых, при заданном уровне стойкости цифровой подписи целые числа, с которыми приходится проводить вычисления, имеют запись как минимум на 20% короче, что соответственно уменьшает сложность вычислений не менее чем на 70% и позволяет заметно сократить объем используемой памяти; во-вторых, при выборе параметров достаточно проверить всего три достаточно легко проверяемых условия; в-третьих, процедура подписывания по этому методу не позволяет вычислять (как это возможно в RSA) цифровые подписи под новыми сообщениями без знания секретного ключа.

Эти преимущества, а также соображения, связанные с возможностью его реализовывать любым разработчиком свободно без коммерческих лицензионных соглашений с держателями патента, компанией RSA Data Security, и возможностью свободного безлицензионного экспорта такой технологии из США послужили главным мотивом для принятия в 1994 году национального стандарта цифровой подписи (DSS) на его основе.

Кроме того, в практике в последние годы нередко встречаются алгоритмы цифровой подписи, основанные на вычислениях с алгебраическими кривыми. Эти алгоритмы позволяют значительно сократить длину цифровой подписи при сохранении надежности защиты от подделки, но научная основа оценок их надежности настолько сложна математически, что говорить о широко известной сложной задаче, лежащей в основе надежности цифровой подписи, уже не приходится. В этом случае пользователю приходится полностью доверять мнению

очень узкой группы экспертов. И даже поверхностное представление о современных оценках надежности этих алгоритмов получить не просто.

Литература

1. W. Diffie and M.E. Hellman. New directions in cryptography//IEEE Trans. on Info. Theory, vol. IT-22, pp. 644-654, Nov. 1976.
2. R. Rivest, A. Shamir, and L. Adleman. A Method for Obtaining Digital Signatures and Public Key Cryptosystems//Commun. of the Assoc. of Comp. Math., Vol. 21, pp. 120-126, Feb. 1978.
3. T. El Gamal. A Public - Key Cryptosystem and a Signature Scheme Based on Discrete Logarithm// IEEE Trans. on Info. Theory, vol. IT-31, pp. 469-472, July 1985.

НЕКОТОРЫЕ АСПЕКТЫ ПРОБЛЕМЫ ИСПОЛЬЗОВАНИЯ ЭЛЕКТРОННОЙ ПОДПИСИ

Д.П. Урбанович

(БГУИР, г. Минск)

Введение

Тенденции развития вычислительной техники и математики стимулируют развитие новых, принципиально отличающихся технологий решения информационных задач в различных сферах. Одним из таких направлений является *электронная коммерция*. Проблемы, возникающие и решаемые в указанной области, активно обсуждаются на конференциях и в печати (см., например, [1]). Ниже проанализируем особенность одной из проблем: *электронную подпись*.

О подписи вообще

Все современные информационные технологии, связанные с обменом электронных документов, в своей основе содержат "кирпичик", который получил название *цифровая подпись*. К системам, использующим такие технологии, относятся автоматизированные банковские системы типа "Клиент - Банк", системы для обеспечения электронных платежей в Интернет, платёжные системы на основе *smart-card*, другие коммерческие и секретные системы связи.

Любая подпись, будь-то обычная или цифровая, всегда выполняет, по крайней мере, три функции: первая - это удостоверение того, что подписавшийся является тем, за которого мы его принимаем (функция авторизации); вторая - это то, что подписавшийся не может отказаться от документа, который он подписал; и третья - подтверждение того, что отправитель подписал именно тот документ, который отправил, а не какой-либо иной. Другими словами, ему нельзя навязать другой или похожий документ, поскольку у него есть подпи-

санная копия оригинала. Заметим, что две первые функции обеспечивают защиту интересов лица, для которого предназначен документ (приемника), а третья - защищает интересы подписывающего (передатчика). Во всех этих случаях "работает" свойство подписи, называемое *аутентичность*, т.е. подлинность. Это свойство переносится на документ, под которым стоит подпись.

Аутентификация сообщений является жизненно важным фактором для всех абонентов как коммерческих, так и секретных систем связи. Например, лица, принимающие чек, обычно настаивают на подтверждении личности выписывающего чек - аутентификации источника информации, или передатчика, а лицо, выписывающее чек, проставляет сумму не только цифрами, но и прописью. Таковы простейшие способы аутентификации передаваемой информации или сообщений.

Говоря в доступных терминах, аутентификация - это не более и не менее, как установление приёмником и, возможно, арбитром того факта, что при существующем протоколе (правилах) аутентификации данное сообщение послано санкционированным (законным) передатчиком и что оно при этом не заменено и не искажено. Большинство методов аутентификации электронных сообщений базируются на тех или иных криптографических алгоритмах. Такие методы аутентификации электронных сообщений существуют давно, но только с появлением нового направления в криптографии [3] они стали выполнять все требования, которые предъявляются к цифровой подписи.

Новое направление в криптографии связано с введением понятия *системы с открытыми ключами*. Одна из таких систем появилась в 1978 году, как результат работы трёх её авторов R. Rivest, A. Shamir, L. Adleman, и сейчас носит название RSA [3].

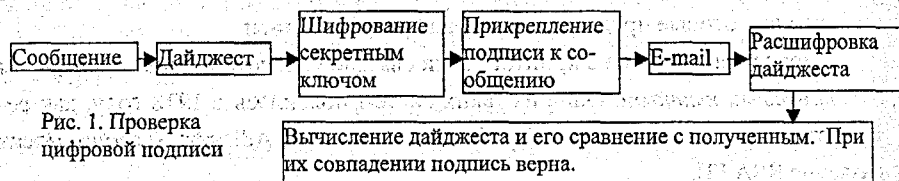
Такие криптосистемы с самого начала были ориентированны на обеспечение возможности выполнения с помощью них цифровой подписи электронных документов. Для полноты картины здесь необходимо упомянуть ещё одну систему с открытыми ключами, автором которой является Т. El Gamal и которая стала основой для создания государственных стандартов на цифровую подпись США (Digital Signature Standard - DSS).

Цифровая подпись

Предположим, что некоторый абонент А хочет подписать какое-либо сообщение и отправить его абоненту В. Для этого он, с помощью специальной математической функции, так называемой *хеш-функции*, создаёт *дайджест* (слепок) этого сообщения. Односторонняя хеш-функция не использует ключ.

Это обычная формула для преобразования послания любой длины в одну строку символов (дайджест послания). При использовании 16-байтной хеш-функции обработанный ей текст будет иметь на выходе длину 16 байт — например, послание может быть представлено цепочкой символов CBVV235ndsAG3D67. Каждое послание образует свой случайный дайджест. Затем зашифровывает его своим секретным ключом Е. Свойства хеш-функции таковы, что полученный с помощью её дайджест “жестко” связан с сообщением. Зашифрованный дайджест “прикрепляется” к сообщению, теперь он является цифровой подписью сообщения.

Абонент В использует открытый ключ абонента А для расшифровки цифровой подписи и получает копию дайджеста послания от А. Поскольку он сумел расшифровать цифровую подпись открытым ключом А, то значит, А является ее автором. Затем В использует ту же самую хеш-функцию (о которой оба договорились заранее) для подсчета собственного дайджеста для открытого текста послания А. Если полученная им строка совпадает с той, что прислал А, то он может быть уверена в аутентичности цифровой подписи. А это означает не только то, что отправитель послания А, но также и то, что послание не было изменено. На рис. 1 показана упрощенная схема процессов выполнения подписи документа и проверки подписи получателем в таких системах.



Для шифрования открытого текста послания следует дополнительно использовать симметричный алгоритм с секретным ключом. Но это приведет к дальнейшему усложнению процесса. Таким образом, цифровая подпись на основе систем с открытыми ключами полностью выполняет три функции подписи, которые были перечислены выше.

Литература.

1. Урбанович Д.П. Принципы организации и использования возможностей электронной коммерции и бизнеса// II International Symposium NEET'2001. New Electrical & Electronic technologies & their industrial implementation. Symposium Proceedings. Poland. 14-17.02.2001.
2. Kosiur D. Understanding electronic Commerce, Microsoft Press, 1998. – 288 p.
3. R. Rivest, A. Shamir, and L. Adleman, A Method for Obtaining Digital Signatures and Public Key Cryptosystems, Commun. Of the Assoc. of Comp. Math., Vol. 21, pp 120-126, Feb. 1978.

ПРИКЛАДНЫЕ АСПЕКТЫ ИНФОРМАТИКИ И МАТЕМАТИКИ**ОДНОМЕРНАЯ МОДЕЛЬ МИКРОСТРУКТУРЫ
СТРОИТЕЛЬНЫХ МАТЕРИАЛОВ**

А.Р. Афонин

(БГТУ, г. Брест)

Большинство строительных материалов имеют сложную микроструктуру, в которую входят поры и скелет материала, содержащий, как правило, разнородные включения. Среди способов количественного описания микроструктуры материалов наиболее широко применяются два. Первый способ состоит в измерении распределения пор по радиусам с помощью, например, ртутной интрузии. Второй способ заключается в наблюдении под микроскопом и измерении линейных размеров сечений частиц (пор) материала, находящихся на прямолинейном отрезке. Появляется естественный вопрос, каким должно быть распределение пор по радиусам или же распределение линейных размеров сечений частиц при предположении, что частицы (поры) распределены наиболее хаотично.

По-видимому, простейшей моделью, описывающей хаотичное распределение пор по размерам, является одномерная модель, представляющая материал в виде плоских параллельных слоев скелета, разграниченных такими же плоскими параллельными порами. В этом случае структура материала определяется распределением длин сечений пор (или скелета), расположенных на прямолинейном отрезке, перпендикулярном плоским слоям вещества. При наблюдении материала под микроскопом основной характеристикой структуры также является распределение длин сечений на прямолинейном отрезке.

Предположим, что распределение длин сечений одной компоненты материала (например, пор) не зависит от распределения длин сечений остальных компонент (например, элементов скелета). Таким образом, рассматривая распределение одной компоненты, можно удалить все остальные, заменив их точками на отрезке. Полученная структура распределения изучаемой компоненты представляет собой отрезок, разбитый на части точками. Предположим

также, что точки, лежащие на отрезке, распределены по нему независимо одна от другой и равномерно, что соответствует максимальной хаотичности.

Пусть отрезок длины L разбит на n отрезочков с длинами $x_k \geq 0$ ($k=1, \dots, n$):

$$\sum_{k=1}^n x_k = L. \quad (1)$$

Упорядочим отрезочки по возрастанию длины:

$$x_k \leq x_{k+1}, \quad (k=1, \dots, n-1). \quad (2)$$

Выражая x_n из (1), получим систему неравенств, описывающую область в $n-1$ – мерном пространстве, каждая точка которой представляет собой один из вариантов разбиения:

$$\begin{cases} x_1 \geq 0; \\ x_k \leq x_{k+1}, \quad (k=1, \dots, n-2); \\ x_{n-1} \leq L - \sum_{i=1}^{n-1} x_i. \end{cases} \quad (3)$$

Нас будет интересовать математическое ожидание такого упорядоченного разбиения. Иными словами, будем искать центр масс области (3), исходя из того, что точки в $n-1$ – мерном пространстве распределены равномерно:

$$x_{n,k}^c = \frac{I_{n,k}}{V_n}, \quad (4)$$

где $x_{n,k}^c$ – проекция центра масс на k -ю ось координат;

V_n – объем области (3);

$I_{n,k}$ – момент первого порядка относительно k -й оси.

Величины V_n и $I_{n,k}$ даются интегралами по области (3):

$$V_n = \int_0^{\frac{1}{n}L} dx_1 \cdots \int_{x_{m-1}}^{L - \sum_{i=1}^{m-1} x_i} dx_m \cdots \int_{x_{n-2}}^{L - \sum_{i=1}^{n-2} x_i} dx_{n-1}, \quad (5)$$

$$I_{n,k} = \int_0^{\frac{1}{n}L} dx_1 \cdots \int_{x_{m-1}}^{L - \sum_{i=1}^{m-1} x_i} dx_m \cdots \int_{x_{n-2}}^{L - \sum_{i=1}^{n-2} x_i} dx_{n-1} x_k. \quad (6)$$

Опуская выкладки, запишем результаты интегрирования:

$$V_n = \frac{L^{n-1}}{n!(n-1)!}, \quad (7)$$

$$I_{n,1} = \frac{L^n}{(n!)^2 n}, \quad (8)$$

$$I_{n,k+1} = \frac{1}{(n-k)^2} \left[LV_n + (n-k-1)(n-k)I_{n,k} - \sum_{i=1}^k I_{n,i} \right]. \quad (9)$$

Разделив (8) и (9) на V_n из (7), получим искомое среднее распределение упорядоченных по возрастанию отрезочков в виде рекуррентной зависимости:

$$x_{n,1}^c = \frac{L}{n^2}, \quad (10)$$

$$x_{n,k+1}^c = \frac{1}{(n-k)^2} \left(L - \sum_{i=1}^k x_{n,i}^c \right) + x_{n,k}^c \left(1 - \frac{1}{n-k} \right). \quad (11)$$

Практический интерес представляет ситуация, когда $n \gg 1$. В этом случае можно заменить сумму в (11) интегралом, а разность $x_{n,k+1}^c - x_{n,k}^c$ — производной $\frac{dx_{n,k}^c}{dk}$, считая при этом, что $di = dk = 1 \ll n$:

$$\frac{dx_{n,k}^c}{dk} - \frac{1}{(n-k)^2} \left(L - \int_1^k x_{n,i}^c di \right) + \frac{x_{n,k}^c}{n-k} = 0. \quad (12)$$

Умножая (12) на $(n-k)^2$ и дифференцируя по k , получим дифференциальное уравнение

$$(n-k) \frac{d^2 x_{n,k}^c}{dk^2} - \frac{dx_{n,k}^c}{dk} = 0, \quad (13)$$

решение которого, учитывая (10) и условие (1), записанное как

$$\int_1^n x_{n,k}^c dk = L, \quad (14)$$

имеет вид:

$$x_{n,k}^c = x_{cp} \ln \frac{n}{n-k}, \quad (15)$$

где $x_{cp} = L/n$ — средний размер отрезочка.

Выражая из (15) k/n , будем иметь так называемую интегральную частотную функцию, нормированную на единицу:

$$F_{\text{ч}}(x) = 1 - \exp(-x/x_{\text{ср}}). \quad (16)$$

Дифференцируя по x , получим дифференциальную частотную функцию:

$$f_{\text{ч}}(x) = \exp(-x/x_{\text{ср}})/x_{\text{ср}}. \quad (17)$$

Частотные функции применяются при количественном описании результатов наблюдения материалов под микроскопом.

Интегрируя (15) по k и умножая на Π/L , будем иметь интегральную функцию распределения объема пор по размерам для одномерной модели, представляющей материал в виде плоских параллельных слоев:

$$F_V(x) = \Pi \{1 - (1 + x/x_{\text{ср}}) \exp(-x/x_{\text{ср}})\}, \quad (18)$$

где Π – пористость материала.

Дифференцируя (18) по x , получим дифференциальную функцию распределения объема пор по размерам:

$$f_V(x) = \Pi \exp(-x/x_{\text{ср}}) x/x_{\text{ср}}^2. \quad (19)$$

Функции распределения пор по размерам получаются в результате проведения экспериментов по ртутной порометрии.

Результаты вычислительного эксперимента, моделирующего случайное разбиение отрезка, показали, что формулы (11) и (15) действительно представляют математическое ожидание разбиения отрезка равномерно распределенными точками. Опытные данные для бетона и пенопластов подтверждают пригодность формул (11), (16) и (17) для практических расчетов.

ВОССТАНОВЛЕНИЕ РАСПРЕДЕЛЕНИЯ СОПРОТИВЛЕНИЯ В ЭЛЕКТРОИМПЕДАНСНОЙ ТОМОГРАФИИ

А.К. Васечко
(ГрГУ, г. Гродно)

1. Введение. Электроимпедансный томограф открывает много возможностей для исследования внутренних структур, но он не используется широко в практической медицине. На самом деле считается, что существующие системы электроимпедансных изображений должны предлагать, так называемые, дина-

мические изображения (визуальное наблюдение изображения различий двух измерений). В медицине предпочтение отдается статическим или абсолютным изображениям. В электроимпедансной томографии (ЭИТ), получение таких изображений усложнено, так как необходимо получить набор данных, соответствующих однородному участку удельной электропроводности объекта.

Поскольку, на практике электроды томографа зафиксированы непосредственно на коже пациента, то кажется маловероятным получение дополнительных данных для измерений, соответствующих форме тела пациента ни с помощью подбора необходимой формы поверхности однородной удельной электропроводности, ни с помощью численного решения прямой задачи с соответствующими граничными условиями. Использование контейнера цилиндрической формы заполненного проводящей жидкостью, в которую погружается пациент также неподходяще, так как сводятся к нулю преимущества метода: относительная простота медицинского обследования и минимум неудобств пациенту.

В статье описывается алгоритм восстановления распределения сопротивления поперечного сечения человеческого тела по результатам измерения потенциала на электродах, расположенных на поверхности тела человека.

2. Математическая модель для ЭИТ и регуляризация Тихонова. Наиболее точная математическая модель электроимпедансной томографии, называемая полной электродной моделью, может быть записана в форме:

$$\nabla \cdot (\sigma \cdot \nabla u) = 0, \quad x \in \Omega \quad (1)$$

$$u + z_l \sigma \frac{\partial u}{\partial \nu} = U_l, \quad x \in e_l, l = 1, 2, \dots, L \quad (2)$$

$$\int_{e_l} \sigma \frac{\partial u}{\partial \nu} dS = I_l, \quad x \in e_l, l = 1, 2, \dots, L \quad (3)$$

$$\sigma \frac{\partial u}{\partial \nu} = 0, \quad x \in \partial\Omega \setminus \bigcup_{l=1}^L e_l, \quad (4)$$

Здесь Ω – исследуемое тело, L – число электродов на поверхности тела, e_l – l -тый электрод, x – элементарный участок исследуемой модели, σ – проводимость, z_l – контактное сопротивление между l -ым электродом и телом, $u = u(x)$ – это электрический потенциал, который возникает на элементарном участке, U_l – потенциал на электродах, I_l – ток, проникаемый с электродов.

Прямая задача (1-4) решается методом конечных элементов (МКЭ). В случае, когда сетка МКЭ состоит из треугольных элементов распределение сопротивления можно аппроксимировать в пространстве Соболева $W_1^1[\Omega]$. Сопротивление в этом пространстве будет непрерывным и дифференцируемым в смысле Лебега.

Наблюдаемая физическая модель для ЭИТ имеет вид:

$$V = U(\rho) + \varepsilon \quad (5)$$

где $U(\rho)$ – вектор напряжений, получаемый путем решения модели (1-4), при известном распределении сопротивления ρ , V – напряжение на электродах, снимаемое с прибора, ε – измеряемый шум. Нелинейная относительно ρ модель $U(\rho)$ может быть локализована относительно ρ_0 по формуле Тейлора [2]:

$$U(\rho) = U(\rho_0) + J(\rho_0)(\rho - \rho_0) \quad (6)$$

где $U(\rho_0)$ – вектор напряжения для распределения сопротивления ρ_0 , $J(\rho_0)$ – Якобиан U при $\rho = \rho_0$.

Регуляризация Тихонова для задачи ЭИТ заключается в минимизации функционала:

$$\min_{\sigma} \{ \|V - U(\rho_0) + J(\rho_0)\rho_0 - J(\rho_0)\rho\|^2 + W(\rho) \}, \quad (7)$$

где $W(\rho)$ – стабилизирующий функционал, имеющий вид:

$$W(\rho) = \alpha^2 \|L(\rho - \rho_*)\|^2 \quad (8)$$

где α и L – параметр и матрица регуляризации соответственно, ρ_* – вектор, аппроксимирующий искомое решение. В качестве L зачастую выбирается единичная матрица [2].

3. Численные результаты. Скорость сходимости процесса зависит от выбора начального приближения, поэтому положим, $\sigma=1$ (Ом)⁻¹ и предварительно рассчитаем начальное распределение ρ_0 . Из формулы $U=RI$, где U – напряжение, R – сопротивление, I – сила тока получаем:

$$V = \rho_0 \times I \quad (9)$$

$$U_{\sigma=1} = \rho_{\sigma=1} \times I \quad (10)$$

где V – напряжение на электродах, снимаемое с прибора, ρ_0 – искомое распределение сопротивления, $U_{\sigma=1}$ – вектор напряжений на электродах, получаемый путем решения (1-4) при $\sigma=1$ (Ом)⁻¹, $\rho_{\sigma=1}$ – это сопротивление соответ-

вуюющее проводимости σ : $\rho_{\sigma=1}=1/\sigma=1$ Ом, I – это распределение тока на электродах. С учетом этого, получаем начальное сопротивление:

$$\rho_0 = \frac{V}{U_{\sigma=1}}$$

На каждом шаге решения обратной задачи надо находить решение прямой задачи (1-4) и Якобиан (6). Решение задачи – распределение сопротивления в плоском сечении тела – используется для построения плоского изображения этого сопротивления.

Предлагаемая методика решения поставленной задачи проверена расчетами в системе MATLAB 5.2. Модельное изображение задавалось на треугольной сетке, состоящей из 425 узлов и 784 элементов. Была задана реальная проводимость тела и неоднородности, что позволило получить данные (V) для обратной задачи. Восстановление изображения проводилось в три итерации с начальной проводимостью $\sigma=1$ (Ом)⁻¹ и параметром регуляризации $\alpha=0,000005$. Параметр регуляризации подбирался визуально, с учетом получаемого качества изображения. Ошибка восстановления сопротивления составила $\approx 1-2\%$. Образ восстанавливался с предположением о цилиндрической геометрии объекта (торс тела) для лучшего восприятия (Рис.1).

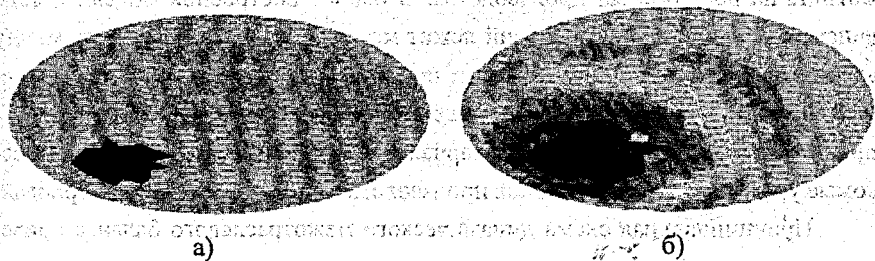


Рис.1. Восстановление распределения сопротивления на модельном примере.

а) – исходное изображение, б) – полученный результат.

В заключение отметим, что качество получаемого изображения может быть улучшено за счет получения образов на различных частотах томографа с последующим их наложением друг на друга, например, системой GRASS.

Литература.

1. Дэннис Дж., Шнабель Р. Численные методы безусловной оптимизации и решения нелинейных уравнений: Пер. с англ. – М.: Мир, 1988.
2. Р. Hua, J.G. Webster, and W.J. Tompkins, "A regularised electrical impedance tomography reconstruction algorithm", Clin Phys Physiol Meas, Suppl A, vol. 9, pp. 137–141, 1988.

ДИНАМИЧЕСКАЯ МЕЖОТРАСЛЕВАЯ БАЛАНСОВАЯ МОДЕЛЬ

Е.В. Гаспадарик

(БГТУ, г. Брест)

Статические межотраслевые балансовые модели [1;2], т.е. модели, в которых все зависимости отнесены к одному моменту времени, разрабатываются лишь для отдельно взятых периодов, причем в рамках этих моделей не устанавливается связь с предшествующими или последующими периодами. В таких моделях капиталовложения вынесены из сферы производства в сферу конечного использования вместе с предметами потребления и производственными затратами, т.е. включены в конечный продукт.

В отличие от статических динамические модели призваны отразить не состояние, а процесс развития экономики, установить непосредственную взаимосвязь между предыдущими и последующими этапами развития и тем самым приблизить анализ на основе экономико-математической модели к реальным условиям развития экономической системы.

В рассматриваемой здесь динамической модели, являющейся развитием статической межотраслевой модели, производственные капитальные вложения выделяются из состава конечной продукции, исследуются их структура и влияние на рост объема производства. В основе построения модели в виде динамической системы уравнений лежит математическая зависимость между величиной капитальных вложений и приростом продукции. Решение системы, как и в случае статической модели, приводит к определению уровней производства, но в динамическом варианте в отличие от статического эти искомые уровни зависят от объемов производства в предшествующих периодах.

Принципиальная схема динамического межотраслевого баланса приведена в следующей таблице:

Производящие отрасли	Потребляющие отрасли									
	Межотраслевые потоки текущих затрат				Межотраслевые потоки капитальных вложений				Конечный продукт	Валовый продукт
	1	2	...	n	1	2	...	n		
1	x_{11}	x_{12}	...	x_{1n}	$\Delta\Phi_{11}$	$\Delta\Phi_{12}$...	$\Delta\Phi_{1n}$	Y_1	X_1
...
i	x_{i1}	x_{i2}	...	x_{in}	$\Delta\Phi_{i1}$	$\Delta\Phi_{i2}$...	$\Delta\Phi_{in}$	Y_i	X_i
...
n	x_{n1}	x_{n2}	...	x_{nn}	$\Delta\Phi_{n1}$	$\Delta\Phi_{n2}$...	$\Delta\Phi_{nn}$	Y_n	X_n

Модель содержит две матрицы межотраслевых потоков. Матрица текущих производственных затрат с элементами x_{ij} совпадает с соответствующей матрицей статического баланса. Элемент $\Delta\Phi_{ij}$ второй матрицы $\Delta\Phi=(\Delta\Phi_{ij})$, $i,j=1\dots n$, показывает какое количество продукции i -ой отрасли направлено в текущем периоде в j -ю отрасль в качестве производственных капитальных вложений в ее основные фонды. Материально это выражается в приросте в потребляющих отраслях производственного оборудования, сооружений, производственных площадей транспортных средств и др.

В статическом балансе потоки капиталовложений не дифференцируются по отраслям и отражаются общей величиной в составе конечной продукции Y_i . В динамической схеме конечный продукт Y_i включает продукцию i -ой отрасли, идущую на личное и общественное потребление, накопление непродуцированной сферы, прирост оборотных фондов, незавершенного строительства, на экспорт. Таким образом, сумма потоков капиталовложений и конечного продукта динамической модели равна конечной продукции статического баланса:

$$\sum_{j=1}^n \Delta\Phi_{ij} + Y'_i = Y_i, \quad i = 1..n.$$

Следовательно, уравнение динамического баланса примет вид:

$$X_i = \sum_{j=1}^n x_{ij} + \sum_{j=1}^n \Delta\Phi_{ij} + Y'_i. \quad (1)$$

Межотраслевые потоки текущих затрат можно выразить из равенства Леонтьева

$$x_{ij} = a_{ij} X_j, \quad (2)$$

где a_{ij} - коэффициенты прямых затрат. Межотраслевые потоки капитальных вложений обуславливают прирост продукции, причем в рассматриваемой модели предполагается, что прирост продукции текущего периода обусловлен вложениями, произведенными в этом же периоде. Если текущий период обозначить через t , то прирост продукции ΔX_j , равен разности абсолютных уровней производства в период t и в предшествующий $(t-1)$ -й период:

$$\Delta X_j = X_j^{(t)} - X_j^{(t-1)} \quad (3)$$

С другой стороны, будем считать, что прирост продукции пропорционален приросту производственных фондов:

$$\Delta \Phi_{ij} = \varphi_{ij} \cdot X_j, \quad i, j = 1..n, \quad (4)$$

где φ_{ij} - коэффициент вложений или коэффициент приростной фондоемкости. Их смысл в том, что они показывают, какое количество продукции i -ой отрасли следует вложить в j -ю отрасль для увеличения производственной мощности j -ой отрасли на единицу продукции.

Окончательно, с учетом (2) и (4) система уравнений (1) представится в виде

$$X_i = \sum_{j=1}^n a_{ij} X_j + \sum_{j=1}^n \varphi_{ij} \Delta X_j + Y_i', \quad i = 1..n \quad (5)$$

Система (5) есть система линейных разностных уравнений первого порядка. Ее можно привести, используя равенства (2)-(4), к обычной системе

$$X_i^{(t)} = \sum_{j=1}^n (a_{ij} + \varphi_{ij}) X_j^{(t)} - \sum_{j=1}^n \varphi_{ij} X_j^{(t-1)} + Y_i^{(t+1)}, \quad i = 1..n \quad (6)$$

Пусть известны уровни валовой продукции всех отраслей в предыдущем периоде $X_j^{(t-1)}$ и конечный продукт отраслей в t -м периоде. Тогда соотношения (6) позволяют определить выпуск продукции в последующем периоде в зависимости от уровня, достигнутого в предыдущем периоде.

Если перейти от дискретных величин к непрерывным, то (4) примет вид

$$\frac{d \Phi_{ij}}{dt} = \varphi_{ij} \frac{d X_j}{dt}$$

и, следовательно, соотношения (5) примут вид

$$X_i = \sum_{j=1}^n a_{ij} X_j + \sum_{j=1}^n \varphi_{ij} \frac{d X_j}{dt} + Y_i', \quad i = 1..n \quad (7)$$

Соотношение (7) - это система n линейных дифференциальных уравнений первого порядка с постоянными коэффициентами. Для ее решения помимо матриц (a_{ij}) и (φ_{ij}) нужно знать уровни валового выпуска в начальный момент времени $t = 0$ и закон изменения величины конечного продукта, т.е. вид функций $Y'(t)$. Решая, таким образом, задачу Коши для системы (7), можно найти уровни выпуска теоретически для любого момента времени.

Литература.

1. Федосеев В.В., Гармаш А.Н. и др. Экономико-математические методы и прикладные модели. -М.: ЮНИТИ. -1999. -391с. 2. Красс М.С. Математика для экономических специальностей. -М.: "ИНФРА-М". -1998. -464с.

ПРИМЕНЕНИЕ ФАКТОРНОГО АНАЛИЗА ДЛЯ КОМПЛЕКСНОЙ ОЦЕНКИ ДЕЯТЕЛЬНОСТИ СУБЪЕКТОВ ХОЗЯЙСТВОВАНИЯ.

Н.В. Гирсева, М.Н. Гриневич

(МГТУ, г. Могилев)

Одним из направлений в методологии исследования деятельности любого субъекта хозяйствования является комплексный экономический подход. Он базируется на изучении объектов как сложных систем, которые состоят из отдельных элементов с многочисленными внутренними и внешними связями. Процессы, протекающие в таких системах, описываются множеством экономических показателей. Однако для анализа и текущего управления многие из этих показателей не являются необходимыми.

Предоставляемая информация должна различаться по содержанию в зависимости от ее назначения и применения в процессе управления. Более подробная информация должна использоваться на низших и средних уровнях системы управления, тогда как в более высокие звенья существующей иерархии управления следует передавать информацию в наиболее сжатой форме. Очевидно, что наличие такой информации в очень серьезной степени способствует совершенствованию процесса управления. Поэтому целесообразно получить как можно меньший набор экономических показателей о наиболее важных сторонах деятельности. Наличие такого рода сведений о протекающих процессах обязательно для проведения быстрой оценки деятельности объектов и своевременного принятия решений на будущий период. Ведь в этом случае внимание руководителей не поглощено изучением обширного перечня аналитических данных, а ограничивается ознакомлением с небольшим количеством обобщенной информации, содержащейся в предлагаемых сводных показателях. Особого внимания при этом заслуживают многомерные сравнения, которые необходимы для комплексной оценки результатов хозяйствования производственных подразделений, предприятий и т.д. Для решения этой задачи довольно широко используют алгоритмы, основанные на методах «суммы мест», геометрической средней и т.д. Но эти методики имеют существенный недостаток, потому что в них не учитывается весомость определенных показателей. Методики многомерного сравнительного анализа с учетом весовых значений показателей несут субъективизм экспертов в виде весов отдельных показателей.

Факторный анализ является наиболее эффективным методом сжатия данных и оценки состояния многомерного объекта управления. Главной целью анализа является установление общих закономерностей, определяющих сущность изучаемого явления. Материалом, на базе которого проводятся такие исследования, служат наблюдения над вариацией значений множества признаков, характеризующих данное явление. Непосредственное раскрытие существующих закономерностей бывает весьма затруднено, а иногда и просто невозможно, если рассматриваемое множество признаков оказывается настолько велико, что избыток информации начинает мешать пониманию наиболее существенных взаимосвязей. Выявление закономерностей облегчается, если среди рассматриваемых признаков найдутся такие, которые сильно коррелированы между собой и потому мало отличаются друг от друга в отношении информации об изучаемом явлении. В таких случаях следует заменить группу сильно коррелированных признаков некой расчетной «синтетической» величиной. Полученная величина после интерпретации называется фактором и рассматривается как одна из закономерностей изучаемого явления. Такая замена групп коррелированных признаков факторами должна производиться с наименьшими потерями информации, заключенной в исходном множестве признаков. Теоретически полное отражение информации, содержащейся в некотором множестве признаков, достигается в том случае, когда число факторов равно числу признаков. На практике же чаще всего такое решение не является необходимым, поскольку лишь первым факторам удается дать ясную экономическую интерпретацию и при этом достигается достаточно полное отражение информации.

Пусть имеется набор элементарных признаков X_j , $j=1, \dots, m$ их взаимодействие предполагает наличие определенных причин, особенных условий, т.е. существование некоторых скрытых факторов. Последние устанавливаются в результате обобщения элементарных признаков и выступают как интегрированные характеристики, или признаки, но более высокого уровня.

Пусть n наблюдаемых объектов оцениваются в m -мерном признаковом пространстве. Переход от множества значений по m элементарным признакам с объемом информации $n \times m$ к ограниченному множеству элементов (r) матрицы факторного отображения ($m \times r$) для каждого наблюдаемого объекта размерностью $n \times r$ производится с использованием методов факторного анализа.

Начинаясь построением матрицы исходных данных X , этот алгоритм завершается получением матриц факторного отображения и значений факторов A и F . Переход от матрицы исходных данных X к матрице стандартизированных значений данных Z осуществляется после пересчета всех элементов x_{ij} по формуле: $z_{ij} = (x_{ij} - x_j) / \delta_j$.

На следующем шаге простым перемножением скаляра $1/n$ и матриц Z' и Z получаем матрицу парных корреляций: $R = (1/n) * Z' * Z$.

Выполнение следующего шага - построение редуцированной матрицы корреляций. В факторном анализе матрица корреляций R преобразуется в Rh с $h_j^2 < 1$, т.е. вариация признаков может быть изменена не на 100%, а несколько меньше, с учетом существования их нераскрываемой характерности.

Этап построения матрицы отображения A заключается в выборе оптимального метода для поиска весовых коэффициентов a_j элементов матрицы A . Наилучшие решения обычно находят при помощи современных методов факторного анализа: главных факторов, максимального правдоподобия и др.

Вращение пространства общих факторов производится в том случае, когда пространственное расположение факторов Fg нелогично или трудно поддается интерпретации. На заключительном этапе алгоритма рассчитывают матрицу значений факторов F , ее элементы - это факторные значения f_i для каждой единицы наблюдения. Тем самым получаем оценку результатов деятельности объектов в виде нескольких интегрированных показателей.

Используя данный подход, проведен анализ деятельности отделений банка за несколько лет. В качестве исходных показателей были взяты: активы, вклады граждан, кредиты клиентам, собственные средства, прибыль, прибыль на 1 работника, прибыльность активов, прибыльность собственного капитала.

В результате применения факторного анализа были получены следующие формулы:

Масштаб операций = 0,9 активы + 0,7 вклады + 0,86 кредиты + 0,81 собственные средства + 0,8 прибыль,

Эффективность = 0,9 прибыльность собственных средств + 0,53 прибыльность активов + 0,64 прибыль на 1 работника.

Также данный метод был применен к анализу автотранспорта Могилевской области как сложной хозяйственной системы. В качестве исходных показателей были взяты грузооборот (Γ), общий пробег по сдельным перевозкам

(ОПС), рентабельность сдельных перевозок (РС), объем перевозок (ОП), платные часы по почасовым перевозкам (ПЧП), рентабельность почасовых перевозок (РП), общий пробег почасовых автомобилей (ОПП).

В результате получены следующие формулы:

Масштаб перевозок = $0,8 Г + 0,83 ОПС + 0,86 ОПП + 0,77 ПЧП$,

Эффективность перевозок = $0,7 РС + 0,37 РП - 0,5 ПЧП - 0,41 ОПП$.

Полученные формулы наиболее легки для экономической интерпретации, что важно для выработки управленческих решений на базе анализа и прогнозирования динамики описываемых этими формулами показателей.

МНОГОУРОВНЕВАЯ СИСТЕМА ОРГАНИЗАЦИИ РАБОТЫ С ИНФОРМАЦИОННЫМИ ПОТОКАМИ ФАКУЛЬТЕТА ВУЗА

Н.В. Десева

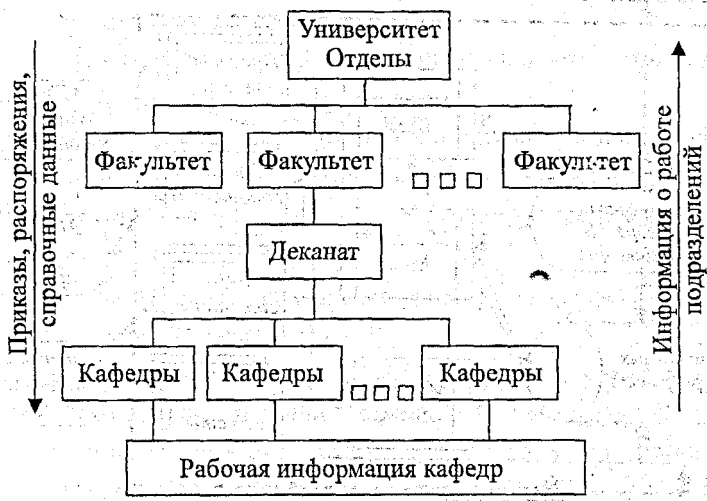
(ГРГУ, г. Гродно)

Высшее учебное заведение, располагая всеми кадровыми, техническими и интеллектуальными возможностями для того, чтобы быть лидером в области синтеза и использования информационных ресурсов, концентрирует и проводит в жизнь идею создания информационного сообщества. Сосредоточение интеллектуальных сил общества в высшей школе определяет ее ведущую роль в развитии информационных систем, телекоммуникационных ресурсов и технологий.

Развитие информационной, управленческой и образовательной инфраструктуры Гродненского государственного университета им. Янки Купалы, а также достигнутая к настоящему времени степень оснащенности подразделений вуза средствами вычислительной техники, однородность технической базы и современный ее технический уровень создали предпосылки для перехода к "качественной" стороне компьютеризации вуза - интеграции служб и подразделений на базе единой системы управления.

Важную роль в организации учебного процесса и управлении им играет взаимодействие кафедр, деканатов факультетов, учебного, учебно-методического, научного отделов и других отделов университета. Взаимодействие ведется на уровне стандартизованных документов и заключается в получении, анализе, подготовке и передаче документов определенного рода. Кафедра в этом документообороте играет одну из ключевых ролей, так как является основным потребителем и производителем информации.

Многоуровневость системы организации работы с информационными потоками факультета вуза обусловлена в свою очередь движением информации и местонахождением узлов ее обработки:



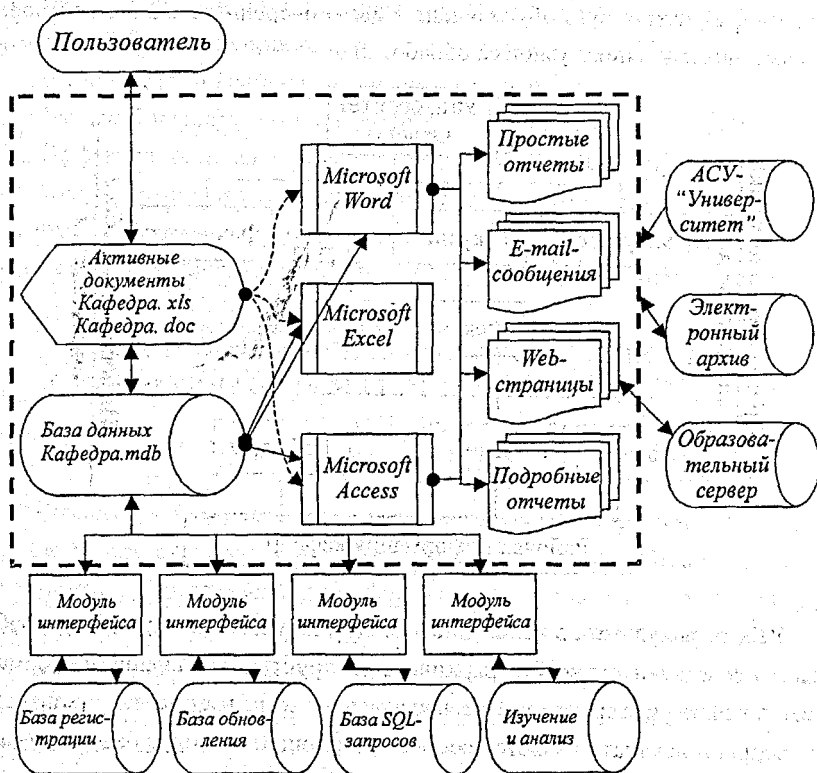
Работа факультета в целом - есть работа кафедр и деканата, и эта работа является фундаментом всей иерархической структуры движения информационных потоков университета. Потому, задача автоматизации делопроизводства кафедры и деканата является основополагающей в системе автоматизации вуза в целом.

Задача управления информационными потоками кафедры решается автоматизированной системой «Кафедра», которая выполняет функции сбора, обработки, ввода и передачи текущей информации по иерархической цепочке.

Для программной реализации системы использована концепция "офисного программирования", которая предусматривает работу с "активными" документами, позволяя, таким образом, работать с его данными, анализировать их, получать на их основе новую информацию, сохранять ее и передавать в другие документы.

Следующий уровень обработки информационных потоков – «Деканат», осуществляет сбор информации с низшего уровня, ее обобщение и обработку для дальнейшей передачи по иерархии. Информационные потоки в свою очередь могут быть как восходящими, так и нисходящими, что подчеркивает важность организации единого информационного пространства.

Схема электронного офиса «Кафедра» приведена ниже:



Организация автоматизированного делопроизводства кафедры и деканата позволяет сделать значительный шаг в компьютеризации учебного процесса и в формировании единого информационного пространства вуза в целом.

ПОСТРОЕНИЕ КРИВОЙ СВОБОДНОЙ ПОВЕРХНОСТИ ПОТОКА НЕРАВНОМЕРНОГО УСТАНОВИВШЕГОСЯ ДВИЖЕНИЯ ВОДЫ В ОТКРЫТЫХ ПРИЗМАТИЧЕСКИХ РУСЛАХ

П.А. Жолудев, Л.О. Каплинская

(БГУТ, г. Гомель)

На начальной стадии проектирования гидротехнического сооружения (плотины, шлюза) на открытых трапециевидных руслах необходимо устано-

вить законы изменения глубины и скорости жидкости вдоль потока. При этом обычно рассматривают задачу о построении кривой свободной поверхности потока. Получив такую кривую, можно в любом сечении русла найти глубину потока и среднюю скорость движения воды.

Задача о построении кривой свободной поверхности потока ставится и решается следующим образом:

- задаются характеристика русла водотока: форма поперечного сечения - симметричная трапеция, b - ширина канала по низу, m - коэффициент заложения откосов, i - уклон русла, n - коэффициент шероховатости, Q - расход воды;

- составляется дифференциальное уравнение неравномерного установившегося движения для участка русла [1];

- интегрируется составленное дифференциальное уравнение неравномерного установившегося движения, в результате чего получаем уравнение кривой свободной поверхности потока [1], т.е. зависимость длины участка русла l от ограничивающих этот участок глубин h_i и h_{i+1} .

Нормальная $h_{\text{норм}}$ и критическая $h_{\text{крит}}$ глубины потока определяются по следующим формулам

$$K(h) = \omega(h) \cdot C(h) \cdot \sqrt{R(h) - Q\sqrt{i}}, \quad (1)$$

$$F(h) = \frac{\omega^3(h)}{B(h) - \frac{\alpha Q^2}{g}}, \quad (2)$$

где $\omega(h) = (b + mh) \cdot h$ - площадь поперечного сечения,

$$C(h) = \left(\frac{1}{n}\right) \cdot R^n - \text{коэффициент Шези,}$$

$$R(h) = \frac{(b + mh) \cdot h}{b + 2h\sqrt{1 + m}} - \text{гидравлический радиус,}$$

$$B(h) = b + mh - \text{ширина канала по верху.}$$

Для нахождения $h_{\text{норм}}$ и $h_{\text{крит}}$ нами был применён метод половинного деления, реализованный в среде MathCad. Определив значения нормальной и критической глубин, мы имеем две гидравлические оси в зависимости от расположения которых существуют несколько видов кривых свободной поверхности.

Кривая свободной поверхности воды определяется как решение следующего дифференциального уравнения неравномерного установившегося движения воды

$$\frac{dh}{dl} = \frac{i - \frac{Q^2}{C^2 \omega^2 R}}{1 - \frac{\alpha Q^2}{g} \cdot \frac{B}{\omega^3}} \quad (3)$$

Уравнение (3) решено нами методом Рунге-Кутты на ПЭВМ средствами MathCad.

Разработанная компьютерная процедура позволяет получить координаты точек кривой свободной поверхности неравномерного установившегося движения воды. Данный подход может быть использован при решении инженерных задач проектирования гидротехнических сооружений.

Литература

1. Угничус А.А., Чугаева Е.А. Гидравлика. Л.: Издательство литературы по строительству, 1971. – 349 с.
2. Самарский А.А., Гулин А.В. Численные методы: Учебное пособие для вузов. – М.: Наука, 1989. – 432 с.
3. Киселев П.Г. Справочник по гидравлическим расчетам. М.: ГОСЭНЕРГОИЗДАТ, 1963. – 352 с.

КОМПЬЮТЕРНОЕ ПРЕДСТАВЛЕНИЕ И СРАВНЕНИЕ АНАЛИТИЧЕСКИХ РЕШЕНИЙ ЗАДАЧ РАСПРОСТРАНЕНИЯ ТЕПЛА В ПОЧВОГРУНТАХ

С.Н. Иванов

(БГУ, г. Минск)

Температура, влагосодержание и структура – это основные параметры грунтов, которые определяют практически все их технологические, агрофизические и физико-механические свойства. В природных условиях в процессе естественного тепло- и массообмена происходят периодические изменения температуры и влагосодержания в верхних слоях почвогрунтов.

Рациональное использование природных ресурсов и охрана среды невозможны без научного прогноза и мониторинга теплового и влажностного режимов в почвенном покрове и верхних слоях грунтов. Прямые задачи теории тепло- и массопереноса сводятся к интегрированию системы дифференциальных уравнений с частными производными при определённых началь-

ных и граничных условиях. Наиболее типично для теории тепло- и массопереноса уравнение, которое в математической физике известно как уравнение теплопроводности:

$$\frac{\partial T}{\partial \tau} C\rho = \operatorname{div}(\lambda \nabla T). \quad (1)$$

Здесь τ – время; T – температура среды; C – удельная теплоёмкость; ρ – плотность; λ – коэффициент теплопроводности.

Решения уравнения теплопроводности при различных начальных и граничных условиях для наиболее типичных задач даны в монографии А.В. Лыкова [1].

В статье рассматривается разработанная система мониторинга аналитических решений уравнения теплопроводности при различных начальных и граничных условиях. Для данной работы были отобраны задачи теплопроводности для полуограниченного тела и неограниченной пластины. Это наиболее часто возникающие эталонные задачи при аналитическом изображении физических процессов. Все аналитические решения разбиты на классы по типу граничных условий и наличию фазовых переходов, реализованы в виде рабочих документов системы.

Программной платформой для реализации системы мониторинга решений был выбран пакет Mathematica® 4.0. Как и многие компьютерные системы, Mathematica поддерживает Windows-подобный интерфейс. Документ, с которым работает данный пакет, может содержать различные математические и специальные символы, графические объекты, однако, внутренним представлением документа всегда является неформатированный ASCII текст [2]. Это позволяет легко переносить документы с одной платформы на другую: В пакете реализованы все основные функции и процедуры, необходимые для современных математических расчётов. Графика системы Mathematica достаточно хорошо себя зарекомендовала и во многом способствовала её высокой репутации среди подобных систем.

Разработанная система представления и сравнения решений задач распространения тепла в почвогрунтах предоставляет пользователю удобный интерфейс, который включает в себя меню, панели настроек параметров, информационные окна и рабочие документы. Главное меню системы обеспечивает удобный доступ ко всем компонентам системы. Присутствуют три панели настроек параметров: панель изменения параметров уравнения теплопро-

водности и граничных условий, панель управления дискретами расчётов и панель управления размерами графики. Информационные окна включают в себя окно с условными обозначениями и окно таймера.

Предоставлены средства мониторинга аналитических решений уравнения теплопроводности для граничных условий первого, второго и третьего рода. Также отдельно рассмотрена задача промерзания/оттаивания влажного грунта. Для каждой задачи даётся краткое пояснение, включающее описание физического смысла того или иного граничного условия, постановку задачи и аналитическое решение. Динамика процесса распространения тепла может быть получена по единственному нажатию кнопки. Начальное распределение может задаваться как постоянное, так и в виде функции от координаты. Причём функция записывается в таком же виде, как она представлена в математической литературе. Потоки на границах могут задаваться как постоянная или функция от времени. На экран выводятся как графики распределения тепла на конкретный момент времени, так и на определённый промежуток с заданным шагом. При помощи стандартных средств Mathematica полученное графическое представление может быть анимировано, т.е. показана эволюция профиля с течением времени. После отображения графика аналитического решения выводится решение, преобразованное с учётом формы начального распределения, потока на границе и параметров задачи.

Система предоставляет удобное средство для задания параметров уравнений и точек (дискретов), в которых может быть получено решение, как по координате, так и по времени. Причём при первоначальной загрузке параметры уже проинициализированы некоторыми реальными значениями.

Реализован механизм сравнения аналитического решения одной и той же задачи для различных параметров (Рис. 1). На приведённой ниже иллюстрации сравниваются аналитические решения задачи теплопроводности с граничными условиями первого рода для полуграниченного тела при различных значениях температуропроводности $a=0.000001$ сплошная линия и $a=0.001$ – пунктирная. Графики приведены на четыре момента времени.

Все получаемые результаты могут быть сохранены в отдельные файлы, как таблицы в виде текстового файла, так и в виде блокнотов Mathematica и использованы в будущем для отображения или сравнения с другими решениями.

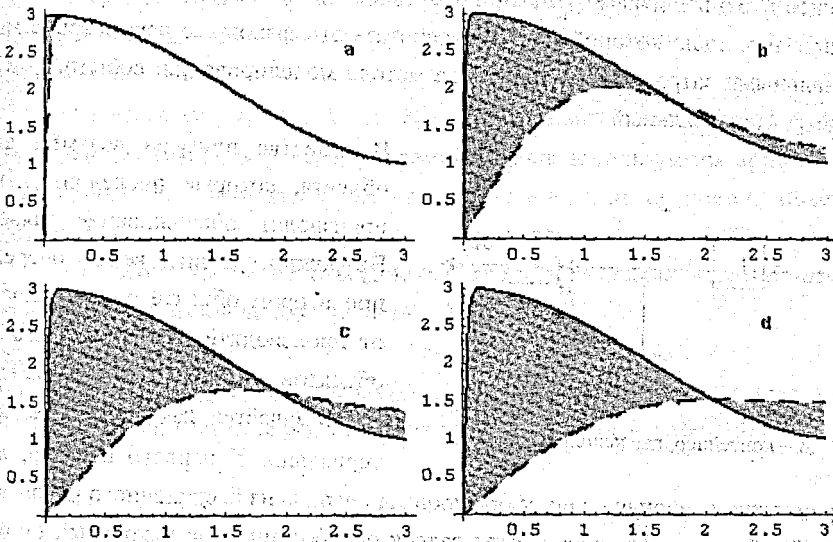


Рис. 1. Пример сравнения решений при различном значении коэффициента температуропроводности

Разработанная система пока не претендует на универсальное средство мониторинга и получения аналитических решений задач теплопроводности. Это система предоставляет лишь самые необходимые механизмы для визуализации и сравнения аналитических решений. Также эта система может быть использована в качестве обучающей, т.к. в ней описаны постановки основных задач теплопереноса при различных краевых условиях и даны их аналитические решения.

Литература:

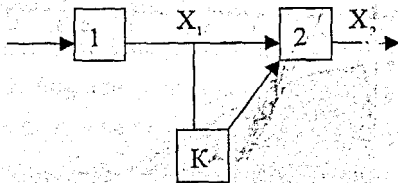
1. Лыков А.В. Теория теплопроводности. – М.: Высш. шк., 1967. – 501 с.
2. Дьяконов В.П. Системы символьной математики Mathematica 2 и Mathematica 3. – М.: СК Пресс, 1998. – 328 с.

ОБ ОДНОМ НЕЧЁТКО-ИНТЕРВАЛЬНОМ ПОДХОДЕ В ИМИТАЦИОННОМ МОДЕЛИРОВАНИИ.

А.В. Морской
(ГрГУ, г. Гродно)

Целью моделирования является получение информации о выходных параметрах рассматриваемой системы (имитационной модели) по заданным

заранее входным параметрам, при этом необходимо такая имитационная модель, с помощью которой можно рассчитать эти выходные параметры с минимальными затратами. Сравним два метода моделирования: событийный и нечётко-интервальный.



К – контейнер, где находится очередь

В качестве примера возьмём два объекта, которые последовательно производят обслуживание заявок. Возможно возникновение очереди при втором объекте в зависимости от производительности каждого из объектов, причём производительность задаётся как $p \pm \Delta p$, т.е. интервально. У первого объекта, для упрощения, первоначально сформирована очередь из бесконечного числа заявок. Требуется найти количество заявок обработанных за некоторый промежуток времени и среднее число заявок в очереди при втором объекте.

Рассмотрим событийный подход. В качестве базиса событий для объекта возьмём три события: время поступления заявки, время начала обработки заявки и время окончания обработки заявки. Таким образом у нас получается имитационная модель, которая должна обрабатывать каждое событие для каждого из объектов, то есть в данном примере необходимо обработать 6 событий.

В общем случае имитационные модели требуют значительного числа испытаний и ресурсов вычислительной техники. В частности это справедливо и для событийного подхода в имитационном моделировании. В случае рассматриваемой модели можно полностью проследить всю динамику, без больших вычислительных затрат.

Воспользуемся следующим нечётко-интервальным методом.

Пусть $P_i = [p_i - \Delta p_i; p_i + \Delta p_i]$ – производительность i -го объекта, где $i = 1, 2$, τ – время от начала эксперимента. Тогда наша модель может быть записана следующим образом

$$\begin{aligned}
 & X_1 = P_1 \tau; \\
 & \text{if } (P_1 > P_2) \{ X_2 = P_2 \tau; K = X_1 - X_2; \} \\
 & \text{else } \{ X_2 = X_1; K = 0; \}
 \end{aligned}$$

где K является контейнером, в котором находится очередь. Таким образом поставленная задача сведена к двум операциям, что значительно сокращает наши вычисления.

Отметим, что X_1, X_2, K, P_1, P_2 — заданы в интервальной форме, т.е. в процессе для решения рассматриваемой задачи используются арифметические операции с нечёткими интервалами и операция сравнения нечётких интервалов.

Таким образом, использование нечётко-интервальных величин позволяет избежать многочисленных испытаний модели.

Литература.

1. Максимей И.В., Имитационное моделирование на ЭВМ. М.: Радио и связь, 1988.
2. Шеннон Р., Имитационное моделирование: искусство и наука. М.: Мир, 1978.

ИССЛЕДОВАНИЕ ВЕРОЯТНОСТНОЙ МОДЕЛИ БАНКОВСКОЙ СЕТИ

А.В. Паньков

(ГрГУ, Гродно.)

Рассматривается модель банковской сети, состоящей из филиалов и центрального отделения банков. Запросы поступают из филиалов в центральный банк, который через некоторое время делает ответ. Обозначим через S_1, S_2, \dots, S_{n-1} - филиалы, а через S_n - центральный банк.

Запросами могут служить: запросы о переводе денег за границу, запросы о совершении операций через межбанковскую валютную биржу. Моделью такой банковской сети может служить сеть массового обслуживания с центральным обслуживающим устройством.

Рассмотрим сеть с двумя периферийными системами обслуживания. Состоянием сети служит вектор числа заявок в системах обслуживания сети. Возможны следующие переходы между состояниями:

$$\{k_1, k_2\} \rightarrow \{k_1 - 1, k_2\} \text{ - с вероятностью } \mu_1 dt \text{ за время } dt,$$

$$\{k_1, k_2\} \rightarrow \{k_1, k_2 - 1\} \text{ - с вероятностью } \mu_2 dt,$$

$$\{k_1, k_2\} \rightarrow \{k_1 + 1, k_2\} \text{ - с вероятностью } \mu_n dt,$$

$$\{k_1, k_2\} \rightarrow \{k_1, k_2 + 1\} \text{ - с вероятностью } \mu_n dt,$$

Переход из $\{k_1, k_2\} \rightarrow \{k_1 - 1, k_2\}$ означает поступление запроса из S_1 в S_3 ; $\{k_1, k_2\} \rightarrow \{k_1 + 1, k_2\}$ - означает поступление ответа в S_1 из S_3 . Аналогично определяются два других состояния.

При переходе между состояниями S_j получает некоторые доходы r_{ij} или терпит некоторые убытки r_{ij} (доходы $(-r_{ij})$):

$\{k_1, k_2\} \rightarrow \{k_1 - 1, k_2\}$ - доход r_{13} (перевод денег из S_1 в S_3),

$\{k_1, k_2\} \rightarrow \{k_1, k_2 - 1\}$ - доход r_{23} (перевод денег из S_2 в S_3),

$\{k_1, k_2\} \rightarrow \{k_1 + 1, k_2\}$ - доход $(-r_{31})$ (перевод денег из S_3 в S_1),

$\{k_1, k_2\} \rightarrow \{k_1, k_2 + 1\}$ - доход $(-r_{32})$ (перевод денег из S_3 в S_2).

Пусть, например, матрица интенсивностей переходов имеет вид

$$A = \begin{bmatrix} 2 & -2 \\ 1 & 4 \end{bmatrix},$$

а матрица доходов от переходов между состояниями:

$$R = \begin{bmatrix} -2 & -4 \\ 1 & 5 \end{bmatrix}.$$

Тогда вектор нормы выручки Q с компонентами q_i получается из $q_i = r_{ii} + \sum_{j \neq i} a_{ij} r_{ij}$:

$$Q = \begin{bmatrix} -10 \\ 6 \end{bmatrix}.$$

Требуется определить полные ожидаемые доходы. Используя теорию марковских случайных процессов с доходами [1], можно показать, что доходы определяются из системы линейных дифференциальных уравнений

$$\frac{d}{dt} v(t) = Q + Av(t),$$

где $v(t)$ - вектор-столбец полных ожидаемых доходов, которые система получает за время t , q - вектор-столбец нормы доходов.

Зададим начальные условия: $v(0) = 0$: Тогда

$$\frac{d}{dt} v(t) = Q + Av(t).$$

Для решения этого уравнения воспользуемся преобразованием Лапласа:

$$w(s) = \frac{1}{s} (sI - A)^{-1} Q + (sI - A)^{-1} v(0).$$

Последняя формула связывает преобразование Лапласа $w(s)$ вектора $v(t)$ с матрицей $(sI - A)^{-1}$, вектором нормы выручки Q и вектором доходов в момент начала процесса. Вектор дохода $v(t)$ можно найти при помощи обратного преобразования Лапласа.

Для указанной выше матрицы A имеем:

$$\frac{1}{s}(sI - A)^{-1} = \frac{1}{s(s - (3 + \sqrt{3}))(s - (3 - \sqrt{3}))} \begin{bmatrix} s-4 & 2 \\ 1 & s-2 \end{bmatrix} = \frac{1}{\eta} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + \frac{1}{\delta} \begin{bmatrix} -4 & 2 \\ 1 & -1 \end{bmatrix},$$

где $\eta = (s - (3 + \sqrt{3}))(s - (3 - \sqrt{3}))$, $\delta = s(s - (3 + \sqrt{3}))(s - (3 - \sqrt{3}))$. Обратное преобразование Лапласа для функции $\frac{1}{(p+a)(p+b)}$ равно $\frac{1}{b-a}(e^{-at} - e^{-bt})$, а для функции $\frac{1}{p(p+a)(p+b)}$: $\frac{1}{ab(a-b)}[(a-b) + be^{-at} - ae^{-bt}]$. Применяя для $w(s)$ обратное преобразование Лапласа, получим

$$v(t) = \frac{1}{2\sqrt{3}} \left(e^{(3+\sqrt{3})t} - e^{(3-\sqrt{3})t} \right) \begin{bmatrix} -10 \\ 6 \end{bmatrix} + \frac{1}{-12\sqrt{3}} \times \\ \times \left(-2\sqrt{3} - (3 - \sqrt{3})e^{(3+\sqrt{3})t} + (3 + \sqrt{3})e^{(3-\sqrt{3})t} \right) \begin{bmatrix} 52 \\ -22 \end{bmatrix}.$$

Если система начинает функционировать с перехода $\{k_1, k_2\} \rightarrow \{k_1 - 1, k_2\}$, то полный ожидаемый доход в момент времени t :

$$v_1(t) = \frac{-5}{\sqrt{3}} \left(e^{(3+\sqrt{3})t} - e^{(3-\sqrt{3})t} \right) - \frac{13}{3\sqrt{3}} \left(-2\sqrt{3} - (3 - \sqrt{3})e^{(3+\sqrt{3})t} + (3 + \sqrt{3})e^{(3-\sqrt{3})t} \right),$$

если с перехода $\{k_1, k_2\} \rightarrow \{k_1, k_2 - 1\}$, то:

$$v_2(t) = \frac{3}{\sqrt{3}} \left(e^{(3+\sqrt{3})t} - e^{(3-\sqrt{3})t} \right) - \frac{11}{6\sqrt{3}} \left(-2\sqrt{3} - (3 - \sqrt{3})e^{(3+\sqrt{3})t} + (3 + \sqrt{3})e^{(3-\sqrt{3})t} \right).$$

Литература.

1. Ховард Р.А. Динамическое программирование и марковские процессы. М.-1964. 192с.

АСПЕКТЫ РАЗВИТИЯ КОМПЬЮТЕРНОЙ СИСТЕМЫ ТЕСТОВОГО КОНТРОЛЯ ЗНАНИЙ В БГТУ

А.А. Паук, В.А. Суслов

(БГТУ, г. Брест, КПУ, Польша)

Представление результатов. В существующем варианте компьютерной системы контроля знаний результаты теста не визуализируются, а записываются в файл протокола, что предполагает возможность их дальнейшей обра-

ботки. Для облегчения анализа результатов можно обеспечить доступ к их наглядному представлению в виде гистограмм: распределения ответов, частот появления вопросов и времени ответа. Такое представление результатов поможет лучше определить такие параметры вопросов, как индекс дискриминации и индекс трудности. Гистограмма распределения баллов поможет определить валидность теста.

Модернизация интерфейса пользователя-студента. Наиболее важные доработки "студенческой" части системы должны касаться обеспечения благоприятных эргономических условий тестирования. При этом следует учесть психологическую ситуацию, в которой находится тестируемый. Одним из решений для улучшения дружелюбности системы по отношению к студенту может быть введение мультимедийных вставок, поощряющих студента и стимулирующих его работу, но не подсказывающих правильных ответов в ходе тестирования [1]. В процессе прохождения теста в облегченном режиме тестируемому может быть предоставлен доступ к глоссарию по предметной области. Если в таком глоссарии реализовать протоколирование графа поиска словарной статьи, то можно накопить дополнительную информацию для оценивания знаний студента.

Доработка базы данных. Необходимые доработки структуры базы данных и алгоритма её обслуживания вытекают из предполагаемой реализации системы по интернет-технологии и сводятся к следующим ключевым моментам:

Существующая структура БД не позволяет вести учёт и не обеспечивает надежной аутентификации пользователей, поэтому требуется ввести таблицу, включающую сведения о пользователе, необходимые для реализации технологии скрытого тестирования и одновременно для самонастройки интерфейса.

Для более эффективного учета запросов пользователем теста следует поддерживать динамическую таблицу сессий, включающую следующие данные: код сессии; идентификатор теста; дату и время заказа теста; предельное время сессии; астрономическое время получения последнего ответа на вопрос. Поскольку период прохождения теста ограничен предельным временем сессии, то по истечении этого срока запись о незаконченной сессии можно автоматически переносить в таблицу результатов теста.

Для одновременной поддержки нескольких методик тестирования следует по коду сессии формировать временные таблицы вопросов и ответов в

соответствии с заданной методикой конкретного теста. Для адаптивного алгоритма во временную таблицу заносится полный комплект вопросов по данной теме, а для классического теста производится случайная выборка заданного количества вопросов. Эти таблицы существуют только до завершения сессии. Изменения должны быть внесены также в порядок поочерёдной выдачи заданий пользователю. Номера заданий следует выбирать в соответствии с методикой тестирования из временных таблиц вопросов и ответов.

Результаты тестов предлагается хранить в нескольких таблицах для избежания дублирования записей и для удобства последующей статистической обработки. Логично разделить общие результаты прохождения теста, такие как дата и суммарное время прохождения теста, и частные результаты ответа на конкретные вопросы: номер вопроса и номер выбранного ответа на него, суммарное время, затраченное на ответ по данному вопросу.

Специфика интернет-реализации требует предусмотреть реакцию системы на обрыв связи и её последующее восстановление по коду сессии. В соответствии с одним из вариантов алгоритма, пользователю в этом случае выдаётся последний вопрос из таблицы прохождения теста. Время обрыва связи, в течении которого можно попытаться возобновить прохождение теста с последнего заданного вопроса, ограничено. Если за предельное время, установленное для ответа на вопрос, ответа не получено, в таблицу прохождения теста подставляется нулевой балл и пользователю выдаётся следующее задание.

Регулирование доступа к базе. Согласно предложенной структуре системы к базе данных имеют доступ с разными правами администратор и две группы пользователей: преподаватели и студенты. Преподаватели должны быть авторизованными пользователями БД. Доступ к БД должен быть разделён таким образом, чтобы при редактировании вопросов и ответов отдельный преподаватель мог просматривать и корректировать вопросы только по своей предметной области, при этом должна существовать возможность перекрывания зон доступа, чтобы несколько преподавателей могли работать над одной предметной областью. Изменения в базе вопросов следует протоколировать. Возможность редактирования непосредственно описаний тестов в режиме удалённого доступа нами не рассматривается так как это упрощает задачу хакера и создаёт трудности в работе администратора.

Преподаватели должны иметь доступ к удаленному просмотру группы результатов для произвольно выбранных пользователей и статистики тестирования. Предполагается, что студент может просмотреть только свои результаты тестов, выбрав их по идентификатору и подтвердив права доступа сетевым паролем.

Введение вспомогательных средств в компьютерную систему тестирования. Наиболее актуальным решением по нашему мнению является разработка интерактивной помощи пользователю-преподавателю. Для того, чтобы результаты тестирования действительно отражали уровень знаний студента в предметной области, необходимо в соответствии с применяемой методикой тестирования строго соблюдать правила построения тестовых заданий и нормы оценивания ответов. Специфика подготовки преподавателей вузов не предполагает наличия у них глубоких знаний в области тестологии, поэтому система помощи должна сыграть определяющую роль в обеспечении корректности компьютерного тестирования. Одна из современных форм такой помощи – расширяемый пользователем глоссарий специфических терминов [2].

Для снижения вероятности фальсификации результатов тестирования может оказаться весьма полезной непрерывная идентификация пользователя, например по клавиатурному почерку или почерку работы с мышью [3, 4], что предполагает использование манипулятора специальной конструкции со встроенными датчиками, реагирующими на некоторые физические параметры человека.

Литература.

1. Skinner B. F., *The Science of Learning and the Art of Teaching* // Harvard educational review vol. XXIV, no. 2, spring, 1954, pp. 86-97.
2. Манако В., Манако А., Синица К., Коллекции интерактивных словарей для непрерывного обучения индивидуала // Educational Technology & Society 4(1) 2001 ISSN 1436-4522 pp. 98-104.
3. Климов А., Дистанционному образованию - дистанционный контроль //Компьютерра №23 (301) <http://www.computerra.ru/offline/1999/301/3746/>.
4. Компьютерная графология // Компьютерные Вести №23, 1999 www.kv.by/index1999232201.htm.

О КОМПЬЮТЕРНОЙ СИСТЕМЕ ТЕСТОВОГО КОНТРОЛЯ ЗНАНИЙ

В БГТУ

А.А. Паук, В.А. Сулов

(БГТУ, г. Брест, КПУ, Польша)

Введение. Компьютерное тестирование знаний находит всё большее применение в вузах, что связано с интенсификацией процесса проверки успеваемости и со стремлением к повышению объективности оценивания. Педагогическое тестирование с помощью компьютера отражает объективную тенденцию к интеграции информационных технологий в образование. Все чаще компьютерное тестирование рассматривается также как форма самоконтроля, например в мультимедийных обучающих программах [1], помогающая студенту в корректировке приобретённых знаний. К настоящему времени в мире разработано несколько методик компьютерного тестирования знаний, отличающихся алгоритмами опрашивания и обработки результатов.

Сетевая система тестирования знаний, основанная на классической методике, была реализована в БГТУ в 1999-2001 годах с участием одного из авторов настоящей работы и показала себя как эффективное средство контроля знаний при приёме зачётов по философии и религиоведению [2]. В состав этой системы вошли модуль тестирования и программа генерации письменных вариантов тестов, написанные на языке Visual Basic. Для хранения базы данных вопросов и ответов с разбивкой по темам и предметам была использована СУБД Access.

В процессе эксплуатации выявились некоторые технические недостатки системы: необходимость наличия соответствующих динамических библиотек на клиентских рабочих станциях и слабая защищённость базы данных. К недостаткам системы можно отнести также отсутствие интерфейса для работы с базой данных, что затрудняет преподавателю самостоятельное проведение педагогических экспериментов, модификацию тестов и настройку системы под специфику дисциплины или кафедры. На основе накопленного опыта и анализа публикаций на тему компьютерного тестирования за последние годы можно предложить пути устранения названных недостатков и обсудить направления дальнейшего развития системы.

Цель работы. Основные цели планируемых работ по модернизации компьютерной системы тестирования (КСТ) – повышение надежности результатов тестирования и обеспечение гибкости системы в соответствии с за-

просами кафедр БГТУ: В качестве тактических путей модернизации мы видим: широкое использование современных интернет-технологий, конструирование специализированных интерфейсов для пользователей КСТ и введение технологических расширений системы. При этом представляется целесообразным создание не законченной обучающей или контролирующей продукции, а своеобразного электронного конструктора, позволяющего преподавателю реализовать собственные педагогические идеи, не прибегая к программированию на алгоритмическом языке.

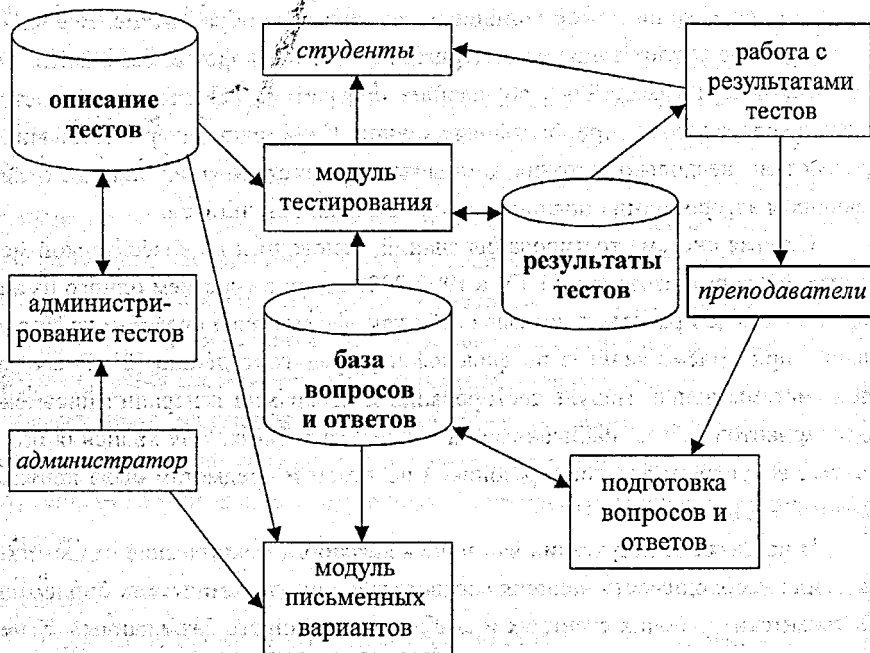


Рис. 1. Схема взаимодействия элементов системы

Аспекты модернизации КСТ. Общая структура предлагаемой нами модернизированной системы тестирования может быть представлена схемой взаимодействия компонентов, которая приведена на рис. 1. Обсудим отдельные технические аспекты предлагаемой модернизации.

Необходимость перехода к Интернет-технологиям. Наибольшей универсальностью, по нашему мнению, обладает система тестового контроля, основанная на современных интернет-технологиях. Она позволяет реализовать тестирование как на выделенном компьютере, так и в режиме удаленного

доступа через интрасеть или Интернет. Некоторые современные технологии обучения (например, дистанционное образование) уже предполагают активное применение компьютерного тестирования знаний в режиме удаленного доступа с использованием Интернет [1]. Компьютерное тестирование через Интернет используется также при сертификации специалистов по вычислительной технике. К существенным преимуществам такой технологии, важным для условий Республики Беларусь, можно отнести невысокие требования к аппаратуре и отсутствие специфических требований к программному обеспечению пользователя. Построение КСТ на основе интернет-технологий снимет ряд указанных выше недостатков действующей системы.

Проектирование программной оболочки для пользователя-преподавателя. Для обеспечения гибкости системы тестирования необходимо представить преподавателю возможность самостоятельной настройки теста. В частности, преподаватель должен иметь возможность изменения методики тестирования, выбора способа расчета результирующего балла, выбора методов статистической обработки и форм визуализации результатов тестирования.

При классической методике тестирования вопросы выбираются случайным образом. При использовании более совершенного адаптивного алгоритма тестирования выбор вопроса осуществляется на основании оценки способностей, пересчёт которой происходит после каждого ответа на вопрос. Следующий вопрос выбирают так, чтобы его сложность наилучшим образом соответствовала знаниям тестируемого. Подробное описание методики адаптивного тестирования с использованием теории ответа на вопрос на примере модели Бирнбаума можно найти в [3].

В действующей классической системе тестирования, применённой в БГТУ [2], результирующий балл подсчитывается после окончания теста как среднее взвешенное. По мнению авторов работы [4] в этом случае можно также учитывать время ответа на вопрос. При адаптивной методике в качестве результата используется оценка способностей, вычисленная после ответа на последний вопрос, сложность вычисления зависит от модели информационной функции вопросов [3].

Литература.

1. Гребенюк В.А., Катасонов А.А., Учебный процесс и контроль знаний в системе виртуального образования // Дистанционное обучение, № 1, М., 1999, <http://www.mesi.ru/joe/st151.html>

2. Куниш А.Л., Паук А.А., Компьютерные тестирующие программы по гуманитарным наукам и их использование в учебном процессе ВУЗов // Вестник Брестского государственного технического университета, 2000, №6, стр. 48-53.
3. Rudner L. M., An On-line, Interactive, Computer Adaptive Testing Tutorial, 11/98 <http://ericae.net/scripts/cat>
4. Кожевников Ю.В., Медведева С.Н., Дидактическое проектирование компьютерных технологий обучения для профессиональной математической подготовки по специальности "Прикладная математика и информатика" // Educational Technology & Society 3(4) 2000, pp. 203-217.

МЕТОДИКА АНАЛИТИЧЕСКОГО РАСЧЕТА ПАРАМЕТРОВ ВИДЕООЦИФРОВКИ НЕРЕГУЛЯРНЫХ ПОВЕРХНОСТЕЙ

Ю.В. Полозков

(ВГУ, г. Витебск)

Возросшая популярность трехмерного компьютерного проектирования в различных отраслях отечественного производства вызвала необходимость в создании наиболее эффективных, простых и быстрых способов и средств описания объектов, имеющих пространственно сложную (нерегулярную) форму. В результате проведения исследований, в области описания пространственно сложных поверхностей, была разработана компактная система видеооцифровки нерегулярных объектов [1]. Построение объемных цифровых моделей нерегулярных поверхностей с помощью этой видеосистемы осуществляется на основе специально разработанной математической модели обработки видеоизображений [2]. В этой фотограмметрической модели видеоизображение рассматривается как результат идеального центрального проецирования точек поверхности объекта прямыми лучами, проходящими через центр проекции и падающими на идеальную плоскость видеоснимка. В действительности такое условие не соблюдается, что вызывает искажения объемных цифровых моделей объектов оцифровки. Исследования факторов, вызывающих погрешности при обработке видеоизображений и построении цифровых моделей поверхностей, показали, что основными причинами возникновения искажений являются погрешности фокусного расстояния видеокамеры, положения главной точки изображения и углового ориентирования снимка.

Конструктивным исполнением большинства стандартных видеокамер не предусмотрена фиксация промежуточных значений фокусного расстояния. Поэтому, в соответствие с разработанным способом видеооцифровки, при съемке объекта применяются вертикально натянутые нити. Используя горизонтальный размер видеоизображения участка вертикально натянутой нити, обозначенного опорными точками с известными пространственными координатами, можно рассчитать масштабный коэффициент видеосъемки:

$$K = L_{гориз} / P_u \quad (4)$$

где $L_{гориз}$ – горизонтальный размер изображения в мм, P_u – размер поля изображения по горизонтали в мм.

Так как масштабирование при съемке сохраняется по всем направлениям, то найденное K можно подставить в условие пропорциональности координат ранее указанной математической модели видеооцифровки. Откуда, при заданных одинаковых пространственных координатах опорных точек по вертикали, вычисляется значение фокусного расстояния видеокамеры.

Из отношения, определяющего глубину резкости, которая характеризует минимальное и максимальное расстояния от центра проекций до точек объекта, которые изображаются на снимке с достаточной четкостью, рассчитывается минимальное расстояние от объекта до видеокамеры [3]:

$$\delta = f^2 / nR_m \quad (1)$$

где δ – диаметр кружка нерезкости; f – фокусное расстояние камеры; n – знаменатель относительного отверстия объектива; R_m – минимальное расстояние от передней главной плоскости объектива до точки объекта.

Знаменатель относительного отверстия объектива находится из следующей формулы:

$$R = 1800/n \quad (2)$$

где R – разрешающая способность объектива (число линий на 1 мм):

$$R = n_p / 2 * L_i \quad (3)$$

где n_p – количество пикселей видеоизображения по горизонтали или вертикали; L_i – горизонтальный или вертикальный размер видеоизображения в мм.

Также с помощью отмеченных нитей можно аналитически определить угловое ориентирование видеоснимка (рис. 1) [4].

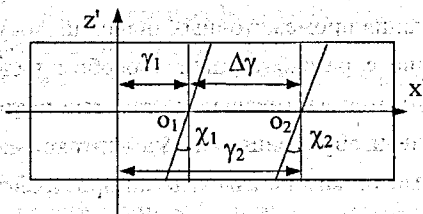


Рис. 1. Схема для определения угловых элементов внешнего ориентирования видеоснимка

На плоском видеоснимке отвесная линия отображается прямой. Это позволяет определить угол μ между изображенной прямой и осью Z:

$$\operatorname{tg} \mu = (x_2 - x_1) / (z_2 - z_1) = K, \quad (4)$$

где x_2, x_1, z_2, z_1 — координаты произвольных точек, выбранных на изображении отвесной линии.

Используя известные выражения для направляющих косинусов и формулы, выражающие зависимости координат точки на снимке от координат этой же точки в пространстве получаем:

$$\left. \begin{aligned} \frac{\operatorname{Cos} \omega \operatorname{Sin} \chi Y^{M1}}{\operatorname{Sin} \omega K^1 S^1} - \frac{\operatorname{Cos} \omega \operatorname{Cos} \chi Y^{M1}}{\operatorname{Sin} \omega S^1} + 1 - \frac{X^{M1}}{K^1 S^1} &= 0 \\ \frac{\operatorname{Cos} \omega \operatorname{Sin} \chi Y^{M2}}{\operatorname{Sin} \omega K^2 S^2} - \frac{\operatorname{Cos} \omega \operatorname{Cos} \chi Y^{M2}}{\operatorname{Sin} \omega S^2} + 1 - \frac{X^{M2}}{K^2 S^2} &= 0 \end{aligned} \right\} \quad (5)$$

где ω, χ — угловые элементы внешнего ориентирования; X^{Mi}, Y^{Mi} — пространственные координаты точек, расположенных на 1-й и 2-й нитях, S^i — длины отвесных нитей.

Из этой системы уравнений определяются угловые элементы внешнего ориентирования видеоснимка ω, χ .

Таким образом, известное пространственное положение опорных точек, расположенных на вертикально натянутых нитях, используемых при видеооцифровке, позволяет выполнить аналитический расчет параметров съемки по полученным видеоизображениям. Расчетные значения этих параметров позволяют повысить точность результатов при построении трехмерных цифровых моделей пространственно сложных поверхностей с помощью видеооцифровки. Повышение точности видеооцифровки расширит сферы применения трехмерных цифровых моделей при проектировании новых нерегулярных

объектов на малых и средних предприятиях отечественной промышленности и повысит эффективность их производства.

Литература.

1. Свирский Д.Н., Полозков Ю. В. Технология и оборудование для трехмерного сканирования в компактной системе быстрого прототипирования. // Материалы, технологии, инструменты. 2000, т. 5; № 4: – С. 97-102.
2. Завацкий Ю. А., Полозков Ю. В., Свирский Д.Н. Математическое моделирование процесса оцифровки пространственных объектов. // Веснік ВДУ. 1999, №3. - С. 49-53.
3. Келья Л. Н., Корнилов Ю. Н. и др. Фотограмметрия. - М.: Недра, 1989. – 319с.
4. Гонин Г. Б. Фотограмметрическая обработка и дешифрирование аэрофотоснимков. - Л.: Наука, 1967. – 167 с.

ОБ ИСПОЛЬЗОВАНИИ ГРАФОВЫХ МОДЕЛЕЙ В КУРСАХ МАТЕМАТИКИ И ИНФОРМАТИКИ: СОСТОЯНИЕ И ПЕРСПЕКТИВЫ

О. О. Пронжилло

Нам бы хотелось еще раз обратиться к проблемам современного математического образования, от качества которого непосредственно зависит успешность развития математики как науки. В частности, мы хотели бы рассмотреть вопросы изучения графовых моделей, которые широко используются при решении всевозможных прикладных задач и которые можно успешно использовать в обучении школьников.

Моделирование является важнейшим компонентом современного математического образования. Для большинства традиционных моделей естественных явлений их математической основой служат уравнения, системы уравнений или неравенств. Умениями и навыками построения таких моделей учащиеся овладевают при решении текстовых задач.

Общеизвестно, что решение текстовых задач вызывает трудности у довольно большого числа учащихся. Это связано с тем, что процесс формализации данных задачи требует развитой способности к абстрагированию и идеализации. В результате возникает психологический дискомфорт, теряется уверенность в собственных силах. Большую помощь в таких ситуациях могут оказать рисунки, схемы, графики – любые наглядные объекты, которые являются посредниками между реальной ситуацией, описанной в задаче и ее математической моделью. Одним из таких средств построения моделей являются графы.

Язык теории графов оказывается очень удобным при описании дискретных систем объектов самого различного характера. С помощью графов, например, можно описать схему дорог, календарный план работ, химическое соединение атомов, электрическую схему, расписание занятий, старшинство в организации, генетический эксперимент и пр. Великое множество таких моделей можно найти в литературе по теории графов и ее применениям. Совсем недавно вышло в свет замечательное пособие по теории графов для школьников, где собрано более 100 задач, моделируемых графами [1].

Наглядные рисунки графов обеспечивают связь мышления с конкретными ситуациями и одновременно служат средством получения нового знания. Часть информации, которую учащиеся получили через словесный текст или речь учителя, представляется в форме, более удобной для восприятия и запоминания. Графы позволяют зафиксировать многие ценные детали, которые часто теряются в абстрактных понятиях, что, в свою очередь, может натолкнуть мысль на решение задачи.

Следует также отметить еще тот факт, что математика за последние десятилетия существенно изменилась, стала более алгоритмизированной. Интенсивное развитие получили ее дискретные разделы, связанные с применением вычислительной техники. Теория графов является одним из разделов дискретной математики, изучение которого не только доступно для школьников, но и позволяет осуществить стыковку математики и информатики.

Определенные шаги в этом направлении уже сделаны. Элементы теории графов включены в программу для классов с углубленным изучением информатики средних общеобразовательных учреждений Республики Беларусь [2].

Основы теории графов мы находим в учебнике В. М. Котова и О. И. Мельникова «Информатика: методы и алгоритмы» для 10-11 классов с углубленным изучением информатики [3]. Этот учебник позволяет ознакомить школьников с такими алгоритмами теории графов, как поиск в ширину; поиск в глубину, поиск кратчайшего пути, построение эйлерового цикла, максимального потока в сети, построение минимального остовного дерева. Эти алгоритмы в дальнейшем используются для исследования графов или решения задач.

Большую помощь учителю, желающему использовать графы в преподавании информатики, может оказать методическое пособие А. А. Харланова

[4]. Его методика основана на решении прикладных задач при помощи построения гафовых моделей и последующей реализации алгоритмов обработки графов на языке *Pascal*.

Элементы сетевого планирования можно найти в известном пособии для учителей Л. Ю. Березеной [5]. Также в нем излагаются прикладные задачи обработки деревьев.

Очень большую помощь в использовании математического аппарата теории графов на уроках информатики могут оказать компьютерные программные продукты. Нам известны несколько программ, позволяющих изучать и обрабатывать графы: «Graphlet», «Groups & Graphs», «Grin», «AlGra». Если попытаться дать краткую характеристику этих программных продуктов, то можно сказать, что «Graphlet» имеет много возможностей для визуального представления графа. Эта программа позволяет создавать очень красочные изображения и может оказать большую помощь в создании наглядных пособий. «Groups & Graphs» предназначена для специалистов по теории графов, но также может использоваться и в учебных целях, хотя и довольно ограниченно. «Grin» (Grahp Interface) позволяет создавать, редактировать и исследовать графы. С ее помощью можно не только получить информацию по теоретическим вопросам, но и в интерактивном режиме исследовать свойства графов, редактировать их с помощью встроенного редактора. Эта система может быть использована как для обучения основам теории графов, так и для проведения исследований ориентированных и неориентированных графов. Обучающая программа «AlGra» создана на кафедре прикладной математики и информатики БГПУ им М. Танка. Она позволяет создавать, редактировать неориентированные графы и в интерактивном режиме овладеть такими алгоритмами теории графов, как поиск в ширину, поиск в глубину, построение эйлерового цикла, определение связности и планарности графа, построение кратчайшего пути между вершинами, построение минимального остовного дерева.

Таким образом, можно сделать вывод, что на данный момент имеются все предпосылки для широкого внедрения графовых моделей в школьные курсы математики и информатики, что позволит осуществить на практике стыковку этих двух предметов. Есть учебники и учебные пособия, есть программные продукты, которые могут оказать помощь в овладении основами теории графов и решении прикладных задач. Необходимо лишь сотрудниче-

ство ученых-методистов для распространения опыта внедрения графовых моделей в математическое образование школьников и студентов.

Нельзя сказать, что в этом направлении ничего не осуществляется. Курс дискретной математики читается на педагогическом потоке мехмата БГУ доцентом О. И. Мельниковым. Изучение алгоритмов на графах является составной частью курса информатики в Академии последипломного образования. Нами в качестве эксперимента ведется спецкурс по основам теории графов на математическом факультете БГПУ им. М. Танка. В преподавании мы используем метод обучения через решение задач и перечисленные выше компьютерные программы. При отборе теоретического материала мы руководствовались принципами познавательности и профессиональной направленности в обучении. Цель нашего курса – показать возможности использования графов в преподавании, как математики, так и информатики. Очень хотелось бы сотрудничать с другими педагогическими вузами, обмениваться опытом преподавания теории графов, но пока нам не удалось установить контактов в других городах кроме Минска. Надеемся, что в будущем такие контакты появятся.

Литература.

1. Мельников О. И. Занимательные задачи по теории графов. Мн., ТетраСистемс, 2001.
2. Программы средней общеобразовательной школы. Информатика VIII-XI классы. Мн., 2000.
3. Котов В. М., Мельников О. И. Информатика: методы и алгоритмы. Мн., 2000.
4. Харланов А. А. Методическое пособие для учителей и преподавателей средних учебных заведений и учебных заведений нового типа в классах с углубленным изучением информатики. Мн., 1997.
5. Березина Л. Ю. Графы и их применение. М., Просвещение. – 1979.

СТОХАСТИЧЕСКАЯ МОДЕЛЬ ОБРАБОТКИ ИСКОВ В СТРАХОВОЙ КОМПАНИИ

Т.В. Романюк

(ГрГУ, г. Гродно)

Рассматривается функционирование страховой компании на интервале времени $[0, T]$. Полагается, что страховая компания заключает со страхователями договора страхования двух типов, причем общее число заключенных договоров страхования определяется в момент времени t , $t \leq T$, некоторой функцией времени $K(t)$. Т.е. в некоторый момент времени t , $t \in [0, T]$, ком-

панией заключено со страхователями $K_1(t)$ договоров страхования первого типа и $K_2(t)$ договоров второго типа, $K_1(t) + K_2(t) = K(t)$. При наступлении страхового случая компании предъявляется иск страхователя, который проходит две стадии обработки – стадию оценки и стадию выплаты. Оценкой исков типа r занимаются m_r , $r = 1, 2$, специалистов компании (оценщики), выплатой – один кассир. Иски страхователей могут находиться в одном из следующих состояний: C_0 - иск не предъявляется (с объектом страхования ничего не случилось), C_1 - иск находится на стадии оценки, C_2 - иск находится на стадии выплаты.

Предполагаем (для того, чтобы ниже введенный случайный процесс $k(t)$ являлся марковским), что вероятность перехода иска типа r из состояния C_0 в состояние C_1 на интервале времени $[t, t + \Delta t]$ равна $\mu_r(t)\Delta t + o(\Delta t)$, где $\mu_r(t)$ - интенсивность такого перехода, $r = 1, 2$. Времена обработки исков типа r оценщиками и времена между переходами исков из состояния C_2 в состояние C_0 распределены по показательному закону с интенсивностями μ_1, μ_2 соответственно, $r = 1, 2$. Будем предполагать, что наша система в некоторый момент времени t находится в состоянии $k(t) = (k_1(t), k_2(t), k_3(t))$, если в этот момент времени $k_1(t)$ исков типа r , $r = 1, 2$ находятся в состоянии C_1 , а $k_2(t)$ исков – в состоянии C_2 . Качество функционирования компании можно определить функционалом

$$W(T) = W(T, m_1, m_2) = \frac{1}{T} \int_0^T [K(t) \sum_{i=1}^3 (d_i n_i(t) + E_i l_i(t))] dt, \quad (1)$$

описывающим потери компании на интервале времени $[0, T]$, причем коэффициенты $d_i, E_i, i = 1, 2, 3$, имеют определенный стоимостный смысл; здесь

$$n_i(t) = M \left\{ \frac{k_i(t)}{K(t)} \right\}, l_i(t) = \frac{m_i}{K(t)}, i = 1, 2, 3, m_3 = 1.$$

Нас интересует следующая задача: требуется найти число оценщиков $m_r, r = 1, 2$, которые должны работать на различных интервалах времени, чтобы среднее число исков типа r , находящихся в момент времени t в состоянии оценки и выплаты, т.е. $K(t)n_r(t)$ и $K(t)l_r(t)$ не превышало соответственно m_r и 1, $r = 1, 2$, и чтобы потери $W(T)$ были минимальными:

$$\begin{cases} W(T) \rightarrow \min_{m, i=1,2}, \\ K(t)n_i(t) \leq m_i, i=1,2,3, t \in [0, T]. \end{cases} \quad (2)$$

Отметим, что стохастической моделью процесса обработки исков в данном случае может служить замкнутая сеть массового обслуживания, состоящая из четырех систем обслуживания S_0, S_1, S_2, S_3 с числом линий обслуживания соответственно $K^*, m_1, m_2 \geq 1, m_3 = 1$, причем считаем, что $1 << K(t) \leq K^*$. Вероятности перехода заявок между системами сети - $p_{0r} \neq 0, p_{r3} = p_{30} = 1, r = 1,2, p_{ij} = 0$ в остальных случаях; в сети обслуживаются в момент времени t $K(t)$ заявок; дисциплины обслуживания заявок в системах сети - FIFO.

Установлено, что плотность распределения вероятностей $p(x, t) = p(x_1(t), x_2(t), x_3(t))$ вектора $\frac{k(t)}{K(t)} = \left(\frac{k_1(t)}{K(t)}, \frac{k_2(t)}{K(t)}, \frac{k_3(t)}{K(t)} \right)$ с точностью до $O(\varepsilon^2(t))$, где $\varepsilon(t) = l_3(t)$, удовлетворяет уравнению в частных производных

$$\frac{\partial p(x, t)}{\partial t} = - \sum_{i=1}^3 \frac{\partial}{\partial x_i} (A_i(x, t) p(x, t)) + \frac{\varepsilon(t)}{2} \sum_{i, j=1}^3 \frac{\partial^2}{\partial x_i \partial x_j} (B_{ij}(x, t) p(x, t)) + 3\varepsilon(t) K'(t) p(x, t), \quad (3)$$

где $A_i(x, t) = \sum_{j=1}^3 \mu_j q_{ji} \min(l_j(t), x_j(t)) + \mu_{0i}(t) (1 - \sum_{j=1}^3 x_j(t))$; $\mu_{03}(t) = 0$,

$$q_{ji} = \begin{cases} -1, j=i, i=\overline{1,3}, \\ 1, j \neq i, i=3, \\ 0, j \neq i, i=\overline{1,2} \end{cases} \quad B_{ij}(x, t) = \begin{cases} \sum_{j=1}^3 \mu_j \min(l_j(t), x_j(t)) + \mu_{0i}(t) (1 - \sum_{j=1}^3 x_j(t)), i=j, \\ -2\mu_i \min(l_i(t), x_i(t)), i \neq j, j=3, \\ 0, i \neq j, j=1,2. \end{cases}$$

Уравнение (3) отличается от уравнения Фоккера-Планка-Колмогорова только присутствием в нем выражения $3\varepsilon(t)K'(t)$, поэтому можно попытаться найти его решение в виде плотности распределения вероятностей трехмерной случайной величины (важно отметить, что нас больше интересует не само решение уравнения (3), а компоненты вектора $n(t)$):

$$p(x, t) = \frac{1}{\sqrt{(2\pi)^3}} \sqrt{|D|} \exp \left[-\frac{1}{2} \sum_{i,j=1}^3 (x_i(t) - n_i(t)) d_{ij}(t) (x_j(t) - n_j(t)) \right], \quad (4)$$

где $D = \|d_{ij}\|_{3 \times 3}$ - положительно определенная матрица. С учетом того, что мы должны искать решение оптимизационной задачи при ограничениях $\{0 \leq n_i(t) \leq l_i(t), i = 1, 2, 3\} = A$, уравнение (3) можно представить следующим образом:

$$\begin{aligned} \frac{\partial p(x, t)}{\partial t} &= [\mu_1 + \mu_2 + \mu_3 + \mu_{01}(t) + \mu_{02}(t) + 3\varepsilon(t)K'(t)] \times p(x, t) + \\ &+ [\mu_1 x_1(t) - \mu_{01}(t)(1 - x_1(t) - x_2(t) - x_3(t)) - \varepsilon(t)\mu_{01}(t)] \frac{\partial p(x, t)}{\partial x_1} + \\ &+ [\mu_2 x_2(t) - \mu_{02}(t)(1 - x_1(t) - x_2(t) - x_3(t)) - \varepsilon(t)\mu_{02}(t)] \frac{\partial p(x, t)}{\partial x_2} + \quad (5) \\ &+ [\mu_3 x_3(t) - \mu_2 x_2(t) - \mu_1 x_1(t)] \frac{\partial p(x, t)}{\partial x_3} + \\ &+ \frac{\varepsilon(t)}{2} \mu_{01}(t)(1 - x_1(t) - x_2(t) - x_3(t)) \frac{\partial^2 p(x, t)}{\partial x_1^2} + \\ &+ \frac{\varepsilon(t)}{2} \mu_{02}(t)(1 - x_1(t) - x_2(t) - x_3(t)) \frac{\partial^2 p(x, t)}{\partial x_2^2} \end{aligned}$$

Разложим коэффициенты уравнения (5) в ряд Тейлора в окрестности точки $(n_1(t), n_2(t), n_3(t))$, ограничиваясь первыми членами разложения, затем подставим полученные выражения и плотность (4) в уравнение (5). Приравняв в полученном уравнении члены при одинаковых степенях $(x_i(t) - n_i(t))$, $i = 1, 2, 3$, получим следующую систему ОДУ для определения компонент вектора $n(t)$:

$$\begin{cases} \frac{dn_1(t)}{dt} = -\mu_1 n_1(t) + \mu_{01}(t)(1 + \varepsilon(t) - \sum_{i=1}^3 n_i(t)), \\ \frac{dn_2(t)}{dt} = -\mu_2 n_2(t) + \mu_{02}(t)(1 + \varepsilon(t) - \sum_{i=1}^3 n_i(t)), \\ \frac{dn_3(t)}{dt} = \mu_1 n_1(t) + \mu_2 n_2(t) - \mu_3 n_3(t). \end{cases} \quad (6)$$

Система ОДУ в случае $K(t) = K$ рассмотрена в [1].

Учитывая вид функций $\mu_{oi}(t)$, $i = 1, 2$, $K(t)$, можно используя метод фундаментальных матриц найти общее решение системы (6), а с его помощью решение оптимизационной задачи (2).

Литература.

1. Астахов А.М., Матальцкий М.А., Романюк Т.В. О применении системы ОДУ для анализа модели обработки разнотипных исков в страховой компании // Тезисы докладов Международной математической конференции "Дифференциальные уравнения и системы компьютерной алгебры". – Брест: БрГУ, 2000. – С. 7-8.

INTERNET-СИСТЕМА ТЕСТИРОВАНИЯ УЧЕБНЫХ ПРОГРАММ

С. Рында, Д. Данилович, А. Лисовский

(ГрГУ, г. Гродно)

В каждом высшем учебном заведении преподаются курсы, связанные с лабораторными занятиями по программированию, проводятся олимпиады и конкурсы.

Для облегчения проведения подобных трудоемких мероприятий возникла потребность в создании автоматизированных программных средств, которые позволили бы быстро и объективно, а главное, с максимальной автоматизацией процесса, тестировать учебные программы, разрабатываемые студентами.

Проверка даже одной программы-задачи, скажем прямо, процесс трудоемкий. Во-первых, следует сформировать набор тестов, позволяющих проверить правильность выполнения программы-задачи. Во-вторых, тестов может быть много, либо программа-задача обрабатывает большое количество данных, проверить которые не легко. В-третьих, все мы люди, и не железные, и, к примеру, допустить ошибку при проверке задания может каждый. Ну, и, в-четвертых, объективность проверки задачи... А если задач несколько сотен...

В докладе представлена реализация автоматизированной системы, предназначенной для автоматизации процесса тестирования программ, разработанных пользователями (студентами, школьниками) для решения поставленных задач. Система функционирует как Internet-приложение, что обеспечивает доступ к ней в рамках intranet-сети Гродненского государственного университета.

Данный проект реализован с использованием среды разработки Visual C++. Это обусловлено тем, что эта система, используя все мощь объектно-ориентированного языка программирования C++, как ни одна другая, на наш взгляд, позволяет реализовывать довольно сложные программы, и при этом ее код является компактным и быстрым. Для реализации сетевых возможностей используется набор программ, написанных с использованием Perl.

Автоматизированная Internet-система тестирует программы, написанные с использованием языков программирования Pascal, C и C++.

В процессе работы автоматизированная система создает несколько потоков. Один из них является «главным» и обеспечивает функционирование всей системы. Для каждой задачи «главный» поток создает отдельный поток, который управляет тестированием отдельной задачи. Количество одновременно тестируемых задач фиксировано и определяется, главным образом, производительностью сервера.

Для каждой тестируемой задачи определен уникальный номер и связанные с ним набор тестов и максимальное время ее выполнения.

Для программ, написанных на Pascal, запрещено использование любых процедур и функций, не входящих в состав стандартного модуля System, а также использование функций для работы с файлами. Ввод/вывод данных должен осуществляться при помощи стандартных функций ввода/вывода (readln/writeln). Для C/C++ набор возможных библиотек примерно следующий - CONIO.H, MATH.H, STDIO.H, STDLIB.H, STRING.H.

При компиляции программ-задач используются:

– Microsoft (R) 32-bit C/C++ Optimizing Compiler Version 12.00.8168 for 80x86 либо Borland C++ 3.1

– Borland Pascal Compiler Version 7.0

Решение задачи считается верным, если она выдала верные результаты на каждый из тестов. Если выполнение задачей теста превысило отведенный лимит времени, либо получен неверный ответ, то тестирование задачи прекращается и задача считается нерешенной.

Возможные ошибки, на которые реагирует система (см. табл. 1)

Результаты тестирования заносятся во внутренний журнал системы тестирования, и предоставляются пользователю (студенту) в виде отчета. Отчет содержит уникальный номер задачи, отправленной на тестирование, инфор-

мацию о результатах тестирования (если тест не пройден, то сообщается порядковый номер теста, при выполнении которого возникла ошибка), о времени начала и окончания тестирования, имя пользователя, отправившего задачу на проверку.

Таблица 1.

Результат тестирования	Комментарий	Возможные ошибки
1. Ошибка компиляции	В результате компиляции не создан исполняемый файл	1. Синтаксическая ошибка в программе; 2. Неверное расширение файла; 3. Используются недопустимые модули либо библиотеки.
2. Превышен лимит времени	Программа превысила отведенный лимит времени выполнения	1. Нерациональное решение; 2. Ошибка в программе.
3. Ошибка времени выполнения	Выполнение программы завершено с ненулевым кодом завершения.	1. Runtime error; 2. В C/C++ программе отсутствует оператор "return (0)" либо он возвращает ненулевое значение. 3. Использован оператор Halt() с ненулевым параметром.
4. Неверный ответ	В результате выполнения теста получен неверный ответ.	Ошибка при реализации выбранного алгоритма решения.

Планируется размещение автоматизированной системы тестирования на web-сервере факультета, для обеспечения функционирования систем дистанционного образования, а также интеграция программного продукта с виртуальным классом кафедры информатики и вычислительной техники.

КОНТРОЛИРУЮЩЕ-ОБУЧАЮЩАЯ ПРОГРАММА ДЛЯ РЕШЕНИЯ ЗАДАЧ ЛИНЕЙНОГО ПРОГРАММИРОВАНИЯ СИМПЛЕКС-МЕТОДОМ

А.А. Сарычев

(БГТУ, г. Брест)

Важный раздел математики составляют экстремальные задачи, в частности задачи линейного программирования. На многих экономических и тех-

нических специальностях вузов студенты изучают задачи линейного программирования и методы их решения. Самый распространенный метод решения – это симплекс-метод в табличной форме. Сам по себе этот метод не очень сложен, но требует значительных усилий, т.к. пересчет симплексных таблиц является довольно утомительным занятием и требует большого внимания. Поэтому при решении задач линейного программирования очень легко ошибиться и получить неправильный ответ. Чтобы избежать рутинной работы, связанной с пересчетом таблиц, разработана обучающе-контролирующая программа для решения задач линейного программирования симплекс-методом. Данная программа может работать в двух режимах: *демонстрационном* и *контролирующем*.

Демонстрационный режим работы предназначен для обучения студентов. Программа в этом режиме последовательно выводит все таблицы решения задачи, снабжая каждую итерацию краткими пояснениями. По окончании решения задачи пользователь может распечатать отчет о решении задачи. В этот отчет может входить:

1. модель задачи;
2. все или некоторые таблицы;
3. результаты решения.

Контролирующий режим работы предназначен для проверки усвоения симплекс-метода студентом. На каждой итерации алгоритма программа задает пользователю вопросы и контролирует его ответы. Вопросы могут быть связаны как с ходом решения задачи (выбор ведущего столбца, разрешающей строки), так и с итерационными вычислениями. При этом количество вопросов на каждой итерации ограничено, основной объем вычислений проводит компьютер.

Если пользователь с трех попыток не смог правильно ответить на один и тот же вопрос, то ему предоставляется выбор: начать решение задачи сначала, или продолжить решение без претензий на удовлетворительную оценку. В том случае, когда пользователь успешно решил поставленную задачу, ответив на все вопросы (можно ошибаться, но не более двух раз на вопрос), формируется отчет, который можно распечатать на принтере. Наряду с описанием задачи отчет содержит:

1. количество заданных вопросов;
2. количество правильных ответов;

3. заданные вопросы, с указанием количества попыток правильно ответить на вопрос.

Эта информация может быть использована преподавателем при оценке знаний студента.

ПРОГРАММНЫЙ КОМПЛЕКС ВИЗУАЛИЗАЦИИ КАРТОГРАФИЧЕСКИХ ДАННЫХ СИСТЕМЫ МОДЕЛИРОВАНИЯ ПРОЦЕССОВ НЕФТЕДОБЫЧИ

В.В. Седельник

(БГУ, г. Минск)

Постановка задачи

Существующее программное обеспечение моделирования процессов нефтеизвлечения для представления картографической информации использует формат карты MAP. Карта формата MAP – совокупность разнотипных объектов, привязанных к целочисленной системе координат. Каждый тип объектов имеет свой набор атрибутов, определяющих его визуальное представление. Отметим, что большинство атрибутов определяют внешний вид объекта не прямо, а косвенно, с помощью индексации. Это, с одной стороны, обуславливает необходимость поддержки дополнительных структур данных для хранения "настоящих" параметров объекта, но, с другой стороны, позволяет создавать различные стили оформления карт и применять их "на лету", без изменения самих данных. Основные типы объектов карты:

– **Контур** – последовательность точек, соединенных отрезками прямых. Атрибуты линии контура: индекс цвета, стиль, толщина. Внутренность контура может быть пустой либо иметь заполнение шаблонами – небольшими растровыми изображениями, которые образуют узор. Атрибуты заполнения контура: стиль, индекс шаблона.

– **Символ** – специфический картографический значок (например, скважина). Имеет атрибуты индекса цвета и номера символа.

– **Текстовые строки**. Атрибуты: номер шрифта и номер цвета.

– Кроме того, нужны дополнительные структуры данных:

– **Цветовая палитра** (пока используется 16 цветов) и легенда, устанавливающая в соответствие атрибутам заполнения контуров определяемые пользователем цвета;

- Набор шаблонов заполнения контуров;
- Набор шрифтов для вывода текста и символов.

Особенности реализации

Технически программный комплекс реализован в виде Windows-приложения, выполненного по многодокументной технологии (MDI). Таким образом, реализованные технические решения основываются на системных сервисах ОС Windows. И хотя для некоторых элементов стандартных возможностей вполне достаточно, отдельные задачи все же потребовали разработки собственных методов.

Масштабирование

Масштаб MAP-изображения – это отношение длины линии на изображении к длине соответствующей линии в натуре (т.е. на местности). Масштаб обычно задается в виде дроби с числителем, равным 1 (1:10000, 1:25000, ...). Масштабирование – преобразование координат карты в координаты устройства и наоборот. Преобразование координат производится по формуле преобразования подобия с параллельным переносом. Коэффициент подобия вычисляется для каждой координатной оси по формуле:

$$k = M * MapMM * \frac{R}{S}, \quad (1)$$

где k – искомый коэффициент, M – масштаб изображения, $MapMM$ – длина единичного отрезка в миллиметрах, R – разрешение устройства вывода в пикселях, S – размер области вывода в миллиметрах.

Вывод изображения карты

Трудоемкость графического вывода карты обусловлена необходимостью заполнения контуров шаблонами нестандартных размеров. Отсечение вывода за пределы контуров осуществляется с помощью регионов отсечения Windows. При этом система корректно обрабатывает невыпуклые контура и контура с самопересечениями. Вывод непрозрачных заливок осуществляется копированием шаблона на экран. Прозрачные заливки выводятся с применением И- и ИЛИ-масок. При этом цвет результирующего пиксела вычисляется по формуле:

$$R = S \wedge A \vee O, \quad (2)$$

где S – исходный пиксел, A и O – пикселы соответственно И- и ИЛИ-масок. Маски формируются следующим образом:

$$A = \begin{cases} (FFFFFF)_{16}, P - \text{прозр.} \\ 0, P - \text{непрозр.} \end{cases}, \quad O = \begin{cases} 0, P - \text{прозр.} \\ P, P - \text{непрозр.} \end{cases} \quad (3)$$

где P – соответствующий пиксел шаблона.

Основные возможности пакета

Как уже говорилось, программный комплекс представляет собой Windows-приложение, выполненное по многодокументной технологии (MDI). Комплекс обеспечивает одновременную работу с любым количеством дочерних окон в рамках одного экземпляра приложения. Поддерживается 2 типа дочерних окон: окна карты и окна списка.

Работа с картой

Окно карты предназначено для просмотра одного MAP-файла. Окно карты предоставляет пользователю следующие инструменты:

- Лупа – инструмент изменения масштаба. Новое изображение центрируется в заданной точке.
- Фрагмент – инструмент распаивания на все окно выделенного прямоугольника карты.
- Прокрутка изображения может осуществляться как с помощью полос прокрутки, так и мышью в режиме захвата "рукой".
- Настройка изображения – группа инструментов управления режимами вывода отдельных элементов карты.
- Кадр печати – выделенный фрагмент изображения для печати (с визуальным разбиением на страницы) или копирования в буфер (в форматах BMP или EMF).

Работа с палитрой и легендой

Панель палитры предназначена для управления цветовой схемой MAP-изображения. Поддерживается список палитр, каждая из которых включает в себя 16 определенных пользователем произвольных RGB-цветов (с возможностью формирования плавных градиентных переходов).

Работа с легендой осуществляется в диалоговом окне "Легенда". Формирование легенды производится перетягиванием образцов заполнения и назначением необходимых цветов.

Работа со списком

Список – созданная пользователем последовательность карт для поочередного их просмотра. Элементами списка могут быть как MAP-файлы, так и папки. Основные возможности работы со списком:

- Изменение списка: добавление/удаление элементов, изменение порядка элементов («перетягиванием по протоколу Drag'n'Drop»);
- Просмотр списка, с возможностью анимированной смены карт через заданный промежуток времени и автоматическим позиционированием области просмотра в заданную точку.

Другие возможности

Для облегчения одновременной работы с несколькими окнами имеется инструмент синхронизации активных фрагментов карты, который предназначен для совмещения масштабов и центральных позиций нескольких окон.

АНАЛИЗ МОДЕЛЕЙ ДОЛГОСРОЧНОГО СТРАХОВАНИЯ ЖИЗНИ

Н.В. Семенчук

(ГрГУ, г. Гродно.)

Доклад посвящен применению вероятностных методов для анализа моделей долгосрочного страхования жизни. Получены аналитические выражения для нетто-премий и периодических премий. Все эти величины зависят от ряда основных вероятностных характеристик продолжительности жизни, для которых в работе выведены соотношения через функцию выживания. Обычно такие характеристики сводятся в так называемые таблицы продолжительности жизни. Таким образом, имея таблицу значений функции выживания, можно рассчитать основные характеристики продолжительности жизни, свести их в таблицу, и с помощью ее проводить анализ различных моделей страхования. Данный подход позволяет автоматизировать весь этот процесс в работе, то есть составить программу для нахождения нетто-премий и других важных величин, используя эту цепочку операций, для различных видов страхования.

В основе всех расчетов лежат следующие формулы для характеристик продолжительности жизни:

- 1) вероятность смерти человека в возрасте x лет в течение ближайших t лет.

$${}_t q_x = \frac{s(x) - s(x+t)}{s(x)} \quad (1)$$

2) вероятность того, что человек в возрасте x лет проживет еще, по меньшей мере, t лет.

$${}_tP_x = \frac{s(x+t)}{s(x)} \quad (2)$$

3) вероятность того, что человек возраста x проживет еще t лет, но умрет на протяжении и последующих лет.

$${}_t|uq_x = \frac{s(x+t) - s(x+t+u)}{s(x)} \quad (3)$$

Решение задачи нахождения нетто-премии – это важнейший момент в анализе моделей долгосрочного страхования. Предполагается, что покупка страховки производится в виде одиночной премии в момент заключения договора.

Рассмотрены наиболее часто используемые виды долгосрочного страхования и для них получены следующие формулы через функцию выживания.

n -летнее страхование жизни

$$\bar{A}_{x:n} = \frac{i e^{\delta(x-1)}}{\delta s(x)} \sum_{k=x}^{x+n-1} e^{-\delta k} [s(k) - s(k+1)]. \quad (4)$$

n -летнее смешанное страхование

$$\bar{A}_{x:n} = \bar{A}_{x:n}^1 + e^{-\delta n} \cdot \frac{s(x+n)}{s(x)} \quad (5)$$

полное страхование, отсроченное на m лет,

$$\bar{m}/\bar{A}_x = \bar{A}_x - \bar{A}_{x:m}^1, \quad (6)$$

полное страхование жизни (выплата страхового пособия производится в момент смерти)

$$\bar{A}_x = \frac{i \cdot e^{\delta x}}{\delta s(x)} \sum_{k=x}^{\infty} e^{-\delta k} [s(k) - s(k+1)] \quad (7)$$

где $i = e^{\delta} - 1$ – процентная ставка.

В предположении, что премия выплачивается в виде серии платежей в течение оговоренного срока, рассчитываются **периодические нетто-премии**.

Получены следующие выражения для периодических нетто-премий (в рамках полного страхования жизни)

С выплатой премии ежегодно

$$P(\bar{A}_x) = \frac{i}{\delta} \cdot \frac{\sum_{k=x}^{\infty} e^{-\delta k} (s(k) - s(k+1))}{\sum_{n=x}^{\infty} e^{-\delta n} s(n)} \quad (8)$$

С выплатой m раз в год

$$P^{(m)}(\bar{A}_x) = \frac{\bar{A}_x}{a_x^{(m)}}$$

где числитель по (8);

$$a_x^{(m)} = \frac{id}{i^{(m)} d^{(m)}} \cdot a_x - \frac{i - i^{(m)}}{i^{(m)} d^{(m)}} \quad (9)$$

$$\ddot{a}_x = \frac{1}{e^{-\delta x} s(x)} \sum_{n=x}^{\infty} e^{-\delta n} s(n)$$

$i^{(m)} = m(e^{\delta/m} - 1)$ – номинальная, %-ая ставка с частотой m .

$d = 1 - e^{-\delta}$; $d^{(m)} = (1 - (1 - d)^{1/m})$ – номинальная ставка дисконтирования с частотой m .

Таким образом, получены аналитические выражения для нетто-премий для долгосрочного страхования. Все вышеперечисленные характеристики вычисляются с помощью таблицы для функции выживания. Данный подход позволил составить программу на языке Delphi, позволяющую автоматизировать весь процесс их нахождения, получить таблицы данных характеристик и с помощью их проводить анализ моделей страхования. Программа имеет очень простой и удобный интерфейс, что позволяет использовать ее даже непрофессионалу.

МЕТОД ИССЛЕДОВАНИЯ ПРИЧИННО-СЛЕДСТВЕННЫХ СВЯЗЕЙ В СОЦИАЛЬНЫХ И ПРИРОДНЫХ СИСТЕМАХ

П.Н. Стрибук

(ГГУ, г. Гомель)

Для разрешения проблемы реалистичности и адекватности модели социальной или природной системы предлагается вместо одного-двух, чаще

всего линейных, уравнений связи с большим числом переменных перейти к построению иерархической сети уравнений взаимосвязи факторов. В работе при построении регрессионных моделей предлагается использовать проведенную пользователем интерпретацию концептуальной схемы формирования целевого свойства социальных и природных объектов [1]. Все признаки в результате такой интерпретации разбиты на группы по тому, какой компонент целевого функционирования они описывают. В данной схеме присутствуют следующие компоненты целевого функционирования:

– *Средства* – фрагменты среды, пассивной и активной подсистем функционирования, ресурсы которых используются непосредственно в процессе преобразования предмета функционирования;

– *Фон* – фрагменты среды, активной и пассивной подсистем функционирования, косвенным образом определяющие преобразование предмета функционирования;

– *Носитель целевого функционирования* – организм или цельная природная система, на базе которого происходит развитие «плода»;

– *Носитель узла связывания* – рабочее место для осуществления преобразований целевого функционирования;

– *Субъект* – активная составляющая целевого функционирования;

– *Инструмент* – управляемый сознанием фрагмент активной подсистемы функционирования, посредством которого осуществляется перевод части ресурсов (структурных, энергетических, информационных) от средств и входного предмета к выходному предмету функционирования.

Регрессионная модель, основанная на такой интерпретации концептуальной схемы, строится в следующем виде (схематически):

$$ЦС = Средства^{(Субъект и Инструмент)} \cdot Фон \cdot НосительЦФ' \quad (1)$$

при подробном расписывании получим уравнение вида (4).

Другая проблема традиционного подхода заключается в излишней математической «подгонке» коэффициентов модели. Алгоритмы расчета ориентированы на достижения наилучшего результата без учета содержательной природы входящих в модель признаков, поэтому в конце их работы очень часто получаются абсурдные результаты, обусловленные корреляцией между признаками, неинформативностью некоторых признаков и т. п. На практике необходимо получать лучший результат среди удовлетворительно интерпре-

тируемых и подходящих для дальнейшего анализа, пусть и не наилучший с математической точки зрения. Для решения этой проблемы предлагается изменить математические процедуры построения регрессионных уравнений путем наложения ограничений на изменение коэффициентов.

Рассмотрим сначала модифицированный алгоритм для построения мультипликативного уравнения регрессии вида

$$y = F(x) = \alpha_0 \cdot x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdot \dots \cdot x_n^{\alpha_n} \quad (2)$$

1. Находятся α^0_i из уравнения регрессии $y = x_i^{\alpha^0_i}$, при этом остаются в рассмотрении лишь те k признаков, для которых α^0_i достаточно велико и совпадает по знаку с соответствующим коэффициентом парной корреляции.

2. По значениям (α^0_i) строятся ранги (r^0_i), $i=1 \div k$.

3. Задаются пороги α^{δ}_0 и α^{δ}_i для α_0 .

4. Последовательно проходят $t=1 \div t_{max}$ итераций:

- находится шаг (s_i), $i=0 \div k$;
- строятся ранги (r_i), $i=1 \div k$ по значениям ($\alpha^i + s_i$);
- если значение α_0 выйдет за пределы α^{δ}_0 и α^{δ}_i , то s_0 уменьшается вдвое;
- сравниваются ранги r_i и r^0_i ; если отклонение по ним превышает заданный порог (зависит от количества участвующих в построении регрессионного уравнения признаков), то s_i уменьшается вдвое;
- при достижении некоторым s_i заданного порога малости он обнуляется;
- начиная с заданной итерации (например, десятой), проверяем условие вида

$$Err^t \cdot \sum_{i=1}^k \left| \frac{\Delta \alpha_i^t}{\alpha_i^{t-1}} \right| \geq \varepsilon \cdot Err^{t-1} \cdot \sum_{i=1}^k \left| \frac{\Delta \alpha_i^{t-1}}{\alpha_i^{t-2}} \right|, \quad (3)$$

где Err^t – ошибка модели на t -ой итерации, при его выполнении сохраняем состояние $t-1$;

- после выполнения условий сходимости или достижения максимального количества итераций выбираем лучший результат среди сохраненных состояний и результата последней итерации.

Описанный выше алгоритм построения уравнения простой мультипликативной регрессии можно применить и для построения уравнения регрессии более общего вида:

$$y = F(x) = \alpha_0 \cdot x_1^{\alpha_0 + \alpha_1 \cdot z_1^1 + \dots + \alpha_{k_1} \cdot z_1^{k_1}} \cdot x_2^{\alpha_0 + \alpha_1 \cdot z_2^1 + \dots + \alpha_{k_2} \cdot z_2^{k_2}} \cdot \dots \cdot x_n^{\alpha_0 + \alpha_1 \cdot z_n^1 + \dots + \alpha_{k_n} \cdot z_n^{k_n}} \quad (4)$$

Для этого преобразуем (4) к (2) следующим образом:

$$y = \alpha_0 \cdot x_1^{\alpha_1} \cdot \left(x_1^{\beta_1 \cdot z_1^1 + \dots + \beta_{k_1} \cdot z_{k_1}^1}\right)^{\alpha_1} \cdot x_2^{\alpha_2} \cdot \left(x_2^{\beta_1 \cdot z_1^2 + \dots + \beta_{k_2} \cdot z_{k_2}^2}\right)^{\alpha_2} \dots \cdot x_n^{\alpha_n} \cdot \left(x_n^{\beta_1 \cdot z_1^n + \dots + \beta_{k_n} \cdot z_{k_n}^n}\right)^{\alpha_n}, \quad (5)$$

где β^i , фиксируются после построения системы регрессионных уравнений вида

$$y = x_i^{\beta^i \cdot z_1^i + \dots + \beta_{k_i}^i \cdot z_{k_i}^i} = \left(x_i^{z_1^i}\right)^{\beta^i} \cdot \left(x_i^{z_2^i}\right)^{\beta^i} \dots \cdot \left(x_i^{z_{k_i}^i}\right)^{\beta^i}, \quad i=1 \div n. \quad (6)$$

Данные алгоритмы вошли в разработанное математическое программное обеспечение интеллектуального анализа данных, которое успешно применяется в РНИУП «Институт радиологии» при построении радиозокологических и социально-экономических моделей.

Апробация предложенного выше метода осуществлялась при исследовании связей факторов, объясняющих эффективность работы сельскохозяйственных предприятий. Итоги моделирования приведены в табл. 1.

Настоящая таблица представляет собой результат перевода соответствующих моделей нелинейной регрессии с количественного на качественный уровень. В таблице убраны случайные связи и выделены два уровня объяснения. Первый уровень относится к непосредственному объяснению эффективности производства, второй – к объяснению качества управления, который «взял на себя» опосредованное влияние других объясняющих признаков. Так, например, потенциал хозяйства и структура животноводства сказываются на эффективности как непосредственно, так и опосредованно через качество управления.

Таблица 1.

Качественные показатели направлений и силы статистических связей факторов эффективности производства и качества управления

	Кач. управле-ния	Потен-циал хоз.	Обеспеч. труд. ре-сурс.	Балл с/х угод.	Уд. вес активн. осн. ср.	Структ. жив-ства мол/мяс	Структ. произв. раст/жив
Эфф. произв.	↑	↑	↑	↑		↓	
Кач. управления		↑	↓	↑	↑	↓	↑

Обозначения:

	Прямая	Обратная	
Связь:	↑	↓	- слабая
	↑	↓	- умеренная (значимая)
	↑	↓	- сильная (уверенная)

Проинтерпретировав данные статистические связи на конкретном хозяйстве, можно сделать выводы о наличии у него резервов повышения эффективности экономической деятельности, о задействовании наиболее перспективных рычагов управления, предложить наиболее подходящие решения по выходу из кризисной ситуации.

Литература.

1. Осипенко А. Н. Метод и средства автоматизации моделирования активных систем: Автореф. дис... канд.техн.наук.: ГГУ, Гомель(1997)

МЕТОД И СРЕДСТВА ОДНОМЕРНОГО АНАЛИЗА ДАННЫХ ПРИ ИССЛЕДОВАНИИ СОЦИАЛЬНЫХ И ПРИРОДНЫХ ОБЪЕКТОВ

П.Н Стрибук

(ГГУ, г. Гомель)

С целью обеспечения адекватности одномерного анализа данных о социальной или природной системе в предлагаемом методе реализованы возможности: учета объема (при «ядерной» аппроксимации функции распределения признаков значений и при проверке гипотез), взвешивания конкретных значений (что, например, позволяет корректно обрабатывать данные, полученные из различных источников), обработки данных с пропусками и сжатых выборок, расщепления смеси, подбора преобразования, выделения репрезентативной подвыборки для последующего регрессионного анализа, визуализации эмпирического и теоретического распределений.

Одномерный анализ проходит по следующим этапам:

1. Нахождение эмпирических статистических характеристик, которые будут использоваться при дальнейшей работе с данными в том случае, если не удастся подобрать согласующееся теоретическое распределение и рассчитать по нему теоретические параметры.

2. «Ядерная» аппроксимация функции распределения. Выбор данного вида аппроксимации вызван тем, что на практике очень часто приходится работать с малыми выборками, по которым «ядерная» аппроксимация дает лучшую оценку параметров, чем стандартные методы (гистограмма и полигон частот) [1]. К тому же на «сверхмалых» выборках они не работают. Особенно это актуально при построении регрессионных моделей, так как детальная информация имеется лишь по небольшому числу объектов.

3. Проверка гипотез о нормальности и логнормальности распределения. Обнаружение нормальности или логнормальности упрощает дальнейшую работу с выборкой (легко находятся теоретические параметры, нет необходимости подбирать преобразования для приведения к нормальному виду, при выделении подвыборки признак, согласующийся с нормальным распределением, не приводит к сильному разрежению выборки и, как следствие, удалению информативных объектов).

4. Проверка на бимодальность и расщепление смеси. Бимодальность, как правило, возникает в случае, когда не была обеспечена однородность выборки и информация бралась для объектов из разных классов (например, измерения биохимического состава крови стада коров, в котором наряду со здоровыми коровами имеются больные).

5. Подбор преобразования выборки. Практически все методы многомерного анализа опираются на предположение о нормальности распределения входящих в модель случайных величин. Когда мы имеем несимметричную эмпирическую функцию распределения, имеет смысл преобразовать статистические данные так, чтобы получить вид функции плотности, наиболее приближенный к симметричному с тем, чтобы после проверки гипотезы о согласии подобрать теоретические параметры распределения и использовать данный признак в дальнейшем анализе.

6. Выделение подвыборки. На практике нередко возникает задача планирования пассивного регрессионного эксперимента путем выделения по данным массового обследования из исходного множества объектов такого его подмножества, которое удовлетворяет требованиям корректности регрессионных построений (обеспечение по каждому признаку, по крайней мере, одномодалности и симметричности распределения).

7. Оценка теоретических параметров распределения и формирование отчета.

Имеется возможность проводить автоматическое нормирование данных на основе полученной после работы программы информации о выборке.

После проведения анализа по каждому признаку формируется отчет (таблица) следующего содержания:

– Номер признака – NOMER;

– Объем выборки по данному признаку без учета (с учетом) пропусков в данных – N ;

– Доли подвыборок в смеси в случае его обнаружения – Q_1 и Q_2 ;

– Наилучшее значение параметра преобразования выборки (содержит единицу или нуль при обнаружении нормальности или логнормальности соответственно) – $LAMBDA$;

– Эмпирические статистические характеристики (среднее арифметическое – $SRARIFM$; среднее квадратическое отклонение – $SRKVOTKL$; медиана – E_MED ; среднее геометрическое – E_SRGEO ; среднегеометрическое отклонение – E_SGOTKL ; коэффициент вариации – E_VARIAC ; асимметрия и эксцесс – E_ASIMM и E_EKSC ; минимум и максимум – MIN и MAX ; 0.01, 0.05, 0.10, 0.15, ..., 0.90, 0.95, 0.99-й эмпирические квантили – E_Q01, \dots, E_Q99);

– Теоретические параметры распределения, в случае подтверждения гипотез о нормальности или логнормальности, успешности расщепления смеси или подбора преобразования (математическое ожидание – T_MO ; среднее квадратическое отклонение – T_SKO ; медиана – T_MED ; среднее геометрическое для логнормального распределения – T_SRGEO ; среднегеометрическое отклонение для логнормального распределения – T_SGOTKL ; коэффициент вариации – T_VARIAC ; асимметрия и эксцесс – T_ASIMM и T_EKSC ; 0.01, 0.05, 0.10, 0.15, ..., 0.90, 0.95, 0.99-й теоретические квантили – T_Q01, \dots, T_Q99 ; математические ожидания и среднее квадратические отклонения подвыборок в смеси – T_MO1, T_SKO1 и T_MO2, T_SKO2).

Также по каждому признаку создаются файлы необходимых графиков.

Разработанное математическое обеспечение одномерного анализа данных, было апробировано в РНИУП «Институт радиологии» при анализе дозиметрических показателей: дозы внутреннего облучения жителей (по СИЧ-измерениям), содержания радионуклидов в молоке, мясе и т. п. Данное математическое обеспечение основано на ряде авторских разработок, а также усовершенствованных автором алгоритмов, приведенных в [2]. Основные результаты одномерного анализа на примере СИЧ-измерений жителей населенных пунктов Брагинского района приведены в табл. 1.

Фрагмент отчета по результатам работы программы одномерного анализа доз внутреннего облучения жителей населенных пунктов.

Наименование населенного пункта	N	Q1	Q2	...	T_Q01	...	T_Q50	...	T_Q99	T_M01	T_SK01	T_M02	T_SK02
Соболи	143	0,7	0,3	...	0,00	...	0,20	...	0,44	0,16	0,07	0,31	0,08
1 день	119	0,7	0,3	...	0,06	...	0,41	...	0,86	0,35	0,13	0,62	0,16
Кирово	214	0,8	0,2	...	0,09	...	0,32	...	0,73	0,29	0,09	0,50	0,16
Асаревичи	386	0,8	0,2	...	0,00	...	0,21	...	0,57	0,19	0,08	0,43	0,10
Галки	111	0,5	0,5	...	0,05	...	0,26	...	0,54	0,21	0,07	0,34	0,10
Верхние Жары	139	0,8	0,2	...	0,08	...	0,25	...	0,50	0,23	0,07	0,43	0,08
Нижние Жары	70	0,1	0,9	...	0,06	...	0,27	...	0,52	0,35	0,13	0,27	0,08
Алексеевка	202	0,9	0,1	...	0,01	...	0,20	...	0,57	0,19	0,08	0,39	0,14
Переносы	93	0,7	0,3	...	0,02	...	0,18	...	0,47	0,16	0,06	0,30	0,12
Городище	101	0,6	0,4	...	0,07	...	0,23	...	0,61	0,19	0,06	0,37	0,12
Заречье	319	0,9	0,1	...	0,02	...	0,20	...	0,56	0,19	0,08	0,46	0,15
Котловица	192	0,7	0,3	...	0,03	...	0,21	...	0,44	0,19	0,07	0,28	0,09
Малейки	652	0,9	0,1	...	0,00	...	0,23	...	0,71	0,21	0,09	0,58	0,10
Селец	435	0,8	0,2	...	0,01	...	0,22	...	0,63	0,20	0,08	0,41	0,14
Старый Мокрец	99	0,3	0,7	...	0,03	...	0,20	...	0,32	0,13	0,05	0,23	0,05
Красная Поляна	14	0,3	0,7	...	0,02	...	0,16	...	0,27	0,10	0,03	0,18	0,04

Литература.

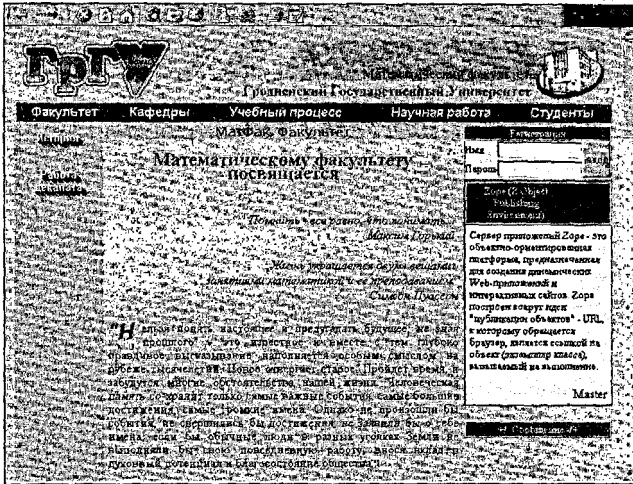
1. Гаскаров Д. В., Шаповалов В. И. Малая выборка. – М.: Статистика, 1978. – 185 с.
2. Айвазян С. А., Енюков И. С., Мешалкин Л. Д. Прикладная статистика: Основы моделирования и первичная обработка данных. – М.: Финансы и статистика, 1983. – 471 с.

ОБРАЗОВАТЕЛЬНЫЙ СЕРВЕР ФАКУЛЬТЕТА НА ПЛАТФОРМЕ СЕРВЕРА ПРИЛОЖЕНИЙ ZORE

А.И. Ступяк, В.С. Скращук, П.В. Картацев, В.С. Никитенко, А.Н. Ваглай
(ГрГУ, г. Гродно)

Характерными особенностями сервера, построенного на платформе сервера приложений Zore являются:

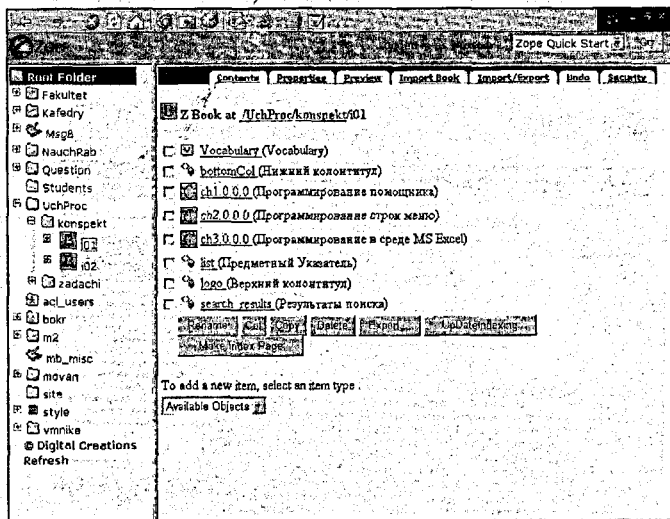
- управление через WWW
- интегрированный контроль доступа
- оперативная модификация содержания
- доступ к распределенным данным
- встроенные средства поиска
- наличие модели разделения данных
- безопасное делегирование полномочий



Основные функции образовательного сервера факультета вуза:

1. Создание единой информационной среды на основе сетевых коммуникаций в рамках факультета. Интеграция с базами данных АСУ «Университет»
2. Поддержка учебного процесса – факультетская доска объявлений, обеспечение функционирования систем дистанционного образования и самостоятельной работы, виртуальных классов, размещение электронных задачников и электронных учебных пособий, размещение тестирующих систем и т.п.
3. Воспитательная функция – среда интерактивного общения и самовыражения, размещение личных web-страниц.
4. Научно-исследовательская – проведение электронных научных конференций, форумов, размещение материалов студенческих научных кружков.
5. Административные функции – публикация объявлений и распоряжений деканата и кафедр, контроль за ходом учебного процесса, ведение расписания, обеспечение доступа к базам данных кафедр и деканатов.

Сервер приложений Zope (продукт фирмы Zope Creations [1]) – это объектно-ориентированная платформа, предназначенная для создания динамических Web-приложений и интерактивных сайтов. Zope построен вокруг идеи "публикации объектов": URL, к которому обращается браузер, является ссылкой на объект (экземпляр класса), вызываемый на выполнение. Сами объекты хранятся в объектно-ориентированной базе данных ZODB.



Инфраструктура ZOPE позволяет разработчику сосредоточиться на проблеме, избавляя от забот о доступности и целостности данных и управлении доступом. Сервер приложений ZOPE может функционировать на различных платформах, как под Windows, так и под операционными системами семейства Unix, он использует два языка – язык шаблонов (представлений) DTML и язык реализации Python. DTML – механизм интерпретации (рендеринга) шаблонов, язык программирования, основанный на тэгах. Архитектура сервера приложений Zope базируется на компонентной технологии. Использование пользовательских компонент (ZClass, ZProducts) позволяет существенно расширить функциональность базовой системы.

В рамках проекта «Образовательный сервер факультета на платформе сервера приложений Zope» разработаны пользовательские компоненты (Z-продукты) Z VClass, Z Book, Z Task, Z MessageBoard, Z Voting Pool.

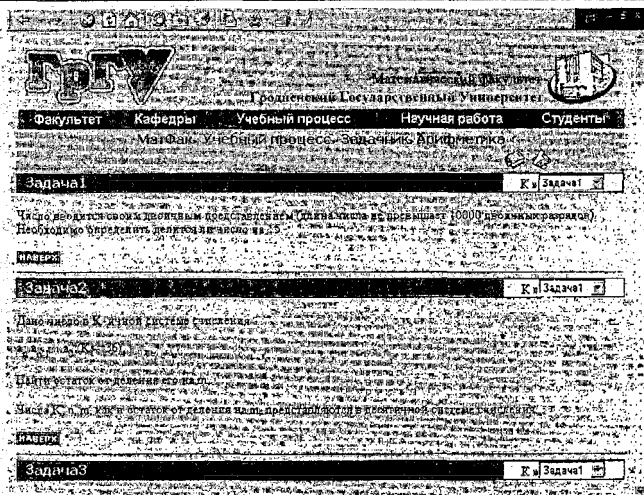
Использование продукта Z VClass (виртуального класса) предполагает

распределение учебного процесса во времени и пространстве, выражающееся в отказе от строгого и одновременного посещения учебных занятий всеми членами учебной группы: средства организации сетевого взаимодействия преподавателя и студента; базы данных для хранения регистрационных данных и данных о ходе работы в виртуальном классе; доступ к продуктам Z Task - электронным задачникам по изучаемым разделам информатики и специальным дисциплинам; доступ к продуктам Z Book – электронным учебным пособиям; средства контроля хода учебного процесса.

Для представления и структуризации учебных материалов в виде электронных пособий разработан продукт Z Book – электронный конспект. Для создания банков задач по темам лабораторного практикума разработан продукт Z Task – электронный задачник.



Основные возможности, предоставляемые продуктами Z Book и Z.Task: представление информации в виде структурированного набора гипертекстовых документов; заполнение страниц конспекта посредством web-интерфейса; наполнение данными путем импортирования архивного файла, содержащего набор html документов и файлов изображений в произвольных графических форматах; встроенная система поиска информации по ключевым словам; встроенная система для создания предметного указателя; встроенная система автоматического создания оглавления; встроенные средства контроля качества и поддержки целостности электронных учебных пособий.



Для публикации новостей и сообщений создан компонент **Z MessageBoard** – электронная система обмена сообщениями. Предполагается наличие несколько уровней, определяемых структурой учебного заведения, для создания и публикации сообщений. Доступ к опубликованным сообщениям регламентируется в соответствии с ранее распределёнными ролями (категориями пользователей). Основные достоинства продукта: возможность оперативного добавления, модификации и удаления сообщений посредством web-интерфейса; наличие системы фильтрации сообщений для их публикации на различных уровнях иерархии; возможность архивации устаревших сообщений с последующим их просмотром; возможность децентрализованного наполнения банка сообщений информацией; наличие двух типов сообщений: новости и долгосрочные объявления.

Для проведения электронных голосований и сбора статистических данных по злободневным вопросам университетской жизни предназначена система электронного голосования **Z Voting Pool**. Обеспечивает возможность оперативного добавления, модификации и удаления тем голосований и вопросов посредством web-интерфейса; графическое представление результатов голосований в виде столбчатых гистограмм; возможность просмотра результатов текущего голосования; наличие защиты от недобросовестного использования (многократное голосование в течение короткого промежутка времени); возможность архивации результатов голосований с последующим их просмотром.

Прототип образовательного сервера математического факультета на платформе сервера приложений Zope функционирует в intranet-сети Гродненского государственного университета.

Литература

1. <http://www.zope.org>

ЛИНЕЙНОЕ ПРОГРАММИРОВАНИЕ В ФИНАНСОВОМ АНАЛИЗЕ И ПЛАНИРОВАНИИ

О.Г. Шапко, К.Л. Пылило

(БГПА, г. Минск)

В финансовом планировании широко используются оптимизационные возможности линейного программирования. Использование линейного программирования предполагает предварительный выбор целевой функции, такой, как максимизация стоимости компании. Модель линейного программирования производит оптимизацию этой целевой функции при соблюдении установленных ограничений (максимально допустимые значения коэффициентов "квоты собственника" и выплаты дивидендов).

Существуют три этапа подготовки задачи для решения методом линейного программирования:

1. Выделить искомые управляемые переменные.
2. Определить целевую функцию, подлежащую максимизации или минимизации, и записать ее с использованием искомых управляемых переменных. Обычно в качестве функции выступает максимизация прибыли или минимизация издержек.
3. На основе искомых переменных посредством линейных уравнений или неравенств установить набор ограничений.

Рассмотрим использование линейного программирования для решения задачи максимизации прибыли.

Производитель игрушек компания «Лорина» производит три типа игрушек: "Королевская кобра" (КК), пистолет "Пит" и "Рок Кули" (РК). Производство во всех случаях состоит в изготовлении пластмассовых отливок и сборке деталей. Расходы времени на отливку деталей и сборку, переменные издержки, цены и прибыль по каждому типу игрушек даны в таблице 1.

Компания «Лорина» финансирует свою деятельность за счет банковских кредитов. По условию кредитования компания должна поддерживать значение коэффициента покрытия на уровне не менее единицы. В противном случае кредит подлежит немедленному погашению. Балансовый отчет компании представлен в таблице 2.

Таблица 1

Производственные и финансовые характеристики компании

Модель	Загрузка машин, часов	Загрузка сборочной линии, часов	Цена, долл./шт.	Переменные издержки, долл./шт.	Прибыль, долл./шт.
КК	5	5	11	10	1
ПП	4	3	8	4	4
РК	5	4	8	5	3
Всего	150	100	-	-	-

Таблица 2

Балансовый отчет компании «Лорина»

Активы, долл.		Пассивы, долл.	
Денежные средства	100	Банковские кредиты	130
Легкорезализуемые ценные бумаги	100	Долгосрочный долг	300
Дебиторская задолженность	50	Акционерная собственность	70
Машины и оборудование	250		
Всего	500	Всего	500

В этом случае целевой функцией является максимизация вклада каждого продукта в прибыль компании. Из таблицы 1 видно, что прибыль по каждому продукту составляет: КК = 1\$, ПП = 4\$, РК = 3\$. Умножив эти величины на число проданных изделий каждого вида, можно получить величину прибыли компании от основной деятельности. Таким образом, целевая функция имеет следующий вид:

$$\max P = X_1 + 4X_2 + 3X_3, \tag{1}$$

где X_1, X_2 и X_3 – величина сбыта продуктов КК, ПП и РК.

Теперь следует установить ограничения для задачи линейного программирования. Производственные возможности компании ограничены фондом машинного времени и времени на сборку. На основании данных таблицы 1 ограничения можно записать следующим образом:

$$5X_1 + 4X_2 + 5X_3 \leq 150 \text{ч (ограничение по машинному времени);} \tag{2}$$

$$5X_1 + 3X_2 + 4X_3 \leq 100 \text{ч (ограничение по времени на сборку).} \tag{3}$$

Существует также ограничение по максимальному объему производства изделий ГП и РК. Маркетинговый отдел определил, что можно продать не более 10 ед. этих изделий, поэтому:

$$X_2 + X_3 \leq 10 \text{ (ограничение по сбыту).} \quad (4)$$

Наконец, предоставляющий кредиты банк требует, чтобы коэффициент покрытия был не меньше единицы. Таким образом:

$$\frac{100 + 100 + 50 - 10X_1 - 4X_2 - 5X_3}{130} \geq 1;$$

$$10X_1 + 4X_2 + 5X_3 \leq 20 \text{ (текущий коэффициент покрытия).} \quad (5)$$

Поскольку объем производства каждого изделия не может быть меньше нуля, можно сформулировать последнее ограничение:

$$X_1, X_2, X_3 \geq 0 \text{ (условие неотрицательности значений).} \quad (6)$$

Решив эту задачу линейного программирования с помощью симплекс-метода, получаем таблицу 3, в которой представлено оптимальное решение.

Таблица 3

Решение уравнения: симплекс-таблица

	Действительные переменные			Нежесткие переменные				
	X ₁	X ₂	X ₃	S ₁	S ₂	S ₃	S ₄	
S ₁	0	0	0,5	1	0	-2	0,5	70
S ₂	0	0	0,5	0	1	-1	0,5	30
X ₂	0	1	1	0	0	1	0	10
X ₁	1	0	0,1	0	0	-0,4	0,1	8
Коэффициенты целевой функции								
Прибыль	0	0	-1,1	0	0	-3,6	-0,1	-48
Общая прибыль	48							

В таблице 3 решения для переменных X₁ и X₂ даны в правой колонке: X₁ = 8 ед. и X₂ = 10 ед. Поскольку X₃ не появляется в окончательном решении, его значение равно 0. Нежесткие переменные говорят о величине неиспользуемых ресурсов. Поскольку S₁ = 70, то компания располагает 70ч неиспользованного машинного времени. Чтобы произвести 8 ед. X₁ и 10 ед. X₂, нужно по 40ч машинного времени, а в сумме – 80ч, что на 70ч меньше, чем доступный фонд машинного времени – 150ч. Поскольку S₁ = 30, то компания располагает дополнительно 30ч времени на сборку. Из S₃ = 0 следует, что ограничение X₂ + X₃ = 10 ед. выполняется. Из S₄ = 0 следует, что ограничение на ве-

личину коэффициента покрытия также выполнено и финансирование, а точнее, нехватка финансирования, эффективно ограничивает объем производства. Если компания изменит условия кредитного договора с банком или найдет необходимые средства где-либо еще, она сможет производить больше. При существующем уровне производства максимально возможная величина прибыли равна 48 долл.

Литература

1. Крувищ Л. Финансирование и инвестиции. Неоклассические основы теории финансов / Пер. с нем. Под общей редакцией В.В. Ковалева, З.А. Сабова. – СПб.: Издательство «Питер», 2000. – 400 с.
2. Ченг Ф. Ли, Джозеф И. Финнерти. Финансы корпораций: теория, методы и практика. Пер. с англ. – М.: ИНФРА-М, 2000. – 686 с.

ИСПОЛЬЗОВАНИЕ СИСТЕМЫ АЛГЕБРАИЧЕСКИХ УРАВНЕНИЙ В ФИНАНСОВОМ АНАЛИЗЕ И ПЛАНИРОВАНИИ

О.Г. Шапко

(БГПА, г. Минск)

В финансовом анализе и планировании используется модель Уоррена и Шелтона (Warren, Shelton), которая основана на системе алгебраических уравнений. Модель FINPLAN охватывает всю сферу финансового планирования в корпорации, а не какую-то ее часть, такую, как, например, распределение инвестиций. Модель FINPLAN не нацелена на оптимизацию каких-либо показателей, но представляет собой средство обеспечения менеджеров нужной информацией. Одним из достоинств этой модели планирования является то, что она позволяет пользователю "проигрывать" различные варианты финансового будущего при изменении таких независимых переменных, как объем продаж, уровень нераспределенной прибыли, соотношение долга и акционерного капитала.

Использование в модели системы алгебраических уравнений, описывающих инвестиционную, финансовую, производственную и дивидендную политику, позволяет ей выявить взаимосвязь этих сфер деятельности компании. Модель Уоррена и Шелтона представляет собой систему из 20 уравнений, перечисленных в таблице 1. Уравнения делятся на подгруппы, соответствующие данным о продажах, инвестициях, финансировании и доходности акций.

Таблица 1

Модель FINPLAN

<p>Раздел 1. Вычисление объемов продаж (sales) и доходов до уплаты процентов и налогов (EBIT) за период t:</p> <p>(1) $SALES_t = SALES_{t-1}(1 + GSALES_t)$;</p> <p>(2) $EBIT_t = REBIT_t SALES_t$.</p>
<p>Раздел 2. Вычисление в суммарной потребности в активах на период t:</p> <p>(3) $CA_t = RCA_t SALES_t$;</p> <p>(4) $FA_t = RFA_t SALES_t$;</p> <p>(5) $A_t = CA_t + FA_t$.</p>
<p>Раздел 3. Вычисление потребностей в финансировании для желаемого уровня активов:</p> <p>(6) $CL_t = RCL_t SALES_t$;</p> <p>(7) $NF_t = (A_t - CL_t - PFDSK_t) - (L_{t-1} - LR_t) - S_{t-1} - R_{t-1} - b_t \{ (1 - T_t) [EBIT_t - i_{t-1} (L_{t-1} - LR_t)] - PFDIV_t \}$;</p> <p>(8) $NF_t + b_t (1 - T_t) [i_t^e NL_t + U_t^1 NL_t] = NL_t + NS_t$;</p> <p>(9) $L_t = L_{t-1} - LR_t + NL_t$;</p> <p>(10) $S_t = S_{t-1} + NS_t$;</p> <p>(11) $R_t = R_{t-1} + b_t \{ (1 - T_t) [EBIT_t - i_t L_t - U_t^1 NL_t] - PFDIV_t \}$;</p> <p>(12) $i_t = i_{t-1} \left(\frac{L_{t-1} - LR_t}{L_t} \right) + i_t^e \frac{NL_t}{L_t}$;</p> <p>(13) $\frac{L_t}{S_t + R_t} = K_t$.</p>
<p>Раздел 4. Вычисление показателей в расчете на акцию за период t:</p> <p>(14) $EAFCD_t = (1 - T_t) [EBIT_t - i_t L_t - U_t^1 NL_t] - PFDIV_t$;</p> <p>(15) $CMDIV_t = (1 - b_t) EAFCD_t$;</p> <p>(16) $NUMCS_t = NUMCS_{t-1} + NEWCS_t$;</p> <p>(17) $NEWCS_t = \frac{NS_t}{(1 - U_t^1 P_t)}$;</p> <p>(18) $P_t = m_t EPS_t$;</p> <p>(19) $EPS_t = \frac{EAFCD_t}{NUMCS_t}$;</p> <p>(20) $DPS_t = \frac{CMDIV_t}{NUMCS_t}$.</p>

Ключевой независимой переменной модели FINPLAN является оценка роста продаж (GSALS_t). Уравнение 1 в таблице 1 показывает, что объем продаж за период t равен объему продаж за предыдущий период, умноженному на скорость роста продаж за период t . Затем мы получаем значение дохода до вычета процентов и налогов (ЕВIT), выражаемого как процент от объема продаж. Затем снова через отношение к объему продаж получаем значение текущих и постоянных активов — $CA/SALES$ и $FA/SALES$. Сложив CA и FA , получаем величину совокупных активов за период.

В третьем разделе таблицы 1 вычисляются финансовые показатели. В уравнении 6, исходя из коэффициента $CL/SALES$, умноженного на $SALES$, мы получаем значение текущих активов. В уравнении 7 вычисляется величина потребности в средствах (NF_t). Модель FINPLAN исходит из предположения, что число привилегированных акций в планируемом периоде остается неизменным. Вычисляя потребность в средствах и их возможные источники, модель FINPLAN использует концепцию учетной идентичности источников и использования средств. Уравнение 7, например, показывает, что активы за период t создают основные финансовые потребности компании. Текущие активы, вычисляемые в уравнении 6, являются источником средств, а поэтому их вычитают из величины активов. Привилегированные акции являются неизменной величиной, а поэтому их также следует вычитать. Первый член уравнения 7 ($A_t - CL_t - PFDSK_t$) определяет потребность в финансировании из внутренних и долгосрочных внешних источников. Выражение во вторых скобках ($L_{t-1} - LR_t$) учитывает обязательства по старым долгам за период t . Затем вычитаются средства, имеющие источником уже размещенные акции и нераспределенную прибыль. Наконец, вычитаются средства, полученные от основной деятельности за период t . Когда мы определили объем денежных средств, необходимых для основной деятельности, с помощью уравнения 8 рассчитываем величину поступления средств от новой эмиссии долгосрочного долга и акций (за вычетом расходов на размещение и процентов по новому долгу). С помощью уравнений 9 и 10 вычисляются новые значения долга и акционерного капитала с учетом новой эмиссии за период t . По уравнению 11 вычисляется новый показатель нераспределенной прибыли с учетом прибыли от основной деятельности за период t , которая может быть источником дивидендных выплат. Здесь b_t является коэффициентом реинвестирования за период t ; $a(1-T_t)$ — есть процент посленалоговой выплаты, который умножают на величину дохода за период, из которого вычли

процентные выплаты по новому и старым долгам. Поскольку дивиденды по привилегированным акциям должны быть выплачены прежде, чем получат и свои деньги владельцы обыкновенных акций, сумму привилегированных дивидендов следует вычесть из дохода, пригодного для выплаты обычных дивидендов. Уравнение 12 вычисляет новую средневзвешенную процентную ставку по долгу. Уравнение 13 вычисляет новое отношение долга к акционерному капиталу за период t .

Раздел 4 таблицы 1 охватывает обыкновенные акции, в том числе дивиденды и рыночную стоимость. Уравнение 17 дает величину доходов, пригодных для дивидендов по обыкновенным акциям, т.е. посленалоговую прибыль. Уравнение 15 вычисляет доход, подлежащий выплате в качестве дивидендов на обыкновенные акции. Уравнение 17 дает новое число размещенных обыкновенных акций с учетом эмиссии за период t .

Как видно из уравнения 17, мы получаем число новых обыкновенных акций, разделив поступления от новой эмиссии на курс одной акции, из которого вычтены расходы на эмиссию. Уравнение 18 определяет курс одной акции как произведение прибыли на акцию и отношения курса акции к прибыли на акцию (m_1). Уравнение 19 дает стандартное определение прибыли на акцию (EPS), как частное от деления прибыли, пригодной для распределения среди владельцев обыкновенных акций, на число размещенных обыкновенных акций. Похожим образом определены дивиденды в уравнении 20.

Литература

1. Крувшиц Л. Финансирование и инвестиции. Неоклассические основы теории финансов / Пер. с нем. Под общей редакцией В.В. Ковалева, З.А. Сабова. – СПб.: Издательство «Питер», 2000. – 400 с.
2. Ченг Ф. Ли, Джозеф И. Финнерти. Финансы корпораций: теория, методы и практика. Пер. с англ. – М.: ИНФРА-М, 2000. – 686 с.

МАТРИЦЫ В УРАВНЕНИЯХ МЕЖОТРАСЛЕВОГО БАЛАНСА

Д.К. Яцушкевич

Связь между отраслями промышленности, как правило, отражается в таблицах межотраслевого баланса. Математическая модель, позволяющая их анализировать, разработана в 1936г. американским экономистом В.Леонтьевым, [1].

Предположим, что рассматривается n отраслей промышленности, каждая из которых производит свою продукцию. Часть продукции идет на внут-

рипроизводственное потребление данной отраслью и другими отраслями, а другая часть предназначена для целей конечного (вне сферы материального производства) личного и общественного потребления. Рассмотрим процесс производства за некоторый период: времени (например, год). Введем следующие обозначения: x_i – общий (валовой) объем продукции i -ой отрасли ($i = 1, 2, \dots, n$); x_{ij} – объем продукции i -ой отрасли, потребляемой j -ой отраслью в процессе производства ($i, j = 1, 2, \dots, n$); y_i – объем конечного продукта i -ой отрасли для непроизводственного потребления.

Так как валовой объем продукции любой i -ой отрасли равен суммарному объему продукции, потребляемой n отраслями, и конечного продукта, то получим систему уравнений вида:

$$x_i = \sum_{j=1}^n x_{ij} + y_i, (i=1, 2, \dots, n), \quad (1)$$

которые называются соотношениями баланса. Будем рассматривать стоимостный межотраслевой баланс, когда все величины, входящие в (1), имеют стоимостное выражение.

Введем коэффициенты прямых затрат:

$$a_{ij} = \frac{x_{ij}}{x_j}, (i, j = 1, 2, \dots, n)$$

показывающие затраты продукции i -ой отрасли на производство единицы продукции j -ой отрасли.

Можно полагать, что в некотором промежутке времени коэффициенты a_{ij} будут постоянными и зависящими от сложившейся технологии производства. Это означает линейную зависимость материальных затрат от валового выпуска:

$$x_{ij} = a_{ij}x_j, (i, j = 1, 2, \dots, n)$$

вследствие чего построенная на этом основании модель межотраслевого баланса получила название линейной. Соотношения баланса (1) примут вид:

$$x_i = \sum_{j=1}^n a_{ij}x_j + y_i \quad (2)$$

Введем матрицы

$$X = \begin{pmatrix} x_1 \\ x_2 \\ \dots \\ x_n \end{pmatrix}, A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix}, Y = \begin{pmatrix} y_1 \\ y_2 \\ \dots \\ y_n \end{pmatrix},$$

где X – вектор валового выпуска, Y – вектор конечного продукта, A – матрица прямых затрат.

Тогда систему (2) можно записать в матричном виде:

$$X = AX + Y \tag{3}$$

Если матрица $(E - A)$ невырожденная, то матричное решение уравнения (3)

$$X = (E - A)^{-1} Y$$

Матрица $S = (E - A)^{-1}$ называется матрицей полных затрат. Каждый элемент s_{ij} матрицы S это величина валового выпуска продукции i -ой отрасли, необходимого для обеспечения выпуска единицы конечного продукта j -ой отрасли.

Написана программа, позволяющая решить следующую задачу: предприятие состоит из двух основных цехов и одного вспомогательного, каждый из которых выпускает один вид продукции.

Цеха	a_{ij}			y_i	Материал	b_{ij}			Стоимость c_i
I	a_{11}	a_{12}	a_{13}	y_1	Сырье S1	b_{11}	b_{12}	b_{13}	c_1
II	a_{21}	a_{22}	a_{23}	y_2	Сырье S2	b_{21}	b_{22}	b_{23}	c_2
III	a_{31}	a_{32}	a_{33}	y_3	Топливо	b_{31}	b_{32}	b_{33}	c_3
					Трудоемкость b_j	b_1	b_2	b_3	P

Входные данные: расходные коэффициенты единиц продукции i -ого цеха; количество единиц i -ого цеха, предназначенных для реализации; расходные нормы двух видов сырья и топлива на единицу продукции соответствующего цеха; трудоемкость продукции в человеко-часах на единицу продукции; стоимость соответствующего материала и оплата за 1 человеко-час.

Выходные данные: уравнение межотраслевого баланса по Леонтьеву; коэффициенты полных затрат; валовый выпуск для каждого цеха; производственная программа цехов; коэффициенты косвенных затрат; суммарный расход сырья, топлива и трудовых ресурсов на единицу конечной продукции каждого цеха; расход сырья, топлива и трудовых ресурсов по цехам; производственные затраты по цехам и на всю производственную программу предприятия; производственные затраты на единицу конечной продукции для каждого цеха.

Литература.

1. Солодовников А.С., Бабайцев В.А., Браилов А.В. Математика в экономике: Учебник: В 2-х ч. Ч.1. – М.: Финансы и статистика, 1999. – 224 с.

СОДЕРЖАНИЕ

АНАЛИТИЧЕСКИЕ И ЧИСЛЕННЫЕ МЕТОДЫ ИССЛЕДОВАНИЙ В МАТЕМАТИКЕ	3
М.А. Акинфина. Численный анализ характеристик сглаженной периодограммы Бартлетта	3
А.С. Андреев. О каноническом лифте подмногообразия однородного пространства	6
А.М. Астахов. Рекуррентные методы анализа средних значений	8
Н.Г. Бородулина, А.В. Морской. Численный метод нахождения коэффициентов характеристического полинома	11
Н.А. Брызгалова. Один из способов представления решения нелинейного разностного уравнения p -го порядка	12
Л.В. Дорошева. Об одном способе выбора параметра регуляризации при решении обратной задачи в оптико-электронной системе дистанционного зондирования	14
Н.А. Илючик, В.М. Мадорский. Метод прогонки для пятидиагональной матрицы	18
А.Н. Ковальчук. Стохастические уравнения в θ -интегралах в алгебре обобщенных случайных процессов	22
А.В. Кот. Сравнительная характеристика способов аппроксимации разностных решений задачи дuffинга	25
О.Н. Курочка. О геометрических характеристиках одномерных подгрупп группы G вращений пространства 2R_4	29
Л.И. Лавринович. Однократно замыкаемые оптимальные обратные связи	30
А.В. Маковский. Построение и анализ аналитических решений задач о мгновенном точечном взрыве	33
О.В. Матысик. Регуляризация некорректных задач методом итераций невязного типа	37
Н.К. Млынчик. Линейные однородные нагруженные дифференциальные уравнения второго порядка	39
Э. В. Мусафиров. Системы с отражающей матрицей представляющей собой произведение двух матричных экспонент	41
Т.Ф. Новик. Некоторые приложения теоремы Силова	44
Р. Ю. Плотников. Ряды Фурье усиленной сходимости	45
Т. В. Соболева. О некоторых методах моделирования устойчивых случайных распределений и процессов	49
Н.Н. Стрилец, В.М. Мадорский. Вычислительные затраты при численном решении периодических уравнений дuffинга и ван-дер-поля	51

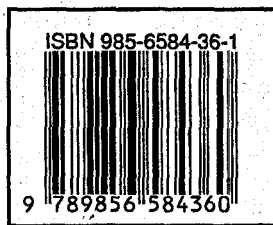
Т.В. Цеховая. Применение m – оценки Хьюбера для вариограммы стационарного случайного процесса	55
В.Н. Шуть, И.Г. Прожерин. Идентификация объектов и процессов по корреляционному образу	58
СОВРЕМЕННЫЕ ТЕХНОЛОГИИ ПРОГРАММИРОВАНИЯ, ИНФОРМАЦИОННЫЕ СЕТИ И СИСТЕМЫ	61
В.Л. Бусько, В.Ю. Вишкевич. Информационная составляющая экспертных оценок	61
А.А. Врублевский. Алгоритм рbsp-деревьев и его применение	66
М.М. Высоцкий разработка программного комплекса для обеспечения живучести однородных программируемых древовидных структур на СБИС ПЛМ	67
А.И. Галабурда. Защита информации в компьютерных сетях	70
А.И. Галабурда. Система аутентификации kerberos	73
Н.В. Маньяков. Вычисление характеристик хаотической диссипативной динамической системы	75
И.К. Мирончиков. Модели живучих однородных программируемых структур	78
А.В. Орлов. Математическая модель распределения и исправления ошибок в элементах памяти	82
Д.М. Романенко. Оптимизация параметров проверочных матриц для линейного и трехмерного итеративного кодов с проверочными символами по диагонали	85
Д.М. Романенко. Алгоритмы коррекции многократных ошибок трехмерным итеративным кодом с проверочными символами по диагонали	88
В.С. Скрацук, В.М. Волчкевич, Д.Н.Кортелев. Использование гиперболических браузеров для визуализации больших иерархических структур	91
А.М. Суходольский., Д.П. Урбанович. Оценки алгоритмов цифровой подписи	95
Д.П. Урбанович. Некоторые аспекты проблемы использования электронной подписи	98
ПРИКЛАДНЫЕ АСПЕКТЫ ИНФОРМАТИКИ И МАТЕМАТИКИ	101
А.В. Афонин. Одномерная модель микроструктуры строительных материалов	101
А.К. Васечко. Восстановление распределения сопротивления в электроимпедансной томографии	104
Е.В. Гаспадарик. Динамическая межотраслевая балансовая модель	108
Н.В. Гиреева, М.Н. Гриневич. Применение факторного анализа для комплексной оценки деятельности субъектов хозяйствования	111
Н.В. Десева. Многоуровневая система организации работы с информационными потоками факультета вуза	114
П.А. Жолудев, Л.О. Каплинская. Построение кривой свободной поверхности потока неравномерного установившегося движения воды в открытых призматических руслах	116

С.Н. Иванов. Компьютерное представление и сравнение аналитических решений задач распространения тепла в почвогрунтах	118
А.В. Морской. Об одном нечётко-интервальном подходе в имитационном моделировании	121
А.В. Паньков. Исследование вероятностной модели банковской сети	123
А.А. Паук, В.А. Суслов. Аспекты развития компьютерной системы тестового контроля знаний в БГТУ	125
А.А. Паук, В.А. Суслов. О компьютерной системе тестового контроля знаний в БГТУ	129
Ю.В. Полозков. Методика аналитического расчета параметров видеооцифровки нерегулярных поверхностей	132
О. О. Пронжилло. Об использовании графовых моделей в курсах математики и информатики: состояние и перспективы	135
Т.В. Романюк. Стохастическая модель обработки исков в страховой компании	138
С. Рында, Д. Данилович, А. Лисовский. INTERNET-система тестирования учебных программ	142
А.А. Сарычев. Контролирующе-обучающая программа для решения задач линейного программирования симплекс-методом	144
В.В. Седельник. Программный комплекс визуализации картографических данных системы моделирования процессов нефтедобычи	146
Н.В. Семенчук. Анализ моделей долгосрочного страхования жизни	149
П.Н. Стрибук. Метод исследования причинно-следственных связей в социальных и природных системах	151
П.Н. Стрибук. Метод и средства одномерного анализа данных при исследовании социальных и природных объектов	155
А.И. Стуляк, В.С. Скрашук, П.В. Картавец, В.С. Никитенко, А.Н. Ваглай. Образовательный сервер факультета платформесервера приложений Zope	158
О.Г. Шапко, К.Л. Пылило. Линейное программирование в финансовом анализе и планировании	163
О.Г. Шапко. Использование системы алгебраических уравнений в финансовом анализе и планировании	166
Д.К. Яцушкевич. Матрицы в уравнениях межотраслевого баланса	169

Научное издание

«СОВРЕМЕННЫЕ ПРОБЛЕМЫ МАТЕМАТИКИ И ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ»

Материалы II региональной конференции молодых
ученых и студентов 28-30 ноября 2001 г.



Ответственный за выпуск: Рубанов В.С.
Редактор: Строкач Т.В.
Технический редактор: Никитчик А.Д.
Лицензия ЛВ №382 от 1.09.2000 г.

Подписано к печати 8.11.01. Формат 60x84 1/16 Бумага писч. Гарнитура Т.Н.Р Усл. п.л. 102.
Уч. изд. л. 11,0 Тираж 100 экз Заказ № 602. Отпечатано на ризографе УО «Брестский
государственный технический университет». 224017, ул. Московская, 267